How the IoT Affects Multibusiness Industrial Companies: IoT Organizational Archetypes

Short Paper

Dominik Bilgeri
ETH Zürich
Weinbergstr. 56/58, CH-8006 Zürich
dbilgeri@ethz.ch

Elgar Fleisch
ETH Zürich
Weinbergstr. 56/58, CH-8006 Zürich
efleisch@ethz.ch

Felix Wortmann
University of St. Gallen
Dufourstr. 40a, CH-9000 St. Gallen
Felix.Wortmann@unisg.ch

Abstract

Innovative technologies, including sensors, cloud-based data analytics and artificial intelligence, are altering the logic of how manufacturing companies conduct business. More specifically, the Internet of Things (IoT), and hence the transition from offering physical products to providing digital solutions, alters manufacturers' manner of value creation and value capturing. Against this background, manufacturers are forced to extend their value creation activities beyond the design, production, operation, and maintenance of complex physical products. Manufacturing companies with multiple business units operating in various industry segments are particularly challenged to realize the potential of IoT. With their diverse set of business activities and their complex IT landscapes, these companies need suitable IoT organizational structures to benefit from effective IS utilization. Based on a multiple case study, we identify six IoT organizational archetypes that depict how multibusiness manufacturing companies allocate and integrate IT capabilities within their organizational structures. In addition, we investigate a set of six influential factors that drive archetype adoption.

Keywords: Internet of Things, Multibusiness Manufacturers, Organizational Archetypes

The ability to provide IoT solutions

The Internet of Things (IoT), and hence the transition from offering physical products to providing digital solutions, will require executives to rethink their companies' manner of conducting business in terms of value creation and value capturing[1]. In fact, multibusiness manufacturing companies are forced to extend their value creation activities and integrate the design, production, operation, and maintenance of complex physical products with the design, development, operation, and maintenance of digital components (Porter and Heppelmann, 2015). In addition to the traditional value proposition of the physical product (e.g., lifting materials in the case of a crane), manufactures can also capitalize on digital services (such as predictive maintenance) (cf. Konecranes, 2017). To realize the potential of smart, connected products and services, companies have to put effective governance in place. This includes IT governance, which is a fundamental

[1] Value creation and value capturing define two essential concepts in strategic management research, referring to companies' ability to create superior value for customers and "the ability to capture [a proportion of this] value in the form of profits" (Morgan & Finnegan, 2014, p. 228).

prerequisite for systematically exploiting the potential of IT (Weill, 2004; Wu et al., 2015). To implement effective governance, companies rely on a set of different mechanisms, such as committees, budgeting processes, approvals, and organizational structure (Wu et al., 2015). Within the research at hand, we focus on the latter. We argue in line with previous studies that the organizational structure is critical to successfully address the changing business environment the Internet of Things poses to manufacturing companies (Reynolds and Yetton, 2015; Porter and Heppelmann 2015). Existing literature identifies three core IT capabilities required to successfully provide IoT solutions: (1) Enterprise IT capabilities are required to operate the core business and to enable integrated, efficient, and reliable business processes; (2) Consumer IT capabilities are about empathizing with end users and providing easy to use and hassle-free solutions to address their needs; (3) Embedded IT capabilities refer to the development and integration of software embedded in hardware products (Peppard and Ward, 2016). Building upon this typology, we investigate how multibusiness manufacturing companies allocate and integrate IT capabilities within their organizational structures.

Manufacturing companies are constantly under pressure to decrease costs and utilize the value of their IT resources, or, in other words, to utilize IT synergies. This is a particularly salient challenge for multibusiness manufacturing companies, which often possess multiple business units operating in different industry segments. Due to industry-specific environmental constraints, business units usually strive for autonomy in terms of their individual IT resources, including IT infrastructures, strategies, stakeholder relations, and personnel. Such decentral allocation of responsibilities, which is often accompanied by a lack of coordination of overall IT activities, involves the risk of significant duplication across business units (Tanriverdi, 2005). Much of this redundancy could be avoided, considering universally applicable IT infrastructure and fundamental principles of good IT management proofing appropriate and valuable across different industries. Several studies have provided evidence that multibusiness companies can significantly benefit from cross-business unit IT synergies (Tanriverdi, 2006).

However, existing research lacks a clear understanding of how the different IT capabilities required to provide IoT solutions are allocated within multibusiness manufacturing companies[2]. Most of the previous studies focus on non-manufacturing industries (e.g., banking) and exclude embedded IT from their analysis or do not reflect recent digitalization developments that often lead to structural separation in practice, i.e., the allocation of IT responsibilities to new organizational units. Against this background, we focus on IoT value creation and provide insights on how multibusiness manufacturing companies allocate and integrate different IT capabilities within their organizational structures[3]. In addition, we offer practitioners an overview of influential factors underlying companies' choices of archetypes. More specifically, we address core questions that executives at many manufacturing companies currently face: *Should manufactures, or should they not, form a new organizational unit dedicated to IoT? And if so, how should its relationship to corporate IT be defined?* We explore these questions by applying a qualitative multi-case study approach. In total, we conducted 16 in-depth interviews with experienced experts from ten multibusiness manufacturers representing well-known international conglomerates and hidden champions.

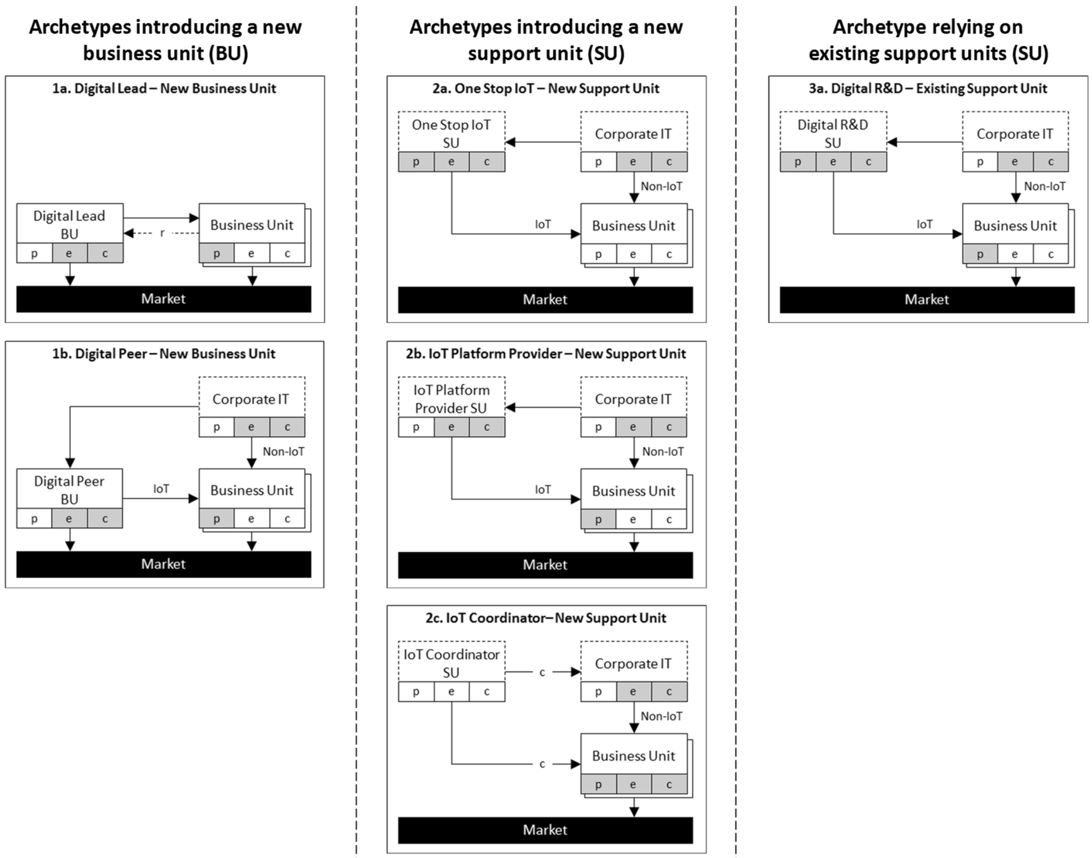
IoT organizational archetypes

Our analysis reveals that large manufacturing companies rely on six organizational archetypes to govern their IT capabilities. The archetypes can be divided into three categories, with their core differentiation referring to the characteristic of the organizational unit holding IT responsibilities in addition to the corporate IT unit. The first category comprises two archetypes that are based on a newly created IoT business unit (BU) with market access. The second category comprises three archetypes that are based on a newly created IoT support unit (SU) without market access. The third category contains the archetype that is based only on existing organizational units. The archetypes are depicted in Figure 1.

---

[2] While earlier studies, including the seminal contribution of Weill and Ross (2004), are well suited to inform our research, we argue that the IoT confronts manufacturers with new organizational challenges.

[3] Focusing on value creation, value capturing is out of scope of this paper. The literature on "Industry 4.0" extensively discussed two fundamental methods for multibusiness manufacturers to capture value of IoT solutions. They can either use the monetization potential associated with external customers or benefit from IoT solutions through internal process optimization. Two interesting publications include Clemons et al. (2017) and Trantopoulos et al. (2017).



Units:	BU – business unit (boxes in solid lines); SU – support unit (boxes in dotted lines)
IT capabilities:	p – embedded (physical) IT capabilities; e – enterprise IT capabilities; c – consumer IT capabilities; shaded capabilities indicate that the respective unit possesses related capabilities
Relationships:	Arrow indicates supplier relationship; c – coordinates (the support unit in archetype 2c acts as a coordinator); r – reports into (BUs' IT management in 1a also reports to head of digital lead BU)

Figure 1. IoT organizational archetypes

The first two archetypes (labeled 1a and 1b in Figure 1) are characterized by the introduction of a new IoT business unit (BU). This new organizational unit focuses on delivering a broad portfolio of IoT offerings to both internal and external customers. These offerings include IoT services such as consulting, IoT applications, and, most importantly, an IoT platform. The latter refers to providing "a comprehensive set of application-independent functionalities that can be utilized to efficiently build IoT applications" (Wortmann and Flüchter, 2015, p. 223). First and foremost, the platform is used by the established BUs to build IoT applications for their own customers. The central distinctions between the two archetypes Digital Lead and Digital Peer concern the BU's relationship with corporate IT and its leadership model. For instance, at case company Industry B Inc., which applies the archetype Digital Lead, corporate IT was merged into the newly created IoT BU after the IoT BU had established itself. The unit is led by an empowered chief digital officer (CDO), who is part of the management board (cf. Tumbas et al., 2017). Moreover, the top IT managers of the BUs also report to the CDO. In contrast, applying archetype Digital Peer, case company Automotive Supplier Inc. has a distinct corporate IT unit. Hence, the newly created BU acts as the internal and external IoT service provider, relying on fundamental IT resources provided by corporate IT. Corporate IT remains the internal IT supplier for all non-IoT services. For both archetypes, the main responsibility for embedded IT lies with the established BUs.

The next three archetypes (labeled 2a, 2b and 2c in Figure 1) are characterized by the introduction of a new IoT support unit (SU). Established BUs are offering IoT applications to their customer segments, whereas the new IoT SU does not have its own market responsibility. Instead, it focuses on the exploitation of IT synergies across the IoT-related BU activities. The degree of vertical integration of IT capabilities within this new SU varies across the three archetypes, being the highest for *One-stop IoT*, intermediate for *Platform Provider* and lowest for *Coordinator*. At the core of the archetype One-stop IoT is a SU with embedded, enterprise, and consumer IT capabilities. It offers IoT services to BUs that do not have any IT capabilities. For instance, the business units of case company Polymer Inc. did not offer products with embedded IT capabilities until recently, when it started implementing a new IoT product strategy. Hence, there was no need for the BUs to develop corresponding IT capabilities. The archetype Platform Provider takes into account that the established BUs already have embedded IT capabilities. Hence, the centralized IoT SU is focused on IoT-related enterprise and consumer capabilities, as is the case for companies Automation A Inc., Automation B Inc., Automotive Inc., and Chemistry Inc. The SU provides an IoT platform to the established BUs, on top of which they can build IoT applications for their customers. However, the SU is closely collaborating with third parties, utilizing existing commercial off-the-shelf solutions to provide its internal IoT platform offering. The third archetype Coordinator captures the case in which the established BUs have already developed substantial IoT solutions and respective capabilities in recent years. Hence, the new SU focuses on coordination without providing operational IoT services to the BU. The SU aligns BU-specific IoT activities and ensures cross-BU synergies. Its capability set is not focused on embedded, enterprise, or consumer IT capabilities, but rather on generic product management as well as business and organizational development capabilities.

Finally, the archetype *Digital R&D* (labeled 3a in Figure 1) relies on existing support units. In this archetype, established BUs offer IoT applications to their customer segments and an existing SU is entrusted with new IoT responsibilities to exploit synergies between IoT-related BU activities. Two companies in our sample, Lighting A Inc. and Lighting B Inc., implemented this archetype and have enhanced their R&D units' responsibilities. Hence, their R&D units now also act as internal IoT service providers, relying on fundamental IT resources provided by corporate IT. These digital R&D units closely collaborate with BUs and their embedded IT teams to develop and operate IoT solutions.

Influencing factors driving archetype adoption

To gain a better understanding of multibusiness manufacturers' preferences for specific IoT organizational archetypes, we identified a set of six influential factors that drive archetype adoption on the basis of three key contextual concepts, i.e., organization, culture, and strategy (Weill and Olson, 1989). All or a selection of these influential factors drive the choice for each IoT organizational archetype as shown in Table 1.

The first two factors that we identified are related to the respective organization and its capabilities[4]. A large majority of study participants highlighted that the *existence of a fundamental set of embedded IT capabilities* within their organizations is a key influential factor for their companies' choices. Thus, in a first step, it is not relevant whether the capabilities are anchored in a central unit or in BUs. The case company Polymer Inc. is the only company in our sample without any IoT experience. Polymer Inc. had to start from scratch in implementing its IoT strategy and bundled all three types of IT capabilities in a newly created SU to ensure sufficient initial momentum. In contrast to Polymer Inc., companies might also face the opposite situation in terms of existing capabilities. Industry A Inc., for example, had already developed substantial IoT solutions and corresponding capabilities across its BUs in recent years. Hence, the company's organization was characterized by *strong decentralized capabilities to provide IoT solutions*. To realize synergies without major disruptive reorganizations, Industry A Inc. decided to introduce a new SU to coordinate IoT activities across BUs. Other companies in our sample (e.g., Automation A Inc., Automation B Inc., Automotive Inc., and Chemistry Inc.) had only limited decentralized IoT-related capabilities within their BUs. Hence, they made the decision to develop the missing capabilities in a central IoT SU.

We identified two further factors in the context of strategy[5]. The first factor is related to the *separation of IoT and the creation of a centralized IoT-only unit*. Although it is a viable option that missing IoT-related capabilities are developed within well-established units (such as corporate IT, R&D, or BUs), most of the

[4] The term *capability* refers to the "ability of an organization to perform a coordinated set of tasks, utilizing organizational resources, for the purpose of achieving a particular end result" (Helfat and Peteraf, 2003, p. 999).

[5] We define *strategy* as the position a company wants to achieve within an environment as well as the plan (i.e. "how") to get there. For further details, see Mintzberg (1987).

companies in our sample opted against this approach and created new dedicated IoT units. Core arguments for this strategic choice are the desire to secure sufficient IoT management attention, gain transparency about IoT initiatives, and bundle complementing capabilities. While a clear separation ensures that IoT does not end up as "one of many topics" within existing units, a dedicated IoT unit might not be beneficial in terms of synergies. The second strategic factor is related to diversification. According to Ansoff's seminal work on different product-market expansion strategies, companies can develop new products, enter new markets, or follow both paths simultaneously (Ansoff, 1987). Firms applying the latter strategy are pursuing market diversification. Whereas all case companies in our sample indicated their desire to generate new solutions and potentially enter new markets, most of them emphasized the importance of the IoT to increase internal efficiency and to address existing customers with new offerings. Only Industry B Inc. and Automotive Supplier Inc. followed a distinctive *IoT platform diversification strategy* with a strong focus on diversification. Both companies implemented this strategy by introducing a new BU.

				Influential factors				
			Existing capabilities		Strategy		Culture	
			Fundamental set of embedded IT capabilities	Strong decentralized capabilities for IoT solutions	IoT platform diversification	Separation of IoT, centralized IoT-only unit	Entrepreneurial & market-based organizational culture	Entrepreneurial and market-based IT culture
Archetypes	New BU	Digital Lead	yes	no	***yes***	no	***yes***	no
		Digital Peer	yes	no	***yes***	yes	***no***	no
	New SU	One-stop IoT	***no***	no	no	***yes***	-	no
		Platform Provider	yes	***no***	no	***yes***	-	no
		Coordinator	yes	***yes***	no	***yes***	-	no
	Exist. SU	Digital R&D	yes	no	no	***no***	-	***no***

Legend: - = not applicable; highlighted in bold = of particular relevance for case companies' archetype adoption

Table 1. Influential factors for IoT organizational archetype adoption (cf. Xue et al., 2008)

Finally, two factors are related to organizational culture[6]. The case studies provide evidence that in case of an IoT platform diversification strategy, an *entrepreneurial and market-based organizational culture* that is risk-taking and performance-oriented can foster the adoption of a digital lead BU. In line with their execution-oriented performance culture, case company Industry B Inc. introduced a digital lead BU to enforce the rapid delivery of innovative IoT solutions throughout the established BUs. The digital lead BU is managed by a C-suite manager with strong reporting lines into the established BUs. In contrast, case company Automotive Supplier Inc. is characterized by a more consensus-oriented culture and implemented a digital peer BU that is less assertive and acts internally as an IoT-provider for the established BUs. Finally, IT culture, i.e., the pattern of shared values and beliefs present in the corporate IT department, is an important factor that influences archetype selection. All case companies discussed whether corporate IT could be the central entity to coordinate and enable IoT across the organization. However, the case companies in our sample perceived their existing IT culture as a core obstacle to IoT success and hence did not empower their existing IT departments. More specifically, they articulated a lack of *entrepreneurial and market-based IT culture*. The decisions of Lighting A Inc. and Lighting B Inc. underpin this particularly well. These companies ultimately decided to empower corporate R&D rather than corporate IT.

Implementing effective IoT organizational structures

Recent IS research emphasizes the importance of IT governance, however its proper implementation remains a challenge for most organizations (Weill, 2004). Against this background, we aim to formulate actionable guidelines that provide executives with useful recommendations regarding a specific governance

[6] We define *organizational culture* as "the pattern of shared values and beliefs that help individuals understand organizational functioning and thus provide them with the norms for behavior in the organization" (Deshpande and Webster, 1989, p. 4).

mechanism, i.e., organizational structure. Analogous to several previous studies, we develop these recommendations based on our rich interview data and analytically derive them from our study results.

Overall, there is no "one best solution". In essence, our results suggest that if companies start their IoT journey from scratch and do not possess any embedded IT capabilities, it might be reasonable to bundle all IoT-related capabilities in a single new SU to gain sufficient momentum (One-stop IoT). In contrast, when BUs have already developed substantial IoT solutions and respective capabilities, a central SU (Coordinator) that focuses on cross-BU coordination to ensure synergies can be implemented. In case BU capabilities are less developed or less closely aligned, bundling these capabilities in a central SU (Platform Provider, Digital R&D) enables utilization of significant synergies. Finally, implementing a dedicated IoT BU that also serves as an internal IoT service provider is a viable option for an IoT platform diversification strategy (Digital Lead, Digital Peer). Practitioners should be aware that capabilities and organizational setups are two separate concepts. Hence, the necessity of newly allocating IT capabilities to master IoT should not be misinterpreted as an argument for the introduction of different IT units, each with a single dedicated IT capability. Rather, we encourage executives to differentiate between distinct IT capabilities and carefully reflect on how to allocate and integrate them within their companies' organizational structures. More specifically, our analyses reveal critical design dimensions that are relevant in practice when implementing IoT organizational archetypes.

Choose a dedicated strategy of separation or integration of IT capabilities

Regarding the first research question, whether manufactures should form a new organizational unit dedicated to IoT, our case studies demonstrate that the majority of companies choose to separate IoT activities (i.e., smart, connected products) from other IT efforts (i.e., enterprise systems, etc.) in an early phase of the digital transformation to gain sufficient initial momentum[7]. In addition, companies must make a strategic decision on whether they want to fundamentally diversify their service portfolio based on an IoT platform offering such that a dedicated IoT business unit is justified.

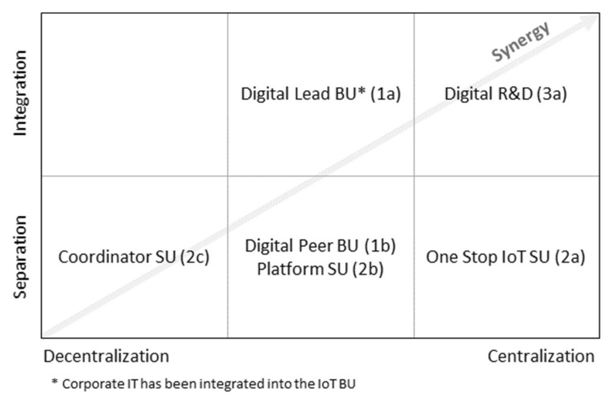


Figure 2. IoT archetypes according to IoT separation and centralization

As displayed in Figure 2, most of the identified archetypes centralize a substantial part of the IT capabilities that are core to IoT in a central unit to realize synergies across BUs. However, these capabilities are most often not integrated into existing corporate units, such as corporate IT or corporate R&D, but rather separated into a dedicated corporate IoT unit. Most companies assume that separation has a positive impact on value creation and efficiency, both known antecedents of organizational performance (Rivard et al., 2006). The interviewees highlighted that separation increases customer focus, IoT awareness, and the agility to deliver IoT services by introducing a dedicated centralized IoT unit. Furthermore, they noted that such a unit can also mitigate cultural conflicts between existing IoT units. Finally, we gathered first evidence that with general diffusion of IoT-related capabilities, the positive effects of separation might diminish.

[7] From a strategic perspective, structural separation has been intensely discussed in ambidexterity literature. For a profound overview, see Gibson and Birkinshaw (2004).

Clearly define the relationship to corporate IT

Manufacturing companies, which decide to introduce a new unit dedicated to IoT are then required to define its relationship to corporate IT. Regarding the second research question, several companies in our sample emphasized a rising rivalry between corporate IT units and newly introduced entities dedicated to IoT activities (cf. Bilgeri et al., 2017). The interviewees elaborated on three existing scenarios how to define the relationship between the corporate IT unit and the newly emerged IoT unit. In the first scenario, one organizational unit is responsible for both IT and IoT related activities (see archetype 1a in Figure 1). This allows for an optimal use of resources, but it remains doubtful whether classic IT units can fit themselves into such a complementary role, without slowing speed in IoT domains. Our case companies apparently have had similar concerns, with only one organization applying this archetype. In the second scenario, the corporate IT unit supports the newly implemented IoT unit with back-end operations, while at the same time offers all non-IoT activities to business units (see archetypes 1b, 2a, 2b and 3a in Figure 1). This allows multibusiness manufacturing companies to use the resources available in their corporate IT and benefit from new units to gain speed in IoT domains. Finally, in the third scenario, the new IoT unit acts as a coordinator, aiming to manage and align the interaction between corporate IT and business units as well as between business units (see archetype 2c in Figure 1). For companies with decentralized IoT-related capabilities this can ensure strategic adherence and identification of synergy potential.

Be aware of the need for adaptation over time

Overall, it is important to mention that the cases are snapshots of setups at a specific point in time and interviewees expect them to be subject to change. More precisely, with increasing IoT experience, new organizational archetypes might emerge and existing ones might become obsolete. Indeed, there is early evidence that companies strive for more synergies with increasing experience. Industry B Inc., applying the Digital Lead archetype, has integrated corporate IT into the IoT BU to increase synergies. Automotive Supplier Inc., which is currently applying the Digital Peer archetype, considers splitting the central IoT BU and moving domain-specific capabilities into BUs and cross-BU expertise into corporate IT.

About this research

This paper is part of a larger research project. The study at hand employs a qualitative multiple-case-study method and is of an explorative nature (Eisenhardt, 1989; Yin, 2013). Such an approach is well suited to investigate how and why research questions. We apply a two-step procedure to obtain the presented results. In a first stage, eleven informal conversations with managers and executives of various large companies across the IoT ecosystem of multibusiness manufactures were conducted, aiming to select particularly important themes to be discussed with interviewees. In combination with the latest insights from related research, this information built the foundation for the case study interview guideline. In the second stage, ten case studies were analyzed. The case studies were selected by applying the following criteria: 1) the corporations are established multibusiness manufacturing companies; 2) the manufacturing companies have had digital transformation on their corporate agenda for at least five years and are currently within the process of digital transformation; 3) all corporations have already included or are in the process of offering IoT solutions as part of their portfolios; 4) the participating interviewees are experienced experts holding different functions and positions and hence are capable of providing deep insights into the organizational structures of their organizations. Since the organizational structure and potential plans to change it are perceived as critical company information to gain competitive advantages in an IoT context, all participating companies and a large majority of interviewees insisted on staying fully anonymous.

Table 2 lists the 16 in-depth expert interviews conducted. While the majority of them were held face-to-face to obtain good-quality data, some individual interviewees were only accessible via phone. The second-stage expert interviews were conducted in English or German and were audio-recorded and fully transcribed to ensure completeness and accuracy of the data. Two interviews could not be recorded. In one case due to the company's compliance restrictions and in the other case the interview was conducted at a symposium. For these interviews, the authors created field keyword notes. Data triangulation was performed by analyzing additional sources of information, including companies' websites, brochures, and internal presentations. Three researchers examined the data independently, in a first phase investigating each case individually, and in a second phase comparing the companies through a cross-case analysis. This approach aimed to identify organizational archetypes by applying a qualitative content analysis method and to analyze the interviews based on inductive archetype building, utilizing a systematic, rule-and-theory-based procedure (Mayring, 2002). To derive IoT organizational archetypes, the authors independently coded the archetypes using a common coding scheme (see Figure 1). The coding of an archetype followed a three-step procedure. First, key organizational units that are core to IoT value generation were identified. Second, the identified organizational units were characterized in terms of their IT capability types. Finally, the supplier-provider relationships between the identified units and the market was coded. The categorization process was iterative in nature. The authors compared the archetypes and agreed on five out of the six archetypes. By jointly reviewing the existing interview documentation, an agreement regarding the controversial archetype was reached. The identified archetypes were discussed and verified with a subset of the interviewees.

No.	Case	Number of employees	Interviews (Partners)	Roles (anonymized)
1	Industry A Inc.	More than 300'000	3(3)	Vice President Innovation, Head of Business Development, Manager Digital Company
2	Automotive Supplier Inc.	More than 300'000	3(3)	Product Owner of IoT Solution, IoT Initiative Project Lead, Head of Digital Solutions
3	Industry B Inc.	More than 300'000	1(1)	Chief Digital Officer
4	Chemistry Inc.	From 100'000 to 199'999	2(2)	Manager BM Development, Sen. Digital Business Developer
5	Automotive Inc.	From 100'000 to 199'999	1(1)	IT Manager
6	Automation A Inc.	From 100'000 to 199'999	1(1)	Head of Digital Operations
7	Lighting A Inc.	From 100'000 to 199'999	1(1)	Director Alliance Management
8	Polymer Inc.	From 20'000 to 49'999	2(2)	Team Digitalization & Industry 4.0, Head of Digital
9	Lighting B Inc.	Less than 20’000	1(1)	Executive Vice President Services
10	Automation B Inc.	Less than 20’000	1(1)	Chief Technology Officer

Table 2. List of case companies and interviews conducted

Limitations and next steps

The results of this study should be assessed in light of its limitations. Building upon a convenience sample, our selection of case companies was small and opportunistic, thus restricting our ability to generalize. However, the companies in our sample represent large manufacturing companies, including well-known global players and hidden champions from various industries at the forefront of digital transformation. The setting allowed us to obtain in-depth data and rich stories regarding a sensitive topic. In addition, although case study research is well suited for explorative studies and complex processes across various organizational units, other methodological means as well as the consideration of smaller firms might provide further insights. A second limitation is that whereas we have emphasized the role of six influential factors that drive archetype adoption, other factors may also be influential, possibly including companies' positions within their environment. Future research that empirically validates the identified influential factors and additional influential factors as well as their impact on archetype adoption is needed. Finally, this short paper focuses on a specific governance mechanism identified in previous studies as critical to successfully addressing new challenges in an IoT context.

In fact, we hope that this short paper can build a fruitful foundation for further extended studies. We identify several promising research avenues for us and fellow researchers to further investigate this interesting phenomenon. In a next step, we aim to advance our research by gaining a deeper understanding of additional governance mechanisms and their suitability to successfully manage IoT initiatives in multibusiness manufacturing companies. In this regard, our data indicates a high relevance of deviating collaboration models to orchestrate IT capabilities across different organizational units (e.g., between centralized corporate units and more decentralized business units). In addition, we strongly encourage scholars to investigate the unique ability of specific IoT organizational archetypes to enable manufacturing companies to realize new means of value creation and value capturing[8]. Thereby, we suggest paying specific attention on IoT separation as described in this paper.

[8] Existing literature offers fruitful means to inform such research, see for instance Miles et al. (1978).

Acknowledgments

We thank the ICIS review team, Timo Gessmann and Jannis Beese for their valuable feedback as well as express our gratitude to all participating companies. This research is supported by the Bosch IoT Lab.

References

Ansoff, H. I. (1987). *The concept of corporate strategy*. Homewood, IL: Irwin.

Bilgeri, D., Wortmann, F., and Fleisch, E. (2017). How Digital Transformation Affects Large Manufacturing Companies' Organization, *ICIS 2017*, Seoul, South Korea.

Clemons, E. K., Dewan, R. M., Kauffman, R. J., & Weber, T. A. (2017). Understanding the Information-Based Transformation of Strategy and Society. *J. Manag. Inf. Syst.*, 34(2), 425-456.

Deshpande, R., & Webster Jr, F. (1989). Organizational culture and marketing. *J. Mark.*, 53(1), 3-15.

Eisenhardt, K. (1989). Building theories from case study research. *Academy of Mgmt. Rev,* 14(4), 532-550.

Gibson, C. B., & Birkinshaw, J. (2004). The antecedents, consequences, and mediating role of organizational ambidexterity. *Academy of management Journal*, 47(2), 209-226.

Helfat, C. E., & Peteraf, M. A. (2003). The dynamic resource-based view: Capability lifecycles. *Strategic Management Journal*, 24(10), 997-1010.

Konecranes (2017). *KONECRANES RENTALL. You don't always have to buy a crane*. Retrieved from http://www.konecranes.com/equipment/overhead-cranes/konecranes-rentall.

Mayring, P. (2002). Qualitative content analysis – Research instrument or mode of interpretation? in *The role of the researcher in qualitative psychology*, M. Kiegelmann (ed.), Ingeborg Huber, 139–148.

Miles, R., Snow, C., Meyer, A., & Coleman Jr, H. (1978). Organizational strategy, structure, and process. *Academy of Management Review*, 3(3), 546-562.

Mintzberg, H. (1987). The strategy concept I: Five Ps for strategy. *California Mgt. Rev.*, 30(1), 11-24.

Morgan, L., & Finnegan, P. (2014). Beyond free software: An exploration of the business value of strategic open source. *Journal of Strategic Information Systems*, 23(3), 226-238.

Peppard, J., & Ward, J. (2016). *The Strategic Management of Information Systems: Building a Digital Strategy*, Chichester: John Wiley & Sons.

Porter, M. E., & Heppelmann, J. E. (2015). How Smart, Connected Products Are Transforming Companies. *Harvard Business Review,* 93(10), 96-114.

Reynolds, P., & Yetton, P. (2015). Aligning business and IT strategies in multi-business organizations. *Journal of Information Technology*, 30(2), 101-118.

Rivard, S., Raymond, L., & Verreault, D. (2006). Resource-based view and competitive strategy: An integrated model of the contribution of information technology to firm performance. *The Journal of Strategic Information Systems*, 15(1), 29-50.

Tanriverdi, H. (2005). Information technology relatedness, knowledge management capability, and performance of multibusiness firms. *MIS Quarterly*, 29(2), 311-334.

Tanriverdi, H. (2006). Performance effects of information technology synergies in multibusiness firms. *MIS Quarterly*, 30(1), 57-77.

Trantopoulos, K., von Krogh, G., Wallin, M. W., & Woerter, M. (2017). External Knowledge and Information Technology: Implications for Process Innovation Performance. *MIS Quarterly*, 41(1), 287-300.

Tumbas, S., Berente, N., & vom Brocke, J. (2017). Three Types of Chief Digital Officers and the Reasons Organizations Adopt the Role. *MISQ Executive*, 16(2), 121-134.

Weill, P. (2004). Don't just lead, govern: How top-performing firms govern IT, *MISQ Executive*, 3(1), 1-17.

Weill, P., & Olson, M. H. (1989). An assessment of the contingency theory of management information systems. *Journal of Management Information Systems*, 6(1), 59-86.

Weill, P., & Ross, J. (2004). *IT governance: How top performers manage IT decision rights for superior results*. Harvard Business Press.

Wortmann, F., & Flüchter, K. (2015). Internet of Things - Technology and Value Added. *Business & Information Systems Engineering*, 57(3), 221-224.

Wu, S. P. J., Straub, D. W., & Liang, T. P. (2015). How information technology governance mechanisms and strategic alignment influence organizational performance. *MIS Quarterly*, 39(2), 497-518.

Xue, Y., Liang, H., & Boulton, W. R. (2008). IT governance in IT investment decision processes: The impact of investment characteristics, external environment, and internal context. *MIS Quart.*, 32(1), 67-96.

Yin, R. (2013). *Case study research: Design and methods*. Thousand Oaks: Sage.