Stuck in Pilot Purgatory: Understanding and Addressing the Current Challenges of Industrial IoT in Manufacturing

Nico Abbatemarco
SDA Bocconi School of Management
nico.abbatemarco@sdabocconi.it

Severino Meregalli
SDA Bocconi School of Management
severino.meregalli@sdabocconi.it

Aakanksha Gaur
SDA Bocconi School of Management
aasha.gaur@sdabocconi.it

Abstract

The Industrial Internet-of-Things (IIoT) is one of the most hyped concepts embedded in the Industry 4.0 paradigm. IIoT can provide a multitude of benefits to firms, such as enhanced productivity and better insight into company operations. Despite these benefits, manufacturing companies are considerably struggling to realize the potential of IIoT. Several consulting companies, such as McKinsey and Deloitte, coined the term "pilot purgatory" to define the state of being in which most IIoT projects get stuck. Based on a series of interviews with 12 experts in the field, this study identifies and addresses IIoT-specific challenges in manufacturing. Our study provides two main contributions. First, our analysis provides a broad, practice-based overview of IIoT challenges by considering both the technological, organizational and environmental contexts of manufacturing firms, following the TOE framework as a theoretical lens to structure the results. Second, we derive specific management guidelines for each of the identified challenges.

1. Introduction

Industry 4.0 is undoubtedly one of the buzzwords that dominated the digital transformation market in recent years [1, 2]. Several academic and practitioner studies highlighted its potential benefits; these range from a better understanding of the company's internal production processes [3, 4] to the increased integration of OT data with that of the rest of the company [5], from the reconfiguration of products in terms of programmability and traceability [6] to an expansion of the traditional business model towards new ones [7] such as manufacturing servitization, where *the manufacturer monitors the product on behalf of the customer and retains responsibility for product performance* [8].

In the vast majority of cases, the beating heart of Industry 4.0 initiatives is represented by the Industrial Internet-of-Things (hereafter IIoT) [9, 10]. The IIoT can be seen as an umbrella term for a set of technologies, both digital and physical, whose ultimate purpose is to collect data from a large number of connected industrial systems and use them as a catalyst to improve industrial performance [11]. Specifically, the IIoT could bring very tangible benefits to manufacturing companies even from the early stages of implementation, thanks to applications such as real-time monitoring, remote diagnosis, and predictive and proactive maintenance [12, 13, 14].

Yet, despite all the talk around Industrial IoT, many practitioners consider the IIoT to be still underrated and underapplied [15, 16]. Recent market analyses reinforce this evidence, highlighting how the IIoT's growth has been way slower than expected, and further impacted by the Covid-19 pandemic [17, 18, 19]. This slowdown can be (at least partially) explained thanks to a not-so-flattering concept: pilot purgatory, which implies *programs traveling at a snail's pace* [20]. Several consulting companies, such as Capgemini, Cisco, McKinsey, and Deloitte, highlighted how a relevant percentage of IIoT projects – around 75% - gets stuck in pilot mode for over a year, and approximately 30% of such projects for over two years [20, 21]. Therefore, despite its many potential benefits, the IIoT earned the reputation of being a complex technological object, difficult to adopt and even more to exploit successfully.

Thus, the purpose of the study is to understand:

RQ1. What are the key challenges that are hindering the adoption of the IIoT in manufacturing companies?

RQ2. Based on practitioners' experience, what recommendations/guidelines can help addressing such challenges?

URI: https://hdl.handle.net/10125/80170
978-0-9981331-5-7

To answer these questions, we interviewed a panel of IIoT experts, belonging to the European and Italian contexts, using the TOE framework as a guiding theoretical lens.

The structure of this work is as follows. First, in section 2 we provide a more detailed description of the IIoT and its role in the context of Industry 4.0 and in the manufacturing sector. Second, in section 3 we motivate the need for practice-based research in this area and explain the study's methodology as well as its data analysis process. In section 4 we present a comprehensive overview of the main challenges related to the adoption of IIoT technology in the manufacturing sector; then, in section 5 we propose a recommendation / guideline for each of these challenges. Finally, we discuss the macro-trends that emerged from the analysis of the various challenges and the limitations of the research in section 6.

2. Industrial IoT in Manufacturing and in the broader Industry 4.0 context

Boyes et al. [22] define the IIoT as *a system comprising networked smart objects, cyber-physical assets, associated generic information technologies and optional cloud or edge computing platforms, which enable real-time, intelligent, and autonomous access, collection, analysis, communications, and exchange of process, product and / or service information, within the industrial environment, so as to optimize overall production value.* Starting from this definition, it is possible to understand in detail what are the actual features that characterize the IIoT. From a technological point of view, IIoT is an umbrella term that comprises:

- a broad range of hardware devices that produce data as an input and / or react to data as an output (mainly sensors and actuators, but also drones and cobots);
- a wide set of wired and wireless communication technologies;
- a series of both hardware and software solutions to collect, process and analyze data (including but not limited to supervisory control and data acquisition systems - SCADA, distributed control systems - DCS, programmable logic controllers - PLC, manufacturing execution systems – MES, manufacturing operations management systems – MOM, application-specific machine learning algorithms, cloud and edge servers, etc.).

By simply looking at this technological perspective, it is easy to understand why the IIoT represents the core of Industry 4.0. Almost all technologies usually mentioned in relation to Industry 4.0 are included in a typical IIoT project, apart from only a few, such as Virtual and Augmented Reality.

The second part of the definition – *within the industrial environment* – helps to contextualize the IIoT with respect to the more generic IoT. While IoT refers to both the enterprise and customer contexts, the term IIoT refers exclusively to the enterprise world. However, IIoT does not solely refers to the manufacturing sector, as the name may suggest, but potentially to any industrial sector. Nonetheless, the manufacturing sector represents the biggest market for the IIoT, accounting for around 60% of the total [19, 23].

Finally, the third part of the definition highlights how the primary purpose of the IIoT is the optimization of the value of company production. In a short-term perspective, the benefits brought by the IIOT translate into an increased operational efficiency and an improved capacity of monitoring production processes; in the long run, the IIoT could even transform the way the company operates, increasing its understanding of the supply chain (both upstream and downstream) and even revolutionizing its business model [6, 7, 13, 14].

3. Methodology and Data Analysis

3.1. The TOE framework

To gain a comprehensive view on the challenges of IIoT adoption within the European context, and the Italian context in particular, this study builds upon the TOE framework developed by Tornatzky and Fleischer [24]. The TOE framework is specifically designed for enterprise-context adoption of new technologies and has been widely applied to examine technological innovation [25]. The TOE considers three dimensions: the technological, organizational, and environmental contexts.

The technological context describes the pool of both internal and external technologies relevant to the company, including elements such as their technical compatibility and complexity, the learning curve, the possibilities of experimentation with pilot / proof of concept projects [26, 27]. The organizational context describes a wide range of the firm's characteristics, including but not limited to its scope, managerial beliefs and supports, organizational culture, complexity of managerial structure, and quality of human capital [28, 29]. Finally, the environmental context describes the external factors to which the company is exposed in its specific sector, such as government incentives and regulations, customer

mandates, competitive peers' pressures, and vendor support [30, 31].

In this study, the TOE framework is used to examine the adoption of IIoT in the manufacturing sector. In recent years, several studies applied the TOE framework for similar purposes. For example, the works by Lin et al. [5] and Sivathanu [11] used the TOE framework to analyze the factors that drive Industry 4.0 respectively in the Chinese and Indian manufacturing contexts. Other works, such as that of Prause [32], used the TOE to identify the most relevant challenges of Industry 4.0 adoption, specifically in the Japanese context.

While other studies highlight the specific IIoT challenges in the Industry 4.0 context (including those that use different adoption models, such as Sisinni et al. [33]), practice-based research on the topic is still limited, and, as far as the authors are aware, no other study provides guidelines on how to address the pitfalls of IIoT adoption and implementation.

The rationale behind the research is therefore that, despite the hype behind Industry 4.0 and IIoT, there is still a considerable research gap regarding their challenges and the approaches to overcome them. One of the pioneering works in this area is that of Masood & Egger [34], who applied the TOE framework to identify challenges and provide a series of recommendations in relation to the use of Augmented Reality in Industry 4.0.

As a result of the above, we deem the TOE framework as an appropriate theoretical background to investigate the challenges of IIoT adoption in the manufacturing sector, and to provide guidelines and recommendations to address them.

3.2. Data collection and analysis

In order to get a holistic, state-of-the-art vision of IIoT, and to avoid focusing on firm-specific challenges, we decided to build on the knowledge of professionals with significant expertise in the field, following an expert panel approach as proposed by Boyce & Neale [37]. This choice seemed appropriate to collect *"rich and in-depth information about the experiences of individuals"* and to identify challenges and possible guidelines useful for the practitioner community.

Thus, for data collection, we conducted semi-structured interviews with 12 experts from 8 different companies in April-May of 2021. All the interviewees had more than 5 years of work experience in the field of IIoT and represented a wide range of technical and business backgrounds. The experts worked from companies belonging to three main groups:

- system integrators (SI): companies specialized in implementing, planning, coordinating, scheduling, testing, improving and sometimes maintaining a computing operation [35];
- enterprise software houses (ESH): software houses specialized in the production of enterprise application software including for example CRM, ERP and SCM software;
- data integrators (DI): companies specialized in creating software solutions for combining data residing in different sources and providing final users with a unified view of them [36].

Experts participating in the interviews were classified according to their company's group (SI, ESH, DI) and to their target customer's size. The profile of the interviewed experts is presented in the following table:

Table 1. Experts' profile and interview data

ID	Group	Company	Target customer	Expert profile	Duration
#1	DI	A	Mid / Large	Account Director	87:29
#2	DI	A	Mid / Large	Principal Data Scientist	87:29
#3	SI	B	Small / Mid	Innovation Lead	35:28
#4	SI	C	Small / Mid	Digital Transformation Advisor	37:12
#5	ESH	D	Large	Business Solutions Architect	91:31
#6	ESH	D	Large	Director of Business Development & Strategy	91:31
#7	ESH	D	Large	Sales Development Manager	91:31
#8	ESH	E	Large	Head of Presales	35:24
#9	SI	F	Mid / Large	Business Development Manager	41:33
#10	SI	F	Mid / Large	Partner	41:33
#11	SI	G	Mid / Large	Associate Executive Director	46:24
#12	SI	H	Small / Mid	Head of Innovation	48:36

We found semi-structured interviews particularly useful for the purposes of the study, as they allowed for an open exchange with the participants. Every interview followed a similar set of questions to guide the conversation, but eventually left room for the emergence of new ideas, as prescribed by Myers [38].

The interviews were conducted individually for each company to avoid distortion. To ensure internal validity, each interview was conducted by at least two of the three authors of the paper, with one of the authors being present during all interviews.

In total, approximately 420 minutes of interviews were transcribed. To analyze the transcribed data, each of the authors independently performed the coding process proposed by Saldaña [39]. Topic and structural coding were used to represent the answers as challenges and related guidelines and to iteratively aggregate them. The coding was performed

independently, but once identified, all the codes were discussed and conceptually refined by the three authors together. Once defined, the challenges were organized into the three macro-dimensions of the TOE framework. During the data analysis, the TOE framework proved to be an adequate tool as it made it possible to frame all the challenges that emerged from the discussions. In the following sections, we refer to the interviews according to their ID (e.g., I1).

4. The challenges of IIoT adoption

In this section, we present the challenges related to the adoption of the IIoT in the manufacturing sector in accordance with the TOE framework. Table 2 summarizes the results.

Table 2. Challenges of IIoT adoption

Context	Challenge
Technological	**1.** Increased cyber risk **2.** Aggregation of IIoT data and integration with legacy systems **3.** Edge-cloud balance **4.** Devices' interoperability **5.** Inadequate bandwidth capabilities of factories
Organizational	**1.** Unclear value of IIoT initiatives **2.** Undefined strategic approach to IIoT initiatives **3.** Frictions between IT and OT **4.** Cultural change **5.** Lack of adequate professional skills
Environmental	**1.** Fear of missing out

4.1. Technology context

One of the first evidence that emerged from the interviews is that, despite the IIoT showing several challenges from a technological point of view, none of these were indicated as prevalent by interviewees.

The most important technological challenge is cyber security, which was mentioned by all interviewees. The increased number of connections and access points brought by the IIoT exposes the company network to many more cyber risks than in the past. In recent years, several manufacturing companies were hit hard by cybersecurity attacks targeting their IIoT systems [40]. Despite this threat, an interesting finding was that the majority of our respondents (except four: I3, I4, I9, I10), considered cybersecurity as a minor challenge. Everyone agreed that cyber risk represents a great danger for manufacturing companies, but to date this does not seem to represent a big problem from an IIoT adoption point of view. The primary reason is the specific weight of the CISO and the cybersecurity unit in the company. Being often subjected to CIOs, or in any case often playing a secondary role in the management hierarchy, the CISO in most cases does not have the power to exercise a veto over the implementation of an IIoT project. Indeed, for small / medium enterprises (hereafter SME), the issue of cybersecurity is sometimes not perceived as a challenge simply because there is still no knowledge of cyber risk at all in the company (I3, I12).

Another argument about cyber risk is that, even in companies where it is perceived as relevant, there is often some distance between the security team and the business units. This can lead to equally negative outcomes, such as the practice of "gold-plating". In the European Union context, gold-plating is a term used *whereby the powers of an EU directive are extended when being transposed into the national laws of a member state* [41]. In a similar manner, gold-plating in cyber security means trying to answer to cyber risk with a disproportionate and costly effort, exceeding the real needs of the project: *"sometimes, we observe that the misalignment between security and business brings to gold-plating […]. The CISO does not knows the project and its requirements well because he does not really know his own company works. So, to stay on the safe side, he starts adding requirements upon requirements, to the point that many of them become redundant or don't even make sense in the specific context"* (I3).

The second most quoted challenge in the technological context concerns the aggregation of data from the IIoT world and the integration with classic corporate IS, in particular with ERPs. One of the advantages of the IIoT, cited in both academic and practitioner literature, is that of creating an application environment capable of communicating the insights generated in the OT environment to the rest of the existing enterprise IT infrastructure [5]. Most of the interviewees, especially those belonging to the ESH group, stressed that to get the most out of IIoT systems it is necessary to integrate them with existing legacy systems, for example with CRM if you intend to aim at customized production processes, with SCM to maximize flexibility of production, and in general with the ERP to monitor the whole supply chain. However, aggregating IIoT data is already a complex task itself: *"we still lack a standardized IIoT architecture, and this leaves to users and integrators the burden to put all the pieces of the IIoT puzzle together"* (I2). The respondents belonging to the SI group emphasized that developing an IIoT solution starting from the legacy IT is even more problematic and can very easily lead to the infamous pilot purgatory.

The third challenge is related to the use of edge computing. Due to the stringent requirements of some use cases in terms of latency, bandwidth and possibly

security (e.g. very heavy workloads, with very high transmission frequencies, involving critical data for the company), the IIoT requires sometimes to process data already on the factory floor. In such cases, edge computing plays a key role in the new IIoT infrastructure, as it complements what is possible to do with cloud computing. The major elements of complexity reported for this challenge (I1, I2, I4) related to how to identify the workloads to process locally, how to balance the resources between edge and cloud, and how to manage edge servers on the factory floor.

Finally, two minor challenges are those related to device interoperability and to the factory's data transmission capabilities. The increase of sensors and actuators deployed in the factory required by the IIoT seems to be the main reason for both challenges. In fact, on the one hand this boosts the chances that one or more of the devices will not be able to "talk" to all the others. The interoperability issue is particularly felt in the world of discrete manufacturing, traditionally characterized by the presence of very different machinery compared to the world of process manufacturing (I1, I2). On the other hand, the abundantly increased data flow generated by such sensors can put a strain on a factory's bandwidth and latency capabilities.

4.2. Organizational context

The first challenge is related to how IIoT creates value. Often constrained by budgets, SMEs' managers need to carefully select the innovation projects to promote, and the IIoT does not have an easy life. Although there is *"a fairly widespread perception that the use of assets and monitoring of processes could be improved"* (I3), the return of such projects is very difficult to measure compared to other options, such as the purchase of simply more powerful equipment.

For large corporations, the problem is often not so much that of the budget, but rather the lack of a holistic strategic approach. Many large companies start IIoT projects because *"managers just have it in their budget for 202x"* (I4), without any link to the long-term strategy and vision of the company. Furthermore, the wide variety of plant configurations that a large company has, might aggravates the issue. The deployment of IIoT with a top-down approach can easily be halted by differences between the various plants, while a bottom-up approach risks to end up with a localized solution that is impossible to scale in other plants (I3, I4, I5, I6).

The third organizational challenge is the integration and coordination between OT and IT. The IIoT is by its nature a hybrid project, which requires both the experience gained on the field by the OT and the tech skills of IT. However, the OT / IT mix can very easily turn into a trap. The main risk arises at the very moment in which the project is approved. If it is the COO who proposed the project, the CIO may perceive it as an invasion of his / her area of expertise (I3, I4): *"it's his vendors, he's the one who keeps the relationships with them, and then overnight he sees them walking around his company without his permission: it's an invasion!"* (I4). On the contrary, if the CIO proposes the project, the risk is that the IIoT project may not fit well with the needs perceived by the COO (I11, I12). However, the communication issues between IT and OT do not only concern the upper management but the entire units. Many companies are not aware of how much their units work as separate silos (I5, I7, I9, I10).

Another related theme is cultural change. Very often, OT experts are experienced figures who have a decennial experience on their production line; they can perceive the arrival of the IIoT as a threat, both for their job survival and for *"the usual way of doing things"* (I6). Also, their scepticism can be motivated by a certain difficulty in interacting with technological innovation, as they mainly belong to a generation less familiar with the latest digital technologies (I11). The idea of leaving the control of a production line that they have handled manually for years to automated ML algorithms can be unacceptable for them and generate opposition towards the IIoT project.

The final issue is the lack of adequate professional figures. The lack of skills can be perceived on several fronts in an IIoT project: on the factory floor (lack of automation engineers), in data management and integration (lack of data scientists / data science team), and on the IT side (lack of cyber security experts / communication technologies experts). The problem is further exacerbated by the fact that such skills must be complemented by practical experiences: *"you cannot only be prepared on technologies; you also have to understand what to do with them, and you need the seniority to take charge of the related risks"* (I5).

4.3. Environmental context

In terms of pressures from the surrounding environment, one theme that emerged strongly is that of the fear of missing out, i.e., the fear of not being able to grasp the benefits brought by the IIoT in time. This challenge is reflected in two ways, depending on whether the company is a SME or a large one.

For SMEs, this fear is linked primarily to the chance to get tax incentives. Several countries in the European context launched Industry 4.0 initiatives (e.g., the Industrie 4.0 initiative in Germany, the

Factory of the Future in France, the Piano Nazionale Industria 4.0 in Italy) encouraging SMEs to rejuvenate their production assets and to adapt to the new industrial models driven by digital technologies. However, in many cases these initiatives only provided SME with financial incentives to buy new equipment, not really bringing organic innovation to the manufacturing system: *"National Industry 4.0 incentives in many cases work like this: you buy a new and more powerful machine, and if it has even an infinitesimal part of digital tech, you can enjoy the tax hyper-amortization bonus. However, you haven't changed anything in the way you operate"* (I12).

On the other hand, the fear perceived by large companies is otherwise motivated. Large corporations are afraid of falling behind their main competitors, well aware of the competitive advantage that digital technologies may offer. For this reason, executives (and especially CIOs) often undertake IIoT initiatives in a hurry, without these being aligned with the company's digital transformation plans (I5, I6, I7, I8).

5. Practice-based guidelines for IIoT adoption

In this section, we propose some recommendations and guidelines to potentially address each of the previously described challenges, summarized in Table 3. These guidelines are based on the lessons learned from the cases discussed during the interviews, and further supported by academic and practitioner literature on the topic when available.

Table 3. Guidelines for IIoT adoption

Context	Challenge
Technological	**1.** Enforce basic security hygiene + avoid "gold-plating" practices + carry out periodic interventions **2.** Avoid starting from legacy IS + take advantage of IIoT-specific platforms and applications + build a shared data lake **3.** Identify best edge-cloud balance by testing different configurations **4.** Promote use of devices compatible with Open-source communication standards **5.** Upgrade bandwidth capabilities of factories
Organizational	**1.** Select use cases where IIoT has an edge **2.** Tailor IIoT approach to the readiness of the plants **3.** Promote common storytelling + foster integration with mixed teams **4.** Back cultural change with dedicated initiatives **5.** Hire talents, reskill employees, partner with universities and competence centers
Environmental	**1.** Align external pressures to long-term digital transformation strategy

5.1. Technology context

Cyber risk and cyber security perception

On one hand, companies that lack a cyber risk strategy should hurry to introduce it and enforce at least the basic security hygiene practices, whatever their rate of technological innovation (I3, I4, I12). Cyber risk is no longer avoidable in the current world [40], and facing it represents a step that companies should have already taken a few years ago.

On the other hand, companies that already consider cyber security as a serious concern should avoid treating it as a due diligence, standardizable task. To avoid practices such as gold-plating, the CISO should frequently speak with the business units so to be able to tailor the cyber security policies based on its specific organization. This is even more relevant in manufacturing than in other sectors, as the diversity that can exist between various production plants implies that each plant might need a cyber security customization (I3, I11). Furthermore, the company should consider that the role of the CISO does not ends with the definition of the initial projects' requirements. The CISO will have to continuously carry out periodic interventions, such as penetration testing and system updating and patching: otherwise, cybersecurity will *"exist only on paper"* (I4), therefore becoming obsolete in a very short time (I3, I4).

Integration of data between IIoT systems and traditional enterprise systems

Companies should avoid starting from legacy systems when first implementing an IIoT project. This recommendation does not refute the effectiveness of connecting IIoT systems and traditional enterprise systems in the long run. However, the advantages of this option (e.g., increased flexibility of production systems, possibility of customizing production based on specific customer needs) will only be relevant in long-term term, while a stand-alone implementation of IIoT can already lead to considerable benefits in the short-medium term (I1, I2, I3, I4, I9, I10, I12). For example, many big players specialized in IIoT solutions (such as Bosch, ABB, Schneider Electric, …) have already released independent platforms and applications capable of generating valuable insights by themselves. Also, this choice does not prevent an integration in the future. The interviewees of the DI group proposed an interesting compromise in this sense: when introducing IIoT, companies should also lay the foundations for a homogeneous data lake, so that in the future all business applications, both IIoT

and legacy, can feed (and feed from) this common source.

Edge – Cloud balance

First, companies should identify which workloads require low latencies, closed loops, and actionable insights in real time to gain process efficiency (I9, I10), so as to define which ones will require the use of edge resources. Then, companies should execute each workload with different edge-cloud configurations, test the results and verify which ones allow to optimize resources without having repercussions on the use case (I1, I2, I12). Indeed, great differences between plants, especially in terms of bandwidth availability and workload characteristics, could create an incentive to optimize the cloud-edge balance in a customized way for each factory (I3).

Device interoperability and bandwidth constraints

Finally, waiting for upcoming technological evolutions seems the best option to solve the last two challenges. Regarding interoperability, efforts have been underway for years to make all IIoT devices capable of speaking a common language, even when manufactured by different vendors. The diffusion of multiplatform, open-source communication standards such as the Message Queuing Telemetry Transport (MQTT) and the Open Platform Communication Unified Architecture (OPC UA), seems to suggest that this complex issue will be solved in the next few years (I11) [42].

In terms of bandwidth and latency, today there are many solutions available on the market (e.g., optical fiber in combination with one or more wireless technology such as of Wi-Fi, Bluetooth Low Energy, LTE-M, Narrowband IoT, etc.) [43]. Companies should recognize that in the future these capabilities will contribute to their competitive advantage and begin to consider them on par with any other production investments. Obviously, this infrastructure will have to be monitored more closely by the company IT. Furthermore, the interviews revealed the importance of the imminent arrival of enterprise 5G, a technology which could greatly expand the communication capabilities of a plant, in some cases also impacting the edge-cloud balance by allowing to move more workloads onto the cloud side (I6, I7, I12).

5.2. Organizational context

Unclear value of IIoT initiatives

The exact return on investment (RoI) of an IIoT project is difficult to ascertain a priori, because often the IIoT replaces elements that were not really considered by the company. For example, it is difficult to compare an IIoT machine learning solution, costly to develop and refine, versus the experience of an OT veteran, which is virtually "free" for the company (I9). However, there may be specific use cases where IIoT definitely has an edge over other alternatives: *"we had a customer that, after the second wave of the Covid-19 pandemic, needed to rapidly increase its production. However, the company was not sure that the increase would remain stable over time so to justify the investment in an entire new production line. [Implementing an IIoT solution] allowed them to increase productivity to the required levels, at a reduced cost, while retaining a greater production flexibility*. In this case, the IIoT investment allowed to get the desired outcome at a lower cost and to cope with the limitations imposed by the circumstances. Another use case mentioned during the interviews was the reduction of scrap – one of the possible benefits of IIoT adoption [12, 14] – that could help the company to pursue its long-term sustainability objectives (I11).

Strategic approach to IIoT initiatives

It is essential that IIoT projects are not conceived as stand-alone initiatives, but rather as a declination of the broader digital transformation strategy of the company (I5, I7, I8). While it is not possible to define a best approach between top-down and bottom-up, companies can take some steps to decide which of the two fits better with their characteristics. For example, companies can start by assessing the degree of digital readiness of their factories. A company with a similar level of readiness could opt for a basically bottom-up approach, with a "lighthouse" plant acting as an icebreaker and driving the initiative [44]. On the contrary, a company with a high rate of diversity could opt for a basically top-down approach, focusing its efforts on realizing a common data infrastructure shared across all the company's plants, from which plant-specific applications can then be deployed (I3).

IT/OT Integration

IIoT initiative requires skills from both areas, and it is not possible to draw a clear line between what is the responsibility of the OT and what is the responsibility of IT (I3, I4, I6, I8). Whoever the bearer of the request, CIO or COO, he / she will have to take charge of involving the other with a storytelling common to both parties (I11). In this case, the most onerous task falls on the CIO, who – having a wider visibility on the company IS and knowing the technologies available on the market – should help dictating the long-term vision of the project and avoid a focalization on the short-term results (I11). At the same time, the COO should engage the CIO well

before contacting any potential vendor, in order to minimize the perception of "field invasion" (I3, I4). Beyond the top management figures, companies should consider the formation of small mixed groups: agile teams comprising middle-management figures from both units capable of bridging the two (I3, I4, I11, I12). In this sense, the vendor(s) of the IIoT solution can help the company: user-friendly software interfaces, that systematically put IT and OT into communication, can contribute to the shared management of the project (I8).

Cultural change

For SMEs, cultural change can be facilitated by making the benefits of IIoT more tangible for the final users. For example, in companies where the data collection process already exists, it may be easier to promote it: *"if every morning I spend the first two hours collecting data from the machines, and the next two hours uploading them to Excel, then I only have half a day left to understand how to put them to good use. With the IIoT, when I arrive at the office in the morning, I already have all the data ready to be analyzed. When those who work in OT grasp this difference, then suddenly promoting cultural change becomes much easier"* (I3). As for large companies, the first step they should take is an assessment of the degree of digital awareness of their OT staff (I11), followed by a change management program aimed at aligning the competences of the entire company. A good solution can be selecting some "champions" in the agile mixed teams to act as motivators and sponsors of the project within their own units (I9, I10). These champions could be entrusted with the organization of periodic workshops in which to involve representatives of both IT and OT (I11). Furthermore, the company might also consider involving some of external partners, such as its main suppliers within these workshops (I5, I6, I7).

Lack of skills and knowledge

Universities in recent years identified the IIoT skill gap and are now trying to fill it (I9), but the scarcity is likely to remain so for the next few years, given that the skills required are on the one hand shared with many other digital transformation projects, and on the other must be accompanied by experience in the field that cannot be obtained but with time (I5, I6, I7, I11, I12). In the meantime, companies can provide training to all those employees who are likely to be involved in the project. For example, people taking care of the maintenance of the machines can be trained with little effort to also do maintenance of the related sensors (I11). In addition, companies should evaluate the possibility of establishing a partnership with universities or competence centers in its area. For example, as part of its Industry 4.0 national plan, Italy identified eight competence centers to carry out education and training activities for companies (especially SMEs) on Industry 4.0 initiatives [46]. Finally, whenever possible for either budget availability or contingent situations (e.g., a talented person who does not want to move too far away from his hometown), the company should always try to hire people with skills in the fields of automation engineering and data science (I11).

5.3. Environmental context

Fear of missing out

With regard to government incentives, the main risk to avoid is to make partial or very short-term investments only to solve a *"temporary stomach-ache"* (I12) or to enjoy tax advantages without even considering the long-term strategy (I11). As far as large companies are concerned, the fear of falling behind their main competitors is justified, but in some ways less so than in other industrial sectors. Ultimately, the main competitive advantage in manufacturing is still represented by the final product, and less by the process itself. Consequently, *"it makes no sense to run after your competitors just to say you have done IIoT, if you are just creating unnecessary complexity in the company and making the final product worse"* (I12). In both cases mentioned above, the key concept remains that presented in the previous paragraph: the adoption of an IIoT project must be guided by a medium-long term business strategy, knowing that in the coming years the IIoT infrastructure will probably become the essential "skeleton" to continue operating in the manufacturing sector (I5, I11).

6. Conclusions and further research

Despite the benefits promised by its adoption, the level of IIoT implementation in manufacturing remains far from the initial expectations. By applying the TOE framework to structure data emerging from a set of semi-structured interviews with experts in the field of IIoT, this study highlights the key challenges that are causing this slowdown and identifies some guidelines to overcome them. Tables 2 and 3 summarize the individual challenges and the related recommendations, according to the three dimensions of the TOE framework.

One of the most important evidence that emerged from the study – common to many other digital transformation projects [47, 48] – is that the key

factors blocking IIoT are not technological, but rather organizational.

This does not mean that there are no technological obstacles. First, the maturity of cyber security in the manufacturing sector is still dangerously low: this poses a significant risk not only to IIoT deployments, but to any digital initiative that the company may start. A second pitfall is that of data aggregating IIoT data and further integrating with enterprise legacy systems. While there are partial measures that can be taken, such as the creation of a shared enterprise data lake, a long-term, standardized solution to this problem is not yet in sight. Finally, other issues – such as striking the right edge-cloud balance, ensuring the interoperability of IIoT devices, and enhancing the bandwidth capabilities of the various plants – still pose a hurdle, but it is likely that they will be solved in the next few years.

On the contrary, our study sheds light on how organizational obstacles are proving still very complex to solve. The value that IIoT adoption can bring, especially in terms of operational efficiency and process transparency, is often unconsciously perceived by managers but not easy to quantify in economic terms. Therefore, a careful selection of business cases, tailored to the needs of the company, may represent a good starting point for companies to start experimenting with this technology. Government incentives can play an important role in this process, but they should not represent the main selection criterion.

At a managerial level, coordination between CIO and COO is essential. The former must be able to integrate IIoT in the long-term digital strategy of the company and avoid hindering the project due to the "field invasion" feelings. The latter must help in pointing out the company's operational needs and trust the CIO about the project architecture. Integration and communication should be further promoted among their entire units and backed with various programs, such as mixed agile teams and recurring workshops, involving figures from both IT and OT.

Moreover, a deep lack of skill and knowledge related to IIoT emerged. Companies cannot do much about this last issue, but, when possible, they should hire new talents, reskill their current employees, and collaborate with universities and competence centers to train new experts.

Finally, companies should not let their IIoT investments be driven by the fear of missing out, but rather plan such investments strategically and integrate these into their long-term digital transformation strategy.

As to any kind of research, also this study is subject to a certain number of limitations. First, the study is based on 12 interviews with experts from companies on the offer side of the IIoT market. An increased number of interviews may allow to gain a broader overview of the challenges of IIoT adoption and their possible solutions. Also, direct interviews with manufacturing companies may allow to gain insights on firm-specific issues.

Second, our respondents are mainly from Europe. This implies that the results of the research might not be generalized to other contexts. Factors such as the government tax incentive system, the average maturity level of cybersecurity, the size of the companies (which was defined according to thresholds determined by EU recommendation 2003/361 [49]), are peculiar of the European context and may greatly differ in other parts of the world.

7. References

[1] Sony, M. and Naik, S., "Key ingredients for evaluating Industry 4.0 readiness for organizations", Benchmarking: An International Journal (2019).

[2] Wang, K., "Intelligent predictive maintenance (IPdM) system–Industry 4.0 scenario", WIT Transactions on Engineering Sciences, 113, 259-268 (2016).

[3] Nadj, M., Jegadeesan H., Maedche, A., Hoffmann D. and Erdmann, P., "A Situation Awareness Driven Design for Predictive Maintenance Systems", ECIS, Rome, Italy (2016).

[4] Coreynen, W., Matthyssens P., and Van Bockhaven W., "Boosting Servitization through Digitization", Industrial Marketing Management (2017).

[5] Lin, D., Lee, C. K., Lau, H., and Yang, Y., "Strategic response to Industry 4.0: an empirical investigation on the Chinese automotive industry", Industrial Management & Data Systems (2018).

[6] Whitmore, A., Agarwal A., and Da Xu L., "The Internet of Things: A Survey of Topics and Trends", Information Systems Frontiers 17-2: 261–274 (2015).

[7] Lyytinen, K., Yoo Y., and Boland Jr., R. J., "Digital Product Innovation within Four Classes of Innovation Networks", Information Systems Journal 26 (2016).

[8] Baines, T., Ziaee Bigdeli A., Bustinza, O., Shi V., Baldwin J. and Ridgway K., "Servitization: Revisiting the State-of-the-Art and Research Priorities", International Journal of Operations & Production Management 37-2: 256–278 (2017).

[9] Munirathinam, S. "Industry 4.0: Industrial internet of things (IIOT)", Advances in computers 117-1 (2020).

[10] Aheleroff, S., Xu, X., Lu, Y., Aristizabal, M., Velásquez, J. P., Joa, B., & Valencia, Y., "IoT-enabled smart appliances under industry 4.0: A case study", Advanced engineering informatics, 43 (2020).

[11] Sivathanu, B., "Adoption of industrial IoT (IIoT) in auto-component manufacturing SMEs in India", Information Resources Management Journal 32 (2019).

[12] Kagermann, H., Wahlster, W., and Helbig, J., "Recommendations for Implementing the Strategic

Initiative Industrie 4.0", National Academy of Science and Engineering: Frankfurt am Main, Germany (2013).
[13] Oesterreich, T.D. and Teuteberg, F., "Understanding the implications of digitisation and automation in the context of Industry 4.0", Computers in Industry 83 (2016).
[14] Lasi, H., Fettke, P., Kemper, H. G., Feld, T., & Hoffmann, M., "Industry 4.0", Business & information systems engineering 6-4: 239-242 (2014).
[15] Farkash, E., "Industry 4.0: Don't Believe the Hype, Yet", IndustryWeek (2021).
[16] Garg A., "Hype vs. Reality: What's Happening with IIoT In Manufacturing?", Plex (2020).
[17] Patel, M., Shangkuan, J. and Thomas, C., "What's new with the IoT", McKinsey (2017).
[18] Shirer M. and Torchia M., "Worldwide Spending on the IoT Will Slow in 2020", IDC (2020).
[19] Merritt R., "IoT Growth Slower Than Expected", EETimes (2017).
[20] Vause C., "What is "Pilot Purgatory" and Why Every Start-Up Should Know This Term", Medium (2020).
[21] Liozu S., "8 Reasons Why Your IIoT Project Is Stuck in Pilot Purgatory", IndustryWeek (2019).
[22] Boyes, H., Hallaq, B., Cunningham, J., & Watson, T., "The industrial internet of things (IIoT): An analysis framework", Computers in industry 101: 1-12 (2018).
[23] I-Scoop, "IoT 2019: spending, trends and hindrances across industries", I-Scoop (2019).
[24] Tornatzky, L.G., and Fleischer, M., "The Processes of Technological Innovation", Lexington Books, Lexington, MA (1990).
[25] Chao, P.Y.K., and Tam, K.Y., "Factors Affecting the Adoption of Open Systems", MIS Quarterly, Hong Kong (1997).
[26] Doolin, B. and Troshani, I., "Organizational adoption of XBRL", Electronic Markets 17-3: 199-209 (2007)
[27] Rauniar, R., Rawski, G., Yang, J. and Johnson, B., "Technology acceptance model (TAM) and social media usage", Journal of Enterprise Information Management 27 (2014)
[28] Salwani, M., Marthandan, G., Norzaidi, M. and Chong, S., "E-commerce usage and business performance in the Malaysian tourism sector", Information Management & Computer Security 17 (2009).
[29] Low, C., Chen, Y. and Wu, M., "Understanding the determinants of cloud computing adoption", Industrial Management & Data Systems, 111 (2011).
[30] Oliveira, T. and Martins, M., "Literature review of information technology adoption models at firm level", The Electronic Journal Information Systems Evaluation 14-1: 110-121 (2011).
[31] Musawa, M. and Wahab, E., "The adoption of EDI technology by Nigerian SMEs", Journal of Business Management and Economics 3-2: 55-68 (2011).
[32] Prause, M., "Challenges of industry 4.0 technology adoption for SMEs: the case of Japan", Sustainability 11-20 (2019).
[33] Sisinni, E., Saifullah, A., Han, S., Jennehag, U., and Gidlund, M., "Industrial IoT: Challenges, opportunities, and directions", IEEE Transactions on Industrial Informatics 14-11: 4724-4734 (2018).
[34] Masood, T., and Egger, J., "Augmented reality in support of Industry 4.0", Robotics and Computer-Integrated Manufacturing 58: 181-195 (2019).
[35] Gartner, "Definition of SI", retrieved from https://www.gartner.com/en/information-technology/glossary/si-system-integrator (2021).
[36] Lenzerini, M., "Data integration: A theoretical perspective", Proceedings of the twenty-first symposium on Principles of database systems (2002).
[37] Boyce C. and Neale P., "Conducting in-depth interviews: A guide for designing and conducting in-depth interviews for evaluation input", Monitoring and Evaluation (2006).
[38] Myers, M.D., "Qualitative Research in Business and Management", SAGE, Los Angeles (2013).
[39] Saldaña J., "Goodalls verbal exchange coding: An overview and example," Qualitative Inquiry 22 (2016).
[40] Tsiknas, K., Taketzis, D., Demertzis, K., and Skianis, C., "Cyber Threats to Industrial IoT: A Survey on Attacks and Countermeasures", IoT 2 (2021).
[41] Boci, M., De Vet, J. M. and Pauer A., "'Gold-plating' in the EAFRD", Directorate-General for Internal Policies of the Union, Brussels (2014).
[42] Ferrari, P., Flammini, A., Rinaldi, S., Sisinni, E., Maffei, D., and Malara, M., "Impact of quality of service on cloud based industrial IoT applications with OPC UA", Electronics 7-7: 109 (2018).
[43] Sanchez-Iborra, R., & Cano, M. D., "State of the art in LP-WAN solutions for industrial IoT services", Sensors 16-5: 708 (2016).
[44] Goreckya, D., Romerob, D., and Kimc, D. Y., "Accelerating Technological Advancement and Adoption of Industry 4.0 Technologies", International Conference on Computational Design and Eng. (2019).
[45] Delgado, M., Romero Gázquez, J., Cruzado, G. and Melero, F., "Gaps between skills required by Industry 4.0 and academic programs focused on ICTs", 10th International Conference of Education, Research and Innovation, Sevilla (2017).
[46] Ministero dello Sviluppo Economico, "Centri di competenza ad alta specializzazione", retrieved from https://www.mise.gov.it/index.php/it/incentivi/impresa/centri-di-competenza (2018).
[47] Kane, G. C., Palmer, D., Phillips, A. N., Kiron, D., and Buckley, N., "Strategy, not technology, drives digital transformation", MIT Sloan Management Review and Deloitte University Press 14: 1-25 (2015).
[48] Tabrizi, B., Lam, E., Girard, K., and Irvin, V., "Digital transformation is not about technology", Harvard Business Review 13: 1-6 (2019).
[49] EU Commission, "Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises", Official Journal (2003).