The Stakeholder Playbook

IIoT Market Adoption Lessons from Eight Standardisation Cases

CoSEM Master's Thesis

Boris van Dongen

Delft University of Technology

The Stakeholder Playbook

IIoT Market Adoption Lessons from Eight Standardisation Cases

by

Boris van Dongen

to obtain the degree of Master of Science Complex Systems Engineering and Management
at the Delft University of Technology,
to be defended publicly on Friday January 10, 2024 at 14:00.

This is an anonymised version of the original thesis, prepared for public access.

Chair & First supervisor:	Geerten van de Kaa
Second supervisor:	Marcel Ludema
Project Duration:	June - November 2024
Faculty:	Faculty of Technology, Policy and Management
Student number:	5412455

Summary

This thesis investigates the impact of stakeholder characteristics on the market adoption of standards within the Industrial Internet of Things (IIoT) sector. It consists of a literature review, an empirical analysis, exploration of influence mechanisms and a discussion on the results. There are three main topics that are discussed in this thesis: Standardisation is a cooperation among industry, consumers, public authorities and other interested parties for the development of technical specifications; Stakeholders are organisations or individuals that have an interest or influence in the standardisation process. Stakeholders can be entities like customers, investors, and governments. Theory (de Vries et al., 2003) points out that a balanced representation of stakeholders is vital for the quality of standards; The Internet of Things (IoT) involves devices and systems that (need to) communicate and operate seamlessly together. This requirement for interoperability has led to a significant number of standards and protocols competing for dominance. This thesis focuses on Industrial Internet of Things (IIoT). IIoT shows great potential in industrial application, for example in harbours, production facilities, and warehouses.

The literature review explores academic sources like Scopus, Web of Science, Google Scholar, and SciSearch. The search strategy included keywords focusing on standardisation, stakeholder influence, and IIoT to identify studies commenting on the respective (or interplay of) these factors. From these studies, it was revealed that large multinational corporations dominate standardisation processes, often imposing proprietary standards that inhibit interoperability, limit accessibility, and create barriers for smaller entities. Regulatory bodies, while central to ensuring standards align with public interests, frequently struggle to keep pace with rapid technological evolution, leaving significant gaps in security, data privacy, and compatibility. Additionally, literature showed us that common standards are difficult to reach due to problems with stakeholder infrastructure, as multiple researchers have laid foundation to further research stakeholder infrastructures in standardisation. Hence the reason this thesis will aim to investigate the patterns that stakeholder characteristics and infrastructure have with the emergence of common standards. This led to the main research question:

• To what extent do stakeholder characteristics influence the development of technological standards in industrial IoT?”

To answer the main research question, two sub-questions were formulated:

• How does the classification of stakeholders—organised into a matrix based on their levels of power, legitimacy, and urgency—affect the emergence of technological standards in IIoT?

• How can policymakers, researchers, or businesses influence stakeholders to shape the standardisation process in Industrial IIoT?

The first sub question aims to be answered by an empirical analysis. This analysis focusses on eight IIoT standardisation cases across the four different phases in IIoT: data ingestion (where IIoT sensors collect data from the environment, like temperature), data transmission (where data is transmitted to a local or cloud solution), data processing (where data is processed, e.g. aggregated or decrypted), and data utilisation (which often involves human-computer interaction and an application: presents dashboards & insights). For each phase, two standards were selected, one with market adoption and one without. The cases were:

1) Data Ingestion:
• RFID UHF (adopted)
• Zephyr Project (not adopted)

2) Data Transmission:
• LoRaWAN (adopted)
• Sigfox (not adopted)

3) Data Processing:
- EPCIS (adopted)
- UPnP (not adopted)

4) Data Utilisation:
- Ignition (adopted)
- GE Predix (not adopted)

The methodology employed an approach based on de Vries et al. (2003), using nine search directions, like production firms, end-users and regulators. After identification of the stakeholders, they are classified according to their power, legitimacy, and urgency in the standardisation process. The research combined desk research, case studies, and expert interviews to gather data about stakeholder characteristics. The extensive empirical research led to a collection of sixteen tables showing the involved stakeholders and their power, urgency and legitimacy to the standard. This output was summarised in a large table to detect patterns in whether certain types of stakeholders contributed positively or negatively to the market adoption of a standard. The patterns that arise from the empirical analysis are:

1) End-user engagement is essential: End users and related organisations are more prevalent in standards with market adoption. Their involvement as dominant or definitive stakeholders contributes significantly to the adoption and implementation of the standard.

2) Dangerous stakeholders hinder adoption: In 3 out of 4 standards without market adoption, there is at least one dangerous stakeholder. Their presence correlates with the lack of adoption, indicating that stakeholders who have power and urgency but lack legitimacy can create obstacles in the standardisation process.

3) Definitive stakeholders drive market adoption: Standards with market adoption have a higher average number of definitive stakeholders (4) compared to those without market adoption (1.75). This suggests that the involvement of stakeholders possessing power, urgency, and legitimacy is crucial for a standard's success in the market.

4) Higher stakeholder participation in adopted standards: Standards that have been adopted in the market involve more stakeholders on average (11.25) compared to those without market adoption (7.5). Broad stakeholder participation enhances the standard's credibility and acceptance.

5) Absence of stakeholders with only power or urgency: Stakeholders possessing only power (type E) or only urgency (type G) do not appear in the table. This absence indicates that power or urgency alone is insufficient to impact standard adoption.

These patterns are subsequently translated into policy recommendations on how to influence the standardisation process. This was done to answer sub question 2. To influence stakeholders and improve standardisation efforts, the research identified policy recommendations:

1) Stimulating end-user engagement through:
- Creating well-established stakeholder groups
- Eliminating fees for participation
- Offering free consultation on standardisation efforts

2) Managing dangerous stakeholders by:
- Finding ways for them to participate with approval from other stakeholders
- Implementing review mechanisms through special committees

3) Increasing stakeholder participation by:
- Focusing on quality over quantity in standardisation efforts
- Providing resources to enhance stakeholder capabilities
- Creating regulatory frameworks that prioritise standardisation

The discussion highlights that the findings from this thesis align with previous research emphasising the importance of user engagement. According to a professor expert on the matter, the caveat is that this is only beneficial when users can provide clear, unambiguous requirements. Also, the methodology used in this thesis represents a novel application of de Vries' 2003 stakeholder identification method, particularly in creating a stakeholder/standard matrix. Other than this thesis, the methodology has been applied in a few other scholarly cases and by Professor van de Kaa. At last, the discussion tells that the research contributes to standardisation literature by empirically analysing market adoption across multiple cases. Important aspects are the confirmation of the importance of end-user engagement and the identification of dangerous stakeholders as a threat to standardisation.

Future recommendations of the study include the need for further research on effective methods for involving end-users in standardisation processes, particularly through empirical studies. Also, further investigation of mechanisms to identify and manage dangerous stakeholders is important, as this remains underexplored in current literature. With concerns to the methodology applied, application of the stakeholder identification and classification method across different sectors would validate its broader applicability. Because of the dynamic environment of stakeholders, standardisation and IIoT, longitudinal studies are advised to capture how standards evolve with technological advancement and changing stakeholder dynamics. At last, more research on how to increase stakeholder salience levels and the impact this has on standardisation success is advised.

Contents

List of Figures

List of Tables

Abbreviations

Abbreviation	Definition
BLE	Bluetooth Low Energy – energy-efficient Bluetooth standard for short-range communication
CoAP	Constrained Application Protocol – lightweight protocol for restricted-resource environments
EPCIS	Electronic Product Code Information Services – GS1 standard for tracking product movement in supply chains
HTTP	Hypertext Transfer Protocol – protocol for transferring hypertext on the web
IEC	International Electrotechnical Commission – organisation for electrical/electronic standards
IIoT	Industrial Internet of Things – IoT applied to industrial settings
IoT	Internet of Things – network of interconnected devices
ISA	International Society of Automation – professional association for automation
ISA-95	Business to Manufacturing Markup Language Standard – ISA standard for integrating enterprise and control systems
ISO	International Organization for Standardization – global standards developer
LPWAN	Low Power Wide Area Network – wireless network type for long-range, low-bandwidth communication
MQTT	Message Queuing Telemetry Transport – lightweight messaging protocol for IoT
NFC	Near Field Communication – short-range wireless connectivity for devices
OPAF	Open Process Automation Forum – consortium for developing open process automation standards
OPC UA	Open Platform Communications Unified Architecture – machine-to-machine communication protocol for industrial automation
RFID	Radio Frequency Identification – technology for automatic identification using electromagnetic fields
SCADA	Supervisory Control and Data Acquisition – system for monitoring and controlling industrial processes
SMBs / SMEs	Small and Medium-sized Enterprises / Small and Medium-sized Businesses – organisations characterised by a limited number of employees and revenue.
UPnP	Universal Plug and Play – protocols enabling device discovery and connectivity in a network
Wi-Fi	Wireless network protocols based on IEEE 802.11 – for wireless local area networking

1 Introduction

Rapid growth in the Internet of Things (IoT) industry has led to a multitude of competing technological standards. This fragmentation makes for challenges with regards to interoperability: it hinders the seamless integration of IoT devices and systems. As a result, some standards never see widespread adoption, limiting the IoT's potential to deliver benefits in monitoring, data creation and cost reduction. Understanding the complex landscape of stakeholders and their interactions is crucial for identifying the factors that contribute to the success or failure of technological standards. This thesis investigates the relationships among various stakeholders for different standards in the IoT industry and examines how these interactions influence the development and adoption of technological standards.

1.1. Link to study programme

From the perspective of Complex Systems Engineering and Management, this problem is placed within a broader context of technology ecosystems. The ecosystem of stakeholder involvement in IIoT standardisation, is complex and adaptive, characterised by interdependencies between various actors, technologies and institutions. The program's focus on integrating technology, policy, and management makes it an ideal context for exploring how stakeholders navigate and influence these standardisation processes through different strategies.

1.2. The standardisation process

Standardisation is a voluntary cooperation among industry, consumers, public authorities and other interested parties for the development of technical specifications (EU, 2009). Guillemin et al., 2013 identifies standardisation as follows: *"Standardisation complements market-based competition, typically in order to achieve objectives such as the interoperability of complementary products/services, to agree on test methods and on requirements for safety, health and environmental performance. Standardisation also has a dimension of public interest. Standard makers should be close to standard users/implementers."*

The impact that standards such as Wi-Fi and USB-C have had on various industries present the relevance of the initial problem. These standards not only enhance interoperability but also drive competitive advantage, creating a battleground where various stakeholders are driven to establish their preferred protocols as the market norm. This competitive environment, often referred to as "standards (or technology) battles" (van de Kaa et al., 2015), is crucial for understanding how technological adoption takes place and the strategies used by different actors within the ecosystem (van den Ende et al., 2012).

Standards battles refer to the competition between different technologies striving to become the industry-wide standard. In this thesis, the success of a technological standard is measured by its market adoption - the extent to which it is accepted and used by users and the market. High market adoption not only signifies widespread acceptance but also enhances the standard's value through network effects, where the utility increases as more users adopt it (Tucker, 2018). The process of market adoption differs depending on the type of standard: standards can be de facto, emerging through widespread market acceptance (sometimes without formal approval) or committee based (de jure), established through formal processes by SDOs (Ciciora et al., 2004). De facto standards gain dominance due to market forces and user preferences, while committee-based standards result from market adoption among users, producers, and regulatory bodies, leading to a formally ratified standard. A standard can also be both, like well-known Adobe PDF. Created in 1993, it gained traction as one of the most popular file formats, becoming a de facto standard. It took until 2005 before PDF/A became a de jure standard under ISO 19005-1:2005 (ISO, 2008). This timeline shows one of the key differences between de facto and de jure standards: adoption speed.

1.3. Stakeholder impact on the standardisation process

Stakeholders are organisations or individuals that have an interest or influence in this case, the standardisation process. Most of the time, stakeholders include customers, employees, investors, suppliers, communities and governments (CFI Team, n.d.). With regards to standardisation, according to De Vries et al. (2003), stakeholders in information technology include manufacturers, regulators, and users, each playing a crucial role in shaping the standards. De Vries (2003) emphasises that balanced representation of stakeholders is vital for the quality and acceptance of standards. However, challenges such as underrepresentation of users and lack of systematic stakeholder identification can hinder this balance, which impacts the effectiveness of the standardisation process.

1.4. The Industrial Internet of Things

More specifically than IoT, this thesis focuses on Industrial Internet of Things (IIoT). IIoT shows great potential in industrial application. Application of IIoT in harbours, production facilities, and warehouses enables monitoring and optimisation of the operation, track the movement of goods, and improve safety through predictive maintenance. This connectivity enhances efficiency, reduces downtime, and lowers operational costs. Port of Rotterdam utilises IIoT to predict and analyse water levels and wave heights through the use of 44 sensors in and around the harbour in combination with prediction models (Port of Rotterdam, 2022). Hapag-Lloyd deploys over 3.000.000 IIoT trackers in its containers.

IIoT consists out of four phases (Grasso, 2023) (Deloitte, 2022): data ingestion, data transmission, data processing, and data utilisation. An example of the process of these phases is as follows: Data ingestion refers to the first phase where IoT devices, such as sensors, collect raw data, such as temperature, from their environment. In the transmission phase data is sent from the devices to a platform such as a cloud solution using communication protocols. The processing phase involves transforming raw data into meaningful information through aggregation, analysis or decryption. Finally, in the utilisation phase, the processed data is presented to users via applications, so it can be used to make decisions. These interconnected phases are very important to ensure full functionality of the IIoT system.

The IIoT is an interesting example in the context of standardisation processes, because of its complexity and need for interoperability . IIoT involves an array of devices and systems that (need to) communicate and operate seamlessly together. This requirement for interoperability has led to a significant number of standards and protocols competing for dominance. The interplay of stakeholders, from technology developers to regulatory bodies and end-users, complicates the landscape. Tiburski et al. (2016) highlights the important aspect of standardisation within the (I)IoT space as well as the challenges that appear with regards to safety.

1.5. Chapter breakdown

The outline of the thesis, breaking down each of the following chapters, is found in Table 1.1 below:

Table 1.1: Outline of this thesis

Section	Header	Description
Chapter 2	Literature review & methodology	Literature review analysing relevant literature related to the stakeholders in IIoT standardisation, leading to the research questions, problem statement and empirical methodology. This methodology outlines the stakeholder identification, classification and case selection methods for the analysis of stakeholder influence on IIoT standardisation.
Chapter 3	Results	Empirical analysis presenting findings from the case studies and interviews, examining patterns in stakeholder involvement and how these characteristics influence IIoT standardisation outcomes. Answer to SQ1.
Chapter 4	Analysis	Explores the theoretical and practical implications of the findings, showing how the standardisation process can be influenced by agents in the IIoT industry. Answer to SQ2.
Chapter 5	Discussion	Discussion on the theoretical and practical contributions, verification of research result and overview of limitations.
Chapter 6	Conclusion	Key findings & recommendations for future research.
Appendices	Supporting materials	Supporting materials, potential selected cases, interview questions and expert and interview backgrounds.

2
Research method

To determine the research method, this chapter begins with a literature review that lays the theoretical foundation for the study, examining existing research on stakeholder influence within standardisation processes in the context of the Industrial Internet of Things (IIoT). The themes highlighted in the literature review guide the formulation of the problem statement. This problem statement serves as a bridge to the empirical aspect of the research. Following the establishment of the problem statement, the chapter describes the empirical research approach. This details the process for identifying and analysing stakeholders.

2.1. Literature review

The research methodology for this literature review is structured to align with the guidelines outlined by Van Wee (2015):
1) Search strategy
2) Inclusion and exclusion criteria
3) Screening and selection process
4) Data extraction and results
5) Analysis
6) Conclusion

The search strategy used for the literature search was to identify relevant articles to the topic of interest. A total of four electronic databases (Scopus, Web of Science, Google Scholar and SciSearch) were used while searching for papers that evaluated the impact of Stakeholder influence on IIoT Standardisation. The search concerned articles written both in English and Dutch. The keywords employed for the search included a search query similar to the form of (”technological standards” OR ”standardisation” OR ”standards battles” OR ”standards development”) AND (”stakeholder characteristics” OR ”stakeholder infrastructure” OR ”stakeholders”) AND (“IIoT” OR ”IoT” OR “Industrial Internet of Things” OR ”Internet of Things” OR ”cyber-physical systems”). Article inclusion criteria involved a preference for sources that were published in the last ten years to provide robust results in areas of research. The search had to be representative, focus on academic sources and encompass popular sources too, addressing the advantages and disadvantages of stakeholder engagement in the process of standards development. In addition to the sources originating from database searches, papers were selected on forehand by recommendation or prior knowledge, noted in Figure 2.1 as Records identified through other sources. The full review is depicted in a PRISMA flow diagram, visually outlining the process of selecting studies for systematic reviews. The PRISMA Statement calls for a high level of reporting detail in literature reviews: an integral part of the methodological description of a review is a flow diagram (Haddaway et al., 2020).

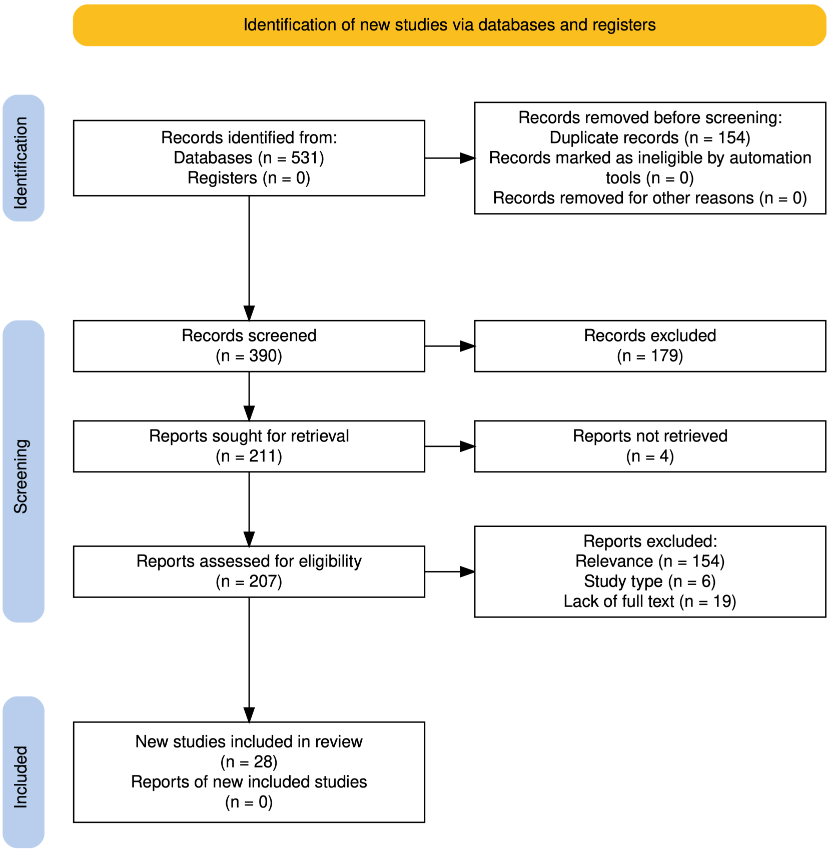

Identification of new studies via databases and registers
Identification
Screening
Included
Records identified from:
Databases (n = 531)
Registers (n = 0)
Records removed before screening:
Duplicate records (n = 154)
Records marked as ineligible by automation tools (n = 0)
Records removed for other reasons (n = 0)
Records screened
(n = 390)
Records excluded
(n = 179)
Reports sought for retrieval
(n = 211)
Reports not retrieved
(n = 4)
Reports assessed for eligibility
(n = 207)
Reports excluded:
Relevance (n = 154)
Study type (n = 6)
Lack of full text (n = 19)
New studies included in review
(n = 28)
Reports of new included studies
(n = 0)

Figure 2.1: Search strategy denoted in PRISMA flow diagram

The identified studies were grouped according to the study type and its subject. The complete list is shown in Table 2.1.

Table 2.1: Literature overview of included studies

Reference	Title	Study type
Brass, I., & Sowell, J. H. (2021)	Adaptive governance for the Internet of Things: Coping with emerging security risks	Theory
Cranmer, E. E., Papalexi, M., tom Dieck, M. C., & Bamford, D. (2022)	Internet of Things: Aspiration, implementation and contribution	Empirical study
de Vries, H. J., Verheul, H., & Willemse, H. (2003)	Stakeholder identification in IT standardization processes	Theory
de Vries, H., Verheul, H., & Willemse, H. (n.d.)	Standard Making: A Critical Research Frontier for Information Systems	Theory
Ehie, I. C., & Chilton, M. A. (2020)	Understanding the influence of IT/OT Convergence on the adoption of Internet of Things (IoT) in manufacturing organizations	Empirical study
Fischer-Hübner, S., et al. (2021)	Stakeholder perspectives and requirements on cybersecurity in Europe	Case study
Graz, J. C. (2018)	Global corporations and the governance of standards	Theory
Hoogerbrugge, C., van de Kaa, G., & Chappin, E. (2023)	Adoption of quality standards for corporate greenhouse gas inventories: The importance of other stakeholders	Case study

Continued on next page

Table 2.1 – continued from previous page

Reference	Title	Study type
Kedia, M., Sekhani, R., & Katiyar, T. (2020)	The Role of Standards in Diffusion of Emerging Technologies Internet of Things (IoT)	Policy study
Kim, D. H., Lee, H., & Kwak, J. (2017)	Standards as a driving force that influences emerging technological trajectories in the converging world of the Internet and things: An investigation of the M2M/IoT patent network	Patent study
Kopetz, H., & Steiner, W. (2022)	Real-Time Systems: Design Principles for Distributed Embedded Applications	Theory
Meddeb, A. (2016)	Internet of Things standards: who stands out from the crowd?	Industry analysis
Mouha, R. A. R. A. (2021)	Internet of Things (IoT)	Overview
Mukherjee, A. (2019)	Stakeholder management in the standardisation process	Theory
Petrik, D., & Herzwurm, G. (2020)	Towards the IIoT ecosystem development-understanding, the stakeholder perspective	Empirical study
Saleem, J., et al. (2018)	IoT standardisation: Challenges, perspectives and solution	Challenges & solutions
Scheepers, C. E., et al. (2014)	Shifting from car to active transport: A systematic review of the effectiveness of interventions	Systematic review
Tassey, G., & Economist, S. (1999)	Standardization in Technology-Based Markets	Theory
Trautman, L. J., et al. (2020)	Governance of the Internet of Things (IOT)	Governance study
van de Kaa, G. (2023)	Standards adoption: A comprehensive multidisciplinary review	Literature review
van de Kaa, G., & de Vries, H. J. (2015)	Factors for winning format battles: A comparative case study	Case study
van de Kaa, G., & Greeven, M. (2017)	LED standardization in China and South East Asia: Stakeholders, infrastructure and institutional regimes	Case study
van de Kaa, G., et al. (2011)	Factors for winning interface format battles: A review and synthesis of the literature	Literature review and theory
Wang, P., Jung, C., & Lee, H. (2016)	Organizational motivation in adopting IT standards: A stakeholder analysis approach	Theory

2.2. Results

IIoT has transformed industries by allowing devices to transact with one another. IIoT is rapidly changing, with some threats mainly associated with creating compatible standards for integration and security, as well as the encompassing solution to accommodate the vast number of connected devices (Ehie & Chilton, 2020). Naturally, standards adoption is fuelled by factors like the standard's technological superiority, relative advantage, or customisability (van de Kaa, 2023). However, the focus here lies in the factors influenced by stakeholders. The standardisation process depends on other actors, such as tech firms, regulatory authorities, and consumer protection organisations (Lechowski & Krzywdzinski, 2022). This is because larger corporations utilise their bargaining power to set standards that align with their objectives (Graz, 2018), while the regulatory authorities aim to achieve the public's best interest. However, at times, they fail to implement measures to ensure that new technologies meet these objectives (Kedia et al., 2020).

Furthermore, the review indicates that large Multinational Corporations dominated IIoT standardisation processes because of their ample resources compared to smaller enterprises. They frequently act as initiators of standardisation processes, being either directly involved in standardisation committees or managing them, and usually advocate for standards that meet their strategic objectives (Kopetz &

Steiner, 2022). This dominance is particularly significant in the use of proprietary standards that lead to the inability to integrate IIoT systems across different platforms (Lechowski & Krzywdzinski, 2022).

On the other hand, regulatory bodies, although they play the crucial role of ensuring that standards meet the public interest—such as security and fair competition—generally adopt a more reactive stance. As highlighted by Saleem et al. (2018), they find it challenging to keep pace with the rapidly evolving advancements in IIoT technology, which can hinder the timely implementation of necessary standards. Moreover, consumer advocacy groups, albeit not as powerful as corporations and regulatory agencies, are extremely important for raising awareness of standards crucial for user anonymity and personal data protection. According to Kedia et al. (2020), these groups actively engage in the standardisation process by representing consumer interests and lobbying for stricter privacy regulations. Consumer pressures can even drive or push organisations to adopt standards (Hoogerbrugge et al., 2023), showing their efficacy within standardisation.

The studies that were under review adopted diverse methodological perspectives, such as qualitative case investigations and quantitative studies. While qualitative methods allowed for developing an understanding of the stakeholder interaction dynamics, quantitative methods were useful in studying the trends and patterns in stakeholder power dynamics (Kopetz & Steiner, 2022). The review also divided the legal, economic, communicative, and physical tools employed by stakeholders—showing that the efficacy of such tools depended on the stakeholder group and the context (Graz, 2018).

Several emerging themes were identified, notably the importance of power dynamics in standard-setting. Power imbalances enable dominant firms to influence standards to their advantage, often at the expense of smaller entities (Brass & Sowell, 2021). This dynamic contributes to the tension between rapid technological innovation and slower regulatory responses. Adding to the difficult to navigate power imbalances, research by Mukherjee (2019) indicates that the management of stakeholders within the standardisation process is a hard task because of the nature of the engaged constraints and variables. The review underscores the need for greater collaboration among stakeholders to develop more inclusive and widely accepted standards. Public-private partnerships are highlighted as a means to address these imbalances and achieve successful standardisation outcomes (Cranmer et al., 2022).

2.3. Analysis

The existing literature points out high level of hierarchy in favour of large firms that wield power and control over IIoT standardisation because of their massive capital and market strength (Trautman et al., 2020). This dominance enables them to call for proprietary standards that are favourable to their objectives, which may hinder the IIoT market from expanding and access to interoperability among the different IIoT platforms. Of the four dynamic interactions, this suppresses innovation from the smaller players and puts up entry barriers to new firms, which slows the overall growth in the IIoT ecosystem (Lechowski & Krzywdzinski, 2022).

Supervisory authorities are central to ensuring that the specific needs of the public interest, including security and fairness, are met by standards. However, they lag behind the advancement of IIoT technology. This delay can actually lead to issues such as standards becoming obsolete or very unfriendly to update, compounding problems of standards compatibility and vulnerability (Kedia et al., 2020). Firms that create de facto ICT standards can have great competitive advantage over firms that lag behind or are involved in committee based de jure standardisation (Lyytinen & King, 2006).

International, national, and local partners, including small and medium-sized enterprises, regulators, and consumer associations, should work together to formulate open and adaptable rules. Nonetheless, the competitively driven process, which is mainly challenging for large corporations, can significantly challenge such efforts, resulting in the establishment of multiple standards that do not support interoperability (Graz, 2018). In addition to the lack of interoperability, if multiple standards exist for longer periods of times, it limits economies of scale and network externalities – limiting total market growth (Tassey, 1999).

As for future research, (Kim et al., 2017) recommends there should be a further examination of the impact of stakeholders on IIoT standardisation. This should involve the use of real problems that show the differences in the strategies to be followed by various players in the market including the global firms, the regulatory agencies, and the consumers' organisations: something this thesis aspires to do. An analysis of this sort would yield interesting information on how power relations within and between organisations influence the process of standardisation, which could reveal how organisations can work together more effectively and fairly. Also, the research should examine the potential collaboration between the stakeholders to address the issues of proprietary standards and market consolidation (Fischer-Hübner et al., 2021).

Despite extensive research on technological standards and stakeholders, there remains a significant gap in understanding why achieving common standards is so challenging. This difficulty arises mainly due to issues within the stakeholder infrastructure, such as coordination problems and misaligned interests among stakeholders (van de Kaa et al., 2017). The knowledge gap identified by Van de Kaa (2017) in his paper on LED standardisation in Asia serves as the main motivation for this thesis.

The paper by De Vries et al. (2003) present methods for identifying and classifying stakeholders involved in standardisation efforts. Building on this foundation, Wang et al. (2016) found that organisations are more motivated to adopt a standard when a more diverse set of stakeholders is involved in its development. Similarly, van de Kaa (2023) demonstrated that stakeholder diversity and legitimacy are statistically significant determinants of standard adoption. De Vries et al. 2003 method for identifying and classifying stakeholders has been used successfully before by three scholars (Gottlieb, 2003) (Verheul, 2003) (Karaöz, 2004) (Jorritsma, 2024) and by van de Kaa, for example in 2015 and 2017.

2.4. Problem statement

This thesis focuses on standardisation and the IIoT industry within the European Economic Area (EEA), with a particular emphasis on the Benelux and Northern-west Europe regions. The problem owner includes both standardisation organisations and the IIoT industry, as they face challenges in creating interoperable, scalable standards that can be universally adopted. The urgency of addressing this issue is highlighted by sources such as McKinsey, which stress that without robust, agreed-upon standards in IIoT crucial areas like network protocols, the development of IIoT solutions may be slowed (Chui et al., 2021).

The literature review answers the question how according to literature, stakeholders and their characteristics influence the emergence of technological standards in IIoT. It indicates that large corporations dominate IIoT standardisation due to the resources they have and the goals they seek to achieve. Such dominance can have adverse consequences, such as the promotion of lock-in solutions, which negatively affect the compatibility, interoperability and evolution of the IIoT system. Also, while regulatory authorities are crucial in protecting the public interest, such as security and competition, they face problems with the fast-paced evolution of technology: Kedia (2020) shows that them lagging behind leads to obsolete or vulnerable standards. The review also stresses the significance of unifying a wide array of participants, including small businesses or consumers, in the development of inclusive and popular standards. To avoid such fragmentation and achieve efficient IIoT standardisation, the creation of open and versatile legal bases and the encouragement of Public-private partnership concepts are essential. Overcoming these power structures and increasing involvement from a wider range of stakeholders are critical factors in sustaining IIoT standards.

Regarding the policy implications of the research, there is a necessity for more studies on how flexible and adaptable policies should be in enhancing the framework towards the establishment of a universally acceptable standard for IoT. These policies should seek to enable and promote collaboration with the public and private sectors to foster the establishment of an open, secure, and interoperable IIoT that is efficient for all involved parties (Meddeb, 2016). Such policies can also help reduce power imbalances by encouraging public-private collaborations and engaging different factions to participate in the creation of IIoT standards that should be sustainable in the long run.

As the theory (Van de Kaa, 2017) (Kim et al., 2017) reflects, common standards are difficult to reach due to problems with stakeholder infrastructure. A stakeholder infrastructure can be made by using De Vries et al., 2003 method on identifying and classifying stakeholders. Multiple researchers have laid foundation to further research stakeholder infrastructures in standardisation, hence creating the opportunity for this thesis to research patterns in stakeholder characteristics and infrastructure with regards to the emergence of common standards. More specifically this research will dive into the IIoT space to see what challenges this particular industry holds. IIoT seems a particularly fitting industry because of its technical complexity, fast developments and wide range of stakeholders.

Building upon the knowledge gap identified and insights gained from the literature review, this study seeks to answer the following main research question:

MRQ: *To what extent do stakeholders' characteristics and infrastructure in standardisation processes influence the development of technological standards in industrial IoT?*

To address this main question, two sub-questions are posed:

SQ1: *Empirically, how does the classification of stakeholders—organised into a matrix based on their levels of power, legitimacy, and urgency—affect the emergence of technological standards in industrial IoT?*

This question explores real-world cases to examine, from an empirical perspective, the influence of stakeholder classification on the development of technological standards in IIoT.

SQ2: *How can agents such as policymakers, researchers, and businesses effectively influence stakeholders' characteristics and infrastructure to improve the standardisation process in Industrial IIoT?*

Building on insights from the literature review and empirical analysis, this question aims to explore how agents like policymakers, researchers, and businesses can strategically engage with stakeholders to influence their characteristics and infrastructure, ultimately improving the effectiveness and outcomes of the standardisation process in industrial IoT.

Drawing on findings from the literature review and empirical data, this question seeks to uncover how actors such as policymakers, researchers, or businesses can effectively intervene in or shape the stakeholder dynamics to impact the standardisation process in IIoT.

2.5. Empirical research approach

The method for finding patterns in for stakeholder salience in standardisation in the empirical analysis is based on De Vries et al., 2003. This paper outlines how to identify stakeholders and determine their positions regarding the standardisation process. Through desk-research, case study analysis and interviews, the stakeholder will be identified, and their characteristics will be researched. The stakeholder analysis applies both of De Vries' (2003) identification process and power-legitimacy-urgency framework to gain a comprehensive understanding of the stakeholders and their position in the standardisation process for each case. The systematic approach used here consists of three steps:

1) Case selection At first, a long list of possibly interesting cases within the IIoT space will be made. Thereafter the cases subject to this study will be selected based on relevance and availability of experts and information. For each of the IIoT phases two standards will be selected: one with market adoption and one without market adoption. Market adoption will be the variable that explains the success of the standards because it precisely captures the level of acceptance and implementation of a standard within the sector. It is a practical and quantifiable measure of a standard when it comes to impact and relevance. A widely adopted standard signifies that it addresses the market needs and has been well accepted by the important stakeholders, whereas the absence of market acceptance might indicate various flaws regarding complexity and awareness for market needs. The four IIoT phases and two levels of market adoption (yes/no) forms a series of eight and should yield a balanced result to recognise patterns in.

2) Stakeholder identification The stakeholders are identified through nine search directions as laid out by De Vries (2003). These search directions are based on the different ways on a stakeholder could pose relevant to the standardisation process. This systematic approach will help ensure that all relevant stakeholders are considered in our analysis. Each of the nine search directions poses a different angle, which can be seen below in Table 2.2.

Table 2.2: Search directions (de Vries et al., 2003)

No.	Search direction	Summary
1	Production chain	Includes all firms in production, from raw material suppliers to disposal. Involves transporters, service, and maintenance.
2	End users and related organisations	Separate stakeholders with significant influence on standards. Includes helpdesk providers, large firms, SMEs, and employees.
3	Designers	Stakeholders who design the product, often involved in production. Key in IT security system design.
4	Physical system	Interaction with technical systems, hardware/software compatibility. Involves developers of surrounding systems.
5	Inspection agencies	Conduct inspections or certifications. Include producers, customers, testing labs, and government bodies.
6	Regulators	Governments and regulators ensure standards comply with existing laws. Their cooperation boosts standard adoption.
7	Research and consultancy	Universities, research institutes, and consultants influence and are influenced by standards. Key in IT management.
8	Education	Involves organisations responsible for educational programs that include standards, ensuring clarity and accessibility.
9	Representative organisations	Serve member interests (e.g., unions, consumer groups). Often involved independently in standardisation processes.

3) Stakeholder classification When the stakeholders for the different cases are identified, they can be classified based on their power, urgency and legitimacy. This classification model of salience by Mitchell et al., 1997 shows the prominence of a stakeholder. After Mitchell et al., 1997, De Vries et al., 2003 adopted it in the paper on stakeholder identification in IT standardisation. Because of this, other stakeholder analysis theory, like Mendelow (1991) is less relevant. Additionally, most stakeholder analysis methods identify only on two axes, while Mitchell's 2003 method uses three axes: Power tells whether the stakeholder has the time, expertise and financial resources to affect the success of the standard. Urgency tells us about the degree to which stakeholders desire quick action. Legitimacy shows if the stakeholder's actions are deemed legitimate by others within the standardisation process. The assessment of stakeholders' characteristics is done through interviews, media sources, expert insights, and case studies. The experts selected and their backgrounds can be found in Table 2.4. A Venn diagram on stakeholder salience adopted from Mitchell et al. (1997) is depicted in Figure 2.2.

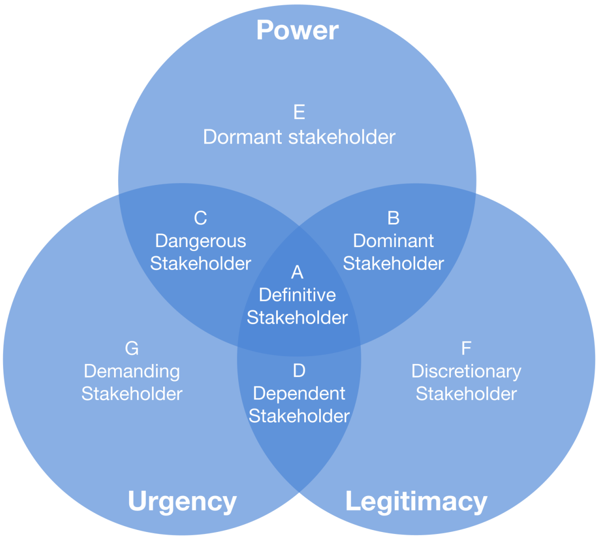


Figure 2.2: The stakeholder salience model (Mitchell et al. 1997)

The assessment of the power, urgency and legitimacy allows for the classification of stakeholders as for example dormant, dominant or dangerous, based on their possession of either of these factors. This matrix and classification then show the stakeholder's influence and involvement in the standardisation process. A series of these matrices will be constructed for eight industrial IIoT cases. Whether a stakeholder demonstrates these attributes—power, urgency, or legitimacy—is determined through coding of the interview data. For example, every time urgency is mentioned in connection with a stakeholder, this reference is coded under the "urgency" category. From this series of matrices, an analysis of the complete matrix, combining the eight stakeholder classifications, will be done. This analysis aims to identify patterns linking stakeholder classifications to the emergence of technological standards. This approach will help answer SQ2: In practice, how does the classification of stakeholders—organised into a matrix based on their levels of power, legitimacy, and urgency—influence the emergence of technological standards in IoT?

2.6. Case selection

Through desk research and exploratory talks with experts in the (I)IoT field, a list of dozens of standardisation cases has been put together. From this list eight cases have been selected based on their relevance, IIoT phase (1 through 4) and level of market adoption. Market adoption is measured as a variable in yes/no. Whether it is a yes or a no can be found in secondary sources, denoted in the table. The full table of the reviewed cases can be found in Appendix 6.2. Below in Table 2.3 the selected cases are shown:

Table 2.3: Selected cases for the empirical analysis

Building Block	Standard	Market adoption	Function	Chapter
1) Data Ingestion	RFID UHF	Yes (Chang, 2023)	Long range, high frequency RFID technology.	4.1.1
	Zephyr Project	No (Github, 2024)	Open-source Realtime operation system for resource-constrained IIoT devices.	4.1.2
2) Data Transmission	LoRaWAN	Yes (Fremont, 2024)	Long-range, low-power wireless protocol for IoT.	4.2.1
	Sigfox	No (IoTNow, 2022)	Low-power, wide-area network for IoT.	4.2.2
3) Data Processing	EPCIS	Yes (HDA Research Foundation, 2021)	Standard for sharing RFID data in the supply chain.	4.3.1
	UPnP	No (Arghire, 2020)	Network protocol for automatic device communication without requiring manual configuration.	4.3.2
4) Data Utilisation	Ignition	Yes (Hechtman, 2022)	Industrial automation platform for visualising and managing data.	4.4.1
	GE Predix	No (Bold Business, 2017)	IIoT platform designed to analyse data from industrial machines.	4.4.2

2.6.1. Expert selection

Following the case selection, potential interview participants were identified through various channels, including LinkedIn, academic paper contact information, web searches and conferences. These experts consequently were invited to participate in semi-structured interviews. The interview questions can be found in Appendix B. Due to time constraints and scheduling limitations, not all experts were interviewed in full. In some cases, insights were gathered through conversations or presentations at conferences. Where applicable, this has been supplemented with information from existing research, professional profiles, and case studies. The data gathered from these sources collectively informed the empirical research. The in-text citations indicate the source from which the information was obtained. For example, [1] for Expert 1 or a parenthetical citation for a public source. The corresponding sources are for the purposes of this publication anonymously listed in Table 2.4 below and the reference list.

Table 2.4: List of selected experts for primary empirical data collection

Expert No.	Affiliation	Position	Standard
Expert 1	IoT Solution Provider	Director	LoRaWAN
Expert 2	IoT Solution Provider	Director	LoRaWAN
Expert 3	Digital Manufacturing	Consultant	General
Expert 4	Standards Developing	Manager	EPCIS
Expert 5	IoT Solution Provider	Chief Officer	LoRaWAN
Expert 6	Telecommunications	Product Manager	LoRaWAN
Expert 7	Academia	Professor	General
Expert 8	Standards Developing	Manager	EPCIS / RFID UHF
Expert 9	RFID Technology	Chief Officer	RFID UHF
Expert 10	Semiconductors	Fellow	LoRaWAN / General
Expert 11	R&D Engineering	Chief Officer	General
Expert 12	Embedded Systems	Engineer	IRNAS
Expert 13	IoT Platform Provider	Founder	LoRaWAN / General
Expert 14	Antenna Design	Chief Officer	General
Expert 15	Industrial Automation	Manager	Ignition / General
Expert 16	Academia	Professor	General

2.7. Conclusion

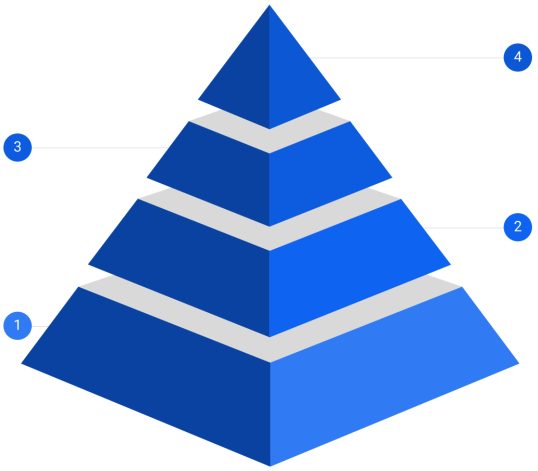
A literature review that explored the existing body of research on stakeholder influence in the standardisation processes of the Industrial Internet of Things (IIoT). The review identified key themes, such as the dominance of large corporations in developing standards, the important role of stakeholder diversity and the challenges of achieving interoperability in (IIoT) standardisation. The lack of understanding of stakeholder dynamics and their impact on the emergence of technological standards led to the problem statement and research questions. The research questions aim to give insight to what extent and which stakeholder characteristics influence the development of technological standards in IIoT.

To answer these questions, on the basis of the literature review the empirical approach was designed. It uses the search directions for stakeholders (De Vries et al., 2003) and stakeholder salience model (Mitchell et al., 1997) to identify subsequently and classify stakeholders based on their power, legitimacy, and urgency. Eight IIoT cases have been selected for this stakeholder analysis, from four different phases and two levels of market adoption, resulting in diverse standards to give a comprehensive perspective. The eight cases are subject to the identification and classification of their respective stakeholders within the standardisation process. This is done by using primary data from the expert sources listed in Table 2.4 and secondary data collection through desk research.

3

Finding stakeholder salience patterns in IIoT standardisation

Standards within the Internet of Things are categorised in one of four phases: Data Ingestion, Data Transmission, Data Processing and Data Utilisation. Each of these phases is crucial for the system to work. A simple IIoT system for your home would look something like this: A sensor within the house ingests temperature data. This data is then transmitted wirelessly via Wi-Fi to a cloud platform. The data processes into meaningful information. Finally, the processed data is displayed on a mobile app, allowing the user to monitor their home temperature in real-time. A more complex IIoT solution would look something like this: Sensors within a factory monitor equipment vibration data. This data is then transmitted via an industrial network to a central control system or cloud data lake. The data is processed (aggregation, decrypting, transformation, etc.) into actionable insights. Finally, the processed data is displayed on an operator dashboard, allowing maintenance teams to monitor equipment health in real-time and schedule predictive maintenance. The phases of IIoT fit naturally within the standard framework for standardisation. Compared to the Open Systems Interconnection (OSI) model, which was developed by ISO to provide standardised layers for standards development, each of the four phases shown in Figure 2 correspond with OSI's layers. An overview of the phases can be found in Figure 3.1. This figure is adopted from (Grasso, 2023), (Deloitte, 2022) & (Rastegari, 2019), who divide (I)IoT in four or five different phases. Derived from these sources, Figure 3.1 bundles this information and shows the different phases this empirical analysis will address. The following sections go over each of the four phases, showing the eight standardisation cases and the stakeholders that are involved.



Data Utilisation
Often involves human-computer interaction and an application. Presents processed data via dashboards & insights. Relates to the OSI Session and Presentation layers (5&6) - where data is structured.

Data Processing
Data is processed, e.g. aggregated, decrypted and/or transformed. Aligns with the OSI Physical and Data Link layer (1&2) - where sensors collect raw data.

Data Transmission
Data is transmitted to a local or cloud solution. Most commonly via cables, gateways or cellular. Corresponds to the OSI Application Layer (7) providing user interfaces and insights.

Data Ingestion
IoT sensors collect data from the environment (e.g. temperature or pressure). Corresponds to the OSI Network and Transport layers (3&4) - routing and delivering data.

Figure 3.1: Phases in IIoT. Adopted from (Grasso, 2023), (Deloitte, 2022) & (Rastegari, 2019)

3.1. Data ingestion standards

Data ingestion is the first phase in IIoT systems. Devices like sensors collect raw data from the environment, converting physical ‘information’ into digital signals. This could mean capturing temperature, motion, humidity, pressure or the registration through scanning, detecting or reading. While the current market offerings are quite cloud centred, meaning that most solutions move the data from the sensor to the cloud, edge computing is the next big thing. Edge computing revolves around the fact that the preliminary data processing occurs near the data source, for example on the PCB itself, to reduce latency, bandwidth and energy usage.

As for standardisation, data ingestion corresponds to ISO’s OSI model to Physical Layer 1, involving hardware sensors and transceivers and the Data Link Layer 2, managing error detection and data links. The two standards that have been selected for this phase are RFID UHF (Ultra High Frequency) and the Zephyr Project. RFID UHF uses electromagnetic fields to automatically identify, and track RFID tags attached to objects. This makes it ideal for purposes like inventory management and asset tracking. The Zephyr Project is an open-source real-time operating system (RTOS) designed for IIoT devices with limited energy or bandwidth resources. It aims to provide a secure and scalable platform to manage the hardware side of the sensors. Comparatively, RFID UHF specialises in automatic identification and data capture of physical objects, like OSI model’s Physical Layer 1. The Zephyr Project offers a software solution supporting the hardware of a wide range of sensors and multiple data types, like OSI model Data Link Layer 2.

3.1.1. RFID UHF

Radio Frequency Identification on Ultra High Frequency (RFID UHF) is a technology that uses radio waves to identify tags on objects. It is a de jure standard under ISO/IEC 18000-6:2013. The high frequency of the standard makes for a long read distance. At the start of this millennium, big companies in supply chain and retail came together to develop standardised protocols, leading to a first GS1 standard by 2007. The RFID sector is strongly pushed by RFID integrators such as chip manufacturers, RFID label vendors and system integrators. The main catalyst of the technology in Europe has been Decathlon where it implemented the usage of the technology throughout the whole supply chain. It started source-tagging all its own branded products at the manufacturing plants in 2013, and since a few years, shoppers use the technology to check-out in their stores (Cisper, n.d.).

RFID systems consist of three main components: tags, readers, and a backend system for data processing. In UHF RFID, the tags contain an antenna and an integrated circuit (IC) with a unique identifier. The reader emits radio waves within the UHF range, powering the passive RFID tags. This interaction allows the reader to capture information such as the tag’s unique identifier and additional data. The data is then processed, which for examples facilitates real-time tracking and inventory management. In Europe, the radiofrequency was standardised by ETSI, determining that the used frequency should be 865.6 - 867.6 MHz (GS1, 2024).

In an interview with Expert 8 the question that came to mind with this technology was: If retail stores are able to widely deploy RFID, enabling easy checkout and supply chain visibility, why isn’t it more widely adopted? Well, the dissuasion when it comes to applying RFID is that 100% of your products need to be tagged for the system to work effectively. Expert 8: ”Supermarkets won’t work because you need 100% [RFID tagging], otherwise it won’t work. Because if a product costs 30 cents, then 5-10 cents [for an RFID tag] on a product that costs so little is too much... If you don’t have 100% of your items tagged, then it’s chaos at checkout.”

This presents a significant challenge for supermarkets and similar retailers. Unlike specialised stores like Decathlon, which successfully implemented RFID, supermarkets face unique obstacles. This economic barrier makes it unfeasible for supermarkets to implement RFID across their entire inventory. Moreover, if not all items are tagged, it creates chaos at checkout: what to do with the untagged items? How do they need to be settled and tallied?

Based on the interviews and desk research, the following Table 3.1 outlines the key stakeholders involved in the RFID UHF standardisation process, organised by the search direction they originated from:

Table 3.1: Stakeholders per search direction for RFID UHF

Search Direction	Stakeholder	Description
Production Chain	RFID manufacturers [8]	Produce RFID tags and components for various industries.
	Logistics companies [8]	Use RFID UHF to track goods in transit, streamline supply chains.
	RFID Solution providers [9]	Develop end-to-end RFID UHF solutions, including software and hardware integration.
End-users and related organisations	Decathlon [9]	A major retailer using RFID for inventory management and supply chain optimisation.
	Other retailers (e.g., H&M, Zara) [8]	Utilise RFID UHF for stock control, logistics, and customer experience.
Regulators	Government regulators [8]	Create policies and regulations for RFID frequency use and data privacy.
	Standard setting bodies (ETSI for EU RFID) (EPCIS, 2024)	Set the European used radio frequencies for RFID UHF
Inspection agencies	Certification bodies (e.g., GS1 Europe) [8]	Provide standards and certifications to ensure RFID interoperability and compliance.
Research and consultancy	IT Consulting firms [9]	Offer consulting services to businesses for RFID UHF adoption and integration.
Representative organisations	Consumer organisations (EDRi, 2009)	Monitor RFID UHF use to protect consumer privacy and rights.
	RFID Industry associations (e.g., RFID Experts group - AIM Europe) (AIM Global, n.d.)	Advocate for RFID technology adoption, set industry standards.

As shown in Table 3.1, eleven different stakeholders were identified across six search directions. With these stakeholders mapped out, their roles are further assessed by evaluating their power, legitimacy, and urgency in relation to the RFID UHF standard. From the interviews with Experts 8 and 9 can be found that RFID manufacturers have high power due to their control over technology production and development, legitimacy as key enablers of the RFID infrastructure, and urgency driven by the demand for innovative solutions. Decathlon and other retailers, like H&M and Zara, hold significant power due to their influence on supply chain adoption, legitimacy as major RFID users, and urgency to enhance efficiency and traceability. Logistics companies such as DHL exhibit high power and legitimacy by managing RFID-enabled networks and face urgency due to competitive pressures and operational optimisation. Government regulators and standardisation organisations, including ETSI and certification bodies like GS1 Europe, possess power and legitimacy in shaping regulatory and standard frameworks; however, their urgency is less pronounced, focusing more on long-term compliance and interoperability. RFID solution providers and consumer organisations, while legitimate and facing pressing concerns like user privacy, lack sufficient power to act independently. Lastly, discretionary stakeholders, including IT consulting firms and RFID industry associations, have legitimacy through their support roles but are neither urgent nor influential. The following Table 3.2 categorises each stakeholder based on their power, urgency and legitimacy, offering a clear picture of the stakeholders' characteristics and infrastructure:

Table 3.2: Stakeholder salience for RFID UHF

Stakeholder	Power	Legitimacy	Urgency	Type
RFID manufacturers	X	X	X	A (Definitive) [8]
Decathlon	X	X	X	A (Definitive) [9] [9]
Retailers (e.g., H&M, Zara)	X	X	X	A (Definitive) [8]
Logistics companies	X	X	X	A (Definitive) (DHL Trend Research, n.d.)
Government regulators	X	X		B (Dominant) [8]
Standardisation organisations (e.g., ETSI)	X	X		B (Dominant) [8] [9]
Certification bodies (e.g., GS1 Europe)	X	X		B (Dominant) [8]
RFID Solution providers		X	X	D (Dependent) [8]
Consumer organisations		X	X	D (Dependent) (Clarke & Flaherty, 2008)
IT consulting firms		X		F (Discretionary) [9]
RFID Industry associations (e.g., RFID Experts Group - AIM Europe)		X		F (Discretionary) (AIM Global, n.d.)

RFID UHF manufacturers, major retailers and large logistic companies all have power, legitimacy and urgency in the industry. This means that they're definitive stakeholders with significant influence over the standardisation process of RFID UHF. Other noteworthy elements from the table are the wide range of discretionary stakeholders, which is most likely due to a lack of involvement in the implementation process.

3.1.2. Zephyr Project

The Zephyr Project is a real-time operating system (RTOS) designed for embedded devices (for example, the computer part of an IIoT temperature sensor). The system is open source and has the goal to become the de facto RTOS through uniting developers and users in a community to together to develop the best and scalable solution within the RTOS field. It is optimised for resource-constrained devices on almost all platforms and architectures due to its open-source properties. The development of the Zephyr Project began in earnest in 2015, with its first official public release in early 2016. Over the years, the project has seen multiple iterations. Major milestones in its development include the addition of advanced security features, support for various processor architectures, and compatibility with a growing range of hardware platforms. In 2018, the Zephyr Project introduced the Zephyr Security Working Group. This began the effort to improve the security in RTOS. The problem was that these security improvements came relatively late in the project's lifecycle, making that many companies had already committed to other RTOS solutions.

A key feature of the Zephyr Project is its collaborative nature. From the beginning the project attracted a diverse range of stakeholders with one of the primary driving forces behind the project being Linux Foundation. However, aside from its ambitious vision, Zephyr has struggled to gain widespread market adoption. More established platforms, limited hardware compatibility and the challenges of fostering a vibrant open-source community are great challenges for the platform. The complete software can be found on Github, and extra modules can be found and exchanged within the community.

Based on the interviews and desk research, the following Table 3.3 outlines the key stakeholders involved in the Zephyr Project standardisation process, organised by the search direction they originated from:

Table 3.3: Stakeholders per search direction for the Zephyr Project

Search Direction	Stakeholder	Description
Production chain	Embedded device manufacturers [10]	Develop hardware (e.g., microcontrollers) that the Zephyr RTOS runs on.
	Chip vendors (e.g., Intel, NXP) (Nashif, n.d.)	Provide the microprocessors and system-on-chips (SoCs) supported by Zephyr.
End users and related organisations	End users (e.g., IIoT device makers) (Nashif, n.d.)	Use the Zephyr Project RTOS to build IIoT devices, focusing on embedded systems.
	Zephyr Project members (e.g., Analog Devices, Google, Intel) (Zephyr Project, n.d.)	Platinum, Silver & Associate members of the Zephyr project, funding and developing the application's development.
Designers	Open-source developers [10]	Contribute to the development and maintenance of the Zephyr RTOS, enhancing its features and stability.
Research and consultancy	Universities and research institutes (e.g., Northeastern University, Research Institutes of Sweden) (Zephyr Project, n.d.)	Conduct research on embedded systems, contributing to Zephyr's development and implementation best practices.
Representative organisations	Linux Foundation [10] (Linux Foundation, 2024)	Support Zephyr's growth, provide the base platform, and promote open-source standards for IIoT and embedded systems.

As shown in Table 3.3, eight different stakeholders were identified across five search directions. With these stakeholders mapped out, their roles are further assessed by evaluating their power, legitimacy, and urgency in relation to the Zephyr Project standard. With intelligence gathered from Experts 10, 11, 12 and popular sources it can be derived that Zephyr Project Members, such as Analog Devices, Google, and Intel, were classified as definitive stakeholders due to their financial contributions and decision-making authority, giving them power. Their legitimacy shows in their roles as core contributors to the project's mission, while urgency arises from the rapid pace of IoT innovation and competitive pressures. Similarly, end users like IIoT device makers are definitive stakeholders, having influence through adoption and feedback: their needs are critical and time-sensitive. Embedded device manufacturers and chip vendors, including Intel and NXP, were identified as dominant stakeholders. They hold substantial power due to their role in hardware production and alignment with Zephyr's platform requirements, alongside legitimacy as important industry players. However, they lack direct urgency compared to stakeholders implementing or driving the project's adoption. The Linux Foundation, as a project host, also fits this category, holding power and legitimacy through governance and resource allocation. Open-source developers, arose as dangerous stakeholders due to their potential to significantly disrupt the project's progress if dissatisfied or disengaged. Their urgency stems from the project's dependency on their voluntary contributions. Lastly, universities and research institutes, such as Northeastern University and the Research Institutes of Sweden, were classified as discretionary stakeholders. They contribute legitimacy through research and innovation but lack direct power or urgency. The following Table 3.4 categorises each stakeholder based on their power, urgency and legitimacy, offering a clear picture of the stakeholders' characteristics and infrastructure:

Table 3.4: Stakeholder salience for the Zephyr Project

Stakeholder	Power	Legitimacy	Urgency	Type
Zephyr Project Members (e.g., Analog Devices, Google, Intel)	X	X	X	A (Definitive) [10] [11] (Zephyr Project, n.d.)
End users (e.g., IIoT Device Makers)	X	X	X	A (Definitive) [11]
Embedded device manufacturers	X	X		B (Dominant) [10]
Chip vendors (e.g., Intel, NXP)	X	X		B (Dominant) (Intel, n.d.)
Linux Foundation	X	X		B (Dominant) [10] [11] (Linux Foundation, n.d.)
Open-source developers	X		X	C (Dangerous) [11] (Plate et al., n.d.)
Universities and research institutes (e.g., Northeastern University, Research Institutes of Sweden)		X		F (Discretionary) [11] (Zephyr Project, n.d.)

Table 3.4 reveals that there's only a small amount of stakeholders involved. Additionally, none of the stakeholders are regulatory, governmental or certifying stakeholders. Also, the inclusion of open-source developers as a main stakeholder is interesting because of the lack of legitimacy which makes it a dangerous stakeholder.

3.2. Data transmission standards

Data transmission is the second phase in IIoT systems. After sensors collect the data, this data must be transmitted from the devices to a central server or cloud platform for processing. This involves sending data over networks using communication protocols. Transmission can be wireless or wired depending on the requirements. While traditional methods often rely on cellular networks or Wi-Fi, low-power wide-area networks (LPWAN) are gaining popularity for IIoT applications. This is due to their ability, as the name suggests, to transmit small amounts of data over long distances with low power consumption.

With regards to standardisation, data transmission corresponds to the OSI model's Network Layer 3, which handles routing and addressing, and the Transport Layer 4, responsible data transfer. The two standards that have been selected for this phase are LoRaWAN and Sigfox 0G. LoRaWAN (Long Range Wide Area Network) is an open-standard protocol designed for wireless communication in LPWANs. It uses a modulation technique named LoRa, that, without diving too deep into the dazzling technical details, is based on a radio communication technique derived from the Chirp spread spectrum, that uses changing frequencies, like a chirping sound, which makes the signal clear and recognisable over long distances. Sigfox is a global IIoT network operator that provides a dedicated LPWAN service using ultra-narrowband technology. It's a way of sending information using very tiny slices of radio waves—much narrower than usual. The Sigfox 0G standard focuses on offering devices the ability to transmit small messages over long distances with very low power consumption. It's suited for applications such as asset tracking and security systems.

Both LoRaWAN and Sigfox 0G aim to be the de facto standard for long rage, low energy networking, but with different properties. Also, both standards stretch the OSI model's Network Layer 3 and Transport Layer 4 - "transmission of data segments and managing a multi-node network" (Microsoft, 2023).

3.2.1. LoRaWAN

LoRaWAN emerged as a promising standard for energy-efficient, long-range, low-power wireless communication, particularly suited for Internet of Things (IoT) applications. While it offers significant advantages like cost-effectiveness and wide coverage, LoRaWAN faced challenges in gaining widespread adoption. Key stakeholders include Semtech (the original developer), the LoRa Alliance (managing the standard), network operators like KPN, and community initiatives like The Things Network and Helium. The technology is seen as potentially disruptive to traditional telecom providers due to its low infrastructure and operational costs. Despite some initial hurdles, LoRaWAN is gaining traction, driven by factors such as climate change, energy transition, and the need for efficient IIoT connectivity in various sectors including municipalities, water management, agriculture and offshore operations. The interest from these sectors is due to the low-power, long-range properties of LoRaWAN. LoRaWAN its stakeholders like Semtech and The Things Network aim for it to become a de facto standard, and it is already a de jure standard of the International Telecommunication Union (ITU) under ITU-T Y.4480.

Based on the interviews and desk research, the following Table 3.5 outlines the key stakeholders involved in the LoRaWAN standardisation process, organised by the search direction they originated from:

Table 3.5: Stakeholders per search direction for LoRaWAN

Search Direction	Stakeholder	Description
Production chain	Semtech	The original developer of LoRa technology, holding a monopoly on the chips used in LoRa-based devices. [1][2]
	Device manufacturers	Companies that produce IIoT devices equipped with LoRa technology for various applications (e.g. sensors, smart meters).
End users and related organisations	Telecom companies	Telecom providers that offer LoRaWAN services. In the Netherlands, KPN is the largest provider, offering nationwide LoRaWAN coverage. Other international companies include providers like Orange (France), Swisscom (Switzerland), and Bouygues Telecom (France). [1][2][5]
	The Things Industries	A commercial entity providing LoRaWAN solutions, including hardware, software, and infrastructure to support LoRaWAN deployment.[2][5][6]
	Municipalities	Local governments that implement LoRaWAN networks for smart city applications, such as water management, traffic monitoring, and environmental sensing. (Provincie Drenthe, n.d.) (Hartholt, 2015)
Designers	Solution providers	Companies that provide partial or end-to-end solutions for LoRaWAN technology into specific use cases. [5]
Regulators	Government regulators	Governments regulate data privacy and cybersecurity. In contrast to other network protocols or radio frequencies, there’s no process of frequency allocation. [1][2]
	Standard setting bodies	Organisations such as ETSI (European Telecommunications Standards Institute) that oversee the regulation and standardisation. [5][6]
Education	Academic institutions	Universities and research institutions that conduct research on LoRaWAN technology – the standard began as a student idea. [1][2]

Continued on next page

Table 3.5 – continued from previous page

Search Direction	Stakeholder	Description
Representative organisations	The Things Network	A global community-driven initiative that provides open access LoRaWAN networks, allowing anyone to connect their devices to the network and contribute to the infrastructure. [1][2][5]
	LoRa Alliance	A consortium of companies that promote the use and standardisation of LoRaWAN technology globally, ensuring interoperability and driving adoption. [1][2][5]

As shown in Table 3.5, eleven different stakeholders were identified across six search directions. With these stakeholders mapped out, their roles are further assessed by evaluating their power, legitimacy, and urgency in relation to the LoRaWAN standard. From the interviews with Experts 1, 5 & 6 and publications like Hartholt (2015) and Slats (2020), the stakeholder salience table for LoRaWAN was constructed to identify the roles and significance of various stakeholders. Semtech, the creator of LoRa technology and current main chipmaker, was classified as a definitive stakeholder due to its high power, legitimacy as the primary technology developer and urgency because of its leadership in advancing LoRaWAN's adoption. The Things Industries and The Things Network also emerged as definitive stakeholders from the interviews, driving the adoption and implementation of open IoT networks. The LoRa Alliance was similarly categorised as a definitive stakeholder because the interviews covered its governance role, providing legitimacy and influencing standards with urgency tied to market needs. Telecom companies were included in the same category due to their critical role in deploying LoRaWAN infrastructure and connecting various applications. Device manufacturers and solution providers were identified in the interviews as dominant stakeholders, as they contribute significantly to hardware and software alignment with LoRaWAN standards, yet lack the immediate urgency of network deployment for their own use. The municipalities are indicated as dependent stakeholders by the interviews: they have a role in implementing LoRa-based solutions, for example in smart city projects, but are reliant on partnerships with more powerful entities. Government regulators, standard-setting bodies, and academic institutions were classified as discretionary stakeholders through the interviews. They provide legitimacy through regulations and research contributions but lack direct influence or pressing urgency in the immediate deployment of LoRaWAN systems. The following Table 3.6 categorises each stakeholder based on their power, urgency and legitimacy, offering a clear picture of the stakeholders' characteristics and infrastructure:

Table 3.6: Stakeholder salience for LoRaWAN

Stakeholder	Power	Legitimacy	Urgency	Type
Semtech	X	X	X	A (Definitive) [1][2] (Semtech, n.d.)
The Things Industries	X	X	X	A (Definitive) [1][6]
The Things Network	X	X	X	A (Definitive) [1][6] (The Things Industries, n.d.)
LoRa Alliance	X	X	X	A (Definitive) [1][5] (LoRa Alliance, n.d.)
Telecom companies	X	X	X	A (Definitive) [1][6]
Device manufacturers	X	X		B (Dominant) [2][5]
Solution providers	X	X		B (Dominant) [1][5][6]

Continued on next page

Table 3.6 – continued from previous page

Stakeholder	Power	Legitimacy	Urgency	Type
Municipalities		X	X	D (Dependent) [1] (Provincie Drenthe, n.d.) (Hartholt, 2015)
Government regulators		X		F (Discretionary) [1][2]
Standard setting bodies		X		F (Discretionary) [5][6]
Academic institutions		X		F (Discretionary) [1][2][5] (Slats, 2020)

What's noticeable from Table 3.6 is that government regulators are classified as Discretionary stakeholders, as they have legitimacy in the field but may not have significant power or urgency in the standardisation process. For this type of stakeholders this is an abnormality: in many situations government(al subsidiaries) hold some type of power or urgency. But since the LoRaWAN network is open for everybody and no radio permits are needed, this is not the case here. The setup of a LoRaWAN gateway does not have to be compliant with any rules or regulations.

The LoRaWAN standard has gained widespread market adoption in the IIoT industry, recognised for its effectiveness in low-power, wide-area network applications. Despite this agreement on the standard itself, some challenges to its widespread adoption persist. Semtech's current monopoly on LoRa chips creates a potential bottleneck, though increasing demand is expected to drive innovation in chip manufacturing. Traditional telecom companies, initially viewing LoRaWAN as a threat to their established models, are now beginning to recognise its potential as a complementary technology for their IIoT offerings. The technology continues to mature, and currently works on 130 million devices (In comparison with 2.6 billion Bluetooth & 973 million cellular devices). It also faces healthy competition from other low-power or long-range IIoT connectivity solutions such as LTE-M, NB-IoT, and Sigfox, driving further innovation in the LPWAN space, but LoRa acts as the frontrunner.

The growing adoption of LoRaWAN is driven by collaborative efforts from major stakeholders, who are increasingly pushing for widespread implementation. This unified approach is accelerating adoption rates and fostering a more cohesive ecosystem. As the technology matures and success stories emerge, potential adopters are gaining confidence in LoRaWAN's long-term viability and support, further boosting its adoption.

3.2.2. Sigfox 0G

Sigfox is a French network operator specialised in wireless networks for low-power objects like smart meters. Although its 2016 USD 600 million valuation, it went bankrupt in January 2022 and was reacquired by French network operators and UnaBiz, a Singaporean IIoT solution provider, for EUR 25 million three months later. Sigfox focusses on the development of Sigfox 0G, a low-power wide-area network (LPWAN). Sigfox currently supports the connectivity of 11 million devices worldwide. The aim of its parent company UnaBiz is for Sigfox to become a de facto standard in the LPWAN realm. The interest in Sigfox stems from its simplicity, cost-effectiveness and ability to operate in areas with poor traditional cellular coverage. The hesitancy in the technology's development as a de facto standard originate from the limited bandwidth and scalability and the dependence on the key stakeholder's sustainability.

Based on the interviews and desk research, the following Table 3.7 outlines the key stakeholders involved in the Sigfox 0G standardisation process, organised by the search direction they originated from:

Table 3.7: Stakeholders per search direction for Sigfox 0G

Search Direction	Stakeholder	Description
Production chain	Sigfox operators	Operate the Sigfox network infrastructure, providing connectivity services for Sigfox devices in various regions. (Michaslki, 2017) (Sigfox, n.d.)
	Device manufacturers (e.g., Adeunis, Sagemcom)	Design and produce IIoT devices and sensors compatible with the Sigfox 0G network. (Adeunis,n.d.)
	Chip vendors (e.g., ON Semiconductor, STMicroelectronics)	Provide the radio transceivers and chipsets for Sigfox-enabled devices, ensuring compliance with Sigfox's protocol. (Sigfox Partner Network, n.d.)
End users and related organisations	End users (e.g., Logistics companies, utility providers)	Implement Sigfox-enabled IIoT solutions for applications like asset tracking, utility metering, and environmental monitoring. [13]
	Solution providers (e.g., Thinxtra, UnaBiz)	Offer integrated IIoT solutions using the Sigfox network, including software, hardware, and platform services. (UnaBiz, n.d.)
Research and consultancy	Research institutes (e.g., IIoT Research Labs, IEEE)	Conduct research on LPWAN technologies and Sigfox's application in various IIoT fields, influencing its development and adoption. (Lavric et al.,2019)
Representative organisations	Sigfox S.A.	The company behind Sigfox, responsible for maintaining the global network, protocol development, and promoting adoption of the Sigfox standard. [13] (UnaBiz, n.d.)

As shown in Table 3.7, seven different stakeholders were identified across four search directions. With these stakeholders mapped out, their roles are further assessed by evaluating their power, legitimacy, and urgency in relation to the Sigfox 0G standard. With help from Expert 13 and sources such as Lavric et al. (2019), Heliot Group (2024), and Morris (2023), the stakeholder salience table for Sigfox 0G was constructed. From these sources it can be told that Sigfox operators, such as Heliot, were classified as definitive stakeholders due to their control over network deployment, making them powerful. Their legitimacy originates from the upkeep of the Sigfox ecosystem, and urgency arises from the competitive landscape and the need for expansion. Similarly, device manufacturers like Adeunis and Sagemcom are definitive stakeholders, as their influence is critical in the production of devices that utilise Sigfox technology. This makes their contributions both legitimate and time-sensitive. Solution providers, including Thinxtra and namely UnaBiz, also emerged as definitive stakeholders from the sources because of their involvement in implementing and maintaining Sigfox solutions. Chip vendors, such as ON Semiconductor and STMicroelectronics, were identified through the sources as dominant stakeholders: They hold power due to their role in hardware production and alignment with Sigfox requirements, alongside legitimacy as essential and recognised players in the ecosystem. However, their urgency is relatively lower than the before named stakeholders.

Lunden (2022) classified Sigfox S.A. as a dangerous stakeholder. It lacks legitimacy due to its financial and operational challenges. It still possesses power as the founder of the Sigfox technology and urgency stemming from itsposition in the market. End users, such as logistics companies and utility providers, were categorised as discretionary stakeholders. They provide legitimacy by adopting Sigfox solutions but there are no signs of direct influence or urgency in Sigfox' standardisation process. Research institutes, such as IIoT Research Labs and IEEE, were also identified as discretionary stakeholders by the sources as they contribute legitimacy through research. The following Table 3.8 categorises each stakeholder based on their power, urgency and legitimacy, offering a clear picture of the stakeholders' characteristics and infrastructure:

Table 3.8: Stakeholder salience for Sigfox 0G

Stakeholder	Power	Legitimacy	Urgency	Type
Sigfox operators (e.g. Heliot)	X	X	X	A (Definitive) (Lavric et al., 2019) (Heliot Group, 2024)
Device manufacturers (e.g., Adeunis, Sagemcom)	X	X	X	A (Definitive) (Adeunis,n.d.) (Sigfox Partner Network, n.d.)
Solution providers (e.g., Thinxtra, UnaBiz)	X	X	X	A (Definitive) (Morris, 2023)
Chip vendors (e.g., ON Semiconductor, STMicroelectronics)	X	X		B (Dominant) (Sigfox Partner Network, n.d.)
Sigfox S.A.	X		X	C (Dangerous) (Lunden, 2022)
End users (e.g., Logistics companies, utility providers)		X		F (Discretionary) [13]
Research institutes (e.g., IIoT Research Labs, IEEE)		X		F (Discretionary) (Lavric et al., 2019)

The current situation of Sigfox 0G shows challenges due to the lack of diverse stakeholders, particularly in the areas of regulators and standardisation bodies. This absence complicates the adoption and long-term viability of Sigfox, as regulatory involvement could be important for ensuring compatibility and adherence to standards. The power within the ecosystem lies heavily with the operators, who can directly influence network reach and implementation. However, Sigfox S.A., the company behind the technology, lacks the necessary legitimacy, making it a potentially dangerous stakeholder. This poses a risk to the market perception.

On a positive note, recent rumours of a collaboration between Sigfox and LoRaWAN could benefit both technologies by combining their strengths, enhancing coverage, and improving network reliability. Yet, the success of this partnership will depend on how effectively it addresses current limitations. Additionally, Sigfox's use of an unregulated radiofrequency allows flexibility but presents challenges for standardisation. The crowded nature of this frequency band may result in interference, potentially affecting the quality of service and complicating efforts to prevent signal congestion over time.

3.3. Data processing standards

Data processing is the third phase in IIoT systems. After data has been transmitted from devices to a central server or cloud platform, it needs to be processed to extract meaningful insights and enable informed decision-making. This involves organising, analysing, and interpreting the collected data. Data processing can include filtering out irrelevant data, aggregating data points, transforming data formats, and integrating data from multiple sources to provide a coherent picture.

With regards to standardisation, data processing corresponds to the OSI model's Session Layer 5, which manages sessions between applications; the Presentation Layer 6, which translates data between application and network formats. The two standards that have been selected for this phase are EPCIS and UPnP: EPCIS (Electronic Product Code Information Services) is a GS1 standard designed to enable businesses to capture and share information about the movement and status of products, logistics units, and other assets in the supply chain. It provides a standardised way to record and communicate event data—such as what happened to an item, when and where it happened. Crucial information for supply chain visibility, of course. EPCIS allows different systems and organisations to interoperate by providing a common language for data exchange, facilitating better tracking, tracing, and authentication of products.

UPnP (Universal Plug and Play) is a set of networking protocols that allows devices to automatically discover and communicate with each other on a network, enabling seamless data sharing and control (Open Connectivity Foundation, 2016). While UPnP is often associated with device discovery and configuration, it also plays a role in data processing by allowing devices to expose their capabilities and share data services without manual setup. Comparatively, EPCIS focuses on capturing and sharing detailed event data across different organisations and systems, aligning with the OSI model's Presentation Layer 6, standardising how data is formatted and communicated, ensuring interoperability in complex environments like global supply chains. On the other hand, UPnP facilitates seamless communication and data sharing between devices on a local network, corresponding to the Session Layer 5 and Presentation Layer 6 of the OSI model. It manages sessions between devices and ensures that data is presented in a format that can be understood by different systems, thus aiding in the processing and integration of data from various sources within a network.

3.3.1. Electronic Product Code Information Services (EPCIS)

EPCIS is standard for sharing supply chain event data, particularly in industries like fast-moving consumer goods (FMCG), food industries, technical industries and pharmaceutical companies. The European rail sector is also a large user of the standard. Through the standard, businesses can capture and share product information with the supply chain, showing locations and statuses, allowing for traceability. It is not limited to manufacturing and supply chain contexts - EPCIS can also support a variety of use cases, including compliance and tracking. There are two 'versions' of the de jure standard: a GS1 developed instance, and an ISO/IEC (ISO/IEC 19987 + 19988) standard developed on the basis of the GS1 standard used for regulatory purposes. It is expected that there will be an updated version of the standard by 2025, improving on some errors in implementation and implementing user feedback.

In the standardisation process of EPCIS, stakeholders play two main roles: contributing user requirements and driving technical development. Retailers and manufacturers often bring in user perspectives, while solution providers and academics focus on prototyping and technical aspects. EPCIS standardisation involves gathering business requirements, developing solutions, and iterating based on feedback. The process is managed by GS1: it's a collaborative and democratic process ensuring that each participating organisation has a voice, regardless of size. This ensures relevance and effectiveness in meeting industry needs. The flexibility of EPCIS also allows it to adapt to different legal regulations, supporting organisations in complying with various standards and regions.

The EPCIS standard and its requirements from the end users seem to be pushed from regulatory changes. New EU legislation like the Green Deal, the product passport and fishing regulations demand more visibility and traceability from the respective industries. EPCIS and other supply chain efficiency and visibility improvements enable this.

Based on the interviews and desk research, the following Table 3.9 outlines the key stakeholders involved in the EPCIS standardisation process, organised by the search direction they originated from:

Table 3.9: Stakeholders per search direction for EPCIS

Search Direction	Stakeholder	Description
End users and related organisations	Retailers (e.g., FMCG, fashion)	Use EPCIS to track product movement and manage supply chains efficiently. [4][8]
	Manufacturers (e.g., Pharma, technical industries)	Implement EPCIS for product traceability, compliance, and quality management. [4][8]
	Other end users (e.g., Logistics companies, EU rail sector)	Utilise EPCIS to improve inventory management, tracking, and supply chain visibility. [4][8]
Regulators	Government regulators	Create policies and regulations for RFID frequency use and data privacy. [8]

Continued on next page

Table 3.9 – continued from previous page

Search Direction	Stakeholder	Description
Designers	Solution providers	Develop and implement EPCIS-compatible systems, offering solutions for traceability and data exchange. [4]
Research and consultancy	Academic institutions (e.g., Universities, research institutes)	Conduct research on EPCIS applications, contributing to the development and improvement of standards. [4][8]
Representative organisations	GS1	Maintains and promotes EPCIS standards, ensuring alignment with industry requirements and regulatory compliance. [4][8]
Physical system	Hardware providers (e.g., RFID, barcode manufacturers)	Supply hardware that captures EPCIS data (e.g., RFID tags, barcode scanners) to support tracking and data exchange. [4][8]
Inspection agencies	Certification bodies (e.g., ISO)	Provide standards and certifications for EPCIS implementations, ensuring compliance with global supply chain regulations. [8]

As shown in Table 3.9, nine different stakeholders were identified across seven search directions. With these stakeholders mapped out, their roles are further assessed by evaluating their power, legitimacy, and urgency in relation to the EPCIS standard. Experts 4 and 8 were consulted in the assessment of the stakeholders' salience. GS1, as the organisation maintaining and advancing the EPCIS standard, was classified as a definitive stakeholder. Retailers, spanning industries such as FMCG and fashion, and manufacturers in sectors like pharmaceuticals were similarly classified as definitive stakeholders because of their critical role in using EPCIS for operational efficiency and compliance. Also, the interviews stated that they have urgency with regards to EPCIS because of the need to meet regulatory demands like the European Green Deal and Digital Product Passport.

Other end users like logistics companies were identified as definitive stakeholders as well, contributing to and relying on EPCIS for data exchange across their supply chains. Hardware providers, such as RFID and barcode manufacturers, were categorised as dominant stakeholders. They hold power in providing essential infrastructure and are legitimate contributors to the EPCIS ecosystem, though their urgency is lower compared to direct adopters of the standard. Certification bodies like ISO and IEEE and government regulators are classified as dominant stakeholders because of their roles in ensuring compliance and setting overarching frameworks. Solution providers and academic institutions, such as universities and research institutes, were classified in the interviews as discretionary stakeholders: they provide legitimacy through innovation and research contributions but they lack influence or urgency in the immediate deployment of EPCIS. The following Table 3.10 categorises each stakeholder based on their power, urgency and legitimacy, offering a clear picture of the stakeholders' characteristics and infrastructure:

Table 3.10: Stakeholder salience for EPCIS

Stakeholder	Power	Legitimacy	Urgency	Type
GS1	X	X	X	A (Definitive) [4][8]
Retailers (e.g., FMCG, fashion)	X	X	X	A (Definitive) [4][8]
Manufacturers (e.g., Pharma, Technical industries)	X	X	X	A (Definitive) [4][8]

Continued on next page

Table 3.10 – continued from previous page

Stakeholder	Power	Legitimacy	Urgency	Type
Other end users (e.g., Logistics companies, distributors)	X	X	X	A (Definitive) [4][8]
Hardware providers (e.g., RFID, barcode manufacturers)	X	X		B (Dominant) [4][9]
Certification bodies (e.g., ISO, IEEE)	X	X		B (Dominant) [8]
Government regulators	X	X		B (Dominant) [8]
Solution providers		X		F (Discretionary) [4][9]
Academic institutions (e.g., Universities, Research institutes)		X		F (Discretionary) [4]

Retailers and manufacturers, key end-users of EPCIS, hold significant power and urgency as they depend on EPCIS for tracking product movement, ensuring supply chain visibility, and maintaining compliance with industry standards. Their active involvement is crucial for driving the adoption of EPCIS across sectors. GS1, as the primary body behind the maintenance and promotion of EPCIS standards plays a pivotal role in aligning industry requirements and regulatory compliance. The democratic process involved in the EPCIS standard ensures everyone relying on and involved in the standard has their fair share of voting power when it comes to new protocols, regulations or other changes (GS1, n.d.).

3.3.2. Universal Plug and Play (UPnP)

Universal Plug and Play, or UPnP, is set of networking protocols that enables devices to discover each other's presence in the network (Open Connectivity Foundation, 2016). It was introduced in 1999 by Microsoft and aimed to increase the ease of configuration devices on the network, primarily in homes or small businesses. At first it was widely adopted in consumer electronics, supported by major companies like Sony & Intel and became a standard for routers and servers. Since 2016 the standard has been managed by the Open Connectivity Foundation. The UPnP device architecture was adopted as a de jure standard by ISO and IEC under ISO/IEC 29341. Despite being the first recognised standard for IP-based networking, UPnP faced significant challenges in market adoption due to security vulnerabilities. These security risks undermined consumer trust and limited its widespread adoption, even though it was standardised by ISO/IEC.

UPnP does not use any form of authentication, requiring devices using the protocol to use additional security measures – making the devices not using it vulnerable for cyber-attacks. Researcher Daniel Garcia exploited another security flaw in 2011. Subsequently, in 2013 and 2020, more security flaws of the protocol came to light, pushing the UPnP forum and the Open Connectivity Foundation to deploy updates. The problem however was that the devices using the protocol where not easily updateable. Although UPnP ease of use has great promises for usage in IoT, the security problems contributed to the fact that from a IIoT standpoint the technology never delivered.

Based on the interviews and desk research, the following Table 3.11 outlines the key stakeholders involved in the UPnP standardisation process, organised by the search direction they originated from:

Table 3.11: Stakeholders per search direction for UPnP

Search Direction	Stakeholder	Description
Production chain	Device manufacturers (e.g., Consumer electronics, IIoT devices) (Messer, 2014)	Develop UPnP-compatible devices, including smart TVs, routers, printers, and home automation systems, ensuring seamless network integration.
	Network equipment manufacturers (e.g., Cisco, Netgear) (Messer, 2014)	Produce routers, switches, and network equipment that support UPnP protocols to facilitate device discovery and connectivity.
End users and related organisations	End users (e.g., Home users, SMBs) (UPnP Implementers Corporation, 2006)	Utilise UPnP-enabled devices for ease of network configuration, media sharing, home automation, and remote access.
Designers	Software developers (e.g., Application developers, Firmware engineers) (Messer, 2014) (Miller & van de Beek, 2014)	Develop UPnP-compatible software, applications, and firmware for device discovery, control, and communication.
Research and consultancy	Academic institutions (e.g., Universities, Research labs) (Arunachalam, 2016)	Conduct research on UPnP security, interoperability, and network efficiency to inform standard improvements.
Inspection agencies	Certification bodies (e.g., UPnP Forum, IEEE) (Mitsugi et al., 2014) (Belimpasakis & Stirbu, 2007)	Certify devices and software to ensure compliance with UPnP standards.
Representative organisations	UPnP Forum (Messer, 2014)	Develops and maintains UPnP standards, ensuring compatibility across different devices and applications, while facilitating collaboration among stakeholders.
	Open Connectivity Foundation (OCF) (Open Connectivity Foundation, 2016)	Maintains UPnP standards and promotes interoperability for Internet of Things.

As shown in Table 3.11, eight different stakeholders were identified across six search directions. With these stakeholders mapped out, their roles are further assessed by evaluating their power, legitimacy, and urgency in relation to the UPnP standard. Sources such as the Open Connectivity Foundation (n.d.), Messer (2014), and academic studies like Miller & van de Beek (2014), showed that The Open Connectivity Foundation (OCF) is a definitive stakeholder. It is the governing body for UPnP standards, defining and maintaining the UPnP protocol. It has legitimacy through being a global consortium, and urgency because of the need to address interoperability and security challenges. Device manufacturers, including those producing consumer electronics and IIoT devices, were identified as dominant stakeholders because of their power in the market and their legitimacy as key adopters of the standard. However, their urgency was less clear when compared to the OCF's role in standardisation. Network equipment manufacturers and software developers were also classified as dominant stakeholders because of their role to deploy the UPnP standard. The UPnP Forum was classified as a dangerous stakeholder due to its role in establishing the open nature of the standard, which has led to significant security vulnerabilities. The open connection architecture of UPnP allows for potential exploitation resulting in unauthorised access and data breaches. Certification bodies, such as IEEE and ISO, along with end users like home users and SMBs, were classified as discretionary stakeholders. They provide legitimacy by ensuring compliance and offering real-world feedback. The following Table 3.12 categorises each stakeholder based on their power, urgency and legitimacy, offering a clear picture of the stakeholders' characteristics and infrastructure:

Table 3.12: Stakeholder salience for UPnP

Stakeholder	Power	Legitimacy	Urgency	Type
Open Connectivity Foundation (OCF)	X	X	X	A (Definitive) (Open Connectivity Foundation, 2016)
Device manufacturers (e.g., Consumer electronics, IIoT Devices)	X	X		B (Dominant) (Messer, 2014)
Network equipment manufacturers (e.g., Cisco, Netgear)	X	X		B (Dominant) (Messer, 2014) (Miller & van de Beek, 2014)
Software developers (e.g., Application developers, Firmware engineers)	X	X		B (Dominant) (Miller & van de Beek, 2014) (Messer, 2014) (Open Connectivity Foundation, 2016)
UPnP Forum	X		X	C (Dangerous) (Buckbee, 2022) (Nakutavičiūtė, 2023) (Kost, 2024)
Certification bodies (e.g., IEEE, ISO)		X		F (Discretionary) (Mitsugi et al., 2014) (Belimpasakis & Stirbu, 2007)(ISO, 2008)
End users (e.g., home users, SMBs)		X		F (Discretionary) (UPnP Implementers Corporation, 2006)
Academic institutions (e.g., Universities, Research labs)		X		F (Discretionary) (Open Connectivity Foundation, n.d.)

UPnP standardisation presents an interesting distribution of power, legitimacy, and urgency among its stakeholders. None of the production chain stakeholders, such as device manufacturers or network equipment manufacturers, are classified as definitive stakeholders. While they hold significant power and legitimacy in producing UPnP-compatible devices, they do not exhibit enough urgency to drive immediate change or adoption in the standards because of the multitude of available alternatives.

The UPnP Forum, a key player in developing and maintaining UPnP standards, stands out as a dangerous stakeholder. While it has power and urgency with regards to the standardisation process, its involvement can introduce risks if its direction or priorities diverge from the broader interests of the ecosystem. Other stakeholders, such as software developers and the Open Connectivity Foundation (OCF), play a dominant role but lack the urgency to speed up the standard evolution. There is a notable lack of urgency across most stakeholders, particularly within the production chain. This slower pace of change hinders the development and adoption of UPnP standards. End-users and certification bodies depend on the standards but do not possess the power to enforce changes, such as security improvements, highlighting a dynamic where collaboration and negotiation are critical for progress.

3.4. Data utilisation standards

Data utilisation is the fourth and final phase in IIoT systems. After data has been processed and meaningful insights have been extracted, this phase focuses on presenting the data to end-users in an actionable and comprehensible manner. This involves creating dashboards, generating alerts, and providing tools for monitoring and controlling devices. Visualisation transforms complex data sets into graphical representations, enabling users to identify patterns, trends, and anomalies quickly.

Current trends in data utilisation include the integration of advanced analytics, machine learning, and artificial intelligence to enable predictive maintenance, anomaly detection, and automated decision-making. With regards to standardisation, data utilisation corresponds to the OSI model's Application Layer (Layer 7), which provides services directly to end-user applications. The two standards that have been selected for this phase are Ignition and GE Predix.

Ignition, developed by Inductive Automation, is an industrial application platform for building SCADA (Supervisory Control and Data Acquisition) systems, HMI (Human-Machine Interface), and IIoT (Industrial Internet of Things) applications (Inductive Automation, n.d.). Ignition provides a platform for data visualisation, control, and analytics. It allows users to create custom dashboards, set up alarms and notifications, and generate reports. Ignition supports integration with various industrial devices, standards and databases, offering flexibility for organisations of all sizes.

GE Predix is a platform-as-a-service (PaaS) developed by GE Digital since 2015, specifically for the industrial internet. Predix provides tools and services for data analytics, visualisation, and application development tailored to industrial environments. It enables the creation of applications that can monitor equipment performance, predict maintenance needs, and optimise operations. Predix uses its own cloud environment to handle large volumes of industrial data

Both Ignition and GE Predix aim to enhance data visualisation and utilisation in industrial IIoT systems but differ in their deployment and focus areas. Ignition offers a flexible platform with strong real-time control capabilities, suitable for organisations prioritising in-house infrastructure. GE Predix provides a cloud-based solution with analytics and scalability, built for large-scale industrial operations.

3.4.1. Ignition

Ignition by Inductive Automation is a software platform that unifies Supervisory Control and Data Acquisition (SCADA), IIoT and Manufacturing Execution System (MES) functionalities into a single system (Inductive Automation, n.d.). Ignition has been widely adopted across industries such as manufacturing, energy and transportation due to its scalability and flexibility. The platform makes businesses able to quickly design industrial applications reducing costs associated with traditional automation software. A key strength of Ignition is its adherence to standards and support of protocols standard in the industry like OPC UA and MQTT. These connectors facilitate integration with existing systems and devices. This interoperability promotes real-time data sharing and monitoring important for IIoT devices, and it enables predictive maintenance. However, challenges in the platform's broader adoption stem from the lack of universal standardisation in the industrial automation sector. Nonetheless, Ignition can be seen as a de facto standard for SCADA/MES systems in IIoT.

Based on the interviews and desk research, the following Table 3.13 outlines the key stakeholders involved in the development of Ignition, organised by the search direction they originated from:

Table 3.13: Stakeholders per search direction for Ignition

Search Direction	Stakeholder	Description
Designers	Inductive Automation [14] (Inductive Automation, n.d.) System integrators [14] (Inductive Automation, n.d.) (ATS-Global, n.d.)	Develops and maintains the Ignition software platform. Design, implement, and customise Ignition solutions tailored to clients' specific industrial needs.
Production chain	Industrial hardware manufacturers [14]	Produce hardware devices (PLCs, sensors, HMIs) compatible with Ignition for data acquisition and control.
End users and related organisations	Industrial companies (e.g., manufacturers, energy firms) [14]	Utilise Ignition for real-time monitoring, control, and analytics to optimise operations.
Physical system	OPC Foundation (Inductive Automation, n.d.) MQTT standard organisations (e.g., OASIS) [14] (OASIS, 2016)	Maintains OPC UA standards which Ignition supports for device interoperability and data exchange. Maintain MQTT protocol standards used by Ignition for efficient IIoT messaging.
Regulators	Government regulators (Panacea Technologies Inc., 2019)	Establish policies and regulations on industrial automation, cybersecurity, and data protection affecting Ignition's deployment.
Inspection agencies	Certification bodies (e.g. NIST) (Inductive Automation, n.d.) Cybersecurity firms (e.g. SafeBase) (Boeger, 2023) (Inductive Automation, n.d.)	Provide standards and certifications and ensures Ignition's compliance. Provide security solutions and audits for Ignition-based systems to ensure secure operations.
Research and consultancy	IT Consulting firms (e.g. ATS Global) [14] Universities and research institutes (Inductive Automation, n.d.)	Offer consulting services for Ignition adoption and integration, optimising its use in businesses. Conduct research on industrial automation technologies and innovations involving Ignition.
Education	Educational institutions (Inductive Automation, n.d.)	Include Ignition and related technologies in engineering and technical curricula to train future professionals.
Representative organisations	Industry associations (e.g., International Society of Automation) (Tarapure, 2024)	Advocate for automation best practices, and influence standardisation. Ignition helps with businesses on adhering to ISA95.

As shown in Table 3.13, thirteen different stakeholders were identified across all nine search directions. With these stakeholders mapped out, their roles are further assessed by evaluating their power, legitimacy, and urgency in relation to the Ignition standard. From the interview with Expert 15 and sources such as Inductive Automation and Boeger (2023) can be derived that Inductive Automation, as the primary developer and promoter of Ignition software is a definitive stakeholder. Industrial companies like manufacturers and energy firms are also classified as definitive stakeholders because they invest and rely heavily on Ignition for operational efficiencies. Government regulators were similarly identified as definitive stakeholders because their oversight of compliance and safety standards grants. System integrators, industrial hardware manufacturers and cybersecurity firms were recognised as dominant stakeholders due to their critical roles in integrating Ignition systems, providing necessary infrastructure, and ensuring security against potential threats. Physical system and representative organisations stakeholders like the OPC Foundation, MQTT Standard Organisations, and the International Society of Automation were also classified as dominant stakeholders. Their power and legitimacy comes from their standardisation efforts, though their urgency remains less immediate: Ignition is not the only standard they are invested in. Certification bodies and IT consulting firms were identified as dependent stakeholders. While contributing to the ecosystem's legitimacy, they lack independent power and rely on collaboration with more salient stakeholders. Educational institutions and research labs were categorised as discretionary stakeholders, providing innovation support but without direct urgency or significant influence in the immediate deployment of Ignition systems. The following Table 3.14 categorises each stakeholder based on their power, urgency and legitimacy, offering a clear picture of the stakeholders' characteristics and infrastructure:

Table 3.14: Stakeholder salience for Ignition

Stakeholder	Power	Legitimacy	Urgency	Type
Inductive Automation	X	X	X	A (Definitive) [14] (Inductive Automation, n.d.)
Industrial companies (e.g., manufacturers, energy firms)	X	X	X	A (Definitive) [14]
Government regulators	X	X	X	A (Definitive) [14][8]
System integrators	X	X		B (Dominant) [14] (ATS-Global, n.d.)
Industrial hardware manufacturers	X	X		B (Dominant) [14] (OnLogic, n.d.)
OPC Foundation	X	X		B (Dominant) (Inductive Automation, n.d.)
MQTT Standard Organisations (e.g., OASIS)	X	X		B (Dominant) [14] (OASIS, 2016)
Industry associations (e.g., International Society of Automation)	X	X		B (Dominant) (Inductive Automation, n.d.) (ISA, n.d.)
Cybersecurity firms	X	X		B (Dominant) (Boeger, 2023) (Inductive Automation, n.d.)
Certification bodies (e.g. NIST)		X	X	D (Dependent) (Inductive Automation, n.d.)
IT Consulting firms		X	X	D (Dependent) [14]
Educational institutions		X		F (Discretionary) (Inductive Automation, n.d.)
Universities and research institutes		X		F (Discretionary) (Inductive Automation, n.d.) (Inductive Automation, n.d.)

The wide range of stakeholders can be explained by both the success of the standard as well as the size of and possibilities within the platform. Government regulators emerge as Definitive stakeholders due to their enforcement of regulations (for example, legislation like the Green Deal) and has legitimate authority over compliance, cybersecurity, and data protection. The urgency is associated with enforcing regulations that directly impact Ignition's deployment. Certification bodies such as ISO and IEC are considered Dependent stakeholders. While they have legitimacy and their certifications are urgently needed for industry compliance, they lack direct power to influence the platform independently. The underlying dynamics between the stakeholders help the adoption of the Ignition platform. While Inductive Automation drives the core development, the collaboration and support from Dominant stakeholders like system integrators, hardware manufacturers, and standard organisations enhance the platform's interoperability. The urgency for industrial companies to have integrated software, data and visualisations drives the standard forward.

However, there are some challenges for standardisation in the industrial automation sector. The dependence on continuous updates and support from a single vendor raises concerns about long-term sustainability. The involvement of government regulators as powerful stakeholders underscores the importance of compliance with evolving regulations on cybersecurity and data protection.

3.4.2. GE Predix

GE Predix is an industrial Internet of Things (IIoT) platform designed to connect industrial machines and equipment. It captures and analyses operational data to drive better decision-making in industries like manufacturing, energy, aviation, and healthcare. Predix was initially positioned as a leading solution for digital transformation for real-time monitoring, and predictive maintenance in complex industrial systems.

However, while Predix saw early adoption in GE's core sectors, it faced challenges with integration and scalability, limiting market success. The platform was complex to implement, particularly for non-GE systems, and struggled to compete with more flexible and widely adopted platforms like Microsoft Azure and Ignition. In the meantime, GE burnt through 7 billion USD in developing the platform and still failed to become widely adopted (Pereira, 2022), with an estimated market share of 0% (6sense, 2024). Aside from stakeholder infrastructure, its failure to become a de facto standard is reported to be due to an overly ambitious scope, reliance on external consultants and the failure to start small and iterate. Predix's challenges led to GE scaling back its investment in the platform, focusing more on partnerships and custom solutions for industrial clients. Based on the interviews and desk research, the following Table 3.15 outlines the key stakeholders involved in the Predix standardisation process, organised by the search direction they originated from:

Table 3.15: Stakeholders per search direction for Predix

Search Direction	Stakeholder	Description
Designers	General Electric (GE) (GE Vernova, 2024)	Develops and maintains the Predix platform.
Production chain	Industrial hardware manufacturers (Weber, 2017)	Produce hardware (sensors, PLCs, industrial equipment) that generate data processed by Predix.
End users and related organisations	Manufacturing, energy, aviation, healthcare companies (Pereira, 2022)	Use(d) Predix for asset performance management, predictive maintenance, and operational optimisation.
Physical system	Independent software vendors (ISVs) (Simha et al., n.d.)	Developed applications and solutions on top of the Predix platform.
Regulators	Government regulators (GE, n.d.)	Set policies on data security, privacy, and industrial IIoT affecting the use of Predix in various sectors.

Continued on next page

Table 3.15 – continued from previous page

Search Direction	Stakeholder	Description
Inspection agencies	Certification bodies (e.g., ISO, IEC) (GE, n.d.)	Ensure compliance with international standards for data security, quality, and operational safety in Predix deployments.
Research and consultancy	IT consulting firms (e.g., Accenture, Deloitte) (GE Vernova, 2024)	Offer consulting services for the integration and optimisation of Predix in industrial environments.
	Universities and research institutes (GE Aerospace, 2018)	Conduct research on industrial IIoT innovations, often focusing on platforms like Predix.

As shown in Table 3.15, eight different stakeholders were identified across seven search directions. With these stakeholders mapped out, their roles are further assessed by evaluating their power, legitimacy, and urgency in relation to the Predix standard. Sources like Pereira (2022) and Weber (2017) identify the roles and saliences of various stakeholders. General Electric, as the creator and primary driver of the Predix platform is a definitive stakeholder. IT consulting firms, including Accenture and Deloitte, were classified as dominant stakeholders because of their General Electric's reliance on them in integrating and scaling Predix solutions for industrial clients, alongside legitimacy as trusted advisors to enterprise customers. Similarly, industrial hardware manufacturers were identified as dominant stakeholders due to their role in providing compatible hardware for the Predix platform. Certification bodies such as ISO and IEC, along with government regulators, were also categorised as dominant stakeholders, holding power and legitimacy through their oversight of compliance and safety standards but lacking the immediate urgency tied to standard. End users, including companies from manufacturing, energy, aviation, and healthcare sectors, were also considered dominant stakeholders, given Predix' focus on providing solutions for all industries they were alreadu active in. The end users had a role in driving the platform's requirements and adoption. Independent software vendors were classified as dependent stakeholders as they rely on Predix for ecosystem opportunities but lack independent power or urgency. The following Table 3.16 categorises each stakeholder based on their power, urgency and legitimacy, offering a clear picture of the stakeholders' characteristics and infrastructure:

Table 3.16: Stakeholder salience for Predix

Stakeholder	Power	Legitimacy	Urgency	Type
General Electric	X	X	X	A (Definitive) (GE, n.d.)
IT Consulting firms (e.g., Accenture, Deloitte)	X	X		B (Dominant) (PwC, n.d.) (Pereira, 2022)
Industrial hardware manufacturers	X	X		B (Dominant) (Weber, 2017)
Certification bodies (e.g., ISO, IEC)	X	X		B (Dominant) (GE, n.d.)
Government regulators	X	X		B (Dominant) (GE, n.d.)
End users (e.g., Manufacturing, Energy, Aviation, Healthcare Companies)	X	X		B (Dominant) (GE, n.d.)
Independent Software Vendors (ISVs)		X	X	D (Dependent) (Simha et al., n.d.) (Higgins, 2016) (CIO, 2016)
Universities and research institutes		X		F (Discretionary) (GE Vernova, 2024) (GE Aerospace, 2018)

The stakeholders involved in GE Predix highlight some of the critical challenges the platform faced. GE relied heavily on external consultants like Accenture and Deloitte for the implementation and customisation of Predix solutions, which added complexity and cost. Their lack of urgency in pushing rapid advancements limited the platform's scalability and flexibility. Also, it is rare that consultancy agencies act as a dominant stakeholder. Furthermore, GE's ambitious decision to build its own cloud infrastructure rather than leveraging established providers like AWS or Microsoft added an operational & financial load. Typically, industrial platforms would rely on existing cloud services to handle infrastructure challenges, but GE chose to go the more complex route (Kumar, 2019).

Additionally, GE's approach of creating a ”one size fits all” platform for its many verticals (aviation, oil & gas, healthcare, and more) resulted in overextension. The platform was stretched across too many industries, leading to inefficiencies and lack of focus. This broad scope, combined with insufficient involvement from end users during development, made it difficult for Predix to deliver tailored solutions for specific industrial needs. Instead of deeply engaging with key end users, the platform was designed to cater to too many sectors at once, ultimately failing to meet the unique demands of any single industry effectively.

3.5. Results

Now after the process of interviewing, data collection and stakeholder classification, it is time to combine the results. Together, the tables from the past chapters make up a matrix showing all search directions, stakeholders, standards and stakeholder classifications together. The goal here is to derive patterns from this matrix. As part of the results the answers to SQ2 are sought: In practice, how does the classification of stakeholders—organised into a matrix based on their levels of power, legitimacy, and urgency—influence the emergence of technological standards in IoT?

To provide a clear overview of the interrelations between stakeholders and technological standards in the IIoT landscape, the compiled matrix the data in a unified format. This comprehensive table aligns stakeholders with the specific standards they influence, indicating their levels of power, legitimacy, and urgency. By organising the information this way, patterns and trends become more apparent, allowing for a deeper understanding of how different stakeholder attributes contribute to the emergence and adoption of IIoT standards. This structured visualisation is essential for analysing the practical effects of stakeholder classifications, as it highlights the dynamics that answer SQ2. More specifically, it shows how the combined influence of power, legitimacy, and urgency among stakeholders impacts the development of technological standards within IIoT. The results can be found on the next page in 3.17.

For readability's sake, the letters in Table 3.17 correspond with stakeholder classification as found in Figure 3 as follows:
A: Definitive stakeholder, possesses power, urgency, and legitimacy.
B: Dominant stakeholder, possesses power and legitimacy but lacks urgency.
C: Dangerous stakeholder, possesses power and urgency but lacks legitimacy.
D: Dependent stakeholder, possesses urgency and legitimacy but lacks power.
E: Dormant stakeholder, possesses power only.
F: Discretionary stakeholder, possesses legitimacy only.
G: Demanding stakeholder, possesses urgency only.

Table 3.17: Stakeholder / standard matrix, showing the results of all stakeholder tables combined

	Standards							
	Market adoption				**No market adoption**			
Stakeholders	RFID UHF	LoRaWAN	EPCIS	Ignition	Zephyr Project	Sigfox 0G	UPnP	GE Predix
Production chain								
RFID manufacturers	A							
Logistics companies	A							
RFID solution providers	D							
Embedded device manufacturers					B			
Chip vendors					B	B		
Semtech		A						
Sigfox operators						A		
Device manufacturers		B				A	B	
Network equipment manufacturers							B	
Industrial hardware manufacturers				B				B
End-users and related organisations								
Decathlon	A							
Other retailers	A		A					
End-users					A	F	F	B
Zephyr project members					A			
Telecom companies		A						
The Things Industries		A						
Municipalities		D						
Manufacturers			A					
Logistic companies, distributors			A					
Industrial companies				A				
Designers								
Open-source developers					C			
Solution providers		B	F			A		
Software developers							B	
Inductive automation				A				
System integrators				B				
General Electric								A
Physical system								
Independent software vendors								D
Hardware providers			B					
OPC foundation				B				
MQTT standard organisations				B				
Inspection and regulatory								
Certification bodies	B		B	D			F	B
Cybersecurity firms				B				
Government regulators	B	F	B	A				B
Standard setting bodies	B	F						
Research and education								
IT consulting firms	F			D				B
Universities and research institutes			F	F	F	F	F	F
Educational institutions	F			F				
Academic institutions		F						
Representative organisations								
Consumer organisations	D							
Industry associations	F			B				
Linux foundation					B			
The Things network		A						
LoRa alliance		A						
Sigfox S.A.						C		
GS1			A					
UPnP forum							C	
Open connectivity foundation							A	

Now, from this table we can dive into the statistics. Table 3.18 show the standards with market adoption. Table 3.19 shows the standards without it. Afterwards we can make comparisons between the two. Since there are no dormant or demanding stakeholders in both tables, they have been removed from the overview.

Table 3.18: Statistics for standards with market adoption

Statistic	RFID UHF	LoRaWAN	EPCIS	Ignition	Average
Number of stakeholders	12	11	9	13	11.25
Number of Definitive stakeholders	4	5	4	3	4
Number of Dominant stakeholders	3	2	3	6	3.5
Number of Dangerous stakeholders	0	0	0	0	0
Number of Dependent stakeholders	2	1	0	2	1.25
Number of Discretionary stakeholders	3	3	2	2	2.5

Table 3.19: Statistics for standards without market adoption

Statistic	Zephyr P.	Sigfox	UPnP	Predix	Average
Number of stakeholders	7	7	8	8	7.5
Number of Definitive stakeholders	2	3	1	1	1.75
Number of Dominant stakeholders	3	1	3	5	3
Number of Dangerous stakeholders	1	1	1	0	0.5
Number of Dependent stakeholders	0	0	0	1	0.25
Number of Discretionary stakeholders	1	2	3	1	1.75

The patterns that can be found in Table 3.17, 3.18 and 3.19 are as follows, sorted by relevance and prominence:
1) End-user engagement is essential: End users and related organisations are more prevalent in standards with market adoption. Their involvement as dominant or definitive stakeholders contributes significantly to the adoption and implementation of the standard.
2) Dangerous stakeholders hinder adoption: In 3 out of 4 standards without market adoption, there is at least one dangerous stakeholder. Their presence correlates with the lack of adoption, indicating that stakeholders who have power and urgency but lack legitimacy can create obstacles in the standardisation process.
3) Definitive stakeholders drive market adoption: Standards with market adoption have a higher average number of definitive stakeholders (4) compared to those without market adoption (1.75). This suggests that the involvement of stakeholders possessing power, urgency, and legitimacy is crucial for a standard's success in the market.
4) Higher stakeholder participation in adopted standards: Standards that have been adopted in the market involve more stakeholders on average (11.25) compared to those without market adoption (7.5). Broad stakeholder participation enhances the standard's credibility and acceptance.
5) Absence of stakeholders with only power or urgency: Stakeholders possessing only power (type E) or only urgency (type G) do not appear in the table. This absence indicates that power or urgency alone is insufficient to impact standard adoption.

3.6. Conclusion

This chapter investigated the stakeholders across eight Industrial Internet of Things (IIoT) standardisation cases. By employing the power-legitimacy-urgency framework, stakeholders were systematically identified, classified and analysed. The results are patterns in stakeholder salience and composition between standards with and without market adoption.

Standards that achieved market adoption tended to have higher stakeholder engagement, with a more presence of definitive stakeholders who possess all three salience attributes. In contrast, non-adopted standards often featured dangerous stakeholders: those with power and urgency but lacking legitimacy. They seem to hinder the standardisation process. Additionally, the results underscored the critical role of end-users, whose involvement positively correlates with market adoption.

These findings directly address sub-question 1 by demonstrating the impact of stakeholder classifications on the emergence and adoption of technological standards. The analysis also highlights the importance of comprehensive stakeholder inclusion and effective management of potentially disruptive actors.

4

Ways to influence the standardisation process

The results of the previous chapter clearly indicate what favourable conditions are for stakeholder ecosystems in IIoT. The next question that logically arises is how to reach these favourable conditions. This chapter aims to answer SQ2: How policymakers, researchers, SDOs or businesses, influence the standardisation process in Industrial IoT? The four relevant patterns from chapter 3 are translated into policy recommendations. Section 4.1 dives into how to stimulate end-user engagement, 4.2 analyses the possibilities on reducing (the effects) of dangerous stakeholders and 4.3 explains how to increase the number of stakeholders. Pattern 5: absence of certain stakeholder types is excluded because of its limited relevance with regards to policy implications.

4.1. Stimulating end-user engagement

The first conclusion of the results was that end-user engagement is essential - they are more prevalent in standards with market adoption. To determine effective policy recommendation the question is posed; how can end-user engagement be stimulated?

Jakobs (2006) endorses the importance of user-engagement in standardisation processes. Specifically, the contribution of user requirements poses a major task during it: "They have to feed their intimate knowledge of local particularities, which nobody else can possibly possess, into this process." However, the same paper outlines the problem that SDOs main focus is developing generic standards, useful for as many entities as possible. A take-away from this is that a focus on more specific and operationally viable standards development should increase the likelihood of end-users engaging. Expert 4 says that in order to drive engagement, the standard should aim to improve business activity: "The most motivating thing for decision takers is to increase sales or cut costs, which inherently supports collaboration in standardisation activities. Such drivers are essential as they align with top management's priorities, making the company more profitable."

A study by Backhouse et al., 2006 shows that active participation by end-users brings legitimacy and practical relevance to the standard, which endorsement alone may not achieve. The study shows a similar example to this thesis results: UK businesses' early adoption of standard BS7799 and their involvement in its development allowed the standard to gain momentum and legitimacy. In addition, Gasson et al., 1995 argues that IT professionals use their power to exclude end-users from the standardisation process. If (and if, because not always the case) end-user requirements are used as input for the standardisation process, requirements are re-defined at a later stage according to Gasson et al. The theory tells us that there's a certain prejudice against end-users and their involvement. In stages after the system requirement setting, it is not uncommon for requirements to be changed or interpreted differently by technical developers creating bias in the standard development process. Expert 16 confirmed that these claims are most likely still true. A recent report on SMEs and civil society inclusiveness in European standardisation (High-Level Forum on European Standardisation, 2024) also points out that 35 percent of small-medium businesses and civil societies lack awareness of National Standards Bodies and their work.

To increase end-user engagement, the High-Level Forum on European Standardisation prescribes various best practices:
1) Create well-established stakeholder groups, involving underrepresented stakeholders like end-users in the standardisation process
2) Do not require fees for information on or participation in standardisation processes
3) Offer free in-person consultation on standardisation efforts

4.2. Avoiding dangerous stakeholders

The second pattern that arises in the results is that dangerous stakeholders hinder adoption. In three out of four standards without market adoption, there is a stakeholder present possessing power and urgency, but no legitimacy. As stated before, legitimacy is a dynamic variable, meaning that before legitimate stakeholders could turn into illegitimate stakeholders later. For example, in 2017, when Kobe Steel falsified steel strength data on already sold goods. The Central Japan Railway Company discovered that the supplied steel did not meet safety standards: the aluminium produced for use on a bullet train was ten percent weaker than the strength set under Japan Industrial Standards (BBC, 2018) (Mainichi, 2017).

De Vries et al. (2003) in a paper on ergonomics standards speaks about addressing dangerous stakeholders in standard setting. For dangerous stakeholders some means need to be found that they can participate with approval from the other stakeholders, achieving legitimacy and converting them into a definitive stakeholder. The paper examples this by a powerful organisation that could possibly trigger negative publicity if not involved in the standardisation process.

Specific literature on how to manage dangerous stakeholders in standardisation settings is unavailable but work by Werle & Iversen (2006) reflect on the legitimacy problems in standardisation as a whole, particularly on standardisation output. They state that SDOs are aware of a bias caused by under- and overrepresentation of certain stakeholders, doubting the legitimacy of standards. To mitigate this issue, they present two options:
1) Emphasise the requirement side of the standardisation process, through direct participation of all involved stakeholders. The paper states that although this should increase legitimacy, but most likely overloads the standardisation process.
2) Appoint special committees from outside the SDOs and let them review the work of the standards committees. An assessment is made if the outcome is legitimate.
Although both mitigation options are likely to have a positive influence on the legitimacy of the standardisation process as a whole, it is difficult to see how this would avoid the inclusion of dangerous stakeholders. It can be concluded that avoiding dangerous stakeholders is a difficult task to navigate and remains underexposed in the theory.

4.3. Increase the number of (definitive) stakeholders

The third and fourth pattern from the results is that higher stakeholder participation, especially from definitive stakeholders, drives market adoption. This leads to the question of how to involve these (definitive) stakeholders. There are two ways about this:

1) Involve more stakeholders in the standardisation process
De Vries et al. (2003) in the aforementioned paper on ergonomics standards highlights that an effective way of increasing the number of committed stakeholders is by “shifting the attention from increasing the quantity of standards towards increasing the quality”. Rather than deploying more and more standardisation cases, focus the efforts and ask stakeholder to commit to less but higher quality standardisation processes. This should lead to more useful, desired and used standards. Jakobs, 2008 agrees to this. He mentions that companies are forced to participate in many standardisation processes because of the lack of coordination between consortias and SDOs. A higher level of cooperation would lead to fewer, higher quality standardisation processes, with more actively engaged stakeholders.

2) Increase the salience of the current stakeholders
Besides attracting new stakeholders, another option to increase the number of definitive stakeholders would be to increase the salience levels of stakeholders already involved in the standardisation process. In all the standards without market adoption there are plenty of stakeholders involved that could be influenced to become more powerful or urgent to the matter. Funding or providing resources to potential definitive stakeholders could translate to them becoming more powerful. Policymakers can create or amend laws and regulations to prioritise standardisation and increase urgency.

4.4. Conclusion

This chapter explored policy recommendations and strategies for influencing the standardisation process in the Industrial Internet of Things (IIoT), focusing on stakeholder dynamics. Building on the findings of stakeholder salience patterns from the previous chapter, it examined how end-user engagement, the management of dangerous stakeholders and increased participation of (definitive) stakeholders can improve the market adoption of standards. The Table 4.1 gives an overview of all the policy recommendations:

Table 4.1: Policy recommendations for stakeholder engagement in standardisation

Challenge	Policy recommendation	Description
Stimulating end-user engagement	Create well-established stakeholder groups.	Ensure inclusivity by involving underrepresented stakeholders.
	Do not require fees for participation in standardisation processes.	Eliminate financial barriers to participation.
	Offer free in-person consultation on standardisation efforts.	Provide accessible support to encourage involvement in standardisation.
	Address bias against end-users in the standardisation process.	Mitigate exclusionary practices by IT professionals and ensure end-user requirements are not redefined or distorted during the system development phase, maintaining their original intent and relevance.
Avoiding dangerous stakeholders	Emphasise the requirement side of the standardisation process through direct stakeholder participation.	Enhance legitimacy by involving all relevant stakeholders in the requirement-setting phase.
	Appoint special committees to review standards outputs.	External reviews ensure the legitimacy of the standardisation outcomes and mitigate over- or under-representation issues.
	Facilitate participation of potentially dangerous stakeholders to convert them into legitimate stakeholders.	Engage with stakeholders who may pose risks to standardisation to integrate their contributions positively.

Continued on next page

Table 4.1 – continued from previous page

Challenge	Policy recommendation	Description
Increasing the number of stakeholders	Involve more stakeholders by focusing on fewer, higher-quality standardisation processes.	Reduce the burden on organisations to participate in too many processes, promoting deeper engagement and higher-quality outputs.
	Increase the salience of current stakeholders.	Provide resources or funding to boost stakeholder power and urgency, while creating regulatory frameworks to enhance their influence on standardisation.

In conclusion, this chapter provides a roadmap for actionable stakeholder management strategies. They aim to positively influence the standardisation process in IIoT.

5
Discussion

5.1. Verification of results

The involvement of end-users in the standardisation process has previously been highlighted as a key factor for successful standardisation. Research by Kai Jakobs underscores this: Jakobs emphasises that standards shaped without significant user input risk becoming irrelevant or incompatible with the actual needs of users. He points out that users in the ICT domain, must contribute their specific requirements early in the process to ensure that standards meet their operational environments. Moreover, Jacobs highlights that coordinated user representation in standards-setting bodies is crucial to avoid the development of standards that benefit only a select few (Jakobs, 2005). However, the same Jakobs argues in 1998 that this isn't always the case. To make sure what the current state of things is, an interview was conducted. Jakobs said there's a case to be made for both situations: "Yes, user-engagement is beneficial to the standardisation outcome, but only if the end-users can come to an unambiguous set of user requirements. If the user requirements are contradictory because of a diverse stakeholder group, this is naturally counterworking."

The discussion also included talks on how to involve the end-users in standardisation processes. Jakobs stated that for this to succeed, he proposes a dedicated requirement elicitation process prior to the current process. Here end-users could sort their requirements out, agree on a set of requirements and then feed that into the technical department, even before any standard development is done. This is not a new proposal: Werle & Iversen (2006) proposes a similar process to mitigate the risk of bias in standardisation: emphasising the requirement side, through direct participation of the stakeholders.

5.2. Theoretical contributions

The methodology employed in this thesis is a logical extension of the stakeholder identification method outlined in Henk de Vries' 2003 paper. Remarkably, aside from its use in research conducted by van de Kaa and some of de Vries' own students, this methodology has not been widely applied in other studies. According to de Vries, the approach has not been previously used as in the manner presented here, particularly regarding the creation of a stakeholder/standard matrix. He comments on how his 2003 methodology is "being misapplied by organisations like NEN" and that "proper application of this stakeholder identification method proved successful in attracting more committee members to standardisation efforts". This success underscores the method's efficacy in stakeholder mapping and thus enhancing stakeholder engagement. However, the inadequate use of the methodology today correlates with a lower growth of committee membership. This suggests that when correctly applied, the methodology can significantly impact the standardisation process by effectively identifying and involving key stakeholders.

Recently a new adoption of the used method was published by de Vries (2024). Over the last 13 years, de Vries worked on the method, and it grew out to an elaborate, complex model showing standardisation management activities and influences. The new model looks intriguing and promising, however, research similar to this thesis couldn't have been carried out with this research method – it seems too complex for the multitude of cases used in the empirical analysis of this thesis.

This thesis helps in standardisation and stakeholder literature by empirically analysing the process of market adoption of eight standardisation cases. The main finding, increasing end-user engagement, supports the argument made in standardisation literature (Jakobs, 2005 & 2006) that influence of end-users in the development of standards, especially in complex technological ecosystems like IIoT is beneficial the standard's relevance. It makes the standard more likely to gain widespread adoption because of alignment with actual market needs.

As for the presence of illegitimate (dangerous) stakeholders being of negative influence on the standardisation process, it is shown in chapter 5.2 that literature reflecting on this specific outcome is scarce. Thus, the main theoretical contribution here would be to have more exploratory or empirical future research on the matter. At last, that a generally higher stakeholder involvement proves to be important factors for market adoption of standards is a highlighted theme in standardisation literature. The outcomes of this thesis emphasise that literature is right and that SDOs and businesses should focus on a higher level of cooperation. This would lead to fewer, higher quality standardisation processes, with more actively engaged stakeholders. The second option shown in chapter 5.3, reflecting on increasing the salience or characteristics of stakeholders already involved is not something previously found in literature. Therefor it is recommended that theoretical and possibly empirical research towards finding out if and how this can be done is conducted.

5.3. Practical contributions

The results of the study show that stakeholder involvement and balancing are essential to market adoption of IIoT standards. The type of stakeholders involved must be of concern to the committees responsible for standardisation. Stakeholders with definitive characteristics; power, legitimacy and urgency are essential for standards to be successful. Committees can become more effective than before, if they optimise for diversity across stakeholder types as much as possible. In particular, end-users should be included. On the other end, "dangerous" stakeholders should be avoided. These are stakeholders that have a lot of power and urgency but don't have legitimacy. Such stakeholders often create barriers, postponing or preventing adoption. Committees should also try to incorporate smaller entities, as well as larger, to counter the monopolistic tendencies of very large multinationals whose private standards may inhibit open interoperability. This balanced approach is consistent with the public interest mandate of standardisation. It leads to the development of standards that serve a wider range of industry and public needs.

With regards to the IIoT industry, the empirical findings show how to navigate your standard to widespread adoption. Try and involve plenty of different stakeholders, especially end-users, and make them as committed to the project as possible. During this process, tread carefully and detect and avoid illegitimate stakeholders that could impair the development of the standard. Especially the second factor is important, as legitimacy was not necessarily a factor stakeholders considered. This was highlighted in an interview with an IIoT entrepreneur: "The discussion about legitimacy fades somewhat into the background" [5].

5.4. Limitations

One of the limitations is the range of standard types scanned, particularly in an attempt to distinguish between de facto and de jure standards. De facto standards emerge due to predominance and wide acceptance on the market, while de jure standards are ratified by SDOs. For instance, RFID UHF became a widespread de jure standard in industries like retail and logistic value chains, which greatly benefited from stakeholder buy-in and official support through regulatory bodies, thus yielding remarkable market effects. On the contrary, the Zephyr Project is the source of a rather niche open-source de facto standard that so far has not achieved key market penetration and did not reach any formal status. These distinctions introduce variability in adoption patterns, possibly complicating the ability to generalise findings across both de facto and de jure standards.

This study examined a diverse range of IIoT standards: each technology type and corresponding standard presents unique challenges in terms of interoperability, user demand, and compatibility requirements. The diversity between technologies—such as the RFID UHF standard versus the Zephyr

Project standard could limit the comparability of findings across cases. RFID UHF represents a mature, hardware-intensive technology with specific use cases in asset tracking, whereas the Zephyr Project is an evolving, open-source software standard targeting resource-constrained IIoT devices. Such technological heterogeneity could trouble the interpretation of stakeholder influence and the generalisation of patterns across cases. Thus, the results obtained are not to be unthinkingly generalised for other technologies or standardisation efforts outside the context of IIoT.

Another limitation of this research is the unavailability of experts for standards that have not reached market acceptance. In the case of standards that failed to reach market acceptance, such as UPnP, it was difficult to identify and interview relevant experts. This shall not be surprising in such cases, as in the case of an unsuccessful standard, the industrial engagement will gradually decrease over time. Because some of these standards had nobody actively working or advocating for them, deep information about specific challenges and stakeholder interactions was limited.

Additionally, another limitation is the longevity of the research's results. The IIoT industry is marked by rapid technological changes coupled with fluctuating market demands. Also, the stakeholder characteristics as mentioned afore are subject to rapid changes as well. Given that standardisation is usually a time-consuming process, the different standards reviewed within this study could be at varied stages of their life cycle and stakeholder properties could change leading to a shift in results.

Finally, despite the best effort to make representative the selection of stakeholders, there is the possibility that responses could be biased by the background of experts in the standardisation ecosystem: for example, stakeholders from more dominant organisations may stress the advantage of proprietary standards, while those sitting in smaller entities may underline the need for open and inclusive approaches. This bias, though inevitable, may therefore affect the results coming from the empirical analysis.

6 Conclusion

6.1. Key findings

The thesis aimed to answer the Main research question: To what extent do stakeholders' characteristics and infrastructure in standardisation processes influence the development of technological standards in industrial IoT? And it did so by examining how stakeholder characteristics, such as power, legitimacy, and urgency, interact within standardisation processes to influence technological standards in the Industrial Internet of Things (IIoT). Through a literature review, an empirical analysis of eight cases across the four IIoT phases—data ingestion, transmission, processing, and utilisation and a series of policy recommendation, the research helps better understand stakeholders' characteristics and infrastructure and their impact on market adoption of standards. The literature review highlighted the importance of diverse stakeholder involvement and the large power that large corporations wield over standardisation processes. It also made a framework for how this research could empirically identify useful patterns of stakeholder salience. The literature review poses Public-Private Partnerships as a solution to address power imbalances.

The first sub-question, Empirically, how does the classification of stakeholders—organised into a matrix based on their levels of power, legitimacy, and urgency—affect the emergence of technological standards in industrial IoT?, was addressed by categorising stakeholders in the selected IIoT case studies using the framework outlined by De Vries et al. (2003) for identifying and classifying stakeholders. It can be concluded that the following classifications of stakeholders affect the emergence of technological standards in industrial IoT:
1) End-user engagement is essential: End users and related organisations are more prevalent in standards with market adoption. Their involvement as dominant or definitive stakeholders contributes significantly to the adoption and implementation of the standard.
2) Dangerous stakeholders hinder adoption: In 3 out of 4 standards without market adoption, there is at least one dangerous stakeholder. Their presence correlates with the lack of adoption, indicating that stakeholders who have power and urgency but lack legitimacy can create obstacles in the standardisation process.
3) Definitive stakeholders drive market adoption: Standards with market adoption have a higher average number of definitive stakeholders (4) compared to those without market adoption (1.75). This suggests that the involvement of stakeholders possessing power, urgency, and legitimacy is crucial for a standard's success in the market.
4) Higher stakeholder participation in adopted standards: Standards that have been adopted in the market involve more stakeholders on average (11.25) compared to those without market adoption (7.5). Broad stakeholder participation enhances the standard's credibility and acceptance.
5) Absence of stakeholders with only power or urgency: Stakeholders possessing only power (type E) or only urgency (type G) do not appear in the table. This absence indicates that power or urgency alone is insufficient to impact standard adoption.

The second sub-question, How can agents such as policymakers, researchers, and businesses effec-

tively influence stakeholders' characteristics and infrastructure to improve the standardisation process in Industrial IIoT? Was explored through policy recommendations and practical strategies derived from the case studies and literature. Key methods to influence stakeholders include:
1) Stimulating end-user engagement through:
- Creating well-established stakeholder groups
- Eliminating fees for participation
- Offering free consultation on standardisation efforts

2) Managing dangerous stakeholders by:
- Finding ways for them to participate with approval from other stakeholders
- Implementing review mechanisms through special committees

Sidenote: It is evident dangerous stakeholders should be avoided – but this is easier said than done. The literature sparingly writes about illegitimacy of stakeholders within standardisation and if there is something on the topic, it misses a resounding conclusion.

3) Increasing stakeholder participation by:
- Focusing on quality over quantity in standardisation efforts
- Providing resources to enhance stakeholder capabilities
- Creating regulatory frameworks that prioritise standardisation

So, to answer the main research question, research suggests that stakeholders' characteristics and infrastructure do to a large extent influence the development of technological standards in industrial IoT. The thesis demonstrates that stakeholders' power, legitimacy, and urgency and the composition of a set of diverse, committed group of stakeholders is crucial in determining the success or failure of standards.

6.2. Recommendations for future research

Building on the findings of this thesis, there is a requirement to improve the engagement of end-users in standardisation processes. End-users bring valuable insights drawn from their direct experiences. This helps ensuring that the developed standards are not only technically robust but also applicable to real-world situations. Despite this, the most effective methods for involving end-users remain underexplored. To overcome these challenges and identify more strategies for active end-user engagement, further empirical research is recommended. This research should focus on exploring innovative engagement methods such as interactive workshops, online platforms, or collaborative design sessions. Additionally, future research should aim to develop best practices and frameworks, for example based on empirical studies. Empirical studies like the one deployed in this thesis, with interviews and statements from actual stakeholders, bring new points of view to the discussion.

The involvement of illegitimate or dangerous stakeholders in standardisation processes is shown as a barrier to the market adoption of standards. These stakeholders lack the necessary legitimacy because of questionable intentions, lack of expertise, conflicting interests or financial issues. Their participation is a problem for collaboration among stakeholders required to develop effective standards. Future empirical research could focus on Identification and verification mechanisms, researching criteria to verify the legitimacy of stakeholders that help ensure that only qualified stakeholders are involved. Also to enhance transparency, research on more involve open meetings and clear communication channels in the difficult to navigate standardisation space could allow for better legit checks. Thirdly, as shown by stakeholder interviews, awareness of illegitimate stakeholders is an issue. Raising awareness about the importance of legitimate participation can help organisations recognise the influence of dangerous stakeholders. Research on how to provide informational resources and raising awareness on this matter can give involved stakeholders the knowledge to identify potentially dangerous stakeholders. Another recommendation for future research is to apply and refine the stakeholder identification and classification method across sectors. This proved the usefulness of the structured approach to identifying, classifying, and analysing the stakeholder patterns in the IIoT standardisation process. Further research may apply this method to a broader range of sectors and standardisation contexts. Such a comparison across these domains allows research to find out whether the stakeholder dynamics developed in IIoT are similar in other domains, too, or if different patterns are developed. Additionally, empirical studies could explore how these typologies interact and how shifts in stakeholder influence over time impact standards development. It would, for example, consider in what way threatening stakeholders gain legitimation, power or urgency.

Longer lasting studies can be helpful in capturing standards that are continuously changing with time, at the rate of technological advancement. These studies shall be important since the researcher can identify changes occurring in stakeholder influence, market conditions, and the regulatory environment as standards mature or as competing standards emerge. Longitudinal empirical research on the evolution of standards over long periods could further indicate how standards are sustained, what contributes to long-term adoption, and what roles various stakeholders perform during the life cycle of a standard.

References

(1) (PDF) Internet of Things Standardisation - Status, Requirements, Initiatives and Organisations. (n.d.). Retrieved September 30, 2024, from https://www.researchgate.net/publication/255897630_Internet_of_Things_Standardisation_-_Status_Requirements_Initiatives_and_Organisations

(4) Internet of Things: how the data management cycle works | LinkedIn. (n.d.). Retrieved October 25, 2024, from https://www.linkedin.com/pulse/internet-things-how-data-management-cycle-works-linda-grasso/

21 CFR Part 11 Compliance with Inductive Automation's Ignition Platform | Inductive Automation. (n.d.-a). Retrieved October 23, 2024, from https://inductiveautomation.com/resources/article/21-cfr-part-11-compliance-with-inductive-automations-ignition-platform

21 CFR Part 11 Compliance with Inductive Automation's Ignition Platform | Inductive Automation. (n.d.-b). Retrieved October 25, 2024, from https://inductiveautomation.com/resources/article/21-cfr-part-11-compliance-with-inductive-automations-ignition-platform

(73) Lessons to learn from the failure of GE's IIoT Platform, Predix? | by Ravi Kumar. | Products, Platforms, Business & Innovation in Industry 4.0/IIoT | Medium. (n.d.-a). Retrieved October 23, 2024, from https://medium.com/world-of-iot/73-lessons-to-learn-from-the-failure-of-ges-iot-platform-predix-3b3d20eccd42

(73) Lessons to learn from the failure of GE's IIoT Platform, Predix? | by Ravi Kumar. | Products, Platforms, Business & Innovation in Industry 4.0/IIoT | Medium. (n.d.-b). Retrieved October 25, 2024, from https://medium.com/world-of-iot/73-lessons-to-learn-from-the-failure-of-ges-iot-platform-predix-3b3d20eccd42

(73) Lessons to learn from the failure of GE's IIoT Platform, Predix? | by Ravi Kumar. | Products, Platforms, Business & Innovation in Industry 4.0/IIoT | Medium. (n.d.-c). Retrieved October 25, 2024, from https://medium.com/world-of-iot/73-lessons-to-learn-from-the-failure-of-ges-iot-platform-predix-3b3d20eccd42

A Brief History of LoRa®: Three Inventors Share Their Personal Story at The Things Conference. (n.d.). Retrieved October 25, 2024, from https://blog.semtech.com/a-brief-history-of-lora-three-inventors-share-their-personal-story-at-the-things-conference

An App for that? GE Aviation and Boston University team up to go digital | GE Aerospace News. (n.d.). Retrieved October 23, 2024, from https://www.geaerospace.com/news/articles/people-technology/app-ge-aviation-and-boston-university-team-go-digital

Annual Analysis Reveals Steady Growth in Industrial Network Market. (n.d.). Retrieved September 30, 2024, from https://www.hms-networks.com/news/news-details/17-06-2024-annual-analysis-reveals-steady-growth-in-industrial-network-market

Arshad, S., Azam, M. A., Rehmani, M. H., & Loo, J. (2019). Recent advances in information-centric networking-based internet of things (ICN-IoT). *IEEE Internet of Things Journal*, *6*(2), 2128–2158. https://doi.org/10.1109/JIOT.2018.2873343

Arunachalam, K., & Ganapathy, G. (2016a). Research on UPnP protocol stack for applications on a home network. *International Journal of Engineering and Technology*, *8*(4), 1728–1736. https://doi.org/10.21817/IJET/2016/V8I4/160804413

Arunachalam, K., & Ganapathy, G. (2016b). Research on UPnP protocol stack for applications on a home network. *International Journal of Engineering and Technology*, *8*(4), 1728–1736. https://doi.org/10.21817/IJET/2016/V8I4/160804413

Associate – Zephyr Project. (n.d.). Retrieved October 25, 2024, from https://zephyrproject.org/members_category/associate/

Backhouse, J., Hsu, C. W., & Silva T Bauer, L. C. (2006). CIRCUITS OF POWER IN CREATING DEJ^RE STANDARDS: SHAPING AN INTERNATIONAL INFORMATION SYSTEMS SECURITY STANDARD^.

Belimpasakis, P., & Stirbu, V. (2007a). Remote access to Universal Plug and Play (UPnP) devices utilizing the atom publishing protocol. *3rd International Conference on Networking and Services,ICNS 2007*, 59–64. https://doi.org/10.1109/ICNS.2007.101

Belimpasakis, P., & Stirbu, V. (2007b). Remote access to Universal Plug and Play (UPnP) devices utilizing the atom publishing protocol. *3rd International Conference on Networking and Services,ICNS 2007*, 59–64. https://doi.org/10.1109/ICNS.2007.101

Blind, K., & Heß, P. (2023). Stakeholder perceptions of the role of standards for addressing the sustainable development goals. *Sustainable Production and Consumption*, *37*, 180–190. https://doi.org/10.1016/J.SPC.2023.02.016

Book-2011 Kopetz Real-time systems Design principles for distributed embedded applications.pdf | Free download. (n.d.). Retrieved October 25, 2024, from https://www.slideshare.net/slideshow/book2011-kopetz-realtime-systems-design-principles-for-distributed-embedded-applicationspdf/251918835

Botzem, S., & Dobusch, L. (2012). Standardization Cycles: A Process Perspective on the Formation and Diffusion of Transnational Standards. *Organization Studies*, *33*(5–6), 737–762. https://doi.org/10.1177/0170840612443626

Brader, S. (n.d.-a). *Nick Simha Global Head of Independent Software Vendors GE Digital Independent Software Vendors Driving Market Share Through ISV Partnership and Innovation*.

Brader, S. (n.d.-b). *Nick Simha Global Head of Independent Software Vendors GE Digital Independent Software Vendors Driving Market Share Through ISV Partnership and Innovation*.

Brass, I., & Sowell, J. H. (2021). Adaptive governance for the Internet of Things: Coping with emerging security risks. *Regulation & Governance*, *15*(4), 1092–1110. https://doi.org/10.1111/REGO.12343

Brunsson, N., Rasche, A., & Seidl, D. (2012). The Dynamics of Standardization: Three Perspectives on Standards in Organization Studies. *Organization Studies*, *33*(5–6), 613–632. https://doi.org/10.1177/0170840612450120

Burrows, J. H. (1999). Information Technology standards in a changing world: the role of the users. *Computer Standards & Interfaces*, *20*(4–5), 323–331. https://doi.org/10.1016/S0920-5489(98)00068-3

CallStranger: UPnP Flaw Affecting Billions of Devices Allows Data Exfiltration, DDoS Attacks - SecurityWeek. (n.d.). Retrieved November 8, 2024, from https://www.securityweek.com/callstranger-upnp-flaw-affecting-billions-devices-allows-data-exfiltration-ddos-attacks/

Ciciora, W., Farmer, J., Large, D., & Adams, M. (2004). Consumer Electronics Interface. *Modern Cable Television Technology*, 903–940. https://doi.org/10.1016/B978-155860828-3/50025-4

Clarke, I., & Flaherty, T. B. (2008a). RFID and Consumer Privacy. *Journal of Internet Commerce*, *7*(4), 513–527. https://doi.org/10.1080/15332860802507370

Clarke, I., & Flaherty, T. B. (2008b). RFID and Consumer Privacy. *Journal of Internet Commerce*, *7*(4), 513–527. https://doi.org/10.1080/15332860802507370

Connecting Dots: Ignition And The Automation Pyramid | Inductive Automation. (n.d.-a). Retrieved October 23, 2024, from https://inductiveautomation.com/blog/connecting-dots-ignition-and-the-automation-pyramid

Connecting Dots: Ignition And The Automation Pyramid | Inductive Automation. (n.d.-b). Retrieved October 25, 2024, from https://inductiveautomation.com/blog/connecting-dots-ignition-and-the-automation-pyramid

Cranmer, E. E., Papalexi, M., tom Dieck, M. C., & Bamford, D. (2022). Internet of Things: Aspiration, implementation and contribution. *Journal of Business Research*, *139*, 69–80. https://doi.org/10.1016/j.jbusres.2021.09.025

de Vries, H. J. (n.d.). *The Classification of Standards*. https://doi.org/10.1007/978-1-4757-3042-5_9

de Vries, H., Verheul, H., & Willemse, H. (n.d.). *Standard Making: A Critical Research Frontier for Information Systems MISQ Special Issue Workshop STAKEHOLDER IDENTIFICATION IN IT STANDARDIZATION PROCESSES*.

Decathlon's Thriving Frugality: The Unseen Power of RFID in Retail Efficiency (IoT Expo China-IOTE® Expo) | by IIoT EXPO | Medium. (n.d.). Retrieved September 30, 2024, from https://medium.com/@ioteventinchina/decathlons-thriving-frugality-the-unseen-power-of-rfid-in-retail-efficiency-iot-expo-china-iote-afdf1aacd5c2

Digital Transformation Services | Digital Advisory | GE Digital. (n.d.-a). Retrieved October 23, 2024, from https://www.ge.com/digital/services/digital-transformation-advisory-services

Digital Transformation Services | Digital Advisory | GE Digital. (n.d.-b). Retrieved October 25, 2024, from https://www.ge.com/digital/services/digital-transformation-advisory-services

Distributors | Sigfox Partner Network | The IIoT solution book. (n.d.). Retrieved October 25, 2024, from https://partners.sigfox.com/companies/distributor

Drents Internet der Dingen Initiatief brengt toeristen bij schaapskuddes - Provincie Drenthe. (n.d.-a). Retrieved October 23, 2024, from https://www.provincie.drenthe.nl/actueel/nieuwsberichten/mede-mogelijk/drents-internet/

Drents Internet der Dingen Initiatief brengt toeristen bij schaapskuddes - Provincie Drenthe. (n.d.-b). Retrieved October 25, 2024, from https://www.provincie.drenthe.nl/actueel/nieuwsberichten/mede-mogelijk/drents-internet/

Educational Engagement Program | Inductive Automation. (n.d.-a). Retrieved October 23, 2024, from https://inductiveautomation.com/educational-engagement

Educational Engagement Program | Inductive Automation. (n.d.-b). Retrieved October 25, 2024, from https://inductiveautomation.com/educational-engagement

Ehie, I. C., & Chilton, M. A. (2020). Understanding the influence of IT/OT Convergence on the adoption of Internet of Things (IoT) in manufacturing organizations: An empirical investigation. *Comput. Ind.*, *115*. https://doi.org/10.1016/J.COMPIND.2019.103166

Ergonomics standards: identifying stakeholders and encouraging participation. (n.d.).

EPCIS IMPLEMENTATION BENCHMARKING SURVEY. (n.d.). Retrieved November 8, 2024, from https://www.hda.org/getmedia/6ba442b9-54a6-4223-b283-65630753d410/HDA-Foundation-EPCIS-Report-Spring-2021.pdf

Everything you need to know about IIoT | GE Digital. (n.d.). Retrieved October 23, 2024, from https://www.ge.com/digital/blog/what-industrial-internet-things-iiot

Explaining Sigfox. (n.d.-a). Retrieved October 23, 2024, from https://ubidots.com/blog/explaining-sigfox/

Explaining Sigfox. (n.d.-b). Retrieved October 25, 2024, from https://ubidots.com/blog/explaining-sigfox/

Fischer-Hübner, S., Alcaraz, C., Ferreira, A., Fernandez-Gago, C., Lopez, J., Markatos, E., Islami, L., & Akil, M. (2021). Stakeholder perspectives and requirements on cybersecurity in Europe. *Journal of Information Security and Applications*, *61*, 102916. https://doi.org/10.1016/J.JISA.2021.102916

Foray, D. (1994). Users, standards and the economics of coalitions and committees. *Information* Economics and Policy, 6(3–4), 269–293. `https://doi.org/10.1016/0167-6245(94)90005-`1

Fremont, C. (2024). https://lora-alliance.org/lora-alliance-press-release/lora-alliance-issues-2023-annual-report-highlighting-lorawan-maturity-robust-adoption-and-diversity-of-end-to-end-solutions/.

GE Aviation and Czech Technical University team up on groundbreaking collaboration for turboprop engines | GE News. (n.d.). Retrieved October 25, 2024, from https://www.ge.com/news/press-releases/ge-aviation-and-czech-technical-university-team-groundbreaking-collaboration

GE Digital + PwC - Tech alliances - Digital - PwC. (n.d.-a). Retrieved October 23, 2024, from https://www.pwc.nl/nl/dienstverlening/tech-alliances/ge-digital.html

GE Digital + PwC - Tech alliances - Digital - PwC. (n.d.-b). Retrieved October 25, 2024, from https://www.pwc.nl/nl/dienstverlening/tech-alliances/ge-digital.html

GE Digital expands its Predix platform portfolio. (n.d.). Retrieved October 23, 2024, from https://www.windpowerengineering.com/ge-digital-expands-predix-platform-portfolio/

GE Digital Launches Collaborative App Development Program to Expand Digital Industrial Ecosystem | GE News. (n.d.-a). Retrieved October 23, 2024, from https://www.ge.com/news/press-releases/ge-digital-launches-collaborative-app-development-program-expand-digital-industrial

GE Digital Launches Collaborative App Development Program to Expand Digital Industrial Ecosystem | GE News. (n.d.-b). Retrieved October 25, 2024, from https://www.ge.com/news/press-releases/ge-digital-launches-collaborative-app-development-program-expand-digital-industrial

GE Digital Transformation Failure With Pedrix Hitting Rough. (n.d.). Retrieved November 8, 2024, from https://www.boldbusiness.com/digital/predix-hits-rough-water/

GE 'Predix' the Future of Manufacturing | 2017-03-29 | Assembly Magazine | ASSEMBLY. (n.d.). Retrieved October 25, 2024, from https://www.assemblymag.com/articles/93763-ge-predix-the-future-of-manufacturing

GE wants Predix to be the Windows of industrial IIoT | CIO. (n.d.-a). Retrieved October 23, 2024, from https://www.cio.com/article/236602/ge-wants-predix-to-be-the-windows-of-industrial-iot.html

GE wants Predix to be the Windows of industrial IIoT | CIO. (n.d.-b). Retrieved October 25, 2024, from https://www.cio.com/article/236602/ge-wants-predix-to-be-the-windows-of-industrial-iot.html

Gemeenten aan de slag met Internet of Things-platform. (n.d.-a). Retrieved October 23, 2024, from https://www.binnenlandsbestuur.nl/digitaal/gemeenten-aan-de-slag-met-internet-things-platform

Gemeenten aan de slag met Internet of Things-platform. (n.d.-b). Retrieved October 25, 2024, from https://www.binnenlandsbestuur.nl/digitaal/gemeenten-aan-de-slag-met-internet-things-platform

Github. (n.d.). https://github.com/zephyrproject-rtos/zephyr/issues/79744. Github.

Gottlieb, A. (2003). *Casestudie naar ISO 15181 Paints and varnishes-Determination of release rate of biocides from antifouling paints'*.

Graz, J.-C., Graz, & Jean-Christophe. (2018). *Global corporations and the governance of standards*. 448–462. https://EconPapers.repec.org/RePEc:elg:eechap:16821_28

GSMP Manual | GS1. (n.d.). Retrieved October 25, 2024, from https://www.gs1.org/standards/gsmp-manual/current-standard

Haddaway, N. R., Page, M. J., Pritchard, C. C., & McGuinness, L. A. (2022). PRISMA2020: An R package and Shiny app for producing PRISMA 2020-compliant flow diagrams, with interactivity for optimised digital transparency and Open Synthesis Campbell Systematic Reviews, 18, e1230. https://doi.org/10.1002/cl2.1230

Hanafizadeh, P., Hatami Lankarani, F., & Nikou, S. (2022). Perspectives on management theory's application in the internet of things research. *Information Systems and E-Business Management*, *20*(4), 749–787. https://doi.org/10.1007/S10257-022-00569-0/FIGURES/5

Havenbedrijf Rotterdam neemt Internet of Things platform in gebruik | Port of Rotterdam. (n.d.). Retrieved June 21, 2024, from https://www.portofrotterdam.com/nl/nieuws-en-persberichten/havenbedrijf-rotterdam-neemt-internet-things-platform-gebruik

Henk J. de Vries, Hugo Verheul, & Harmen Willemse. (2003). *(PDF) Stakeholder identification in IT standardization processes*. https://www.researchgate.net/publication/228429345_Stakeholder_identification_in_IT_standardization_processes

Hoogerbrugge, C., van de Kaa, G., & Chappin, E. (2023). Adoption of quality standards for corporate greenhouse gas inventories: The importance of other stakeholders. *International Journal of Production Economics*, *260*, 108857. https://doi.org/10.1016/J.IJPE.2023.108857

How GE burned $7B on their platform (and how to avoid doing the same). (n.d.). Retrieved October 12, 2024, from https://platformengineering.org/blog/how-general-electric-burned-7-billion-on-their-platform

https://edri.org/our-work/edri-gramnumber7-10rfid-european-commission-recommandation/. (n.d.).

IEEE Xplore Full-Text PDF: (n.d.). Retrieved June 5, 2024, from https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7785882

Ignition OPC UA Module | Add OPC UA Server and Client Functionality. (n.d.-a). Retrieved October 23, 2024, from https://inductiveautomation.com/ignition/modules/ignition-opc-ua

Ignition OPC UA Module | Add OPC UA Server and Client Functionality. (n.d.-b). Retrieved October 25, 2024, from https://inductiveautomation.com/ignition/modules/ignition-opc-ua

Inductive Automation Certified to Two New Standards for Company-Wide Secure Software Development Lifecycle | Inductive Automation. (n.d.-a). Retrieved October 23, 2024, from https://inductiveautomation.com/blog/inductive-automation-certified-to-two-new-standards-for-companywide-secure-software-development-lifecycle

Inductive Automation Certified to Two New Standards for Company-Wide Secure Software Development Lifecycle | Inductive Automation. (n.d.-b). Retrieved October 25, 2024, from https://inductiveautomation.com/blog/inductive-automation-certified-to-two-new-standards-for-companywide-secure-software-development-lifecycle

Inductive Automation: system-security. (n.d.). Retrieved October 25, 2024, from https://inductiveautomation.com/ignition/system-security

Inductive Automation Trust Center | Powered by SafeBase. (n.d.-a). Retrieved October 23, 2024, from https://security.inductiveautomation.com/

Inductive Automation Trust Center | Powered by SafeBase. (n.d.-b). Retrieved October 25, 2024, from https://security.inductiveautomation.com/

INDUSTRY4.0 TECHNOLOGY BATTLES IN MANUFACTURING OPERATIONS MANAGEMENT non-technical dominance factors for IIoT & MES. (2021). www.equinoxia.eu

Ioannis, Z. (n.d.). *Economic implications and policy developments SUMMARY*.

IoTNow. (2022). https://www.iot-now.com/2022/01/27/118862-sigfox-goes-into-receivership-after-raising-and-spending-e300mn-seeks-buyer-in-6-month-court-protection/.

ISA95, Enterprise-Control System Integration- ISA. (n.d.). Retrieved October 25, 2024, from https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa95

ISO - ISO/IEC standard on UPnP device architecture makes networking simple and easy. (n.d.-a). Retrieved October 23, 2024, from https://www.iso.org/news/2008/12/Ref1185.html

ISO - ISO/IEC standard on UPnP device architecture makes networking simple and easy. (n.d.-b). Retrieved October 25, 2024, from https://www.iso.org/news/2008/12/Ref1185.html

ISO 32000-1:2008 - Document management — Portable document format — Part 1: PDF 1.7. (n.d.). Retrieved October 25, 2024, from https://www.iso.org/standard/51502.html

Jakobs, K. (n.d.-a). *ICT Standardisation Management A multidimensional perspective on company participation in standardisation committees RSM-a force for positive change*.

Jakobs, K. (n.d.-b). *ICT STANDARDISATION-CO-ORDINATING THE DIVERSITY*.

Jakobs, K. (n.d.-c). *User Participation in Standardisation Processes Impact, Problems and Benefits*.

Jakobs, K. (2006). Shaping user-side innovation through standardisation: The example of ICT. *Technological Forecasting and Social Change*, *73*(1), 27–40. https://doi.org/10.1016/J.TECHFORE.2005.06.007

Jakobs, K. (2008). ICT standardisation - co-ordinating the diversity. *International Telecommunication Union - Proceedings of the 1st ITU-T Kaleidoscope Academic Conference, Innovations in NGN, K-INGN*, 119–126. https://doi.org/10.1109/KINGN.2008.4542257

Japan's Kobe Steel indicted over quality scandal. (n.d.-a). Retrieved October 25, 2024, from https://www.bbc.com/news/business-44895564

Japan's Kobe Steel indicted over quality scandal. (n.d.-b). Retrieved October 25, 2024, from https://www.bbc.com/news/business-44895564

Jia, H., & Qi, Z. (2009). Research on the implementation of secure UPnP architecture. *Proceedings of 2009 2nd IEEE International Conference on Broadband Network and Multimedia Technology, IEEE IC-BNMT2009*, 433–437. https://doi.org/10.1109/ICBNMT.2009.5348530

Jiang, H., Gao, S., Zhao, S., & Chen, H. (2020). Competition of technology standards in Industry 4.0: An innovation ecosystem perspective. *Systems Research and Behavioral Science*, *37*(4), 772–783. https://doi.org/10.1002/SRES.2718

Jorritsma. (2024). *CASEVERSLAG CODE VOOR INFORMATIEBEVEILIGING 2*. http://www.c-cure.org/7799history.htm

Kedia, M., Sekhani, R., & Katiyar, T. (2020). The Role of Standards in Diffusion of Emerging Technologies Internet of Things (IoT). *Indian Council for Research on International Economic Relations (ICRIER) Report*. https://ideas.repec.org/p/bdc/report/20-r-04.html

Kim, D. hyu, Lee, H., & Kwak, J. (2017). Standards as a driving force that influences emerging technological trajectories in the converging world of the Internet and things: An investigation of the M2M/IoT patent network. *Research Policy*, *46*(7), 1234–1254. https://doi.org/10.1016/j.respol.2017.05.008

Lavric, A., Petrariu, A. I., & Popa, V. (2019a). SigFox Communication Protocol: The New Era of IoT? *2019 International Conference on Sensing and Instrumentation in IIoT Era, ISSI 2019*. https://doi.org/10.1109/ISSI47111.2019.9043727

Lavric, A., Petrariu, A. I., & Popa, V. (2019b). SigFox Communication Protocol: The New Era of IoT? *2019 International Conference on Sensing and Instrumentation in IIoT Era, ISSI 2019*. https://doi.org/10.1109/ISSI47111.2019.9043727

Lechowski, G., & Krzywdzinski, M. (2022). Emerging positions of German firms in the industrial internet of things: A global technological ecosystem perspective. *Global Networks*, *22*(4), 666–683. https://doi.org/10.1111/GLOB.12380

Leech, N. L., Dellinger, A. B., Brannagan, K. B., & Tanaka, H. (2010). Evaluating Mixed Research Studies: A Mixed Methods Approach. *Journal of Mixed Methods Research*, *4*. https://doi.org/10.1177/1558689809345262

Lerche, C., Hartke, K., & Kovatsch, M. (2012). Industry adoption of the Internet of Things: A constrained application protocol survey. *IEEE International Conference on Emerging Technologies and Factory Automation, ETFA*. https://doi.org/10.1109/ETFA.2012.6489787

LoRa Alliance - Homepage - LoRa Alliance®. (n.d.-a). Retrieved October 23, 2024, from https://lora-alliance.org/

LoRa Alliance - Homepage - LoRa Alliance®. (n.d.-b). Retrieved October 25, 2024, from https://lora-alliance.org/

Main Keynote: Exploring 10 Years of Growth & Innovation | Inductive Automation. (n.d.). Retrieved November 8, 2024, from https://inductiveautomation.com/resources/icc/2022/main-keynote-exploring-10-years-of-growth-innovation

Markus, M. L., Steinfield, C. W., Wigand, R. T., & Minton, G. (2006). Industry-wide information systems standardization AS collective action: The case of the U.S. residential mortgage industry. *MIS Quarterly: Management Information Systems*, *30*(SPEC. ISS.), 439–465. https://doi.org/10.2307/25148768

Meddeb, A. (2016). Internet of things standards: Who stands out from the crowd? *IEEE Communications Magazine*, *54*(7), 40–47. https://doi.org/10.1109/MCOM.2016.7514162

Mendelow, A. L. (1981). *Association for Information Systems AIS Electronic Library (AISeL) Environmental Scanning-The Impact of the Stakeholder Concept*. http://aisel.aisnet.org/icis1981/20

MES | Inductive Automation. (n.d.). Retrieved October 23, 2024, from https://inductiveautomation.com/blog/tags/mes

Messer, A. (2014a). *Delivering the Internet of Things with UPnP*.

Messer, A. (2014b). *Delivering the Internet of Things with UPnP*.

Miller -Intel, K., & van der Beek -Cisco, W. (2014a). *UPnP Internet of Things*.

Miller -Intel, K., & van der Beek -Cisco, W. (2014b). *UPnP Internet of Things*.

Mitchell, R. K., Agle, B. R., & Wood, D. J. (1997). Toward a Theory of Stakeholder Identification and Salience: Defining the Principle of Who and What Really Counts. *The Academy of Management Review*, *22*(4), 853. https://doi.org/10.2307/259247

Mitsugi, J., Sato, Y., Ozawa, M., & Suzuki, S. (2014a). An integrated device and service discovery with UPnP and ONS to facilitate the composition of smart home applications. *2014 IEEE World Forum on Internet of Things, WF-IoT 2014*, 400–404. https://doi.org/10.1109/WF-IOT.2014.6803199

Mitsugi, J., Sato, Y., Ozawa, M., & Suzuki, S. (2014b). An integrated device and service discovery with UPnP and ONS to facilitate the composition of smart home applications. *2014 IEEE World Forum on Internet of Things, WF-IoT 2014*, 400–404. https://doi.org/10.1109/WF-IOT.2014.6803199

Mixed Methods Research | Definition, Guide & Examples. (n.d.). Retrieved May 1, 2024, from https://www.scribbr.com/methodology/mixed-methods-research/

Moon, S., & Lee, H. (2021). The Primary Actors of Technology Standardization in the Manufacturing Industry. *IEEE Access*, *9*, 101886–101901. https://doi.org/10.1109/ACCESS.2021.3097800

Narayana, A. (2023). Space Internet of Things (Space-IoT). *Citation*. https://doi.org/10.4233/uuid:07fade0a-fd62-4732-93fa-92cbb0dac538

Network Effects and Market Power: What Have We Learned in the Last Decade? (n.d.-a).

Network Effects and Market Power: What Have We Learned in the Last Decade? (n.d.-b).

Next-generation Connectivity - DHL - Netherlands. (n.d.). Retrieved October 25, 2024, from https://www.dhl.com/nl-en/home/innovation-in-logistics/logistics-trend-radar/next-generation-wireless-logistics.html

Normen voor producten, diensten of bedrijfsprocessen | Certificaten, normen en meetinstrumenten | Rijksoverheid.nl. (n.d.). Retrieved October 23, 2024, from https://www.rijksoverheid.nl/onderwerpen/certificaten-keurmerken-en-meetinstrumenten/normen-voor-producten-diensten-of-processen

OASIS Message Queuing Telemetry Transport (MQTT) TC - OASIS. (n.d.). Retrieved October 25, 2024, from https://groups.oasis-open.org/communities/tc-community-home2?CommunityKey=99c86e3a-593c-4448-b7c5-018dc7d3f2f6

OCF - UPnP Developer Resources. (n.d.). Retrieved October 23, 2024, from https://openconnectivity.org/developer/specifications/upnp-resources/upnp-developer-resources/

OCF - UPnP Standards & Architecture. (n.d.-a). Retrieved October 23, 2024, from https://openconnectivity.org/developer/specifications/upnp-resources/upnp/

OCF - UPnP Standards & Architecture. (n.d.-b). Retrieved October 25, 2024, from https://openconnectivity.org/developer/specifications/upnp-resources/upnp/

OCF Membership List. (n.d.). Retrieved October 25, 2024, from https://openconnectivity.org/foundation/membership-list/

One Industrial Platform for SCADA, IIoT, MES, and More | Ignition. (n.d.). Retrieved October 25, 2024, from https://inductiveautomation.com/ignition/

OnLogic Hardware for Ignition by Inductive Automation | OnLogic. (n.d.-a). Retrieved October 23, 2024, from https://www.onlogic.com/store/computers/ignition-edge-gateways/

OnLogic Hardware for Ignition by Inductive Automation | OnLogic. (n.d.-b). Retrieved October 25, 2024, from https://www.onlogic.com/store/computers/ignition-edge-gateways/

Overview of UHF frequency allocations (860 to 930 MHz) for RAIN RFID. (2022). www.aiti.gov.bn

OWASP Top 10 Risks for Open Source Software | OWASP Foundation. (n.d.). Retrieved October 25, 2024, from https://owasp.org/www-project-open-source-software-top-10/

(PDF) A Stakeholder Approach to Value Creation and Leadership. (n.d.). Retrieved October 23, 2024, from https://www.researchgate.net/publication/332098002_A_Stakeholder_Approach_to_Value_Creation_and_Leadership/figures

(PDF) Competing Standard-Setting Organizations: A Choice Experiment. (n.d.). Retrieved April 26, 2024, from https://www.researchgate.net/publication/356538689_Competing_Standard-Setting_Organizations_A_Choice_Experiment

(PDF) How stakeholder engagement affects IT projects. (n.d.-a). Retrieved April 26, 2024, from https://www.researchgate.net/publication/331976863_How_stakeholder_engagement_affects_IT_projects

(PDF) How stakeholder engagement affects IT projects. (n.d.-b). Retrieved October 25, 2024, from https://www.researchgate.net/publication/331976863_How_stakeholder_engagement_affects_IT_projects

(PDF) Internet of Things Standardisation - Status, Requirements, Initiatives and Organisations. (n.d.). Retrieved October 9, 2024, from https://www.researchgate.net/publication/255897630_Internet_of_Things_Standardisation_-_Status_Requirements_Initiatives_and_Organisations

(PDF) Promoting Legitimacy in Technical Standardization. (n.d.). Retrieved October 25, 2024, from https://www.researchgate.net/publication/42632398_Promoting_Legitimacy_in_Technical_Standardization

(PDF) Towards the IIoT Ecosystem Development - Understanding the Stakeholder Perspective. (n.d.). Retrieved October 25, 2024, from https://www.researchgate.net/publication/341234513_Towards_the_IIoT_Ecosystem_Development_-_Understanding_the_Stakeholder_Perspective

(PDF) User involvement in decision-making in information systems development. (n.d.). Retrieved October 23, 2024, from https://www.researchgate.net/publication/28675322_User_involvement_in_decision-making_in_information_systems_development

Pehkonen, V., & Koivisto, J. (2010). Secure universal plug and play network. *2010 6th International Conference on Information Assurance and Security, IAS 2010*, 11–14. https://doi.org/10.1109/ISIAS.2010.5604189

Prebanić, K. R., & Vukomanović, M. (2023). Exploring Stakeholder Engagement Process as the Success Factor for Infrastructure Projects. *Buildings 2023, Vol. 13, Page 1785*, *13*(7), 1785. https://doi.org/10.3390/BUILDINGS13071785

Preferred Partner for Ignition SCADA Globally | ATS Global. (n.d.-a). Retrieved October 23, 2024, from https://www.ats-global.com/ats-partner-products/ignition-scada/

Preferred Partner for Ignition SCADA Globally | ATS Global. (n.d.-b). Retrieved October 25, 2024, from https://www.ats-global.com/ats-partner-products/ignition-scada/

Press Releases | Linux Foundation | Zephyr. (n.d.-a). Retrieved October 23, 2024, from https://www.linuxfoundation.org/press/tag/zephyr

Press Releases | Linux Foundation | Zephyr. (n.d.-b). Retrieved October 25, 2024, from https://www.linuxfoundation.org/press/tag/zephyr

Project Members – Zephyr Project. (n.d.-a). Retrieved October 23, 2024, from https://zephyrproject.org/project-members/

Project Members – Zephyr Project. (n.d.-b). Retrieved October 25, 2024, from https://zephyrproject.org /project-members/

Radouan Ait Mouha, R. A. (2021). Internet of Things (IoT). *Journal of Data Analysis and Information Processing*, *09*(02), 77–101. https://doi.org/10.4236/JDAIP.2021.92006

Ramazan Karaöz. (2004). *Project Verbetering formele normalisatieproces*.

Rastegari, H., Nadi, F., Lam, S. S., Ikhwanuddin, M., Kasan, N. A., Rahmat, R. F., & Mahari, W. A. W. (2023). Internet of Things in aquaculture: A review of the challenges and potential solutions based on current and future trends. *Smart Agricultural Technology*, *4*, 100187. https://doi.org/10.1016/J.ATECH.2023.100187

RFID Case Study: Automation of logistic processes - Cisper Electronics B.V. (n.d.). Retrieved October 23, 2024, from https://www.cisper.nl/en/case-studies/rfid-case-study-automation-of-logistic-processes

RFID Case Study: Decathlon uses Tageos RFID labels to identify millions of items worldwide - Cisper Electronics B.V. (n.d.-a). Retrieved September 29, 2024, from https://www.cisper.nl/en/case-studies/rfid-case-study-decathlon-uses-tageos-rfid-labels-to-identify-millions-of-items-worldwide

RFID Case Study: Decathlon uses Tageos RFID labels to identify millions of items worldwide - Cisper Electronics B.V. (n.d.-b). Retrieved October 25, 2024, from https://www.cisper.nl/en/case-studies/rfid-case-study-decathlon-uses-tageos-rfid-labels-to-identify-millions-of-items-worldwide

rfid-experts - AIM Global. (n.d.). Retrieved October 25, 2024, from https://www.aimglobal.org/rfid-experts/

Saleem, J., Hammoudeh, M., Raza, U., Adebisi, B., & Ande, R. (2018). IIoT standardisation-Challenges, perspectives and solution. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3231053.3231103

SAP Cloud Platform vs GE Predix: Platform-as-a-Service (PaaS) Comparison. (n.d.). Retrieved October 25, 2024, from https://6sense.com/tech/platform-as-a-service-paas/sapcloudplatform-vs-gepredix#free-plan-signup

Scheepers, C. E., Wendel-Vos, G. C. W., den Broeder, J. M., van Kempen, E. E. M. M., van Wesemael, P. J. V., & Schuit, A. J. (2014). Shifting from car to active transport: A systematic review of the effectiveness of interventions. *Transportation Research Part A: Policy and Practice*, *70*, 264–280. https://doi.org/10.1016/J.TRA.2014.10.015

Scopus - Document details - 6G: The Path Toward Standardization | Signed in. (n.d.). Retrieved June 4, 2024, from https://www.scopus.com/record/display.uri?eid=2-s
2.0-85137226090&origin=resultslist&sort
=r-f&src=s&sid=b31852
e55fd594508e753a47de61c1c3&sot=b&sdt=b&s=TITLE-ABS-KEY%28%28%22standardisation%22+OR+%22
standards%22+OR+%22standardization%22%29+AND+%28%22stakeholder%22+OR+%22stakeholders
%22%29+AND+%22iot%22%29&sl=224&sessionSearchId=b31852
e55fd594508e753a47de61c1c3&relpos=2

Scopus - Document details - Distributed ledger technology applications in food supply chains: A review of challenges and future research directions | Signed in. (n.d.). Retrieved June 4, 2024, from
https://www.scopus.com/record/display.uri?eid=2-s2.0-
85104191861&origin=resultslist&sort=plf-f&src=s&sid=b31852e55fd594508e753a47de61c1c3&sot=b&sdt=b&s=KEY%
+standardisation+%22+OR+%22+standards+%22+OR+%22+standardization+%22+AND+%22+stakeholder+%22+OR
+%22+AND+%22+iot+%22%29&
sl=224&sessionSearchId=b31852e55fd594508e753a47de61c1c3&relpos=0

Scopus - Document details - Emerging Construction Technologies: State of Standard and Regulation Implementation | Signed in. (n.d.). Retrieved June 4, 2024, from https://www.scopus.com/record/display.uri?eid=2-
s2.0-8507952
2679&origin=resultslist&sort=plf-f&src=s&sid=b31852e55fd594508e753a47de61c1c3&sot=b&sdt=b
&s=KEY%28%22+standardisation+%22+OR+%22+standards+%22+OR+%22+standardization+%2

2+AND+%22+stakeholder+%22+OR+%22+stakeholders+%22+AND+%22+iot+%22%29&sl=224&sessionSearchId=b31852e55fd594508e753a47de61c1c3&relpos=3

Scopus - Document details - Implementing IIoT in India—A Look at Macro Issues and a Framework for Recommendations | Signed in. (n.d.). Retrieved June 4, 2024, from https://www.scopus.com/record/display.uri?eid=2-s2.

Scopus - Document details - Internet of Things (IoT) adoption barriers of smart cities' waste management: An Indian context | Signed in. (n.d.). Retrieved June 4, 2024, from https://www.scopus.com/record/display.uri?eid=2-s2.0-85087764176

Scopus - Document details - IIoT security: Experience is an expensive teacher | Signed in. (n.d.). Retrieved June 4, 2024, from https://www.scopus.com/record/display.uri?eid=2-s2.0-85119278569

Scopus - Document details - IIoT Standardization Strategies in ISO/IEC JTC 1/SC 41 | Signed in. (n.d.). Retrieved June 4, 2024, from https://www.scopus.com/record/display.uri?eid=2-s2.0-85164106838&origin=results

Scopus - Document details - Linked data for smart homes: Comparing RDF and labeled property graphs | Signed in. (n.d.). Retrieved June 4, 2024, from https://www.scopus.com/record/display.uri?eid=2-s2.0-85092160328&origin=resultslist

Scopus - Document details - Standardising the IIoT - Collaboration or competition? | Signed in. (n.d.). Retrieved June 4, 2024, from https://www.scopus.com/record/display.uri?eid=2-s2.0-79955127598

Security Review Guidelines | Predix Platform | GE Digital. (n.d.). Retrieved October 25, 2024, from https://www.ge.com/digital/documentation/predix-platforms/srg.html

Semtech LoRa Technology Overview | Semtech. (n.d.). Retrieved October 25, 2024, from https://www.semtech.com/lora

Sense (and) the city | TU Delft Repository. (n.d.). Retrieved July 16, 2024, from https://repository.tudelft.nl/record/uuid:72623442-5791-4cfe-8a60-89410f2b3d00

Shao, A. ;, Ishengoma, D. R. ;, Alexopoulos, F. R., Saxena, C. ;, Nikiforova, S. ;, & Matheus, A. (2023). Integration of IIoT into e-government. *Foresight Citation*, *25*(5), 734–750. https://doi.org/10.1108/FS-04-2022-0048

Shinkansen parts produced by Kobe Steel didn't meet designated industrial standards - The Mainichi. (n.d.-a). Retrieved October 25, 2024, from https://mainichi.jp/english/articles/20171013/p2a/00m/0na/022000c

Sigfox | Adeunis. (n.d.). Retrieved October 25, 2024, from https://www.adeunis.com/en/partenaires/sigfox-2/

Sigfox - Heliot Europe. (n.d.-a). Retrieved October 23, 2024, from https://www.heliotgroup.com/en/technologies/sigfox/

Sigfox owner Unabiz and LoRa group The Things Industries make deal on "unified LPWAN." (n.d.). Retrieved October 23, 2024, from https://www.rcrwireless.com/20230227/internet-of-things-4/sigfox-owner-unabiz-and-lora-group-the-things-industries-make-deal-on-unified-lpwan

Sigfox, the French IIoT startup that had raised more than $300M, files for bankruptcy protection as it seeks a buyer | TechCrunch. (n.d.-b). Retrieved October 25, 2024, from https://techcrunch.com/2022/01/27/sigfox-the-french-iot-startup-that-had-raised-more-than-300m-files-for-bankruptcy-protection-as-it-seeks-a-buyer/

Sigfox-Ready LoRaWAN-Ready IIoT Products – UnaBiz. (n.d.). Retrieved October 25, 2024, from https://www.unabiz.com/products/

Stakeholder - Learn About the Different Types of Stakeholders. (n.d.). Retrieved October 25, 2024, from https://corporatefinanceinstitute.com/resources/accounting/stakeholder/

Standard making: A critical research frontier for information systems research. (2006). *MIS Quarterly: Management Information Systems*, *30*(SPEC. ISS.), 405–411. https://doi.org/10.2307/25148766

Standards Stakeholders: Who Should, and Who Does, Set Standards? - ConsortiumInfo.orgConsortiumInfo.org. (n.d.). Retrieved October 23, 2024, from https://www.consortiuminfo.org/metalibrary/standards-stakeholders-who-should-and-who-does-set-standards/

System Integrator Search | Find an Ignition Integrator. (n.d.-a). Retrieved October 23, 2024, from https://inductiveautomation.com/integrators/

System Integrator Search | Find an Ignition Integrator. (n.d.-b). Retrieved October 25, 2024, from https://inductiveautomation.com/integrators/results

Tamtomo, T. D., Rarasati, A. D., & Adiwijaya, A. J. S. (2019). The Role of Stakeholders in Infrastructure Development that supports the Higher Education Innovation Ecosystem in Indonesia. *Journal of International Conference Proceedings*, 2(1). https://doi.org/10.32535/JICP.V2I1.497

Tassey, G., & Economist, S. (1999). *Standardization in Technology-Based Markets*.

The inside story on why UnaBiz bought Sigfox and what it did next. (n.d.). Retrieved October 25, 2024, from https://www.lightreading.com/iot/the-inside-story-on-why-unabiz-bought-sigfox-and-what-it-did-next

The LoRaWAN Network server for scale | The Things Industries. (n.d.-a). Retrieved October 23, 2024, from https://www.thethingsindustries.com/

The LoRaWAN Network server for scale | The Things Industries. (n.d.-b). Retrieved October 25, 2024, from https://www.thethingsindustries.com/

The Things Network. (n.d.). Retrieved October 23, 2024, from https://www.thethingsnetwork.org/

The Zephyr Story: How It Became a Self-Sustaining Ecosystem. (n.d.-a). Retrieved October 23, 2024, from https://www.intel.com/content/www/us/en/developer/articles/community/zephyr-story-how-became-self-sustaining-ecosystem.html

The Zephyr Story: How It Became a Self-Sustaining Ecosystem. (n.d.-b). Retrieved October 25, 2024, from https://www.intel.com/content/www/us/en/developer/articles/community/zephyr-story-how-became-self-sustaining-ecosystem.html

Tiburski, R. T., Amaral, L. A., de Matos, E., de Azevedo, D. F. G., & Hessel, F. (2016). The Role of Lightweight Approaches Towards the Standardization of a Security Architecture for IIoT Middleware Systems. *IEEE Communications Magazine*, *54*(11), 56–62. https://doi.org/10.1109/MCOM.2016.1600462CM

Trautman, L. J., Molesky, M., Hussein, M., & Ngamassi, L. (2019). Governance of the Internet of Things (IoT). *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.3443973

UPnP ^{TM} Technology-The Simple, Seamless Home Network. (n.d.-a).

UPnP ^{TM} Technology-The Simple, Seamless Home Network. (n.d.-b).

UPnP ^{TM} Technology-The Simple, Seamless Home Network. (n.d.-c).

van de Kaa, G. (2023). Standards adoption: A comprehensive multidisciplinary review. *Heliyon*, *9*(8), e19203. https://doi.org/10.1016/J.HELIYON.2023.E19203

van de Kaa, G., & de Vries, H. J. (2015). Factors for winning format battles: A comparative case study. *Technological Forecasting and Social Change*, *91*, 222–235. https://doi.org/10.1016/J.TECHFORE.2014.02.019

van de Kaa, G., & Greeven, M. (2017). LED standardization in China and South East Asia: Stakeholders, infrastructure and institutional regimes. *Renewable and Sustainable Energy Reviews*, *72*, 863–870. https://doi.org/10.1016/J.RSER.2017.01.101

van de Kaa, G., van den Ende, J., de Vries, H. J., & van Heck, E. (2011). Factors for winning interface format battles: A review and synthesis of the literature. *Technological Forecasting and Social Change*, *78*(8), 1397–1411. https://doi.org/10.1016/J.TECHFORE.2011.03.011

van den Ende, J., van de Kaa, G., den Uijl, S., & de Vries, H. J. (n.d.). *The Paradox of Standard Flexibility: The Effects of Co-evolution between Standard and Interorganizational Network*. https://doi.org/10.1177/0170840612443625

van Wee, B., & Banister, D. (2015). Transport Reviews How to Write a Literature Review Paper? How to Write a Literature Review Paper? *Transport Reviews*, *0*. https://doi.org/10.1080/01441647.2015.1065456

Verheul, H. (n.d.). *Verbetering formele normalisatieproces*.

Verkleij, R. A. H. (2023). *THE INFLUENCE OF DIVERSITY AND SIZE OF STANDARD SETTING ORGANISATIONS AND STANDARDS CONSORTIA ON STANDARD SUCCESS*.

Wang, W., Zhang, S., & King, A. P. (2016). Research on the adoption barriers of the engineering construction standards in China. *Structural Survey*, *34*(4–5), 367–378. https://doi.org/10.1108/SS-02-2015-0010

Werle, R., & Iversen, E. (2006). *Promoting Legitimacy in Technical Standardization*. https://doi.org/10.17877/DE290R-12756

What is Predix Platform? | Edge Software and Services 2.10 Documentation | GE Vernova. (n.d.-a). Retrieved October 23, 2024, from https://www.ge.com/digital/documentation/edge-software/c_what_is_predix_platform.html

What is Predix Platform? | Edge Software and Services 2.10 Documentation | GE Vernova. (n.d.-b). Retrieved October 25, 2024, from https://www.ge.com/digital/documentation/edge-software/c_what_is_predix_platform.html

What is Sigfox 0G technology? | Sigfox build. (n.d.-a). Retrieved October 23, 2024, from https://build.sigfox.com/sigfox

What is UPnP and why is it Dangerous? (n.d.-b). Retrieved October 25, 2024, from https://www.varonis.com/blog/what-is-upnp

What is UPnP and why you should disable it immediately | NordVPN. (n.d.-a). Retrieved October 23, 2024, from https://nordvpn.com/blog/what-is-upnp/

What is UPnP (Universal Plug and Play)? (n.d.). Retrieved October 23, 2024, from https://phoenixnap.com/blog/what-is-upnp

What is UPnP? Yes, It's Still Dangerous in 2024 | UpGuard. (n.d.). Retrieved October 23, 2024, from https://www.upguard.com/blog/what-is-upnp

Where and how to capture accelerating IIoT value | McKinsey. (n.d.). Retrieved October 23, 2024, from https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/iot-value-set-to-accelerate-through-2030-where-and-how-to-capture-it

Wiegmann, P. M., Eggers, F., de Vries, H. J., & Blind, K. (2022). Competing Standard-Setting Organizations: A Choice Experiment. *Research Policy*, *51*(2). https://doi.org/10.1016/J.RESPOL.2021.104427

Wiegmann, P. M., Henk, I., de Vries, J., & Eom, D. (2023). *Measuring societal impact of standards*. www.tue.nl

Windows network architecture and the OSI model - Windows drivers | Microsoft Learn. (n.d.). Retrieved October 25, 2024, from https://learn.microsoft.com/en-us/windows-hardware/drivers/network/windows-network-architecture-and-the-osi-model

WORKSTREAM 3 NSBs peer-review (including SMEs and civil society inclusiveness) Summary of findings from the questionnaires and interviews. (2024).

Yu-Han Chang. (2023, May 9). https://www.idtechex.com/en/research-article/exploring-the-growth-and-market-breakdown-of-passive-rfid/29245.

Zephyr Project Welcomes ZEISS as a Platinum Member and Hunan University as an Associate Member – Zephyr Project. (n.d.). Retrieved October 23, 2024, from https://zephyrproject.org/zephyr-project-welcomes-zeiss-as-a-platinum-member-and-hunan-university-as-an-associate-member/

Appendix A
Case selection

Table 1: Case Selection Overview

Standard	Building block	Market adoption	Function
Zigbee & IEEE 802.15.4	Data Ingestion	Yes	Wireless protocol for low-power, low-bandwidth IIoT devices.
RFID EPCglobal	Data Ingestion	Undecided	RFID tags standard for inventory and logistics.
MTConnect	Data Ingestion	Yes	Protocol for connecting manufacturing equipment to networks.
EPC Gen2 (ISO 18000-63)	Data Ingestion	Yes	UHF RFID tags standard for supply chains.
IEEE 1451	Data Ingestion	No	Smart transducer interfaces standard for sensors and actuators.
Bluetooth Low Energy (BLE)	Data Ingestion/Data Transmission	Yes	Wireless standard for short-range, low-power devices.
Z-Wave	Data Ingestion/Data Transmission	Yes	Wireless protocol for smart home devices.
HART	Data Ingestion/Data Transmission	Yes	Protocol for smart field instruments in process industries.
Ethercat	Data Ingestion to Data Transmission	Yes	High-performance fieldbus system for real-time data.
LoRaWAN	Data Transmission	Yes	Long-range, low-power wireless protocol for IoT.
IPv6	Data Transmission	Yes	Internet protocol for addressing and routing devices.
MQTT	Data Transmission	Yes	Lightweight messaging for sensors and mobile devices.
CoAP	Data Transmission	Yes	Low-power communication for constrained devices.
AMQP	Data Transmission	Yes	Messaging standard for organizations.
Wi-Fi HaLow (802.11ah)	Data Transmission	Yes	Long-range, low-power Wi-Fi for IIoT devices.
NB-IoT	Data Transmission	Yes	LPWAN technology for cellular networks.
Sigfox	Data Transmission	Yes	Ultra-narrowband IIoT network connectivity.

Continued on next page

Table 1 – continued from previous page

Standard	Building block	Market adoption	Function
PROFINET	Data Transmission	Yes	Industrial Ethernet for real-time data.
M-Bus	Data Transmission	Yes	Standard for remote utility meter reading.
Wi-SUN	Data Transmission	Yes	Wireless protocol for smart utility networks.
Thread / Matter	Data Transmission	Yes	Mesh networking for IIoT home automation.
ISA-100	Data Transmission	Yes	Wireless standard for industrial automation.
WirelessHART	Data Transmission	Yes	Wireless protocol for process automation.
OneM2M	Data Transmission	Yes	Global standard for M2M and IIoT communication.
IEEE 802.11ac	Data Transmission	Yes	High-speed Wi-Fi for wireless networks.
IEEE 802.11ax	Data Transmission	Yes	Enhanced Wi-Fi for better performance.
Wi-Fi Direct	Data Transmission	Yes	Peer-to-peer Wi-Fi for device communication.
NFC	Data Transmission	Yes	Short-range wireless for contactless communication.
ISO/IEC 14443	Data Transmission	Yes	Contactless smart cards standard at 13.56 MHz.
3GPP (5G NR)	Data Transmission	Yes	Global standard for 5G mobile networks.
Apache Kafka	Data Transmission/Data Processing	Yes	Stream processing for real-time data feeds.
OPC UA	Data Processing/Data Visualisation	Yes	Unified architecture for industrial IIoT data exchange.
CAN bus protocol	Data Processing	Yes	Communication standard for automotive and vending machines.
Modbus	Data Processing	Yes	Communication for industrial devices over serial/TCP/IP.
BACnet	Data Processing	Yes	Building automation and control networks protocol.
DNP3	Data Processing	Yes	Data communication in electric and water utilities.
IEC 61850	Data Processing	Yes	Communication standard for electrical substations.
ISA-88	Data Processing	Yes	Standard for batch control in industrial automation.
IEC 61131-3	Data Processing	Yes	Programming languages standard in industrial automation.
RFID UHF	Data Ingestion	Yes	Long range, high frequency RFID technology.

Continued on next page

Table 1 – continued from previous page

Standard	Building block	Market adoption	Function
Zephyr Project	Data Ingestion	No	Open-source Realtime operation system for resource-constrained IIoT devices.
LoRaWAN	Data Transmission	Yes	Long-range, low-power wireless protocol for IoT.
Sigfox	Data Transmission	No	Low-power, wide-area network for IoT.
EPCIS	Data Processing	Yes	Standard for sharing RFID data in the supply chain.
UPnP	Data Processing	No	Network protocol for automatic device communication without manual configuration.
Ignition	Data Utilisation	Yes	Industrial automation platform for visualising and managing data.
GE Predix	Data Utilisation	No	IIoT platform designed to analyse data from industrial machines.
FDT/DTM	Data Processing	Yes	Device integration in automation systems.
DLMS/COSEM	Data Processing	Yes	Standard for smart meter data exchange.
JSON	Data Processing	Yes	Lightweight format for easy data exchange.
ISA-106	Data Processing	No	Standard for procedural automation in process industries.
SML	Data Processing	No	Middleware services standard in industrial automation.
ISO 10303	Data Processing	Yes	Standard for exchanging product model data.
OPC Classic	Data Processing/Data Visualisation	Yes	Original standard for industrial communication.
EdgeX Foundry	Data Processing	No	Open-source platform for edge computing in IoT.
OPAF	Data Processing	No	Standard for interoperable process automation.
HyperCat	Data Processing/Data Visualisation	No	IoT data discovery and interoperability standard.
VDMA 24582	Data Processing	No	Machine-readable data exchange standard in industry.
XML	Data Transmission to Data Processing	No	Markup language for data exchange.
OPC	Data Transmission to Data Processing	No	Communication protocol for data exchange.
EPCIS	Data Processing/Data Transmission	Yes	Standard for sharing RFID data in the supply chain.

Continued on next page

Table 1 – continued from previous page

Standard	Building block	Market adoption	Function
ISA-95	Data Processing/Data Transmission	Yes	XML-based standard for enterprise-control information exchange.
TAPPI T1	Data Transmission	No	Standard for IIoT applications in the paper industry.
DDS	Data Transmission	Yes	Real-time data distribution in distributed systems.
XMPP	Data Transmission	No	Communication for message-oriented middleware.
HTTPS	Data Transmission	Yes	Secure protocol for web data transmission.
RESTful APIs	Data Transmission	Yes	Standard for web services and APIs.
ISA-18.2	Data Processing	Yes	Alarm management standard in industrial automation.
GSI	Data Transmission	Yes	Standards for barcodes, RFID, and supply chain data exchange.
OPCUA over TSN	Data Transmission	No	Real-time communication combining OPC UA and TSN.
EPCIS	Data Processing/Data Transmission	No	Standard for sharing RFID and sensor data.
ISO/IEC 18092	Data Transmission	Yes	NFC standard for industrial and supply chain applications.
IEC 62443	Data Security	Yes	Security standards for industrial automation systems.
ISA-99	Data Security	Yes	Cybersecurity standard for industrial control systems.
ISO/IEC 27001	Data Security	Yes	Standard for information security management.
ISO 28000	Data Security	Yes	Security management standard for the supply chain.
ISO/IEC 29167	Data Security	Yes	Cryptographic protection in RFID systems.
IEC 61508	Data Security	Yes	Functional safety standard for electrical systems.
OPC UA TSN	Data Transmission	Yes	Real-time data transmission for industrial automation.

Appendix B
Interview questions

Stakeholder identification and search direction

1. Production chain
Who are the main suppliers and partners involved in the production and distribution of the standard?
Identifying key contributors

2. End-users and related organisations
Who are the primary end users of the standard, and how do they interact with it?
Evaluating end-users' influence and their direct experience with the standard.

What support services or organisations assist end users effectively?
Understanding the ecosystem supporting standard implementation.

3. Designers
Who is responsible for designing and developing your product or system?
Recognising stakeholders who shape technical features and implementation.

Do external designers or consultants contribute significantly to the product's development?
Assessing the role of external expertise in the design phase.

4. Physical system
What existing technical systems or infrastructures does the standard integrate with?
Examining interoperability dependencies.

Who are the developers of the systems that the standard interacts with or depends upon?
Identifying key technical stakeholders influencing integration.

5. Inspection agencies
Which organisations conduct inspections, testing, or certification of the standard?
Identifying certification bodies that validate the standard.

What industry standards or certifications must the standard adhere to?
Assessing external pressures on standard conformity.

6. Regulators What government agencies or regulatory bodies oversee the industry?
Understanding the formal authorities impacting the standard.

How do current laws and regulations impact development?
Assessing the regulatory framework affecting decision-making.

7. Research and consultancy
Are any universities or research institutions involved in research related to the standard?
Testing the influence of academic research on development.

How do consultants influence the development or implementation of your product?
Evaluating consultancy influence on shaping the standard.

8. Education What educational institutions offer training or courses related to the standard and industry?
Understanding how education supports knowledge transfer and skills.

9. Representative organisations
What industry associations or trade groups are associated with the standard?
Clarifying the role of formal representative bodies in shaping standards.

Do consumer advocacy groups or unions influence the perception of the standard in any way?
Understanding public pressure and representation.

Stakeholder power
Which stakeholders have the most influence over the standardisation decisions?
Power assessment: Directly identifying the most impactful players in decision-making.

What resources (e.g., financial, technical expertise, market access) do these stakeholders control that give them power?
Resource assessment: Mapping the resource control that fuels stakeholder power.

Can you provide examples of how this influence has manifested in the standardisation process?
Power validation: Understanding real-world examples of influence.

Stakeholder legitimacy
Which stakeholders are considered legitimate participants in the standardisation process?
Legitimacy assessment: Determining key actors who are widely recognised as valid participants.

What factors contribute to their legitimacy (e.g., regulatory authority, industry reputation, community support)?
Legitimacy drivers: Identifying what confers legitimacy upon these stakeholders.

How is this legitimacy recognised or challenged by other stakeholders?
Interaction dynamics: Assessing how legitimacy is contested or affirmed.

Stakeholder urgency
Which stakeholders are pushing for immediate action or decisions in the standardisation process?
Urgency assessment: Identifying stakeholders who prioritise rapid progress.

What are the reasons for their urgency (e.g., market competition, regulatory deadlines, technological advancements)?
Motivational analysis: Understanding why stakeholders feel urgency.

How does this urgency impact the decision-making process?
Process influence: Gauging how urgency affects timelines and outcomes.

Interaction dynamics
How do the interactions between stakeholders with different levels of power, legitimacy, and urgency affect the standardisation outcomes?
Power-legitimacy-urgency interaction: Exploring how dynamics shape the final standard.

Can you describe any conflicts or collaborations that have occurred due to these dynamics?
Conflict/collaboration analysis: Identifying areas of stakeholder friction or alignment.

How are these interactions managed or mediated within the standardisation process?
Governance and mediation: Evaluating mechanisms for managing stakeholder interactions.

Influence on outcomes
How do you think the characteristics of these stakeholders (power, legitimacy, urgency) influence the success or failure of the standardisation efforts?
Outcome assessment: Understanding how stakeholder characteristics correlate with outcomes.

Are there any patterns or trends you've observed in how these characteristics shape the standardisation outcomes?
Pattern identification: Exploring recurring factors affecting standardisation success.

What lessons can be drawn from these cases that might apply to future standardisation efforts?
Future implications: Extracting actionable insights for future projects.

External influence
How do external factors (e.g., government policies, market trends, technological advancements) influence the power, legitimacy, or urgency of the stakeholders?
External context: Assessing how outside forces reshape stakeholder dynamics.

Have any external agents played a role in shifting the balance of power or urgency among stakeholders?
Power-shift assessment: Understanding external interventions in the process.

Future implications
What changes do you foresee in the stakeholder landscape for future standardisation efforts?
Trend forecasting: Anticipating changes in stakeholder involvement and influence.

How might these changes impact the standardisation process and outcomes?
Impact prediction: Exploring future outcomes based on changing stakeholder dynamics.

Closing questions
Is there anything else you would like to add regarding the role of stakeholders in the standardisation process?
Final insights: Allowing space for additional, unaddressed reflections.

Would you be willing to provide any documentation or additional contacts that might help deepen the understanding of stakeholder dynamics in this context?
Resource identification: Requesting additional materials for further exploration.