Intellectual Property Strategy Transformation for Digital Retrofitting of Industrial Products

Master's Thesis in Management & Economics of Innovation

Sebastian Andersson & Gustav Elm

DEPARTMENT OF TECHNOLOGY MANAGEMENT AND ECONOMICS
DIVISION OF ENTREPRENEURSHIP AND STRATEGY

CHALMERS UNIVERSITY OF TECHNOLOGY
Gothenburg, Sweden 2026
www.chalmers.se

Master's Thesis 2026

Intellectual Property Strategy Transformation for Digital Retrofitting of Industrial Products

SEBASTIAN ANDERSSON
GUSTAV ELM

CHALMERS
UNIVERSITY OF TECHNOLOGY

Department of Technology Management and Economics
Division of Entrepreneurship and Strategy
Chalmers University of Technology
Gothenburg, Sweden 2026

Intellectual Property Strategy Transformation for Digital Retrofitting of Industrial Products

SEBASTIAN ANDERSSON
GUSTAV ELM

Supervisor: Thomas Ewing, Chalmers University of Technology
Examiner: Marcus Holgersson, Chalmers University of Technology

Master's Thesis 2026
Department of Technology Management and Economics
Division of Entrepreneurship and Strategy
Chalmers University of Technology
SE-412 96 Gothenburg
Telephone: +46 31 772 1000

Typeset in LaTeX
Printed by Chalmers Reproservice
Gothenburg, Sweden 2026

Intellectual Property Strategy Transformation for Digital Retrofitting of Industrial Products
SEBASTIAN ANDERSSON
GUSTAV ELM
Department of Technology Management and Economics
Chalmers University of Technology

Abstract

This thesis investigates how an industrial company's intellectual property (IP) strategy transforms when a legacy physical product is digitally retrofitted and connected to digital ecosystems. Grounded in Industry 4.0, the Internet of Things (IoT), and servitization, the thesis provides an empirically grounded transformation map (gap analysis) of how value creation and appropriation shift from a pre-digital, artifact-centered era, where patents and design rights were primary, to a post-retrofitting context in which control over data, software, algorithms, interfaces, and relationships becomes increasingly essential. The thesis is based on an abductive exploratory case study in a European context. The empirical material consists of 29 semi-structured interviews with employees at the case company, across R&D, Strategy, Sales, and Law/IP.

The findings show that real-time access to product-generated data, together with insights derived from it, becomes a central asset. These capabilities enable new services such as predictive maintenance and support emerging business models based on subscriptions, leasing, and outcome-based agreements. At the same time, retrofitting introduces additional risks, particularly related to cybersecurity, brand reputation, and difficulty detecting digital IP intrusions. Traditional IP remains important as a foundational layer, signaling reliability and regulatory compliance. Meanwhile, new digital assets are increasingly complemented by trade secrecy, contractual agreements, and control over APIs, standards, and data access to manage new ecosystem dependencies and reduce the risk of disintermediation. The thesis also finds implications for a hybrid, layered IP strategy for digital retrofitting, in which formal IPRs and IP mechanisms jointly support appropriability across the physical and digital layers. Furthermore, it highlights the tension between regulatory demands for data sharing, such as those introduced by the Data Act, and the strategic need to maintain exclusivity. This tension underscores the importance of carefully designed contractual agreements, classification of trade secrets, and technical access controls to ensure appropriability and long-term competitiveness as new and established actors compete for control of the customer interface. The main changes between the pre- and post-digitalization eras of IP strategy are synthesized and summarized in an overview table, providing a structured representation of the thesis' key findings.

Keywords: Intellectual Property Strategy, Digital Retrofitting, Digital Ecosystems, Internet of Things (IoT), Servitization, Appropriability Regimes

Acknowledgements

We would like to thank the case company and its employees for the warm welcome and support throughout the course of this thesis. We truly felt part of your organization and appreciate the opportunity to study such an interesting topic in your industry.

We would also like to extend our appreciation to all interviewees who generously shared their time, insights, and experiences. Without your valuable contributions, we would not have been able to complete this thesis. A special thank you goes to our supervisor at the case company for your expertise, guidance, and encouragement - both in pushing us further and in reminding us when something was *good enough*.

We also wish to thank our examiner, Marcus Holgersson, and our supervisor, Thomas Ewing, at Chalmers University of Technology, for their engaging discussions and continuous support throughout the course of this thesis.

Finally, we would like to thank our family members and friends for their patience and support, and for enduring our many passionate discussions about IP strategy.

We hope you will enjoy reading this thesis
as much as we have enjoyed writing it.

Sebastian Andersson & Gustav Elm Gothenburg, June 24, 2026

List of Acronyms

Below is the list of acronyms that have been used throughout this thesis, listed in alphabetical order:

AI	Artificial Intelligence
API	Application Programming Interface
B2B	Business-to-Business
ERP	Enterprise Resource Planning
EU	European Union
FRAND	Fair, Reasonable, and Non-Discriminatory
FTO	Freedom To Operate
GDPR	General Data Protection Regulation
IP	Intellectual Property
IPR	Intellectual Property Rights
IoT	Internet of Things
KPI	Key Performance Indicator
NDA	Non-Disclosure Agreement
NCA	Non-Compete Agreement
PaaS	Product-as-a-Service
PSS	Product-Service System
R&D	Research and Development
WIPO	World Intellectual Property Organization

List of Key Definitions

Below is a list of the key definitions used in the thesis:

Appropriability Regime	An innovator's ability to capture profits from innovation is influenced by technological characteristics and the effectiveness of legal and non-legal protection mechanisms.
Complementary Assets	Assets needed to commercialize an innovation (e.g., manufacturing, marketing, service); categorized as generic, specialized, and co-specialized.
Digital Ecosystem	A set of firms linked by a shared digital technology to enable product or service innovation.
Digital Platform	A software-based infrastructure that enables the integration of services, data, and external actors, acting as a core mechanism for value creation and control in digital ecosystems.
Digital Retrofitting	Adding digital technologies (software, connectivity, IoT/data functions) to existing products to enable new functions and remote data access.
Hybrid IP Systems	A layered IP approach combining formal IPRs with other mechanisms (e.g., contracts, secrecy, lead time) to control value across physical and digital layers.
Intellectual Property	Intangible assets protected or controlled through rights (e.g., patents, trademarks) and other mechanisms (e.g., secrecy, contracts).
Intellectual Property Rights	Codified legal rights that assign/protect ownership of intellectual property, they are transferable/licensable, temporary, restricted, and not self-enforcing.
Internet of Things (IoT)	A network of connected physical devices with sensors and connectivity that collect and exchange data, enabling digital retrofitting and real-time insights.
Legacy Product	An older-generation product is still used or sold due to compatibility, cost, regulation, or customer dependence.
Servitization	Shifting from product sales to product-service offerings and outcome-based models enabled by connectivity and data.

Contents

List of Figures

List of Tables

1
Introduction

This chapter introduces the background to the research, what earlier research has suggested, and what will be investigated, along with an overview of the thesis outline. Further, the project's delimitations and scope are presented to provide a deeper understanding of the context in which the thesis operates.

1.1 Background

Industry 4.0 is reshaping the competitive landscape. Being part of the digital world is becoming a necessity for remaining competitive, creating challenges for industrial firms specialized in tangible products (Verhoef et al., 2021). Digital enablers such as the Internet of Things (IoT), Big Data, Artificial Intelligence, and the growing adoption of Anything-as-a-Service provide new ways of conducting business (Cardona & Serrano, 2023).

One of the central aspects of industrial firms transforming into the digital world is *retrofitting*, in which legacy physical products are complemented by digital enablers such as IoT devices (Paolone et al., 2022). These IoT devices enable continuous data gathering, new service offerings, and integration into digital ecosystems. Retrofitting not only creates new functionalities and business opportunities but also challenges and evolves the existing IP environment for companies. As data, software, and other digital resources are used in an industrial firm, the management of these intellectual properties needs to be taken into consideration as well.

Simultaneously, IP accounts for an increasing share of firms' assets, underscoring its growing strategic importance (Holgersson & Granstrand, 2018). As firms are increasingly valued for their intangible assets and IP (Almeling, 2012), industrial companies undergoing digital transformation must adapt their IP strategies to manage new forms of IP that differ from traditional, product-focused IP (Holgersson & Granstrand, 2018).

1.2 Prior Research

The foundation of this research is built on four main themes, which form the basis of the literature: i) IP Strategy and Appropriability, ii) Digital Transformation and Servitization, iii) IP in the Digital Environment, and iv) Digital Ecosystems and

Platforms.

The importance and value of IP have increased over the years (Almeling, 2012; Holgersson & Granstrand, 2018). IP plays an increasingly important role in sustaining companies' competitive advantages over time (Holgersson & Granstrand, 2018), and should therefore be understood as more than a legal appropriation mechanism. Instead, IP constitutes a strategic resource that affects a company's ability to create, protect, and capture value from innovation. This implies that a company's IP portfolio and IP strategy need to be integrated with and aligned to its overall business strategy and technological focus (Holgersson & Wallin, 2017), especially in digitalized and technologically complex industries where IP rights are distributed across multiple actors and technologies (Holgersson & Granstrand, 2018).

Research on appropriability has long emphasized the roles of complementary assets, first-mover advantages, and the strength of IP-based exclusion in capturing innovation profits (Teece, 1986, 2018). Firms can adopt patent strategies ranging from defensive to more aggressive approaches, implemented through rights, licensing, and enforcement (Somaya, 2012). Exclusion typically draws on a portfolio of IPRs, such as patents, design rights, and trademarks, as well as mechanisms such as secrecy, complexity, and lead time (B. Hall et al., 2014; Holgersson & Wallin, 2017). With digitalization elevating the importance of software and data, trade secrets are increasingly used to protect innovations that cannot, or should not, be disclosed through registrable IPRs (Almeling, 2012; Ozcan et al., 2023).

Prior research on digital transformation highlights how data, IoT, and AI create new ways of conducting business and services (Kumar & Kumar, 2020; Verhoef et al., 2021; Xu et al., 2018). For B2B firms, the transition into outcome-based business models through digitally enhanced service innovation demands new capabilities (Kowalkowski et al., 2024; Oliva & Kallenberg, 2003; Tukker, 2004; Vandermerwe & Erixon, 2023). *Digital retrofitting*, which is the addition of sensors, connectivity, and computation to legacy physical products, opens up new opportunities through product-platform thinking (Gokhale et al., 2018; Halman et al., 2003; Paolone et al., 2022).

The transition to the digital environment emphasizes the importance of software offerings, and in digital contexts, firms often perceive patents as less effective due to costs, disclosure concerns, and enforcement difficulties, and therefore rely more on alternative mechanisms such as secrecy and lead time (B. Hall et al., 2014). Licensing agreements become a central means of reusing assets and participation through complementary actors and assets (B. Hall et al., 2014; Voss et al., 2017; Zimmerman, 2015). Data and algorithms are often best protected through secrecy, contracts, and cybersecurity, while some jurisdiction also provides opportunities for database rights (B. Hall et al., 2014; Ozcan et al., 2023). Access and sharing of data are further regulated by directives, acts, and legal measures in the European Union, such as the Data Act, creating tension between data governance and IP boundaries (Lazarotto, 2024; Mylly, 2024).

Retrofitting physical products creates new types of value, but even greater value can be achieved when the product operates within a digital ecosystem (Bresciani et al., 2021). A digital ecosystem entangles multiple actors who co-create value by contributing complementary assets such as apps, cloud solutions, and additional services through platforms. Platforms, following, require orchestration, roles, and rules of participation to ensure mutual benefits and value (Bresciani et al., 2021; Cusumano et al., 2019; Koch et al., 2022; Valdez-De-Leon, 2019). The integration into an ecosystem also broadens the industry in which the firm operates, creating new opportunities but also attracting new kinds of competitors (Selander et al., 2013). Relationships and choices about relationships become essential (Baptista & Nunes, 2025; Holmlund & Törnroos, 1997), and IP strategy following needs to take into account the degree of openness the firm is willing to have towards other ecosystem actors, in which data sharing and contractual agreements become central (Asadullah et al., 2018; Ma et al., 2024; Oberländer et al., 2025).

1.3 Problem Statement

Industrial firms that retrofit legacy physical products with digital devices to participate in digital ecosystems shift from artifact-centric protection, where mechanical patents and design rights are central, to a broader portfolio including software, data, algorithms, interfaces, and platform contracts. While prior research clarifies appropriability and complementary assets (Somaya, 2012; Teece, 1986, 2018) and maps IP protection choices (B. Hall et al., 2014; Holgersson & Wallin, 2017), it offers limited guidance on how retrofitting specifically reshapes these dynamics. In particular, retrofitting can alter the role of existing IP, such as legacy patents and know-how, by turning them into complements for digital control, safety, and compliance functions. At the same time, it introduces new forms of IP and value-creation mechanisms, including software copyrights and patents, trade secrets for algorithms and data-processing models, and database or contractual rights governing data. Moreover, retrofitting transforms ecosystem interdependencies and governance structures, influencing decisions about interface openness, licensing arrangements, data-sharing practices, and participation terms. Finally, it necessitates a reconsideration of the alignment between IP and business models, as firms increasingly shift toward subscription-based, outcome-based, or platform-oriented revenue logics (Cusumano et al., 2019; Kowalkowski et al., 2024; Valdez-De-Leon, 2019).

To summarize, there is a lack of an actionable, empirically grounded understanding of IP strategy adaptation when legacy industrial products are digitally retrofitted for ecosystem participation. Following this, this thesis contributes by providing an empirically grounded gap analysis of how IP strategy transforms during the transition from a pre-digital to a digitally retrofitted context. Specifically, the thesis analyzes: i) what new IP emerges, ii) how the role of existing IP changes, iii) how participation in digital ecosystems reshapes IP strategy, and iv) how IP strategy needs to align with evolving business models.

1.4 Research Aim

This thesis aims to analyze how digital retrofitting for participation in digital ecosystems reshapes the role of IP strategies in legacy product industries.

1.5 Research Questions

Main Research Question: *How does a firm's intellectual property strategy change when a legacy product is retrofitted to digital ecosystems?*

Research Question 1: *What new intellectual property emerges with the introduction of digital functionalities?*

Aims at mapping which new kinds of intellectual property emerge, how to control them, and what kind of value they bring.

Research Question 2: *How does digital retrofitting change the role of existing IP?*

This question aims to understand the role of IP, which was central during the electromechanical era, and how it is affected by the retrofitting.

Research Question 3: *How do evolving ecosystem interdependencies influence intellectual property strategy?*

This question will provide insights into how relationships and dependencies evolve as a result of digitalization, and what this implies for the IP strategy.

Research Question 4: *How does digital retrofitting drive firms to reconsider the relationship between their IP strategy and their business model?*

The questions focus on how digitalization enables new business models and how they affect IP strategy, particularly regarding what is important to control and protect.

1.6 Scope & Delimitations

i) To ensure feasibility and analytical focus, this thesis is limited to a single industrial firm and a specific legacy product within the European context.

ii) The focus will be on IP and not only IPRs, which means that software, data, technical knowledge, and organizational capabilities will be included.

iii) The thesis will not include any technical testing or technical performance evaluations of the IoT solution.

iv) Legal analysis of specific legislation will be limited to a conceptual level and will be based on an EU jurisdiction standpoint.

v) There will only be internal perspectives from the studied company; external partners, suppliers, and competitors will not be analyzed empirically.

vi) The thesis focuses on the current phase of the retrofitting process and does not provide a longitudinal case thesis over time.

vii) The thesis applies established literature related to IP, digital transformation, servitization, and digital ecosystems; other theoretical perspectives, such as business modeling or technical system architecture, are not within the scope.

1.7 Thesis Outline

The thesis is structured into seven chapters, followed by references and an appendix. Chapter 1 introduces the background, research problem, aim, questions, and scope of the study. Chapter 2 presents the theoretical framework, covering intellectual property, appropriability, and the impact of digitalization, including concepts such as Industry 4.0, ecosystems, IoT, and servitization. Chapter 3 outlines the research design and qualitative methodology, including data collection, sampling, and trustworthiness. Chapter 4 presents the empirical findings from the collected data, while Chapter 5 analyzes these findings in relation to the theoretical framework. Chapter 6 summarizes the main conclusions, answers the research questions, and highlights key theoretical and practical implications. Finally, Chapter 7 discusses the contributions and limitations of the study and suggests directions for future research. The thesis concludes with a list of references and an appendix containing the interview guide.

2

Theoretical Framework

This chapter presents the main theory underpinning the thesis and its approach to answering the research questions. The theory provides insights into the basics, challenges, and opportunities of IP, as well as IP's business value perspective.

2.1 Intellectual Assets & Intellectual Property

This section explores the relationship among intangible assets, intellectual assets, and intellectual property, as well as their associated intellectual property rights.

2.1.1 Intangible Assets & Intellectual Assets

Intangible assets are the result of some kind of expenditure where the result is of a non-tangible nature (R. Hall, 1989). Among intangible assets are *intellectual assets*. Intellectual assets are "...assets whose essence is an idea or knowledge, and whose nature can be defined and recorded in some way" (R. Hall, 1989, p. 54). Examples of intellectual assets include a firm's reputation, knowledge, and an employee's skills, which are of value (R. Hall, 1989). Intellectual assets can be divided into two categories: i) *Intellectual Property* (R. Hall, 1989), also known as *Legal assets* (Tao et al., 2005), which are intellectual assets which can be owned, for example, patents and trademarks, and ii) *Knowledge assets*, where property rights can not be obtained, such as the skills of an employee or the reputation of a firm (R. Hall, 1989). However, knowledge could sometimes be protected through other mechanisms such as non-disclosure agreements and trade secrets (Tao et al., 2005). This makes the distinction between intellectual property and knowledge less absolute due to the overlap.

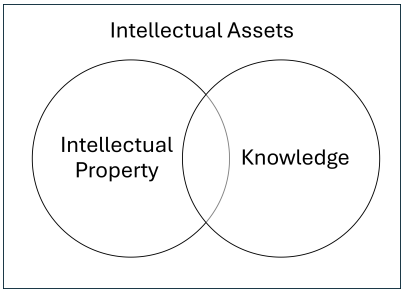

Figure 2.1: Visualization of the relationship between Intellectual Assets, Intellectual Property, and Knowledge.

Intellectual assets are generated, handled, and extracted across multiple functions within an organization, such as Technology and R&D, Product Development, and Legal (Tao et al., 2005). Although the way that the different functions use and are exposed to intellectual assets differs. For example, the R&D function both *creates* and *applies* legal assets such as patents, while also creating knowledge assets by codifying new inventions and capabilities among employees.

2.1.2 Intellectual Property

Property is a resource that could be provided ownership (Granstrand & Holgersson, 2015), and *intellectual property* is therefore, in its broad sense, property obtained as a result of an intellectual activity (World Intellectual Property Organization, 2004). Intellectual property consists of rights related to a wide scope of intangible assets. Some forms of intellectual property require registration to obtain exclusive rights for a limited period, such as patents, trademarks, and design rights (B. Hall et al., 2014). All intellectual property is also an intellectual asset, but not all intellectual assets are intellectual property.

There are other ways to protect and/or control IP (B. Hall et al., 2014). These mechanisms include secrecy, lead times, contractual agreements, confidentiality, and complexity. Although intellectual property is largely associated with patents, the literature review by B. Hall et al. (2014) indicates that companies often rely more on other forms of protection. Holgersson and Wallin (2017) also adds that other means of appropriation are often considered more effective than patenting. Instead, trade secrets, learning costs, lead time, switching costs, and cost reductions are considered more commonly used mechanisms (B. Hall et al., 2014; Holgersson & Wallin, 2017).

2.1.3 Intellectual Property Theft

IP theft is one of the many forms of cybercrime committed daily (Blaskovic et al., 2023). IP theft is not only the theft of technological writings, but also the theft of creators' thoughts and ideas. There are four types of IP theft: copyright infringement, trademark infringement, trade secret theft, and patent infringement (Blaskovic et al., 2023). When IP theft affects corporations, they may lose significant revenue and suffer brand damage, while creators also lose potential income (Almeling, 2012; Blaskovic et al., 2023). McAfee, a computer security firm, estimated that data leakage caused costs for over $9 trillion globally in 2008 (Almeling, 2012).

According to Blaskovic et al. (2023), one of the most important steps when IP theft is suspected is to determine who has access to the IP. This is especially important when the company is dealing with external actors; in such cases, the organization should also identify which of these actors could benefit from the information. When theft occurs, it is unlikely that the perpetrator seeks immediate financial gain; rather, the motivation is often future profit, as the stolen information may be used to replicate and develop their own resources. However, the motivations may differ depending on whether the perpetrator is an individual or a firm.

2.2 Intellectual Property Rights

This section introduces the main types of intellectual property rights (IPRs). IPRs are codified legal rights that assign and protect the ownership of intellectual assets (Granstrand & Holgersson, 2015). All IPRs are licensable or transferable, and restricted rights over an intellectual asset, thereby excluding others from commercializing the specific asset (Granstrand & Holgersson, 2015). They are also temporary, except for trade secrets and trademarks. Furthermore, the requirements for protection include the novelty and uniqueness of the assets. However, IPRs are not self-enforcing, meaning that the owner must initiate legal action to enforce these rights.

2.2.1 Patents

Patents are legal barriers of imitation of an invention (Somaya, 2012). An invention is a "solution to a specific problem in the field of technology. An invention may relate to a product or a process." (World Intellectual Property Organization, 2004, p. 17). In general, patents are most effective for product-oriented inventions (Holgersson & Wallin, 2017), and considered ineffective for process-oriented inventions (Teece, 1986). According to B. Hall et al. (2014), process patents are too easy to invent around and reveal too much information to competitors. The term of patents is commonly 20 years from the filing date and applies only to the jurisdictions where it is filed. A common misinterpretation of patents is that they grant rights to manufacture and sell the patented invention (Holgersson & Wallin, 2017; World Intellectual Property Organization, 2004). In reality, patents grant exclusive rights to exclude others from making and selling the invention, thereby preventing imitation (Holgersson & Wallin, 2017).

An invention needs to fulfill three prerequisites in order to be patentable (Somaya, 2012): i) the invention needs to be *novel*, i.e., new to the world (Granstrand & Holgersson, 2015), ii) the invention needs to be *non-obvious to a skilled person* within the technological field, and iii) it needs to be *useful*. When a patent is granted, the invention, how to use it, and how to make it, must be disclosed publicly with the purpose of increasing the invention within the field (Voss et al., 2017). Because patents require disclosure of an invention, it may be easier for others to design around the patent and develop alternative solutions (Teece, 1986).

Industry-specific conditions might also affect the applicability of patenting an innovation (B. Hall et al., 2014). For example, in the biotech industry, where R&D costs are substantial, and patents are highly inimitable, patenting becomes almost a necessity rather than an option to ensure a return on investment. On the other hand, the software industry is an environment where patents are considered less effective means of protecting innovations, as these innovations are easy to invent around.

The term *software patent* is used as an abbreviation for patents on inventions that are partly or largely in software; however, it is not a distinct legal category of patent

(Laub, 2006). In Europe, the expression *computer-implemented inventions* is used to cover claims involving computers, computer networks, or other programmable objects in which one or more features are implemented by software (European Patent Office, 2025). To be patentable, the invention must solve a technical problem and produce a technical solution beyond standard data processing.

2.2.2 Copyrights

Copyright provides automatic protection for creators' works, including books, music, and other intellectual creations (World Intellectual Property Organization, 2004). As soon as something is written, drawn, or saved on a computer, it is subject to a certain level of copyright protection (B. Hall et al., 2014), meaning that it is an unregistered right. This further means that copyright can be used not only for published works but also for works that are kept secret. Copyright can be used to prevent copying of works such as programs, music, artwork, or documents, including reproducing parts of them (Voss et al., 2017). Although *ideas* are not eligible for copyright protection, the *expression* of an idea is. Following, copyrights do not protect solutions based on the same functionality or idea and are therefore often combined with other protection mechanisms, such as patents, contracts, or secrecy (Zimmerman, 2015). There are three basic requirements for copyright protection: i) it must be a work of authorship, ii) it must be the original, and iii) it must be fixed in a tangible medium of expression (Zimmerman, 2015).

The duration of copyright protection typically ranges from 50 to 100 years after the creator's death (Granstrand & Holgersson, 2015). Additionally, there is no fee or requirement to maintain copyright protection (Voss et al., 2017). Ownership of copyright is typically with the creator, although contractual agreements can be made to transfer it (Zimmerman, 2015). If there is a single author, that person owns the copyright. When there are two or more owners, they are considered joint owners. Each has the power to exploit the work without the other owners' permission, unless they contract otherwise. Copyrights can be transferred only by an assignment in writing (Zimmerman, 2015).

If someone infringes on the copyrighted material, one can sue in court for copyright infringement. For a copyright infringement to be determined, a two-part rule is used: i) the owner needs to prove that the infringer had access to the content, ii) there must be substantial similarities between the owner's and the infringer's work.

2.2.3 Trademarks

A *trademark* is something distinct that could be in the form of a logotype, pattern, color, sounds, etc., which directly associates the given product or service with a single firm, and thereby acts as an indicator of origin (World Intellectual Property Organization, n.d.-b). Trademarks also work as an indication of quality and an advertising tool (World Intellectual Property Organization, 2004). To be eligible for trademark protection, what is to be protected must be distinctive, meaning that it

is not something generic.

Trademark registration is conducted at the regional level, although the World Intellectual Property Organization (WIPO) maintains the Madrid System, which forwards trademark applications to national offices in over 130 countries and, if the requirements are met, allows the trademark to be filed (World Intellectual Property Organization, n.d.-a). Trademark protection remains mainly for ten years (World Intellectual Property Organization, n.d.-b), but can be kept as long as it is kept in use and registration is renewed (World Intellectual Property Organization, 2004).

2.2.4 Trade Secrets

Trade secrets are confidential technical or commercial information that provides an advantage to the owner since it is not generally known or easily acquired (World Intellectual Property Organization, 2004). Trade secrets include both *industrial secrets*, such as production methods, manuals, prototypes, and *commercial secrets*, including contractual models, pricing information, customer profiles, sales and distribution channels, marketing strategies, and lists of suppliers and customers. It is important to distinguish between trade secrets as a legal right and secrecy as a managerial practice: while the former can be legally enforced under certain conditions, the latter refers to organizational efforts to maintain confidentiality. To qualify as a trade secret, the information needs to be i) known by a limited number of persons, ii) the owner must have an interest in the information to be kept secret, and iii) reasonable efforts have been made to keep the information secret. The definition of trade secrets is broad, such that they apply even to inventions for which patents are unavailable due to a lack of novelty or an inventive step (B. Hall et al., 2014). Due to the secretive nature of trade secrets, there is no reliable way to measure them. However, reports by Almeling (2012) and B. Hall et al. (2014), among others, highlight an increase in litigation concerning trade secret misappropriation. To successfully bring a claim for trade secret misappropriation, the owner must demonstrate that the information has value and that reasonable steps have been taken to protect it. Although trade secrets can be difficult and costly to enforce in court (B. Hall et al., 2014), they are sometimes considered a more cost-effective alternative to patents.

A trade secret is protected only as long as it remains secret and therefore cannot be disclosed publicly (Granstrand & Holgersson, 2015; Holgersson & Wallin, 2017). On the other hand, trade secrets can therefore be held indefinitely. An important aspect to consider is that a product that withholds a trade secret can easily be accessed once launched on the open market, whereby trade secrets are mostly seen as suitable for environments without external accessibility (Arundel, 2001).

Almeling (2012) argues that there are several reasons to the increase of both the importance of trade secrecy and the increase in litigations: i) The culture of being at the same workplace for an entire work life is changing, employees are nowadays frequently changing employer and thus takes, both intentionally and unintentionally, trade secrets from their former employee and use them at their new employer,

and ii) The digital era changes the way trade secrets are stored and how they can be accessed. As Almeling (2012) exemplifies, before the digital era, trade secrets were protected behind doors and locks, now they are stored on the company's file system in the cloud, making them easier to access and easier to transfer outside of the organization, iii) Intrusions into IT-systems are increasing, hackers try on a daily basis to gain access into companies' IT-environment to take possession of intellectual assets such as trade secrets.

Trade Secrets can, in some cases, for example when embedded in processes, be seen as an alternative to a patent (Teece, 1986). An example of this is manufacturing processes, which, due to their protected environment within the manufacturing facility, can often be kept secret from competitors for longer (Arundel, 2001). The choice between a patent and secrecy often depends on the negative impact that disclosure would have (B. Hall et al., 2014). For more factors that affect the choice between patenting or leveraging secrecy, see Table 2.1. Leveraging trade secrets is often seen as a mutually exclusive alternative to using patenting for IPR protection (Arundel, 2001; B. Hall et al., 2014; Holgersson & Wallin, 2017).

Table 2.1: Factors Affecting the Patent-Secrecy Choice, from B. Hall et al. (2014, p. 390). Modified.

Factor	**Patents**	**Secrecy**
Disclosure (codifiable knowledge)	Yes	No
Ease of delimiting invention	Yes	Not clear
Reverse engineering allowed in general	No	Yes
Subject matter	Limited	Broader
Timing	After invention	Work-in-progress
Process versus product	Both	Easier for process
Length	Twenty years	Longer (potentially)
Cost to obtain	Higher	Nonzero
Enforcement cost	Expensive	Expensive (potentially)

The use of trade secrets is exceeding patents (B. Hall et al., 2014; Ozcan et al., 2023). One reason trade secrets have grown in popularity is the lower financial costs compared to patents (Ozcan et al., 2023), as patents require application and renewal fees. Meanwhile, a trade secret requires whatever means are needed to keep it secret, ranging from contractual agreements to internal HR training on maintaining trade secret confidentiality. B. Hall et al. (2014), on the other hand, argues that trade secrets can be expensive to manage due to confidentiality agreements and ongoing internal knowledge management, such as secrecy policies. Another way to reduce access to internal trade secrets is to divide R&D tasks into smaller segments, with each department responsible for one, thereby reducing employees' understanding of the complete technology, product, or innovation. Among the largest weaknesses among policymakers and managers in trade secret protection are cybersecurity, low levels of business awareness, and limited identification of valuable trade secrets (Ozcan et al., 2023).

Ozcan et al. (2023) emphasizes the importance of the organization's maturity in understanding trade secrets, noting that mandatory, continuous learning provides employees with exposure to trade secrets and reinforces the need to handle them appropriately. At the same time, maintaining trust in employees has been shown to be an important factor in reducing the risk that employees, both intentionally and unintentionally, share trade secrets when transferring to a new employer.

For legal approaches, trade secrets can be controlled and protected through non-disclosure agreements (NDA), confidentiality clauses in employee contracts, and noncompete agreements (NCA) (Ozcan et al., 2023). An NCA reduces the employee's mobility, thereby reducing the risk of trade secrets being taken to other firms. The NCA comes with a cost: additional compensation and salary increases. For offensive organizational approaches to control and protect trade secrets, continuous re-evaluation of permissions to access resources, such as databases, and to sensitive areas, such as laboratories, is needed (Ozcan et al., 2023). Ozcan further emphasizes that this re-evaluation is of particular importance in companies where knowledge is in dynamic change.

2.2.5 Design Rights

Design rights protect the appearance and shape of a product, but not its technical function or the underlying idea (World Intellectual Property Organization, 2004). Design right protection needs to be applied for at a national or regional level, and is initially granted for a period of five years from the filing date. Although it can then be renewed in five-year periods up to a maximum of 25 years (European Union Intellectual Property Office, 2025).

For a design to be protected, it must be novel, meaning that no identical design has previously been made available to the public (European Union Intellectual Property Office, 2025). The design must also possess some individual character, meaning that the overall impression can not be simple or generic.

2.2.6 Database Rights

Database rights are an intellectual property right (Granstrand & Holgersson, 2015) that consists of two mechanisms: *copyright* and the *sui generis right* (European Union, 2025). Copyright protects the structure of the database, provided it is an intellectual creation. The *sui generis* right protects the content of the database, given that efforts have been made to collect, verify, or present the data. The *sui generis* right gives the creator the right to prevent reutilization of parts or the whole of the database for a period of 15 years from the creation date.

2.3 Digitalization & Regulatory Environment

Digitalization of industrial products introduces data access and sharing as key strategic implications. Simultaneously, EU regulations affect how data can be used and shared. In this section, the Data Act and its relation to contracts, responsibilities, and information protection are introduced, which is important for competition, especially regarding trade secrets.

2.3.1 The Data Act

The Data Act has been the last proposed Act of the European Data Strategy (Lazarotto, 2024). The main objective of the Data Act is to enhance the EU's data economy and foster a competitive data market by making data more accessible and usable by introducing mandatory business-to-business data-sharing contracts, as it clarifies who can use what data under which conditions (European Commission, 2025).

In practice, this means that the Data Act requires users of connected products to be able to access product-related data and related service data in an *easy* and *safe* way, and in some circumstances requires the data to be shared with a third party (The European Parliament, 2023). For manufacturers of connected products and services, this indicates a requirement to design data access by design, while also specifying access, how it may be used, and responsibilities through contractual agreements. This creates tension between value capture through data and insights (Mylly, 2024) and the requirements for data access, thereby increasing the importance of contracts, secrecy classifications, and a clear distinction between raw data and the insights generated from it.

The scope of the act includes *manufacturers of the products* and *suppliers of related services*, but with the exception of excluding IoT product providers or similar services that qualify as micro or small enterprises (Lazarotto, 2024). Furthermore, the Act covers any type of connected object that contains sensors enabling it to collect, generate, and communicate data over the internet, but excludes products designed to display, record, or transmit content. The Data Act covers a broad spectrum of data, including both personal and non-personal data. The right to data portability is free of charge for the user exercising it; however, in a business-to-business context, reasonable compensation may be required. This concept is also essential for data protection. Lastly, the original Data Act aims to achieve a balanced data market by excluding gatekeepers from receiving data.

2.3.2 The Data Act & Trade Secrets

The purpose of the Data Act, as mentioned, is to facilitate the sharing and access of information (Mylly, 2024). Meanwhile, data-sharing incentives raise new concerns for companies that rely on data as part of their competitive advantage, where access to the data requires exclusivity to be considered a trade secret. Being obliged

to share the data following decreases exclusivity, and the requirement of not being known to the public is reduced by each person who gets access to the information. However, not all kinds of data qualify as trade secrets; Mylly (2024) exemplifies *raw data* that normally fall into this category. Meanwhile, data that qualifies as trade secrets can, under exceptional circumstances, be denied access.

Following on the ability to deny access to data, the scope of the data-sharing is regulated by the Data Act, as defined by Recital 15 (The European Parliament, 2023):

> "[...] Data which are not substantially modified, meaning data in raw form, also known as source or primary data, which refer to data points that are automatically generated without any further form of processing [...]"

Additionally, Recital 15 further clarifies which information is not regulated by the Data Act (The European Parliament, 2023):

> "[...] By contrast, information inferred or derived from such data, which is the outcome of additional investments into assigning values or insights from the data, in particular by means of proprietary, complex algorithms, including those that are a part of proprietary software, should not be considered to fall within the scope of this Regulation and consequently should not be subject to the obligation of a data holder to make it available to a user or a data recipient, unless otherwise agreed between the user and the data holder."

From these clarifications, it is clear that insights derived from processing raw data do not fall under the Data Act (Mylly, 2024). On the other hand, providing access to the raw data is sufficient to raise concerns for the data holder, even if it does not constitute a trade secret. In the same way the data holder might analyze the data to generate insights, others with access to the data could potentially reach the same insights. Following Mylly (2024) suggests that the distinction between trade secrets as a result of data processing and the raw data per se is not as obvious as the definition from Recital 15 might indicate.

If the data had to be shared with such a limited number of persons within the industry to still meet the requirement of not being known to the public, the need to make reasonable efforts to keep the information secret would need to be considered. Mylly (2024) exemplifies this by using contractual agreements to further restrict access to data and confidentiality obligations, especially when data is shared over data networks. Trade secret protection is also said to be highly uncertain, as long data chains are difficult to control, and the risk of confidentiality breaches and access restrictions may be difficult to manage and monitor.

Mylly (2024, p. 384) further emphasizes that the Data Act "takes away a trade secret holder's decision-making power over the authorization of access to its information" and following dilutes the competitive advantage the trade secret withholds. Further, the ability to choose whom to share the data with is one of the main factors for successful and trusted collaborations, a factor that diminishes when the data holder

no longer has this decision-making power. On the other hand, Arts. 4(10) and 6(2)(e) explicitly states that the data derived from the data holder is not to be used for purposes or shared in a way that may compete with the product of the data holder from which the data is extracted.

2.4 IP Strategy

IP strategy refers to the strategic choices firms make regarding intellectual property and intellectual property rights (van Santen & Holgersson, 2026). It extends beyond patenting to encompass how firms create and acquire IP, as well as how they govern, control, and exploit it in order to both protect and share innovations. An IP strategy should therefore be aligned with the business, technological, and corporate strategies to enhance the value and potential of technologies (Holgersson & Wallin, 2017). Having an IP strategy is especially important when industries converge towards more complex technological environments (Holgersson & Granstrand, 2018).

2.4.1 Patent Strategy

Somaya (2012) argues that patents should be viewed not only as legal rights but also as strategic tools that firms actively manage to create and capture value. Patents function as isolating mechanisms that help companies protect technical knowledge and secure appropriability from innovation. Conversely, patents are described as imperfect and uncertain because their scope and enforceability are often unclear until tested in litigation. Somaya (2012) further organizes patent strategy into three main domains: *rights*, which concerns acquiring and maintaining patents, *licensing* regarding sharing/commercializing the patented technology through licensing arrangements, and *enforcement*, which is litigation or threats of litigation to stop infringement or obtain royalties. These together shape how firms capture value from innovations and defend their technological positions in the market. Grzegorczyk and Gowiski (2020) similarly argues that IP management should be integrated with broader corporate strategies, since patents not only contribute to legal protection but also to technological positioning and sustainable competitive advantage.

A central theme in Somaya (2012) is the three generic patent strategies: proprietary, defensive, and leveraging strategies. The proprietary strategy is rooted in the resource-based view and focuses on using patents to create barriers to imitation. The firms that are adopting this strategy seek exclusive control over important technologies by building strong patent portfolios and fences. Proprietary strategies could be particularly important for technologies that are central to a firm's long-term competitive advantage.

The defensive strategy seeks to preserve a firm's FTO in industries that are characterized by fragmented patent ownership (Somaya, 2012). In these industries, companies risk being sued or blocked by competitors that own complementary patents. As noted by Grzegorczyk and Gowiski (2020), a defensive strategy is to minimize constraints arising from third-party patent rights. Therefore, defensive strategies in-

clude building large patent portfolios, entering into cross-licensing agreements, and participating in patent pools to reduce litigation and strengthen bargaining power (Somaya, 2012). This strategy is especially common in industries where products often incorporate many interdependent innovations.

The leveraging strategy focuses on using patents to generate bargaining power and economic rents through negotiations, licensing, and legal pressure (Somaya, 2012). Companies may license technologies to competitors to negotiate favorable terms or use threats of litigation to obtain royalties. According to Grzegorczyk and Gowiski (2020), leveraging strategies do not necessarily require firms to patent every substitute technology, but rather to secure strategically important patents that are difficult for competitors to design around. This strategy has become increasingly common with the rise of patent trolls, firms that rely primarily on licensing revenues and litigation rather than manufacturing products (Somaya, 2012). In this context, patents are used not only to protect innovation but also as tools for extracting economic value.

2.4.2 Strategic Disclosure

As markets become more dynamic and more technically complex, the handling of IP has evolved from a primary juridical function to a strategic tool (Peters et al., 2013). Three central developments contribute to these new dynamics: i) the increased availability of information via the internet, ii) improved databases for prior art, and iii) changes in patent law (Peters et al., 2013). These changes have increased industry competitiveness and made it more difficult for companies to maintain their exclusive positions. Anton and Yao (2002) further argues that strategic disclosure can act as a signaling mechanism in markets where ideas are difficult to protect and contract over. In such settings, companies may intentionally disclose parts of their technological knowledge to attract partners or establish claims over technological space, even when disclosure risks imitation.

Strategic disclosure is defined as a conscious public disclosure of technical information to create prior art and prevent other actors from patenting or protecting the same or similar innovations (Peters et al., 2013). Companies, therefore, contribute to the knowledge base to limit competitors' room for action. Also, strategic disclosure contributes to freedom to operate (FTO), meaning companies can operate without infringing on competitors' IP. Strategic disclosure helps FTO to block competitors from patenting it and reduces the risk of legal enforcement. Lev (1992) further describes disclosure as a mechanism for competitive positioning and entry deterrence, in which firms strategically communicate information to influence competitors' market behavior and expectations. Strategic disclosure offers several advantages over traditional patenting. It has an immediate effect as prior art, reduces uncertainty in patenting processes, and also provides opportunities to anonymize strategic intentions (Peters et al., 2013). Another financial advantage is that strategic disclosure has lower costs than patents. It additionally provides global reach through a single publication and reduces legal and administrative costs. There are also some risks

with strategic disclosure, such as a missed opportunity to patent the innovation independently. Disclosure also reduces the ability to appropriate value from future innovations. Because it is relatively unused in organizations, they generally lack knowledge and routines about this approach. Strategic disclosure further demands a high degree of strategic awareness and coordination between departments.

2.4.3 Secrecy

Secrecy represents a strategic alternative to patenting inventions, where value can be appropriated directly as long as the information remains secret (Holgersson & Wallin, 2017). In this sense, secrecy allows firms to retain exclusivity without the costs and disclosure requirements associated with patents. However, because secrecy does not constitute prior art, it does not give FTO protection, and firms risk competitors independently developing and patenting similar inventions, potentially restricting future commercialization opportunities.

From an IP strategy perspective, the choice between secrecy, patenting, and disclosure depends not only on the nature of the technology but also on the firm's ability to safeguard the underlying knowledge and the likelihood of imitation, leakage, or independent development (Holgersson & Wallin, 2017; Ozcan et al., 2023). Empirical evidence suggests that firms frequently rate secrecy as more effective than patents in protecting innovations, indicating that secrecy constitutes a central component in many firms' appropriation strategies, particularly where control over information can be maintained (Arundel, 2001).

Strategically, secrecy is often used to avoid the disadvantages associated with patenting, most notably the requirement to disclose the invention (Arundel, 2001). Such disclosure may reveal valuable information to competitors, enabling them to identify promising technological fields or develop alternative solutions (Arundel, 2001). Consequently, secrecy is particularly attractive in contexts where the risk of competitors designing around a patent is high or where the competitive advantage is closely tied to confidential knowledge.

At the same time, a secrecy-based IP strategy requires substantial organizational capabilities (Ozcan et al., 2023). Firms must actively manage and protect knowledge through a combination of technical, organizational, and human resource practices, including restricted access to sensitive information, controlled information flows, and employee training. For example, DalleMule and Davenport (2017) reports that 70% of employees typically have access to data they should not. This highlights that secrecy is not merely a passive protection mechanism, but rather an integrated strategic choice that must be embedded in the firm's overall innovation and IP management processes (Ozcan et al., 2023).

2.4.4 IP Modularity

IP modularity refers to designing a system such that the boundaries of technical modules align with different IP statuses, for example, open and proprietary components (Henkel et al., 2013). This allows firms to open certain parts of a platform to external actors for collaborative innovation, while protecting core components to ensure value capture. However, achieving IP modularity may require deviations from the technically optimal design, creating a trade-off between value creation and value capture. An example of IP modularity for digital platforms is shown in Figure 2.2a, where proprietary components (A) and open components (B) are entangled within the same module, leading to potential IP conflicts. In Figure 2.2b, the platform is designed in such a way that proprietary parts (A), such as core algorithms, are in an exclusive module where open components (B) are not present. Following this, external innovation is possible while key IP can be kept within the internal environment.

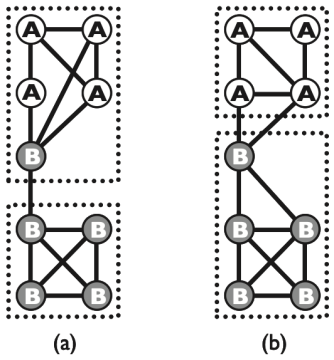

Figure 2.2: Comparison of a (a) Modular structure and an (b) IP-Modular structure, where A and B elements are under distinct IP status. From (Henkel et al., 2013, p. 69)

2.4.5 IP Disassembly

Granstrand and Holgersson (2013) develops the concept of the IP disassembly problem, which describes the challenges firms face when separating, transferring, or terminating interdependent IPRs in collaborative innovation projects, or open innovation projects. Modern innovation increasingly depends on multiple technologies, patent holders, and complex licensing relationships. Making IP management increasingly more difficult in technological industries. As technologies become more interconnected, firms must not only solve the problem of acquiring IPRs but also disentangle them when collaboration, projects, or ownership changes. Granstrand and Holgersson (2013) connects this to the tragedy of the anticommons, which describes the underuse caused by excessive fragmentation of exclusion rights across many actors. In innovation-intensive industries, fragmented ownership can create barriers to commercialization because companies must negotiate access to multiple complementary patents simultaneously, increasing costs, legal complexity, and interfirm dependence.

Granstrand and Holgersson (2014) distinguishes between background-, foreground-, sideground-, and postground knowledge. *Background knowledge* refers to technologies and IP provided before collaboration begins, while *foreground knowledge* is jointly created during the collaboration. *Sideground knowledge* refers to technologies developed independently outside the collaboration, and *postground knowledge* concerns the technologies developed after the collaboration ends. Granstrand and Holgersson (2014) further argues that effective IP management requires carefully designed contractual arrangements that regulate ownership, access, control, and future use of technologies. Licensing agreements, grant-back clauses, grant-forward clauses, and change-of-control clauses are important mechanisms for managing interdependencies between firms. These contractual tools help companies preserve FTO while also reducing risks associated with technological dependence and future disputes.

2.4.6 Patent strategy in Multi-Invention Context and Ecosystems

Somaya et al. (2011) extends patent strategy theory by examining innovation in a multi-invention context, in which products rely on numerous interconnected patents and technologies. In some industries, firms must combine inventions from multiple actors to create commercially viable products. This creates significant IP complexity because firms need access to complementary technologies and patent rights simultaneously. Therefore, most companies must align their organizational business model with their IP strategy. Chen and Lu (2019) further develops this perspective in the context of IoT. They argue that IoT industries operate within ecosystems characterized by multi-invention and multi-supply contexts, where value creation increasingly depends on cross-company and cross-technology collaboration. In these ecosystems, IP must support openness, interoperability, and ecosystem coordination rather than only the protection of individual firms. Emphasizing that the IP strategy must align with ecosystem dynamics, combine multiple forms of IP protection, and integrate with industry solutions.

2.5 Appropriability Regimes

An appropriability regime is the potential for an innovator to capture the profits from an innovation, which depends on a variety of factors (Teece, 1986). The most important factors are considered to be i) the nature of the technology itself, which sets the height of barriers to imitation, and includes the product, processes, the degree of tacit and codified knowledge (Ceccagnoli & Rothaermel, 2016), and ii) how efficient the legal mechanisms of protection are, including patents, copyrights, trade secrets, etc (Teece, 1986). Gemser and Wijnberg (1995) highlights that a strong IPR regime is not a guarantee of high value capture, but that value capture also depends on other mechanisms such as lead time and learning curves. In a *weak* appropriability regime, it is therefore difficult and less probable to capture the profits from

the innovation due to the innovation being difficult to protect (Teece, 2018), while a *tight* appropriability regime increases the potential for the innovator to capture the profits due to the innovation being easier to protect. *Actual appropriation* then depends on how effectively and which appropriability mechanism the innovator uses (Yang & Hurmelinna-Laukkanen, 2022).

Teece (1986) explains that patents can often be invented around for a limited cost, indicating that a patent might create a certain degree of appropriability. As explained in Teece (2018), IP is not generally self-enforcing, meaning that possible IP infringements have to be identified and processed in court by the patent holder at their own expense. Appropriability potential depends not only on formal rights of protection but also on the broader set of mechanisms that can delay, deter, or prevent imitation. In Teece (1986, 2018), particularly strong appropriability regimes often emerge through institutional and regulatory exclusion mechanisms, for example, pharmaceutical approval systems, where the regulations themselves create substantial barriers to entry. Additionally, appropriability is influenced by the efficient use of IP mechanisms (Holgersson & Wallin, 2017). Among these are the applicability and effectiveness of lead times, switching costs, and secrecy. Lead times refer to the advantages gained by entering the market earlier than competitors, allowing firms to establish relationships, gain learning effects, and build market positions before imitation occurs (B. Hall et al., 2014). Switching costs increase appropriability by making it expensive for customers to change to competing products or services once they have adopted a focal firm's solution. First-mover advantages similarly enable companies to benefit from early market entry, through brand recognition, installed base effects, or access to complementary assets before competitors catch up (B. Hall et al., 2014; Teece, 1986). While secrecy is a mutually exclusive alternative to patenting (Arundel, 2001), other mechanisms can serve as complements to patents (Holgersson & Wallin, 2017).

Gemser and Wijnberg (1995) adds a view on appropriability with relation to the industrial life cycle. Gemser and Wijnberg (1995) states that in the early phases of the cycle, the industry faces high uncertainty and the absence of a dominant design, which makes imitation relatively easy and increases the difficulty of appropriating from innovation. In the more mature stages, a shift occurs from radical product innovation to a more stable innovation environment in which incremental improvements and process innovation dominate. At the same time, the barrier to entry increases and the number of actors decreases while vertical integration strengthens. In the later stages, the main way of differentiating is through, for example, design, where appropriability can once again be difficult due to the expiration of IPRs, and imitation can be done relatively easily by established actors.

2.5.1 Complementary Assets

Complementary assets play an important role in establishing a strong market position and appropriate from the innovation (Ceccagnoli & Rothaermel, 2016; Teece, 1986). Complementary assets are needed to successfully commercialize an innova-

tion, including marketing, manufacturing capabilities, sales channels, and after-sales support (Gemser & Wijnberg, 1995; Teece, 1986). There are three categorizations of complementary assets, as seen in Figure **??**: i) *Generic assets*, which are not innovation specific but can easily be used in different applications, ii) *Specialized assets*, which has a unilateral dependence with the innovation, exemplified by (Ceccagnoli & Rothaermel, 2016) as the reputation of quality of a manufacturer which makes it easier for that firm to commercialize a variety of innovations within that segment of products, and iii) *Co-specialized* with a bilateral relation, such as container ships and ports (Teece, 1986), as cospecialized assets are assets which are more valuable together than isolated (Ceccagnoli & Rothaermel, 2016).

By leveraging complementary assets, Ceccagnoli and Rothaermel (2016) states that innovators may, to some extent, influence the strength of the appropriability regime through their strategic choices, although the regime itself is mainly determined by legal and technological factors. In particular, firms that control specialized complementary assets may have incentives to purposely weaken the appropriability regime. An example of this is Tesla, where Elon Musk opened up the patent portfolio to allow others to innovate. From this, Tesla could benefit from increased adoption of electric vehicles through its complementary assets in electric-battery R&D and manufacturing, although it remains uncertain whether it will be able to capture returns from its innovation. Conversely, Apple in the 1980s has been argued to have maintained a too-tight appropriability regime through its defensive IP strategy in the computer market, which made other PC businesses more attractive platforms for developing computers and thereby allowed competitors to benefit from network effects that Apple missed out on.

To capture profits from complementary assets, Teece (1986) suggests that they be handled differently depending on their category, either by contracting or by integrating. In practice, there are hardly any pure cases of either contracting or integration (Teece, 1986). Consequently, organizational arrangements are often characterized by *mixed modes* that combine elements of both.

Contracting is when complementary assets are provided by suppliers under a contractual agreement (Teece, 1986). Contracting is especially useful in a tight appropriability regime where access to complementary assets from different sources and sufficient capacity are available. One of the main upsides is that the innovator does not need to make any large up-front investments that are highly capital-intensive and high-risk. Writing a good contract can be difficult, especially in the early stages of the industry life cycle, when needs and designs remain unclear. The contracting also creates a risk that the supplier will imitate the innovation and become a competitor, especially if the contractor controls crucial complementary assets, which puts them in a good position to profit from the innovation. Although contracting can appear simple, it becomes challenging when suppliers need to make innovation-specific investments or adaptations, since this effectively asks them to take on part of the commercial risk. In contrast, if the complementary assets are generic and the technology is well protected, the innovator retains leverage because multiple suppli-

ers can provide similar assets, limiting dependency and hold-up risk.

Integrating refers to ownership of the complementary asset, hence gaining control of it (Teece, 1986). In cases where complementary assets play a crucial role in generating profits from an innovation, such as when the innovation is easy to imitate, control, and access to scarce complementary assets is highly important (Gemser & Wijnberg, 1995). This perspective is extended by Winter (2006), who highlight the so-called *Hirshleifer case*, in which value capture may come not only from the innovation itself but also from control of complementary assets that increase in value when the innovation is introduced. In some cases, this means that more value can be captured through a timely move in these assets, rather than from the innovation itself (Winter, 2006). Needless to say, when imitation is easy, building or acquiring specialized complementary assets with close attention to competitors' moves is strategically important (Teece, 1986). There is little value in developing such assets if imitators can do so more quickly or at lower cost. Gemser and Wijnberg (1995) and Teece (1986) also add an industry life-cycle perspective to the importance of integrating complementary specialized assets: At the beginning of the life cycle, when uncertainty is high and sales volumes are low, it is less important to possess specialized assets. Although in the later stages, when the volume increases, it is of high importance.

2.5.2 Appropriability Regimes in the Digital Environment

Teece (2018) offers a perspective on appropriability in the digital environment, in which platform innovators and their associated complementors create an ecosystem. The platform then depends on both the platform owner and the complementors. Complementarity is described as the main purpose of a platform; its primary functionality is to provide an ecosystem. An example of this is Apple's ecosystem, where Apple has integrated complementary assets that are most innovation-intensive, such as hardware, including the microprocessor. Meanwhile, its app store, where third-party developers launch and develop apps, creates an appropriability opportunity for Apple. A digital platform is therefore described as an efficient way to support new business models and create a position of control from which the ecosystem can be enhanced while also enabling appropriation from it. In case of a platform-to-platform competition, Teece (2018) states that the winner is often the one who is able to capture both high quality and quantities of complementors - hence the importance of complementary actors is increasingly important.

The importance of standards in the digital environment is also brought up in Teece (2018). Standards in the digital environment are of greater concern and importance because they are often used to ensure compatibility and interoperability across other ecosystems and industries. The importance of interoperability is linked to modularity, whereby firms with specialized knowledge and capabilities can cooperate within the platform ecosystem.

2.6 Industry 4.0

Industry 4.0, also known as the Fourth Industrial Revolution, refers to the trend toward digital technologies in the industry (Xu et al., 2018). The first wave of Industry 4.0 began in the 2010's when new technologies such as Internet of Things (IoT), machine learning, and cloud services emerged (Cardona & Serrano, 2023). This marks the beginning of the era when large-scale data collection and the ability to analyze vast amounts of data were introduced.

The second wave in the evolution of Industry 4.0 began around 2016, when Artificial Intelligence (AI) and Intelligent Automation introduced new tools that significantly extended capabilities in data analysis and enabled more reactive, autonomous systems (Cardona & Serrano, 2023). Industry 4.0 is commonly linked to IoT, big data/analytics, cloud computing, cybersecurity, and horizontal/vertical system integration (Kumar & Kumar, 2020). These technologies enable connected products and continuous data generation, but also create challenges related to data availability, security, and confidentiality issues that become central for governance and IP protection in digitalized industrial offerings.

Industries across sectors will become interconnected, and the boundaries of individual industries will therefore fade (Xu et al., 2018). Enterprises will likely maintain their legacy products or systems while simultaneously incorporating new applications. The ability to effectively use technical integration to coordinate end-to-end activities across industrial ecosystems provides the necessary technical support to realize the initiative's goals. The new trend is that businesses of all sizes that are associated with Industry 4.0 will need to share and exchange data. Therefore, systems must be interconnected, and the applications that compose information systems must increasingly work together.

2.6.1 Digital Transformation of Industrial Firms

A digital transformation consists of three phases (Verhoef et al., 2021): i) *digitization* transforms analog information into digital in terms of data. An example is the transformation of paper-based analog surveys into a digital survey. Digitization is mainly changing internal and external processes, with little to no changes in the value of the activity, then ii) *digitalization* is how the new digital technologies can be used to create new business opportunities, enhance customer experiences, and process improvements to increase efficiency. The changes are therefore made on a sociotechnical level, exemplified by Verhoef et al. (2021) how online communication channels changed the way customers interact with companies, lastly iii) *digital transformation* concerns the company-wide change that results in new business models and how business is conducted. This involves changes in organizational tasks but also expands beyond earlier boundaries with suppliers, competitors, and customers.

Gaining maximum benefits from digital transformation is challenging, especially for industrial firms (Lundin & Kindström, 2023; Verhoef et al., 2021). Among

the challenges are the tensions and barriers to incorporating digital artifacts into their existing businesses. Verhoef et al. (2021) emphasizes that there are three main external drivers of digital transformations: i) *Digital Technologies*, such as Internet of Things (IoT) and Artificial Intelligence, are expected to make large positive impacts on current and future businesses, such as efficiency and possible reduced need for human labor, ii) *Digital Competition*, created by technologies that reshape whole markets, such as online stores, iii) *Digital Customer Behavior*, where digital presence is becoming more or less an expectation from customers, and businesses that fail to live up to their expectations fall behind.

2.6.2 Internet of Things (IoT)

Internet of Things (IoT) is a network of real-time connected physical objects that aims to control something, or exchange and collect data without human interaction (Kowalkowski et al., 2024). IoT devices can thereby be seen as a bridge between the physical and digital world (Gokhale et al., 2018). The physical objects consist of electrical components with sensors and some form of network connectivity. A sensor is a device that measures a property of a physical entity, and the digital measurement can be transmitted over a network (Paolone et al., 2022). The data generated by the devices is then shared over wired or wireless networks with servers located in the cloud or on-premises.

Today's customers are increasingly technologically proficient and increasingly buy experiences rather than goods, making the adoption of IoT essential for industries and retailers seeking to keep pace with this trend (Paolone et al., 2022). IoT has the potential to provide personalized services to customers. On the other hand, providing personalized services could raise concerns about protecting customers' identities and data.

An IoT ecosystem can be seen as a special type of business ecosystem in which firms both compete and cooperate around a shared set of assets that connect physical and virtual things (Mazhelis et al., 2012). At a high level, key stakeholders include the industries providing IoT technologies, the developers of IoT solutions, and end customers. Within such ecosystems, data from IoT devices and their sensors enables new insights (Kowalkowski et al., 2024), for example, through predictive maintenance where irregularities in vibration, temperature, or friction may signal declining efficiency or upcoming maintenance needs. Before real-time connectivity, such issues typically required manual inspections, whereas connected monitoring allows firms to automate surveillance and reduce costly on-site work. In this way, earlier physical touchpoints can increasingly be handled through digital means (Lundin & Kindström, 2023).

2.6.3 Digital Ecosystems

Digital ecosystems are among the new business models that have emerged from the introduction of cloud solutions and other digital technologies in the Fourth Industrial Revolution (Ma et al., 2024). There is no universal definition of a digital ecosystem, but for this thesis, we will follow the definition by Selander et al. (2013, pp. 184–185), stating that a digital ecosystem is "a collective of firms that is inter-linked by a common interest in the prosperity of a digital technology for materializing their own product or service innovation". An ecosystem could thereby be seen not only as a new way to conduct business but also as a means to increase growth through new forms of collaboration (Bresciani et al., 2021). At the center of attention in digital ecosystems is what Bresciani et al. (2021) explains: all actors within the ecosystem need to contribute some form of value.

Digital ecosystem also reshapes how value is created (Valdez-De-Leon, 2019). Value chains, which earlier were commonly linear, i.e., organized as a vertical value chain, are now turning into digital ecosystems, where value creation becomes more entangled. An example of this is that the value created for end customers increases as the platform owner provides tools that enable external developers to create new offerings on the platform, which not only creates new value for the customer but also strengthens the platform as a whole by increasing offerings.

Digital ecosystems often span beyond their initial market (Koch et al., 2022; Valdez-De-Leon, 2019). This means that not only competitors within the domestic market could be a potential threat, but also incumbents from other industries. One of the main risks of not participating in a digital ecosystem is, as argued by Valdez-De-Leon (2019), *not* being part of one, missing out on the opportunities it provides. Valdez-De-Leon (2019) emphasizes that transitioning to an ecosystem model can be especially challenging for companies with established operations, as it requires changes not only to their technology resources and capabilities but also to their business strategy and processes.

2.6.4 Digital Platforms

Platforms are not a new concept born out of Industry 4.0. Earlier, platforms have taken place in the form of, for example, *product platforms* where customization of products has been enabled through platform-driven development of product families (Halman et al., 2003).Cusumano et al. (2019) states that having the best product is no longer the most important, but having the best platform is.

Digital platforms can be categorized in various ways. One category is the *integrator platform* model, in which the platform serves as a wedge between external contributors and end users (Asadullah et al., 2018). This model could be applied to some crowdsourcing platforms. The second type of platform is the *product platform* model. Here, external contributors build on the platform owner's foundational technology and sell products or services directly to end users. Thus, in this model, the platform owner has less control over the interaction between external contributors and

the end user. The third category is the *multi-sided platform* model, characterized by external contributors' ability to interact directly and freely with end users via the platform. External contributors are not required to interact with the platform owner during the development of a product or service, although the platform owner may impose certain rules and regulations on them.

In general, platforms aim to connect individuals and organizations to create value-creation opportunities for interactions or innovative activities that they were previously unable to (Cusumano et al., 2019). To exemplify this, Cusumano et al. (2019) provides an overview of Facebook's platform and ecosystem, in which users, advertisers, and applications are connected through Facebook's digital platform.

Digital platforms introduce new kinds of relationships, defined as an "interdependent process of continuous interaction and exchange between at least two actors" (Holmlund & Törnroos, 1997, p. 6). The activities performed in the digital ecosystem depend on real-time collaboration and interaction among different actors, through which information is exchanged (Baptista & Nunes, 2025). This is done through a digital platform, highlighting the need for a robust platform that enables key players to facilitate real-time communication among multiple actors. The platform owner serves as a central host, coordinating connections among ecosystem actors. The host is also the one who needs to attract new actors, as new actors become dependent on the relationship and communication with the host to be part of the digital ecosystem.

2.7 Servitization & Business Model Transformation

As a result of the connectivity provided by IoT devices, in combination with data gathering and AI data analysis, a new B2B service innovation is introduced, where industrial firms are now taking part in digital services by connecting previously unconnected objects. For this thesis, we follow Kowalkowski et al. (2024) in defining a *service* as an offering with the distinctive attributes of being *intangible*, *non-ownership*, and the *central role of customer interaction*.

Notably, service innovation differs significantly from product innovation (Kowalkowski et al., 2024). When customers are to evaluate the quality of tangible products, many physical aspects are taken into consideration (Parasuraman et al., 1985). Quality is then perceived as a combination of color, style, and ease of operating the industrial product. Meanwhile, a service is intangible, underscoring the importance of new evaluation criteria for determining quality. First of all, the *perceived quality* of a service is the difference between the *expected service* and the *given service* (Parasuraman et al., 1985). The given service is determined by both the process and the final outcome. There are different approaches to evaluating service quality. An example of this is that service quality is determined through three dimensions: i) *Physical quality*, such as equipment, and ii) *Corporate quality*, such as the service

company's image and reputation, and iii) *Interactive quality*, which is how well the communication and interaction between the service firm and customer work.

2.7.1 Product-Service Systems

A Product-Service System (PSS) combines tangible products and intangible services to jointly fulfill specific customer needs (Tukker, 2004). To the far left in Figure 2.3, the value is solely or mainly delivered in the form of the tangible product. To the far right, services are the core of the value. In between these two extremes are possible combinations of product- and service-oriented value creation.

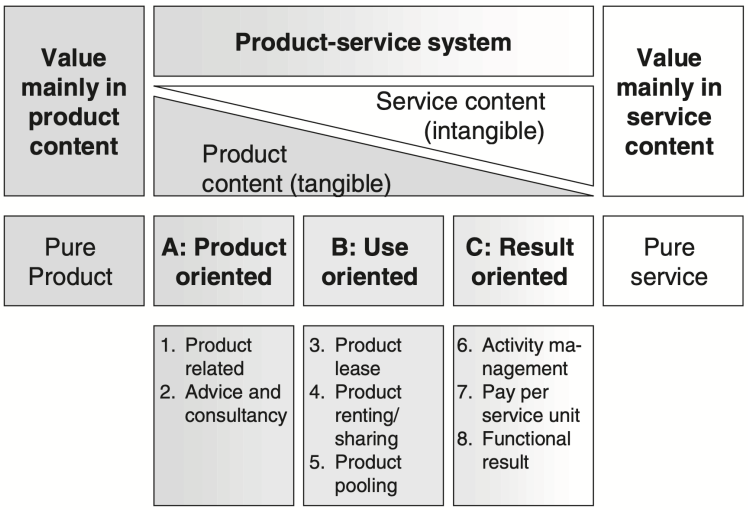

Figure 2.3: The main types of product-service system, with main- and subcategories. From Tukker (2004).

Following, the three main types of product-service systems will be presented from Tukker (2004): i) *Product-oriented services* is when the tangible product remains the primary source of value. Firms mainly focus on selling products, while offering complementary services such as maintenance contracts, take-back agreements, and the supply of consumables, ii) *Use-oriented services* means that the product is still central, but ownership is retained by the provider. Instead of selling the product, customers gain access through rental or leasing, while the provider is responsible for maintenance, repairs, and overall control, lastly iii) *Result-oriented services* is when a certain outcome is agreed upon beforehand (Tukker, 2004). Important to notice, however, is that there might be an absence of usage of a particular product - meaning that the means by which the promised outcome is performed is up to the provider. Result-oriented services consequently provide new liabilities and risks for the provider. This is especially true for results that are difficult to predict the required resources to fulfill, as the resources needed may exceed what the provider expected. This can be compared with a product-oriented approach, where the buyer holds the risk of not achieving the expected result from the given product. An example of this is given by Tukker (2004, p. 251), where a pesticide provider can

sell pesticides and provide instructions on how to use them to a customer, and it is up to the customer how efficiently they work. Although if the company were to sell a result such as a pre-determined percentage of reduction in loss of crops, a lot of pressure and possible economic losses could be required by the company if they do not fulfill its promised results.

2.7.2 Anything-as-a-Service

Digital enablers drive increased adoption of Anything-as-a-Service, in which product ownership is neglected, leading to a focus on creating customer convenience (Vandermerwe & Erixon, 2023). This not only changes ownership but also the firm's incentives to create products that are meant to last longer and possibly even be reused. As the focus of these anything-as-a-service is to provide an outcome, the pricing model changes as well (Vandermerwe & Erixon, 2023). From selling tangible goods with low margins, firms are moving towards subscription- and usage-rate pricing models, which often have significantly larger margins (Oliva & Kallenberg, 2003). As services provide continuous value, the relationship between the customer and the company is often positively affected by increased interactions compared to one-time sales (Vandermerwe & Erixon, 2023).

In an availability-based business model, the service provider is often particularly interested in predictive maintenance, since it directly affects service up-time and contractual performance (Oliva & Kallenberg, 2003). Predictive maintenance is often combined with real-time monitoring via sensors and IoT devices (Kowalkowski et al., 2024), although the technically advanced services are often not of interest to customers because their value is difficult to grasp (Oliva & Kallenberg, 2003). From case studies of manufacturing firms by Oliva and Kallenberg (2003), the main reason customers are so uninterested in monitoring their products is that they cannot see the value that monitoring itself creates. Instead, to make the impact of the monitoring understandable within the customer's business and context, the value provided needs to be presented in terms of increased uptime.

3
Methodology

This chapter describes the thesis's methodology and its application in practice to address the research questions. The chapter showcases the research design and qualitative research methods, including how data were collected through semi-structured interviews, how respondents were selected, and how the interviews were analyzed thematically. Finally, a discussion of the methods' quality and trustworthiness is conducted within the scope of credibility, transferability, dependability, and confirmability.

3.1 Research Design

This thesis adopts an interpretivist research philosophy (Bell et al., 2022) to understand how individuals within the organization perceive and interpret changes in IP. The objective of this thesis is to investigate how the IP strategy changes when an industrial product is retrofitted. Accordingly, the thesis adopts an exploratory qualitative approach to deepen understanding of this phenomenon. An exploratory approach is appropriate in this case to study the evolution of the organizational environments surrounding intellectual assets, given that the retrofitting context remains underdeveloped. This approach enables an in-depth understanding of an emerging phenomenon, rather than testing predefined hypotheses. To support this exploratory perspective, the research was conducted abductively, using existing theory to design the interview guide and then iteratively moving between empirical patterns and theory during coding and interpretation. The abductive approach is therefore aiming to generate insights and potentially develop new theoretical understanding based on empirical findings from interviews. The interpretivist stance further influenced the interviews by encouraging open-ended exploration of how respondents perceive digital transformation and IP strategy, rather than treating them as predefined organizational variables.

The thesis was conducted at a single company and is therefore a single-case study design (Bell et al., 2022). A case study is appropriate because the research focuses on a complex context-dependent phenomenon within an organizational setting. The case can be considered revelatory, as it provides rare insight into the internal processes of IP management during digital transformation. The selected company is currently undergoing a digital transformation of some of its legacy products, making it highly relevant to the study of how its IP strategy evolves in this context. Given the five-month time frame, the research was cross-sectional, meaning the company

was examined at a single point in time.

This research examines a business unit of the case company and its employees at the organizational level of analysis. The thesis examines how the organization's IP capabilities respond to a legacy product undergoing digital transformation. Although the empirical data are collected through individual interviews, the analysis is conducted at the organizational level by aggregating and interpreting individual perspectives to represent broader organizational patterns and capabilities. While this approach enables insights into organizational dynamics, it may also obscure individual variations and contradictory viewpoints.

3.1.1 Description of the Case Company and Product

The case company is a European industrial firm that develops and manufactures technical products for commercial use. The company has an established market position and provides solutions where key attributes are functionality, uptime, and security.

The product to be analyzed is the physical infrastructure used in operational environments. It has traditionally been based on mechanical and electromechanical components but is currently being retrofitted with digital enhancements. These include integrated connectivity and software that enable data collection from the product's sensors.

3.1.2 Data Collection

Data were collected through semi-structured interviews, as this method is well-suited to the research and enables the collection of nuanced, broad, and detailed responses compared to methods such as surveys or structured interviews (Bell et al., 2022). Interviews were mainly conducted via Teams, and all interviewees were asked questions in English, with the option to answer in either Swedish or English. Interviews were voice-recorded, and when allowed, computational transcription was used to complement the manual transcription conducted during the interview. Recordings and transcriptions were stored on the case company's OneDrive, and will be deleted once the Master's Thesis has been approved by the examiner.

The interview guide was based on the literature brought up in the literature chapter, such as how IoT devices and data gathering reshape business and business priorities. As the interview guide was based on the theoretical framework, there is a risk that the framing of questions may have influenced respondents' answers toward the existing theoretical framework. While the approach ensures relevance to the research questions, it may limit the emergence of novel perspectives.

Interviews were conducted with: i) *R&D Department* to gain insights into the technical aspects of the retrofitting, new digital assets, and the implementation of IoT and associated systems, and ii) *Strategy & Business Development* to gain informa-

tion regarding digital ecosystem opportunities and challenges, changes in ways of conducting business such as servitization, and how intellectual assets are a part of the companies' strategies, and iii) *Legal & IP* to understand how the digital transformation shapes the internal environment in terms of focus on IP and mechanisms, and how these are managed currently, and iv) *Sales Department* to assess how the digital transformation affects customer interactions, such as new contractual agreements for data gathering, and how well it aligns with customers' expectations and needs.

Table 3.1: Interview information

This table presents the firm's representatives' roles, and their experience within the firm. The respondents have been assigned an alias to ensure anonymity. It also includes the duration of each interview.

Subject	**Role**	**Years of Experience**	**Duration(min)**
S1	IP Management	5	52
S2	IP Management	11	54
S3	Strategy	23	55
S4	IP Management	15	53
S5	R&D Manager	11	46
S6	Sales Manager	6	50
S7	IP Attorney	2	31
S8	IP Management	5	100
S9	R&D	40	49
S10	Strategy Manager	6	51
S11	R&D Manager	4	52
S12	R&D	27	49
S13	R&D Manager	3	45
S14	IP Management	5	33
S15	Strategy	22	55
S16	Sales Manager	11	47
S17	R&D	8	56
S18	R&D Manager	7	34
S19	IP Management	3	54
S20	Strategy	1	55
S21	Sales	40	55
S22	Strategy	25	55
S23	R&D Manager	11	40
S24	IP Management	6	45
S25	Sales Manager	4	60
S26	Strategy	10	60
S27	IP Management	10	53
S28	R&D Manager	8	47
S29	Strategy	12	44

3.1.3 Sampling

A total of 29 interviews have been conducted through snowball and convenience sampling (Bell et al., 2022), where the aim is to conduct interviews with employees in different roles to gain insights from various functions, including strategy, research and development, sales, and legal, that are involved in or exposed to digital transformation and related intellectual assets. Convenience sampling was used due to the company's complex structure, while snowball sampling facilitated the identification of additional relevant participants with experience in digital transformation. Although convenience and snowball sampling provided access, the logic was primarily purposive, aiming to maximize variation across organizational functions relevant to IP strategy and digital transformation. The respondents were approached through mail and introduction meetings.

However, the use of non-probability sampling techniques may limit the generalization of the findings. Convenience sampling may introduce selection bias, whereas snowball sampling may yield a sample of individuals with similar perspectives (Bell et al., 2022). In addition to the sampling-related biases, the thesis may be subject to internal perspective bias, as all employees are within the same organization. This may result in a dominant organizational narrative and limit the inclusion of external viewpoints. To mitigate internal perspective bias, sampling was conducted across multiple internal departments. During the interviews, questions were designed to probe for trade-offs and tensions, capturing competing interpretations rather than assuming a single coherent view. Despite these limitations, this approach was deemed appropriate for gaining in-depth insights into a relatively unexplored research area.

3.2 Analysis of Method

Qualitative interviews were selected as the primary data collection method, as they allow for the investigation of issues that are difficult or resistant to observation, as is the case in this thesis.(Bell et al., 2022). It also provides informed consent to the researchers, a common ethical requirement in business research.

The chosen method of data analysis is thematic, allowing for the identification of patterns and themes within the empirical material. A hybrid abductive thematic analysis is then applied, combining inductive coding with guidance from relevant theoretical frameworks, consistent with Bell et al. (2022) 's description of iterative qualitative reasoning. This enables both theory development and theory extension, as empirical findings are continuously compared with established frameworks. Data collection was continued until thematic saturation was reached.

The analysis was conducted using a structured, multi-step thematic analysis process to ensure transparency and rigor. First, all interview transcripts were systematically coded to identify recurring themes and patterns, which were then labeled without predefined categories. Altough no predefined thematic categories were imposed, the

coding process was guided by the four research questions. During repeated readings of the transcripts, sections of text relevant to the research questions were assigned as initial codes. These codes were iteratively refined and grouped into broader categories, allowing themes to emerge from the data while keeping the focus to answer the research question. Second, the identified themes were continuously compared across perspectives to analyze differences and similarities, i.e., how interviewees might discuss a topic in different ways or how they differ from one another (Bell et al., 2022). This enables a structured understanding of the changes over time. When opinions diverged, they were noted as contested themes, and cross-functional comparison was used to see why interpretations differed. Third, the empirical findings were interpreted in relation to existing theoretical frameworks, allowing for a deeper understanding of the patterns and contributing to theory development. Throughout the analysis the research questions served as analytical lens guiding the coding and theme development. As themes became more refined, they were systematically reviewed and mapped to the research questions they directly addressed. This enabled a structured comparison of empirical comparison of empirical observations and ensured that the findings remained closely connected to the studies purpose and aim. To enhance the trustworthiness of the analysis, coding decisions and interpretations were continuously discussed among the researchers to reduce individual bias and ensure consistency.

Trustworthiness can be used to evaluate qualitative studies (Bell et al., 2022). For our research, we have chosen to follow the Lincoln & Gubas framework presented in Bell et al. (2022), which consists of credibility, transferability, dependability, and lastly confirmability. Credibility refers to the extent to which the findings of a qualitative study are perceived as believable and accurately represent the reality of what is being studied (Bell et al., 2022). To enhance credibility, respondents were allowed to review the findings. Credibility was further strengthened through triangulation, in which insights were collected from multiple organizational functions, including R&D, strategy, legal, and sales. While the thesis relies primarily on interview data, comparing perspectives across functions helps identify divergent and convergent views within the organization. This thesis will combine semi-structured interviews, theoretical literature, and secondary data, including prior research. By combining the findings across these sources, it was possible to identify patterns and reduce the risk of relying on a single perspective.

As the research is based on a qualitative approach focused on a specific company and product, the transferability to other contexts may be difficult to determine (Bell et al., 2022). To facilitate an understanding of transferability, a description of the case product and its environment, which may influence the results, was provided in the thesis. Although the findings are context-specific, the thesis aims to contribute to generalization by identifying mechanisms and patterns that may be relevant for other industrial firms undergoing digital transformation.

The transferability of the findings is likely strongest in the industrial contexts characterized by long product life cycles, installed bases, and safety or reliability re-

quirements, with increasing digital integration through IoT and servitization. In such contexts, firms often rely on complementary assets that shape how IP strategy evolves during digital transformation. At the same time, the findings may be less transferable to purely digital firms and where ecosystem dynamics differ significantly. Additionally, some findings may be particularly shaped by the company under study's industrial setting, where uptime, reliability, and long-term customer relationships are strategically important.

Dependability implies that a study is consistent, transparent, and can be repeated with similar results (Bell et al., 2022). Though in qualitative research, it is recognized that exact replication is difficult due to different contexts. That is why the focus of this research was to ensure that the research process was documented throughout, including the interview guide, sampling procedures, and coding process, allowing external viewers to understand how conclusions were drawn. To ensure a structured and systematic research process, all stages were clearly documented.

Confirmability is achieved as the results are based on data rather than the researchers' perceptions and beliefs. The analysis is conducted through thematic analysis, supported by citations from the interviews to motivate the themes. Confirmability will also be enhanced by grounding the analysis in empirical data and by direct quotations from interviewees, which are then continuously interpreted and discussed between the researchers to reduce individual bias.

4
Empirical Findings

This chapter reports the empirical findings from the semi-structured interviews. Using thematic analysis, recurring patterns across the interview data were identified and are presented in relation to the thesis's research questions. Accordingly, each section addresses one research question, with subsections detailing the associated themes.

4.1 What New Intellectual Property Emerges with the Introduction of Digital Functionalities?

This section presents the results for research question 1 and highlights the new IP that emerges from digital retrofitting and integration into digital ecosystems. Of particular importance are data, software, and connectivity, as well as how this IP can be controlled through secrecy and contractual agreements.

4.1.1 Data & Insights as Core Assets

Across interviews, the most consistently identified addition from the digitalization is increased *accessibility* to data. Interviewees S6 and S16 explained that data had previously been stored locally in each product's control box, requiring physical access to extract it. With the introduction of an IoT device and real-time connectivity, the key difference is that it becomes "continuously accessible and retrievable remotely". Earlier, on-site extraction meant that data was collected irregularly and primarily used for troubleshooting by service technicians rather than for systematic analysis.

Interviewees stated that access to product-generated data is a prerequisite for realizing value through digital capabilities such as AI and statistics. Without access to the data, analysis cannot be performed, and actionable insights cannot be generated. Views on data ownership differed. Most interviewees stated that the customer owning the product is also the data owner, and that the firm therefore stores and uses the data under contractual agreements, as stated by interviewee S12: "The customer owns the data, but we attach an agreement where they accept that we can collect the data." Others argued that the industrial firm owns the data, but that customers have rights of access under the Data Act. A related view was that the actor who owns the product also owns the data, implying that in leasing arrangements, the firm may be the data owner.

Importantly, interviewees distinguished between *owning* data and *accessing* it. Some, for example, S24 and S25, emphasized ownership to prevent data from being shared with competitors. At the same time, interviewees were largely aligned that it is mainly access that is critical for two reasons: i) enabling new service and business opportunities, and ii) enabling product-related learning for product development and innovational activities.

Beyond raw data, interviewees repeatedly emphasized insights as the central asset created by the digitalization. Usage data was described as particularly valuable for product development, as it provides evidence of how products are *actually* used in customer contexts. Several interviewees also noted implications for the sales department, as a better understanding of usage enables more accurate recommendations regarding product replacements, product configurations, and add-ons. Some suggested that usage-based arrangements could extend to more advanced business models, such as leasing or changing products at no cost to the customer based on observed usage, with contractual licensing forming the foundation. As interviewees summarized, the product's core function is to optimize "a hole in the wall" by alternating between serving as a barrier and an opening. Here, digital usage insights therefore become directly relevant to both performance and value creation.

4.1.2 Digital Functionalities as New IP Assets & Risks

Interviewees described the digital offering as software-based, particularly through a platform that provides customers with modular functionality. Overall, these features were framed as mechanisms to increase customer value while enabling internal efficiency and learning. Several modules were described as enabling the product's behavior to change based on external data or signals from other actors, and the platform was also described as enabling service technicians to read, diagnose, and control products remotely. This remote capability was framed as enabling new service modes, including reducing the need for on-site visits and enabling faster response through remote actions.

A recurring point raised by, for example, S15 and S18 was that modularity enables the firm to extend the platform through new modules and third-party data integrations, thereby increasing usability and value creation. At the same time, interviewees highlighted that entering the digital environment creates new risk exposures. As interviewee S1 stated: "The digital risks are much larger, both regarding brand and reputation. The worst thing that could have happened for hardware protection, such as patents, was that someone copied our invention and we lost a little bit of money." Interviewee S15 emphasized that "digital connectivity removes the requirement of physical presence to interfere with the system, as digital controls may, in principle, be accessed from anywhere in the world". Consequently, interviewees stressed the need for new capabilities and resources related to cybersecurity, both to prevent unauthorized control and to protect product-generated data that is stored and processed.

In addition, interviewees noted that digitalization enables remote firmware updates

via the platform. These updates were framed as a way to enhance or expand functionality over time, thereby strengthening the value proposition and reinforcing the importance of robust security and governance for software changes.

4.1.3 Shift Toward Contracts, Secrecy, & Ecosystem-Based Control

Interviewees repeatedly emphasized that the digital environment differs from the electromechanical environment in how IP is controlled and used. For electromechanical inventions, patents and design rights were commonly cited as relevant forms of protection. For digital assets, including software-enabled features, data processing logic, and ways of working, interviewees more often emphasized non-registrable control mechanisms, particularly contracts and secrecy.

All interviewees described contracts as becoming more central post-digitalization. Contracts were framed as mechanisms to: i) appropriate value from digital features, ii) regulate data access and confidentiality, iii) provide a baseline for new business models, and iv) structure partnerships and responsibilities across actors. An example concerned predictive and preventive maintenance. Prior to digitalization, service contracts were described as optional add-ons and were primarily yearly or reactive, often offered in tiered levels that defined response times and visit fees. With connectivity, interviewees described how sensor data - for example, temperature, number of cycles, and related operational indicators - enables statistical and algorithmic processing to anticipate maintenance needs before breakdowns occur. This was stated to enable predictive maintenance offerings, in which the contractual arrangement becomes central to both profitability and to meeting customer expectations regarding uptime, response, and scope.

Most interviewees also described digitalization as shifting the collaborative environment toward increased partnerships. Joint value creation was frequently associated with system integration, in which interlinked systems deliver more value than standalone solutions. As interviewee S15 stated, platform-based access could enable third-party automation innovations that control products through the firm's platform. At the same time, interviewees emphasized greater complexity, as actors may simultaneously be partners, customers, and competitors depending on the context. This ambiguity was described as making contract design more challenging, as agreements need to enable collaboration while safeguarding against competitive risks and unintended knowledge spillovers.

A recurring theme was the growing importance of secrecy as a means of protection and control. Interviewee S5 argued that "raw, unprocessed product data has limited standalone value, whereas processed outputs and derived insights are what actually matter and should be seen as a trade secret." Interviewee S9 echoed this, suggesting that "an attacker would be more interested in stealing processed data than raw data". In contrast, other interviewees, such as S26, noted that raw data may still be valuable because, even through basic interpretation, it reveals usage patterns that

competitors could exploit. Beyond the data itself, interviewees highlighted that methods of collection, processing, algorithms, and internal ways of working may also be considered sensitive knowledge that should be protected by confidentiality.

In addition, the interviewees raised concerns about data sharing and integrations. As S24 stated, "data sharing should be restrictive to avoid unintended leakage of sensitive information or insights". Some interviewees also questioned the effectiveness of patents for processes and algorithms in digital contexts due to disclosure requirements, as revealing details may help competitors invent around the protected claim. One interviewee (S8) noted that "software patents are used in some cases, while other parts of the overall solution are intentionally kept as trade secrets. This hybrid strategy was described as enabling selective disclosure where disclosure of a smaller part may be of limited value without the complementary secret components".

While brand and reputation were generally mentioned as valuable assets, interviewee S27 added that sub-branding could be an efficient way to protect the main brand against potential harms associated with digitalization. The interviewee emphasized that cybersecurity incidents such as intrusions or data leaks could significantly damage the brand, particularly in safety- and security-oriented industries where such incidents signal unreliability. Sub-brands that are not tightly linked to the core brand were therefore described as a potential way to reduce reputational spillover in the event of an incident.

Finally, interviewees suggested that relationships themselves become more valuable assets in digitally integrated ecosystems. As integration increases, value creation becomes increasingly dependent on access to complementary capabilities, partner ecosystems, and negotiated interfaces, making relational positioning and ecosystem participation part of the firm's broader IP control and appropriation logic.

4.2 How does Digital Retrofitting Change the Role of Existing IP?

This section presents the results for research question 2 and describes the interviewees' perspective on how digital retrofitting affects current IP, shifting from primarily protecting the physical product to more broadly supporting access, risks, and control in the digital environment.

4.2.1 From Core Protection to Foundational Layer

Across interviews, respondents consistently describe digital retrofitting as a shift from value being primarily embedded in mechanical hardware to being increasingly tied to digital layers, including data and software. This also changes how protectable the firm's key assets are perceived to be, with digital assets considered less prone to IPR protection. While a few respondents argue that mechanical IP is rapidly losing strategic relevance as the product becomes commoditized, the dominant view is

that traditional protection rights (patents, trademarks, design rights) remain important. However, they are increasingly framed as a foundational layer, necessary for credibility and compliance, rather than the main source of differentiation. Several respondents emphasize that regulatory requirements and physical security considerations will continue to anchor the importance of hardware-related protections over time.

A recurring theme is that established customer relationships serve as a complementary asset that becomes even more valuable as products are digitalized. Interviewees describe these relationships as a channel for guiding customers through new purchasing and usage patterns in a more digital offering. As S16 notes, "we want to keep our relationship with customers so we could guide them when purchasing products," while also stressing that "we must see through that intermediaries do not take over the relationship." In other words, retrofitting is described as increasing the risk of disintermediation, making continuous contact and trust-building strategically important.

Respondents also highlight that the patent landscape changes when inventions move into software and algorithmic domains. Historically, patents have been a key mechanism for protecting physical hardware, but several interviewees suggest that firms may increasingly face a trade-off between patenting and secrecy for digital inventions. One concern was that algorithm- and software-based inventions can be difficult to patent broadly and easier to invent around. As stated by S19, such inventions may be challenging to protect efficiently to block competitors. In addition, interviewees stress that digital standards and platform ecosystems may expose firms to more complex patent environments. S8, for example, describes a setting in which industry standards are shaped by many patent-holding firms, implying that using a standard may require navigating among multiple actors with potential claims. S8 further adds that firms with large patent portfolios, such as Apple and Ericsson, become a part of their patent environment due to overlapping digital functionalities and data streams, and that the overall number of actors increases the risk of patent disputes and infringements. As a consequence, prior art searches and freedom-to-operate assessments are described as more time-consuming but also increase the importance of patenting.

From a trademark and branding perspective, digital retrofitting is stated to shift the focus of IP value toward brand trust and customer experience. Interviewees describe the brand historically as a quality signal associated with their tangible products, as stated by interviewee S2: "I do not think we can protect our products from being digitalized by competitors other than being first and our relationships. It is about brand and trust, we need to be trusted to do this more than competitors, and be trusted to protect what customers want to protect." But as more value moves into software layers, protecting the brand becomes more critical, as reputational risk is described as potentially more severe in the digital context, as failures in digital IP or cybersecurity can affect the entire group brand, not just a single product line, making brand-related protections and governance more consequential.

4.2.2 From Artifact Protection to Access & Risk Governance

Beyond classic protection mechanisms, respondents indicated a broader scope of IP that needs protection. Rather than only securing artifacts such as mechanical designs, IP increasingly involves governing data access, controlling digital interfaces, and managing cybersecurity risks that can undermine existing protections. A key driver is the difference in development pace, as respondents repeatedly highlighted slower hardware cycles compared to the faster digital iterations. This acceleration was described to make it more difficult for IP functions to file and maintain formal protection in time, and it encourages more selective strategies, such as protecting only parts of an invention while keeping critical elements secret to prevent competitors from reconstructing the whole invention.

Consistent with this, interviewees emphasize that new digital layers introduce intrusion risks that affect both new and established protections. As products become more connected, detecting IP intrusions becomes more difficult, raising concerns about trade secret leakages and unauthorized access to digital functionality. Several interviewees, including S7, S12, and S15, specifically mention the risks of remote access. Alongside direct functional risks, respondents repeatedly highlight reputational exposure, as digital failures can spread quickly and damage trust.

Consequently, respondents describe the protection of new intangible assets as a combination of organizational and technical mechanisms. Secrecy is frequently mentioned as a practical approach, described as of the essence both internally and in collaborations through NDAs, and externally through cybersecurity measures to prevent third-party attacks. Following, IP protection becomes less about single legal rights and more about a coordinated system of legal governance, information management, and technical safeguards.

4.2.3 Changing Enforcement Mechanisms in Digital Contexts

Interviewees also highlight that digitalization changes enforcement conditions and the dynamics of proof. S8 contrasts tangible and digital infringement detection: patent infringements on physical products can often be assessed by inspecting the product, whereas software infringement is harder to detect because the relevant functionality may be hidden in a ”black box”. This makes the verification of IP intrusions more uncertain and reduces the predictability of litigation outcomes. As a result, respondents suggest that the enforcement strategy must adapt by combining legal tools with technical approaches and monitoring capabilities.

At the same time, respondents argue that existing assets retain strategic value but are leveraged differently. The installed base is repeatedly described as a central asset whose importance increases with retrofitting. When products are equipped with sensors and connectivity, the installed base shifts from just being hardware to

an opportunity for vast data collection and service delivery. Even where mechanical patents have expired, respondents suggest that the installed base remains difficult to replace, creating switching costs and reinforcing customer loyalty. Moreover, interviewees describe how a larger installed base can improve data quality and diversity, thereby supporting learning effects and future development that smaller competitors find difficult to replicate. In this sense, IP becomes less static and more cumulative, as more products connect and knowledge becomes part of digital functions and operational activities.

Digital retrofitting also reshapes product knowledge as an intellectual asset. Before digitalization, knowledge was largely associated with engineering expertise and tacit service know-how. With connected products, respondents describe how data becomes a central source of learning, consequently reducing the long-term differentiating power of purely mechanical IP as the firm builds new forms of insight about products and customers. Several interviewees also stressed increased reliance on complementary assets such as service capabilities and resources, integration capabilities, and well-developed relationships. Electromechanical IP is presented not as sufficient to secure these positions, but as a prerequisite for scalability and credibility. Overall, respondents emphasized differentiation through a combination of software, hardware, services, and trust, rather than through a single protected invention, implying that existing IP is valuable as part of a broader system of complements.

Thereafter, respondents stated that retrofitting increases the importance of product and service complexity, which can, in turn, serve as a barrier to imitation. While competitors might copy individual elements, such as hardware components, sensors, or basic software functions, interviewees suggest that replicating the integrated whole is much more difficult. Some interviewees, such as S1, S2, and S6, emphasize that competitors could still attach their own IoT devices to the firm's products, indicating that exclusivity through traditional IP alone is limited. In this environment, existing IP shifts from being the primary protection mechanism to a single layer within a multi-layered defense and control. This layered view also reflects respondents' views on counterfeit enforcement. Interviewees describe the firm as proactive in enforcing trademarks and acting on counterfeits in physical products, where replication is often visual and mechanical. In the digital environment, however, detecting intrusions is expressed to be more difficult.

4.3 How do Evolving Ecosystem Interdependencies Influence Intellectual Property Strategy?

This section highlights the findings from the interviews in the context of research question 3, which shows how increasing ecosystem dependency affects the IP strategy. Here, among the most significant changes are blurred roles among actors, requirements and dependencies on interoperability and standards, and an increased need for contractual agreements and data governance to manage and control value capture in cooperations.

4.3.1 From Linear Value Chains to Blurred Roles and Strategic Uncertainty

Interviewees consistently described how digitalization increases ecosystem complexity and blurs the boundaries between suppliers, partners, competitors, and customers. Rather than operating in a linear value chain with clearly separated roles, the firm is increasingly described as facing multi-actor environments in which the same actor may simultaneously provide infrastructure, access critical data, and compete for control over customer interfaces. Examples raised include cloud providers, platform owners, and building management suppliers that can enable core functionality while also positioning themselves closer to end users.

The multiple roles create strategic uncertainty. As described by the interviewees, partners may become competitors if they acquire sufficient system knowledge or customer proximity, while competitors may become necessary collaborators when integration and interoperability are required. Several interviewees therefore emphasized the importance of retaining control over core assets such as algorithms, protocols, and data-derived insights. Control over a large installed base was also described as a source of leverage, as it strengthens negotiation power, increases switching costs, and can limit partners' ability to appropriate value.

As interdependencies increase due to systems being connected, such as connections to the IoT devices at the customer's site and connections to third-party platforms, interviewees suggested that IP strategy shifts away from a narrow focus on protecting inventions or discrete products. Instead, IP was described to increasingly function as a tool for managing control, dependencies, and bargaining power within ecosystems. Collaboration was often described in terms of sharing data, software components, and jointly developed solutions, making it harder to rely on traditional protection mechanisms alone, as external actors may gain access to previously internal assets. Consequently, interviewees described a movement toward an access-and-control logic, in which questions such as who can use data, who controls interfaces and standards, and under what contractual conditions value is shared arise. In this setting, contracts, licensing structures, and data access agreements become essential complements to formal IP, as IP is intended to control IP use within collaboration rather than to block imitation.

4.3.2 From Linear Value Chains to Ecosystem Complexity

Across interviews, interoperability was repeatedly framed as a strategic control point rather than just a technical requirement. Digitalization was described as increasingly requiring integration with external platforms, including customer management systems, building management systems, and cloud providers. In this context, control over interoperability was not only described as enabling compatibility but also as shaping power dynamics, as actors that control key interfaces can gain leverage over partners and customers by influencing how value and data flow across the ecosystem.

Several interviewees argued that the ability to integrate smoothly with customers' existing systems can be essential for becoming a preferred supplier or partner. Integration was sometimes described as a customer requirement, as customers often prefer to integrate new digital functionality into existing systems rather than adopt entirely new ones. Interviewee S4 illustrated this logic using the Apple ecosystem, as once users have for example an iPhone, iPad, and MacBook, they tend to prefer complementary products that integrate seamlessly into the same environment.

Participation in standard-setting alliances was also described as strategically important. Standards were described to determine which technical solutions become defaults and which firms gain influence over industry architecture. However, interviewees emphasized that standards often demand a degree of openness, creating a tension between contributing enough knowledge to shape the standard while avoiding excessive disclosure that could weaken a firm's competitive position.

Similarly, APIs were described as mechanisms that regulate ecosystem value flows. APIs define which functions and data external actors can access and under what conditions. As ecosystems expand, APIs increasingly act as gatekeepers rather than neutral technical interfaces, shifting strategy toward deciding what to open, how much to open, and to whom. Interviewees noted two opposing risks: opening too much can enable others to replicate functionality and compete for the customer experience, while keeping systems overly closed can reduce adoption, especially when customers or dominant platforms require compliance with common standards.

4.3.3 Contracts & Data Governance in Ecosystems

Interviewees also highlighted that digitalization introduces new ecosystem actors - software firms, service providers, and platform suppliers, who were previously outside the traditional industry. In such relationships, traditional IP rights alone were seen as insufficient because patents, trademarks, and design rights do not directly govern questions of data access, usage rights, and downstream analytics. As a result, interviewees repeatedly highlighted contracts as the primary mechanism for governing value capture and collaboration in ecosystems. Service agreements, licensing structures, and NDAs were described as central for clarifying ownership, access, and permissible use.

In parallel, relationship governance and monitoring were described as increasingly important, as actors' roles can change over time. Several interviewees emphasized the need to decide carefully what to share, with whom, and under which relational conditions. Trust, continuity, and installed-base leverage were described as complements to formal IPRs, helping firms sustain advantage when legal protection is difficult or when collaboration requires controlled openness.

Data management emerged as a critical component of the digital retrofitting. Interviewees stated that connected products generate large volumes of data and that *access* to data, rather than formal *ownership*, often determines competitive advan-

tage. These interdependencies force firms to negotiate data rights in contexts where customers and partners may all claim legitimate interests. Interviewees also described how insights, algorithms, and analytical processes are often kept as trade secrets and protected by internal controls, since disclosure can erode bargaining power within the ecosystem.

Finally, evolving ecosystems were described as reshaping competitive threats. Competition was previously perceived as relatively stable; interviewees argued that connected products create opportunities for new entrants, including software startups and born-digital firms. New competitor categories mentioned included platform actors and systems that are part of customers' core workflows, such as facility management solutions, building management systems, and ERP systems. These actors were described as possibly posing a particular threat because they already sit close to the customer interface and can potentially control data. As interviewee S17 noted, control over the interface can translate into control over data and having close collaboration with the customer, shifting the central fear from product copying to a loss of control over relationships and ecosystem positioning.

4.4 How does Digital Retrofitting Drive firms to Reconsider the Relationship Between their IP Strategy and their Business Model?

This section introduces the findings from the interviews on research question 4. Here, the impact of the IP strategy resulting from digital retrofitting is examined, with new business models, such as outcome-based agreements, discussed. Also, the ability to capture value in digital ecosystems and the importance of an IP strategy in such an environment are brought up.

4.4.1 Shift Toward Service- & Data-Based Value Capture

Several interviewees described digitalization as enabling new ways of capturing value beyond the traditional one-time sale of a product. For example, interviewee S17 outlined outcome- or usage-based models in which the customer could receive the product at no upfront cost but instead pay per opening or another measurable metric. Similarly, interviewees S10 and S21 suggested leasing models structured as subscription services, where the customer pays a fixed recurring fee while the company assumes responsibility for maintenance, service needs, and replacements. As S1 emphasized, such subscription offerings depend on data: "All subscription services are based on data: we can not provide subscription services". In this logic, as S21 noted, operational risk shifts from the customer to the company, which increases the importance of reliable monitoring and service delivery capabilities.

However, while the potential of usage- and subscription-based models was widely acknowledged, some interviewees described internal barriers to implementing them. Interviewees S3, S6, and S12 pointed to the current service offering and spare-

part sales as having high profit margins, which, in turn, increase the barrier to transformation and reduce the willingness to replace or cannibalize parts of the existing business model.

4.4.2 Interoperability Trade-offs & Adoption Constraints

Interviewees also highlighted a strategic tension between ensuring interoperability and preserving differentiation. On the one hand, the products and their digital platform must integrate with other systems to be relevant in customers' environments. Interviewee S4 explained that "customers typically already operate many systems, and adding another isolated system provides little value". Instead, the possibility to integrate and exchange information with existing systems was described as essential for customer interest in digital solutions. On the other hand, interviewees noted that standardization and open digital interfaces can lower switching costs. As S9 argued, standardized interfaces may make it easier for customers to move to alternative suppliers. At the same time, S13 emphasized that the electromechanical products are tailored to their specific placement, making hardware replacement costly and thereby creating a lock-in effect even if customers can switch software providers more easily. Extending this point, S12 suggested that customers may be skeptical of switching systems even when they would like to change hardware, which can make digitally engaged customers less prone to switch once a solution is embedded.

Beyond these strategic considerations, several interviewees described practical constraints that affect adoption and business model change. Some, such as S11, emphasized the difficulty of identifying new customer value propositions enabled by digitalization. Interviewee S3 illustrated this challenge by arguing that many customers view the product primarily as basic functionality or "optimization of a basic functionality", which contributes to skepticism about whether customers will pay for digital features. This skepticism was reinforced by the perceived lack of a clear business case for the digitalized product.

Customer structure and data-related concerns were also raised. One interviewee noted that much of the business is conducted with smaller customers that have only a few industrial products. Meanwhile, S11 observed that larger customers who might otherwise be ideal targets for scalable offerings are often more restrictive regarding data collection and sharing, even though data is necessary to deliver digital features. Security concerns were likewise highlighted, although S10 stated that the company has been able to convince them by demonstrating certification to quality and security standards.

Across interviews, internal value creation and efficiency gains were frequently emphasized as opportunities. Interviewee S25 reflected that the firm would have had access to a large amount of data if it had started collecting data earlier, without trying to charge the customer. At the same time, S10 noted that while digitalization can generate internal efficiencies, short-term internal KPIs, such as immediate rev-

enue, may be less aligned with contract-based models, such as leasing or predictive maintenance, where value and profits are realized over a longer period.

Finally, interviewee S23 described the competitive landscape as another factor shaping prioritization and speed of adoption. According to S23, digital efforts are currently deprioritized, in part, because few to no competitors have launched scalable digital offerings, and customer willingness to pay remains uncertain. The interviewee added that prioritization may increase once competitors bring more mature solutions to market. Still, some interviewees argued that digitalization is increasingly expected across products and industries, with connectivity approaching a ”hygiene factor” for certain customer segments.

5
Analysis

In this chapter, empirical findings from Chapter 4 are connected to the theoretical framework presented in Chapter 2 with the purpose of explaining how digital retrofitting affects IP strategy by looking into which IP becomes central, how current IP is affected, and how its role changes, and how ecosystem dependencies and new business models reshape the IP strategy. The analysis is structured according to the research questions.

5.1 What New Intellectual Property Emerges with the Introduction of Digital Functionalities?

This section investigates research question 1 by comparing the themes found in Chapter 4 with the theoretical framework in Chapter 2, examining how new IP emerges due to the digital retrofit and what IP protection is needed to safeguard it.

5.1.1 The Application, Ownership, and Access to Data

Among the core shifts is the recognition of the importance of *data*. From the interviews, retrofitted products are expected to generate large amounts of data by adding an IoT device and its integrated sensors, which are then sent, in more or less real time, to the case company's servers. What is described as new is the data's accessibility, since the same kind of data had previously been stored locally in each product's control box. However, because this data had to be manually extracted from the control box, it was previously not used for purposes other than service. Now that the IoT device has been added, this data can be fetched automatically and in real time from anywhere in the world. In line with the literature, extensive data collection is one of the main additions when integrating IoT devices into physical products (Gokhale et al., 2018; Paolone et al., 2022), and among the key changes due to digitalization is the need to manage data efficiently (Holgersson & Granstrand, 2018).

For data gathering, having access to an installed base was cited as a competitive advantage, as a large installed base can generate large volumes of data from a variety of customers and applications, which can be combined to identify patterns and opportunities for improvement. The possibility of harvesting large amounts of data was described as laying the foundation for multiple technical advancements, spanning everything from product development to service innovation and new business

models. Following this, the installed base can be seen as a complementary asset that is difficult to replicate through the lens of Teece (1986, 2018), as it provides access to a broad and continuous stream of usage data while also being difficult to replicate.

From an IP strategy perspective, data as an IP asset was identified in the interviews as requiring management and protection through various mechanisms. For the IP strategy, this implies the importance of contractual clauses that restrict others while enabling the firm to monetize data, specify permitted uses, and limit the risk of data being used for competitive purposes. Second, governance and control of data, where data is shared, and access is restricted to actual needs; for example, DalleMule and Davenport (2017) reports that 70% of employees typically have access to data they should not have. Next, an internal trade-secret discipline that covers the full value chain, from raw data to how insights are used. Lastly, cybersecurity measures prevent external actors from intruding and gaining access to data and trade secrets, thereby serving as an IP protection mechanism in line with the importance of cybersecurity for IP protection according to Almeling (2012) and Ozcan et al. (2023).

What is important to notice is that it is described as an interdependence between multiple digital assets. While some highlighted data ownership as of the highest importance rather than just access to it, others argued that having *access* to the data was sufficient, since the company could extract insights from it through advanced data processing. First of all, high-quality and quantity of data are described as needed for advanced data processing. Then, the quality of data processing depends on the efficiency of internal algorithms and AI capabilities. However, the case company's ability to combine this customer's data with data from other actors may provide a competitive advantage by enabling it to identify more complex and nuanced patterns.

Once the data has been processed, the question of how the emerging insights are used and shared within the organization is also of the essence. From the interviews, multiple uses of the insights derived from data were explained: i) data on how products are used can be used for product development purposes, ii) data on failures and usage can be combined to find patterns on when the product is about to break down, so repairs can be done before actual failure through predictive maintenance, iii) through patterns of failure, service technician could gain insights in what is most probable to have broken down even before visiting the site, enabling the service technician to bring the right tools and spare parts at first visit, iv) insights for new business models, such as usage or results-based or product-as-a-service (PaaS).

While data gathering could pose new digital challenges and require new resources and capabilities for an industrial firm, the firm's success also depends on digital assets that transform data into real value. The addition to the IP strategy could therefore be to include a variety of IP mechanisms that were previously less important, with particular emphasis on trade secrets, contractual agreements, and cybersecurity.

5.1.2 Trade Secrets in Relation to Digital Assets

Views differed on raw-data exclusivity: some emphasized insights over data, while others warned that raw-data access can yield similar insights. The importance of exclusivity can be linked to DalleMule and Davenport (2017), where data on, for example, sales is explained to be of little value, but once plotted on a graph and combined with other data, such as a benchmark, it provides insights into how well sales are going. Building on this example, one could cite interviewees who emphasized the importance of ensuring that the data generated by the product is exclusive, as even basic data processing can reveal patterns that are valuable from a business perspective. Therefore, if another actor gained access to a specific customer's raw data, they would likely be able to derive meaningful insights through their own analysis. Consequently, this indicates that firms should treat data access and sharing conditions as central control points.

The Data Act suggests that raw data should not be considered a trade secret (Mylly, 2024; The European Parliament, 2023). On the contrary, the broader definition of trade secrets from World Intellectual Property Organization (2004) appears to be consistent with statements made by several interviewees, according to whom raw data should qualify as a trade secret, given that it i) raw data can hold value as the basis for business-critical insights and business models, ii) it is not generally known, and iii) is subject to reasonable protective measures such as cybersecurity and access controls. However, mandatory data access rights due to the Data Act (European Commission, 2025) challenge the condition of not being generally known, as customers may request and obtain the data. Even if downstream use of the data is formally restricted (Mylly, 2024), interviewees highlighted limited transparency regarding how the data is shared and used by the firm that received it. Proving that the receiving firm has used the data in a prohibited manner could be especially difficult due to limited transparency and insight into its operations. This tension suggests that formal ownership and classification are insufficient for the firm to control access and usage. Consequently, the implication for the IP strategy is not to resolve whether raw data is a trade secret, but to actively define and govern how it is accessed, shared, and contractually restricted.

Regarding data sharing, interviewees appeared open to collaborating with third-party actors, which is essential in a digital ecosystem (Baptista & Nunes, 2025). However, this creates an interesting tension, as the interviewees describe and perceive the digital ecosystem as more complex, with blurred role boundaries, where partners in some contexts may also be customers or even competitors. Since digital collaborations often involve data sharing in one form or another (Asadullah et al., 2018), interviewees' views emphasize the importance of ensuring that data that could be considered trade secrets are handled and shared with care. One requirement for information to qualify for trade secret protection is limiting who has access to the information and how many actors can access it (World Intellectual Property Organization, 2004). As the number of actors with access increases, the risk of unintended leakage rises, and the information may potentially no longer qualify as a trade secret because too many actors have access to it. Therefore, it could be argued that this

further complicates the collaborative environment the firm must navigate, in which the criteria for what should be kept secret must be defined and known to employees handling the data. In accordance with Ozcan et al. (2023), contractual agreements, as part of the IP strategy, are an important factor in limiting how shared data may be used by the receiving actors.

A strategic implication of digital retrofitting is that digitalization makes trade secrets easier to transfer without authorization (Almeling, 2012), thereby increasing the need to detect and respond to intrusions and unauthorized leakage. Almeling (2012) highlights how digital storage and network accessibility increase the risk of leakage, implying that NDAs and access restrictions must be complemented by additional protection mechanisms to maintain the secrecy of digital assets. This, in turn, increases the need to protect and monitor the digital environment through logs and real-time surveillance of data flows to track digital footprints. The importance of strengthened digital protection was also highlighted by the interviewees, indicating that protecting new IP is a matter not only of legal but also of technical concern, which aligns with (Ozcan et al., 2023). Cybersecurity could therefore be understood as a technical protection mechanism of IP, enabling secrecy to be effective in digital environments. For an industrial firm, developing such capabilities may require larger investments in new assets and competencies outside its traditional core.

Historically, IP protection was described as relying primarily on patents, which require disclosure, whereas digital assets are more often associated with trade secrets and controlled access. However, the interviews provided limited insights into the human and organizational dimensions of trade secret protection. Almeling (2012) highlights that one of the main risks of trade secret leakage stems from employees. As employees increasingly change employers, trade secrets may be transferred either unintentionally, due to a lack of awareness of what constitutes a trade secret, or intentionally. This risk is further reinforced in collaborative settings, as Hurmelinna-Laukkanen and Puumalainen (2007) argues that employees acting as gatekeepers or receptors in partnerships are particularly critical, as they are exposed to inter-firm knowledge flows and may carry valuable insights across organizational boundaries. While interviewees primarily emphasized technological protection and contractual control of data, these perspectives suggest that IP challenges are also organizational, as internal processes and employee transitions become central to safeguarding trade secrets.

Ozcan et al. (2023) adds an organizational view on trade secret protection, noting that management and understanding of trade secrets are often lacking even in innovative firms. Ozcan et al. (2023) emphasizes the need for both resources, such as access controls, routines, and employee training, and for flexibility through dynamic capabilities to sense, seize, and reconfigure trade secret protection as threats evolve. Although a need for increased organizational capabilities was not mentioned by the interviewees to any large extent. For an industrial firm undergoing digital transformation, acquiring these resource-based mechanisms becomes an important aspect of IP strategy. This is especially true as firms must continuously reassess

what constitutes a trade secret, particularly since employees are a primary source of trade secret leakage (Almeling, 2012). Consequently, digitalization should be viewed not only as a cybersecurity challenge but also as an organizational one. This implies that as protecting IP increasingly relies on secrecy, firms must complement technical and legal mechanisms with organizational capabilities. In practice, this includes HR-driven processes such as on-boarding and off-boarding routines (Ozcan et al., 2023), employee awareness of confidentiality (Almeling, 2012), and internal governance structures that limit unintended knowledge diffusion (Almeling, 2012; Ozcan et al., 2023).

Figure 5.1: Governance-based control of trade secrets in digital environments. The figure illustrates how value from data is protected through layered governance mechanisms, where contractual, technical, and organizational controls restrict access and usage under external pressures such as the Data Act and ecosystem data sharing.

To summarize, protecting trade secrets becomes a core issue for the IP strategy in the context of digitalization. Maintaining trade secret status also shifts from being solely a legal concern to requiring increased cybersecurity measures to protect against unauthorized access. Increased data sharing, enforced by regulations such as the Data Act, and increased collaboration in data-sharing contexts reduce the ability to maintain data and knowledge exclusivity, increasing the need for efficient control of access, sharing, and the flow of information. As illustrated in Figure 5.1, data and derived knowledge could seemingly gain protection through a layered approach that combines contractual, technical, and organizational mechanisms to control how the data is shared and used in practice.

5.1.3 Contracts as Core IP Governance Mechanisms in Digital Environments

A central theme in the empirical findings is that contractual agreements have become a key mechanism for appropriation compared with earlier periods. Now, contracts

are understood to serve not only as a commercialization approach but also as a means of managing IP by defining who can do what, with what resources, and under what terms. This shift is closely connected to the servitization logic emphasized in the empirical findings. Where digital functionalities such as predictive maintenance and remote control depend on continuous access to data and a clear division of responsibilities between the customer and the firm. In this context, contracts become critical for regulating access to data and safeguarding control over digitally enabled service capabilities.

However, interviewees also stressed that contracts introduce new challenges. For contracts in collaborative settings, one interviewee highlighted the difficulty of designing agreements that simultaneously enable collaboration and protect against competitors. This becomes critical for data, as ownership is often unclear, while access, exclusivity, and rights of use are considered essential to enable value creation. This implies that the case company must make informed, selective decisions about what to share and with whom. Such selective openness aligns with (Peters et al., 2013), who argues that co-creation and innovation require some degree of openness, while increased openness may weaken a firm's ability to protect future opportunities. This indicates that the role of contracts shifts from merely regulating collaborations to actively setting boundaries for information flows, thereby acting as a central mechanism for maintaining secrecy within ecosystems. The theoretical view, therefore, reinforces the interviewees' emphasis on informed, selective boundary-setting in contractual design. Finally, Teece (2018) indicates that formal rights are rarely sufficient for value capture on their own, which coheres with our findings that contracts and secrecy become important control points for digital assets.

Accordingly, the IP strategy in the retrofitting context could benefit from using *contracts, licensing, and NDA* agreements to secure appropriability within ecosystem relationships. On contractual design, Balice et al. (2026) highlights that effective protection of trade secrets in an international context requires consistent contracts across different jurisdictions. In particular, companies should align NDAs and confidentiality agreements across regions to avoid a "weakest-link" problem, where weak protection in one part of the value chain can undermine overall protection. This highlights that contracts are not only about what is to be regulated, but also how and where these regulations can be enforced. This shows that contracts in digital ecosystems are not only tools for sharing data, but also an important part of a company's IP strategy. Balice et al. (2026) implies that clauses on confidentiality, data use, governing law, jurisdiction, and dispute resolution should be clearly designed with enforcement in mind, as these clauses affect where and how a company can enforce its rights if a trade secret is misused.

A recurring risk raised by interviewees is potential disintermediation, where the case company may move further away from the customer interface and be displaced by a supplier or another ecosystem actor. This risk emerges from increased data sharing and openness, in which multiple actors have the opportunity to position themselves

closer to the customer. This concern aligns with ecosystem and platform research, which emphasizes that value capture in digital ecosystems often depends on control over interaction points, in this case particularly the customer interface, rather than the solely on the product itself (Cusumano et al., 2019; Valdez-De-Leon, 2019) In this context, contracts serve not only as commercial arrangements but also as governance instruments that structure interdependence in relationships (Holmlund & Törnroos, 1997). Contracts in such contexts help control critical resources such as data, interfaces, and customer relationships in an otherwise highly dynamic environment.

By establishing, using, and monitoring contractual terms, the case company can remain connected to both suppliers and end customers, gain better insights into market movements, and capture evolving customer needs. Contracts thus function as control points for coordinating interactions and managing complexity in the collaborative environment.

5.1.4 Limits of Patenting in Digital Environments

While patents were described as the primary means of appropriating value from inventions and blocking competitors during the mechanical and electromechanical eras, their efficiency in the digital environment was questioned and met with skepticism by the interviewees. When patents were discussed, it was often in connection with the patenting of data-processing functionalities, especially algorithms for use in predictive maintenance and product development insights. Most interviewees emphasized that patenting, for example, an algorithm, risks disclosing too much information, potentially enabling competitors to invent around the patent more easily and thereby reducing its effectiveness as an IP mechanism for blocking competition. This concern is also consistent with the literature on the downsides of patents, such as Arundel (2001). Holgersson and Wallin (2017) adds that the strategic choice among patents, secrecy, and strategic disclosure depends on the firm's ability to appropriate value from an invention and maintain freedom to operate. In this context, the disclosure requirement associated with patenting seemingly weakens appropriability for digital inventions when the invention is relatively easy to circumvent. Arundel (2001) further suggests that secrecy may be a more effective mechanism in situations where inventing around is relatively easy, if the invention can be kept secret. Furthermore, B. Hall et al. (2014) explicitly notes that interest in patenting software is generally low due to the relative ease of inventing around software patents, and that lead time is often considered a more effective mechanism for appropriating returns from software inventions.

Based on the interviews, IP infringement in digital contexts is described as more difficult to detect because software is often concealed within a "black box", and one usually does not have access to another actor's source code. Consequently, this indicates that digital retrofitting affects what patents can realistically achieve when infringements become harder to identify and prove. Patents are not self-enforcing; they require costly monitoring and, when necessary, prosecution initiated by the

patent owner (Teece, 2018). If potential infringements are increasingly difficult to detect, the associated costs in time, expertise, and resources may outweigh the expected returns from litigation, including any financial compensation awarded. The outcomes of those patent litigations involving software were also described by some interviewees as more uncertain than those in hardware-based litigation. This challenge may be of particular consideration in jurisdictions where damages for IP infringement are relatively low. As a result, this further reinforces the implication of a layered IP portfolio strategy that distinguishes between patents in the mechanical/-electromechanical and software/data layers, given the differences in their relative effectiveness.

An additional observation from the interviews was that the increasing number of actors and the growing volume of patents make it more difficult to assess novelty and conduct prior art searches. As the firm moves into the digital domain, it also enters industries characterized by large and well-established patent holders, such as Apple, Ericsson, and Microsoft. In this context, patenting digital inventions becomes less about blocking imitation and more about managing exposure to patent disputes. Consistent with Teece (2018) and Somaya (2012), patents can serve as a defensive mechanism against litigation and as a tool for dispute resolution (B. Hall et al., 2014). In particular, patent portfolios may be used in cross-licensing negotiations to gain access to critical technologies controlled by other actors (Holgersson & Wallin, 2017; Teece, 2018). Importantly, this does not imply a simple one-to-one exchange of patents. Rather, patents constitute one bargaining resource among several, alongside complementary assets, integration capabilities, and other strategic resources.

As highlighted by Somaya (2012) and Shapiro (2001), patent portfolios can also provide freedom to operate, especially in complex technological environments where multiple interdependent technologies must be combined. This logic is particularly relevant in digital retrofitting contexts, where firms depend on external standards, cloud infrastructure, APIs, and other platform technologies that are often controlled by third parties. Therefore, patents in the digital layer are not only used to protect individual inventions but increasingly function as negotiation tools within the broader ecosystem. This indicates a shift in the strategic role of patents: while their effectiveness as exclusionary tools may be reduced in digital contexts, their importance increases in terms of enabling access, managing dependencies, and securing participation in complex technological ecosystems.

Regarding the pace of innovation, one should also consider the duration of protection, as a patent's 20-year term may be too long for software's lifespan. Patents provide exclusivity for 20 years from the filing date (Granstrand & Holgersson, 2015), but in digital retrofitting contexts, digital functionality is described by interviewees as ongoing and nearly indefinite through continuous updates in short cycles. This differs from hardware development, where the launch of a new version of a specific product type was explained to take several years, and the lifespan of each product could exceed 20 years. Patents may therefore be filed more selectively for stable parts of digital inventions, while components subject to continuous iterative innovation

may be better suited to secrecy and lead-time advantages. Building on interviewees' statements that the digital environment moves faster than the electromechanical one, the findings point toward using multiple patent strategies depending on which technology layer is to be protected. In addition, the electromechanical and digital environments differ in rivalry intensity and in the number of patents granted per year, according to the interviewees.

The appropriability conditions, as follows, seem to differ between the electromechanical layer and the software/data layer from a patenting perspective. A layered IP approach, combining selective patenting with secrecy and contractual controls, therefore aligns with research showing firms' reliance on a broader IP strategy of protection mechanisms (B. Hall et al., 2014; Holgersson & Granstrand, 2018). Additionally, Arundel (2001) suggests that secrecy can be particularly useful during development and pre-market phases. This implies that digital assets such as software and algorithms might be best protected through secrecy during development, and later complemented by patenting or other mechanisms closer to market launch, hence introducing a time perspective to the patenting/secrecy choice.

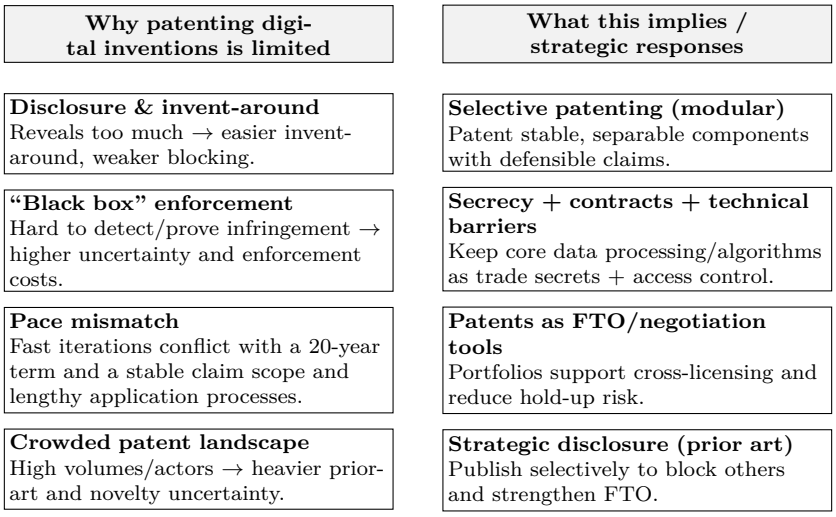

Figure 5.2: Summary of the limits of patenting digital inventions in retrofitting contexts.

The choice between patenting and secrecy becomes a strategic decision for the IP strategy. Practically, this decision can be guided by criteria summarized in Figure 5.2 such as: i) whether the invention is easy to invent around if publicly disclosed, ii) the speed of the development for the invention, iii) whether disclosure damages appropriability or increases imitation risk, and iv) whether patents are needed in the relevant IP environment as a negotiation tool or defensive barrier. In retrofitting contexts, this implies that algorithms, data, and software features/processes are often better protected through secrecy and contractual agreements, as value is frequently embedded in processes rather than in a standalone artifact. Secrecy tends to work better for process inventions as they are harder to observe and therefore to imitate (Arundel, 2001).

In the context of digital retrofitting, many value-creating inventions, such as data-processing methods and operational routines, are process-oriented, which strengthens the case for relying on secrecy combined with technical barriers (Arundel, 2001; Holgersson & Wallin, 2017). However, this increased reliance on secrecy introduces an important strategic trade-off. Unlike patenting or strategic disclosure, trade secrets do not create prior art and therefore do not prevent other actors from patenting similar inventions (Holgersson & Wallin, 2017). As a result, there is a risk that a competing actor independently develops and patents a similar solution, thereby restricting the firm's ability to use its own internally developed technology. Following Holgersson and Wallin (2017), this highlights the importance of considering not only value appropriation but also freedom to operate when choosing between secrecy, patenting, and strategic disclosure.

Building on these implications, the empirical findings suggest that the issue is not a lack of interest in patenting digital inventions, but a shift in what is considered *worth* patenting from an appropriability perspective. When patenting offers weaker exclusion effects, or when disclosure is perceived to increase imitation risk, as several interviewees emphasized, firms appear to rely more on alternative mechanisms such as secrecy, consistent with B. Hall et al. (2014). Overall, the findings support a layered and selective patenting approach combined with secrecy. This, in turn, motivates a modular IP strategy in which patents are used for separable, stable components, while core processes and know-how are kept secret, which aligns somewhat with the logic of IP modularity discussed by Henkel et al. (2013).

5.2 How does Digital Retrofitting Change the Role of Existing IP?

This section analyses the findings in relation to research question 2 by examining how current IP is affected by the digital retrofit. The focus is on how traditional protection, such as hardware-related rights and knowledge, changes in importance and role.

5.2.1 Digital Complementary Assets & Value Enhancement

Digital retrofitting increases the importance of digital IP assets by investing in connectivity, software, and data-driven capabilities, according to the interviewees. At the same time, the interviewees agreed that the ability to create value across the entire value chain and capture profits from it still depends on a robust product foundation. In line with Oliva and Kallenberg (2003), products with long lifespans are especially suitable for enhancement through services, which helps explain why the product remains central even as new digital layers are added. As one interviewee stated, the effectiveness of digital enhancements is, to some degree, dependent on the product's quality and functionality. In the case of providing a product-as-a-service (PaaS) or an outcome-based agreement, the aim is for the product to break

down as infrequently as possible, since services in these business models generally incur costs and do not generate income for the supplier (Oliva & Kallenberg, 2003; Tukker, 2004). Therefore, having a solid foundation and well-functioning products is essential, even when they are retrofitted with digital solutions. This indicates how digital retrofitting changes the role of existing IP: rather than being replaced, legacy electromechanical and mechanical know-how and IP become a foundation for the digital additions.

From a complementary asset perspective, the new digital functionalities align with Ceccagnoli and Rothaermel (2016) and Teece (1986, 2018), who emphasize the role of such assets in profiting from innovation. Here, the IoT device and software can be seen as co-specialized assets (Teece, 1986), as their value depends on integration with the physical product: the digital components have little standalone value, while the product cannot generate continuous insights without them. This co-specialization introduces important implications for ownership and control across both layers, including the IoT device that bridges the physical and digital domains (Paolone et al., 2022). According to Teece (1986, 2018), ownership of both assets becomes particularly critical in contexts characterized by weak appropriability regimes. If another actor were to gain control over one part, it could significantly reduce the case company's ability to capture profits. This concern was echoed by interviewees, who noted that there is essentially nothing preventing another actor from placing a simple IoT device with sensors on the physical product. One interviewee explained that, although such an actor would likely be unable to control the product due to the encrypted control box, they could still generate and collect data and compete by delivering services and selling insights. As a result, value capture is less dependent on traditional exclusionary IPRs and more on relationship and control-oriented mechanisms such as secrecy, contractual governance, and the management of complementary assets (including data access and service interfaces), which is consistent with Teece (1986) and Holgersson and Wallin (2017)'s view of the importance of complementary assets. In this retrofitting context, key complementary assets and resources therefore include, for example: i) who provides the physical product, ii) who gathers and processes the data generated from the product, and iii) who supplies associated services.

While services were part of the business prior to digitalization, interviewees highlighted that data gathering and processing are the primary additions introduced through digital retrofitting. This is consistent with Kowalkowski et al. (2024), which states that digital technologies enable firms to collect and analyze large amounts of operational data. That then could be turned into actionable service intelligence. Thus, although the case company's foundation remains rooted in tangible industrial products, its ability to capture profits over time increasingly depends on securing control over the digital components that enable superior service delivery. However, as one interviewee noted, customers still primarily value a well-functioning, well-constructed product, indicating that service capabilities are not enough. This suggests that existing know-how and IP from the electromechanical and mechanical era continue to play a foundational role, even during digital retrofitting - particularly

given that a transition toward a PaaS business model has not yet been fully realized.

With the introduction of digital complementary assets, the case company appears to operate across two distinct life cycles characterized by different appropriability regimes. Gemser and Wijnberg (1995) argues that both the motivation to engage in innovation networks and their effects on appropriability depend on the stage of the industry life cycle. In early stages, high uncertainty and the absence of a dominant design make imitation easier (Teece, 1986). Firms may therefore participate in networks to access emerging knowledge more rapidly, even at the risk of knowledge spillovers (Gemser & Wijnberg, 1995). In more mature stages, however, firms tend to emphasize differentiation and control over their innovations. In this case, two co-existing life cycles can be identified. First, the electromechanical and hardware-based product development appears to be in a mature phase, where patenting primarily concerns incremental improvements rather than radical innovation, consistent with later industry life cycle stages (Teece, 1986). Second, the digital domain, encompassing IoT devices, data, platforms, and integrations, remains in an earlier stage, characterized by high uncertainty and a lack of dominant standards (Gemser & Wijnberg, 1995). These regimes overlap in integrated offerings such as Product-as-a-Service (PaaS), which rely on both physical products and digital capabilities. Consequently, both empirical findings and prior research suggest the need for a layered IP strategy that accounts for differing levels of competition and uncertainty across physical and digital innovation layers.

An interesting finding from the interviews is that neither copyright nor design rights were mentioned as ways of protecting digital assets. This may suggest that copyright is not perceived as an important strategic mechanism, since it arises automatically and is therefore possibly taken for granted. However, its strategic relevance may increase as the case company develops more code in-house, making the risk of code copying a more salient IP concern. As for design rights, one reason they may not have been raised is that user interfaces and web design in agile development environments change frequently. This makes design registration both costly and difficult to justify. In addition, enforcing design rights against infringement may be perceived as relatively weak, since potential imitation can often be avoided through minor design modifications. Overall, these findings reinforce the thesis pattern: in the digital layers, there is a strong preference for flexible mechanisms of IP control, such as contracts, secrecy, and technical barriers, rather than formal IPRs.

5.2.2 The Power and Risk of Trademarks

A recurring theme among the interviewees is that *trust* from customers becomes increasingly central when a firm that traditionally manufactures physical equipment introduces digital functionalities. If the firm cannot meet expectations for its tangible products, adoption may be hindered, as it becomes more difficult to convince customers to proceed with digitalizing their products, in which sensitive data is stored, and remote operation is enabled. This aligns with the determinants of service quality identified by Parasuraman et al. (1985), in which reliability, compe-

tence, credibility, and security are key evaluation aspects. This is also consistent with trademarks functioning not only as indicators of origin for goods but also for services (World Intellectual Property Organization, n.d.-b), as well as an indication of quality (World Intellectual Property Organization, 2004). Accordingly, a well-known trademark and its associated positive reputation can become particularly valuable when introducing digital solutions within a traditional product segment. Digital retrofitting, therefore, seems to change the role of the trademark by shifting it from being primarily associated with physical product quality to also serving as a credibility-enhancing and risk-reducing mechanism for digital functionalities and services.

As value increasingly shifts from mechanical hardware to digital offerings, the trademark serves as both legal protection and a market-facing interface for value capture. In collaboration with digital partners, the case company can mitigate disintermediation and reputational spillover by contractually ensuring that the customer-facing interface is branded and controlled by the company. A practical implication could be to ensure trademark coverage for digital services through service marks. From an appropriability perspective, the trademark and the trust it signals can therefore be understood as an appropriability mechanism in light of Teece (1986)'s concept of complementary assets. This becomes particularly important from an IP strategy perspective, as trademarks can be renewed, thereby retaining value over time (Granstrand & Holgersson, 2015). The importance of trust also strengthens the rationale for brand architecture choices, such as using sub-brands to isolate the core brand from reputational risks in the event of cybersecurity incidents, as noted in the interviews.

Because customers must rely on the provider when purchasing digital solutions and services due to their intangible nature (Parasuraman et al., 1985), the consequences of mistakes or incidents can be greater after retrofitting. Once customers have entrusted the company with handling and collecting sensitive data, incidents that compromise confidentiality or the product's control mechanisms may significantly undermine that trust, as mentioned in the interviews. When confidentiality or control mechanisms are compromised by incidents such as IP theft, Blaskovic et al. (2023) notes that these events may also damage a firm's brand. As one interviewee described, breaking a product only affects the specific product and any tangible goods in its area, whereas breaking into a central software system or database could grant access to years of sensitive data from multiple sites globally, potentially spanning multiple customers. In line with Almeling (2012), trade secrets and confidential data become more accessible through digital means, increasing risk by easing transferability and distribution. Once an intrusion becomes publicly known, it may not only reduce trust in the company's digital capabilities but also damage the trademark's reputation more broadly.

5.2.3 The Role of Hardware Patents in Digital Contexts

Interviewees described the role of patents for mechanical and electromechanical inventions after digitalization as twofold. Some argued that patenting incremental, minor innovations remains important to prevent competitors from implementing similar solutions. Others highlighted that the industrial product is mature, with many foundational patents expired, implying limited value in protecting further minor improvements. From a patent strategy perspective, patents can support defensive positioning, for example, through portfolio-based deterrence and settlement leverage, and can also be used offensively via enforcement actions (Somaya, 2012), although litigation is often costly and uncertain. Further, B. Hall et al. (2014) notes that patents can provide value through portfolio-based dispute resolution, even when their direct exclusionary effect is limited. Consequently, the decision to patent depends not only on the characteristics of the invention, but also on how effectively patents contribute to defensive positioning and value capture, consistent with Teece (1986) and the strategic choices between patenting, secrecy, and disclosure described by Holgersson and Wallin (2017). While patents may support defensive positioning, interviewees emphasized that preventing disintermediation by upstream actors is important; in many cases, these actors are more likely to rely on contractual restrictions rather than patent exclusion alone, thereby rendering patents less valuable in such situations.

The implication is that electromechanical and mechanical patents, after digital retrofitting, still play a role in the electromechanical and mechanical layers of the IP strategy. The empirical evidence points to the physical product, and the installed base serves as the foundation for the newly introduced digitally enabled offerings; hence, it is a high-importance asset. The main difference from the era before digitalization is that the physical product can no longer be seen as the primary differentiator from competitors, but rather as a means to secure the physical assets needed to deliver the entire new offering. This indicates that one of the core purposes of the electromechanical patents is to determine which parts are essential for protecting and supporting the digital layers of the IP strategy and business model. Moreover, patents can be uncertain in practice, as they are not self-enforcing. Enforcement requires detecting infringement (Teece, 2018) and pursuing litigation at the rightholder's expense (B. Hall et al., 2014), which makes outcomes both costly and difficult to predict. Some interviewees highlighted that patents are mainly sought for minor improvements. The question of whether it is worth patenting may also become relevant. To conclude, the usability of mechanical/electromechanical patents after retrofitting is seemingly moving towards a more selective patenting approach to secure critical physical components, rather than the main point of differentiation and exclusion.

5.3 How do Evolving Ecosystem Interdependencies Influence Intellectual Property Strategy?

This section relates to research question 3 by connecting the empirical findings to the theoretical framework on how digital ecosystems and platforms, and their control, affect IP strategy during retrofitting.

5.3.1 Third-Party Modules in Platforms & Responsibility

The empirical findings highlight two distinct ecosystem configurations, each characterized by different actors, purposes, and control mechanisms, which in turn impose different demands on the IP strategy. The first configuration could be described as a *closed firm-customer ecosystem*, where the main actors are the focal firm and the end customer. A direct connection between the focal firm and the customer is essential for delivering PaaS. Value creation revolves around delivering a reliable, integrated product-service offering. In this setting, the company maintains a relatively strong control over core assets, including the physical product, embedded software, and customer relationships. Something consistent with what the literature characterizes as a relatively tight appropriability regime, in which the focal company has greater control over how value is created and captured (Teece, 1986). The main opportunities lie in capturing value through direct service provision, leveraging the installed base, and utilizing product-generated data for internal optimization and incremental innovation. Control in this configuration is achieved through mechanisms such as ownership over product architecture, customer contracts, switching costs, and control over data access and insights, allowing the firm to preserve a relatively closed and coordinated structure.

In contrast, the second configuration reflects a more *open platform ecosystem*, where value creation involves a broader set of actors, including third-party developers, platform providers, system integrators, and customers. Here, the purpose shifts from delivering a standalone offering to enabling complementary innovation and expanding the platform's functionality through external contributions. This configuration creates opportunities for scalability and increased customer value through modular add-ons to the company's digital platform and integration with third-party systems. Conversely, it reduces direct control, as critical resources such as data flows, interfaces, and interaction points are distributed among multiple actors. This can be further understood from Teece (2018), which highlights that control over the platform's central components, rather than separate innovations, is decisive for value capture. At the same time, platform literature tends to emphasize openness and the role of complementors as mostly positive (Bresciani et al., 2021; Cusumano et al., 2019); meanwhile, the empirical results show that increased openness also increases the risk of disintermediation and value leakage. Therefore, control must be done through more complex governance mechanisms, such as licensing structures, data access agreements, and contractual restrictions that regulate collaboration and limit value leakage. While the closed ecosystem allows for tight control but limited scalability, the open ecosystem enables value expansion at the expense of increased

dependence and risk of disintermediation. The co-existence of these two configurations requires an IP strategy that balances closure and openness.

The emergence and potential of new collaborative innovations are among the most emphasized takeaways from interviews about the opportunities the digital ecosystem offers. Interviewees highlight the potential for third-party actors to complement tangible products with digital functionalities via the case company's digital platform. This aligns with ecosystem literature, which emphasizes that value is co-created through complementary innovation and platform-based interactions (Bresciani et al., 2021; Teece, 2018). Although expanding the platform through digital cooperation increases the product's value, one must also consider the issues of adding third-party actors to the platform. The platform's quality and image depend not only on the foundation the company is responsible for, but also on the platform's overall usability and perceived quality. Prior research also establishes this by emphasizing that platform owners remain responsible for the overall quality and performance of the ecosystem, even if it relies on external complementors (Cusumano et al., 2019; Valdez-De-Leon, 2019). If third-party modules available on the platform do not meet customers' expectations, the platform owner is likely to be adversely affected. In line with service quality theory, perceived quality presumably depends on the gap between expected and delivered service, making the platform particularly vulnerable to external shortcomings (Parasuraman et al., 1985). To take it one step further, in the event of a cybersecurity intrusion or incident caused by a third-party module, the platform's overall security would likely be questioned rather than the third-party integrator. Following this underscores the importance of cybersecurity regulations and requirements to ensure compliance with expected security and quality standards for digital features added by third-party actors. This further highlights the importance of governance mechanisms such as contractual agreements, standards, and cybersecurity requirements to ensure quality and compliance across the ecosystem and to protect the platform's value and the reputation of its trademark (B. Hall et al., 2014; Teece, 2018).

5.3.2 Interoperability, Standards & IP Dependencies

Some interviewees stated that their customers often request that digital functionalities be integrated into their existing platforms and systems. One of the main reasons for this was the reduction in the number of platforms and webpages customers need to engage with on a daily basis. This highlights the importance of interoperability, as customers seek to integrate digital functionalities into their existing systems to reduce complexity and platform fragmentation. From a broader perspective, this user-driven demand for integration aligns with prior research on digital platforms, which emphasizes the importance of enabling external connectivity and accessibility for ecosystem participation (Cusumano et al., 2019; Valdez-De-Leon, 2019). As exemplified by one of the interviewees, if you have an iPhone, MacBook, and AirPods, you would probably be looking for - or even require - your next technological products to be able to connect and function within your Apple ecosystem. However, the demand for interoperability could both introduce new opportunities and new risks.

Regarding opportunities, having a product or platform that integrates easily with other systems could be an advantage, as such products could become more attractive to customers and partners. This aligns with Teece (2018), which highlights that platforms rely on complementors and interoperable structures to expand ecosystem value. Additionally, once integrated, it could provide some stickiness by increasing switching costs. On the other hand, risks arise when the company becomes part of another platform rather than maintaining control, indicating a reduction in control and the need to comply with the platform owner's requirements. Integrating into another party's platform, therefore, creates potential IP dependencies, as the platform owner might require contractual agreements for integration, licenses, and other contractual arrangements that shape how the company can deliver its services. Such dependencies highlight the importance of maintaining FTO in ecosystems, and managing interdependent IP through contractual mechanisms (Granstrand & Holgersson, 2013).

One risk that emerges when transferring data to a third-party platform is the extent to which the platform owner can use the data, especially when integrating with partners that, in other contexts, are seen as customers or competitors. This dynamic could be understood as a 'learning race' described by Ceccagnoli and Rothaermel (2016), in which actors aim to extract as much knowledge as possible from interactions while limiting their exposure. To handle this, contractual agreements on data handling and use once again play a significant role in controlling what knowledge and information is shared in collaborative environments. Here, agreements on how and for what purposes they are allowed to use the data for could be of the essence, for example, to reduce the third party's ability to train their algorithms with the data and ensure that the data is not used in any other way that directly or indirectly competes with the company.

Regarding interoperability, the question of standards was discussed by some interviewees. While standards were described to ensure compatibility with, for example, cybersecurity requirements, other standards were described to facilitate easier integrations between systems. The importance of the ease of integrating different systems to co-create value through standards is also highlighted in Holgersson and Granstrand (2018). This could, from one point of view, make it easier to be interoperable with a large number of systems, while, from another perspective, it could also indicate that it is easier to shift to other actors. While standards can facilitate integration, one interviewee emphasized their dual nature: they enhance interoperability but also require coordination among multiple actors with differing interests, increasing complexity and potentially reducing agility and development speed. Following, choosing between which standards to be a part of and not could be the difference between being at the forefront or having to adapt to other parties in the standard-setting alliance.

When retrofitting depends on or is associated with standards, protocols, API requirements, etc., some patents may become essential for compatibility. Shapiro

(2001) states that this kind of dependency might create a hold-up risk, especially if licensing requirements are left unclear by the IP owner, as they might require substantially higher financial compensation, thereby creating an ex-post hold-up. From an IP strategy perspective, this indicates that an industrial firm undergoing digital transformation might benefit from taking into consideration: i) map the standard essential patent landscape, ii) participate in standard setting alliances to be a part of and influence decisions, iii) emphasize the need for clear licensing requirements and agreements, through for example a FRAND perspective (Granstrand & Holgersson, 2012; Shapiro, 2001), in the standard setting alliance.

In summary, the interviews show that interoperability is an increasing requirement among customers, as they want their digital functionalities across as few platforms as possible. Therefore, the question of integration capabilities becomes a factor of compatibility and becoming a preferred supplier. At the same time, new dependencies on API agreements, licenses, and standards could reduce the company's control and affect its FTO. Standards could therefore be seen as both an enabler of adoption and a new risk due to lock-in effects and potential hold-ups. These can be understood as control points in the ecosystem, including control over APIs and interfaces, data access, participation in standards, and customer relationships. Consequently, IP strategy must actively address these control points through mechanisms such as contractual agreements, licensing, and governance of interfaces and data. Table 5.1 summarizes the central control points and connects them to what value they might create, the associated risks, and how to manage them through IP mechanisms.

Table 5.1: Ecosystem Control Points: Value Creation, Risks, and IP/Governance Responses

Control point	**Upside (value creation)**	**Downside (value capture risk)**	**IP/governance response (practical)**
APIs / Interfaces	Enables interoperability, easier integration into customer systems, supports ecosystem participation.	Loss of control due to third-party platform integration and disintermediation.	API governance (permissions/scopes), modular architecture, contracts restricting use and downstream actions.
Data Access	Enables analytics, service innovation, and customer value creation.	Data leakage enables competitors to build capabilities and lose differentiation.	Data contracts (usage restrictions), access control, trade secrets, and monitoring.
Standards Participation	Facilitates compatibility and large-scale adoption, reduces integration friction.	Dependency on standards, patents, potential hold-ups, and reduced differentiation.	Standards strategy, licensing management, selective patenting.
Customer Interface / Relationship	Direct access to customer needs, control over service delivery and value capture.	Risk of disintermediation if partners access the customer or interface layer.	Contractual restrictions on partner access, control of interface, branding, and service ownership.

5.3.3 Evolving Partnerships & Strategic Dependencies

The empirical findings show that the collaborative environment introduces significant role uncertainty, in which actors can act in multiple roles. This creates not only strategic uncertainty but also implications for the IP strategy, as partner roles are not fixed and may shift in the future if access to data, knowledge, and integration increases. Interviewees commonly spoke about how collaboration often requires sharing data and integrating systems, but such interactions may also strengthen the recipient's capabilities and bring the recipient closer to the customer. One important aspect in this scenario is for the focal firm to leverage its relationships and scale to stay close to the customer. From an IP strategy perspective, it is important to strike the right balance in information sharing. The dynamic can be understood by two complementary lenses. First, Ozcan et al. (2023) emphasizes that strategic disclosure is an important consideration in ecosystems, achieved through withholding information and delaying sharing. Second, Ceccagnoli and Rothaermel (2016) offers another perspective, describing innovation alliances as a "learning race" in which each actor seeks to obtain as much information as possible from the others. In such settings, value leakage does not necessarily occur through direct imitation but through gradual capability-building as other parties internalize knowledge, capture customer relationships, or enforce standards. That may ultimately destroy the innovator's once-held differentiation, even in the absence of formal IP infringement.

This risk is particularly pronounced in digital ecosystems, where control over customer interfaces, data flows, and standards could shift power away from the focal firm towards other ecosystem partners. To mitigate the risk, the focal firm must carefully govern both information access and customer relationships within collaborations. This implies the use of contractual mechanisms and data access rules, which could limit partners' visibility into customer-specific information and restrict their direct interaction with end customers when appropriating (Granstrand & Holgersson, 2013; B. Hall et al., 2014). By doing so, the focal firm transforms the IP strategy from a defensive protection tool into a governance mechanism, aimed at controlling the points in 5.1. Shaping the structure of collaboration, ensuring that value is appropriated by themselves.

Ceccagnoli and Rothaermel (2016) describes three strategic alternatives for commercializing innovation: i) self-integration, ii) co-development through alliances or partnerships while retaining ownership of critical complements, or iii) licensing to capture at least part of the value when imitation and competition are likely. When specialized complementary assets are controlled by external actors, alliances often become necessary, requiring sufficient appropriability to safely share knowledge and information. Something that is further emphasized in Teece (1986), who argues that value capture depends critically on control over complementary assets. When they are then controlled by external actors, the risk becomes that they appropriate value instead. As highlighted in platform contexts, complementors are essential for value creation, but also introduce strategic dependencies that must be carefully governed (Teece, 2018). This aligns with empirical findings, which highlight the need to collaborate without losing control over key assets and value-capture mechanisms. In

retrofitting contexts, where alliances are explained to be of importance, contracts and data access become central governance mechanisms for enabling commercialization while maintaining control. Taken together, this suggests that IP strategy in digital ecosystems shifts from protecting isolated inventions toward managing controlled openness across organizational relationships.

5.4 How does Digital Retrofitting Drive firms to Reconsider the Relationship Between their IP Strategy and their Business Model?

This section explores research question 4 by examining how the empirical findings align with or diverge from the theoretical framework. Implications for IP strategy arising from the introduction of new business models, such as PaaS, are discussed, with data accessibility being important alongside contractual agreements, interfaces, and complementary assets.

5.4.1 Business Model Transformation & Customer Value

Beyond customer-specific drivers, broader market trends are increasingly shifting toward subscription-based business models and the emergence of anything-as-a-service (Kowalkowski et al., 2024; Vandermerwe & Erixon, 2023). However, as noted by the interviewees, few - if any - comparable models have been introduced in the industry under investigation. According to the interviewees, one key reason customers may be interested in a PaaS model is their limited willingness to maintain such products, a point also raised in Tukker (2004). Transferring this responsibility to a service provider can therefore be appealing, as it reduces the time customers need to spend managing their industrial products. In addition, several interviewees highlighted customers' preference for more predictable costs, which are otherwise difficult to achieve when expenses depend on uncertain lifespans, service needs, and replacement cycles. Under a result-based contract, customers can instead anticipate costs over the coming years, providing predictability and a greater sense of control (Oliva & Kallenberg, 2003). From a revenue perspective, this shift implies that revenue generation would increasingly rely on contractual agreements and customer relationships rather than on selling physical artifacts (Kowalkowski et al., 2024). Consequently, contractual design becomes a key mechanism for aligning the business model and IP strategy, rather than merely serving as a legal complement.

The importance of data gathering in relation to new business models aligns well with the prerequisites for anything-as-a-service and outcome-based agreements as discussed by Oliva and Kallenberg (2003) and Tukker (2004). For those business models, data is described as both an enabler and a prerequisite for gathering insights into how the product is used, service needs, etc. This indicates that digitalization demands not only new capabilities and resources for data collection but also a broad portfolio of digital assets to create meaningful value, as reduced quality at one stage

can affect outcomes at the next.

For customers to be willing to adopt a PaaS model, they must believe that the provider can fulfill the contract adequately with reference to Parasuraman et al. (1985)'s three evaluation criteria, in which corporate quality, such as reputation, and interactive quality are of the essence. Here, the firm's reputation and prior experience could play an important role, as noted in Chapter 5.2.2. Differences between expected and perceived service quality may reduce customers' willingness to entrust the firm with control over the product and maintenance responsibilities. While it can be difficult to convince existing customers when previous experiences have not met expectations, a well-known brand and trademark can be a useful IP asset for attracting new customers, aligning with the importance of trademarks highlighted by B. Hall et al. (2014).

5.4.2 IP Governance in Product-as-a-Service

A shift towards a PaaS implies changes in the value offering and in the conditions for capturing profits. In such a transition, the alignment between the new business model and the IP strategy becomes central, as appropriation no longer primarily depends on selling physical artifacts. Instead, it depends on the firm's ability to maintain long-term control over what could be seen as complementary assets (Teece, 1986) related to the service delivery, such as data and customer relationships with reference to Kowalkowski et al. (2024) and Tukker (2004). Consequently, the physical product becomes less central as a standalone source of appropriability, while complementary assets become increasingly important for enabling service provision. Accordingly, the IP strategy needs to be analyzed from an IP control perspective to ensure that profits from the new business model can be captured.

Previously, when customers were charged per service visit, per spare part, or at hourly rates, they had to pay for service costs, according to the interviews. Since spare parts and service were highlighted as having high profit margins, consistent with Oliva and Kallenberg (2003), a shift to outcome-based agreements requires that the new business model sustain profitability when this revenue ceases to be a separate income stream and instead becomes part of service delivery. Although stable recurring revenue may appear attractive from the firm's perspective, adopting PaaS introduces new risks that must be managed, with IP playing a crucial role in doing so. A central risk is that profitability depends on the firm's internal efficiency in delivering the service and on setting the correct monthly fee, aligning with the risks of outcome-based agreements brought up by Tukker (2004). From the empirical evidence and with support from Vandermerwe and Erixon (2023), reliance on digital assets - such as data, statistics, and insights generated through data processing - is what can make the profitability risk acceptable. This was also stated by one of the interviewees, who said that all subscription-based business models rely on some form of data. By processing data, predictions about service needs and associated costs can guide the pricing of the fixed fee to maintain profitability (Oliva & Kallenberg, 2003).

Still, unforeseen service and spare-part costs remain inevitable and therefore pose a risk to margins. This implies that the business model becomes increasingly dependent on the new digital assets such as accurate data and insights, consistent with Vandermerwe and Erixon (2023)'s argument that anything-as-a-service is often enabled by digital technologies. Consequently, the IP strategy's focus shifts toward controlling data, contracts, and internal capabilities to secure delivery and margins in outcome-based agreements.

Winter (2006) emphasizes that the interesting cases emerge when complementary assets are not found in competitors to a given price. They are instead scarce or demand specific investments. In this case, the innovation could trigger a reevaluation of complements, and value capture could be achieved by positioning in complementary assets rather than in the innovation itself. In the so-called Hirshleifer case (Winter, 2006), actors could, in extreme cases, capture appropriate amounts of value through a timely move in the complements. Translated to this case study means that the value does not necessarily become captured by the one who creates the best digital function, but instead by the one who controls the different control points, such as i) customer interfaces and integration to customers' systems, ii) data access and permissions, and iii) service and distribution channels connected to the installed base. The empirical findings further support this by repeatedly highlighting the installed base as a lever. The concern that other actors could collect data through their own IoT devices, and the possibility that interoperability could extend power to platform owners when they are closer to the customer's workflow.

Winter (2006)'s logic has two implications for the PaaS: i) the IP strategy in practice becomes a strategy to ensure that the critical complementary assets do not become another actor's profit center, ii) control over data, interfaces, and contractual agreements could create new risks, such as resistance from customers and partners, regulatory pressure, and reputational risks. This could occur especially when value capture is experienced as just shifting rather than as joint value co-creation. The question is not only about how to protect, but also about how to design control in a way that does not undermine adoption and trust.

When using a result-based contract as a business model, perceived quality must meet or exceed customer expectations (Parasuraman et al., 1985). In this context, contractual design becomes a key IP mechanism, governing access to and control over performance data and service levels. Usage-based data, such as travel distance and service intervals, can inform contract terms and pricing, in line with Oliva and Kallenberg (2003). The key implication is that value appropriation depends less on ownership of physical assets and more on how access to and use of data and services are contractually controlled. Digital assets, including usage data and predictive models, therefore become core IP resources. As Tukker (2004) highlights the importance of predicting customer behavior, IP strategy shifts toward protecting capabilities, data, and system-level knowledge. Consequently, the service delivery system and its underlying data infrastructure may be more critical to protect than

the physical product itself.

5.4.3 Product-as-a-Service and Mechanical Patents

While some interviewees were skeptical about patenting minor mechanical improvements for the industrial product, the economic rationale for such patents might be clearer when the improvement reduces failure rates in cost-driving components within a PaaS business model. To exemplify, consider a hypothetical industrial product consisting of 15 parts, where one specific part accounts for 15% of all service interventions following failures per year. Suppose the firm operates a PaaS model, in which customers pay a fixed fee, and the provider bears the cost of service labor and spare parts in accordance with the literature (Oliva & Kallenberg, 2003; Tukker, 2004). If replacing this specific part costs x SEK (including labor, time, and materials), then even a small improvement in durability can have a measurable impact on service costs and, hence, the profit margin. Assume the firm introduces an incremental mechanical improvement that reduces failures of this part by 20%. The expected reduction in overall service interventions for this specific part per year is then:

$$0.15 \times 0.20 = 0.03$$

A 3% decrease in total service interventions, holding all else equal. In cost terms, this corresponds to avoiding $0.03N$ replacements out of N total service interventions, yielding savings of $0.03N \times x$ SEK. If the improvement is protected by a patent, the firm may additionally limit competitors' ability to implement the same durability-enhancing solution in comparable products, thereby protecting both cost advantages and service margins in the PaaS offering by blocking imitators through the patent, while also being able to deliver a product that has potentially lower downtime. One also has to take into account the cost of filing for a patent compared to the value the patent creates.

5.4.4 Implications of Platform-Based Development for IP

Another important difference between selling tangible products and operating digital subscription-based platforms and software is customers' expectations of continuous updates and improvements. As one interviewee described, this differs significantly from mechanical products, where fixes and improvements are typically bundled into future product models that may take years to develop. Subscription-based software, by contrast, is expected to be updated more frequently, as noted by interviewees, implying ongoing development costs rather than primarily pre-launch investments. Continuous development, therefore, becomes another cost driver, increasing pricing complexity in subscription-based models. This further strengthens the need for a dynamic IP strategy, as value is created through ongoing software updates, lead time, and secrecy. Therefore, contractual constraints may become more relevant, since patent applications could be considered too slow and expensive for continuous software updates. As above, predicting development costs and maintaining internal development efficiency become central concerns for sustained profitability.

Finally, once major industry actors digitalize and adopt similar models, digital assets may become partly commoditized. However, interviewees frequently emphasized the installed base, existing customer channels, and relationships as core assets. This aligns with Teece (1986), in which appropriation depends largely on complementary assets once dominant designs and standardization have been established. Under such conditions, the ability to efficiently distribute, access sales channels, and maintain customer relationships may become a key bottleneck, and the actor controlling these complementary assets is likely to be in a stronger position to appropriate returns from the innovation.

5.4.5 Interdependencies of Digital Assets

If an outcome-based business model were used, profitability would be linked to new digital assets, in which data, algorithms, insights, and predictions play an important role (Kowalkowski et al., 2024; Oliva & Kallenberg, 2003). Building on Oliva and Kallenberg (2003) and Tukker (2004), these digital assets can be interpreted as co-specialized in the sense of Teece (1986), as their value arises primarily through their joint use. Therefore, neither access to data, algorithms, nor tangible artifacts is sufficient to capture most of the value. Instead, it relies on the ability to control the full bundle of complementary assets that are needed for the outcome delivery as visualized in Figure 5.3.

The importance of new digital assets is not only highlighted by the interviewees but also reflects the nature of IoT technology, where IoT devices act as bridges between the physical and digital environments for data gathering, which can then be put to use (Paolone et al., 2022). Kowalkowski et al. (2024) and Teece (2018) also add that IoT may enable a usage-based rental model. While some of the interviewees highlighted that it is how the data is used that determines its value, a few have explicitly highlighted the interdependency between the different digital assets. In a scenario where high-quality, large quantities of data are available but adequate algorithms or data processing are not in place, the data is of little use, as it needs to be processed to provide insights (Kowalkowski et al., 2024).

In a scenario where an accurate algorithm is in place but there is a lack of data in terms of quality and quantity, the algorithm is of little use. As a final scenario, where both sufficient data and a well-functioning algorithm are in place, the question remains: how are the generated insights distributed and how do they support decisions and actions? Through the lens of Kowalkowski et al. (2024) and Tukker (2004), this indicates that value creation and value capture are more strongly dissociated from a single tangible artifact and are instead associated with control over multiple assets through diverse mechanisms, in accordance with B. Hall et al. (2014). In these contexts, value appropriation depends on the ability to control and reduce the availability of combinations of assets through contractual agreements, secrecy, and technical barriers, which aligns with B. Hall et al. (2014) on the use of a bundle of protection mechanisms rather than exclusion based on a single invention. As digital assets are presumably interdependent to provide sufficient value to support

an outcome-based business model, the industrial firm needs to invest not in a single technology but in a whole value chain or ecosystem of technologies. For a company that has previously been mainly into mechanical and electromechanical products and development, the need to acquire new resources and capabilities outside of its current expertise can be seen as especially challenging (Oliva & Kallenberg, 2003).

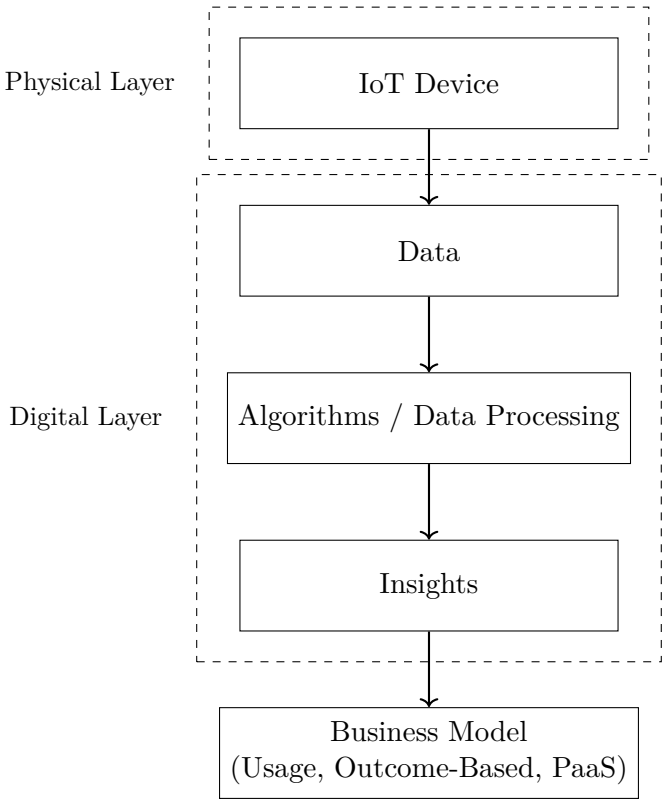

Figure 5.3: Overview of the interdependencies between different digital assets in digital retrofitting, from the IoT device attached to the industrial product to data collection and processing, and lastly, insights and application of the insights.

5.4.6 Organizational Readiness and Urgency for Digitalization

While interviewees agreed on at least some value creation from digitalization, whether for customers or internally, the sense of urgency appears more divided. Arguments in favor of digitalization were, to some extent, linked to broader societal trends, particularly the increased adoption of sensor-equipped and connected products, as also described in Teece (2018). However, some interviewees emphasized that the company currently lacks a strong sense of urgency to digitalize its products, largely due to the limited number of competitors that have done so. At the same time, prior literature suggests that timing becomes especially critical when an innovation is easy to imitate or relies on complementary assets (Teece, 1986). In line with this, several interviewees also referred to the potential first-mover advantages associated with pioneering digital development, in which lock-in effects and switching costs can

be created once digital features are incorporated into customers' ways of working and digital platforms. Despite this, the company appears to exhibit signs of incumbent complacency, as its strong market position reduces the perceived need to differentiate through digital assets to maintain or expand market share.

At the same time, a "wait-and-see" approach can become dangerous, particularly when imitation of an innovation is easy (Teece, 1986). Gemser and Wijnberg (1995) argue that industries often transition from a phase in which actors tend to hesitate to one in which competitors force each other to take risks. In the early stages of establishing a dominant design, uncertainty and imitation are higher, and firms are driven by the risk of being surpassed by other actors (Teece, 1986). However, in later stages, it becomes more rational to adopt a "see-and-wait" strategy until new uncertainties or changes in appropriability conditions once again encourage more aggressive risk-taking behavior (Gemser & Wijnberg, 1995). This provides a theoretical explanation for the empirical findings, where many respondents expressed a lack of urgency to digitalize, largely because only a few competitors currently offer competitive digital solutions, and the customer, indicating that motivation in relation to competitors remains limited.

At the same time, the findings point to a different dynamic emerging in the digital layer, where new actors move closer to the customer interface, increasing the risk of disintermediation. If the company delays action until ecosystem standards, data flows, and control points have already been established by others, it risks becoming an outsider in a network where insiders gain faster access to knowledge, thereby strengthening their advantage in service development and customer integration. With this in mind, the IP strategy must also account for timing considerations, as openness to attract complementors (Teece, 2018) and active network presence may become critical for appropriating from digital additions and new business models.

Another interesting factor contributing to the lack of urgency in digitalization efforts could be the internal environment's orientation toward existing ways of doing business. While the current business is described as relying heavily on service revenue and spare parts, the new outcome-based business models rely on quite the opposite - the company aims to perform as *little* service and as few spare part replacements as possible, as these represent costs that the company itself must bear (Oliva & Kallenberg, 2003). Service and spare parts are thus expected to become part of the overall service delivery, in which unexpected service needs or the replacement of expensive parts directly affect predicted profit margins (Oliva & Kallenberg, 2003; Tukker, 2004). Once again, digital transformation that leverages data to measure average service needs based on customers' product usage becomes a key asset for setting appropriate prices, in accordance with (Oliva & Kallenberg, 2003). This shift requires not only a technological transformation within the organization (Oliva & Kallenberg, 2003) but also a challenge to the current mindset, moving from selling as much service as possible to delivering as little service as necessary. Building on this from an IP perspective, digital assets further play a crucial role in enabling the PaaS business model and supporting predictive maintenance capabilities.

Another important transformation concerns how the IP department itself needs to evolve. As discussed in Chapter 5.1.4, the pace of innovation in software is significantly faster than in traditional hardware development. This implies that the IP department, in close collaboration with R&D, operates under shorter time frames to identify *what* IP should be protected and *how* this protection should be realized before new updates or software releases are deployed. Furthermore, the interviews indicate that the IP department has historically focused primarily on IP rights, such as patents, trademarks, and design rights. In contrast, the emerging IP landscape is increasingly centered around data, contractual mechanisms, and trade secrets. This shift raises questions regarding how the IP department should be integrated into the firm's day-to-day operations, as data becomes a key asset in the digitalized environment, as discussed in Chapter 5.1.1. In particular, the findings suggest that the IP department may need to become involved in parts of the organization where its presence has traditionally been limited.

Since data is often best protected through secrecy, ensuring adequate handling, access control, and sharing practices becomes critical. This implies a broader role for the IP function, spanning areas such as data governance, collaboration agreements, and the design of software architectures that support modularity, where protected core components can be separated from more open interfaces. Moreover, the IP department may need to contribute to internal processes such as employee training on data handling, confidentiality, and trade secret awareness. As the ability to conduct business largely depends on digital assets, the question of how to manage and control them is likely to take up a greater share of the business agenda than it does currently, indicating that the IP department also needs to be more involved in business strategy. The importance of involving the IP department across the organization is also highlighted in Holgersson and Wallin (2017) and becomes particularly important in the context of digitalization (Holgersson & Granstrand, 2018). Taken together, these developments indicate that the IP function must evolve alongside the firm's digital transformation, shifting from a predominantly legal and reactive role toward a more integrated, proactive, and cross-functional capability.

5.4.7 Threats & Competition from New Digital Entrants & Established Actors

The empirical findings suggest that digitalization efforts are currently given lower priority, partly because few competitors have launched mature digital offerings. At the same time, respondents highlight that new actor categories, especially those close to customers' systems and data flows, may pose a greater long-term threat than traditional competitors. This creates a paradox: competitive pressure appears low today, yet the risk of rapid competitive escalation remains high. Building on Ceccagnoli and Rothaermel (2016), this can be understood in terms of the presence of *capable competitors*: when many actors can quickly imitate and commercialize, time and scalability become critical even before competition becomes visible. Accordingly, urgency should be defined by how fast the firm can establish a difficult-

to-move position and strengthen specialized complements before ecosystem power dynamics solidify.

In the context of digitalization, competition shifts toward the digital layer and the customer interface. Interviewees emphasize that even small digital functionalities can create lock-in effects when embedded in customers' daily operations, making switching costly and increasing the strategic value of being *first* to integrate into customers' platforms. Born-digital entrants and startups may have advantages in agility and software development, while incumbents often struggle to reconfigure their structures and processes to support digital and service capabilities (Oliva & Kallenberg, 2003). However, respondents also stress that established industrial firms retain advantages in installed base, service organization, industry-specific (tacit and codified) knowledge, and customer relationships, which are central resources in service-based value creation (Oliva & Kallenberg, 2003; Tukker, 2004). While born digital entrants may excel in software and algorithm development, interviewees further stressed that delivering a full PaaS offering requires a broader service delivery system, including service operations and hardware installation. Building hardware manufacturing and establishing a geographically distributed service organization was described as expensive and time-consuming to replicate, creating barriers for software-centric entrants. This aligns well with Tukker (2004), who highlights that value capture in service-oriented systems depends on controlling essential elements of the service delivery system. Following Teece (1986, 2018), this implies that value capture will increasingly depend on controlling complementary assets such as customer access, service delivery capabilities, and sales distribution channels, assets that are difficult for software-centric entrants to replicate quickly.

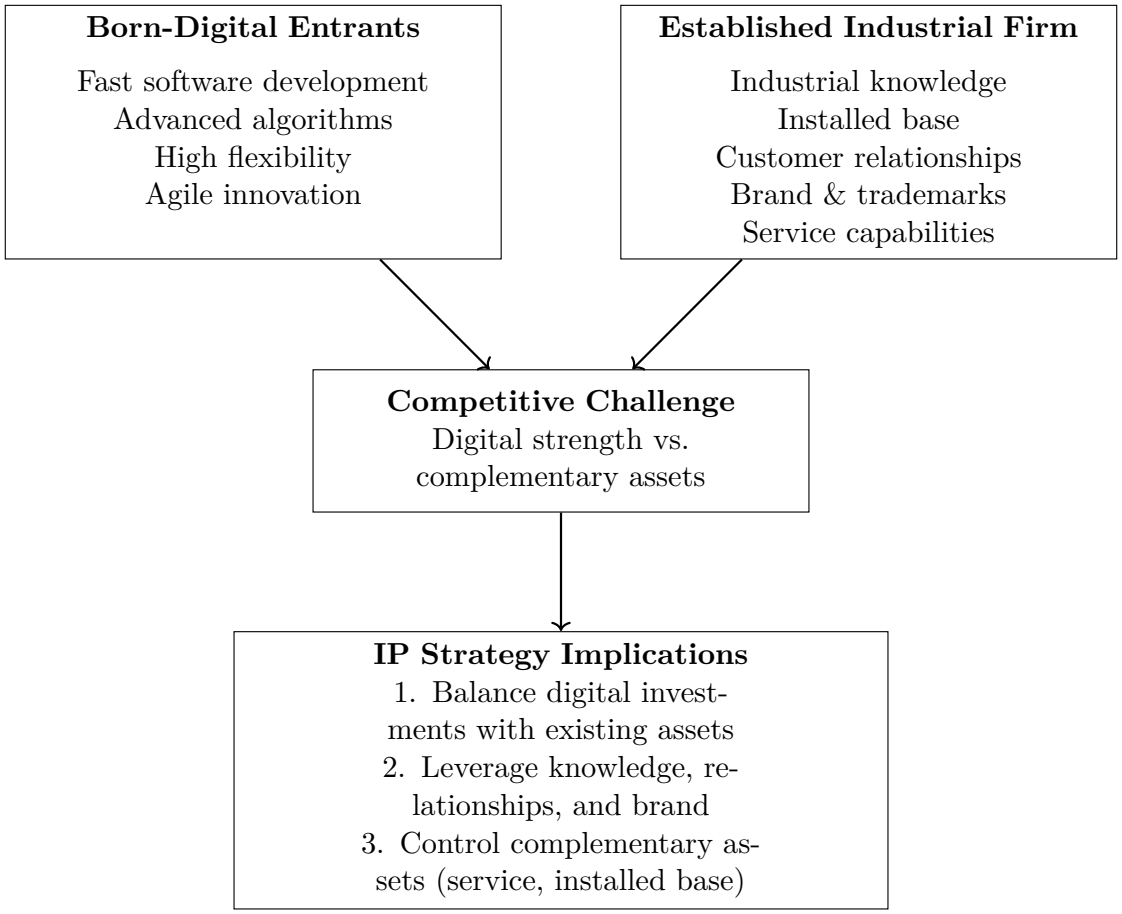

Figure 5.4: Overview of the threat from new digital entrants compared to established actors, and its implications for IP strategy.

6
Conclusion

The purpose of this thesis is to analyze how the digital retrofitting of industrial products affects the IP strategies of industrial firms undergoing this transformation. In this chapter, the findings and implications from Chapter 5 are synthesized to answer the research questions presented in Chapter 1.5, and the main changes and differences for the IP strategy are then summarized in Table 6.1.

6.1 Answer to Research Question 1: What New Intellectual Property Emerges with the Introduction of Digital Functionalities?

The analysis in Chapter 5 shows that data and insights derived from data become central IP assets in the context of retrofitting industrial products. The most significant change is the increased accessibility to data through real-time connectivity enabled by IoT devices, rather than the data itself being fundamentally new. The analysis further indicates that data ownership is unclear among employees at the company under investigation, and that views on the importance of ownership and exclusivity rights to the data are divided. Consequently, the question becomes a strategic concern involving trade-offs among ownership, access, and exclusivity, and is also influenced by regulations such as the Data Act, in which technical barriers and contractual agreements are among the key control mechanisms.

The data is then highlighted to provide the foundation for service innovation, such as predictive maintenance, in which data is processed through new advanced algorithms to predict service needs, and for new business models, such as PaaS. This indicates that the company becomes dependent on a bundle of digital assets, not just the data itself. Digital functionalities are also often associated with digital platforms, where modular functionalities emerge as central components. These create new digital assets and capabilities while simultaneously exposing both data and physical products to digital threats.

A large installed base was highlighted as a core asset for its ability to generate both high-quality and high-volume data, thereby strengthening the accuracy of insights. The installed base was also perceived as a way to attract complementors to co-create value through the digital platform.

Furthermore, the analysis highlights the importance of protecting and controlling digital assets through a bundle of IP mechanisms: i) contractual agreements to manage data access, usage rights, limitations, and commercialization through new business models; ii) trade secrets protected through secrecy measures to protect digital assets and functionalities such as algorithms, data-processing processes, and insights; iii) internal governance and policies for handling and controlling digital IP, such as classification, access rights, and information flows; and iv) cybersecurity measures as a foundation for maintaining secrecy and block intrusions in the digital environment.

Lastly, patents in digital environments are perceived as having limited value, further emphasizing that IP strategies in the digital layer rely primarily on contracts, secrecy, and technical barriers to control and protect digital IP assets.

6.2 Answer to Research Question 2: How does Digital Retrofitting Change the Role of Existing IP?

The findings in Chapter 5 point to the continued importance of traditional IP connected to hardware, especially mechanical patents and know-how, as well as established trademarks. However, their role shifts toward a foundational layer that supports trust, scalability, and regulatory compliance, rather than serving as the primary source of differentiation. A central implication is that IP protection moves from a product-centered approach toward a greater focus on control, access, and governance in the digital layer, including data, interfaces, and cybersecurity. This indicates that the IP strategy becomes layered as a result of digitalization. As a result, the analysis suggests a more selective approach to IP protection, where IP modularity can enable certain parts to be protected through formal mechanisms such as patents, while other parts are better protected as trade secrets through contractual agreements and technical barriers.

The analysis further indicates that trademarks are becoming increasingly strategic in importance, as they serve as a source of trust and quality in evolving digital environments. At the same time, trademarks face new and more significant risks of reputational damage in the event of digital incidents such as intrusions and theft.

Lastly, enforcement conditions are expected to change, as digital intrusions and digital IP infringements are perceived as more difficult to detect than hardware-based intrusions and as litigation outcomes are seen as more uncertain. This implies a stronger need to combine legal and technical mechanisms to protect IP.

6.3 Answer to Research Question 3: How do Evolving Ecosystem Interdependencies Influence Intellectual Property Strategy?

Digital retrofitting increases ecosystem complexity, as actors' roles vary by context and may change over time. A single actor may act as a partner in one situation and as a competitor or supplier in another. As a result, the IP strategy shifts toward a greater emphasis on control, dependency management, and negotiation power within relationships, where a large installed base is leveraged as a bargaining chip.

The analysis identifies interoperability, standards, and APIs as key strategic control points. These enable adoption and integration while simultaneously creating IP dependencies and tensions between openness and competition. This further emphasizes the role of contracts, licenses, and NDAs as primary mechanisms for managing and controlling access, usage rights, and responsibilities in ecosystem relationships, where formal IPRs are often insufficient to govern data- and interface-related concerns.

Finally, digitalization introduces and intensifies threats from actors closer to customer interfaces and data flows. This makes positioning and governance central components of IP strategy within digital ecosystems.

6.4 Answer to Research Question 4: How does Digital Retrofitting Drive Firms to Reconsider the Relationship Between their IP Strategy and their Business Model?

Digital retrofitting enables and drives a shift toward new business models, including outcome-based, usage-based, and subscription-based models, all of which depend on access to data and insights. In this transition, the IP strategy needs to be aligned with the business model by leveraging contracts to control data access rights and govern the relationship between the company and the customer.

The analysis also highlights the interdependence among digital assets, such as data, data processing, and the use of insights, to succeed with new business models. This implies that control and protection must involve the entire bundle of digital assets through contracts, secrecy measures, and technical barriers.

Furthermore, participation in digital platforms and ecosystems increases dependence on partners, indicating that organizational readiness and governance become central to both enabling and protecting new ways of collaborating and conducting business.

Finally, competitive threats stem from both established actors and new digital en-

trants, with the primary threat increasingly linked to control over interfaces and data rather than imitation of physical products.

6.5 Answer to the Main Research Question: How does a Firm's Intellectual Property Strategy Change when a Legacy Product is Retrofitted to Digital Ecosystems?

In summary, the IP strategy shifts from an artifact- and IPR-centered approach, dominated by traditional protection of physical inventions, toward a more layered IP strategy. In this new configuration, appropriation and control are largely achieved through contracts, secrecy, internal governance, and cybersecurity, while traditional IP remains an important foundational layer.

The digital transformation further emphasizes the importance of digital assets such as data, interfaces, and ecosystem positioning. This requires control over access, usage, and responsibilities, rather than primarily focusing on excluding competitors through formal IPRs such as patents.

At the same time, increased ecosystem dependencies and a shift in business models toward services and platforms lead to an IP strategy that increasingly functions as a tool for managing relationships, interoperability, and risks, rather than solely protecting individual technical solutions.

6.6 Overview of Changes from Before- and After Digital Retrofitting for IP Strategy

Table 6.1 summarizes the main changes in the roles of different IP and mechanisms as an industrial firm digitalizes and integrates into a digital ecosystem. By comparing the IP environment before digitalization with the new opportunities and risks that emerge afterward, the table illustrates how value creation and value capture shift from tangible artifacts toward digital and organizational control mechanisms.

Overall, the table synthesizes the main conclusion of this thesis: in digital environments, IP strategy increasingly relies on balancing openness and control through a combination of formal rights, contracts, secrecy, and technical protection mechanisms.

Table 6.1: Overview of IP and mechanisms before and after digitalization: opportunities and risks

IP/governance area	Before digitalization	After digitalization – Opportunities	After digitalization – Risks
1) Patents (hardware/electromechanical)	Patenting as a central exclusion mechanism for product-related inventions/component improvements (5.2.1, 5.2.3).	Patents can be used more strategically (defensive, bargaining power) and protect improvements that strengthen service/PaaS logic (5.2.3, 5.4.3).	Risk that patents lose relative importance as value shifts toward digital layers; misallocation toward "minor patents" that do not drive value capture (5.2.1, 5.2.3).
2) Patents (software/algorithms)	Software not central → limited patent relevance (5.1.4 as contrast: limitations of digital patenting).	Selective patenting can provide negotiation positions for stable, separable digital components (5.1.4).	Disclosure risk + ease of "inventing around," rapid iteration, more challenging prior art/FTO in digital environments (5.1.4).
3) Copyright (code, documentation)	Limited strategic role (digital assets not core) (5.1.1 as contrast).	Baseline barrier for code/modules; can be strengthened via licensing and release governance (5.1.1, 5.1.3).	Does not protect functionality; "black box" effects make infringement harder to detect (5.1.4, 5.1.1).
4) Trade secrets (know-how, processes)	Secrets linked to production/processes and tacit know-how (5.1.2).	Increased strategic importance: algorithms, data processes, ways of working; "hybrid" IP portfolio (5.1.2, 5.4.5).	Digital storage/access increases leakage, and intrusion risk → requires policies, cybersecurity, access control, and training (5.1.2, 5.4.6).
5) Data (raw data) & access	Data is local and primarily used reactively (5.1.1 as contrast: "data becomes central").	Continuous remote access enables services, efficiency, and learning (5.1.1, 5.4.3).	Tensions regarding sharing/ownership and risk that raw data reveals usage patterns; may enable replication of insights (5.4.5, 5.1.1).
6) Insights/derivatives (analytics, models, optimization)	More experience- and tacit-driven than data-driven (5.1.1 as contrast).	Core asset for value capture (development/service/sales) via trade secrets and control mechanisms (5.1.1, 5.4.5).	If others access raw data, insights can be replicated; requires data protection and governance (5.4.5, 5.1.3).
7) Trademarks (trust, quality signal)	Brand primarily signals physical product quality (5.2.2).	Driver of trust for digital adoption; sub-branding can isolate the core brand (5.2.2).	Cyber incidents may broadly impact the brand; digital quality is harder to assess (5.2.2).
8) Design rights	Important for physical form/appearance and protection against copies (5.2.1 as a "foundation layer" of traditional protection).	Continues to be relevant against physical imitation/counterfeits (5.2.1, 5.2.2, 5.2.3).	Risk that design protection loses strategic impact as differentiation shifts to digital layers (5.2.1).
9) Contracts & licensing (customer, partner, supplier)	Contracts primarily support product sales + traditional service (reactive) (5.1.3 as contrast).	Contracts become primary IP governance: data access/use, confidentiality, new business models, licensing, pricing (5.1.3, 5.4.3).	Increased contractual complexity due to role shifts; risk of disintermediation if contracts do not secure control points (5.3.1, 5.1.3).
10) APIs, interfaces & interoperability	Limited integrations; few strategic interfaces (5.3.2 as contrast).	Open interfaces drive adoption; IP modularity: open modules, protected core (5.3.2).	Openness reduces switching costs and may facilitate imitation/"takeover" of the customer interface (5.3.2, 5.3.1).
11) Standards & FTO landscape	FTO more manageable in traditional mechanical domains (5.1.4, 5.3.2 as contrast).	Standards/licensing strategies can provide compatibility and faster ecosystem entry (5.3.2).	Patent thickets, licensing dependencies, increased FTO burden, and hold-up risk (5.3.2, 5.1.4).
12) Cybersecurity as an appropriability mechanism	Focus on physical security/robustness (5.1.1, 5.2.2 as contrast).	Protects secrets/data and strengthens trust; enables secure remote functions/updates (5.1.1, 5.3.1).	Larger attack surface (remote access/updates/integration) → IP loss + brand damage + liability risk (5.2.2, 5.3.1).
13) Ecosystem relationships & role shifts	Linear value chain; clearer roles (5.3.1 as contrast).	Partnerships can accelerate innovation and create complementary value (5.3.1, 5.3.3).	Blurred roles create uncertainty; risk that others take control over interfaces/data (5.3.1, 5.4.7).
14) Business model shift (services, subscription, outcome-based)	Product sales + service/spare parts; IP tied to product differentiation (5.4.2, 5.4.6).	New revenue logics (predictive/availability, leasing, usage-based) where data + contracts drive value capture (5.4.1, 5.4.2, 5.4.3).	Risk shift to provider, KPI misalignment, cannibalization tensions (5.4.3, 5.4.6).
15) Organizational capabilities (IP mapping, cross-functional ownership)	IP mainly within R&D/legal; artifact-centric (5.1.1 as contrast).	Cross-functional governance improves mapping, classification, contracts, and security (5.4.6, 5.1.3).	Risk of responsibility gaps/competence gaps without new routines; may increase dependency on external actors (5.4.6, 5.4.5).

7

Research Contributions and Future Research

7.1 Contribution of Research

Our thesis contributes to the research by demonstrating how an industrial firm's IP strategy transforms when legacy products are retrofitted for integration into digital ecosystems. A central contribution is the overview of how IP rights, such as patents and trademarks, are complemented by contracts, secrecy, and technical protection mechanisms for managing digital assets.

Furthermore, we identify how new forms of IP, particularly data, software, and data-driven insights, become central to value creation. In this context, views on access to and control over data introduce a new consideration rather than relying solely on legal ownership. The thesis also shows that IP strategy increasingly involves managing relationships and dependencies within digital ecosystems, through key control points such as APIs, contractual arrangements, and customer interfaces.

Finally, we highlight the evolving role of existing IP, shifting from a primary source of differentiation to a foundation for trust, credibility, and scalability. Overall, the thesis contributes to a deeper understanding of how IP strategy, business models, and digital ecosystems interact in the modern digitalized industrial environment.

7.2 Research Limitations

The thesis results should be understood with several research limitations in mind. First, the thesis is based on a single case study of a European industrial company and a specific legacy product, which may limit the generalizability and applicability of the findings to other industries, products, and geographical contexts. The empirical data is based solely on interviews conducted within the case company, so external perspectives from suppliers, customers, competitors, and partners are not included. This may result in a somewhat one-sided organizational perspective.

Furthermore, variations in how central concepts, such as IP, are understood and interpreted may have influenced respondents' answers, particularly as some interviewees were not regularly engaged in IP-related work. The limited time frame of five months also constrained both the depth and breadth of the thesis. In addition,

the interviews were conducted digitally, which may have affected the ability to capture non-verbal cues.

Finally, the thesis does not include a technical evaluation of the IoT solution, and the legal analysis is limited to a conceptual level within the EU context. This may affect both the analytical depth and the practical precision of the findings. The results should therefore be interpreted as exploratory and conceptual rather than fully generalizable.

7.3 Suggestions for Further Research

Further research is suggested to deepen the understanding of the specific mechanisms that our thesis identifies as central to IP strategy in digital retrofitting contexts. First, it would be interesting for a more detailed analysis of how firms operationally distinguish between raw data and derived insights, and how these can be effectively protected and commercialized, particularly in contexts where data must be shared with external actors. Second, contractual design could be examined in greater depth, as contracts increasingly function as a core tool for IP governance in digital ecosystems. Future research could, for example, identify which contractual clauses most effectively balance collaboration, value appropriation, and the protection of digital assets. It would also be interesting to see how IP departments are involved in the daily operations of a digital-focused firm compared to an industrial one. Lastly, further studies could investigate how firms design APIs and interoperability strategies to manage the trade-off between openness and control. Together, these research areas enable a shift from the broad perspective of this thesis toward more in-depth analyses of specific control points and IP governance mechanisms.

References

Almeling, D. S. (2012). Seven reasons why trade secrets are increasingly important. https://doi.org/10.15779/Z38SM4F

Anton, J. J., & Yao, D. A. (2002). The sale of ideas: Strategic disclosure, property rights, and contracting. *The Review of Economic Studies*, *69*(3), 513–531.

Arundel, A. (2001). The relative effectiveness of patents and secrecy for appropriation. *Research Policy*, *30*(4), 611–624. https://doi.org/https://10.1016/S0048-7333(00)00100-1

Asadullah, A., Faik, I., & Kankanhalli, A. (2018). Digital platforms: a review and future directions. https://repository.lboro.ac.uk/articles/conference_contribution/Digital_platforms_a_review_and_future_directions/24081825

Balice, S., Dalton, P., Lei, P., et al. (2026, May 14). *A comparative guide to enforcing trade secrets across major jurisdictions*. Retrieved May 22, 2026, from https://www.iam-media.com/trade-secrets/article/comparative-guide-enforcing-trade-secrets-across-major-jurisdictions

Baptista, C., & Nunes, D. (2025). Digital ecosystems and their influence on business relationships. *Review of Managerial Science*, *20*, 29–51. https://doi.org/10.1007/s11846-025-00865-2

Bell, E., Bryman, A., & Harley, B. (2022). *Business research methods* (6th ed.). Oxford University Press.

Blaskovic, A. K., Rusk, J.-D., Parker, V. C., & Payne, B. R. (2023). Cybercrime and intellectual property theft: An analysis of modern digital forensics. In K. Arai (Ed.), *Proceedings of the future technologies conference (ftc) 2022, volume 2* (pp. 536–542). Springer International Publishing.

Bresciani, S., Ferraris, A., Romano, M., & Santoro, G. (2021, June). Digital ecosystems. In *Digital transformation management for agile organizations: A compass to sail the digital world*. Emerald Publishing Limited. https://doi.org/10.1108/978-1-80043-171-320211009

Cardona, M., & Serrano, F. E. (2023). The fourth industrial revolution and disruptive technologies. *2023 IEEE 41st Central America and Panama Convention (CONCAPAN XLI)*, 1–6. https://doi.org/10.1109/CONCAPANXLI59599.2023.10517560

Ceccagnoli, M., & Rothaermel, F. (2016, August). Appropriability strategies to capture value from innovation. https://doi.org/10.1108/S1048-473620160000026001

Chen, Y.-J., & Lu, T.-J. (2019). Intellectual property strategy for the ecosystem of the internet of things. *International Journal of Technology Management*, *80*(3-4), 212–240.

Cusumano, M. A., Gawer, A., & Yoffie, D. B. (2019, June). *The business of platforms : Strategy in the age of digital competition, innovation, and power*. Harper Business.

DalleMule, L., & Davenport, T. H. (2017). What's your data strategy? *Harvard Business Review*, *95*(3), 112–125. Retrieved May 10, 2026, from https://hbr.org/2017/05/whats-your-data-strategy

European Commission. (2025). Data act explained: A comprehensive overview of the data act, including its objectives and how it works in practice.

European Patent Office. (2025). *Guidelines for examination in the european patent office: Index for computer-implemented inventions (part j)*. European Patent Office. Retrieved February 24, 2026, from https://www.epo.org/en/legal/guidelines-epc/2025/j.html

European Union. (2025). *Database protection*. European Commission. Retrieved May 22, 2026, from https://europa.eu/youreurope/business/running-business/intellectual-property/database-protection/index_en.htm

European Union Intellectual Property Office. (2025). *Registered community designs*. Retrieved May 18, 2026, from https://www.euipo.europa.eu/en/designs

Gemser, G., & Wijnberg, N. M. (1995). Horizontal networks, appropriability conditions and industry life cycles. *Journal of Industry Studies*, *2*(2), 129–140. https://doi.org/10.1080/13662719508538559

Gokhale, P., Bhat, O., & Bhat, S. (2018). Introduction to iot. *5*, 41–44. https://doi.org/10.17148/IARJSET.2018.517

Granstrand, O., & Holgersson, M. (2012). The 25% rule revisited and a new investment-based method for determining frand licensing royalties. *les Nouvelles*, *47*, 188–195. https://www.ip-research.org/wp-content/uploads/2012/08/FRAND-20120629a-with-publ-details-for-web-publishing.pdf

Granstrand, O., & Holgersson, M. (2013). Managing the intellectual property disassembly problem. *California Management Review*, *55*(4), 184–210. https://doi.org/10.1525/cmr.2013.55.4.184

Granstrand, O., & Holgersson, M. (2014). The challenge of closing open innovation: The intellectual property disassembly problem. *Research-Technology Management*, *57*(5), 19–25. https://doi.org/10.5437/08956308X5705258

Granstrand, O., & Holgersson, M. (2015, March). Intellectual property. In *The wiley blackwell encyclopedia of consumption and consumer studies* (pp. 1–3). John Wiley & Sons, Ltd. https://doi.org/10.1002/9781118989463.wbeccs151

Grzegorczyk, T., & Gowiski, R. (2020). Patent management strategies: A review. *Journal of Economics and Management*, *40*, 36–51.

Hall, B., Helmers, C., Rogers, M., & Sena, V. (2014). The choice between formal and informal intellectual property: A review. *Journal of Economic Literature*, *52*(2), 375–423. Retrieved February 23, 2026, from http://www.jstor.org/stable/24433813

Hall, R. (1989). The management of intellectual assets: A new corporate perspective. *Journal of General Management*, *15*(1), 53–68. https://doi.org/10.1177/030630708901500104

Halman, J. I. M., Hofer, A. P., & Van Vuuren, W. (2003). Platform-driven development of product families: Linking theory with practice. *Journal of Product*

Innovation Management, *20*(2), 149–162. https://doi.org/10.1111/1540-5885.2002007

Henkel, J., Baldwin, C. Y., & Shih, W. (2013). Ip modularity: Profiting from innovation by aligning product architecture with intellectual property. *California Management Review*, *55*(4), 65–82. https://doi.org/10.1525/cmr.2013.55.4.65

Holgersson, M., & Granstrand, O. (2018). Ip-strategi i digitaliserande industrier: Gammal trend med nya implikationer. *Management of Innovation and Technology*, *2018*, 10–11. https://mgmt.imit.se/artiklar/ip-strategi-i-digitaliserande-industrier/

Holgersson, M., & Wallin, M. (2017). The patent management trichotomy: Patenting, publishing, and secrecy. *Management Decision*, *55*. https://doi.org/10.1108/MD-03-2016-0172

Holmlund, M., & Törnroos, J.-Å. (1997). What are relationships in business networks? *Management Decision*, *35*, 304–309. https://doi.org/10.1108/00251749710169693

Hurmelinna-Laukkanen, P., & Puumalainen, K. (2007). Nature and dynamics of appropriability: Strategies for appropriating returns on innovation. *R&D Management*, *37*(2), 95–112. https://doi.org/10.1111/j.1467-9310.2007.00460.x

Koch, M., Krohmer, D., Naab, M., Rost, D., & Trapp, M. (2022). A matter of definition: Criteria for digital ecosystems. *Digital Business*, *2*(2), 100027. https://doi.org/10.1016/j.digbus.2022.100027

Kowalkowski, C., Wirtz, J., & Ehret, M. (2024). Digital service innovation in b2b markets. *Journal of Service Management*, *35*, 280–305. https://doi.org/10.1108/JOSM-12-2022-0403

Kumar, A., & Kumar, S. (2020). Industry 4.0: Evolution, opportunities and challenges. *International Journal of Research in Business Studies*, *5*(1), 139–148.

Laub, C. (2006). Software patenting: Legal standards in europe and the us in view of strategic limitations of the ip systems. *The Journal of World Intellectual Property*, *9*(3), 344–372. https://doi.org/10.1111/j.1422-2213.2006.00281.x

Lazarotto, B. (2024). The right to data portability: A holistic analysis of gdpr, dma and the data act. *European Journal of Law and Technology*, *15*(1). Retrieved March 3, 2026, from https://ejlt.org/index.php/ejlt/article/view/988

Lev, B. (1992). Information disclosure strategy. *California Management Review*, *34*(4), 9–32. https://doi.org/10.2307/41166701

Lundin, L., & Kindström, D. (2023). Digitalizing customer journeys in b2b markets. *Journal of Business Research*, *157*, 113639. https://doi.org/10.1016/j.jbusres.2022.113639

Ma, L., Zhang, B., Liang, K., Cheng, Y., & Yi, C. (2024). Digital enabled innovation ecosystems: A dual case study of knowledge flows in intellectual property platforms. *European Journal of Innovation Management*. https://doi.org/10.1108/EJIM-07-2023-0610

Mazhelis, O., Luoma, E., & Warma, H. (2012). Defining an internet-of-things ecosystem. *Conference on internet of things and smart spaces*, 1–14.

Mylly, U.-M. (2024). Trade secrets and the data act. *IIC Int. Rev. Ind. Prop. Copyr. Law*.

Oberländer, A. M., Karnebogen, P., Rövekamp, P., Röglinger, M., & Leidner, D. E. (2025). Understanding the influence of digital ecosystems on digital transformation: The oco (orientation, cooperation, orchestration) theory. *Information Systems Journal*, *35*(1), 368–413. https://doi.org/10.1111/isj.12539

Oliva, R., & Kallenberg, R. (2003). Managing the transition from products to services. *International Journal of Service Industry Management*, *14*, 160–172. https://doi.org/10.1108/09564230310474138

Ozcan, O., Pickernell, D., & Trott, P. (2023). A trade secrets framework and strategic approaches. *IEEE Transactions on Engineering Management*, *PP*, 1–17. https://doi.org/10.1109/TEM.2023.3285292

Paolone, G., Iachetti, D., Paesani, R., Pilotti, F., Marinelli, M., & Di Felice, P. (2022). A holistic overview of the internet of things ecosystem. *IoT*, *3*(4), 398–434. https://doi.org/10.3390/iot3040022

Parasuraman, A., Zeithaml, V. A., & Berry, L. L. (1985). A conceptual model of service quality and its implications for future research. *Journal of Marketing*, *49*(4), 41–50. Retrieved February 24, 2026, from http://www.jstor.org/stable/1251430

Peters, T., Thiel, J., & Tucci, C. L. (2013). Protecting growth options in dynamic markets: The role of strategic disclosure in integrated intellectual property strategies. *California Management Review*, *55*(4), 121–142. https://doi.org/10.1525/cmr.2013.55.4.121

Selander, L., Henfridsson, O., & Svahn, F. (2013). Capability search and redeem across digital ecosystems. *Journal of Information Technology*, *28*(3), 183–197. https://doi.org/10.1057/jit.2013.14

Shapiro, C. (2001). Navigating the patent thicket: Cross licenses, patent pools, and standard-setting. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.273550

Somaya, D. (2012). Patent strategy and management: An integrative review and research agenda. *Journal of Management - J MANAGE*, *38*, 1084–1114. https://doi.org/10.1177/0149206312444447

Somaya, D., Teece, D., & Wakeman, S. (2011). Innovation in multi-invention contexts: Mapping solutions to technological and intellectual property complexity. *California Management Review*, *53*(4), 47–79.

Tao, J., Daniele, J., Hummel, E., Goldheim, D., & Slowinski, G. (2005). Developing an effective strategy for managing intellectual assets. *Research-Technology Management*, *48*(1), 50–58. https://doi.org/10.1080/08956308.2005.11657295

Teece, D. J. (1986). Profiting from technological innovation: Implications for integration, collaboration, licensing and public policy. *Research Policy*, *15*(6), 285–305. https://doi.org/10.1016/0048-7333(86)90027-2

Teece, D. J. (2018). Profiting from innovation in the digital economy: Enabling technologies, standards, and licensing models in the wireless world. *Research Policy*, *47*(8), 1367–1387. https://doi.org/10.1016/j.respol.2017.01.015

Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data

Act) (2023, December 22). https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng

Tukker, A. (2004). Eight types of product-service system: Eight ways to sustainability? experiences from suspronet. business strategy and the environment 13: 246 - 260. *Business Strategy and the Environment*, *13*, 246–260. https://doi.org/10.1002/bse.414

Valdez-De-Leon, O. (2019). How to develop a digital ecosystem a practical framework. *Technology Innovation Management Review*, *9*, 43–54. https://doi.org/10.22215/timreview/1260

Vandermerwe, S., & Erixon, D. (2023). Servitization of business updated: Now, new, next. *European Management Journal*, *41*(4), 479–487. https://doi.org/10.1016/j.emj.2023.07.007

van Santen, S., & Holgersson, M. (2026). Threading fashion's paradox knot: Ip strategy in open and sustainable innovation. *European Journal of Innovation Management*, *29*(11), 151–171. https://doi.org/10.1108/EJIM-02-2025-0170

Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Qi Dong, J., Fabian, N., & Haenlein, M. (2021). Digital transformation: A multidisciplinary reflection and research agenda. *Journal of Business Research*, *122*, 889–901. https://doi.org/10.1016/j.jbusres.2019.09.022

Voss, T., Paranjpe, A. S., Cook, T. G., & Garrison, N. D. (2017). A short introduction to intellectual property rights [SI: Innovation in Interventional Radiology]. *Techniques in Vascular and Interventional Radiology*, *20*(2), 116–120. https://doi.org/https://10.1053/j.tvir.2017.04.007

Winter, S. G. (2006). The logic of appropriability: From schumpeter to arrow to teece. *Research Policy*, *35*(8), 1100–1106. https://doi.org/10.1016/j.respol.2006.09.010

World Intellectual Property Organization. (n.d.-a). *Madrid system the international trademark system*. Retrieved January 22, 2026, from https://www.wipo.int/en/web/trademarks

World Intellectual Property Organization. (n.d.-b). *Trademarks*. Retrieved January 22, 2026, from https://www.wipo.int/en/web/trademarks

World Intellectual Property Organization. (2004). *WIPO intellectual property handbook*.

Xu, L. D., Xu, E. L., & Li, L. (2018). Industry 4.0: State of the art and future trends. *International Journal of Production Research*, *56*(8), 2941–2962. https://doi.org/10.1080/00207543.2018.1444806

Yang, J., & Hurmelinna-Laukkanen, P. (2022). Evolving appropriability variation in the relevance of appropriability mechanisms across industries. *Technovation*, *118*, 102593. https://doi.org/10.1016/j.technovation.2022.102593

Zimmerman, M. (2015). The basics of copyright law: Just enough copyright for people who are not attorneys or intellectual property experts. *California Bar Journal*.

A

Appendix - Interview Guide

Why is the electromechanical product an important product for the customers?

How do you think the studied company protects the electromechanical product from competitors?

What parts of the electromechanical product and its services should the studied company keep secret from competitors?

How did the studied company make money when the products were only electromechanical?

What do the digitalized products have that the electromechanical products did not?

What new assets and opportunities are created when the product is digitalized?

Who do you think owns and controls the data generated by the product?

What is the competitive advantage of the digitalized product?

How important does digital protection become compared to hardware protection?

What does digitalization create that the studied company wants to keep secret from competitors?

What do you think is the biggest challenge companies face when protecting connected products?

How does the shift toward digital ecosystems change the way the studied company collaborates with external partners?

Has digitalization created new kinds of competitors?

Who are the studied company most afraid of copying its business: An electromechanical product competitor, A new software startup, or an Established software provider?

What are the opportunities in this kind of ecosystem?

Which new customer benefits might emerge from making the product connected?

In five years, what will be the studied company's most valuable asset?

How might the studied company earn money differently compared to selling only physical products?

What makes it difficult for customers to switch to a competitor with this new offering?

In the future, will the studied company be a hardware company with software, or a software company that uses hardware?

Is there anything else you would like to discuss?

DEPARTMENT OF TECHNOLOGY MANAGEMENT AND ECONOMICS
DIVISION OF ENTREPRENEURSHIP AND STRATEGY
CHALMERS UNIVERSITY OF TECHNOLOGY
Gothenburg, Sweden
www.chalmers.se

CHALMERS
UNIVERSITY OF TECHNOLOGY