TECHNISCHE UNIVERSITÄT WIEN

Diploma Thesis

Intellectual Property Management

Know-how protection in rolling stock business cooperation

carried out for the purpose of obtaining the degree of Master of Science (MSc or Dipl.-Ing. or DI), submitted at TU Wien, Faculty of Mechanical and Industrial Engineering, by

Steffen Nixdorf

Mat.Nr.: 1225457

under the supervision of

Univ.Prof. Dipl.-Ing. Dr.-Ing. Detlef Gerhard

Institute of Engineering Design and Product Development, E307

Signature

Affidavit

I declare in lieu of oath, that I wrote this thesis and performed the associated research myself, using only literature cited in this volume.

Vienna, April 13, 2019

Signature

Acknowledgements

I would like to offer my special thanks to my advisors. Prof. Gerhard Detlef, my academic advisor, for his support extensive feedback and steering me into the right direction whenever it was needed. I am grateful to my company-internal advisor Mr. Martin Kollmann, who gave me constructive comments and generous support. I have greatly benefited from his expertise and without his dedicated involvement this thesis would not have been possible.

Besides my advisors, I want to thank the organisation, my colleagues for giving me the opportunity and necessary support to conduct this thesis. And to my fellow students for many years of helpful discussions on problems we have come across and have not fallen over.

It required more than academic support, I have many people to thank for listening and at times tolerating me for the past months. Most importantly my friends, who carried me through months of overtime working and gave me distraction whenever I needed it.

Finally, I must express my gratitude to my parents and to my brother for providing me with continuous encouragement throughout my years of study and supporting me in my life in general. This accomplishment would not have been possible without them. Thank you.

So the industrious bees do hourly strive
To bring their loads of honey to the hive;
Their sordid owners always reap the gains,
And poorly recompense their toils and pains.

Marie Collier (1739),
in *The Woman's Labour*

Abstract

This thesis discusses know-how protection schemes in rolling stock business cooperation, specifically focusing on transfer of technology. After essential terminology is defined, the state-of-the-art of industrial know-how protection schemes, based on literature research, is presented. The research also encompasses financial assessment methods of knowledge assets and its utilisation. Furthermore, this thesis investigates the current know-how protection conduct of a rolling stock manufacturer and analyses its risks and shortcomings compared to the state-of-the-art. Based on the investigation results several technical concepts for know-how protection are derived. These concepts undergo detailed evaluation of their cost-benefit to the collaborating rolling stock firm. The technical know-how protection method with the best evaluation score is automated data filtering. It uses a converter to automatically create documents from pre-defined content levels, which are then ready for transfer.

Table of Contents

1. Introduction

Intellectual property management has become increasingly important for innovative companies in western economy. This thesis deals with the categories in which intellectual property and know-how protection are defined and which valuation methods can be applied. Furthermore, this thesis provides recommendations for companies especially in rolling stock business to derive appropriate concepts regarding their knowledge protection strategies.

1.1 Motivation

In today's economy – a knowledge-based economy – wealth, investments and growth are mainly driven by intangible assets (OECD, 2013). The success of an enterprise is driven by intangible factors, while control over physical factors becomes progressively unimportant (Volkov and Garanina, 2007). Values obtained from physical resources and traditional factors, such as labour, land and capital are more dependent on the effective usage of knowledge (Andriessen, 2004). Intangible assets are a firm's nonphysical sources of value, such as its patents, brands, trademarks, copyrights, know-how and other intellectual capital. Intellectual property is of great importance to most companies to survive and grow. In fact some companies' intellectual property accounts for as much as 70% of the aggregated value of business (McGavock, 2002). Managing intellectual assets in the information age may be a newly emerged challenge with no close precedent (Teece, 2008).

Intellectual property provides the basis for corporate success. Properties such as patented technologies are the core condition for capturing huge market share, commanding premium prices, gain productivity and maintaining customer loyalty. Intellectual property is characterized by scarce supply and therefore highly valuable (Parr, 2018). An OECD study for United States and European Union suggests that business investment in knowledge-based capital contributes to 20% to 34% of average labour productivity growth. It also shows that in some countries business investment in knowledge-based capital significantly exceeds investment in physical capital and has been relatively resilient throughout recent global crisis (OECD, 2013).

Nowadays, western economy significantly suffers from intellectual property theft and know-how drain towards emergent competition especially from China and India where technological skills from western companies are purposefully and selectively acquired (Lawder, 2016; Mueller, 2005). Towards end of last century product imitations, copies of processes and usage of external know-how was limited on digitally transferable media, such as software, and luxury goods. In recent years more advanced technologies such as electronic devices, all kinds of vehicles, components of vehicles and capital goods, such as machines and equipment are affected (APA, 2015; Branigan, 2016; Larson, 2018).The subsequent effects for companies are ample. Most innovative companies invest extensively in research and development of novel products, technologies. Those investments carry high risks and must be refunded throughout the product lifecycle in order to fund more investments in research and development. A product imitation consisting of state-of-the-art know-how usually prevents the innovator from having the full return of investments. Imitators have less costs regarding research and development for the imitated product, thus can offer more attractive prices. Additionally, those companies are often producing in low-wage countries, which reduces the price as well. In 2013, according to estimations, 2,5% of the world's total trade volume was based on copies and imitations (OECD, 2016). In 2017 estimations by The National Bureau of Asian Research of the United States suggest that the annual cost for pirated software and theft of trade secrets of the U.S. economy exceeds 225 billion and could be as high as 600 billion US dollar (NBR, 2017). Product piracy alone is responsible for the loss of more than 800 000 jobs in the European Union (EESC, 2017). Consequences are severe, especially in industries where returns are rather low and price pressure from low-price competition can eliminate rentability and push companies into bankruptcy. Because intellectual property is an important source of value in companies in high-technology industries managing intellectual property is an important part of technology strategy (Shane, 2009).

Infrastructure and public transportation all over the world are widely under governmental control. Because of political reasons, bidding on rolling stock tenders often demands local added value. Thus, cooperation with a variety of different local companies, manufacturers, suppliers around the world are indispensable to ensure market competitiveness. Handover of know-how, mostly regarding engineering and

manufacturing to those companies is inevitable. Often manufacturers and suppliers from outside the rolling stock industry are enabled to produce major components of rolling stock of state-of-the-art. The emerging risks from an uncontrolled know-how transfer in a severe competitive situation like the rolling stock industry are ample.

The rolling stock market is under immense cost pressure. This is mainly due to recently created Chinese manufacturer CRRC. CRRC has emerged as a dominant market player across all segments and provides global products and services at a highly competitive price level (McKinsey, 2016). Upcoming development of new digital and IT solutions within the rolling stock market will require heavy investments by manufacturers in product development and by operators in product adoption (Leenen and Wolf, 2016).

It is most important to take full advantage of innovations for technological market leaders and protect intellectual property and know-how against market competition in order to maintain competitiveness and gain rentability growth (Porter, 1998). Furthermore, since intellectual assets are of most importance to any modern technology-based company, careless management thereof can ultimately be liable. In most legislations, the managing board is responsible to shareholders and creditors by law in terms of diligent conduct. It is apparent that mismanagement of any company's asset will hurt the competitive position of the company and thus, if happening carelessly, qualify for legal prosecution. In exceptional cases the directors are under threat of personal liability (Bundesrepublik Deutschland, 1966; Republik Österreich, 1966; Campbell, 2007). Table 1 gives an overview of common risks of insufficient knowledge protection and its corresponding benefits.

Knowledge potential	
Benefits of knowledge property	**Risks of knowledge drain/theft**
source of value	high technology imitations
growth driver	competition growth
investment driver	risking returns
market share acquisition	market share loss
further innovation	competitor`s education/learning
stock market growth	liability for senior management

Table 1: Knowledge potential

1.2 Goals and scope

This thesis has four main goals.

Firstly, a common understanding of the used terminology, such as intellectual property, transfer of technology and know-how, and its definitions are given. A description of all kinds of know-how, internal and external origins thereof are given. It is further looked at the rolling stock specific subjects of know-how and intellectual property. Identification of existing know-how is excluded from this thesis.

Secondly, the four categories of knowledge protection, legal, strategical, organisational and technical approaches are described and various concepts, specifically for protection of engineering know-how, introduced. This section answers the question, how knowledge in industrial circumstances can be protected. The organisational knowledge protection engages in structuring an organisation in terms of departments and interfaces to stakeholders, in order to achieve a most suitable organisational setup. In terms of organisational knowledge protection commonly underlying IT security systems and cyber security will not be further considered. Modern cyber security is a subject area of its own and certainly specifically contemplated elsewhere. Legal knowledge protection engages in intellectual property rights, such as patents, copyrights and trade secrets, and how to take most advantage of those instruments. Additionally, it is looked at common contractual protection mechanisms. The rolling stock market does not rely on trademark and branding rights. Hence, those legal instruments will not be looked at in detail. From the technical standpoint of knowledge protection, this thesis focuses on pre-emptive data protection and briefly engages in protection of physical knowledge but does not consider reactive data protection at all. For pre-emptive data protection this thesis gives an overview of the most promising concepts at the state of the art. Strategic knowledge protection engages in the shape of the business, specifically regarding rolling stock business. How does the structure of business in terms of customers, suppliers, partners, employees and other stakeholders affect knowledge protection and which strategic decision can be made in order to protect knowledge?

Thirdly, this paper describes common methods of know-how assessment and protection. It is exclusively looked at financial assessment of know-how, any technical

classification methods of the state-of-the-art are not discussed. The financial assessment focuses on the monetary compensation for knowledge and their different calculation approaches. In order to decide whether knowledge has to be protected or compensated if transferred, the company has to estimate the value of the particular intellectual property. This thesis looks at the different methods for financial assessment and discusses strengths and weaknesses. There will not be given any specific guideline to assess value of knowledge of any specific kind, even not for rolling stock specific knowledge, due to most likely exceeding the framework of this thesis by far.

Fourthly, this thesis investigates the knowledge protection conduct of a rolling stock manufacturer. All four categories of knowledge protection, legal, strategical, organisational and technical perspectives, are taken into account and specifically investigated regarding significant deviations to state-of-the-art conducts. Moreover, this thesis assesses the risk potential of the knowledge protection conduct currently exercised by the rolling stock manufacturer. It summarises the risks in knowledge leakage and its potential long-term effects on the business. It is looked at which kind of knowledge is at most risk and where the origins of such dangers lie. There is not any assessment of short-term effects on knowledge leakage. This thesis does not assess whether given conducts are diligently followed.

Fifthly, this thesis, based on the investigation of the current state at a rolling stock manufacturing company and the discussion of the state-of-the-art, derives concepts of know-how protection strategies. These concepts are further defined in a practical manner. For evaluation of the applicability and benefit of the derived concepts, a weighted analysis is introduced. The expected result is a most suitable knowledge protection method to close the gap regarding current and state-of-the-art protection conducts for the investigated rolling stock manufacturer. In principle the valuation is adjustable to any third party by adapting the weighted criteria and specific valuation. The derivation of the underlying criteria is contemplated. The criteria are weighted according to a paired comparison.

All major findings and future work needed, to achieve ideal knowledge protection for rolling stock business, are discussed in the last section.

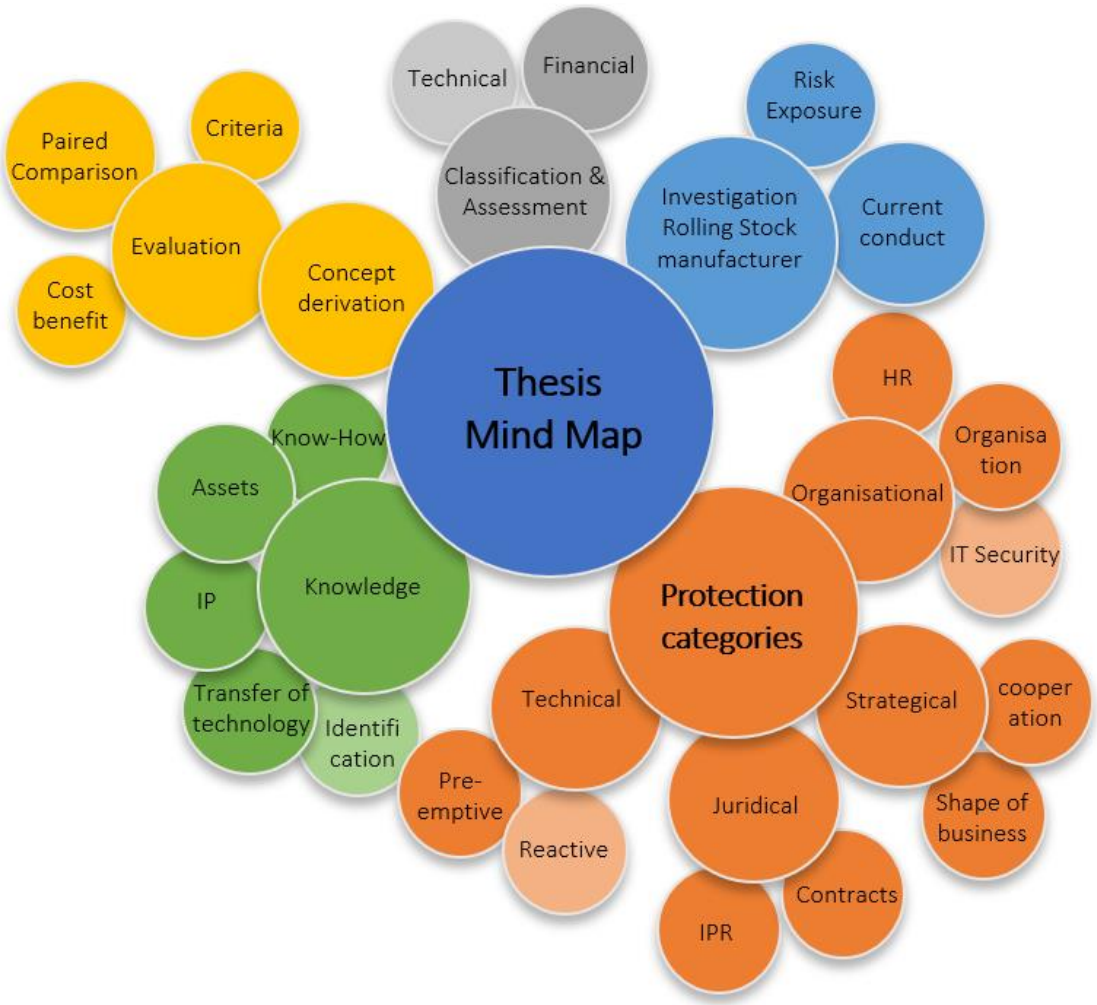

Figure 1: Thesis Mind Map

1.3 Approach and methodology

The work carried out is written in tight collaboration with a rolling stock company but nonetheless most of the goals are adjusted in a way of use for the business of the respective company. The methodology of this thesis primarily encompasses qualitative research approaches. In order to gain insight of intellectual property management and its protection schemes, a substantial amount of literature on the topic is reviewed and summarised. The literature review focuses not only on the relevant academic literature, but on popular science, non-academic sources and industrial institutes of standardization or registered societies of specific industry areas, which offer a broad set of practical approaches. Popular science or non-academic sources may be brought in occasionally to illustrate a point, but the central interest is always on the theories put together by recognized experts, academical or as representatives of a specific industrial sector. The literature review looks at as much of existing research as possible. It reviews major scholarly books in the relevant area, but will also take interest in journal articles, which in many subjects offer more up-to-date material. It is pursued to get a good balance between substantial academic sources and more recent journal articles. On many occasions, this thesis extracts information from codes of law and reviews for actual law of several of the more important legislations, such as United States, China or the European Union. This thesis summarises models for know-how protection, especially within business cooperation, mostly from literature review. These models follow a generic approach on a more conceptual basis, where specific schemes are derived in order to close the gaps between actual and desired knowledge protection conduct.

This thesis investigates current protection schemes for intellectual property at a rolling stock company, which is kept anonymous. Major sources are effective guidelines for know-how protection, process guidelines, interviews with experts of the intellectual property management and collecting personal experiences of protagonists within the business cooperation interfaces. Information from written guidelines and regulations is valued most, because of the official character of such, and possibly supported by expert experiences. Extracted information from such sources is kept anonymous. Interviews are only possible on a small-scale set. Assessing individual perspectives on the problem are more valuable than own investigations only. Large-scale interviews, in

order to establish a proper quantitative approach, is not possible, due to lack of interviewees. Nevertheless, it is expected to generate important additional insights from those interviews.

All findings are evaluated and draw a complete picture of the current know-how protection models within the company. The risk exposure is derived from all shortcomings relatively to the state-of-the-art protection methods.

This thesis also encompasses a quantitative research approach. Previously summarised models for technical know-how protection are examined through weighted analysis and further developed to fit rolling stock business conditions and specifics. The examination is mostly based on the model’s pros and cons and their applicability in the rolling stock business. The criteria are weighted through a paired comparison method and applied on to the analysis of protection schemes.

2. Terminology and definitions

A consistent processing of this topic demands definitions and uniform understanding of the terms in use. The following chapter defines and differentiates the most important terms, such as knowledge, intellectual property, know-how and gives an overview of knowledge transfer.

2.1 Knowledge assets and know-how

Knowledge is described in manifold ways and thus finding a generic definition seems hard. Knowledge is formed by information, experiences, values, standards and expertise. Knowledge can be differentiated into implicit and explicit knowledge categories. Implicit knowledge is composed by individual experiences, memories and values, thus tied to a person, hard to be formalised and communicated. Explicit knowledge is consciously describable, structured and thus easy to communicate (Nonaka, 1998).

Other sources apply different distinctions of knowledge. The term is divided into knowledge as information of any complexity and knowledge as a set of skills and competences. In this perspective knowledge is regarded as an asset. In a production process knowledge may appear both as an input (competence) and as an output (innovation). Under certain circumstances, it can be privately owned and bought and sold in the market as a commodity (Foray and Lundvall, 1998).

Davenport and Prusak define knowledge as a fluid mix of framed experiences, values, contextual information, and expert insight that provides a framework for evaluation and incorporating new experiences and information (Davenport and Prusak, 2000), which is similar to the definition by Nonaka (1998). Some sources define knowledge closely related to the ability to take action and decision making (Applehans and others, 1999; Dixon, 2000; Johannessen and others, 2001; Liebeskind, 1996). Knowledge can have many characteristics, most importantly knowledge is complex and neither completely public nor completely private (Lundvall, 2003).

For the purpose of this thesis, knowledge is divided in four categories according to Lundvall and Johnson (1994).

- Know-what
- Know-why
- Know-who
- Know-how

Know-what refers to facts, which is close to what is normally known as information. Know-why refers to knowledge about scientific principles, laws of nature or society. It enables to explain certain occurrences and gives an economic advantage if used for technological development in science-based areas. Mastering those categories of knowledge can be obtained through reading books, attending lectures or accessing information in any way. It is in greater or lesser extent openly accessible (Foray and Lundvall, 1998).

Know-who is the social part of knowledge. It involves the social ability to communicate and to co-operate and information about who bears knowledge about what. This kind of knowledge is important in the modern economy where there is a need to access many kinds of knowledge and skills. These are widely dispersed due too highly developed division of labour among the organisation (Foray and Lundvall, 1998).

Know-how is the fourth part of knowledge, as discussed above. It refers to skills and is closely related to actions and the ability to do something (Fantl, 2017; Lewis, 1990; Maier, 2018). Even though the economic value of know-how might seem limited to skills of production workers or machine operators, this conclusion is misleading. Know-how lies in various economic activities, not only the apparent practical skills, but managing skills or making business decisions, e.g. selecting the right personnel or screening market opportunities (Lundvall, 2003). Typically know-how is the kind of knowledge which is kept inside a company's border, where it was developed and obtained in the first place, usually from years of experience (Foray and Lundvall, 1998).

Know-how is the kind of knowledge with the most limited public access and for which transfer is the most complex. Attempts to use information technology to develop know-how show that it is difficult and costly to transform expert skills into information that can be used by others. It has also been demonstrated that the transformation always involves changes of the content of know-how (Hatchuel and Weil, 1995). Companies

usually get access to know-how by hiring experts or merging with companies which already possess particular know-how.

A distinction between know-how and knowledge has been made. This thesis does not model around openly accessible knowledge, but on know-how, since this is commonly kept inside the organisation. Know-how can further be distinguished in individual and collective know-how and internal, external and tacit know-how. An individual know-how is borne by an individual whereas collective know-how is borne by a collective. A know-how of an organisation is therefore a collective know-how (Ghrab and others, 2017). Furthermore, know-how is distinguished between internal, external know-how and tacit, explicit know-how (Nonaka and Toyama, 2003). Internal know-how is held internally by an individual, a collective, a unit or the organisation itself. External know-how is know-how held by an individual or collective external to the organisation (Ghrab and others, 2017). This distinction is based on perspective and helps to distinguish between the organisations own and external know-how. Whereas internal know-how qualifies for protection, external know-how cannot be protected as it is held by others. Whenever the term know-how is used, it genuinely stands for both, internal and external know-how, but it may be kept in mind that know-how protection is associated with internal know-how only.

Tacit know-how is rooted in actions, procedures, routines, commitment, ideals, values and emotions (Nonaka and others, 1996). It is difficult to communicate and to be formalised, thus mostly implicit. Tacit know-how is specifically bonded to time and space and can be acquired through shared direct experience, typically through practical hands-on experience. For instance, apprenticeship is based on this transfer of tacit know-how (Truch, 2004; Wang and Lv, 2017). Usually the possessor of the tacit know-how is unaware of its existence, due to its implicit nature. Tacit know-how contains expressible parts as well. Contrary to most tacit know-how, explicit know-how can be easily uttered, formalised, is accessible and transferable. Explicit know-how can be formulated in sentences and captured in drawings and writings (Nonaka and Krogh, 2009).

The first step of any sufficient protection of know-how is the identification of know-how (Abele and others, 2011). Without knowledge about the existing intellectual assets,

protection schemes are not able to cover the companies' know-how. The numerous existing methods for identification will neither be presented nor assessed in this thesis.

2.2 Intellectual property right

An important difference between tangible and intangible assets is the availability and enforceability of property rights. Physical assets are generally well protected. Ownership is relatively easy to define and the boundaries of the property relatively easy to ascertain. Not so with intangibles. Intellectual property tries to cover the protection of intangible assets (Nonaka and Teece, 2001).

Before a definition of intellectual property will be given, a short introduction to the terms of intellectual assets and intellectual capital is inevitable.

The difference between company market value and company book value has prompted academics and practitioners to consider the concept of intellectual capital as a key determinant of value creation for companies. In this sense, the identification and evaluation of knowledge, and other intangibles that produce or create value are main concerns related to wealth creation in the context of the knowledge-based economy (Viedma and Salmador, 2013). Intellectual capital has no commonly agreed definition. Marr and Schiuma define intellectual capital as the group of knowledge assets that are attributed to an organisation and most significantly contribute to an improved competitive position of this organisation by adding value to defined key stakeholders (Marr and Schiuma, 2001). Most definitions of intellectual capital set the knowledge and intangible asset of an enterprise as cornerstone of their definition, eventually resulting in value and benefit (Brooking, 1996; Edvinsson and Sullivan, 1996; Lev, 2001; Roos and others, 1997; Sveiby, 1997).

Poltorak and Lerner use a more practical approach and define intellectual capital as the sum of all knowledge in an enterprise. It is the knowledge of the company and provides the economic advantage. Intellectual capital includes the knowledge and skills of employees; the processes, ideas, designs, inventions, and technologies utilized by the firm, and the relationships it has developed with both customers and suppliers. It includes software, business methods, manuals, reports, publications, and databases.

It is basically what is left of an enterprise after it has been reduced by its tangible assets, such as land, buildings, machinery, inventory, and cash (Poltorak and Lerner, 2011). The various definitions are widely conformal and agree on a limited existence of intellectual capital, which lies in the context of the enterprise.

The proliferation of definitions regarding intellectual assets, revealed difficulties. According to OECD, the term intellectual asset is not commonly accepted, and some countries tend to use the term intellectual capital or intangibles or even knowledge capital. There is a widespread tendency to use the terms interchangeably. The core definition is common, a nonphysical asset with a potential stream of future benefits (OECD, 2006). While the OECD uses intellectual assets and intellectual capital as synonyms, Poltorak and Lerner define intellectual assets as intellectual capital that is identified, documented, and available to be shared and replicated within the organisation (Poltorak and Lerner, 2011).

These contradicting definitions hinder a proper discussion of intellectual property. For the purpose of this thesis, the definition by Poltorak and Lerner will be followed. The terms context is further depicted in Figure 2.

Figure 2: Overlapping intellectual property

Intellectual property is a term originating from legal practices and was largely limited to professionals operating in the field of intellectual property (Parr, 2018; Poltorak and

Lerner, 2011). Intellectual property (short: IP) establishes rights for inventions, writings, music and any other expressions of intellect falling into a favoured category. IP rights are rights for ownership created by law and granted automatically or by government agency or decree. IP rights receive protection, anything failing to belong to the favoured categories of expression is unprotectable and belongs to the public (Frank, 2006). Since the protected intellectual capital is supposed to be expressed, the boundaries shrink to intellectual assets in the definition above, which are documented and shareable. The right is not enforceable by possession but by action. A party holding those rights can, if it has the inclination, take action to prevent someone else who has no rights over that intellectual property from using it (Elmslie and Portman, 2006; Parr, 2018).

Intellectual property laws seek to benefit the general public by providing a rich, diverse, efficient, and competitive marketplace (Parr, 2018). Most intellectual property doctrines are crafted to balance two potentially conflicting goals. Firstly, provide an incentive to create by giving creators property rights, secondly, to provide the greatest possible competitor and public access to products of creativity to promote a competitive marketplace and progress. The diverse kinds of intellectual property rights, such as patents, copyrights, trademarks and trade secrets, all have different purposes. In the case of trademarks and related unfair competition doctrines, the law promotes marketplace competition and protects consumers from deception (Barrett, 2008; Elmslie and Portman, 2006). A further, more elaborated dedication to the topic of legal protection, will be given later, in section 3.1.1.

2.3 Knowledge in rolling stock industry

Knowledge management is widely recognized in the industry. Managing knowledge creation and sharing within and across the organisation is increasingly important (Wiig, 1999). Knowledge transfer is important, either within the firm and between different firms. The success of enterprises can be based on their ability to transfer knowledge in any form from one organisation unit to another (Szulanski, 1996; Wong and Aspinwall, 2005) as well as to improve their competitiveness by assimilating new technology (Camisón and Forés, 2010). During the past decades knowledge

management and tacit knowledge have become major research areas in corporate management (Bergman and others, 2004). Knowledge protection can be recognized as fraction of knowledge management. Knowledge management is known for sharing knowledge within the organisation and gaining access (Pandey, 2016). Having a true image of what kind of knowledge an enterprise possesses and which knowledge has to be created, in order to be successful, is significant either way. Thus, most companies have functioning processes for identifying knowledge.

Knowledge in rolling stock industry is mainly dictated by the product itself. A railway vehicle is generally engineered, manufactured, put into and maintained in service. Typically, rolling stock business is modelled around engineering knowledge, including industrial engineering focusing on manufacturing. Engineering design is linked to various kinds of knowledge, such as explicit and tacit know-how, but also scientific-based know-why. Engineering design is the process of transforming a set of requirements into a product description in compliance with a set of predetermined laws and procedures. Design is a labour intensive, knowledge rich, and creative activity (Mili and others, 2001).

Know-how in engineering activities is mostly tacit and often related to certain employees. The creative activity, whose fundamentals are based on know-why, is hard to communicate or explicated to others. Mili and others stated, that creative engineering is an activity rich in knowledge, in know-how and know-why. Many engineers gain their specific know-how through years of experience. The results of the creative process are easily recorded in drawings, design calculations and specifications. This is the explicit part of the design know-how and can be obtained through studying the resulting documents, or even reverse engineering (Teece, 1998). The creative know-how, e.g. the ideal parameters for strength calculations, is closely tied to the respective engineer. To conclude, it is important to divide into explicit know-how, which is depicted in drawings, specifications and calculation reports, and tacit know-how which is held by the engineer and its peers, also referred as competence (Teece, 1998).

Manufacturing know-how includes knowledge about assembly, function of machinery, course of production process, information about which measures are to be carried out at which time. Kryssanov and others emphasized that the know-how about

manufacturing can be acquired by way of instructions and training only. Even though the former commonly implies an explicit character, manufacturing related know-how is mostly tacit (Ahmad and others, 2014) and only transferable through proper training procedures (Kryssanov and others, 1998). While clues about manufacturing process may sometimes be cleaned by closely serving product, much about process technology can be protected if the owners of process technology are diligent in protecting the trade secrets in the factory. Thus, process technology is inherently more protectable than product technology, patent system put to one side (Ahmad and others, 2014; Teece, 1998). The level of knowledge needed for manufacturing depends heavily on the product. For railway vehicles a rather high amount of knowledge is needed. Even with outsourcing strategies and collaboration with many suppliers, rolling stock companies usually have know-how in welding of various materials, bonding with adhesive substances, mechanical and electrical assembly, commissioning and testing competences. Sourcing strategies, specifically in rolling stock business, are always guided by locational factors, such as access to knowledge (Ketokivi and others, 2017). This shows how important qualified personnel, which possesses the needed know-how, is to engineering and production facilities.

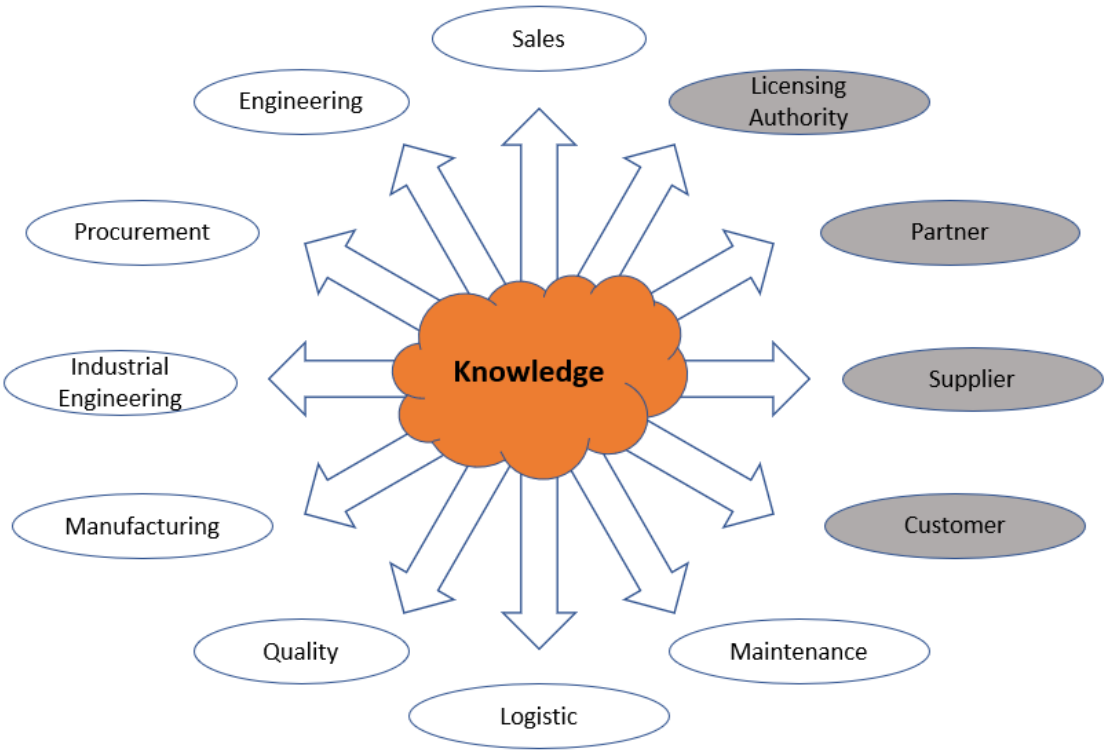

Figure 3: Knowledge transfer between internal and external functions

Rolling stock business specific knowledge is held by more stakeholders than just engineering or manufacturing. Figure 3 visualises all major knowledge owners and the multilateral transfer between knowledge owners. Furthermore, it illustrates that know-how is transferred internally and externally. These transfers may often be intended.

Within this thesis it will be looked at external know-how transfer, because knowledge leaving the company is of the most interest regarding risks of impeding competitiveness. While there is a severe development in intellectual property crime (Burgess and Power, 2008), this thesis will focus on transferred know-how rather than imitations, reverse engineering and other spill overs. Their existence suggests that it is possible to acquire technology without it being transferred, while at the same time not being independently developed. External know-how recipients can be customers, suppliers, partners or licensing authorities, even consultants to some extent. The knowledge subject to transfer, might be contained by products, processes, procedures, skills, competences and any kind of documentation, from bill of material or product specification to testing protocols. External know-how transfer is intended (Radosevic, 1999), even though often not fully under control (Wahab and others, 2011). Whenever a company transfers a product specification to a supplier, there is know-how transferred. Whenever a rolling stock company works with manufacturing partners, regardless of the underlying legal setup being a consortium or a joint venture, there is know-how transfer in order to enable the manufacturing partner to fulfil their scope of production. Often these partners have never had experiences with railway vehicle manufacturing. But even if they had, they are not familiar with the specific vehicle, which is planned to be manufactured and was beforehand engineered by others.

2.4 Where is knowledge protection applied?

Knowledge protection for industrial business is needed for preservation of knowledge and within business cooperation, specifically cooperation that demands transfer of technology between two firms. In the following paragraphs, both fields are discussed.

2.4.1 Transfer of technology

The systematic transfer of know-how in order to manufacture a product, apply a process, render a service is called transfer of technology (Albino and others, 1998; Di Benedetto and others, 2003; Radosevic, 1999; Sullivan, 1995; Wahab and others, 2011). Technology transfer does not only include the transfer of technical know-how and knowledge required to produce the product to the recipient but also the capacity to master, develop and later produce autonomously (Wahab and others, 2011). Gopalakrishnan and Santoro distinguish technology transfer and knowledge transfer in terms of their purposes. Knowledge transfer focuses on a broader and more inclusive construct which is directed more towards the “why” for change, whereas technology transfer focuses on a narrow and more targeted construct that usually embodies certain tools for changing the environment (Gopalakrishnan and Santoro, 2004). Even though there are different approaches existing, the majority of researchers agree that knowledge is the core of technology transfer. Hence, various parties are likely to hold different views and perceptions on these two concepts (Wahab and others, 2011).

The knowledge transfer between two or more actors (individuals or organisations) can be defined as the process by which the knowledge of one actor is acquired by another (Albino and others, 1998; Chun, 2007). It can take place by means of different ways, such as interaction of personnel, patent disclosures, publications, assets, service exchange and many more. It is possible to identify four components of a framework which are describing and influencing the knowledge interaction between two or more actors.

The actors of knowledge transfer can either be the organisation or the individuals. The actors’ relationship defines the effectiveness of the transfer. The context represents the conditions in which inter-organisational relationships take place, such as market characteristics, expectations of cooperation or socio-cultural aspects (Albino and others, 1998), but primarily the legal setup of the companies relationship (Radosevic, 1999).

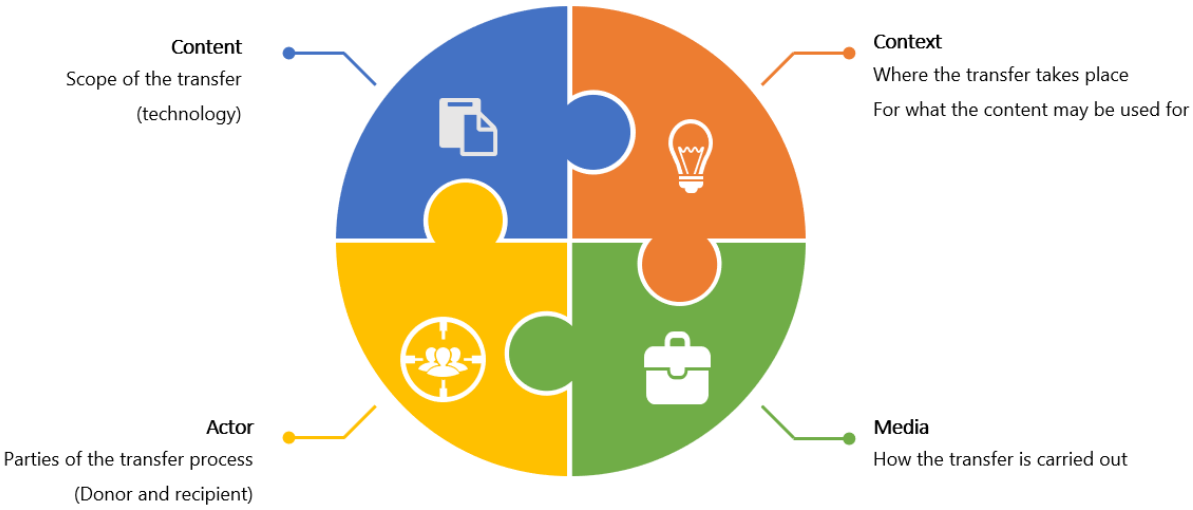

Figure 4: Transfer of technology framework

The knowledge transfer is then successful and only then when the ability associated with the transferred knowledge (owned by the transferring actor) is assimilated by the receiving actor. The necessary knowledge and the instruction to gain an ability is defined as content of the transfer. Media can be considered as every means useful for transferring data and information (Albino and others, 1998; Radosevic, 1999). Figure 4 depicts the discussed dimensions of transfer of technology.

Best practices and benchmarking knowledge can be transferred between different manufacturers. Customer agents may share product design knowledge with customers and receive customer requirements knowledge. While several knowledge transfer activities may have beneficial impacts on the company, harmful knowledge transfer activities are also possible. The context of technology transfer in rolling stock business depends on the legal setup of the actors. Legal setups which are devoted most attention to are joint ventures, consortiums, suppliers and licensing agreements. In perspective of rolling stock industry, actors are rolling stock companies and their specific partners. Content and media is mostly inseparable, e.g. transferring a certain product or component leads to defining the product as content and as media simultaneously (Bozeman, 2000). In rolling stock partnerships, transfer of technology contains products, components, processes, service instructions, skills, which can be

transferred via drawings, trainings, coaching and the product itself, also documentation which is relevant to suppliers, customers and authorities is transferred.

The technology transfer process involves transactional elements (costs, skills needed to perform transfer) as well as specific institutional setups. The transactional elements influence the measurement of transferred technologies, they are often inseparable from what is being transferred. Hence, it is difficult to identify the magnitude of technology transfer and almost impossible to separate trade of components and products from technology transfer (Radosevic, 1999; Wahab and others, 2011). Additionally, the magnitude of the transfer depends on the maturity level of the technology. Teece suggests that it is substantially easier to transfer a known technology for which there is operating and transfer experience than it is to constantly and continuously transfer state-of-the-art technology (Teece, 2000).

The conditions of the transfer of technology between collaborating firms are defined by a transfer agreement, a contract which rules all circumstances and scope of the transfer. The mutual understanding of the exact scope of knowledge transfer often draws difficulties with it. Hence resulting in a huge threat to know-how which initially was not an object of transfer. This issue is further contemplated in section 3.1.2.

2.4.2 Preservation of knowledge

Knowledge management is about creating, sharing and protecting knowledge. It is of most importance for knowledge-based companies to protect their knowledge from leakage or loss. Preservation of knowledge prevents losses and keeps knowledge at hand. This thesis is particularly discussing knowledge protection within business cooperation, thus focusing on transfer of technology and accompanied risks, however preservation is equally important. Preventing loss of knowledge is often a requirement for protection against leakage and exploitation by business partners or thirds. Hence, preservation is always drawn into consideration for knowledge protection schemes, the derivation of concepts and selection thereof. Most protection schemes for knowledge leakage that are further discussed also play a role in preservation.

3. Fundamental ideas of knowledge protection

Knowledge-intense data created and utilized in modern industrial systems is particularly at risk, because many stakeholders access sensitive content. In systems like the transfer of technology between firms, there is demand of appropriate means to limit the scope of transfer and to ensure know-how protection. Strong access restrictions are not always advantageous because cooperation between participants is interfered as well as the ability and efficiency of the collaboration systems thought is compromised. In the conflict between knowledge provision and knowledge protection, industrial enterprises demand appropriate protection means that solve the problem.

Protecting valuable knowledge and intellectual property of companies is assisted by various existing protection means. These can be distinguished in four different categories (Figure 5) depending on their type of utilization and implementation into corporate processes and infrastructure. In the following chapters, these categories and respective concepts for suitable means are discussed.

Practice shows that, none of the contemplated protection means is capable of solving the conflict of goals, the piracy and plagiarism situation or knowledge drain alone. Hence, the industry demands a wide range of different means to establish sufficient know-how protection (Grimm and Anderl, 2013).

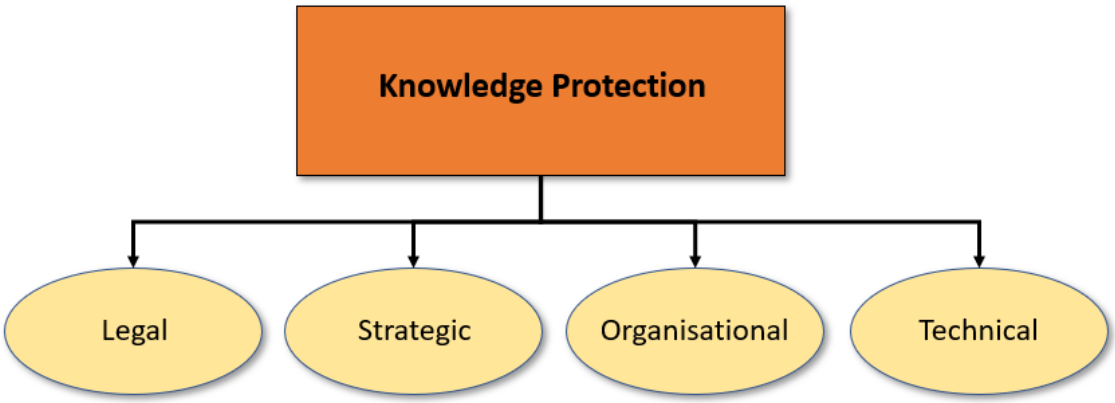

Figure 5: Knowledge protection categories

3.1 Legal knowledge protection

Legal protection means are primarily associated with intellectual property rights, such as patents, copyright, trademarks or trade secrets. Patents and trade secrets have substantial value for industrial environments. Trademarks and copyrights are just briefly covered. As explained above, the knowledge created, transferred and utilized within collaborations is at most risk. It is mostly overlooked that any collaboration agreement, such as consortium, joint venture, consulting collaborations or supplier agreements are based on contracts which rule the scope of exchanged information. Hence, these agreements give plenty of room to have appropriate means established prior to any meaningful other protection means. These instruments can be categorised as legal protection means. In the following section both frameworks and mechanisms to protect sensitive data are contemplated.

3.1.1 Protection under intellectual property rights

The term of intellectual property and its definition is covered in section 2.2. In this section intellectual property rights are under further review.

Intellectual property rights, such as design patents, utility patents or trademarks are well-established instruments to protect own intellectual property. They set a legal framework for the utilization of protected knowledge and enable the owner to pursue economic interests by civil law in case of illegitimate plagiarism or piracy. Importantly, those protection laws are subject to national law and can vary between different legislations (Neemann, 2007). Hence, this thesis adducts the standard of the World Intellectual Property Organisation (WIPO), which most countries have agreed upon.

Most importantly, intellectual property rights prevent the competitor just from using the obtained knowledge, not from initially obtaining it. Thus, it has to be assumed, that from publishing knowledge under intellectual property rights, competitors gain knowledge in general.

3.1.1.1 Patents

Patents are the most common protection right for technology-based intellectual property. National economies try to spread scientific progress and inventions through official publications thereof. The inventor usually lacks the incentive to publish the innovation, since there will be a lot of return lost by sharing the innovation to the public. Thus, most legislations offer a guaranteed, but temporary right for the monopolistic exploitation of the respective innovation. Patent rights ensure, that the inventor, who had the risk and all the expenditures for development of the innovation, get the deserved returns (Neemann, 2007). The duration of patent rights depends on national legislation and are commonly established for around 20 years. A patent conveys to its owner the right to prevent others from making, using, selling, offering for sale, or importing the patented invention. Patents are national in nature, having effect only within the territory of the issuing country. Patent law forbids a third party to use the patented innovation or to distribute products, which infringe patent law (Frank, 2006; Sas and others, 2014; Wölfel, 2003).

There are several different patent rights, plant patents, design patents and utility patents (Frank, 2006; Neemann, 2007). Plant patents cover reproduced plants and are primarily of interest only to plant breeders. Design patents cover the design of a product to the extent that the design or appearance is dictated by aesthetic, rather than functional, considerations. The majority of patents are utility patents, which this thesis focuses on. A utility patent may cover a device or an article, a composition of matter, a method or process of doing or making something, or, less commonly, a new application for an existing device or material, or a product made by particular new process (Poltorak and Lerner, 2011).

Any utility patent application needs to fulfil certain requirements to be issued. An invention has to be novel, useful and nonobvious. Novelty is applicable if the invention is not already state-of-the-art and not yet published. Usefulness is granted if the invention can be of industrial use and value. Non-obviousness is the most challenging requirement (Liebeskind, 1996; Parr, 2018; Poltorak and Lerner, 2011). To satisfy this requirement, the invention must not be merely a combination of elements of prior works, such as would be apparent to a person of ordinary skill who was seeking to

solve the problem to which the invention is directed (Neemann, 2007; Sas and others, 2014).

Patent rights are accessible in all countries, which are members in the World Trade Organisation (WTO) through the Agreement of Trade-Related Aspects of Intellectual Property Rights (TRIPS) and are mostly harmonised (Sas and others, 2014; WIPO, 2019). Patent law follows the principle of territoriality and is only applicable in the nation it has been issued (Parr, 2018; Sas and others, 2014). To circumvent plenty of single applications in several countries in order to have a wide scope of knowledge protection, there are two centralised institutions for patent application. Firstly, the European Patent Office (EPO) which is an institution established by the European Union and separately grants patent rights in all member countries upon issue of a single application. Secondly, the Patent Cooperation Treaty (PCT), which is an institution by the World Intellectual Property Organisation (WIPO) and has similar procedures (WIPO, 2019). Importantly, a successful application always follows a separate issue by the participating countries (Neemann, 2007).

Infringement actions are notoriously expensive (Poltorak and Lerner, 2011). Many patent disputes are resolved peacefully by commercial common sense because both parties realise that it is in no one's interest to fight a case out in court. Patent infringement actions usually involve a claim by the patent holder of infringement and a counter-claim by the alleged infringer that the patent is invalid and should never have been granted. As well as being expensive, patent actions are notoriously time-consuming and smaller competitors are usually at a disadvantage to larger companies with substantial funds to fight claims (Elmslie and Portman, 2006). In general, a patent owner can obtain money damages for past infringement and an injunction to prevent future infringement. Money damages may be based on the patent owner's lost profits or a court's estimation of a reasonable royalty (Frank, 2006).

Patent rights are well suited for the protection of any invention. It is then lawfully forbidden to make, use, sell, offer for sale, or import the patented invention for the specific countries, where the patent is pending and the yearly fees are paid, in all other countries the published invention is free to be used. Imitation and reverse engineering is thus less attractive to competitors. After a period of time - 20 years for utility patents in most legislations – the patent right expires and the invention is freely accessible.

While infringement actions are expensive, as explained above, the most profitable patent management might be licensing the invention to competitors. Licensing provides the opportunity to monetise technology beyond the inventors own capacities (Elmslie and Portman, 2006; Frank, 2006). It is distinguished between exclusive and non-exclusive licenses. Exclusive licenses are only granted to one other party, which creates duopolistic permission to use the invention. A non-exclusive license can be granted to numerous contractors. Both versions can be paid by a fixed figure or royalty-bearing, which defines a payment based on the actual revenues (Frank, 2006; Parr, 2018). Licensing offers an easy method to exploit patent properties.

3.1.1.2 Trade secrets

The patent and copyright laws encourage disclosure, bestowing protection as a means of ensuring the free exchange of ideas and information. Trade secret law performs quite the opposite function. It assists active efforts to maintain confidentiality. The law of trade secrecy is quite unconcerned with protecting innovation. The goal, instead, is to enforce norms of commercial conduct and prevent unfair competition (Frank, 2006). In some jurisdictions such secrets are referred to as “confidential information” or “classified information” (Sas and others, 2014).

Under the Uniform Trade Secrets Act (National Conference of Commissioners, 1985) trade secrets mean:

> “information, including a formula, pattern, compilation, program, device, method, technique, or process, that (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.”

A trade secret is information that is not generally available and that confers a competitive advantage upon its possessor (Elmslie and Portman, 2006). This broad definition means that nearly any type of business information can qualify as a trade secret. Hence, information that is not otherwise patentable can qualify.

Know-how is like trade secrets. As Correa states, for some authors know-how should be synonymous with trade secret. Although secrecy is certainly a condition for the validity of confidentiality obligations, it is not necessary for the classification of certain knowledge as know-how (Correa, 1981). Know-how is an industry knowledge or a skill capable of reproduction in some form, which is of value to a business. If it is not a secret, know-how is harder to protect. Supplier lists, parts specifications, and quality assurance and testing procedures generally fall into this category. This is, nevertheless, a requirement that is often overlooked. If information is to be accorded trade secret status, it must be treated as a secret by its possessor. At a minimum, it must be marked confidential, and reasonable steps should be taken to assure its security (Poltorak and Lerner, 2011). One of the advantages of trade secrets is, that it is not limited in time. But as soon as secret know-how is disclosed to another party, it loses its protection. Even though it can be protected by imposing a contractual obligation on a party, to whom it is disclosed, not to use it for other purposes, it is difficult to show that there has been an abuse of the obligation by a business partner (Elmslie and Portman, 2006). Transfer of technology, for instance, could be protected by contracts, but as soon as manufacturing processes, or techniques of any kind are disclosed, it is certainly harder to keep track of the formerly secret information. What makes infringement harder to discover, opposite to patent law, is that an infringer who has independently discovered the patented invention is an infringer nonetheless (Poltorak and Lerner, 2011), but not so with trade secrets. So long as the secret was rediscovered lawfully through independent research, reverse engineering, discovery under license from the owner, observation in public or obtaining from public literature, the trade secret protection is lost (National Conference of Commissioners, 1985). This usually occurs, for instance when know-how owner of a firm changes to another firm and carries valuable know-how, which might be even tacit. Effectively, the owner must have evidence, that it is an unlawfully infringement and was not obtained elsewhere. The level of protection granted to trade secrets varies significantly from country to country, but is generally considered weak, particularly when compared with the protection granted by a patent (Parr, 2018). Once confidential information leaks out it is difficult to recapture its value (Elmslie and Portman, 2006).

Trade secrets are best employed as protection for manufacturing or other processing techniques that are performed in the privacy of one’s own facility and that cannot be

discerned from an examination of the product produced thereby. Another suitable application involves information as to which only temporary protection is required. Most commonly, this involves a new product or process for which protection is sought only until market introduction to obtain the first mover advantage. Most business methods, if not patented, should be treated as trade secrets (Poltorak and Lerner, 2011).

3.1.1.3 Copyright and trademarks

For the sake of completeness of all intellectual property protection rights, copyrights and trademarks are briefly covered.

The copyright law does not play a major role for technology-based inventions. A copyright is a form of protection provided to the authors of original works of authorship, including literary, dramatic, musical, artistic, and certain other intellectual works both published and unpublished. It protects the form of expression rather than the subject matter of the work (Neemann, 2007; Parr, 2018). While it is applicable on software, it only protects against actual copying and independent development is not an infringement (Frank, 2006), thus computer software has recently become the subject of patent applications (Poltorak and Lerner, 2011). The eligibility criteria for copyright are minimal, it needs to have a certain originality and fixation in a tangible medium of expression. Since copyright does not have a major impact on knowledge protection for technology-based companies, it is not engaged in any details.

Trademarks and brands are generally playing an increasingly important role in the process of making and selling products (Elmslie and Portman, 2006). For industrial knowledge, trademarks are not applicable.

A trademark is used to identify the source of a product or service and to distinguish that product or service from those coming from other sources. It can be a word, symbol or combination thereof (Poltorak and Lerner, 2011). A trademark also serves as an assurance of quality. The consumer comes to associate a level of quality with the goods or services bearing a given trademark. They convey product characteristics such as quality, value, safety, and prestige (Parr, 2018). Trademarks are beneficiary

where the customer has no direct contact to the producer and has to rely on trademarks as assurance of origin.

Intellectual property rights as protection means are all limited to some extent. They are extremely limited or non-existent for knowledge that is only partially original, or tacit, or is long lived. Thus, there is a significant amount of knowledge that may be valuable to a given owner but cannot be protected against expropriation and imitation under the law. Patents, copyrights and trade secrets qualify for codified knowledge only, tacit knowledge is excluded. Patents and copyrights only apply for entirely original products or processes and protection has a limited lifetime. Patents also only protect against observation and publicity but reveal knowledge to the competition. Trade secrets do not reveal knowledge but don't protect against reverse engineering or independent invention. All intellectual property rights are costly to enforce, and patents additionally are costly to be defined and registered. In addition to that, they can be circumvented and even legitimate actions for injunction or compensation often take a long time.

3.1.2 Legal protection means in business agreements

Collaborations between firms are usually supported by contracts. This applies to consultants, partners within joint ventures or consortiums or suppliers. Contracts can explicitly identify information that has been designated as proprietary and define which information and capabilities are to be shared, as well as expressly identify information and capabilities that are not to be shared (Correa, 1981). A more active approach imposes contractual or legal penalties if an alliance partner deliberately accesses or uses information inappropriately. For instance, a contractual clause may specify monetary penalties or contract termination for violations of knowledge protection agreements (Norman, 2001). If a violation occurs, significant damage is already done. Another problem is that violations may not always be detected.

Confidentiality agreements or non-disclosure agreements (NDA) are commonly signed before potential partners exchange valuable information or start negotiating. It is one of the most important business contract types. A non-disclosure agreement is a legal contract between at least two parties that outlines confidential material, knowledge, or information that the parties wish to share with one another for certain purposes but

wish to restrict access to by third parties. It is a contract through which the parties agree not to disclose information covered by the agreement. An NDA creates a confidential relationship between the parties to protect any type of confidential and proprietary information or trade secrets. As such, an NDA protects non-public business information. Reliance on NDAs to protect critical knowledge adequately may create a false confidence in many instances. Norman suggests, that NDAs are one of the least effective knowledge protection methods (Norman, 2001).

For transfer of technology agreements, the exact definition of what is transferred and what not, is most important to have a mutual understanding and not get forced to transfer more than agreed upon in the first place. Agreements therefore must be well negotiated and be rather specific when it comes to transfer content and responsibilities for the collaboration. For example, enabling a manufacturing partner to produce a specific new product can range from transferring the necessary technical documents to having full-time support on site for the entire duration of manufacturing. Not having defined exact boundaries of such contracts can lead to unforeseen knowledge drain and additional costs.

Employees usually must sign confidentiality agreements upon hiring as well. Since employees are major knowledge sources, this is specifically contemplated in section 3.3.2,**Error! Reference source not found.** under human resource specific organisational knowledge protection.

Contractual protection means in business cooperation, such as NDAs, are considered weak as detection and prosecution of infringement is difficult and expensive. Even though it sets a legal framework for the handling of confidential information, it does not protect the company from the contractual partner obtaining any information that the partner is disclosed to. NDAs are most useful to regulate confidentiality towards a third party. Existing patents in the same area and the use of non-disclosure agreements may have the same enhancing effect on the willingness to share knowledge because each partner’s inventions are protected. It is easier to detect which rights belong to each of the partners when there are patents protecting the background knowledge. This could reduce the need for time-consuming negotiations about rights and prevent unwanted disputes in unclear situations.

3.2 Strategic knowledge protection

Strategic knowledge protection is targeted at controlling knowledge in a long-term company strategy. Strategic means can be divided into two categories, assessment of knowledge and derivation of policies, guidelines and procedures. Strategic knowledge protection is strongly connected to the firm's senior management (Norman, 2001). It is not specifically about the final protection mechanism, but enhancing awareness within the firm, developing a strategy for knowledge protection, even funding the efforts (Norman, 2001; Sveen and others, 2007) and building the cornerstone for successful knowledge protection. A clear corporate vision that emphasises the organisation's goals and values and the role that knowledge plays in achieving those goals are fundamental parts of a strong knowledge culture. A decision whether knowledge shall be shared with others and whether strategic alliances shall be established, is also a part of senior management decision-making and essential for shaping the strategy on knowledge assets. A question with strategic character that must be answered by the management, is whether knowledge sharing and gained competitive advantages outweigh the drawbacks drawn into the system. Senior management must be aware of existing knowledge assets and probable risk exposure in order to make reasonable decisions.

Knowledge protection derives from knowledge management strategy of the firm. A research paper by Maldonado-Guzman and others suggests, that dedication to knowledge management results in creation of more intellectual property (Maldonado-Guzmán and others, 2016). This emphasises, that dedication to knowledge management by senior management may result in more innovations and creation of knowledge assets, that need protection.

It is important to note, that capabilities of firms to protect knowledge depend on the legal-regulatory context in which the firm operates (Liebeskind, 1996). Some jurisdictions are far more restricting when it comes to controlling actions of employees or enforcement of intellectual property rights or claiming contract infringement. This must always stay in consideration when determining a strategy.

In the following sections the categories, in which strategic knowledge protection is defined, are further discussed.

3.2.1 Technical assessment of knowledge assets

Knowledge that is valuable, rare and non-substitutable needs to be identified accompanied by the risks that need to be considered for these assets. The identification is key to mitigate risks arising from knowledge transfer. A typical risk assessment process begins with identifying data, information and technology assets that might be exposed to risk, and quantifying threats associated with them (Rees and others, 2003). The evaluation can be challenging since it can be highly subjective. As soon as the identification and assessment is done, experts can design, select and apply the most sufficient mechanisms to protect the knowledge (Aljafari and Sarnikar, 2009). Having a well-functioning and systematic identification and classification frame can assist in identifying threats and later identifying protection policy. Ahmad and others suggest, that many firms lack systematic analysis of knowledge and risk assessment (Ahmad and others, 2014).

The first step is always locating the knowledge asset source and assessment of the asset. The following Figure 6 about knowledge reservoirs, which helps identifying the sources of knowledge, is adapted from literature (Aljafari and Sarnikar, 2009).

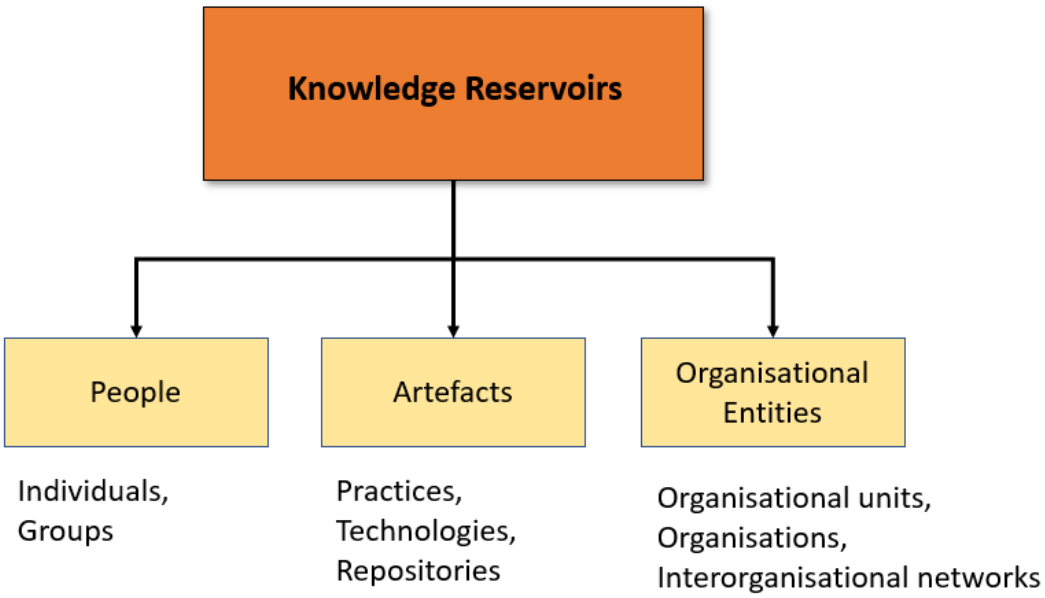

Figure 6: Knowledge sources

Knowledge assets are further assessed by value, rareness and imitability. One of the recognized schemes after Carlsson:

- Value: Does the knowledge enable the firm to sense and respond to opportunities and threats in the business environment?
- Rareness: To what extend do competing firms possess similar knowledge?
- Imitability: Is the knowledge resource costly and difficult to acquire for other organisations that do not own it to obtain or imitate? (Carlsson, 2003)

These assessments are recommended to be conducted in collaboration with the respective owners and users of knowledge. Senior management levels usually do not have enough expertise in the field to assess knowledge assets diligently by themselves. In further assessments, the company identifies inter-organisational knowledge sharing practices, collaboration technologies in order to derive current vulnerability and threats to the system (Aljafari and Sarnikar, 2009). Thus, the firm can answer the question which knowledge should be protected, and which should not. Knowledge protection is very costly, and overprotection will excess costs. At best companies only protect their unique and valuable knowledge, which is capable of repaying the costs for protection (Liebeskind, 1996). Examples of valuable and rare assets include key employees, products, processes, routines or procedures (Ahmad and others, 2014). In section 4, this thesis discusses how knowledge assets can be classified in terms of financial value, which is required to weigh up protection costs against value.

3.2.2 Procedures, guidelines, policies

Strategic management actions to protect knowledge assets focus on the development, implementation and resourcing of policies, procedures and guidelines in order to control the flow of sensitive data and knowledge. Additionally, protection processes and mechanisms need to monitor knowledge flows between stakeholders and owners of knowledge (Bloodgood and Salisbury, 2001; Desouza and Vanapalli, 2005). Which mechanism or combination of mechanisms shall be used to protect valuable knowledge is an important question. Using too many protective measures at the same time will incur excess costs. Some knowledge flows are essential for innovation,

especially regarding collaborations (section 3.2.3), which could lead to trade-off decisions between protection and innovation.

Knowledge related processes can be distinguished into acquisition-oriented processes, conversion-oriented processes, application-oriented processes and security-oriented processes (Gold and others, 2001). Security-oriented processes are designed to protect the knowledge from inappropriate or illegal use or from theft. A field study by Ahmad and others suggests that formal policies, procedures and guidelines for the purpose of knowledge protection are rather rare (Ahmad and others, 2014). Senior management needs to implement suitable policies, procedures and guidelines on intra- and interorganisational knowledge sharing and acceptable use of collaborative and communication technologies. Procedures and guidelines help employees to have an identical understanding of the right behaviour in terms of knowledge protection and connects all established mechanisms to one functioning frame of either knowledge transfer or knowledge protection. Such guidelines need to be practical to assure proper realisation. Operational processes are further contemplated in section 3.3.1. A knowledge protection culture may need to develop as well in order to raise additional awareness. Forming such an organisational culture is challenging, it is primarily impacted by the interaction of employees within the firm and their behaviour in communication and teamwork (Gold and others, 2001).

Protection of knowledge assets demands monetary efforts as well. Management needs to fund knowledge protection efforts (Norman, 2001; Sveen and others, 2007). Without sufficient resources, none of the proclaimed protection schemes is likely to work.

3.2.3 Business connections

The high level of technological change and complexity, the ability to access and leverage diverse knowledge-based assets from complementary sources are essential, thus networking and collaboration gets increasingly important (Hurmelinna-Laukkanen, 2011; Miles and others, 2005). Alliances between organisations necessitate some sharing of information between business partners (Ahmad and others, 2014).

Alliances also introduce the potential of knowledge leakage (Norman, 2001), possibly losing competitive advantage if core knowledge flows out to competing organisations (Hurmelinna-Laukkanen, 2011). Some studies confirm that increasing circulation of knowledge increases the risk of leakage (Desouza and Vanapalli, 2005; Easterby-Smith and others, 2008; Trkman and Desouza, 2012). However, a study by Hurmelinna-Laukunnen suggests, that in addition to the benefits derived from preventing and delaying imitation, embedded in the protection mechanisms also resides the potential for improved exploitability of the knowledge assets through safe and controlled knowledge exchange (Hurmelinna-Laukkanen, 2011). Companies with well-functioning protection mechanisms may have to worry less about other organisations abusing it, thus engage in different joint operations and share its knowledge more freely in joint innovation. This offers many opportunities to gain more advantages in the collaboration. However, engaging in business collaborations impacts the introduced knowledge protection means. Selection of protection mechanism requires careful consideration of knowledge sharing.

For rolling stock business partnership, this means that for research and development within an interorganisational collaboration a strong knowledge protection mechanism improves innovation performance and increases knowledge sharing. In terms of manufacturing partnership, it is less likely to have similar advantages. In this case it just serves the protection purpose to prevent imitation and leakage. Hence, senior management must be aware of certain aspects regarding knowledge sharing and leakage in business connections upon making a partnering decision. When outsourcing, it is recommended to not simply clone part of the production environment to send oversees, this leads to an increase in knowledge leak. It needs to be ensured that the outsourcing partner is fully prepared to handle sensitive information. This helps preventing the firm from poor decisions in partner selection and maintaining governance over the shared knowledge (O'Donoghue and Croasdell, 2009). Manufacturing partnership is usually accompanied by transfer of technology, as contemplated in section 2.4.1. Whether transfer of technology can be provided without strengthening a potential competitor must be well-considered and is a top down decision by senior management as well.

3.3 Organisational knowledge protection

Organisational knowledge protection mechanisms engage in structuring an organisation in terms of departments and interfaces to stakeholders, regulations on an operational level and employment management. IT security facilities are closely connected to interfaces within a firm but will not be part of this thesis. Engaging on IT security would exceed the frame of this thesis by far.

3.3.1 Operational processes

Operational-level knowledge protection processes are essential to secure sensitive organisational knowledge (Gold and others, 2001). Such processes affect the conditions of knowledge and information flows and impact activities associated with organisational collaboration (Ahmad and others, 2014). Examples include processes that compartmentalise knowledge to specify off-limit knowledge and limit information flows between different parties (Desouza and Vanapalli, 2005).

Knowledge protection processes include mechanisms to classify knowledge in terms of its sensitivity level as a basis for allocating access rights to organisational employees. There are basically two contradicting knowledge processes, one is preventing knowledge loss by making knowledge explicit and the other is preventing leakage through keeping knowledge tacit (Graf, 2011; Norman, 2001). Both processes must be implemented to keep a stable balance between the need to prevent loss and the need to prevent leakage.

3.3.1.1 Compartmentalisation of organisations

Operational regulations rule the interfaces of stakeholders, their processes, inputs and outputs. Many organisations are divided in departments of various competences, functions and tasks. Most companies organise departments in teams, enhancing communication by sharing offices and forming own hierarchical levels. Hence, the firm’s activities, competences and its knowledge are compartmentalised. Operational

processes are often used to control the information flow between departments and teams. Controlling the communication leads to control over information. Potential leakages can be minimised by having the core knowledge split between departments and people (Bloodgood and Salisbury, 2001; Desouza and Vanapalli, 2005; Liebeskind, 1996). Having consciously set barriers for information transfer between stakeholders in the supply chain can have a big impact on knowledge protection. This can be applied for manufacturing partnership as well (Neemann, 2007). A company could provide incognito raw material to a manufacturing partner, that is not able to imitate the process without knowing the composition of the raw material. Another example is a component supplier, that may have the knowledge on mechanical manufacturing of the component but do not know anything about the subsequent vernier adjustment or implementation of control software, which are very knowledge-heavy work steps.

3.3.1.2 Classification of information

Knowledge is not always equal to knowledge thus it needs to be distinguished in order to apply a reasonable behaviour. The distinction is mostly done by individuals on their own assumptions and interpretation. Most of the literature presumes rationality in decision making (Thompson and Kaarst-Brown, 2005), research into interpretations of information technology has indicated that the same systems can be interpreted differently (Kaarst-Brown and Robey, 1999). It is therefore highly dependent on human judgment, because it requires someone to interpret the content of the document. Classification can be automated by establishing algorithms that classify after certain keywords or phrases as well. If the sensitivity level cannot be obtained from text phrases, but considering the overall context is needed, then classification is considerably more complex and requires an understanding of which cues individuals are more sensitive to (Thompson and Kaarst-Brown, 2005). Judgement is best supported by existence of rules or guiding schemes. Organisations need to establish a common understanding about classification schemes to have proper handling of the respective knowledge assured.

3.3.1.3 Codifying vs. keeping knowledge tacit

As we discussed previously in section 2.1, there are two general classifications of knowledge with which firms must cope. These are explicit knowledge and tacit knowledge. Companies intent to gather information and knowledge in explicit form. This is either because explicit knowledge can be spread better than tacit knowledge and cannot be accidentally lost as easily as tacit knowledge. On the other hand tacit knowledge is a lot safer. It is less likely to get leaked because it lies in the individuals. In matter of knowledge management, there are two processes. One is focusing on gathering knowledge, codifying it and sharing it within the organisation, preventing loss of knowledge. The other is managing tacit knowledge, keeping tacit knowledge implicit and preventing costly leakage (Graf, 2011; Norman, 2001). Tacit knowledge is easier to protect. Factors that make replication difficult also make imitation difficult. Thus, the more tacit the firm's productive knowledge the harder it is to replicate by the firm itself or its competitors. When the tacit component is high, imitation may as well be impossible, absent the hiring of key individuals and the transfer of key organisational processes (Teece, 1998). Which process suits the transfer of knowledge the best depends on the circumstances and matter. For instance, in product development collaborations it is usual to gather extensive data on the product to share information between the involved stakeholders easily. Manufacturing partnering, the training of staff in specific processes is better conducted in transfer of tacit know-how.

3.3.2 Binding of human resource

The most valuable intellectual capital of a company often lies in the knowledge reserves of its employees. The available options to a company to protect tacit knowledge also depend heavily on its employees' ability and willingness to protect their tacit knowledge against any third party. An employee departing a firm always means losing some tacit knowledge. If the tacit knowledge is previously codified, the protection means demand higher efforts than before (Olander and others, 2015). Commitment to an organisation and its goals, and an intention to stay with the organisation, are desirable. Companies actively promote positive organisational citizenship behaviour

and trust and affect reduced turnover, increased productivity, and job satisfaction. These kinds of promotions are mostly carried out by means of rewards enhancing ownership behaviour and bonding the employer to the company. An organisational capability that allows firms to protect knowledge is the ability to design jobs and write employment contracts. When an individual becomes an employee, they agree, contractually, to obey the orders of their employers (Ahmad and others, 2014). Thus, a primary feature of an employment contract are rules. Through such rules a firm can restrict the actions of an employee. Two types of rules are particularly important in relation to knowledge protection, which are employee conduct rules and job designs.

Employee conduct rules serve to reduce the mobility of the employees and hereby reducing the mobility of the knowledge they possess. Employment contracts stipulate that the employee must work exclusively for the employer in question which is considered anti-competitive clause. In addition there are confidentiality agreements (Ahmad and others, 2014) within the employment contract and a firm may write a contract that contains a non-competition clause that forbids the employee from working for a competitor for a given period of time after leaving the firm (Liebeskind, 1996). Having genuinely loyal employees is even better. Enhancing loyalty, also means enhancing commitment-based knowledge protection (Olander and others, 2015). Knowledge leakage through fluctuation is thus limited. Any measure, that prevents fluctuation or enhances the attachment of the employee to the firm also reduces potential knowledge leakage (Liebeskind, 1996).

Another valuable knowledge protection method in employment is disaggregation of information. Disaggregation can be achieved by adjusting job designs. By compartmentalizing processes, information can be divided between stakeholders in a way that none of the stakeholders has the entire information. Hence, leaking valuable information voluntarily or by accident is not possible.

3.4 Technical knowledge protection

Technical knowledge protection is a main topic of this thesis. Technical knowledge protection can be distinguished in protection of data and protection of physical objects. Both have quite an important standing in industrial context. Data protection can further

be divided in pre-emptive and reactive protection mechanisms. Reactive mechanisms are excluded from this thesis, the overall focus lies on pre-emptive protection means.

The general context in which technical protection mechanisms are discussed, is the transfer of technology in collaborations. It is further discussed how know-how can be protected by means of technical protection measures.

3.4.1 Technical protection of physical objects

Physical objects such as prototypes or complete products contain and represent knowledge in a materialized form, which can be protected by obfuscation methods, decomposition barriers and design methods (specialised manufacturing process, surface technology). These will further be contemplated. In addition to that, different identification technologies can be used to tackle plagiarism, piracy and loss of knowledge in cooperation and supply chains (Grimm and Anderl, 2013). Since rolling stock business does not suffer from simple plagiarism and product piracy, these identification technologies for assuring the origins of the product are not applicable and therefore excluded from this thesis.

3.4.1.1 Obfuscation of objects

Obfuscation methods hinder reverse engineering by potential imitators. Obfuscation methods are also applicable for protecting designs of prototypes (Seeger, 2014). Obfuscation works after a black boxing principle (Neemann, 2007). Either functional components are encapsulated, which is known as functional black boxing, or fake black boxing is used to mislead reverse engineering. Fake black boxes just pretend to have a significant function and eventually provoke the imitator to stop reverse engineering efforts. Increasing the resistance to reverse engineering by increasing the necessary efforts, enhances protection.

Using functional black boxes requires the component to have a minimum function within a modular product system. In practice, electronic devices have the highest

inclination to obfuscation, besides digital elements. Software often consists of program elements that are easily black boxed and hard to analyze. Mechanical black boxing is rather rare. A mechanical concealment of a function can offer additional protection, if opening the box is not possible without destroying the function itself. This directly leads to knowledge protection through decomposition barriers.

3.4.1.2 Decomposition barriers

Decomposition barriers are protection mechanisms that permanently destroy the product or a single component when deconstructed. It can only be applied in components, that must not be deconstructed by customers but by a potential imitator in order to reverse engineer the product. Decomposition barriers are commonly known as self-destruction elements and fulfil the purpose of denying access to functional elements of the product. These elements hinder the imitator to acquire the know-how which is materialised in the respective element. Several possible decomposition barriers are conceivable, for instance rapidly aging mechanical devices (rapid corrosion) or systems capable of physically disappearing in a controlled, triggerable manner, such as predetermined breaking point (Hsu, 2015). Neemann suggests that decomposition signals that are emitted when a device is deconstructed, may be able to destroy another function of the product (Neemann, 2007). The number of potential barriers is ample.

3.4.1.3 Design methods

After an imitator has obtained knowledge from reverse engineering or any other source, which is enough to allow an imitation, the reproduction of the specific product can be further impeded. Through complicating manufacturing, the imitator is possibly not able to reproduce the product. There are several mechanisms that are discussed in the following paragraph and are summarised under manufacturing-related protection mechanisms. All these methods work regardless of where the imitator has the knowledge obtained from. The acquisition of knowledge in this case is not limited to

physical objects. However, manufacturing leads to a physical imitation. Since these measures are preventing an imitator to imitate a physical object, it is listed in this section. Further discussed measures are de-standardisation of components, own development of jigs and fixtures and one-time cost intensive manufacturing.

De-standardisation is based on industrial standards for components, which are established to save costs through scaling and ease of integration. De-standardisation does not use standard components, but components which are not accessible for an imitator. De-standardisation can also be used to mislead imitators. Neemann suggests that the actually utilised de-standardised components should not be evident in order to mislead the imitator. This works exceptionally well in products where small deviations have a major impact on the product quality (Neemann, 2007).

Development of own jigs and fixtures for manufacturing processes is crucial for manufacturing industries. Jigs and fixtures need to be engineered and manufactured in order to produce a legitimate imitation. Without having access to the jigs & fixtures the imitator needs own engineering efforts or needs to reverse engineer these as well. Both increase the protection level substantially.

Imitators are discouraged to enter a market with an imitation, if the manufacturing is one-time cost intensive. On one hand this requires a lot of investment from the imitator to establish a production and on the other hand it increases the dangers of flop. For instance, if legal infringement is confirmed and the sales of the imitation are prohibited, the extensive investments backfire (Neemann, 2007).

3.4.2 Technical protection of data

Digital product data can be protected by using methods that influence the processing of data or manipulation of data. This sub-category can be divided into reactive and pre-emptive protection methods (Grimm and Anderl, 2013). Latter are further discussed, and reactive protection means are excluded from this thesis. Data is defined as immaterial information.

3.4.2.1 Pseudonymisation

Pseudonymisation of documents is a knowledge protection mechanism that takes effect when technical product data, such as drawings, specifications, design reports, are obtained by potential imitators. Pseudonymisation of documents means, that the origins and purpose of such documents are not obvious. This includes removal of the firm's symbol and identification, use of internal product nomenclature and use of acronyms and abbreviations. It is assumed to have particular permission to use documents without the real nomenclature. In rolling stock business, the customer always gets uncodified, real documentation. Thus, pseudonymisation of documents might only be applicable in product development phases and loses its protection as soon as commercialisation of the product is started. In collaborations for product development, pseudonymisation protects against a third party only. The partner firm needs to have certain keys to resolve pseudonymisation in order to access the real information.

Pseudonymisation is a particularly strong protection mechanism if the characters and numbers play a significant role in protection of the underlying information.

3.4.2.2 Data filtering

For internal use, documents usually depict the full extent of information. Documentation is archived in the same way and whenever a business partner needs specific information, the documents are handed over in their original version. Manufacturing partners, suppliers, customers, consultants get access to the same document but have different needs of information. Thus, the collaborative partner gets access to a data set which exceeds the information needed. In order to prevent such leakages, the transferred data gets filtered. This approach is known as data filtering. Data filtering is the most important engineering knowledge protection approach that is based on knowledge reduction principles (Grimm and Anderl, 2013; VDI 5610-2, 2017). Individual elements containing valuable knowledge are intentionally removed from documents before these documents are exchanged. Hence, the overall knowledge

amount stored in specific documents is decreased to minimize risk of knowledge loss. Prior to removing parts of documents, knowledge containing elements have to be identified and classified first. Manual filtering of data is time consuming and an error-prone process, once knowledge is removed, filtered documents can be securely distributed. Automated data filters circumvent high efforts in manually filtering information. A predetermined distinction of which partner receives which level of information, enables preparation of such data by software tools.

The industry association ProSTEP ivip suggests the use of a knowledge editor. The editor software searches for valuable information requiring protection. The editor can cancel the respective information on a digital twin of the original document and then transfers the filtered document to its intended receiver. The knowledge editor is applicable for smaller groups of components or single parts. Editing bigger volumes of information is not sufficient (Stjepandic and others, 2008).

3.4.2.3 Special agreement with authorities

In many industrial sectors, manufacturers are obligated to fulfil certain requirements for documentation of their products. Because of the rising issues with product imitations, many authorities allow exceptions in documentation (Neemann, 2007). Those exceptions make it harder for imitators to acquire information. Such special agreements are rather rare. Safety-related documentation on homologation must be part of official product documentation.

3.4.2.4 Enterprise rights management

Modern systems engineering in product development is characterized by various engineering environments and collaboration settings. Hence, new challenges and higher demands on protection emerge (Grimm and Anderl, 2013). Typical data exchanges in collaborative product development between stakeholders include design and manufacturing knowledge of the product and its components, software knowledge,

such as algorithms and compilers. Every single member of a joint product development program contributes its own unrivalled knowledge which should not leave the company.

Enterprise rights management designates the encryption of documents based on a digital role and rights administration. Thus, complete databases are only exchanged in encrypted form. A rights assignment server regulates who may use the documents in what way and in what time frame (VDI 5610-2, 2017). There are numerous existing setups for pre-emptive data protection in collaborative systems engineering. Some are assessed in a study by Grimm and Anderl. They assessed systems engineering approaches under criteria of usability of protection means, effectiveness of knowledge protection and process efficiency in collaboration. They found that enterprise rights management (ERM) is the most sufficient method for a small scale product development case with three joining parties (Grimm and Anderl, 2013). ERM is based on data encryption and control mechanisms. ERM infrastructure consists of access rights server and clients. The server manages access policies and user identities and provides cryptographic keys to authorized clients, which request access to specific content. Then software decrypts the protected content in trusted end-user applications on the client and enforces the permission policy assigned to the particular user. Unauthorized users do not have access.

4. Financial assessment of knowledge

Companies create, identify and protect knowledge. Intangible assets comprise the bulk of a company's value, yet that value is not reflected in its financial statements (Mellen and Evans, 2010). For stock market value, business transactions and sharing knowledge externally in transfer of technology or sales, assessing value of knowledge is necessary. The evaluation of knowledge encompasses financial and strategic benefits. Financial benefits are current and future cash flows which can be allocated to the knowledge and potential avoided costs through ownership of the intellectual property (CEN TS 16555-4, 2014). Strategic benefits of knowledge assets are impacting future market development and building new incentives for collaboration. In this thesis, financial assessment of knowledge is discussed in detail.

Another aspect of financial assessment of intangibles is discussed in regard to transfer pricing. Especially multinational companies exploit cross-country tax differences via transferring incomes to low tax countries. Thus, transfer prices are often tax-motivated (Clausing, 2003). Many economies are worried for losing real economic activity (Bartelsman and Beetsma, 2003). OECD conducts rule transfer pricing. Knowledge assets must be priced in order to ensure correct taxation. If transfer prices are valued incorrectly, either the underlying income is multi-taxed or, in certain instances, it may be subject of tax fraud (OECD, 2017).

Financial assessment is quite difficult, since the market value of a particular technology is hard to ascertain. Financial assessment demands a high quality of forecasts for market development and technology. It is most important for estimating the value of transfer of technology, sale of intellectual property and licensing of particular patents. A valuation must describe the property rights presumed to be the focus of a transaction and the terms assumed.

There is no single method for determining a fair market value of intangible assets. However, there does exist a generally accepted theoretical foundation to the process of valuing these assets revolving around the three generally accepted valuation approaches throughout all appraisal disciplines: the income approach, the cost approach, and the market approach (Mellen and Evans, 2010). All three are discussed

separately in the following sections, however without contemplating mathematical methodology.

4.1 Market approach

The market approach is the most direct and the most easily understood valuation technique (Anson and others, 2005). It measures the present value of future benefits by obtaining a consensus of what others in the marketplace have judged it to be. The market approach uses prices and other relevant information generated by market transactions involving identical or comparable assets. The fundamental assumption within the market approach is that other buyers of comparable assets were willing, had knowledge of all relevant facts, and consummated a deal that was fair and, therefore, represented fair value at that time and for that asset (Mellen and Evans, 2010). It is based on the principle of substitution that instructs hat a prudent buyer would not pay more for property than it would cost to purchase a comparable substitute. There are two primary conditions for valid market approach valuation methods, an active, public market and an exchange of comparable properties (Poltorak and Lerner, 2011).

A major benefit of the market approach is its simple application when a truly comparable transaction is available. The exchange of intellectual property in the marketplace typically is completed as part of the exchange of an entire company or division. Transactions for the purchase of specific patents or portfolios focused on a specific commercial activity are rare (Parr, 2018). The uniqueness of intellectual properties makes finding similar market transactions another challenge (Poltorak and Lerner, 2011). Thus, valuation is difficult, since often exists little or no comparable transactional data. The market approach is not often used for the valuation of intangible assets and intellectual property, largely because of the absence of an active market for comparable properties. For assessing the value of intangible assets within a transfer of technology, the market approach is not sufficient. It is unlikely to find similar assets exchanged in similar industrial environments at a fair market value. Generally, the application of the market approach is rare for intangible assets (Mellen and Evans, 2010).

4.2 Cost approach

The cost approach determines the value of a property by considering the costs required to replace the subject property, that are unique assets and not available for purchase in a marketplace (Parr, 2018; Walker and Weber, 1984). Value is determined by summing all the costs to re-create an asset, install it, test it, and bring it to an operational state. It is very useful for valuing tangible assets, such as specialty equipment, but not very helpful for most types of intellectual property. The cost approach provides an indication of value by considering the costs to create and/or obtain the subject asset (Poltorak and Lerner, 2011). The cost approach does not directly consider the amount of economic benefits that can be achieved over a period. This approach is often employed together with the assumption that economic benefits are reasonable high and duration of return of investments reasonable long in order to justify the developmental expenditures. Using a cost approach to estimate an indication of market value, however, requires a consideration to what extent future economic benefits will support an investment at the indicated value (Williamson, 1981).

There are several methods to derive the needed information to determine replacement costs. A company can restate historical costs in current value from detailed records of the development of the considered asset (Anson and others, 2005). This works for intangible assets as well, especially newly invented assets (Reilly, 2012), as long as the information has been collected. The accounting behind might be complex, since a lot of information is needed, but the approach is also applicable on intangibles. For instance, assembled workforce can also be valued by considering all the costs associated with identifying, hiring, and training the existing workforce (Parr, 2018). Still, the cost approach is not as comprehensive as the other two approaches. Many of the important factors that drive value are not directly reflected in this approach and must be considered apart from it (Mellen and Evans, 2010). The cost approach for valuation does not incorporate information about the amount of future economic benefits associated with the property and how long these can be exploited. The worth of intellectual property depends on market development, which can be downward or in a good position to excel in a trending market with huge growth rates. The risk associated with receiving the expected economic benefits is not directly factored as well (Parr, 2018). Since the cost approach only considers historical development, it is limited on

valuation of assets that may be obtained by competitors anyway. The cost approach is most appropriate for the valuation of trade secrets, assembled workforces, corporate practices and procedures and distribution networks. Trade secrets as such can be freely obtained by anybody through own development or reverse engineering efforts. Valuation of trade secrets via cost approach is reasonable. The replacement cost effectively places an upper limit on the value of trade secrets. An investor would pay no more for an asset than the amount necessary to replace it (Mellen and Evans, 2010). The value of a patent for example, which is protected of external use by property rights, depends more on future benefits over the patent duration and thus not suit the cost approach.

4.3 Income approach

The income approach focuses on a consideration of the income from ownership and exploitation of the property. The underlying theory is that the value of property can be measured by the present value of the net economic benefit to be received over its life, for example patent duration. Generally, the present value of the income flows to be generated over the intangible asset's remaining economic life is determined (Mellen and Evans, 2010). The income approach looks at the future economic benefits a property will generate in the future and converts the amount of benefits into a present value after considering the risk of receiving the expected benefits (Anson and others, 2005).

The income approach is best suited to situations where the property owner neither uses the underlying technology nor seeks to deny its use to competitors. Hence, it has no direct value to the owner, other than the income it may produce. Income can come from selling the intangible asset, or royalties from licensing the patent. However, if the property owner competes in the same market and has reason to use it, valuation gets more complex (Poltorak and Lerner, 2011). In many cases, the income approach is the best approach for valuing intellectual property and intangible assets. The approach can be most useful if the subject intangible asset has the potential to become an income-producing property (Mellen and Evans, 2010). Unlike the cost and market approaches, the income approach determines value from inputs that directly consider the revenues

and profits derived from commercialization of a property. It directly reflects the potential for earnings growth and the risk associated with commercializing an intellectual property.

The calculation is straightforward, but the analysis for developing calculation inputs is rather complex. The three fundamental components of the income approach include a projection of economic income, an estimation of the time period to project economic income, and the selection of appropriate risk-adjusted discount and capitalization rates (Mellen and Evans, 2010). Identifying future cash flows and outcomes are difficult. Intangible assets and intellectual property often are considered the highest risk asset components (Parr, 2018), thus having rather low rate of returns. Risk assessment is equally difficult as projecting future cash flows. Often the companies' risk of business fluctuates and changes significantly over time (Cohen, 2005).

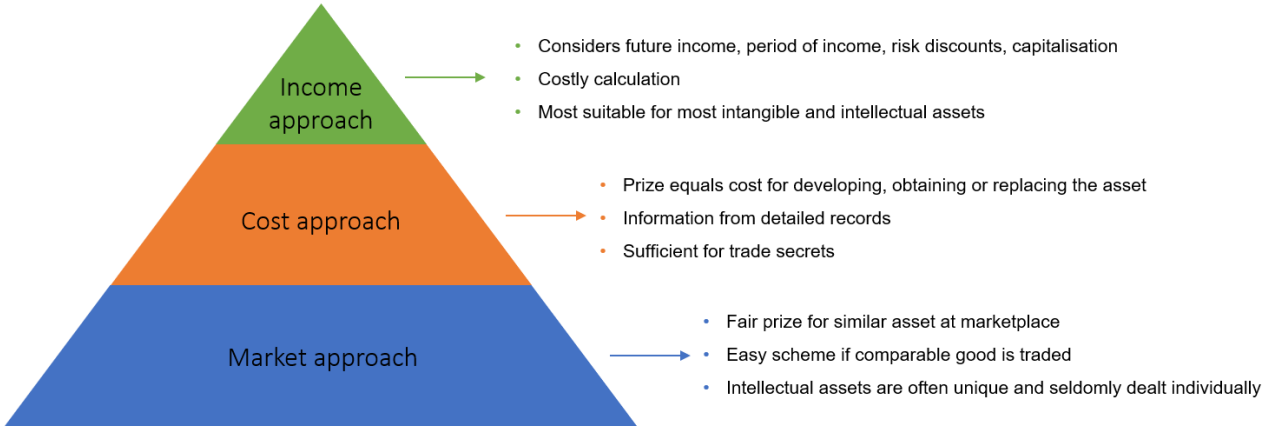

Figure 7: Approaches for financial assessment

5. Current know-how protection conduct at rolling stock manufacturer

In this section the conduct for knowledge protection which is currently in place at the investigated rolling stock manufacturer is discussed. Knowledge protection schemes for business cooperation are particularly discussed. The discussion refers to the state-of-the-art, which was described in section 3. Major sources are effective guidelines for know-how protection, process guidelines, interviews with experts of the intellectual property management and collecting personal experiences of protagonists within the business cooperation interfaces. Information from written guidelines and regulations is valued most, because of the official character of such, and possibly supported by expert experiences. Extracted information from such sources is kept anonymous. Interviews are only possible on a small-scale set. Assessing individual perspectives on the problem are more valuable than own investigations only. Large-scale interviews, in order to establish a proper quantitative approach, are not possible, due to lack of interviewees. Nevertheless, it is expected to generate important additional insights.

All findings are evaluated and draw a complete picture of the current know-how protection models within the company. The risk exposure is derived from all shortcomings relatively to the state-of-the-art protection methods and literature review of possible risks regarding intellectual property mismanagement.

5.1 Legal protection

It is not possible to publish statistics about patent properties and recent applications due to confidentiality issues.

At the investigated firm there has been a patent commission established, which assesses the economic value of new inventions. The commission decides whether an invention gets to apply for a patent or is just held under reasonable secrecy, thus protected with trade secret law. In rare instances an innovation which does not meet patent requirements and may not be protectable under trade secret law is published in order to prevent competitors from patenting similar inventions. For patent infringement

there is no systematic observation of competitors existing. It is rather relied on fortunate detections and observations. However, the competitor's offers for specific projects in which the manufacturer is involved as well, are more closely reviewed in order to detect patent infringement. Patents are further utilised for marketing purposes, which is the main reason none of the obtained patents had been licensed to competitors. Trade secret protection is relatively new in place, thus experiences are rare. The main problem for application of trade secret law is the challenging argumentation for infringement thereof. Possession of worthless patents is avoided in order to reduce inherent fees.

In many collaborations with partners and suppliers, a kind of transfer of technology is essential to grant access to all required information in order to receive a binding offer. Limiting access to specific information, e.g. specifications or interfaces of components, hinders the supplier to adequately design the requested component. Thus, transferring substantial information is inevitable. In order to grant reasonable protection, these business partnerships are always led by non-disclosure agreements between the negotiating parties. However, there had been some negotiations started before a non-disclosure agreement was signed due to being under significant time pressure. The then exchanged information was not protected and put featured knowledge under immense risk. In recent years the responsible stakeholders have been boosting the awareness to assure that non-disclosure agreements are in place upon start of negotiations. The investigated rolling stock manufacturer's NDAs are standardised. In many instances the standard is slightly adapted in mutual understanding with the supplier, though major changes are unusual. Typically changes are made to penalties, scope of confidentiality or under which jurisdiction the agreement is effective. In addition to having NDAs for specific projects and specific products, a more general approach was introduced recently. A frame contract for NDAs was developed, which rules any exchange of information the parties may have regardless of project or products specifics for a period of five years. Thus project teams with substantial time pressure can immediately start conversations about sourcing activities without any delay, even before any specific non-disclosure agreement is signed. However, it is mandatory for engineers and responsible procurement managers to clarify whether agreements are in place before contacting another party, even though these frame contracts are increasingly established. Fortunately, in most business connections

confidentiality agreements are mutually required. Knowledge-rich suppliers do not risk transfer of technology without reasonable protection on their own. However, these would typically not be the ones that gain much from obtaining external know-how.

5.2 Strategical protection

Proven and stable know-how is transferred only. Know-how is proven if it is tested, reliable and not considered a recent innovation. Stable know-how refers to knowledge being definite and not only partially available or still evolving at the time it is considered for transfer. If these conditions are met, the rolling stock manufacturer's know-how could be transferred via transfer of technology. From a strategic standpoint it is not sufficient to transfer knowledge without significant returns. While it is not definitely specified where a minimum return would lie, it is understood that it is a separated decision in any individual case. Expected returns are compared to not only the transfer price of the knowledge but the possible future damages the transferred know-how can do in the hands of the respective recipient. Latter is not easy to assess. In many cases the transfer of technology is priced extra, on top of all transactions. Know-how must not be transferred without valid transaction contracts between recipient and donor. These contracts, commonly known as transfer of technology agreements, specify which knowledge is transferred, roughly when and how. The transferred technology is often essential for the recipient to fulfil their scope of the business. Hence, the payment for transfer of technology is mostly part of the partnering contract.

Technical classification of know-how is done by so-called know-how owners, who aggregate all the know-how from the functional direction they are responsible for. The know-how is then evaluated on a two-dimensional scale. Firstly, it is assessed whether the specific know-how is relevant to competitors and secondly, whether it is difficult to imitate without having access to the specific know-how. Both scales are set from one to five. Figure 8 depicts the two-dimensional scheme. On this scale, one refers to low relevance to competition and low difficulty of imitation, five refers to decisive technical difference to competition and high difficulty to imitate the particular component. Hence, category III marks relatively dispensable know-how, while category I marks the most important know-how.

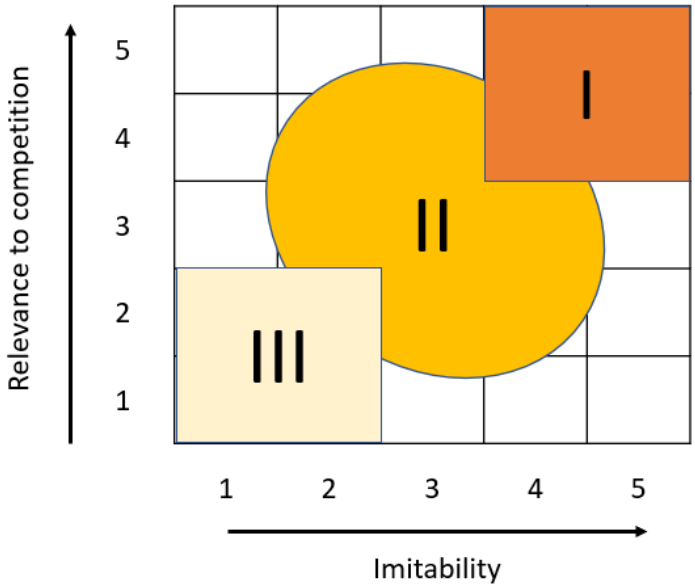

Figure 8: Technical classification

A lot of the area is not even covered, because such a combination is not expected to exist at all. Every know-how owner updates the evaluation at least once a year. Based on this evaluation it is decided whether knowledge is transferred or not, which depends on the recipient of the know-how. The recipient is also evaluated, which can range from external competitor to subsidiary enterprise of the donor. While subsidiary enterprises are not likely to have limited access to know-how of the donor, external competitors are not eligible to receive any know-how other than category III, the least valuable know-how. Accordingly, every recipient has access to certain categories of know-how, which is based on their evaluation. In rare instances the scope of tolerable know-how transfer can be extended by senior management decision. The decision must be clear and approved before the transaction is executed. The know-how that is eventually transferred can then be financially assessed, the other know-how stays under protection.

Fundamental awareness about knowledge protection in senior and strategic management is found during the investigation. However, there are know-how protection processes which are not continuous, which is further discussed in section 5.3. For strategical decisions regarding footprint, partnering and market acquisition, know-how protection is always considered. First of all, the assessment of respective

know-how is conducted. Then the recipient is also assessed in order to make the right strategic decision. The assessment of the recipient can be based on the considered region or country and its conditions or on a specific partner. The risk evaluation is based on those assessments. Cost for transfer of technology and its risks in business cooperation must be surpassed by potential market share acquisition through low cost production or establishing local content. For strategic decisions regarding mergers and acquisitions or sales of portfolio units, the procedure is quite similar. For acquisitions it is looked at the know-how which can be gained from merging with other firms. Sales of portfolio units does usually not require transfer of technology, but the portfolio probably consists of know-how which must be evaluated in order to determine a proper sales price. A financial assessment of the underlying intangible assets follows calculation approaches discussed in section 4. The most suitable approach for intangible asset is applied, even though each has its own inconsistencies. The rolling stock manufacturer had positive experiences in transfer of technology, which got increasingly important within the early 21st century. Establishing know-how in diverse markets around the world lead to development and growth of the respective markets and substantial returns. However, there have been a couple of regrettable partnering decisions in the recent past as well, which led to financial losses but not any severe knowledge leakage.

5.3 Organisational protection

There are five major mechanisms to organisational know-how protection available.

Firstly, knowledge management conduct at the investigated firm focuses on enhancing communication and making knowledge available for internal use only. Granting access to knowledge is especially supported through various channels, which are not further discussed. Knowledge protection for the purpose of preservation and for transfer of technology is regulated separately. Knowledge protection to prevent leakage in transfer of technology is ruled in an operational process, which specifically orchestrates the necessary steps to identify, classify and release all knowledge assets that are subject to transfer. The basic procedure for classification is contemplated in section 5.2. The operational process defines roles that need to be established, and tasks that

need to be executed in order to protect knowledge and release transfer of knowledge. Diligently following the process demands high efforts. The responsible know-how manager for the transfer of technology collects updated classifications according to scope of the transfer. Then the recipient is assessed as well and subsequently a restriction is applied to every single asset. Key knowledge is mostly forbidden to be transferred to competitors, while transfer to non-competition is restricted less. However, the regulation often restricts knowledge that is essential to the recipient in order to ensure an efficient production or knowledge that was even agreed upon to be transferred before an evaluation was carried out. Then every single restriction in question must be separately released by know-how protection management, which is typically assigned to senior management. This can be highly time consuming.

Secondly, the investigated rolling stock manufacturer is aware, that knowledge split in ownership of many different participants enhances protection. Compartmentalisation is applied in various instances. The firm is split into divisions for the purpose of concentrating specific knowledge about products, such as expertise in sales and project execution, and operations, mainly logistics, engineering and manufacturing. On one hand the concentrated expertise and explicated knowledge of each department are beneficiary to solving the related tasks and on the other hand lead to major dependencies between the departments and eventually divisions. While this is often criticised for its slow workflow mechanics, it enhances knowledge protection. Any participant owns specific knowledge about certain processes related to the owner's specific tasks, but commonly does not gain close insight in core know-how of other groups. However, there is no strict separation between departments and therefore compartmentalisation as such is not fully utilised, a common trade-off between spreading knowledge and know-how protection.

Thirdly, in many instances the last mentioned method is utilised in addition to keeping knowledge tacit. For manufacturing know-how in particular, where the knowledge-rich manufacturing processes are both explicated and kept tacit. Manufacturing knowledge exists in descriptions, procedures, pictures and in workers in tacit form. The overlap of knowledge of the different explicated sources is minimised in order to suffer the least possible damages to knowledge protection from such documents falling into competitors' hands. The knowledge is only complete and valuable when all components are joint together. Similar mechanics are facilitated in departments, which

can be generally united to engineering-related workgroups. Even though tacit knowledge is different to the tacit knowledge in manufacturing, a substantial amount lies in the engineer's expertise. Information resulting from engineering efforts, such as drawings or specifications can possibly be imitated and utilised as slavish copies, which defines copies that are outright duplicated (Neemann, 2007). Though the underlying engineering knowledge is not included and thus the value of the imitation drops. This does grant considerable protection, since rolling stock projects often demand unique adaptions to the product.

Fourthly, tacit know-how is protected extra. Every employee must sign a standardised confidentiality agreement in order to state their compliance upon employment, which covers explicit know-how as well. Signing these confidentiality agreements is mandatory. Even though there are significant differences in the value of know-how held by employees from various departments or positions, there is none in scope of the confidentiality agreement. Furthermore, whenever an employee resigns, an immediate release of the employee is considered, which depends on the judgement of the employer. Releasing an employee immediately impedes abstraction of explicit knowledge. The employee still carries tacit know-how, which can be valuable for competitors. Yet, non-competition clauses are not established, mainly because these are not expected to be compliant with local employment law. This reasoning depends on the local conditions and might be ruled differently in other legislations. The principle for know-how protection in human resourcing at the investigated rolling stock manufacturer can be summarised as containing leakage instead of preventing it at any cost. The incentive schemes for current and future employees align to that principle. Employees can take part in share matching programs to become shareholders of their employer. This mainly increases ownership mentality within the firm's staff, but since the programs run for several years, it is expected to bind personnel to the company for the timespan as well. Another incentive is a monthly payment to a private retirement fund, which is extra to the salary and can be received upon retirement if the employment exceeded three years. The deposit is a percentage share of the salary and can be raised individually. In addition to those unique incentives, the collective agreement schedules raises after certain periods of affiliation. Even though this applies for the entire industry sector nationwide, it is expected to be an advantage compared to competitors from outside the area of the collective agreement's validity. In terms of

recruiting, a further incentive might be the product itself. Taking part in a business which models around sustainable mobility can lead to either bind employees to the company or attract new employees. A corporate policy featuring sustainability as a major objective is considered to be appealing for job applicants (Klein, 2015).

Fifthly, confidentiality is always a major concern for the organisation. Confidentiality of documents is classified in four steps, ranging from unrestricted to highly confidential. Classified information may not be sent internally without encryption and externally at all. Most documents carrying explicit business information are classified accordingly. These restrictions are supported by the IT infrastructure. While it is certainly important to limit knowledge leakage and leakage of classified information in daily business, this is rarely applicable to intentional transfer of knowledge. Moreover, this is mainly subject to IT and cyber-security, thus explicitly beyond the scope of this thesis.

5.4 Technical protection

Technical know-how protection is distinguished in protection of physical objects and data, both are further discussed separately.

Protection of physical objects, such as the rolling stock product itself, is difficult. Only customers get to handle the complete product, which usually does not result in any severe consequences in terms of knowledge leakage. Business cooperation in manufacturing carries way more risks. Even when manufacturing partners do not have the know-how to qualify as a future competitor, they can obtain the necessary knowledge through the cooperation. Obfuscation of components is rarely applicable. Customers demand low maintenance efforts, which contrasts physical concealment of components. Exchanging components gets harder and accession is further limited. Cost for concealment are often just too high and the increase in weight negatively impacts energy consumption and sustainment of tracks. However, obfuscation of already assembled components that just get installed at the manufacturing partner's site is used. This is often applied to electrical components or air-conditions. Specialised manufacturing is important to knowledge protection in business cooperation for the investigated rolling stock firm. Even though some eligible technologies are not currently featured. Some manufacturing processes are complex in nature. The complexity of

numerous welding technologies, such as spot welding or friction stir welding, occasionally prevents the technology from being successfully transferred even when it is actively aimed for. Even though the main competitors and global players of the rolling stock market do possess the needed know-how, companies outside the industry sector usually do not. Additive manufacturing is considered to offer similar protection. Additive manufacturing is expected to be applied in the future, as soon as development reaches stage of maturity and costs are significantly reduced.

For protection of data, the current procedure follows section 5.2. Where documents are assessed and classified according to Figure 8. Documents can then be checked for eligibility for transfer. This procedure is further supported by manual data filtering. Whenever a document is not eligible for transfer, but carries essential information to the recipient, it can be filtered manually. This way, excess information is excluded from the transfer. Joint development of products is not common, thus exchanging knowledge-rich data to engineering consultants or competitors does not occur.

6. Current risk exposure and deficits

In this section the deficits and relevant risks are briefly discussed. The term risk is used in this thesis to refer to the potential damage, loss, or negative effect of knowledge sharing and leakage. The section is divided in four paragraphs, referring to four categories of knowledge protection, as described in section 3.

Firstly, protection under intellectual property rights works as it is supposed. For comprehensive protection a closer investigation of competitors is advisable. Relying on sales to detect patent infringement within a specific project tender, demands training of sales personnel in terms of patent awareness. Otherwise an infringement cannot be excluded and is possibly not detected at all. In addition, the investigated company does not license patents to competitors, even though this would match perfectly well with low prosecution efforts. If a rolling stock manufacturer is not able to detect infringement, licensing patents and earning from royalties is the superior alternative. Patents have rather high lifetime costs and not exploiting the property increases the risk of financial damages. For non-disclosure agreements it is important to leave out knowledge transfer without valid NDAs in place. Otherwise there is no legal foundation for prosecution. However, checking whether NDAs are established needs improvement as well. Currently there is no direct access to existing NDAs. Engineers or procurement managers often need to contact legal department in order to learn about the contract status. This could be optimised to reduce efforts and the risk of just passing on the necessity.

Secondly, a major risk in current know-how protection conduct lies in the continuation of the transfer of technology process. This applies to both, strategical and organisational knowledge protection. The process is currently not conducted continuously. Due to recent changes within the company’s organisational setup the know-how representative on senior management level is not assigned. Hence, deviations from the regulation in terms of whether knowledge can be transferred despite of opposite ruling by the regulation, cannot be diligently resolved. Thus, the current know-how conduct suffers from severe uncertainty, coming from lack of senior management awareness. This vacuum is advised to be filled as soon as possible.

Thirdly, the previously discussed process also lacks on operational level. Marking whether documents are allowed for transfer manually is not sufficient. Due to its time-consuming nature and error-proneness, it should be automated. Possibly through automatically releasing the results, based on the existing knowledge classification and assessment of the transfer recipient. This requires access to up-to-date know-how classification, which requires more than the scheduled once a year update of know-how classification.

Fourthly, technical protection of knowledge is further developed in section **Error! Reference source not found.**. Based on the following deficits, some concepts for rolling stock business are derived. Leaking knowledge through physical objects is an existing risk, even though top-tier competitors might get access to rolling stock products through winning maintenance tenders only. Besides top-tier competitors, it's the manufacturing partners that spark the risks, because they get access to physical objects regularly. In combination with documents a significant portion of know-how can be obtained. Obtaining engineering knowledge and manufacturing knowledge simultaneously could result in serious long-term damages to the business by building up a potential competitor. The mentioned methods to enhance protection of physical and knowledge-rich components should be more closely looked at. The same applies to protection of data. It does not matter how well the classification for documents is conducted, when they are transferred regardless or must be manipulated manually to do so. Transferring knowledge-rich documents to recipients that, according to the previously discussed regulation, are not eligible to receive this knowledge, can cause severe consequences. Often this comes from previously agreed transfer of technology agreements, that include know-how, which was not assessed and eventually not released. To fulfil those contracts, an individual release is mandatory. Even though these documents are released by senior management decision, the risks of transferring too much of valuable know-how stay the same. Also, customers and homologation authorities usually get full sets of documents without further consideration of knowledge protection risks. It cannot be ruled out that released know-how does not eventually get into the wrong hands. Possible concepts to take care of these deficits are derived in the following chapter.

7. Know-how protection concepts for rolling stock

In section 6 numerous deficits are discussed and potential additional remedies mentioned. For the derivation of detailed concepts suitable for rolling stock industry, this thesis is confined to technical protection methods. Firstly, because here lies a significant potential in terms of further protection in order to limit risk exposure and secondly, because it is the sector with the most direct access for the author of this thesis.

This chapter is divided into a short description of potential technical protection methods to support current conduct is given, followed by a discussion about the consulted criteria for evaluation of the introduced concepts. Lastly, the introduced concepts are evaluated, and the evaluation results are published and shortly discussed.

Know-How protection methods	**Objects to be protected**
Black boxing	Physical object
Decomposition of components	Physical object
Specialised manufacturing process	Physical object
Holistic pseudonymisation	Data
Subject pseudonymisation	Data
Automated data filtering	Data
Special agreement with customer	Data
Special agreement with authority	Data

Table 2: Know-how protection concepts overview

7.1.1 Black boxing

Black boxing essentially is an obfuscation method. Even though the majority of components have to be easily accessible and exchangeable for maintenance purposes, concealment of such carries knowledge protection potential. The harder it is to an imitator to get access to a specific functional component, the better its knowledge is protected. Anything that increases the resistance to obtaining knowledge is beneficiary to protection. It is not applicable on all knowledge-rich components, nevertheless there are numerous opportunities to utilise black boxes. Furthermore, black boxing can also be faked in order to mimic protected content, which in fact does not carry any function. In practice, electronic devices have the highest inclination to black boxing, besides digital elements. Software often consists of program elements that are easily black boxed and hard to analyse. Mechanical black boxing is rather rare. If a manufacturing partner is assigned to assemble components, these components could be protected from reverse engineering by being black boxed. Any already finished component is to some extent black boxed, but necessary efforts in reverse engineering to obtain the knowledge can be further increased by obfuscation measures. Components being considered for black boxing are wall profiles to protect carbody production know-how and components that are entirely installed within assembly work. Possible mechanical black boxes could consist of functional elements that are casted into resin, which cannot be deconstructed without physically harming the component. Hence, black boxing synergises well with decomposition methods.

Black boxing demands several adaptions in engineering. First, current products need to be adapted to exploit obfuscation immediately and development of novel products need to consider black boxing. Obfuscation of components eventually leads to higher engineering costs, since knowledge-rich components need additional dedication.

The advantages are apparent. Any manufacturing partner that carries out assembly and receives install-ready components could only investigate the finished components in order to learn about the function. If these functions are protected by reasonable obfuscation, the partner firm is not able to obtain the withheld knowledge. Same applies to customers that carry out maintenance work and might only be able to exchange complete components.

The disadvantages lie in applicability. The scope split between manufacturing partners varies, which counters black boxing, since components may be partly assembled elsewhere. This varies from project to project and not only counters the obfuscation itself, it also negates the efforts made in engineering in order to obfuscate components in the first place. Another drawback lies in maintenance. It is not cost-efficient to change entire components instead of a limited number of fatigued elements, thus knowledge protection eventually impairs bid success.

7.1.2 Decomposition of components

Decomposition barriers are protection mechanisms that permanently destroy the product or a single component when deconstructed. It can only be applied in components, that must not be deconstructed by customers but by a potential imitator in order to reverse engineer the product. It can be used to mainly protect the function of electrical components from being discovered. For example, circuit boards could suffer from extra fast corrosion damages due to extraordinary sensible material. Thus, the original function is eliminated. Decomposition must not run contrary to safety, which limits its applicability. Similar to obfuscation, it does need additional engineering efforts to install these self-destructive elements, which can add extra costs for special material as well.

The main advantage is, that it is not possible to conclude the engineering know-how from the physical object. Through eliminating the original function, the know-how is protected and a possible imitator would need to have access to the original engineering documents of the component. Hence, the level of protection is increased.

Low level of applicability is the main drawback of decomposition methods. Firstly, safety must not be interfered with and often decomposition contrasts maintenance as well. Even though it synergises well with obfuscation of components it suffers from similar drawbacks.

7.1.3 Specialised manufacturing processes

Specialised manufacturing processes are a know-how asset itself. For rolling stock business there are lots of manufacturing processes that are very sensitive and difficult to handle. This alone can be used to protect the product from imitations. Manufacturing processes such as spot welding or friction stir welding cannot be easily reproduced. It is not likely that potential competitors can implement these processes into their procedures. However, this does not work for the top-tier competitors, which possess the needed know-how too. Introducing specialised manufacturing processes for rolling stock comes at high costs, either from engineering or manufacturing. Hypothetically the amount of specialised manufacturing processes is almost infinite. Additive manufacturing is currently on the rise and many others are passed on, mainly because they are too expensive.

There are advantages that can be exploited through applying specialised methods. Often these processes bring their own technical advantages, such as higher stability or being more flexible. However, these often carry higher costs as well. The affected work steps can then not be easily transferred to manufacturing partners. The know-how is well protected, but it might not be possible to exploit low wage production at localised manufacturing sites. Hence, the decision for specialised manufacturing is a balancing act between an easy and low-cost production that can be shifted to different sites or a specialised and more expensive process which cannot be localised.

7.1.4 Holistic and subject pseudonymisation

Pseudonymisation is a quite efficient protection method for documents. It is easily applicable and offers considerably protection. It is available in various models. Typically, documents that are transferred to external recipients do not carry real names and information. Instead the name and information of a document are encoded. The coding can only be resolved with a specific digital key. If the key is safe and protected, the whole document cannot be misused. Thus, a leaked document without the fitting key is worthless. Another advantage is, that either the key or the document itself can be personalised, thus intentional leakage could be more easily traced. This concept is

called holistic pseudonymisation. The implementation is rather expensive, due to the automated and individual encoding and separation of keys, including reasonable protection. Hence, a slimmer approach must be considered for this thesis as well.

Documents that do not carry the companies' name, identification and subject cannot be collated without substantial investigation efforts. It does not require a digital key, even though recipients must be enabled to collate the documents to its subject. Often it is enough to change the subject's name to a nickname, that is used internally, but is unknown outside of the rolling stock firm. This is further referred to as subject pseudonymisation. Both methods could be applied to engineering drawings. However, the information is only protected against unintentional leakage, the protection mechanism does not work as well for intentional leakage. For transfer of documents within a transfer of technology, both methods can be used to safely transfer the information, but it will not impede the recipient from obtaining the included knowledge. The same is true for document transfer to customers or homologation authorities. While this must be separately agreed on with the involved parties, it offers another application for both pseudonymisation methods, which is synergetic with other methods.

7.1.5 Automated data filtering

Data filtering is a procedure that is occasionally in use for CAD data. This can be elevated to an automated process in which a converter creates documents to three levels of content. The first level contains the unlimited dataset of the 3D model, with all relevant data for manufacturing. The first level is for suppliers and partners. The second level is a plain 3D model, containing material data and main geometry only, which is adequate for assembly or to convey respective interfaces of the component. The third level of information is limited to a plain 2D view model, excluding main dimensions. This model carries the least information and is uncritical in terms of know-how protection. For customers and homologation authorities this information level is usually sufficient.

The automated data filtering must be supported by engineers, who define the depth of information in each document and cluster it in order to define the three mentioned levels of information. This consumes minimal additional time and is thus rather

inexpensive. Data filtering is applicable for specifications or descriptions as well. Eventually every document can be divided into three levels of content worthy of protection. The author conducts the classification as soon as the document is finished. Thus, additional efforts are minimised. Adapting documents retrospectively is not recommended, because of the extensive time consumption.

The converter is connected to the enterprise resource planning software. The converter filters the data and automatically generates the document with the needed information level, which is then ready for transfer. The IT solution to establish a converter is not straightforward and is expected to trigger rather high costs.

7.1.6 Special agreements on documentation

Specialised agreements which limit the external transfer of documents to customers and homologation authorities protect knowledge-rich documents. For receiving a license from homologation authorities, a rolling stock firm must deliver an almost complete documentation. Customers usually get an even more complete documentation about the delivered vehicle. These contain a lot of protect-worthy know-how. Reducing the critical content through special agreements with customers and authorities would have a positive impact on know-how protection in general. It is not entirely sure how far this protection method may go in practice but considering the low invested effort to negotiate the respective terms, it should not be overlooked. This protection method is limited in applicability. It prevents suffering from leakage of knowledge-rich documents but cannot be applied as protection in collaborations with transfer of technology. It is important to note, that the use of this method depends on contract negotiation and must therefore be agreed on by the respective customer or authority.

7.2 Evaluation of concept portfolio

In this section the evaluation of know-how protection concepts is contemplated. The work is carried out in a two-step procedure, in which the criteria is first discussed and weighted and then the evaluation results are depicted. Both evaluations are suited to the investigated rolling stock firm, while the procedure stays the same the underlying weight of criteria and assessment of the portfolio can be freely adapted. The established criteria in Figure 9: Criteria weightFigure 9 are defined in the following.

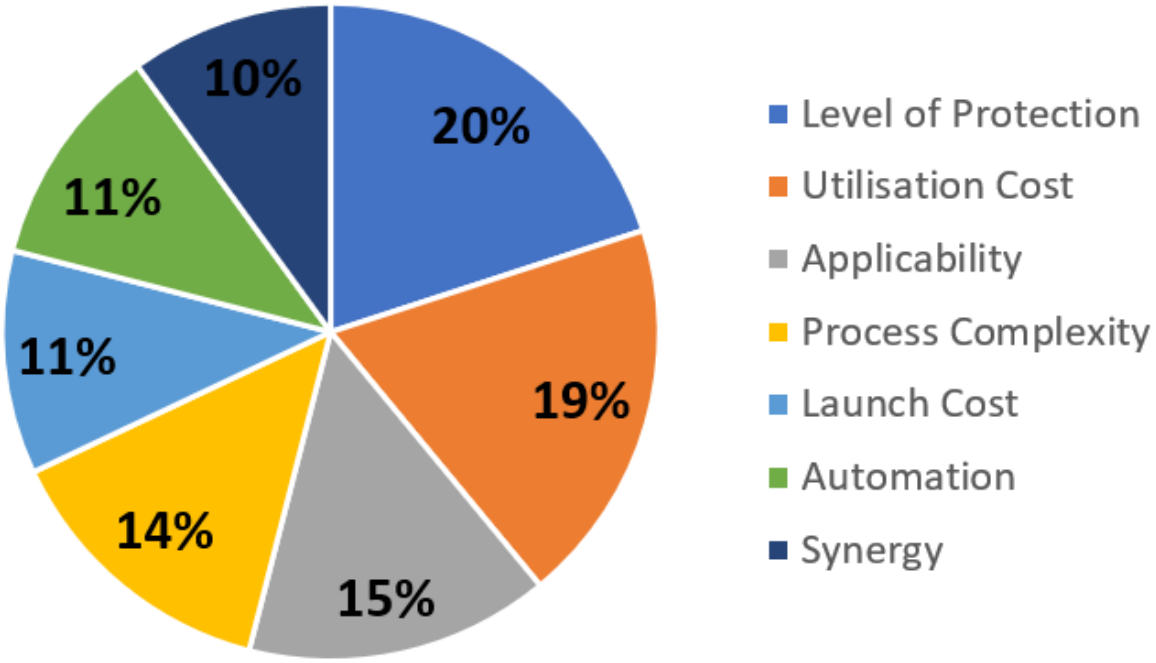

Figure 9: Criteria weight

Launch Cost

The efforts to establish a certain concept are evaluated in a qualitative approach. This criterion includes all one-time costs and investments necessary to introduce a certain method.

Utilisation Cost

The necessary effort to make use of the protection method in specific projects. Utilisation of a certain concept should be rather inexpensive as it occurs regularly. This includes potential operating costs and efforts that are specifically carried out with almost no worth to posterior projects.

Applicability

It evaluates whether a method has a wide range of utilisation or is very specific and for certain occasions only. The more a know-how protection method possibly protects, the higher the applicability. Offering a broad range of utilisation is favourable.

Synergy

It is looked at the synergy a method has with already established protection methods or proposed concepts. Additionally, this criterion encompasses assessment of whether a method has complementary coverage to already established methods. Utilising know-how protection methods that offer complement protection is favoured.

Process Complexity

The difficulty of applying the protection concept is evaluated. Utilisation cost already contains assessment of the necessary efforts. However, this criterion answers whether a proposed protection scheme needs extra trained personnel. A high process complexity increases the risk of the process not being carried out at all. It seldomly happens that rather complex processes get circumvented. It also increases the risk of possible errors, which could affect the level of protection.

Level of Protection

Level of protection assesses the benefit in terms of overall know-how protection a concept is expected to generate. This also includes a relative assessment to the currently established method. The gain in protection from the proposed method and the total level of offered protection are both considered. A rather high process complexity might cause errors along the process, which impacts the level of protection. This is covered by process complexity and does not influence the evaluation of the level of protection.

Automation

The proposed concepts might be suitable for automation. Even though this is not subject to the proposal itself, the process could be automated upon broad utilisation in order to lower the time expenditure.

The criteria are weighted according to the following paired comparison in Table 3. The comparison between the significance of two criteria is evaluated in 1, 2 or 3. In which 2 stands for equally important criteria, 1 is for the one with lower and 3 for the criterion with higher significance. The individual results are summed to weighted factors. The comparison is carried out with support of a group of experts from the collaborating rolling stock firm. Hence, the results are specifically customised to rolling stock business and the discussed topic. It is recommended to consult a reasonable number of experts on the topic of know-how protection in order to get valid results.

	Launch Cost	Utilisation Cost	Applicability	Synergy	Process Complexity	Level of Protection	Automation		Sum	Rank	Weighted Factor
Launch Cost		1	1	2	1	1	3		9	5	0.11
Utilisation Cost	3		2	3	3	2	3		16	2	0.19
Applicability	3	2		3	2	1	2		13	3	0.15
Synergy	2	1	1		1	1	2		8	7	0.10
Process Complexity	3	1	2	3		1	2		12	4	0.14
Level of Protection	3	2	3	3	3		3		17	1	0.20
Automation	1	1	2	2	2	1			9	5	0.11
								Σ	84		

Table 3: Weighting criteria

Level of protection is the most important criterion, followed by utilisation cost and applicability. An increase of the level of protection is basically the pursued goal of any know-how protection method, that is or will be established. Commercial assessment of those methods is crucial for a potential implementation as well. Whereas launch costs are less significant due to its one-time nature, utilisation costs are weighed higher. Utilisation costs accumulate when the method is used and thus have a higher influence on the overall costs, if the method is used for a rather long period.

The proposed know-how protection concepts have been evaluated. The results are depicted in Table 4. The concepts are graded in every aspect from one to five points. Five points is the maximum achievable grade. All grades are weighted according to Table 3 and summed to an overall score. The evaluation was carried out under counsel of experts on knowledge protection, which is recommended since a group of various individuals is a better reflect of the firm.

Automated data filtering is the concept with the highest overall score. It achieves ideal scores in level of protection, utilisation cost and applicability, which are the most important criteria according to the paired comparison and more than any other assessed concept. Automated data filtering is a potential add-on to the current conduct, with which it synergises well. The almost entirely automated process carries rather low complexity and overall costs. However, capital expenditures for automated data filtering, which includes a converter is considerably higher than for most other data protection concepts. Automated data filtering is closely followed by the pseudonymisation concepts. Even though both are quite different, their overall score differs marginally. Holistic pseudonymisation offers higher level of protection, whereas subject pseudonymisation is one step ahead in costs. Comparing those two concepts comes down to weighing level of protection against costs. For pursuing an implementation of one of those pseudonymisation concepts, both aspects have to be defined in more detail in order to make a judgement for either one.

Special agreements with customers and authorities both score rather low, compared to the mentioned frontrunners. Both processes cannot be automated, it is always a separate negotiation and agreement necessary, probably for every single project. Hence, both score minimal points on this matter. They score mediocre at costs, applicability and synergies, mostly because they are very situational. Whereas process complexity and level of protection are rather high. Agreements with authorities and customers to withdraw critical knowledge from the documentation has know-how protection potential, even though it is not expected to have the impact of the methods mentioned above. They are undermatched by the protection concepts for physical objects only. They comprehensively score low at overall costs, automation and complexity. However, since they cover an entirely different aspect of knowledge, they should still be considered for potential implementation. Special manufacturing processes scored highest under these concepts. If it is expected to generate

advantages in other areas, such as product innovation or long-time cost reduction, the implementation of novel manufacturing processes is a reasonable method to maintain knowledge lead. Hence, it scores particularly well at synergy and level of protection. But, decomposition of components is the only concept that score less on costs. Automation, process complexity and applicability carry rather low results for all three protection methods for physical objects. Black boxing particularly scores worst in utilisation cost and synergy. Concepts for protecting physical objects suffer from demanding extensive engineering efforts.

The results suggest that protection of data is the subject of choice. These methods are easier, cheaper and offer better level of protection than the protection concepts for physical objects. Furthermore, the results suggest that automated data filtering is the best proposed concept for rolling stock industry.

Criteria	Weighted Factor	Black boxing		Decomposition of components		Specialised manufacturing processes		Holistic pseudonymisation		Subject pseudonymisation		Automated data filtering		Special agreement with customer		Special agreement with authorities	
		Evaluation	Weight	Evaluation	Weight	Evaluation	Weight	Evaluation	Weight	Evaluation	Weight	Evaluation	Weight	Evaluation	Weight	Evaluation	Weight
Launch Cost	0.11	**5**	0.55	**3**	0.33	**2**	0.22	**4**	0.44	**5**	0.55	**2**	0.22	**4**	0.44	**3**	0.33
Utilisation Cost	0.19	**1**	0.19	**1**	0.19	**3**	0.57	**5**	0.95	**5**	0.95	**5**	0.95	**3**	0.57	**3**	0.57
Applicability	0.15	**2**	0.30	**2**	0.30	**2**	0.30	**3**	0.45	**3**	0.45	**5**	0.75	**3**	0.45	**3**	0.45
Synergy	0.1	**2**	0.20	**3**	0.30	**4**	0.40	**3**	0.30	**3**	0.30	**4**	0.40	**3**	0.30	**3**	0.30
Process Complexity	0.14	**2**	0.28	**1**	0.14	**2**	0.28	**4**	0.56	**4**	0.56	**4**	0.56	**4**	0.56	**4**	0.56
Level of Protection	0.2	**4**	0.80	**4**	0.80	**4**	0.80	**5**	1.00	**4**	0.80	**5**	1.00	**4**	0.80	**4**	0.80
Automation	0.11	**1**	0.11	**1**	0.11	**2**	0.22	**4**	0.44	**4**	0.44	**4**	0.44	**1**	0.11	**1**	0.11
		Sum	**2.43**	**Sum**	**2.17**	**Sum**	**2.79**	**Sum**	**4.14**	**Sum**	**4.05**	**Sum**	**4.32**	**Sum**	**3.23**	**Sum**	**3.12**

Table 4: Evaluation results

8. Conclusions and outlook

In this thesis the know-how protection conduct of a rolling stock manufacturer is investigated. The current risk exposure is presented and shortcomings discussed. Based on a discussion of state-of-the-art know-how protection mechanisms, a proposal for implementation of novel concepts at the rolling stock firm has been presented. The state-of-the-art is identified by a qualitative approach. The proposed concepts for technical know-how protection have been evaluated according to customised criteria. The evaluation is carried out within a quantitative approach.

Important findings are that the rolling stock manufacturer shows several shortcomings in its current know-how protection conduct, especially in business cooperation. The four main issues are listed in the following: Firstly, a discontinuous know-how protection process for transfer of technology. Secondly, prematurely signing agreements with business partners about the scope of transfer of technology, even though the demanded technology is partly kept under strict protection. Thirdly, ignoring lack of non-disclosure agreements, because of time pressure. Fourthly, manually filtering information from documents for transfer, that have been individually, but conditionally released.

The evaluation results suggest that protection of data is favourable to address compared to protection of knowledge in physical objects. The results further suggest that automated data filtering is the most promising concept for the rolling stock manufacturer.

This thesis offers a foundation on which implementation of the proposed concepts can be further pursued on. Utilising the detected shortcomings to evolve the know-how protection conduct and add suggested technical know-how protection concepts to the portfolio is a justifiable expectation for future work on this subject. In addition to the discontinuous process for know-how protection in transfer of technology is expected to be resolved.

Bibliography

Abele, E., Kuske, P., and Lang, H., editors, 2011, Schutz vor Produktpiraterie: ein Handbuch für den Maschinen- und Anlagenbau: Springer, Berlin.

Ahmad, A., Bosua, R., and Scheepers, R., 2014, Protecting organizational competitive advantage: A knowledge leakage perspective: Computers & Security, v. 42, p. 27–39.

Albino, V., Garavelli, A. C., and Schiuma, G., 1998, Knowledge transfer and inter-firm relationships in industrial districts: the role of the leader firm, *in* Technovation: Elsevier Science, p. 53–63.

Aljafari, R., and Sarnikar, S., 2009, A framework of assessing knowledge sharing risks in interorganozational networks: AMCIS 2009 Proceedings, p. Paper 592.

Andriessen, D., 2004, Making Sense of Intellectual Capital:

Anson, W., Suchy, D. P., and Ahya, C., 2005, Intellectual property valuation: a primer for identifying and determining value: American Bar Association, Section of Intellectual Property Law, Chicago, IL.

APA, 2015, Plagiate verursachen Milliardenschäden bei deutschen Firmen: DerStandard.

Applehans, W., Globe, A., and Laugero, G., 1999, Managing Knowledge: Addison Wesley, Boston.

Barrett, M., 2008, Intellectual property: Aspen Publishers, New York.

Bartelsman, E. J., and Beetsma, R. M. W. J., 2003, Why pay more? Corporate tax avoidance through transfer pricing in OECD countries: Journal of Public Economics, v. 87, p. 2225–2252.

Bergman, J., Jantunen, A., and Saksa, J.-M., 2004, Managing knolwedge creation and sharing - scenarios and dynamic capabilities in inter-industrial knolwedge networks, *in* Journal of knowledge management: Emerald.

Bloodgood, J. M., and Salisbury, W. D., 2001, Understanding the influence of organizational change strategies on information technology and knowledge management strategies: Decision Support Systems, v. 31, p. 55–69.

Bozeman, B., 2000, Technology transfer and public policy: a review of research and theory: Research Policy, v. 29, p. 627–655.

Branigan, T., 2016, Does China deserve a reputation as the land of copycats? The Guardian.

Brooking, A., 1996, Intellectual capital: Core assets for the third millenium enterprise: Thompson Business Press, London.

Bundesrepublik Deutschland, 1966, Aktiengesetz vom 6. September 1965 (BGBl. I S. 1089), das zuletzt durch Artikel 9 des Gesetzes vom 17. Juli 2017 (BGBl. I S. 2446) geändert worden ist:

Burgess, C., and Power, R., 2008, Secrets stolen, fortunes lost: preventing intellectual property theft and economic espionage in the 21st century: Elsevier Science, Burlington, MA.

Camisón, C., and Forés, B., 2010, Knowledge absorptive capacity: New insights for its conceptualization and measurement: Journal of Business Research, v. 63, p. 707–715.

Campbell, D., editor, 2007, International liability of corporate directors: Yorkhill Law Pub., Salzburg, Austria.

Carlsson, S., 2003, Strategic Knowledge Managing within the Context of Networks, *in* Holsapple, C. W. ed., Handbook on Knowledge Management: Knowledge Matters: Springer-Verlag, New York.

CEN TS 16555-4, 2014, Innovationsmanagement – Teil 4: Management des geistigen Eigentums:

Chun, C. L., 2007, Modeling the technology transfer to Taiwan from China, *in* International research journal of finance and economics:, p. 48–66.

Clausing, K. A., 2003, Tax-motivated transfer pricing and US intrafirm trade prices: Journal of Public Economics, v. 87, p. 2207–2223.

Cohen, J. A., 2005, Intangible assets: valuation and economic benefit: Wiley finance series, Wiley, Hoboken, N.J, 161 p.

Correa, C. M., 1981, Legal nature and contractual conditions in know-how transactions, *in* Georgia Journal of International and Comparative Law.:

Davenport, T. H., and Prusak, L., 2000, Working knowledge: How organizations manage what they know: Harvard Business School Press, Boston.

Desouza, K. C., and Vanapalli, G. K., 2005, Securing knowledge in organizations: lessons from the defense and intelligence sectors: International Journal of Information Management, v. 25, p. 85–98.

Di Benedetto, A., Calantone, R., and Zhang, C., 2003, International technology transfer, *in* International Marketing Review: London, p. 446–462.

Dixon, N., 2000, Common knowledge: Haravard Business School, Boston.

Easterby-Smith, M., Lyles, M. A., and Tsang, E. W. K., 2008, Inter-Organizational Knowledge Transfer: Current Themes and Future Prospects: Journal of Management Studies, v. 45, p. 677–690.

Edvinsson, L., and Sullivan, P., 1996, Developing a model of managing intellectual capital, *in* European management journal:, p. 356–364.

EESC, editor, 2017, Fake products cost 800,000 jobs annually:

Elmslie, M., and Portman, S., 2006, Intellectual property: the lifeblood of your company: Chandos, Oxford.

Fantl, J., 2017, Knowledge how, accessed December 26, 2018, at The stanford encyclopedia of philosophy at https://plato.stanford.edu/archives/fall2017/entries/knowledge-how/.

Foray, D., and Lundvall, B.-A., 1998, The knowledge-based economy, *in* Neef, D., Siesfeld, G. A., and Cefola, J. eds., The economic impact of knowledge: Butterworth-Heinemann, Boston, p. 115–121.

Frank, S. J., 2006, Intellectual property for managers and investors: a guide to evaluating, protecting, and exploiting IP: Cambridge University Press, Cambridge.

Ghrab, S., Saad, I., Kassel, G., and Gargouri, F., 2017, A core ontology of know-how and knowing-that for improving knowledge sharing and decision making in the digiatal age, *in* Journal of Decision Systems:, p. 138–151.

Gold, A. H., Malhotra, A., and Segars, A. H., 2001, Knowledge Management: An Organizational Capabilities Perspective: Journal of Management Information Systems, v. 18, p. 185–214.

Gopalakrishnan, S., and Santoro, M. D., 2004, Distinguishing Between Knowledge Transfer and Technology Transfer Activities: The Role of Key Organizational Factors: IEEE Transactions on Engineering Management, v. 51, p. 57–69.

Graf, H., 2011, Gatekeepers in regional networks of innovators: Cambridge Journal of Economics, v. 35, p. 173–198.

Grimm, M., and Anderl, R., 2013, Intellectual Property Protection and Secure Knowledge Management in Collaborative Systems Engineering: Procedia Computer Science, v. 16, p. 571–580.

Hatchuel, A., and Weil, B., 1995, Experts in Organisations: Walter de Gruyter, Berlin.

Hsu, J., 2015, New U.S. military chip self destructs on command: IEE Spectrum.

Hurmelinna-Laukkanen, P., 2011, Enabling collaborative innovation – knowledge protection for knowledge sharing: European Journal of Innovation Management, v. 14, p. 303–321.

Johannessen, A. J., Olaison, J., and Olsen, B., 2001, Mismanagement of tacit knowledge, *in* International Journal of Information Management: Elsevier Science, Amsterdam.

Kaarst-Brown, M. L., and Robey, D., 1999, More on myth, magic and metaphor: Cultural insights into the management of information technology in organizations: Information Technology & People, v. 12, p. 192–218.

Ketokivi, M., Turkulainen, V., Seppälä, T., and Rouvinen, P., 2017, Why locate manufacturing in a high cost country? A case study of 35 production location decisions, *in* Journal of operations management: Elsevier B.V., p. 20–30.

Klein, N., editor, 2015, Employer Branding: Wie können Unternehmen den “War for Talents” gewinnen und qualifizierte Mitarbeiter binden? ScienceFactory, München.

Kryssanov, V. V., Abramov, V. A., Fukuda, Y., and Konishi, K., 1998, The meaning of manufacturing know-how, *in* Jacucci, G., Olling, G., Preiss, K., and Wozny, M. eds., Globalization of manufacturing in the digital communications era of the 21st century: Innovation, agility, and the virtual enterprise: Springer US, Boston, MA, p. 375–385.

Larson, C., 2018, How China became a tech superpower: WIRED UK.

Lawder, 2016, U.S. keeps China, India on intellectual property shame list: Reuters.

Leenen, M., and Wolf, A., 2016, Global rail market growth set to slow: International Railway Journal.

Lev, B., 2001, Intangible: Management, measurement, and reporting: The Brooking Institution, Washington, DC.

Lewis, D., 1990, What experience teaches, *in* Lycan, W. G. ed., Mind and cognition: Blackwell, p. 29–57.

Liebeskind, J. P., 1996, Knowledge, strategy, and the theory of the firm, *in* Strategic Management Journal: John Wiley & Sons, p. 93–107.

Lundvall, B.-A., 2003, The economics of knowledge and learning:

Maier, J., 2018, Abilities, accessed December 26, 2018, at The stanford encyclopedia of philosophy at https://plato.stanford.edu/archives/spr2018/entries/abilities/.

Maldonado-Guzmán, G., Lopez-Torres, G. C., Garza-Reyes, J. A., Kumar, V., and Martinez-Covarrubias, J. L., 2016, Knowledge management as intellectual property: Evidence from Mexican manufacturing SMEs: Management Research Review, v. 39, p. 830–850.

Marr, B., and Schiuma, G., 2001, Measuring and managing intellectual capital and knowledge assets in new economy organisations, *in* Bourne, M. ed., Handbook of Performance Measurement: Gee, London.

McGavock, D. M., 2002, Intangible assets: A ticking time bomb.:

McKinsey, 2016, Huge value pool shifts ahead – how rolling stock manufacturers can lay track for profitable growth:

Mellen, C. M., and Evans, F. C., 2010, Valuation for M&A: building value in private companies: Wiley, Hoboken, N.J, 383 p.

Miles, R. E., Miles, G., and Snow, C. C., 2005, Collaborative entrepreneurship: how communities of networked firms use continuous innovation to create economic wealth: Stanford Business Books, Stanford, Calif, 132 p.

Mili, F., Narayanan, K., and VanDenBossche, D., 2001, Domain knowledge in engineering design: Nature, representation, and use, *in* Rajkumar, R. ed., Industrial knowledge management: A micro-level approach: Springer, London.

Mueller, 2005, Bharat Forge fordert ThyssenKrupp heraus. Mit deutscher Technik und indischen Kosten zum Weltmarktführer für Schmiedeteile.: Handelsblatt.

National Conference of Commissioners, 1985, UNIFORM TRADE SECRETS ACT WITH 1985 AMENDMENTS, *in* National conference of commissioners on uniform state laws – Minneapolis.

NBR, 2017, Update to the IP Commission Report:

Neemann, C. W., 2007, Methodik zum Schutz gegen Produktimitationen: Berichte aus der Produktionstechnik, Shaker, Aachen.

Nonaka, I., 1998, The knowledge-creating company, *in* Neef, D., Siesfeld, G. A., and Cefola, J. eds., The economic impact of knolwedge: Butterworth-Heinemann, Boston, p. 175–187.

Nonaka, I., and Krogh, G., 2009, Perspective-tacit knowledge and knowledge conversion: Controversy and advancement in organizational knowledge creation theory., *in* Organization Science:, p. 635–652.

Nonaka, I., and Teece, D. J., editors, 2001, Managing industrial knowledge: creation, transfer and utilization: SAGE, London.

Nonaka, I., and Toyama, R., 2003, The knowledge creation theory revisited: knowledge creation as a synthesizing process, *in* Knolwedge management research & practice:, p. 2–10.

Nonaka, I., Umemoto, K., and Senoo, D., 1996, From information processing to knowledge creation: a paradigm shift in business management, *in* Technology in society: Elsevier Science, p. 203–218.

Norman, P. M., 2001, Are your secrets safe? Knowledge protection in strategic alliances: Business Horizons, v. 44, p. 51–60.

O'Donoghue, N., and Croasdell, D. T., 2009, Protecting knowledge assets in multinational enterprises: a comparative case approach: VINE, v. 39, p. 298–318.

OECD, editor, 2006, Intellectual assets and value creation: Implications for corporate reporting: OECD Publishing, Paris.

OECD, editor, 2013, Supporting investment in knowledge capital, growth and innovation: OECD, Paris.

OECD, editor, 2016, Trade in counterfeit and pirated goods: mapping the economic impact: OECD Publishing, Paris.

OECD, editor, 2017, OECD Transfer Pricing Guidelines for Multinational Enterprises and Tax Administrations 2017: OECD Publishing.

Olander, H., Hurmelinna-Laukkanen, P., and Heilmann, P., 2015, Human resources – strength and weakness in protection of intellectual capital: Journal of Intellectual Capital, v. 16, p. 742–762.

Pandey, K., 2016, Paradigms of knowledge management: Springer Berlin Heidelberg, New York.

Parr, R. L., 2018, Intellectual property: valuation, infringement, and joint venture strategies: Wiley, Hoboken, New Jersey.

Poltorak, A., and Lerner, P., 2011, Essentials of intellectual property: law, economics, and strategy: Wiley, Hoboken, N.J.

Porter, M. E., 1998, Competitive advantage: creating and sustaining superior performance.: Free Press, New York.

Radosevic, S., 1999, International technology transfer and catch up in economic development: Edward Elgar, Cheltenham.

Rees, J., Bandyopadhyay, S., and Spafford, E. H., 2003, PFIRES: a policy framework for information security: Communications of the ACM, v. 46, p. 101–106.

Reilly, R., 2012, Intangible asset cost approach valuation procedure: American Bankruptcy Institute Journal, p. 58–59, 80–82.

Republik Österreich, 1966, 98. Bundesgesetz vom 31. März 1965 über Aktiengesellschaften:

Roos, J., Roos, G., Drganonetti, N. C., and Edvinsson, L., 1997, Intellectual capital: navigating the new business landscape: Macmillan, London.

Sas, B., Vocht, S. de, and Jacobs, P., 2014, Intellectual property and assessing its financial value:

Seeger, H., 2014, Fahrzeugdesign – informativ, *in* Basiswissen Transportation-Design: Springer Fachmedien Wiesbaden, Wiesbaden, p. 217–230.

Shane, S., 2009, Managing your intellectual property assets: Business Expert Press, New York.

Stjepandic, J., Liese, H., and Rulhoff, S., 2008, Intellectual property protection in virtual engineering, *in* 11. IFF-Wissenschaftstage – Magdeburg.

Sullivan, N. F., 1995, Technology transfer: making the most of your intellectual property: Cambridge University Press, New York.

Sveen, F. O., Rich, E., and Jager, M., 2007, Overcoming organizational challenges to secure knowledge management: Information Systems Frontiers, v. 9, p. 481–492.

Sveiby, K. E., 1997, The new organizational wealth: managing and measuring knowledge-based assets: Barret-Kohler, San Francisco.

Szulanski, G., 1996, Exploring internal stickiness: impediments to the transfer of best practice within the firm, *in* Strategic Management Journal:, p. 27–43.

Teece, D. J., 1998, Capturing value from knowledge assets: The new economy, markets for know-how, and intangible assets, *in* California Management Review:, p. 55–77.

Teece, D. J., 2000, Strategies for managing knowledge assets: the role of firm structure and industrial context, *in* Long Range Planning: Elsevier Science, p. 35–54.

Teece, D. J., editor, 2008, Technological know-how, organizational capabilities, and strategic management: business strategy and enterprise development in competitive environments: World Scientific, New Jersey.

Thompson, E. D., and Kaarst-Brown, M. L., 2005, Sensitive information: A review and research agenda: Journal of the American Society for Information Science and Technology, v. 56, p. 245–257.

Trkman, P., and Desouza, K. C., 2012, Knowledge risks in organizational networks: An exploratory framework: The Journal of Strategic Information Systems, v. 21, p. 1–17.

Truch, E., editor, 2004, Leveraging corporate knowledge: Gower, Aldershot, England.

VDI 5610-2, 2017, Wissensmanagement im Ingenieurwesen:

Viedma, J. M., and Salmador, M. P., 2013, Strategic management of intellectual capital in firms: attempting to bridge the gap between theory and practice: Knowledge Management Research & Practice, v. 11, p. 99–100.

Volkov, D., and Garanina, T., 2007, Intangible Assets: Importance in the Knowledge-Based Economy and the Role in Value Creation of a Company, *in* The Electronic Journal of Knowledge Management:, p. 539–550.

Wahab, S. A., Rose, R. C., and Osman, S. I. W., 2011, Defining the Concepts of Technology and Technology Transfer: A Literature Analysis: International Business Research, v. 5.

Walker, G., and Weber, D., 1984, A Transaction Cost Approach to Make-or-Buy Decisions: Administrative Science Quarterly, v. 29, p. 373.

Wang, R., and Lv, Y., 2017, Incentive Mechanisms for Tacit Knowledge-Sharing in Master-Apprentice Pattern Based on The Principal-Agent Theory, *in* MATEC Web of Conferences.:

Wiig, K. M., 1999, What future knowledge management users expect, *in* Journal of knowledge management:, p. 155–165.

Williamson, O. E., 1981, The Economics of Organization: The Transaction Cost Approach: American Journal of Sociology, v. 87, p. 548–577.

WIPO, 2019, About Intellectual Property, accessed January 26, 2019, at https://www.wipo.int/about-ip/en/.

Wölfel, T., 2003, Marken- und Produktpiraterie: eine Studie zu Erscheinungsformen und Bekämpfungsmöglichkeiten: Außenhandelspolitik und -praxis, Ibidem, Stuttgart.

Wong, K. Y., and Aspinwall, E., 2005, An empirical study of the important factors for knowledge-management adoption in the SME sector, *in* Journal of Knowledge Management:, p. 64–82.

List of figures

List of tables