Industry 4.0

Challenges when implementing Smart Factory.

Industri 4.0
Utmaningar vid en implementering av smarta fabriker.

Simon Broomé
Anton Renström

Health, Science and Technology
Master of Science in Industrial Engineering and Management
Master thesis: 30 ECTS
Supervisor: Alexandre Sukhov
Examinator: Peter Magnusson
2018-06-06
Issue: 1

Abstract

Industry 4.0 and the smart factory concept are both relevant for academia and companies. Many are talking about it but few understand the challenges that exist before, during, and after an implementation. The thesis aim is to map out the largest challenges with an implementation and also dive deeper into the question of which competence that will be required in a smarter production. To address these questions a qualitative study with thirteen interviews has been conducted, ten of which with practitioners and three with experts in the area. From the interviews the following findings and conclusions could be drawn. Firstly, the largest challenges with implementing industry 4.0 and smart factories will be, large CAPEX (Capital Expenditure) investments, organisational change management, and cyber threats. Secondly, Industry 4.0 is not going to be a revolution it is more going to be an evolution. Thirdly, implementing the smart factory concept is linked to a lot of uncertainty and especially uncertainty related to which competences that will be required. No one can with certainty define exactly what competences that are required but an education in IT and statistics with an analytical mindset will be key elements. There is also a model for how companies are recommended to think when filling vacancies created in the transition to a smarter production in the analysis chapter.

Keywords: Industry 4.0, Smart factory, Digital transformation, Change Management, Challenges

Sammanfattning

Industri 4.0 och konceptet den smarta fabriken är relevant både för akademin och företag. Många pratar om det men få förstår de utmaningar som existerar före, under och efter en implementation. Uppsatsens mål är att kartlägga de största utmaningarna och dyka djupare ned i frågan om vilka kompetenser som kommer att efterfrågas i en smartare produktion. För att adressera dessa frågor har en kvalitativ studie utförts med tretton intervjuer var av tio med praktiker på företag som kommer att eller har påbörjat en implementation. Ytterligare tre intervjuer har genomförts med externa experter som besitter sakkunskap inom ämnet. Från intervjuerna kunde följande slutsatser dras. Den första är de största utmaningarna som företag ställs inför är stora investeringar, organisationens förändringsbenägenhet och IT relaterade hot. Den andra är att Industri 4.0 inte kommer att vara en revolution det kommer att vara mer av en evolution. Den tredje är att en implementation av konceptet smarta fabriker är länkad till mycket osäkerhet och särskilt mycket osäkerhet när det kommer till vilka kompetenser som kommer att behövas i en smart fabrik. Ingen kan med säkerhet peka ut exakt vilka kompetenser som kommer att efterfrågas men en utbildningsbakgrund i IT och statistik samt ett analytiskt sinne kommer att vara nyckelelement. I analysen finns även en modell för hur företag rekommenderas att resonera när man fyller tjänster som skapats i transformationen mot en smartare produktion.

Nyckelord: Industry 4.0, Smarta Fabriker, Digital Transformation, Change Management, Utmaningar

Acknowledgements

The thesis is our final project in our Masters in Industrial Engineering and Management at Karlstad University.

First we would like to thank our supervisor Alexandre Sukhov for his guidance and support. We would also thank Hans-Owe Sjöö and his colleagues at the industry department at Ekan Management for their insights and encouragement.

We are especially grateful to all of you who have shared your knowledge with us during the interviews. It is because of your helpfulness and willingness to participate that made this thesis possible.

Lastly, we would thank our family and friends for your support during the process.

Karlstad, June 2018

Simon Broomé

Anton Renström

Table of content

List of Figures

List of Tables

List of Abbreviations

CPS	–	Cyber Physical System
DDoS	–	Distributed Denial of Services
DoS	–	Denial of Services
IoT	–	Internet of Things
IoS	–	Internet of services
CAPEX	–	Capital Expenditure
RoI	–	Return of Investment

1. Introduction

1.1. Background

There have been three industrial revolutions in the history of the manufacturing industry (Rüttimann & Stöckli 2016). A major technological change in the industry has followed each and every one of these revolutions (Lu 2017). Currently, in the brink of new technological advancements such as the Internet, smart algorithms, and rise of the IT sector/era, the manufacturing industry is facing a new industrial revolution, called "Industry 4.0". Industry 4.0 have since 2011 been on both researchers and practitioners mind. Questions like "how will Industry 4.0 shift the industry" and "how can companies be prepared for the change" are heavily researched right now (Lu 2017). Understanding how Industry 4.0 will change the manufacturing industry is a key factor for companies to be able to prepare for the challenges that follow (Lu 2017). It is important to understand how companies view Industry 4.0 and what potential pitfalls that stand in the way.

The first industrial revolution took place with new technologies to run machinery based on water and steam power, which started in the end of the 19th century. The second industrial revolution started during the early 20th century. The manufacturing industry started to work in more structured ways, employing a large workforce and the introduction of electrical power. It drastically decreased lead times and increased productivity. It took until the beginning of the 1970s before the industry faced a new technical advance big enough to shift the industry. The third industrial revolution brought an automatized production line, introduced electronics, and internet based technology (Lu 2017). The automatized production line decreased the need of manual labour, which resulted in a radical reduction in personnel.

All industrial revolutions have brought new technological advances but also alterations in how people work and what people are working with. These social interventions combined with technological advances have paved the way for the previous industrial revolutions. Coming in to the first quarter of the 21st century there is an alteration in how people are working. Individuals work less 9 to 5 and more flexible at the same time as consulting is a growing profession and companies choose to outsource a growing part of its business (Lu 2017). The transition into Industry 4.0 will take the manufacturing industry to the next level by adding more value and integrating knowledge management

(Lu 2017). The more advanced production will set new requirements on what kind of competences that will be sought after. It will be essential for companies to find and recruit talent that fit the new requirements to be able to be in the forefront of the technical era. It is important that manufacturing companies always develop and implements new technologies in its operations to be able to maintain a competitive advantage (Lu 2017). With the global market place companies are competing with each other on an international scale. It is especially important for companies that are active in countries with high labour costs to have a lean production since its competition is located in low cost countries (Ministry of Enterprise and Innovation 2016).

A step in being Industry 4.0 is implementing the smart factory concept. The idea behind the concept is to create customized products with high quality at a low price. It can be done with the help of smart manufacturing equipment that can communicate with each other and use business analytics to optimize its work (Wang et al. 2016). The data from the smart equipment are gathered and autonomous decisions are made by a cyber physical system (Parvin et al. 2013). The decisions are later carried out in physical actions in the factory. These decisions could for example be changing the temperature in an oven, dependant on humidity. The connection between highly automatic machines and the cyber-physical systems creates opportunities for the Swedish manufacturing industry to lower production costs.

There are not only benefits linked to the concept, it also involve challenges. Not all best practices are applicable for interconnected environment (Wang et al. 2017). Companies need to be able to protect themselves from more than just the old analog threats. New digital threats are something that needs to be at all companies agenda. The static types of security systems that are used today are not secure, security systems need to be updated constantly. Static systems are weak and will become easy targets for attacks. It is therefore important that the security system is evaluated multiple times per year and continuously upgraded (Wang et al. 2017).

Moreover, the United Nation came up with Sustainable Development Goals on September 25th 2015. There are 17 goals all of which have the purpose to create a more sustainable future (United Nations 2015). The smart factory concept could if implemented be a part solution to some of these goals. The most obvious one is goal number eight “Decent Work and Economic Growth”, it states as one of the goal criteria

“Achieve higher levels of economic productivity through diversification, technological upgrading and innovation, including through a focus on high-value added and labour-intensive sectors” (United Nations 2015). With an implementation of a smart factory concept the labour intensive sectors such as manufacturing can be optimised. Monotone and dangerous tasks can be removed and the over all health amongst workers can be improved.

1.2. Aim and research question

Industry 4.0 and the smart factory concept will bring along a change in the manufacturing industry. The challenges with implementing the smart factory concept are not clearly articulated in current research. However, the implications of introducing the smart factory concept affect more than just the company itself, it affects all stakeholders. The thesis aims to provide an explanation of the biggest challenges associated with an implementation of Industry 4.0.

Research question 1: What kind of future challenges will the smart factory concept create in the manufacturing industry?

Research question 2: How will a smarter production change the future requirement for competence in the context of manufacturing industry?

By addressing RQ1 and RQ2 can the connection between challenges with implementing the smart factory concept and with finding competent personnel be made. The connection will show how well the companies are suited to take on an implementation of the smart factory concept.

1.3. Case company

To study Industry 4.0 and the concept smart factory, Ekan Management (Ekan) that helped to facilitate the empirical investigation. Ekan is a management consulting company that was founded in 1985 that aid organizations both in private and public sectors. It has its headquarter in Gothenburg and employs over 50 management consultants with revenues of about 70 millions SEK (2016). Ekan’s competences lies within change management in a wide array of industries (Ekan 2013). Its consultants are experts within change management and have provided essential support in the different stages of the thesis.

1.4. Thesis outline

Chapter 1 presents the introduction. The reader is introduced to the research area and research questions.

Chapter 2 present the theoretical framework. The reader is provided with knowledge in the subject so that she can understand the analysis and result. The chapter give an explanation of Industry 4.0 and the smart factory concept from three different perspectives, technological, social, and managerial.

Chapter 3 explains the methodology that has been used in the thesis. There is also a discussion to why the methods are beneficial to use in both the collection and analysis phase. An explanation of trustworthiness and ethical matters is found in the end of the chapter.

Chapter 4 present an analysis of the data from the collection phase.

Chapter 5 provides the main findings and how they are linked to the theoretical framework as well as a model for deciding how to fill a vacancy created by a smarter production.

Chapter 6 provides a discussion of the main findings as well as the conclusions.

Chapter 7 presents the imitations of the thesis along will insights on where future research is needed.

2. Theoretical framework

2.1. Industry 4.0

The concept Industry 4.0 was firstly used in Germany to describe the country's high tech strategy and has become a buzzword that practitioners and academics are using to describe the fourth industrial revolution (Hofmann & Rüsch 2017). Professor Dieter Wegener provides a description of Industry 4.0 (Geissbauer et al. 2014, p. 8):

> The essence of the Industry 4.0 vision, the "Internet of Things", is the ubiquitous connection of people, things and machines. This connection is intended to produce a variety of new goods and services. Products, means of transport or tools are expected to "negotiate" within a virtual marketplace regarding which production elements could best accomplish the next production step. This would create a seamless link between the virtual world and the physical objects within the real world.

The parts of Industry 4.0 that professor Wegener suggests in his definition are Internet of Things (IoT), with interconnected devices and people, Internet of Services (IoS), the virtual market place, and Cyber-Physical Systems (CPS) with the seamless link between the virtual world and the physical world. That IoT, IoS, and CPS are major parts of industry 4.0 is supported by Hofmann and Rüsch (2017). After implementing a smart factory concept, productivity is proposed to increase with more than 10 % (Rüßmann et al. 2015; Hartigan et al. 2017). As the productivity increases there is a higher rate of output per input. Rüßmann et al. (2015) also suggest that the cycle time could decrease with up to 30 percent. The increase in productivity and decrease in cycle time can alter how an organisation deals with technological, social, and managerial changes. These areas all touch upon the topic of cyber security since it is present in the entire organisation.

2.1.1. Technological aspects

The first and oldest part of industry 4.0 is IoT. The concept of IoT is that multiple different devices are connected to the Internet and use it to be able to communicate with each other. The smart fridge that adds milk on the shopping list when the bottle is running low, is one of the most commonly used examples (Hoy 2015; Weber 2016). According to Hoy (2015), the smart fridge just brushing the surface and is barley an IoT device. A better example is the car that informs the air condition at home that the user left work early and will according to the GPS be home 45 minutes earlier than normal. Multiple different devices are communicating, the interconnectivity is an essential part of Industry 4.0. To be able to maximize the customer value the customer needs to be able to interact with the supplier and provide feedback to future improvements. The services can then be refined and create a higher level of customer value (Ketchen & Short 2011).

The importance that suppliers have a steady feedback loop with its customers is emphasised by Hofmann and Rüsch (2017). Internet of Services is described as a platform where customers can interact with the supplier. The platform is a place where customers can provide feedback and co-create services instead of just buying the suppliers services without any input. To work with customers provides a major benefit. Co-created services or products typically have a higher perceived value than services and products that had little or no influence by customers (Aarikka-Stenroos & Jaakkola 2012). Sales and perceived value are according to Ketchen and Short (2011) positively correlated. To be able to offer optimal customer value, the company need to be able to provide customized products with short delivery time at a low price. It will require a highly flexible production.

To decrease lead-time and cost and at the same time increase flexibility will require a higher level of automation. To use Cyber-Physical Systems will according to Parvin et al. (2013) make production more flexible and cost efficient. A CPS is made up by a virtual platform that makes autonomous decisions, which are then carried out in physical actions. The main difference between IoT and CPS is that a CPS does not need to be linked to the Internet to make decisions. However, Internet is often used to interconnect different machines to gather a larger pool of data to support decisions made by the virtual platform (Lee et al. 2015). Wang et al. (2016) presents BMW´s self-driving cars as a CPS system with hundreds of sensors that feed the virtual brain with information, which makes decisions based on the changing environment around it.

To have an interconnected and highly automated machine park and a customer feedback loop are parts of the smart factory concept with a more adaptable manufacturing strategy. The concept of smart factories is according to Wang et al. (2016) built on four different layers. The first layer is the physical recourse layer where the implementation of smart artefacts is made. A smart artefact is defined as everything from manufacturing equipment that reports how many items that are made every minute to fully autonomous devices that make decisions on their own. The second layer is a platform where the smart artefacts can communicate. The communication platform needs to be flexible and virtual so that new equipment easily can be added and removed. The third layer is the cloud layer, where gathered data is saved and tracked so that big data analytics can be used to improve the workflow and increase productivity. The forth and last layer is the control layer, all the artefacts can be monitored and configured here (Wang et al. 2016).

Wang et al. (2016) sees the smart factory as a dual closed-loop system where one of the loops contains the first, second, and third layer and the second loop is the third and forth layer see figure 1 for a visualization. There are financial benefits since it will provide a more streamlined production. One example of this is working with smart artefacts that make their own decisions and function autonomously based on orders provided directly by customers.

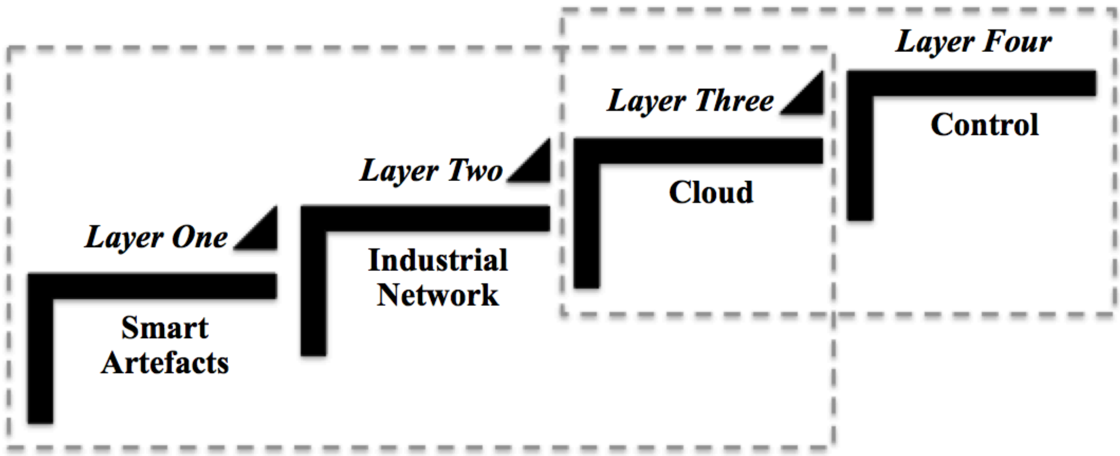

Figure 1, the figure visualises the layer on layer principle with two feedback loops from Wang et al. (2016).

Another more general description of what a smart factory is comes from Radziwon et al. (2014). A smart factory is described as a factory that is, flexible, lean, agile, and low cost. There are multiple links between the work from Radziwon et al. (2014) and Wang, et al. (2016). Radziwon et al. (2014) provides some insights in what traits that would be desirable in a smart factory and Wang et al. (2016) answers with a technical framework that would give the factory these desirable traits. For a factory to truly become smart it has to be able to produce customized products to a limited cost with a low level of waste, which can be achieved with the “layer on layer”-principle presented by Wang et al. (2016). There is not one formula for how a factory can become smart. It is more of a process where IoT, IoS, and CPS are tools that can be used. The technology exists and it is up to the companies to find its own version and level of how to adapt to the current trends.

The topic of cyber security is something that should be mentioned and discussed as smart factories is discussed. Since a big part of the concept is to make the entire production line more digital. The first thing that needs to be done is to establish what a threat actually is. There are many definitions and few clear answers. According to the International Organization for Standardization (ISO) a threat is described as:

> A threat is a potential event. When a threat turns into an actual event, it may cause an unwanted incident. It is unwanted because the incident may harm an organization or system. (ISO 27001 2005)

Another description of a threat is from the National Institute of Standards and Technology (NIST). A threat is according to NIST discribed as:

> Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. (National Institute of Standards and Technology 2006, p. 9)

From the previous descriptions of threats it is concluded that a threat is a potential event that could harm the organisation in some way. Recent studies concluded that there are four different categories of targets which are, individual, organizational, supply chain, and societal. For the purpose of the thesis only organizational targets are relevant since the thesis is limited to company level. According to Meulen et al. (2015) an organization is targeted with the purpose to:

- Access information about products and services.
- Access production means (including money and patents).
- To disrupt the organisations reputation.
- Decrease the organizations trustworthiness.

Companies that are targeted with cyber attacks are often attacked by criminals that are profit-driven. A profit-driven criminal is a person with the main goal to gain monetarily from an attack (Meulen et al. 2015). When an organisation is targeted by profit-driven criminals “unauthorised access” is a common attack technique. It is a broad technique that builds on other techniques. The attacker gains access to the organisation IT structure and can in a latter stage destroy and lockdown systems. Both of these strategies can have catastrophic financial impact on organisations. When dealing with CPS, attacks that build on Denial of Services (DoS) and Distributed Denial of Services (DDoS) are amongst the worst ones since the attacks are built upon limiting the information between the sensors and the virtual brain (Parkinson et al. 2017). A DoS or a DDoS attack can also disrupt the communication between the different machines as which could have severe consequences.

2.1.2. Social aspects

The manufacturing industry is facing its fourth revolution, it will result in large changes where simple jobs will become obsolete (Manyika et al. 2017). According to Manyika et al. (2017) up to 14 percent of total workforce will have to develop a new skillset and find new jobs since their current job will be replaced by an automated solution. Companies that are investing heavily in making its production smarter are then faced with massive investment costs, an unmotivated workforce, and the challenge of finding personnel with the correct skillset (Manyika et al. 2017).

It will be crucial that companies have employed managers that are experts in change management before the company starts investing in a smarter production (Ashkenas 2013). To find people that fit the company’s new needs is a great challenge. When a new position is created there are three different ways to fill the vacancy which are to, outsource, new hire, or educate excising personnel. All three have their advantages and disadvantages. When using consultants it is important not to outsource important core competences, it can make the organization hollow (Harland et al. 2005). The advantage is that the companies can buy knowledge without having to maintain it. Good tasks to outsource are tasks that are made seldom, speciality maintenance for example.

To use consultants to do everyday tasks such as general maintenance or operating manufacturing equipment is not preferred according to Harland et al. (2005). As the role of a machine operator changes there will be a shift in the competences needed, status quo is not an option. The first option is to hire new personnel with the required profile. Both the hiring process and the introduction process are costly elements (Baggot et al. 2005). The upside with hiring external personnel is that the company gains a new perspective. The downside is the costs associated with the hire and the risk of the new hire quitting. To educate and promote already excising personnel can be less costly and be motivating, ensuring a securer long-term employment (Chan 1996). The downside is that the company does not gain new insights. There is also the possibility that there is no one in the organisation that can take on the new tasks. One example is if there is a large difference in the excising competences and the required. Educating existing personnel would then be very costly and in some instances impossible (Chan 1996).

Not all security concerns come from outside the company. A big security risk comes from within the organization with workers stealing information and sabotaging (Dtex Systems 2017). It can for example be people who quit and start working for a competitor that bring customers with them to the new organization (Dtex Systems 2017). It is hard to limit since knowing who the customers are is a requirement to be able to accomplish the job properly. There are techniques to find out if it happened with for example implementing fictive customers with email addresses that bounce back to the original company. The company knows that there has been a security breach and can take quick actions to limit the damages. Other examples of internal security breaches could be that the personnel do not understand that their behaviour is posing a security risk (Dtex Systems 2017).

2.1.3. Management aspects

There are more differences between an analog production and a digital one. Analog protection has been more or less the same for centuries (Dtex Systems 2017). To protect something, build a wall around it and hire guards to defend it. The taller the wall is and the more guards that are used the harder it will be to get what ever that need to be protected. The old strategy is something that people understand and can plan for. The difference is when it comes to a digital production. A firewall that is not always evolving is within a few years going to become a sitting duck, not to improve the protection is the same thing as not having any protection at all (Peasley et al. 2017). Cyber security is linked to the economical factors as well. Companies need to invest heavily in protection against cyber threats to be able to enjoy the perks of the smart factory concept (Peasley et al. 2017).

The total cost of implementing the smart factory concept is much higher than the initial investment. A large cost is the increased vulnerability, which is resulting in a larger investment in IT security. Other hidden costs are the increased complexity and increased monitoring of personnel, network, and systems (Peasley et al. 2017). There is a financial aspect of the challenge with competence in the choice between new hire, education of old employees, or outsource.

To introduce the smart factory concept in a business is about creating a competitive advantage. Creating and maintaining a competitive advantage is crucial in today's business environment, especially for the European manufacturing industry since it is competing with companies active in countries with lower labour costs (Ketchen & Short 2011). The European manufacturing industry will invest more than €140 billion annually in creating smarter production lines and the topic of creating a smarter production is one of the most important questions amongst top management (Geissbauer et al. 2014). These statements suggest that companies are racing each other to be the first one to introduce a highly autonomous production. There is a significant decrease in direct labour costs when the production is autonomous in comparison to traditional manufacturing (Peasley et al. 2017). Direct labour costs are one of the most prominent expenses in Swedish manufacturing. With the introduction of smart factories, Swedish companies can compete with companies that are active in countries with a lower wages. It could bring back more of the production that has been lost during the last 40 years (Ministry of Enterprise and Innovation 2016).

2.1.4. Summary

Industry 4.0 is something large that spans over the entire organisation while smart factory a digitalization of the production. Smart factory is therefor considered a subcategory to Industry 4.0. Smart factory looked upon from three different aspects, technological, social, and managerial. In the chapter about the technology side of smart factory is the layer on layer principle and the three components of it described. The both the social and the managerial aspect of smart factory points out different ways to work with change management and how to appoint vacancies. All of the three sides that the smart factory concept has been reviewed from boils down to three main challenges, large investments, cyber threats, and unmotivated workforce. Figure 2 shows a visualization of how the theoretical framework is built up.

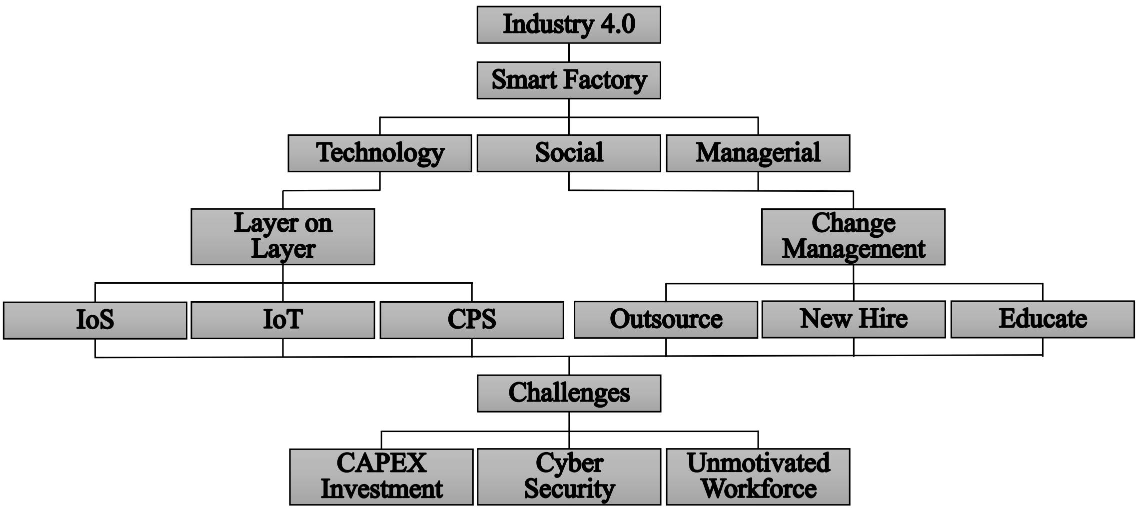

Figure 2, it is a visualization of how the theoretical framework is built up and what challenges that are identified.

3. Methodology

3.1. Research purpose

The purpose of the thesis is to explain the challenges and key factors when a manufacturing company progresses from traditional manufacturing techniques to a smarter production. The thesis is structured after Kothari's description of an exploratory research study. An exploratory study is about understanding a phenomena and the problem description (Kothari 2004). The strength with exploratory studies is that phenomenon's are examined in a new light providing the researcher with new insights and a greater understanding (Saunders et al. 2009). There is according to Saunders, et al. (2009) three different ways to gather data in exploratory studies, a literature review, expert interviews, or focus groups interviews. Expert interviews and interviews with practitioners were used for data collection in the thesis. When an exploratory research method is used, it is important to be flexible because the researcher needs to fit the research questions to the results to present all new insights (Saunders et al. 2009).

3.2. Research strategy and research design

To best answer the aim of the thesis a qualitative research approach has been used, in order to provide the researchers a deeper understanding about the underlying motives behind an implementation process of a smart factory concept. The decision to choose a qualitative research method was supported by the strong link between the exploratory research and qualitative research (Bryman & Bell 2011). The data collection phase and analysis phase are often two phases that are done in parallel (Bryman & Bell 2011). To investigate the future opportunities and key factors with smart factories, a multiple case study has been used. A case study approach is defined as "A research strategy that focuses on understanding the dynamics present within single settings" (Eisenhardt, 1989 p. 534). The method is usually used in industrial network research (Dubois & Gadde 2002). The case study method fits the purpose to gain a greater understanding of the research context (Saunders et al. 2009). There are different types of case studies but Eisenhardt (1989) and Yin (2009) argue that a multiple case study provides better explanation than a single case study since there is more data to ground theories on.

3.3. Research process

To make the thesis in a structured way a systematic combination approach has been used (Dubois & Gadde 2002). The idea behind systematic combining is to match theory with reality. It is a non-linear, path-dependent process of combining efforts with the objective (Dubois & Gadde 2002). Systematic combination is a method where the theoretical framework, empirical fieldwork, and case analysis evolve simultaneously (Dubois & Gadde 2002). Systematic combination can be divided into two different parts, first matching theory and reality then dealing with direction and redirection. The research process is identified step by step in retrospect. The research process can be seen in detail in figure 3. The process has moved back and forth between fieldwork and literature study and from empirics to theory. The development of the authors understanding of the concept smart factory can be seen in figure 3.

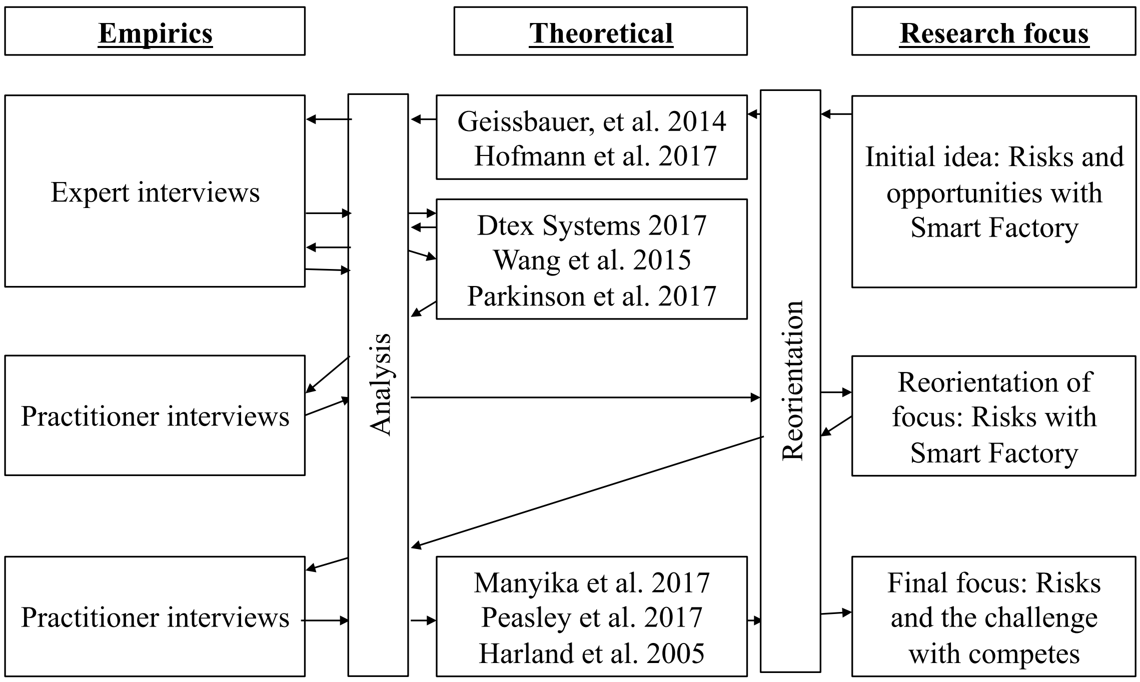

Figure 3, is a visualization of how the research process has been conducted, inspired from Huhtala et al. (2014)

The goal of the first step in the research process was to work out the research questions as well as the incentives for the thesis. It was done through cooperation with experts at Karlstad University and Ekan Management. The second step was to get a greater understanding of smart factory and the concept's different building blocks. To get an overview of the most important parts, three unstructured interviews were conducted with experts in the field of smart factories. Through the expert interviews and the literature study, of scientific articles, the theoretical framework started to take form. The next step was to conduct ten semi-structured interviews with practitioners that are either working with the implementation of smart factory or have good insight in the process. The interview phase and the analysis phase was done in parallel with the development of the theoretical framework. The data analysis generated several data sets that were analysed to answer the research questions. A comparison between existing theory and the findings were examined. The comparison, analysis, and findings are further presented as the conclusion.

3.4. Data collection

As previously mentioned, conducting interviews is a good research method when collecting data in exploratory research studies (Saunders et al. 2009). The type of one-time interviews is according to Saunders et al. (2009) a cross-sectional study. Many case studies are based on interviews done over a short period of time. It was therefore a natural choice to use a case study with interviews as the data collection method.

3.4.1. Unstructured interviews

Unstructured interviews approach was selected for the expert interviews because it provides the opportunity to have an open, in-depth discussion about the topic (Saunders et al. 2009). It means that there is no questionnaire that forms the basis for unstructured interviews. It is only an interview topic that governs the interview and points out the direction (Saunders et al. 2009). According to Gray (2017) unstructured interviews gives the respondent a lot of space to talk freely around a given subject.

3.4.2. Semi-structured interviews

Semi-structured interviews were selected for the interviews with the practitioners because it gives the interviewer the freedom to go deeper and probe on specific topics, which fits an exploratory study well (Saunders et al. 2009). The questions in the interview are based on both the outcome of the expert interviews and theoretical framework. When conducting semi-structured interviews an interview guide is used with so called “grand tour questions”. These are questions that lead the interviewee on to a specific topic, the interviewer can then steer the interviewee with probe questions to get more out of the interview. Working with semi-structured interviews ensures that the discussion is within the given framework (Saunders et al. 2009; Bryman & Bell 2011). There is no specific order that the grand tour questions needs to be asked during the interview (Gray 2017). Semi-structured interviews give the respondents the opportunity to express feelings and expand on the answers (Gray 2017). It is crucial that the interviewer takes a neutral position related to the topic, to conduct a successful interview (Yin 2011).

3.4.3. Description of interviews

The ambition with the interviews were to perform them at the location of the respondents ordinarily workplace or on another place that the respondent picked. In some cases, when in-person interviews was not possible they were conducted over telephone. The reason is that the respondent should feel as relaxed and safe as possible. The respondent should not be exposed to an unusual situation that could potentially lead to less credible answers. All interviews have been conducted in Swedish because both interviewers and the candidates have Swedish as their native tongue. All citations in the thesis have therefore been translated into English. All interviews were recorded using two mobile phones and varied in length from 30 to 75 minutes depending on respondents' availability and willingness to be interviewed. Details of the interviews can be seen in Table 1. The semi-structured interviews were based on a questionnaire that can be seen in the appendix, Appendix 1 for English and Appendix 2 for Swedish. Even questions that are not linked to these forms may be asked but have varied and been specific in each individual interview case.

Table 1, the table shows the order in which the interviews was conducted, position of the interviewees, role in the thesis, and interview length.

Interview	Date	Position	Role in the thesis	Interview Length (hour:min:sec)
1	18-03-07	Associate Professor in Computer Science	Expert	01:01:43
2	18-03-19	Plant Planning & Warehouse Manager	Practitioner	00:31:32
3	18-03-22	Director of R&D	Practitioner	01:13:50
4	18-03-23	Digitalization Manager	Practitioner	00:55:02
5	18-03-27	Software Engineer	Expert	00:46:06
6	18-04-06	IT Manager	Practitioner	00:50:01
7	18-04-06	Improvement Leader	Practitioner	00:52:56
8	18-04-06	Director of Industry 4.0	Practitioner	00:34:15
9	18-04-06	Enterprise Architect - Industry 4.0	Practitioner	01:04:11
10	18-04-12	Digitalisation Development Manager	Practitioner	00:47:49
11	18-04-12	Plant Manager	Practitioner	01:07:53
12	18-04-13	Project Manager - Industrial Digitalization	Expert	00:57:37
13	18-04-13	Managing Director	Practitioner	00:31:39

3.4.4. Sampling

An issue with qualitative research is the fact that it is impossible to collect all data and analyse it. It is a product of access to interviewees, money, and time (Saunders et al. 2009). The limitation in time to 20 weeks affects the thesis and the collection of data. The sample size should therefore be similar to other comparable studies in the same area with similar research questions (Denscombe 2009). With Denscombe (2009) reasoning is 13 interviews a good sample size. Data can according to Saunders et al. (2009) be collected from a sub-group instead from every case or elements. Some research questions can collect data from some cases and then generalize the data over all cases (Saunders et al. 2009). In the case where data collection is to be generalized, it is crucial to choose these people with care. Choosing respondents who have proven to be successful in their area will be able to help create a good understanding and knowledge (Saunders et al. 2009). According to Bryman and Bell (2011) many researchers argue that in research cases with a great depth in a specific phenomenon, representativeness is less important. The samples used in the thesis have been selected carefully from a purposive sampling viewpoint. The idea behind purposive sampling is to choose specific study elements that provide the most relevant and true information in the given area (Yin 2011). When respondents are selected, they should be selected because of their experience and knowledge not because how well they match the theoretical framework, it would damage the study's trustworthiness (Yin 2011).

3.5. Method of analysis

An analysis is according to Gray (2017) a process when data brakes down into smaller units that easier can be handled, characterized and structured. Descriptions can be seen as the base of the analysis, it is a way to understand and explain. Through out the analysis, new insights can be created and connections can be made between different concepts and data sets. These connections can be a basis for new descriptions (Gray 2017).

The Eisenhardt method of analysing data form case studies have been used with within-case analysis and cross-case analysis (Eisenhardt 1989). The method is built upon several steps, adapted for "multiple case" studies. When using the Eisenhardt technique different cases are compared with each other. Different pattern can be recognised over and across a set of data (Gray 2017). The analysis process used can be seen in figure 4.

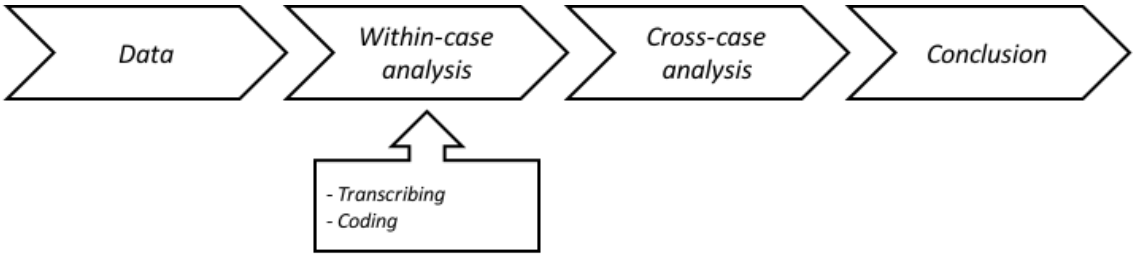

Figure 4, is a visualization of the analysis process.

3.5.1. Within-case analysis

Within-case analysis is the first step in the analyse part to familiarize and greater understand the data (Eisenhardt 1989). The way to do a correct within-case analysis is to transcribe the entire case study (Eisenhardt 1989). The data, an audio recording, gets transcribed so that everything that is said during the interview becomes text. It is the first step when analysing quantitative data according to Saunders et al. (2009). When that is done the data needs to be divided into different categories (Bryman & Bell 2011). The data will first be categorization after the main parts of the theoretical framework then broken down into even smaller subdivisions.

3.5.2. Cross-case analysis

The second step is according to Eisenhardt (1989) a cross-case analysis. A cross-case analysis is done so that the researcher has enough knowledge about the data. The cross-case analysis is about comparing the different data sets to see if there are any similarities and/or differences that may be interesting. It is according to Eisenhardt (1989) important to be open-minded during the process and avoid falling into false assumptions of what the data shows. When the findings are summed up, the different cases in the data set need to be compared to the theoretical framework and interpreted (Yin 2011). The similarities and differences between the finding and the theoretical framework is what the conclusion is built on (Yin 2011; Bryman & Bell 2011).

3.6. Trustworthiness

Trustworthiness is according to Lincoln and Guba (1985) to what extend the findings can be trusted. If the findings cannot be trusted the thesis does not carry any value and does not contribute research. Many researchers think differently when comes to judging the quality of qualitative data (Bryman & Bell 2011). However according to Lincoln and Guba (1985) there are criteria that need to be met. Trustworthiness is built on four principles, credibility, transferability, dependability, and confirmability (Lincoln & Guba 1985).

Credibility is about if the findings in the thesis match with the established theory or not. The credibility can, according to Bryman and Bell (2011), be improved by using respondent validation. Selected quotes and interpretation has been sent to respondents to ensure that no misunderstandings have been made, the mail can be found in Appendix 3.

Transferability is level that the findings can be applied to others organisations than the one studied, also called generalizability. To get a better transferability the reader should be provided with "a database for making judgements about the possible transferability of findings to other milieu" (Bryman & Bell 2011 p. 402). The findings are presented in a descriptive and pedagogical way. And the conclusion is based on a comparison between empirical data and the theoretical framework. The reader can follow and understand the logic behind the study.

Dependability is about on which level a study can be repeated. A way to get a good dependability is to use an auditing approach. The auditing approach has not been used due to a lack of time. Despite it, the possibility to replicate study is good since the research process can be followed step by step. A completely dependability is hard to get because people are different and interpret data differently due to their personal experiences (Bryman & Bell 2011).

Confirmability is the only criterion that can be linked to the researcher. It is about the knowledge the researcher has. The knowledge of the researcher must be sufficient so that it does not affect the result (Bryman & Bell 2011). In order to strengthen the confirmability in the thesis, the respondents' validation has been helpful. By responding to the results, they have confirmed that they reflect their experiences of the phenomenon that has been studied (Bryman & Bell 2011).

4. Analysis

Based on the data from the interviews the analysis was divided into three main parts related to the general perspective, risks, and challenges. The quotes from the interviews serve to provide some examples of what the interviewees said.

4.1. Industry 4.0 – Smart Factory, General perception

Generally, the respondents thought that Industry 4.0 was strongly linked to optimization of factories but many of them thought that Industry 4.0 also spans over the entire supply chain. The production becomes more flexible, predictable, and customer focused with a smarter production:

"My understanding of Industry 4.0 is that you can not distinguish operation from IT, both IT and operation go together, one is used to optimize the other." – Director of R&D

"Industry 4.0 is about the information flow within the business, production should always facilitate as much as possible for the end user." – Digitalisation Development Manager

Some of the respondents thought that Industry 4.0 is harder connected to production and factories than others. Most view the entire company as one unit, production and sales should be linked together with the help of Industry 4.0:

"Industry 4.0 is a wave that rolls through the entire company. It is something that happens horizontally across the entire organization." – Digitalization Manager

4.2. Challenges with Industry 4.0

Risks were something that many respondents needed to think about. Most respondents saw challenges in finding good talents and suppliers. Others saw big risks in large investments and with an uncertain return. IT security was another challenge that most respondents identified with a smart, connected factory:

"People tend to lose work ethic once given new tasks that is not in their old job description, this is a big risk with implementing Industry 4.0." – Improvement Leader

"It is quite clear that Industry 4.0 will require a large investment and I am not sure if everything is fully thought through. It seams like it is a race between different companies." – Plant Planning & Warehouse Manager

"A risk with Industry 4.0 is that you are opening up systems that are not meant to be open. IT-security was not something that was thought through when the systems where created." – Digitalisation Development Manager

How well the respondents know their competitors varied. The overall perception of the respondents was that they do not know what their competitors are doing in regards to Industry 4.0. But most of the interviewees were certain that no company in their industry was significant ahead of the others:

"My understanding is that our competitors are about the same level as we are." – IT Manager

"The interesting thing is that everyone believes that the others are one step ahead. But I am certain that no one is light years before anyone else" – Enterprise Architect - Industry 4.0

"We cooperate with the other companies. We see Sweden as a nation that can prosper if we work together." – Digitalisation Development Manager

The respondents thought that many factors in regards to the smart factory could have a negative impact on the company. The main considerations were change management, large upfront investment, and complex decision-making. Some of the respondents highlighted the fact that no one has fully developed a 100 % smart factory. There are some isolated "islands" that are smart and some pilot projects but nothing major. Since there is no one to benchmark companies tend to take it slow and try out the water before it fully commits to something:

"If smart factory is implemented the wrong way will one of the biggest dangers be stressing the staff, which can reduce productivity and reduce the impact made by the implementation." – Digitalization Manager

Many of the respondents worked at companies that had machines equipped with sensors for data collection. Most respondents use little or no data at all, despite the availability. Three out of ten stated that their company used the data to find patterns in the production to decrease down time. But only one out of ten stated that the data was used in a structured way to optimize production. Some of the respondents mean that the systems required to process all data is expensive and require competence that they do not have right now:

“We do not work that much with the data. It is really where the big value lies but we have not started yet.” – Director of Industry 4.0

“We do not work with the data we collect. The systems are too expensive for us.” – Improvement Leader

“The data has helped us when it comes to optimizing production, but it has all been done by hand, we do not have smart algorithms.” – Digitalization Manager

IT-security was discussed at all of the companies. But only two out of ten thought that their IT-security was effective and that the company was aware of the risk it faced. Half of the companies had an introduction course that new employees have to go through where IT-security as one module. Two out of ten stated that their company outsourced all IT security to an external partner. In general, all respondents thought that it was a challenge to building a safe security that at the same time was not too complex:

“A few years ago, there was no awareness of IT-security. The awareness nowadays is better due to the resent media attention is has gotten. So now there is a general awareness in society but also here.” – Digitalisation Development Manager

“It has been on the agenda for a long time, but one can never say that you are completely protected.” – IT Manager

“We are working hard to build IT-security into our systems.” – Director of Industry 4.0

The respondents thought that they and their organizations were aware of IT security, at least at an average level. At most of the respondents' companies, the managers went through a course in IT security. Many of the respondents thought it was substandard, they would have preferred if all personnel, regardless of position, underwent a similar education to build a stronger knowledge foundation of IT security in the company:

“Within our organization managers must undergo an e-learning class that is touching IT-security. But it does not go beyond the first line manager, it is up to them to take the information further.” – Plant Planning & Warehouse Manager

“It is without hesitation, very poor knowledge.” – Plant Planning & Warehouse Manager

The respondents stated that it is difficult to do capital expenditure (CAPEX) investments since the payback time need to less than 5 years. Some of the respondents said that investments with a payback time over 7 years are rarely, if ever done. The only exception would be if the investment were required for the company’s survival:

“All investments need to have a payback time of less than five years, if not crucial to our business.” – Managing Director

“It depends on the investment. Some investments are required for our survival, other investments must have a return of investment (RoI) of 3 to 5 years.” – Plant Planning & Warehouse Manager

“Investments need to have a RoI of under 2 years to be able to be processed.” – Digitalisation Development Manager

4.3. Social challenges - Competences

Generally, all respondents raised competence as one of the biggest challenges with implementing the smart factory concept. Knowledge is required for an implementation. The respondents said that since no one has implemented a 100 % smart factory it is hard to know what kind of competence that will be necessary. Questions such as “What do we do with our current personnel?” and “How do we recruit competent people if we do not know what we are looking for?” were raised in most interviews:

“Competence is number one and it will be painful, people have built their careers around an area that will with the current trend be useless, the internal map will be redrawn.” – Director of R&D

“Older people will have trouble adapting to the new trends. We will need a new kind of competence within our staff.” – Director of R&D

“To be the best, you need the best personnel. We currently have the best personnel but we will need recruit personnel with a different competence when we become more digitalized and I am not sure where to find that competence.” – Managing Director

The general perception of respondents is that they have not started with mapping out which skills that will be required in the process of transforming into a smarter production. They were aware of the fact that the required competence will be different in the future. All respondents wanted to solve the competence challenge by educating the existing personnel. They also saw that all challenges cannot be solved with educating existing personnel, to employ new people will be an important source of knowledge. In general, they saw an increased need for IT knowledge, but also understanding of statistics and analytics:

“We need to find a way to mapping out and changing routines so we know exactly what kind of knowledge that will be needed.” – Digitalization Manager

“We will try to educate our personnel and if all else fail remove some people from the organization if their proficiency profile no longer fits into the company. We try to limit this impact as much as possible by being open with the change and motivating people to learn more and develop their profile as much as possible.” – Director of R&D

“Competence is a big challenge it is not just about developing your own staff, it is also about gaining skills in general. Looking at digital skills, people with digital skills are currently working in other types of companies.” – Director of Industry 4.0

“A problem is that the people who have senior management roles do not have the right skillset to hold those positions anymore, their knowledge in IT is not good enough.” – Managing Director

“The role of a mechanic will undergo some changes within the next few years, there is a competence shortage there." – Plant Manager

The relationship between the respondents and the subcontractors varies. Less than half of the respondents considered their relationship with subcontractors as stable. Something that was highlighted by several of the respondents was the problem that the expertise they needed was located in small companies. Working with small companies pose a security threat, as security is not as prioritized in small companies compared big ones. All respondents stated that they strive to build long-term streamlined relationships with large suppliers:

“When you work with small players you often become very dependent on the person working. It may happen accidents which can alter the company’s faith.” – IT Manager

“You are very dependent on your subcontractors and consultants. Of course we make certain demands when but the question of IT-security is not a determining factor.” – Plant Planning & Warehouse Manager

5. Discussion

Technology

The first finding is that Industry 4.0 will be less of a revolution and more of an evolution. Many of the respondent stated that it is because of the large upfront investments. The current economy with payback times of three to five years give little or no room for drastic changes in production. The concern with large upfront investments is also addressed in theory as one of hurdles that companies need to surpass. As Wang et al. (2016) states, there are multiple different layers, and to be able to benefit from a smart factory are all of them required. Every layer involves a large investment, which means that implementing a smart factory will result in massive investments.

Moreover, many of the respondents address the issue that to create a safe system it will be too complex to use and at the same time very expensive. Peasley et al. (2017) describes how increased complexity is a result of making systems safer.

Social

Only one out of ten mentioned that the biggest security threat comes form within the organisation, the rest focused on external security breaches. Almost all of the interviewees said that the organization had poor or very poor IT knowledge. Mandatory classes in IT security could increase the knowledge and make the internal risk awareness higher. It is something that is supported by Dtex Systems (2017). If personnel knew better it would be easier to prevent internal mistakes.

Managerial

Another finding is that companies are faced with uncertainty, the sales forces are promising a reduction in production costs with little or no evidence. One respondent said that sales people approached him monthly to inform about the cost benefits with implementing a smarter production. The other respondents affirmed that they had been approached as well and that the sales people never looks at the full picture. The cost to get the correct competences is never in the calculation. Factories that are located in remote locations have problems with filling its vacancies right now and it will be even harder if the requirements are increased. From the interviews it is clear that companies are uncertain to what kind of competences that will be required.

Model for obtaining relevant competence

Competence was during the interviews identified as one of the largest challenges with implementing smart factory. Generally, the respondents wanted to educate existing personnel so they fit into the new role. There are three different ways to fill the vacancies, outsource, new hire, or educate excising personnel. There are different parameters that effect the decision. The following parameters has been identified after examining the literature by Harland et al. (2005), Baggot et al. (2005) and Chan (1996) as well as information from the interviews:

- Core competence, is the task related to the core of the business?
- Knowledge gap, difference between the competence that the company currently has and the required competence to complete the new task?
- Time until retirement, time that the person has before it retires?
- Everyday task, how often does the specific task occur?
- Specialty maintenance is there a need for very specific knowledge that might be hard to come by.

Furthermore, the figure 5 summarizes a method in how to weigh the three different options, outsource, new hire, or educate personnel. The model was composed from the literature from Harland et al. (2005), Baggot et al. (2005) and Chan (1996) as well as information obtained from the interviews. The questions core competences, main business, and everyday task comes from the literature. The rest of the questions and its answer alternatives have been formed based on the interviews.

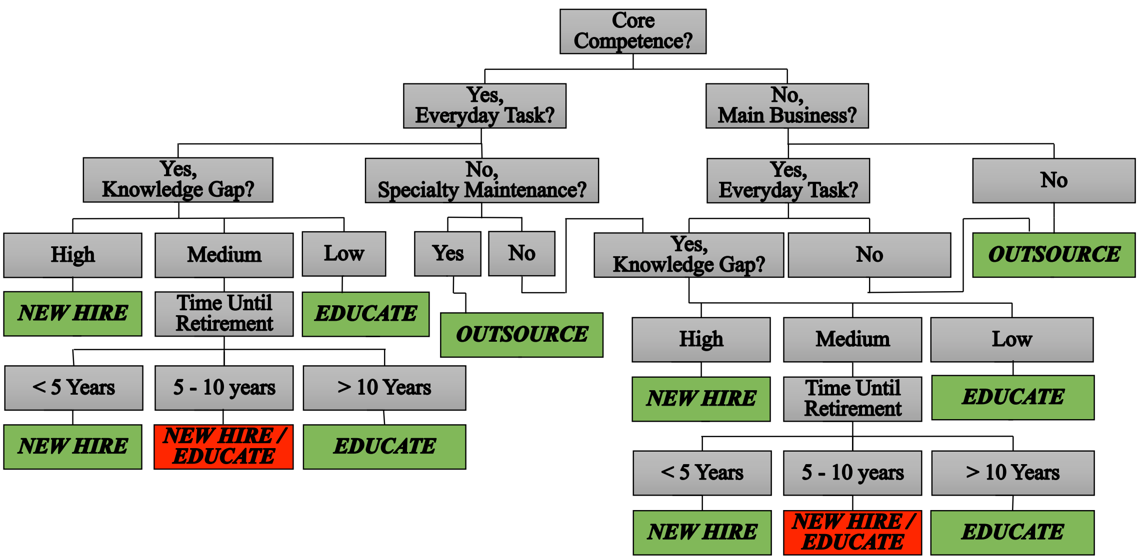

Figure 5, is a visualization of how the decision model on how to solve the competence challenge.

The figure 5 is a general tool that can be applied when management is faced with the decision to outsource, new hire, or educate excising personnel. The tool is easy to use in the most cases but some cases need a deeper analysis. The analysis needs to answer to the questing if it is most profitable to new hire or educate excising personnel. The next section, presents a practical application of the tool.

Example: Outsource, new hire, or educate excising personnel

Trucking ltd. need to increase its productivity and have decided to invest in new manufacturing equipment. The machine operator who is currently working with the old equipment does not have enough knowledge to run the new machine. The company is faced with the choice to either outsource, new hire, or educate.

Review the tool, figure 5, step by step and answer the questions.

Is the task considered a core competence?
Yes, the task has to do with the manufacturing and is an essential part of Trucking ltd business.

Is the task done on an everyday basis?
Yes, the task is done daily.

Knowledge gap, what is the difference between the excising competence level and the new one?
The operator has generally good knowledge about the company but lacks some cutting-edge skills in programming. The knowledge gap is considered to be medium.

Time until retirement, how many years will the worker retire?
The operator has eight years left to retirement.

The tool shows that it is unclear what is most profitable, new hire or educate. A closer analysis is necessary.

Analysis:

The cost to hire a person consists of the two parts, recruitment cost and start-up cost. Recruitment cost is associated with all costs until that the new employee has signed the employment contract. To be able to obtain accurate figures have a company working with recruiting people for vacancies like the one described in the example been contacted and helped with estimated parameters and costs seen in table 2.

Table 2, describes an estimation of the costs linked to a recruitment process.

Parameter	Cost (sek)
Cost, Recruitment Company	
Recuitment process, 1,5 x monthly salary (30 000 SEK)	**45 000,00 kr**
Advertisement	**10 000,00 kr**
Personality test	**5 000,00 kr**
Cost, Trucking ltd.	
Time from Trucking ltd., 10h x Monthly salary, 50 000 SEK/160h	**3 125,00 kr**
Sum	**63 125,00 kr**

The second part of a new hire process is the start-up cost. All costs associated with getting the new employee up to speed. It could be internships, familiarizing the workplace, and getting to know the new colleagues. The costs for Trucking ltd. are estimated in table 3.

Table 3, shows the cost for on-site education.

Parameter	Cost (SEK)
Internships	
E-learning class A	**2 000,00 kr**
E-learning class B	**2 000,00 kr**
Business understanding	**8 000,00 kr**
Product knowledge	**10 000,00 kr**
Other costs	
Learning the job, (It varies with how complex the job is, it might take up to years)	**45 000,00 kr**
Sum	**67 000,00 kr**

The sum of recruitment and start-up cost must be weighted against each other in order to make a decision on what is the most profitable, hire a new employee or educate the current staff. The education costs are costs that are specific to each case. They have been left blank in the example and been replaced by an ultimatum in table 4.

Table 4, describes a comparison between education and new hire.

New hire	Cost (sek)
Recruitment cost	63 125,00 kr
Startup cost	67 000,00 kr
Sum	130 125,00 kr
Educate excising personnel	
Education	x kr
Wage costs during education	y kr
Sum (x+y)	z kr
New hire vs Educate excising personnel	
New hire	130 125,00 kr < z kr
Educate excising personnel	130 125,00 kr > z kr

If the educate cost to educate is lower than 130 125 SEK is that more profitable to educate the machine operator and in the other case it is more profitable to hire someone new. The breakeven point in the example is 130 125 SEK. There are other parameters that the model does not consider such as:

- How long the employee has spent with the company?
- What are the consequences if the employee is not educated?
- Is the employee willing to go educate herself?
- What kind of informal role does the specific person have?

It is important to take these aspects in consideration when making a decision.

6. Conclusion

6.1. Future challenges with the smart factory

The respondents where asked to identify both challenges and advantages with implementing a smarter production. When asked about the benefits most of the respondents had no problem describing plenty of advantages. Many of them spoke almost like sales people and were certain that smart factory is the future. When asked about the risks many of the respondents brought up risks linked to implementation such as large upfront investments and organizational changes. Both of which are well anchored in the literature written by Wang et al. (2016) and Manyika et al. (2017). Another challenge also mentioned is the increased security risks when the implementation is finished, focus is mainly on the external threats. The internal security threats were only mentioned in one out of ten interviews as a factor to consider. It is alarming since most security threats are internal.

Moreover, a challenge that the interviewees also focused on was the challenge with uncertainty. Sales people presenting success stories and untested models had approached many of the respondents. It seamed like it installed some doubt in the interviewee's minds, many of them want to take it slow and test the waters before diving into it. One respondent's company tried to implement a smarter production and it did not have the desired results, strongly due to increased overhead costs and organisational setbacks. The uncertainty with not knowing how the implementation process will look like or what the results will be. It is something that will make decision makers wait with an investment until they are forced to take action.

After discussing with the experts the "We need to do something if we want stay in the game" mindset forces decision makers to take actions without actually thinking it through properly. One expert stated that he have been approached by companies wanting to do "digitalize" its production without considering to do a proper pre-study.

In conclusion, there are many risks linked to implementing a smart factory concept most of which are linked to the theory. The testimonials from the experts accompanied with the interviews with key people from the industry paints a picture that companies are taking it slow and trying to test the water until forced to make a decision. The decision is then poorly thought through and all risks are not weighted in to the decision.

6.2. The future requirement for competence in the context

To be able to discuss RQ2 is it first important to mention that all of the respondents stated that the transition to a smart factory will not be done at a flip of a light switch. It is something that will progress over a longer period of time. The insight that it is more of an evolution rather than a revolution drastically changes the playing field and makes it more complicated. Companies cannot simply remove employees and replace them with new talent with a different skillset, since the company is dependant on the excising personnel to run the factory during the transition phase. Change management will be a very important if not the most important trait amongst managers in the transition phase.

Another challenge managers are facing right now that needs to be looked upon before RQ2 is discussed is that managers are not sure what kind of talent they should look for. As one managing director put it, “Another problem is that the people who have senior management roles do not have the right skillset to hold those positions anymore, their knowledge in IT is not good enough”, what he meant is that managers are unfit to see what kind of skills that are required. When the question “How do you look at skills associated with smart factories?” was asked the answer was wage and responses such as “We have not started mapping that out” and “We try to educate our personnel so they fit the future requirements”. It is a large challenge to fill positions before you know what kind of competences that is required to do the job. Many of the respondents guessed that an educational background in IT with a good understanding of statistics would be preferable when asked to think freely. The educational background should be accompanied by an analytical mindset with an inclination to solve complex problems. Hiring people that fit that profile will be a challenge for the manufacturing industry and as one of the respondents put it “Looking at digital skills, people with digital skills are currently working in other types of companies”. What the respondent mean is that companies are looking to hire talents that are used to work in a totally different way than the company is able to offer. One respondent described how his company needed to hire talent it could not afford to be able to stay ahead of competition.

In conclusion, what kind of competences needed in the future implementation of a smart factory concept is a bit blurred. No one can with certainty describe exactly what kind of skills that are required but an education in IT and statistics with an analytical mindset will be key factors.

Figure 6 is presenting a visualization of how the transition from a traditional factory to a smart factory. As more and more of the machines become smart the need for people with an IT background is increasing (Tech Savvy Supervisors). But it is important to remember that a large portion of the company's revenues in the transition phase comes from the old equipment and therefore the employees holding a competence in mechanics. Change management will be one of the most important traits amongst managers.

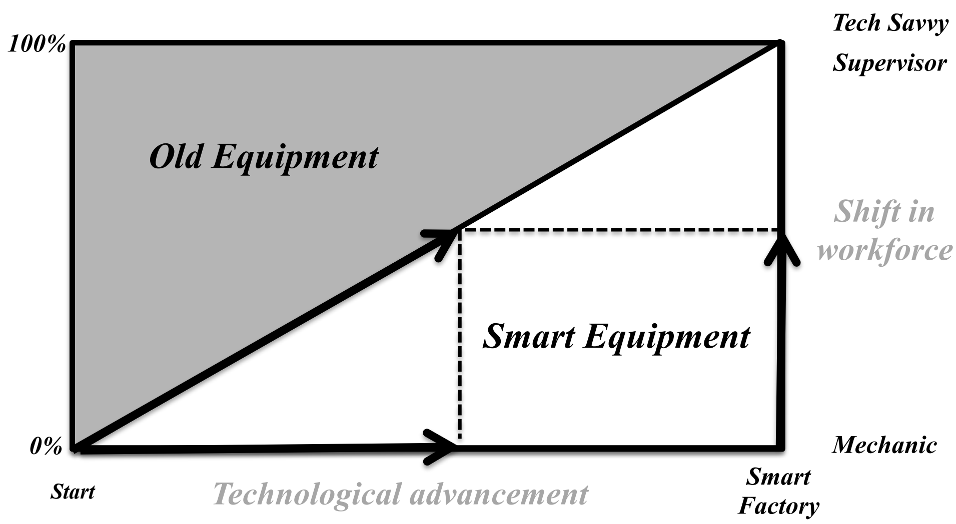

Figure 6, presents a visualization of what a transition from a traditional factory to a smart factory could look like.

6.3. Sustainability

Maybe the most important perspective is the one that views smart factory through the sustainability lenses. The United Nations goals to a more sustainable future go hand in hand with the smart factory concept. It was clear that all respondents took the social factor in to account during the interviews. One respondent stated that one of the main reasons to why he wanted to make the production smarter is to remove monotone elements in the workday for the operator, making their day better. Another aspect that came up during the interviews is that all of the respondents wanted to invest in the current employees and that they wanted to educate them in cyber security. It can improve their overall awareness of cyber threats, making them take better decisions in their personal life.

6.4. Trustworthiness

The thesis addresses the two research questions based on a systematic combining approach. The idea behind systematic combining is to match theory with reality, something that is important for keeping a good credibility. A good credibility has also been maintained by respondent validation. Using a multiple case studies has created a good transferability, since the study is based on several different perspectives from different organisations. The thesis is additionally written in a way so that the reader understands the comparison between the empirics and the theoretical framework. It gives the reader the tools to understand when the findings can be applied. Good dependability has been created through a detailed method chapter where the method is explained step by step, the thesis can be repeated by following these steps. The respondent validation has also provided the thesis with a good confirmability. The respondents have confirmed that their experiences of the phenomenon have been comprehended correctly.

7. Limitations and Future Research

The result of the thesis highlights the challenges that companies are facing during and after an implementation of a smart factory concept. The thesis does not touch by on how companies should work with minimizing these risks nor on how companies should act if the risks become real.

In future research, the risks identified should be analyzed separately in the context of smart factory concept and in other contexts as well. It would be beneficial since when the consequences are understood they could be limited. The consequences of not understanding the risks could be that the implementation fails, which could mean that the company looses its competitive edge. Looking at loosing the competitive edge from a sustainability perspective could mean that the company need to get rid of people to avoid bankruptcy, which is not a sustainable approach. It is therefor important to form easy to use tools that help companies analyze its current challenges but also the new ones that would occur if investing in a smarter production.

Moreover, more research is required on how the actual implementation process of a smart factory would look like. The implementation is something that will progress over a long period of time, which is why it is required to do it in a structured manner. It would act as a road on how to get to Industry 4.0. The road map would be beneficial for companies to get it started so it does not get put in the “we need to do something” position.

In addition, more research should be made regarding the competence challenge that companies are facing. Not only focused on operations but rather on the competence that management hold. More research should be focused on what competences managers and board members should hold to be able to make just decisions.

References

Aarikka-Stenroos, L. & Jaakkola, E., 2012. Value co-creation in knowledge intensive business services: A dyadic perspective on the joint problem solving process.. *Value in Business and Industrial Marketing, Industrial Marketing Management,* January, pp. 15-26.

Ashkenas, R., 2013. *Change Management Needs to Change*. [Online] Available at: https://hbr.org/2013/04/change-management-needs-to-cha [Accessed 24 April 2018].

Baggot, D. M., Hensinger, B., Parry, J., Valdes, M. S. & Zaim, S., 2005. The New Hire/Preceptor Experience. *The Journal of Nursing Administration*, March, pp. 138-145.

Bryman, A. & Bell, E., 2011. *Business research methods*. Oxford: Oxford University Press.

Chan, W., 1996. External Recruitment versus Internal Promotion. *Journal of Labor Economics*, 1 October, pp. 555-570.

Denscombe, M., 2009. *Forskningshandboken: för småskaliga forskningsprojekt inom samhällsvetenskaperna*. Lund: Studentlitteratur.

Dtex Systems, 2017. *Insider Threat Intelligence Report*. [Online] Available at: https://dtexsystems.com/2017-insider-threat-intelligence-report/ [Accessed 24 April 2018].

Dubois, A. & Gadde, L.-E., 2002. Systematic combining: an abductive approach to case research. *Journal of Business Research*, p. 553– 560.

Eisenhardt, K. M., 1989. Building theories from case study research. *Academy of Management Review*, 1 October, pp. 532-550.

Ekan, 2013. *Nytänk skapar framgång – det vet vi av erfarenhet*. [Online] Available at: http://www.ekan.com/om-ekan-management/ [Accessed 3 5 2018].

Geissbauer, D. R., Kuge, S. & & Schrauf, S., 2014. *Pws.nl.* [Online] Available at: https://www.strategyand.pwc.com/de/studien/industry-4-0 [Accessed 30 January 2018].

Gray, E. D., 2017. *Doing research in the business world*. 1 ed. London : SAGE Publications Ltd.

Harland, C., Knight, L., Lamming, R. & Walker, H., 2005. Outsourcing: assessing the risks and benefits for organisations, sectors and nations. *International Journal of Operations & Production Management*, 1 September, pp. 831-850.

Hartigan, M., Laaper, S., Mussomeli, A. & Gish, D., 2017. *The smart factory Responsive, adaptive, connected manufacturing*. [Online]
Available at: https://www2.deloitte.com/insights/us/en/focus/industry-4-0/smart-factory-connected-manufacturing.html [Accessed 10 March 2018].

Hofmann, E. & Rüsch, M., 2017. Research paper: Industry 4.0 and the current status as well as future prospects on logistics. *Computers in Industry*, August, p. 23–34.

Hoy, M., 2015. The "Internet of Things": What It Is and What It Means for Libraries. *Medical Reference Services Quarterly*, 3 July, pp. 353-358.

Huhtala, J.-P., Mattila, P., Sihvonen, A., & Tikkanen, H. (2014). Barriers to Innovation Diffusion in Industrial Networks: A Systematic Combining Approach. *Advances in Business Marketing and Purchasing*, August, pp. 61–76.

Isaksson, R., Garvare, R. & Johnson, M., 2015. The crippled bottom line – measuring and managing sustainability. *International Journal of Productivity and Performance Management*, 2 March, pp. 334-355.

ISO 27001, 2005. *Praxiom*. [Online]
Available at: http://www.praxiom.com/iso-27001-definitions.htm
[Accessed 25 February 2018].

Ketchen, D. & Short, J., 2011. *Mastering Strategic Management*. s.l.:Flatword .

Kothari, C., 2004. *Research Mathodology : Methods and Techniques*. s.l.:New Age International .

Lee, J., Bagheri, B. & Kao, H.-A., 2015. A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems. *Manufacturing Letters*, 1 January, pp. 18-23.

Lincoln, Y. & Guba, E., 1985. *Naturalistic Inquiry*. SAGE Publications, Inc.

Lu, Y., 2017. Industry 4.0: A survey on technologies, applications and open research issues. *Journal of Industrial Information Integration*, 5 June, pp. 1-10.

Manyika, J., Lund, S., Chui, M., Bughin, J., Woetzel, J., Batra, P., Ko, R. & Sanghvi, S., 2017. *Jobs lost, jobs gained: Workforce transitions in a time of automation*, s.l.: McKinsey Global Institute.

Meulen, N. v. d., Jo, E. A. & Soesanto, S., 2015. *Cybersecurity in the European Union and Beyond: Exploring the Threats and the Policy Responses*: Study, s.l.: Rand Corporation.

Ministry of Enterprise and Innovation, 2016. *Smart industry – a strategy for new industrialisation for Sweden*, s.l.: Elanders.

National Institute of Standards and Technology, 2006. *Minimum Security Requirements for Federal Information and Information Systems*. [Online]
Available at: https://csrc.nist.gov/csrc/media/publications/fips/200/final/documents/fips-200-final-march.pdf [Accessed 26 February 2018].

Parkinson, S., Ward, P., Wilson, K. & Miller, J., 2017. Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges. *IEEE Transactions on Intelligent Transportation Systems*, November, pp. 2898-2915.

Parvin, S., Hussain, F., Hussain, O., Thein, T. & Park, J., 2013. Multi-cyber framework for availability enhancement of cyber physical systems. *Computing*, 1 October, pp. 927-948.

Peasley, S., Hajj, R., Waslo, R., Carton, R. & Lewis, T., 2017. *Industry 4.0 and cybersecurity.* [Online]
Available at: https://www2.deloitte.com/insights/us/en/focus/industry-4-0/cybersecurity-managing-risk-in-age-of-connected-production.html [Accessed 24 April 2018].

Rüßmann, M., Lorenz, M., Gerbert, P., Waldner, M., Justus, J., Engel, P. & Harnisch, M., 2015. *Industry 4.0: The Future of Productivity and Growth in Manufacturing Industries*, Boston: Boston Consulting Group.

Rüttimann, B. & Stöckli, M., 2016. Lean and Industry 4.0-twins, partners, or contenders? a due clarification regarding the supposed clash of two production systems. *Journal of Service Science and Management*, September, pp. 485-500.

Radziwon, A., Bilberg, A., Bogers, M. & Madsen, E. S., 2014. The Smart Factory: Exploring Adaptive and Flexible Manufacturing Solutions. *Procedia Engineering*, 1 January, p. 1184–1190.

Saunders, M., Lewis, P. & Thornhill, A., 2009. *Research methods for business students*. s.l.:Harlow : Financial Times Prentice Hall, Pearson Education.

United Nations, 2015. *Sustainable Development Goals: 17 Goales to Transform Our World.* [Online] Available at: https://www.un.org/sustainabledevelopment/
[Använd 6 June 2018].

Wang, S., Wan, J., Li, D. & Zhang, C., 2015. Implementing Smart Factory of Industrie 4.0: An Outlook. *International Journal of Distributed Sensor Networks*, 1 January, pp. 18-23.

Wang, S., Wan, J., Zhang, D., Li, D. & Zhang, C., 2016. Towards smart factory for industry 4.0: a self-organized multi-agent system with big data based feedback and coordination. *Computer Networks*, 4 June.

Wang, Y., Anokhin, O. & Anderl, R., 2017. Concept and use Case Driven Approach for Mapping IT Security Requirements on System Assets and Processes in Industrie 4.0. *Manufacturing Systems 4.0*, 03 March, p. 207 – 212.

Weber, R. M., 2016. Internet of Things Becomes Next Big Thing. *Journal of Financial Service Professionals*, 1 November, p. 43–46.

Yin, R., 2009. *Case Study Research: Design and Methods.* 3 ed. London: SAGE Publications, Inc.

Yin, R. K., 2011. *Qualitative Research from start to finish*. New York: The Guilford Press.

Appendices

A.1 Interview guide (English)

Introduction
- Introduce ourselves
- Tell the respondent about the aim of the thesis and what the material will be used for.
- Tell the respondent how the material will be processed.
- Tell the respondent that the interviews are anonymous.
- Ask for approval for audio recording the interview.

Part 1, Start questions
- Can you tell me about your journey to reach the position you have today?
- Which questions do you work most with?
- Can you describe how a day in your shoes looks?

Part 2, General questions
- Have you heard of the concept Industry 4.0, what does it mean for your business?
- Which parts of the business have Industry 4.0 to do with?
- What do you do to promote this topic, can you give examples?
- What challenges and opportunities do you see with Industry 4.0?
- What are your competitors doing now and how does it affect you?

- How do you work structurally with the development of the factory?
  - How do you capture new concepts and how do you assess if they are worth investing in?
  - How do you then implement the changes and who are involved in the decisions?
  - What do you have for space to invest in new technologies?
- Have you worked in a factory where the smart factory concept has begun to be implemented?
  - What was the purpose of implementing smart factory?
  - How does smart factory connect to IT for you?
- What actions have you taken that are in line with the smart factory concept?
  - What has the action meant for you?
  - What is your vision of how the smart factory concept will work in your factory?
- Have you implemented smart machines?
  - If yes, what values have the implementation provided and is the effect somehow already measurable?
  - If no, why not?
- Is there an opportunity for the machines in your factory to send data to superordinate system?
  - If yes, what consequences has it meant for you?
  - If no, why not?

- Do you work with the data generated from the smart machines to optimize your production?
    - Have you moved the decision-making from man to the machine based on output data?
- How is the production line controlled today?
    - Why have you chosen this way?
- How is the production line optimized today?
    - Why have you chosen this way?

Part 3, Opportunity

- What are the primary opportunities you see when a factory implements the smart factory concept?
    - Why do you see these opportunities?
- How do you generally rate the amount of investment in relation to pay-back time?
    - Is the investments break-even a short period of time, or is it a long-term investment?
    - Which are the most important parameters when deciding to invest or not?
- Do you have other investments / concepts that you consider to be more promising and which you prioritize higher?

Part 4, Challenges

- What challenges do you see between present and your vision of smart factory?
    - Why do you just see these as challenges?
- How does an implementation affect the company negatively?
    - In what way are you prepared to take action that can limit the company to be adversely affected?
- How would you describe that the company's security is changing through an implementation?
- How do you work with IT security in your organization?
- Do you think that you and your organization have sufficient knowledge in IT security?
- Has the risk of smart factory been discussed at your company?
- Are you aware of how a hacker attack could affect your company?

Ending

- Is there something we have not asked about your experiences that you want to tell us?

A.2 Interview guide (Swedish)

Inledning

- Introducera oss själva vilka vi är och vad vi gör.
- Berätta om syftet och vad materialet ska användas till.
- Berätta om hur materialet kommer bearbetas, transkribering endast av oss.
- Berätta att intervjuerna är anonyma.
- Fråga om godkännande för inspelning av intervjun.

Del 1, Uppvärmningsfrågor

- Kan du berätta om din resa som du gjort för att nå den positionen som du har idag?
- Vilka frågor jobbar du mest med?
- Kan du beskriva hur en dag i dina skor hade sett ut?

Del 2, Generella frågor

- Har du hört talas om konceptet industri 4.0 vad betyder det för ditt företag?
- Vilka delar av verksamheten har industri 4.0 att göra med?
- Vad gör ni för att främja detta ämne, kan du ge exempel?
- Vilka risker och möjligheter ser ni med industri 4.0?
- Vad gör era konkurrenter just nu och hur påverkar det er?

- Hur jobbar ni rent strukturellt med utveckling av fabriken?
    - Hur fångar ni upp nya koncept och hur bedömer ni ifall de är värda att satsa på?
    - Hur genomför ni sedan förändringarna och vilka är inblandade i besluten?
    - Vad har ni för utrymme att satsa på nya tekniker?
- Har du arbetat i en fabrik där smart factory konceptet har börjat bli implementerat?
    - Vad var syftet med att implementera smart factory?
    - På vilket sätt kopplar smart factory till IT för dig?
- Vilka åtgärder har ni genomfört som går i linje med konceptet smart factory?
    - Vad har åtgärden inneburit för er?
    - Vilken är eran vision för hur smart factory konceptet skall fungera i er fabrik?
- Har ni implementerat smarta maskiner?
    - Om ja, vilka värden har implementationen tillfört och är effekten på något sätt redan mätbar?
    - Om nej, varför inte?
- Finns det en möjlighet för maskinerna i er fabrik att skicka data till ett överordnat system?
    - Om ja, vilka konsekvenser har detta inneburit för er?
    - Om nej, varför inte?
- Arbetar ni med den data som genereras från de smarta maskinerna för att optimera er produktion?
    - Har ni flyttat beslutfattandet från människan till maskinen baserat på output-data?

- Hur styrs produktionslinorna idag?
    - Varför har ni valt detta sätt?
- Hur optimeras produktionslinorna idag?
    - Varför har ni valt detta sätt?

Del 3, Möjligheter

- Vilka är de främsta möjligheter som du ser när en fabrik implementerar smart factory konceptet?
    - Varför ser du dessa möjligheter?
- Hur bedömer ni rent generellt magnituden av investeringen i förhållande till pay-back tid?
    - Kan denna typ av investering räknas hem på kort tid eller är det en långsiktig investering?
    - Hur vilka är de viktigaste parametrarna som styr vid en investering?
- Har ni andra investeringar/koncept som ni bedömer som mer lovande och som ni prioriterar högre?

Del 4, Utmaningar

- Vilka utmaningar ser du mellan nuläget och er vision av smart factory?
    - Varför ser du just dessa som utmaningar?
- På vilket sätt skullen en implementering påverka företaget negativt?
    - På vilket sätt är ni förberedda att vidta åtgärder som kan begränsa att företaget påverkas negativt?
- Hur skulle du beskriva att företagets säkerhet förändras i och med en implementering?
- Hur arbetar ni med IT-säkerhet i er organisation?
- Känner du att du och din organisation har tillräcklig kunskap inom IT-säkerhet?
- Har riskerna med smart factory diskuterats på ditt företag?
- Är ni medvetna om hur en hackerattack hade kunnat påverka ert företag?

Avslutning

- Är det något vi inte har frågat om dina erfarenheter som du vill berätta för oss?

B.1 Respondent validation e-mail (Swedish)

Hej X!
Tack återigen för att du medverkade på intervju och genom det har gjort vårat examensarbete möjligt.
Vi har valt ut några citat från intervjun med dig som vi önskar att använda i vår rapport. Vill med detta mail kontrollera att vår tolkning överensstämmer med din bild. Har du något du vill tillägga eller ändra på?

”Citat 1”
”Citat 2”
.
.
.
”Citat x

Med vänliga hälsningar,
Simon Broomé och Anton Renström
073-080 07 55 & 076-103 11 31

C.1 Coding of the interviews (Swedish)

	Industry 4.0 – Smart Factory, General perception		
	Konceptet industri 4.0, betyder för företaget		
1	Industri 4.0 är egentligen en ihopsättnig av flera automationsceller för att skapa en fullständig automationskedja, detta kallar vi digitalisering.	Samtliga tycker linande men uttrycker det olika	
2	Vi brukar säga vår förståelse av industri 4.0 är att man inte kan skilja drift teknologier från IT-delen, egentligen sitter ju dessa två delar ihop.		*"My understanding of industry 4.0 is that you can not distinguish operation from IT, both IT and operation go together, one is used to optimize the other."*
3	Ja, Flexabilitet.		
4	Ja, Så det handlar om att informationen ska flöda ihop med själva huvudverksamheten, produktionen. Nu ska man underlätta så mycket som möjligt för slutanvändaren. själva huvudverksamheten, produktionen.		*"Industry 4.0 is about the information flow within the business, production should always facilitate as much as possible for the end user."*
5	För mig är det att hitta smarta system som kan hjälpa oss att förebygga stopp.		
6	Som jag ser det kollar de mycket på flöden, så om du har en bit följer du dennes flöde och loggar massa data. Sen genom detta få hjälp i beslutfattandet kring hur en effektivisering ska genomföras.		
7	Jag ser det som naturlig utveckling av IT.		
8	För mig är det, det är ämnat för att vara, de 4 design principer		
9	Det talas mycket om digitalisering som ett koncept.		
10	Jag kan säga att begreppet betyder kanske inte så mycket men vi i konsernen kallar det digitalisering.		
	Delar i verksamheten förknippade med Industri 4.0		
1	Det är en våg som rullar genom hela fabriken. Något som sker över hela organisationen dvs. det spänner horisontellt över alla pelarstrukturerna.	Samtliga tycker liknande men uttrycker det olika	*"Industry 4.0 is a wave that rolls through the entire company. It is something that happens horizontally across the entire organization."*
2	Det berör alla delar.		
3	Det är framförallt vår produktion och eftermarknadsdel.		
4	Det är väl nästan ingen del som inte är kopplat till det.		
5	Det är framför allt underhåll men tror även det på sikt kan gå ner till operatörsnivå.		
6	Den är ju hårt kopplat till produktion men jag tror det går att anamma i alla verksamheter.		
7	Ja vill se det som en del av allt ting.		
8	Just Industri 4.0 är den digitala transformationen i tillverkning så främsta alla fabriker, processavdelningar och i viss del konstruktionsavdelningen.		
9	Så vitt jag har förstått hittils så jobbar bara vi med digitalisering i sitt IT-ben kan man säga.		
10	Där vi jobbar med olika delar som sedan skall kunna, givet att det fungerar bra kunna annamma detta på andra delar av konsernen.		
	Challenges with Industry 4.0		
	Risker Industri 4.0		
1	Gör man inte detta rätt från början och då får man människor som är negativa och som kommer att arbeta emot dig och då blir det svårt att få igenom det.		
2	Det är vår stora utmaning hur löser vi det här kompetensbehovet vi kommer se.		
3	Risken är att organisationen inte klarar av en sådan här förändring.		
4	Rent fysiskt öppna upp sig i en IT-perspektiv för att kunna utnyttja alla de möjligheter som finns.	4	*"A risk with industry 4.0 is that you are opening up systems that are not meant to be open. IT-security was not something that was thought through when the systems where created."*
5	Riskerna är att de här förmodligen kräver mer kunskap inom IT.		
6	Människor tappar lite arbetsmoral man måste försöka ge dem nya arbetsuppgifter vilket är en stor risk med det.	1, 2, 5, 6, 10	*"People tend to lose work ethic once given new tasks that is not in their old job description, this is a big risk with implementing Industry 4.0."*
7	Jag ser inga direkta risker det handlar om stora inventeringar, det är en risk.		
8	Riskerna är att du inventerar väldigt mycket och får ut väldigt lite.		
9	Det är ganska tydligt det kräver EXTREMA investeringar och jag vet inte om allt är, jag tror att företag, det blir en kapplöpning mellan olika företag, det känns inte som att alla investeringar är helt genomtänkta.	7, 8, 9	*"It is quite clear that Industry 4.0 will require a large investment and I am not sure if everything is fully thought through. It seams like it is a race between different companies."*
10	KOMPETENS, är den största utmaningen.		
	Konkurrenters framsteg		
1	Vi sammarbetar med de andra tillverkarna. Vi ser Sverige som en nation som kan hjälpas åt.	1	*"We cooperate with the other manufacturers. We see Sweden as a nation can prosper if we work together."*
2	-		
3	Det som är intressant är att alla tror att de andra är ett steg före. Men jag kan konstatera att jag inte har sätt någon fabrik som är ljusår före någon annan.	3	*"The interesting thing is that everyone believes that the others are one step ahead. But I am certain that no one is light years before anyone else"*
4	-		
5	-		
6	Jag vet inte, jag har en dålig uppfattning om det.		
7	Det har jag dålig koll på. Min upplevelse är att konkurrenterna är på ungefär samma nivå.	6, 7, 8, 9	*"My understanding is that our competitors are about the same level as we are."*
8	Egentligen har vi inge aning om vad de gör.		
9	Jag vågar inte spekulera i detta på grund av att jag inte vet tillräckligt.		
10	-		

	Påverka företaget negativt?		
1	Gör man det på fel sätt att den största faran är personalen. DVS att personalen blir stressad av en implementering vilket kan minska produktiviteten och det bildas lag eller gäng inom företaget som försöker begränsa implenentationens genomslagskraft. Jag har ännu inte noterat dom jos oss än. Om det inte görs på rätt sätt kommer det vara svårt att få ihop gänget. Även med gänget menar jag även olika produktionslinor och jag menar också mellan olika produktionstänk. Tex produktion vs underhåll. Det att få till helheten. Får man inte det så kommer folk att börja dra åt olika håll. Det kommer att bli kontraproduktivt. Personalen är den störsa risken. Eller att man gör en så dålig digitalisering så att det blir sämre så att man faktsikt producerar sämre produkter än innan. Det kan faktiskt inträffa om man har otur.	1, 4, 8, 9	*"If smart factory is implemented the wrong way will one of the biggest dangers be stressing the staff, which can reduce productivity and reduce the impact made by the implementation."*
2	-		
3	-		
4	Resurser och personresurser är alltid en brist. Mycket kring detta kanske inte är så moget, man vet inte riktigt vad man ska välja ännu. Det finns mycket potentiell men inte så mycket realiserat än. Kollar man runt i världen bland de som är längst inom industrin är det knappt någon som har kommit längre än någon pilotfabrik eller inom någon enstaka applikation. Så vi vet helt enkelt inte hur vi ska göra. Risken är att du hoppar på förmåga coola koncept och slukar dina resurser på det. Man lyckas inte välja rätt koncept och jobba med eller att du försummar din ordinarie verksamhet. Då finns det risk att man halkar efter och går på för mycket.		
5	-		
6	-		
7	-		
8	Att vi investerar i saker som inte levererar det önskade, detta har hänt och beror till viss del på organisationen och andra oförutedda faktorer. Vi har många fabriker och varje fabrik har ett visst kompetenscenter. Eftersom dessa fabriker löser sina problem lokalt görs det mycket saker flera gånger inom företaget. Det drabbar ju dessutom i slutänden samma plånbok. Det vi jobbar med är att centralisera den kompetensen. Utvecklar vi någon plattform ser vi till att den fungerar globalt. Lyckas vi inte standardisera till en hög grad kommer vi få en väldigt hög kostnad. Det skapar också en stor risk.	4, 8, 1	
9	Nej det är inget som vi har tagit hänsyn till när vi har gjort investeringskalkylen. Den stora frågan är snarare att hur man motiverar vi att investeringen skall bli gjord dvs kollar på föredlarna med den. Att sedan kompetensförsörja så att maskinerna kan fungera, det är ingen faktor just nu men det kan bli en faktor i framtiden.		
10	-		
	Insamlad data		
1	Datan har hjälpt oss när det kommer till optimera produktionen, skruva på maskinerna.	1	*"The data has helped us when it comes to optimizing production, but it has all been done by hand, we do not have smart algorithms."*
2	Vi har lärt oss från maskinerna och kunnat i efterhand identifierat vart det gick fel. För att kunna ändra på det till nästa gång. Vi har varit lite dåliga på att ta prediktiva belsut. Datan har mer används att se vart det gick fel.		
3	-		
4	Analysera och hitta mönster för konsekvenser.		
5	Vi använder mycket lite av datan, det enda som vi använder datan är i produktion men som sagt. Vi kan bli så mycket bättre på detta.		
6	Just nu gör vi inte så mycket med datan som vi samlat in. Systemen är för dyra för oss. I framtiden ser jag att vi kommer kunna arbeta med prediktivt underhåll	5, 6, 7, 8, 9,	*"We do not work with the data we collect. The systems are too expensive for us."*
7	Vi har en mängd data men vi har inte kommit igång med analysen av den ännu.		
8	Vi arbetar inte så mycket med datan. Det är egentligen där det stora värdet ligger men vi har inte kommit igång med det än.	2 ,4, 10	*"We do not work that much with the data. It is really where the big value lies but we have not started yet."*
9	Det finns stora möjligheter med datan när det kommer till att göra gysteringar men vi har inte kommit dit ännu.		
10	Vi arbetar till stor del med datan som samlas in. Men det är inte så automatiserat. Vi löser av datan manuellt och sedan med vår yrkeskunskap hittar vi sätt att optimera produktion. Nästa steg för oss är att då maskinerna att hitta olika mönster åt oss.		

	Hur arbetar ni med IT-Säkerhet?		
1	Ansvaret ligger hos IT-chefen. Eftersom jag har disputerat inom detta område kan jag säkert vara behjälplig inom detta. Man har mycket diskutioner inom detta, både i fabriken och i koncernen. Jag har en känsla av att det är mycket kvar innan vi har ett säkert system detta säger jag utan att ha grävt in mig i detta. Frågor som uppkommer är; vilka standards skall vi använda och vilken riktning skall vi gå.		
2	Vi kommer inte ta bort brandväggarna tror jag, Det gör vi inte, ha ha ha. Och som du säger cybersäkerhet är ett otroligt svårt område och kommer säkert få se olika saker som kommer hända. Vi har inte råkat illa ut än så länge vad jag vet. Men man vill inte bygget för säkert system men vill du fortfarande ha möjligheten att utnyttja det fritt. Det finns väldigt många som pratar om supersäkert system. Det jag har pratat med brukar fråga hur säkerheten i mitt system är så säger de att de ska visa vilka risker som finns och vilka potentiella förbättringar jag kan göra. Jag brukar då frågan och säg att det bättre att de berätta för mig hur jag bygger säkert system så jag kan göra. Då brukar diskussionen stanna eftersom de inte kan berätta hur det säkert ska designas.		
3	Det har faktiskt funnits länge, från den dagen internet kom och vi började koppla upp fabrikerna har arbetet med detta pågått. Detta var tidigt 90-tal vi började med det. I samma veva kom det första viruset sen fanns det 15 sen ökade det exponentiellt. Vi var givetvis tidiga med att starta säkerhetsavdelningar. Jag menar vi har hur många hot som helst mot våra brandväggar idag då. Så när infrastrukturen är uppbyggt på golvet har vi flera lager av säkerhet. Utmaningen nu är ju att jag vill ta min givare och stoppa det rätt ut i molnet. Har finns det ett antal skyddsnät men för att detta ska bli möjligt måste vi öppna upp dessa. Vi vill ju att givaren ska kopplas upp i molnet så alla kan komma åt den. Det jobbar inte jag med, jag är kravställare. Men vi har en hel säkerhetsavdelning som jobbar med hur detta ska gå till i praktiken. Vi kommer inte ta några risker så vi kommer vänta tills vi vet att det är helt säkert att gå in med den här teknologin.		
4	För 1–2 år sedan var det dåligt medvetande. Medans nu har det kommit upp i media väldigt mycket på olika fronter. Så nu finns det en allmän medvetenhet i samhället men även här. Man det är nog många som inte vet hur det kopplar till deras personliga vardag. Så där finns ett glapp som vi behöver täcka igen. Vi saknar kompetensen men nu när vi vet kan vi i alla fall köpa in den kompetensen. På så vis kan vi nog jobba sakta framåt. Vi är nog ganska konservativa men ibland tar vi också ganska stora steg. Ibland såväl okontrollerat som kontrollerat.	1, 3, 7, 8, 10	*"A few years ago, there was no awareness of IT-security. The awareness now days is better due to the resent media attention is has gotten. So now there is a general awareness in society but also here."*
5	IT-säkerheten har ju vår it chef hand om. Men vi hyr även in kompetensen idag. Vi har övervägt egen kompetens. Fördelen med detta hade varit om teknikerna hade mer lokalkännedom. Det kan skapa att vi får längre stopp än ibland nödvändigt. Problemen löses men det är inte bra.		
6	Vi har ganska bra koll på det. Vi har ganska hög säkerhet gällande det, vi har först och främst ett intrångsskydd. Jag är inte jätteorolig för detta. Går strömmen idag producerar vi inte redan idag något. Det är samma risk idag om man lägger upp det på någon server som kanske inte är i Sverige. Hela samhället bygger ju på att vi idag är el försörjda för att samhället ska fungera idag. Här är vi körda redan idag om något skulle hända. Såklart det är en viss risk men det var länge sen vi hade bara analogimaskiner som inte behövde el.		
7	Det jobbar koncernen oerhört hårt med. Vi har en egen it-företag. Det har varit på agendan länge, man ska aldrig säga att man är helt skyddad. Det tror jag är svårt att vara i dag, relativt sätt tror jag vi är bra skyddade. Den senaste typen av intrång har vi i hela koncernen klarat oss helt ifrån.	7	*"It has been on the agenda for a long time, but one can never say that you are completely protected."*
8	Alla nyanställda, vita, går en digital kurs där det går igenom hur de ska agera. Vi jobbar som skat mycket med att bygga in IT-säkerheten i systemen. Eftersom många hot kommer inifrån handlar detta om ett personligt beteende, att man har koll på sin dator och sina USBs.	8	*"We are working hard to build IT-security into our systems."*
9	Det är intressant, att man blir sårbar från helt nya hot. Det var väl ett år sedan som flera företag fick sin data låst och sedan fick betala för att få tillbaka den. Det är nya hot som ingen egentligen tänker på eller förutser med. Sen är det så att alla företags IT-avdelningar, för dem är det en jättestor parameter men de är inte insläppta i alla processer. Många maskiner är uppkopplade men IT är inte en del av den installationen. Utan de har hand om och ser till att centrala funktioner så som intranät och mailservrar fungerar. Det är en nog så viktig fråga med mycket känslig information. Men att maskiner blir uppkopplade så är det en annan grej, har man inte datasäkerhet som gör att man har en bra vägg mot vad det nu kan vara för en attack. Då skulle någon kunna ta sig in och stänga av. Jag tror att det är något som kommer att ske i en större utsträckning än vad det är nu. Det är något som måste få ta större plats.		
10	Det är något som står otroligt högt upp på vår lista inom hela koncernen. Men det är som du säger vi har maskiner som är uppkopplade mot våra leverantörer och de kan gå in och kontrollera maskinerna på distans. Det är en risk som finns och som kommer att bli större med tiden.		

	Har ni tillräcklig kunskap om IT-Säkerhet?		
1	Jag vet inte, jag har för dålig koll på människorna som arbetar i organisationen. Det är en fråga för XXX som är IT-chef. Det finns så många olika säkerhetsnivåer på IT. Ofta är den svagaste länken människorna, man lämnar ut lösenord eller något liknande. Jag kan nog inte svara på det för jag känner inte organisationen tillräckligt bra. Jag kan ju hitta på hot så som, har vi en trådlös uppkoppling till en maskin kan någon stå utanför och koppla upp sig själv och sedan komma in på maskinen. Man kan liksom koppla upp sig själv på maskinen så det finns andra typer av aspekter också. Visst måste man också tänka på maskinparken också! Man måste tänka på det också när man designar maskinparken. Hos oss kommer det nog att bli trådat nät. Man kör nog inte trådlös mer än kanske lokalt mellan olika hubbar då. På detta vis kan man läcka företagshemligheter.		
2	-		
3	Det vanligaste säkerhetshotet vi har är email, med länkar. Mailen i säg själv är ganska oskyldiga. Detta är ett problem som existerar hos alla bolag. Hos oss har vi utbildningar där vi försöker lära folk om vad som är på riktigt och inte. Det finns en bra förståelse kring säkerheten runt dagens lösningar. Morgondagens lösningar, industri 4.0, där vet inte branschen själv vilken säkerhet som behövs. Tänk att du köper en givare idag, de har ingen som helst säkerhet. Den förutsätter att du har direkt access till internet så den går att koppla upp. Där är det ingen säkerhet. Så jag tror hela branschen måste jobba med detta. Det syns också, det börjar växa fram några ramverk gällande detta nu det senaste 2 åren. Då är det säkerhet lyfts fram, frågan är då: Hur får jag detta säkert?		
4	-		
5	Absolut, ja det gör vi, vi har en säkerhets grupp där IT sitter som en av deltagarna i. Detta för att diskutera just såna här saker. Om vi skulle få in ett virus skulle hela fabriken kunna bli ner stängd. Det är viktigt. Personalen, vet de om hur man skall bete sig? Inte mer än hur de får arbeta med telefoner och datorer på jobbet.		
6	Nej inte just nu, det är en sån del som behövs jobbas på. Ska vi implementera detta kanske det behövs utbildning ända ner på operatörsnivå. Eller kompetenshöjda till den här nivån åtminstone. Detta är inget man skulle genomföra över en natt.		
7	Alla tjänstemän får genomgå en säkerhetsutbildning av IT. Det är egentligen även viktigt att operatörerna går denna utbildning. Det handlar ju om resurser, men jag tror mer på att jobba med säkra nätverk. Samt att segmentera, inte ha bara ett stort nätverk, utan att bryta ner det i olika delar. Att man segmenterar så som första del ska man skilja på vad som är kontor och vad som är produktionsnätverk. I förlängningen kommer vi jobba på att varje maskin får ett eget nätverk med egna brandvägg. Det gör att man kan säkra upp sig mot intrång utifrån. Sen är det en djungel, bovarna följer alltid med jämna steg, det sker ju en ständig utveckling där med. Känner ni att ni har tillräcklig kunskap angående IT-säkerhet? Jag tror vi kan göra mer men det handlar ju då om vart man ska mer lägga tid och pengar. Ska man jobba med att säkra upp systemen som sådana eller hur man ska jobba. Utbildning är givetvis viktigt men det är svårt att nå hela vägen fram där. Det kommer alltid finnas någon som slarvar eller skriver upp sitt lösenord.		
8	Det vill jag säga. Vi har en separat IT-avdelning och en separat person som är ansvarig för cyber-säkerhet i IoT miljöer. Så det vill jag säga, det handlar framför allt om vad man bygger.		
9	Det är utan att tveka undermåligt, mycket bristfällig kunskap! eller pratar vi central IT så har vi garanterat rätt person på rätt ställe men som sagt behovet spridet sig ut i organisationen hela vägen till golvet och det är många steg där kunskapen behöver komma ut i hela organisationen.	9	*"It is without hesitation, very poor knowledge."*
10	Vi kan säga att inom vårt bolag genomgår vi nätbaserade utbildnignar som vidrör detta. Men den kommer inte längre än första linjens chef. Men det kanske inte kommer hela vägen ner i organisationen. och det är upp till varje linjechef att ta denna informationen vidare i oragnisatioen.	5, 6, 9	*"Within our organization managers must undergo a e-learning class that is touching IT-security. But it does not go beyond the first line manager, it is up to them to take the information further."*
	Payback tid		
1	Vi räknar med tre år, efter det måste vi tjäna pengar. Sen har vi en Lekfaktor där vi kan testa nya saker men det är aldrig några stora investeringar.		
2	-		
3	Investeringsnivån är mycket beroende på vilken typ av maskin som skall köpas in. Olika maskiner har olika livslängder.		
4	Det är beroende på, vi har investeringar på 5 miljarder. Det kommer att ta långt tid att betala tillbaka den, 10-20 år. Det är svårt att byta ut maskienerna. Vi arbetar mer med utveckling av de maskinerna som finns.		
5	Är det en utbytesmaskin är det en utbytesmaskin, ibland får man även en produktionsökning genom bytet. Det kan ju ge möjlighet till merförsäljning om det går. Andra alternativet är att man ökar kapaciteten och minskar antalet mantimmar. Vissa saker måste man ha, det är våra anläggningschefer som räknar på detta. Man ställer olika saker emot varandra. Vi har gjort en flaskhalsanalys. Problemet med fabriken är att den är för liten jämfört mot den mängd av olika produkter som vi tillverka. Mycket för oss handlar om flödeshantering vilket skulle kunna optimera med digitala program.		
6	Vi tänker långsiktigt, det kanske är 30 år på vissa saker.		
7	Det är från investering till investering		
8	Är ROI under två år görs investeringen alltid, är den över tio år görs den aldrig och är den där emellas diskuteras det.	8	*"Investments need to have a RoI of under 2 years to be able to be processed."*
9	Fem år, alltid fem år.	3, 4, 5, 6, 7	*"It depends on the investment. Some investments are required for our survival, other investments must have a RoI of 3 to 5 years."*
10	Den skall räknas hem på 3 till fem år.	1, 8, 9, 10	*"All investments need to have a payback time of less than five years, if not crucial to our business."*

	Social challenges - Competences		
	Utmaningar?		
1	Kunskap är nummer ett, i alla delar av organisationen. Resurser, vem skall ta hand om det?		
2	Kompetens är nummer ett. Sen kommer det att vara smärtsamt, personer som byggt sin karriär kring ett område som sedan tas bort, den interna kartan kommer att ritas om.	1, 2, 3, 4, 5, 6, 7, 8, 9, 10	*"Competence is number one and it will be painful, people have built their careers around an area that will with the current trend be useless, the internal map will be redrawn." "Older people will have trouble adapting to the new trends. We will need a new kind of competence within our staff."*
3	Organisationen är det största problemet med kompetens. Vi måste bestömma oss för vilken typ av kompetens som är viktigast och som vi faktiskt vill ha kvar i organisationen.		
4	Kraven blir högre och högre på verktygen som används. Men kompetens är ett stort problem, äldre personer kommer att ha prblem att anpassa sig. Vi kommer att behöva ha en skruvande programmerare snart.		
5	Rollen underhållstekniker kommer vara annorlunda om några år, har ett kompetensproblem där, den behöver vara så mycekt större. Arbetsmiljön kommer att ändras med mer ensamarbete på grund av att förre personer behövs för att styra produktion.		
6	Arbetssätten, vi kommer att behöva standardisera arbetssätten. Stor kostnad att ta oss vidare till nästa steg. Vi kommer att behöva skapa nya system.		
7	Det är ingens ansvar i vår organisation, sen är kompetens ett stort problem.		
8	Change management, Kompetens, vi har inte rätt personer.		
9	Kompetens och change manangment, Vi behäver betala höga löner för att locka hit personasl.		
10	För att vara bäst behöver man den bästa personalen. VI har problemet att den bästa personalen kanske inte finns hos vår personal just nu om det blir mer digitaliserat.	10	*"To be the best, you need the best personnel. We currently have the best personnel but we will need recruit personnel with a different competence when we become more digitalized and I am not sure where to find that competence."*
	Kompetens		
1	Vi behöver hitta ett sätt att kartlägga och ändra på rutiner så att vi vet exakt vilken typ av kunskap som kommer att behövas.	1, 3, 8, 9, 10	*"We need to find a way to mapping out and changing routines so we know exactly what kind of knowledge that will be needed."*
2	Vi kommer att beöva placera om personer alternativt göra oss av med dem då deras kompetensprofil inte längre passar in i organisationen. Vi försöker begränsa denna påverkan så mycket som möjlight genom att vara öppna med detta och få människor att lära sig mer och utveckla sin profil.	2, 3, 7, 8, 9, 10	*"We will try to educate our personnel and if all ells fail remove some people from the organization if their proficiency profile no longer fits into the company. We try to limit this impact as much as possible by being open with the change and motivating people to learn more and develop their profile as much as possible."*
3	Hitta vilken profil som kommer att behövas. Det vet vi inte riktigt just nu. Det vi behöver mest just nu är dataanalytiker. Vi arbetar ständigt med att utveckla vår personal! Vi behöver ta bort de jobb som är tråkiga och ersätta dem med kul arbetsuppgifter. Den förändringen är något som de flesta kan ställa sig bakom.		
4	Det är ett problem med att kravprofilen växer. Vi kräver en mer analytisk förmåga som vi inte behövde förr. Vi måste ha någon som kan både skruva, vara analytisk och ny vara digitalt bevandrad också. Men det är ett team. Vi kan ha personal som håller vissa av delarna i ett team. Vi outsourcear de som inte är kärnverksamheten. Vi måste dock både gå på nyrektytering och utbilda de gamla anställda annars har vi inte tillräckligt med personal.		
5	Vi behöver ha mer mekaniska it-tekniker men de tror jag inte att det finns. Det är en utmaning men vi kommer inte att komma till att vi behöver göra det än, det kommer att ta några år till.		
6	-		
7	Det finns en del motsättningar i personnalen när det kommer till digitaliseringen. Men de som visar framfötterna bland personalen kommer att försöka utbilda, vi har en del sammarbeten med universitetet vi försöker nyrekrytera därifrån.		
8	Man ser det som en stor utmaning. Det handlar inte bara om att utveckla sin egen personal utan att få tag i kompetens allmänt. Kollar man på digital kompetens jobbar de idag på andra typer av bolag. De har en annan affärsmodell, kostnad och lönebild. För att utbilda personalen handlar det om globala utbildningsprogram som man måst sätt upp i ganska god tid. Kunskapen om industri 4.0 behövs framför allt innan och under införandet. När det väl är utrullat då behövs betydligt mindre kompetens att underhålla den. Så det är nu vi skulle behöva den kompentensen som vi börjar utbilda på. Det är alltid så men affärer man vill vänta in i det sista så man är säker på att behoven finns.	4, 8, 9, 10	*"Competence is a big challenge it is not just about developing your own staff, it is also about gaining skills in general. Looking at digital skills, people with digital skills are currently working in other types of companies."*
9	Det är just det att hitta kompetenser för de nya arbetsuppgifterna som uppkommer. Det blir svårare att felsöka, förr kunde man kanske bara banka på maskinen lite så kan man få igång maskineriet medans nu måste man in i komplicerade datorprogram vilket ställer höga krav på utbildning och datorkompetens.		
10	Det är svårt att göra sig av med människor i Sveige, vi måste utbilda och träna de medarbetarna som inte hänger med. Vi har ett problem till, personerna som sitter på höga roller inom bolag har inte rätt kompetens att sitta där längre, de har inte koll på IT och då behöver de ett nytt stöd	10	*"A problem is that the people who have senior management roles do not have the right skillset to hold those positions anymore, their knowledge in IT is not good enough."*

	Sitter i underleverantörers knä		
1	Det måste göras under kontrollerade former på något sätt. Man behvöer vara väldigt försiktig. Här handlar det om att bygga långsiktiga relationer med detta företaget. Det gäller att hitta konsultbolag som man bygger ett långsiktigtförtroendekapital. De måste veta att de måste leverea rätt produkter vid rätt tid annars är de borta för evigt. Vi snackar 10 års sikt, långsiktighet är viktigt! Vi vill arbeta med några få inte 100 st		
2	-		
3	Det har vi alltid haft. Viss kunskap har vi alltid haft tex kring motorn. Då vi anlitar underleverantörer är det till omkringliggande saker så som transportbanor mm. När en sådan upphandling görs jobbar man väldigt intensivt tillsammans med den leverantören men den antal resurser hos oss för att just göra den kompetensöverföringen. Även efter installationen är klar jobbar vi väldigt mycket med kompetensöverföring. Både mekaniskt och på IT-sidan. Vid såna processer har vi bra ramverk för hur vi ska arbeta.		
4	Den mesta utrustningen hamnar in i samma struktur som vi har och det är samma utrustning. Vi ser gärna att de använder exakt samma saker som vi har pga. underhållsskäl. Då kontrollerar vi ju det eftersom vi vet hur det underliggande systemet är. Applikationen uppe på har inte samma möjlighet att utgöra en risk på det sättet. Då löser man det gärna på så vis. Krävs något annorlunda löses det genom att den blir isolerad samtidigt som den heller kanske inte är produktionskritisk. Vi försöker standardisera.		
5	-		
6	De flesta har mer IT-säkerhet än oss. Vill man få ritningar från en leverantör tar man inte din sticka utan man får en ny från dem. Det är för den risk att saker kan hända. Nu när vi börjar bli mer medvetna om det kommer också vi börja ställa de kraven. Kompetensen är nog den stora delen, ju mer digitalt det blir ju mindre kan vi själva. Ju mer beroende bli vi av andra som hjälper oss, IT-konsulter. Detta är något som bör vägas in i risken. Vi kanske i framtiden delar data med andra anonymt för att lösningen ska bli billigare samtidigt som vi kan dra nytta av andras data för att köra våra maskiner bättre. Tänker vi på underhåll vill ingen utbilda sig till underhållstekniker. Erfarenheten saknas och de har ingen ork att gå i 10 år för att lära sig. För att bli en riktig duktig mekaniker. Tänk de smarta brillorna igen.		
7	När det gäller molnbaserade lösningar gäller det att säkerställa säkerheten hos leverantörerna. Där emot jobbar vi ibland med små spelare som hjälper oss med viss automatisering. Det tycker jag är olyckligt men det har sin förklaring i att de är de som har kunskapen om våra maskiner. Vi har väl inte riktigt kommit dit att våra maskiner är så standardiserade i gränssnitt och så att man kan jobba med vem som helst. Det handlar mycket om specialister. När man jobbar med små spelare blir man ofta väldigt personberoende. Det kan ju hända olyckor och liknande. Vilket vi har sätt. Det finns heller inte samma resurser hos dessa att satsa på säkerhet.	1, 7	*"When you work with small players you often become very dependent on the person working. It may happen accidents which can alter the company's faith."*
8	-		
9	Man blir mycket beroende av sina underleverantörer, Man ställer såklart vissa krav när man upphandlar men frågan är hur väl det egentligen uppfylls och underhålls. Det finns ingen kontroll efter upphandlingen. Det är iallafall min uppfattning. Frågan är om det egentligen är en aspekt som man kollar på när man bestämmer vilken leverantör och konsultfirma som skall användas. Jag skulle tro att det förmodligen inte är något som man kollar på.	1, 3, 4, 10	*"You are very dependent on your subcontractors and consultants. Of course we make certain demands when but the question of IT-security is not a determining factor."*
10	Absolut är det en risk! men det har alltid varit en risk, innan fick vi ringa och fråga hur vi bytte vissa saker nu behöver vi ringa och fråga hur man gör vissa inställningar. Det är nog inte så mycket skillnad.		