FACULTY OF TECHNOLOGY

OPERATIONAL RISK MANAGEMENT IN HIGH-MIX, LOW-VOLUME PRODUCTION

Joonas Mäenpää

Supervisors: Petteri Annunen, Osmo Kauppila, Johannes Soutukorva

INDUSTRIAL ENGINEERING AND MANAGEMENT

Master's thesis

May 2023

TIIVISTELMÄ

Operational Risk Management in High-Mix, Low-Volume Production

Joonas Mäenpää

Oulun yliopisto, Tuotantotalouden tutkinto-ohjelma

Diplomityö 2023, 117 s., 3 liitettä

Työn ohjaajat yliopistolla: Petteri Annunen, TkT & Osmo Kauppila, TkT

Tämän diplomityön tavoitteena on tutkia operatiivisten riskien hallintaa korkean vaihtuvuuden ja matalan volyymin (High-Mix, Low-Volume) tuotantoympäristöissä, pienissä ja keskisuurissa yrityksissä. Työn tavoite saavutetaan vastaamalla kolmeen tutkimuskysymykseen liittyen aiempaan kirjallisuuteen, case-yrityksen nykytilaan ja case-yrityksen toiminnan parantamiseen.

Diplomityö toteutetaan laadullisena tutkimuksena, jossa hyödynnetään kirjallisuuskatsausta ja case-tutkimusta. Kirjallisuuskatsaus muodostaa tutkimuksen teoreettisen viitekehyksen ja vastaa ensimmäiseen tutkimuskysymykseen esittelemällä aiempaa tutkimusta. Case-tutkimusta hyödynnetään case-yrityksen nykytilan kuvaamiseen, mikä antaa vastauksen toiseen tutkimuskysymykseen. Case-tutkimuksen aineisto koostuu case-yrityksen riskienhallintaan liittyvistä dokumenteista, havainnoista ja haastatteluista. Tutkimuksen osana suoritettiin kolme puolistrukturoitua haastattelua ja havainnot kerättiin osallistuvalla havainnoinnilla. Kolmanteen tutkimuskysymykseen vastataan empiirisen tutkimuksen ja kirjallisuuden vertailulla, jonka tuloksena saadaan ehdotuksia case-yrityksen toiminnan parantamiseen.

Tutkimuksen tuloksia ovat empiiriset havainnot yksittäisestä case-yrityksestä sekä parannusehdotukset case-yrityksen operatiivisten riskien hallintaan. Tarkkaan kuvattujen empiiristen havaintojen lisäksi työssä ohjeistetaan aiheeseen liittyvää jatkotutkimusta. Annetut parannusehdotukset ovat suoraan sovellettavissa case-yritykseen ja niiden odotetaan johtavan korkeampaan operatiivisten riskien hallinnan kyvykkyyteen. Toiset organisaatiot ja tutkimukset voivat hyötyä kirjallisuuskatsauksesta ja empiirisistä havainnoista, mutta parannusehdotuksilla on rajallinen yleistettävyys case-yrityksen ulkopuolelle. Jotkin parannusehdotukset voivat kuitenkin olla sovellettavissa yrityksiin, joilla on samankaltaisia käytänteitä tai piirteitä.

Asiasanat: riskienhallinta; tuotanto; maturiteettimalli; High-Mix, Low-Volume.

ABSTRACT

Operational Risk Management in High-Mix, Low-Volume Production

Joonas Mäenpää

University of Oulu, Degree Programme in Industrial Engineering and Management

Master's thesis 2023, 117 pp., 3 appendices

Supervisors at the university: Petteri Annunen, D.Sc. (Tech.) & Osmo Kauppila, D.Sc. (Tech.)

The objective of this Master's thesis is to study operational risk management in High-Mix, Low-Volume production, with a focus on small and medium-sized enterprises. This objective is achieved through answering three research questions regarding previous literature, current state in a case company, and improving practises in the case company.

This thesis is conducted as a qualitative research utilizing a literature review and a single case study. The literature review is utilized to form the theoretical foundation for the thesis, and to answer the first research question, providing the state of previous literature. The case study is utilized to obtain the current state in the case company, which answers the second research question. Case study data includes documentary data, observations, and interviews. Three semi-structured interviews were conducted, and the observations were obtained with participatory observing. The third research question is answered by comparing the empirical study and literature to provide improvement recommendations to the case company.

The findings of this study include the empirical results of operational risk management in a single case example, as well as the proposed improvements for the case company. The empirical observations are described in detail, and guidance for future studies is given. The development proposals are directly applicable to the case company and are expected to result in a higher operational risk management capability. The literature review and empirical observations may be useful to other researchers or organizations, but the recommendations have limited generalizability outside the case company. However, some of the recommendations might be applicable to a company with similar practises or organizational context.

Keywords: risk management; production; maturity model; High-Mix, Low-Volume.

FOREWORD

The topic of this Master's thesis was developed within my first month of employment in the case company. Several potential topics were evaluated, but this was selected as the most suitable for the needs of the case company, while being theoretical and extensive enough to be covered on a Master's thesis. The thesis work was conducted between December 2022 and April 2023.

I want to thank the case company for the trust in letting me propose an interesting topic for my thesis and work on it among my other duties. I want to also thank the interviewees, my co-workers, and other informants of the study for their input and flexibility during the study. Special thanks are due to my supervisors on both the company and university sides, who have provided their insightful input to this thesis and decisively contributed to my employment in the case company.

As the completion of this thesis leads to my graduation, I also want to thank the Industrial Engineering and Management research unit for excellent education and support. For the past five years I have had to work hard, but with the support and growth I have received, it has been well worth it. Last but not least, I want to express my gratitude to my wife and my family for their never-ending support during the writing of this thesis and all the years leading to it.

Oulu, 19.04.2023

Joonas Mäenpää

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

A1	Culture
A2	Process
A3	Experience
A4	Application
AIAG	Automotive Industry Action Group
ASQ	American Society for Quality
B1	Organizational Support
B2	Risk Management Process
B2B	Business-to-Business
B3	Managed Risks
BCBS	Basel Committee on Banking Supervision
BCP	Business Continuity Plan
CAR	Corrective Action Request
CP	Control Plan
D	Detection
DAU	Defense Acquisition University
DFMEA	Design Failure Mode and Effects Analysis
DoD	The United States Department of Defense
DOE	Design of Experiments
DPDTS	Director of Product Data and Test Systems
FMEA	Failure Mode and Effects Analysis
FMECA	Failure Mode, Effects, and Criticality Analysis
FTA	Fault Tree Analysis
GRR	Gage Repeatability and Reproducibility
HMLV	High-Mix, Low-Volume
ICT	Information and Communication Technologies
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
KPI	Key Performance Indicator
KRI	Key Risk Indicator
MRL	Manufacturing Readiness Level
MSA	Measurement System Analysis

MTBF	Mean Time Between Failures
MTTR	Mean Time to Repair
O	Occurrence
ODASD(SE)	Office of the Deputy Assistant Secretary of Defense for Systems Engineering
OEE	Overall Equipment Efficiency
OHS	Occupational Health and Safety
OHSAS	Occupational Health and Safety Assessment Series
OSDMTP	Office of the Secretary of Defense Manufacturing Technology Program
PDCA	Plan-Do-Check-Act
PFMEA	Process Failure Mode and Effects Analysis
PIR	Production Issues Report
PMBOK	Project Management Body of Knowledge
PMI	Project Management Institute
PPAP	Production Part Approval Process
PPT	People, Process, and Technology
QFD	Quality Function Deployment
QM	Quality Manager
QMS	Quality Management System
RCM	Reliability Centred Maintenance
RPN	Risk Priority Number
RQ	Research Question
RR	Risk Register
S	Severity
SC	Special Characteristic
SCRM	Supply Chain Risk Management
SME	Small and Medium-Sized Enterprise
SPC	Statistical Process Control
SWIFT	Structured What-if Technique
TQM	Total Quality management
TRL	Technology Readiness Level
VPPI	Vice President of Platforms Industrialization

1 INTRODUCTION

Risk management has become a prevalent topic in the recent academic research (Rampini et al., 2019). Due to the recent global crises, the interest towards risk management has increased also among companies of all sizes (Dvorsky et al., 2021). This has had an impact especially on Supply Chain Risk Management (SCRM) (Alicke et al., 2020; Marotta, 2020). However, growing interest has been recognized also in the risk management in Small and Medium-Sized Enterprises (SMEs) and operational risk management in the industrial sector (Ferreira de Araújo Lima et al., 2020). According to Ferreira de Araújo Lima et al. (2020) operational risk is one of the most common risk types studied in SMEs. However, according to Falkner and Hiebl (2015) there is a need for more empirical research on the implementation and control of risk management processes in SMEs. In addition, studying risk identification and analysis in SMEs would be useful to SMEs in practise (Falkner & Hiebl, 2015). Nevertheless, very little research exists on risk management in High-Mix, Low-Volume (HMLV) production. Same applies to studies assessing the operational risk management maturity in production.

A need for assessing the operational risk management practises was also recognized in a technology-driven SME based in Oulu, Finland, which acts as a case company in this study. The production operations in the case company can be described as HMLV due to the characteristics of the industry and the company in question. The operations also have characteristics of New Product Development (NPD) and project-based working. The case company operates in the Business-to-Business (B2B) sector, and collaborates with companies in various industries. These industries and stakeholders place their own expectations for the case company's operations, including risk management. The automotive industry is one example of a demanding operational environment (AIAG, 2019; Segismundo & Miguel, 2008).

1.1 Research objective

The objective of this study is to find out how operational risk should be managed in HMLV production SMEs. This is studied through a literature review and a single case study conducted in the forementioned case company. The results are also utilized to propose improvements to the operational risk management practises in the case company. The objective can be condensed into following three research questions (RQs):

- RQ1: How should operational risks be managed in High-Mix, Low-Volume production SMEs according to literature?
- RQ2: How are operational risks managed in the case company?
- RQ3: How can the risk management practises in the case company's production operations be improved?

As depicted in Figure 1 in section 1.2, answers to the RQ1, RQ2, and RQ3 are derived from the literature review, the empirical study, and the discussion, respectively. This forms a chain, where the ideal state is first instated in the literature review, the current state is established in the empirical study, and finally the ideal state and current state are compared to form development proposals in the discussion. Answers to RQ1, RQ2, and RQ3 are given in sections 2.6, 3.5, and 4.2, respectively. The key results are also briefly summarized in section 5.1.

1.2 Research approach

This thesis applies qualitative research principles. Case study was selected as the research strategy and a literature review was conducted to form the theoretical foundation of the study. The methods were selected based on the applicability to the subject in hand as well as to Industrial Engineering and Management research in general. Falkner and Hiebl (2015) and Ferreira de Araújo Lima et al. (2020) provide review articles of studies conducted on risk management in SMEs. Both of the articles highlight, that qualitative empirical studies utilizing either case study, interviews, or both, are common within the studied topic (Falkner & Hiebl, 2015; Ferreira de Araújo Lima et al., 2020). Industrial Engineering and Management is a multidisciplinary area of science, which combines engineering, business economics, and human behaviour (University of Oulu, n.d.).

The research process and its inputs and outputs, as well as their relation to the RQs are presented as a flowchart in Figure 1. The dark rectangles in the figure represent the main steps taken in the study. The lighter shapes represent any inputs and outputs linked to these steps of the process. The linkages are depicted with one-way arrows. Finally, the respective RQs are highlighted to the process outputs with dark circles, and the respective sections of this study are depicted with headings covering certain steps of the process. This process and the inputs and outputs are further described in the following paragraphs.

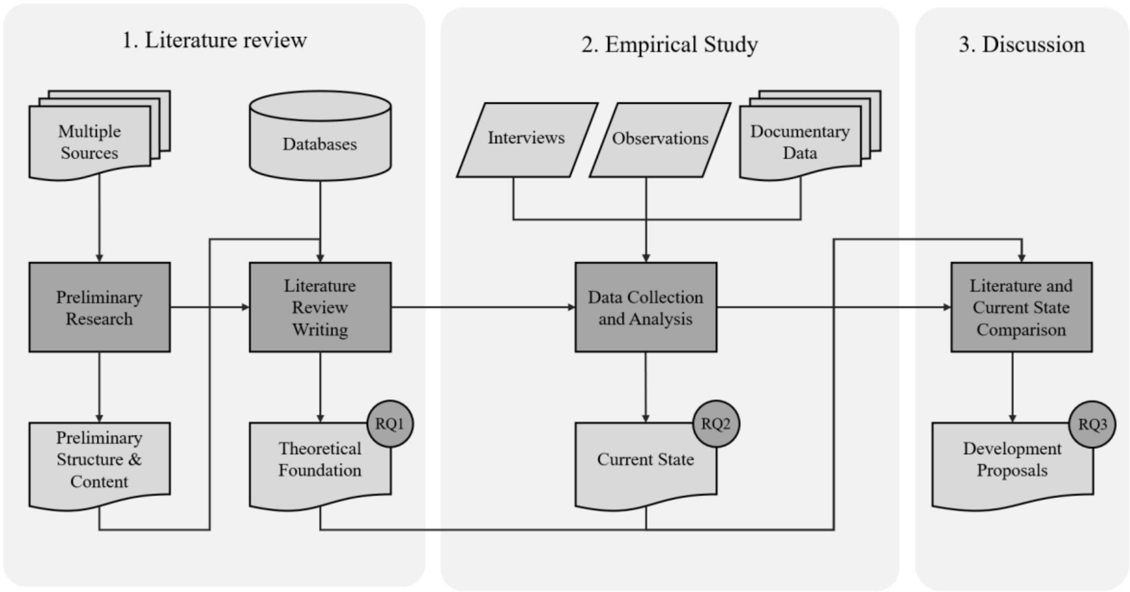

Figure 1. Flowchart of the research process with inputs and outputs and their relation to the research questions.

Tuomi and Sarajärvi (2018, Chapter 1.1.1) highlight the central role of theory in qualitative research. According to Webster and Watson (2002) literature review enables the creation of new information via forming the theoretical foundation and mapping the state of current research, revealing areas where further research needs to be conducted. The literature review presented in section 2 forms the theoretical foundation of this study.

The case company's needs, the International Organization for Standardization (ISO) standards, existing theses, and the University of Oulu Industrial Engineering and Management program's risk management course material were used for obtaining preliminary search terms and table of contents. These are depicted as "Multiple Sources" in Figure 1. The overall contents and structure remained mostly unchanged throughout conducting the literature review, with minor inclusions and exclusions. The initial references were obtained by searching for risk management related articles with most citations or published in well-established journals. Later, more specified searches were performed to obtain references related to a specific topic. Additionally, citation information from the databases and reference lists were used to go forward and backward in the citation chain to obtain more relevant references. This technique is also recommended by Webster and Watson (2002). References were obtained through Google search, Google Scholar, as well as Oula-Finna, EBSCO, and Scopus databases. These are depicted as "Databases" in Figure 1. The publications utilized in the literature review were handled using Mendeley Reference Manager. When possible, documents and metadata related to all publications, including web pages, were saved to the reference manager's library under a collection specific to this thesis. This enabled a reliable and efficient way to manage and store the used references and notes related to them.

Tuomi and Sarajärvi (2018, Chapter 1.3.7) highlight that in social relations there are no objective truths, but all knowledge is related to the context. According to Yin (2003, p. 13) case study investigates a phenomenon within its real-life context. The contexts in relation to this study are discussed in sections 2.2 and 3.2. According to Yin (2003, p. 2) case study allows the investigation of organizational and managerial processes and maturation of industries. Case studies are usually conducted to answer "how" and "why" questions (Yin, 2003, p. 1). In this case, the case study aims to answer the RQ2, to determine how operational risks are managed in the case company.

Case studies rely on past literature and empirical observations (Eisenhardt, 1989). According to Eisenhardt (1989), observations made in a case study need to be compared to both conflicting and supporting literature. This is done in section 4.4. According to Tuomi and Sarajärvi (2018, Chapter 3) most common data gathering methods in qualitative research include interviews, questionnaires, observations, and documentary data. Tuomi and Sarajärvi (2018, Chapter 3.2) claim that combining observations with another data gathering method often yields good results, and that observations might reveal any gaps between norms and the behaviours related to the norms. Utilization and combining of documentary data, interviews, and observations is common among case studies (Eisenhardt, 1989). In this study, observations are used in combination with interviews and documentary data. The methods used in the empirical study are introduced in detail in section 3.1. The interview questions are presented in Appendix 1. The results of the empirical study are analysed based on the theoretical foundation and two risk management maturity models presented in the literature review. The utilized maturity models are summarized in Appendices 2 and 3.

2 LITERATURE REVIEW

The purpose of this section is to form the theoretical foundation of the thesis. After the foundation is set in this section, the current state of the case company can be assessed, and improvement proposals can be made based on the established knowledge.

On section 2.1, risks and risk management will be introduced in a general level. The section 2.2 will then focus on some risk management contexts related to HMLV production and SMEs. The sections 2.3 and 2.4 will introduce some processes and tools for risk management, and section 2.5 introduces frameworks for assessing and improving risk management capability. Finally, the section 2.6 synthesizes the risk definitions, processes, tools, and frameworks that are most relevant to the empirical section of this thesis.

2.1 Risk management overview

2.1.1 Defining risks

The ISO (2018b) defines risk as an uncertain positive or negative effect on the organization’s objectives. The Project Management Institute (PMI) (2013, p. 310) joins this definition of risk in their publication Project Management Body of Knowledge (PMBOK). According to the PMI (2013, p. 310), these objectives can be for example the project’s scope, schedule, cost, or quality. The Office of the Deputy Assistant Secretary of Defense for Systems Engineering (ODASD(SE)) (2014) has a narrower definition for risk. Their risk definition includes only undesired effects, which can be considered more intuitive (PMIS Consulting, 2014). In this definition, positive risks are viewed as opportunities and realized risks as issues. What is common between these definitions is the uncertainty of risk (ODASD(SE), 2014).

According to the ISO (2018b), risks are often expressed using source, event, consequence, and likelihood related to the risk. Hillson (2014, p. 294) gives more examples of risk characteristics that may affect how and when the risk might be managed. These are the manageability of the risk, the schedule for when the risk might occur and when it could be managed, and the risk’s potential to affect the wider organization (Hillson, 2014, p. 294). Both Stewart (2020) and ISO (2018b) emphasize that the likelihood of a risk should not be confused with probability, which is often interpreted mathematically, as not all risks can be expressed using a mathematical probability. Stewart (2020) also challenges the traditional perception of risk as a multiplication of the risk's consequence with its probability. The author claims that reducing the expression of risk to this single numerical value does not communicate the risk adequately, as the possible impact in addition to the probability of the event is often uncertain. Hillson (2014, p. 283) highlights that the definition of risk should not contain only uncertain events but all sources of uncertainty.

Organizations face various risks, which can be categorized and sub-categorized in countless ways. Bailey et al. (2019) and PMI (2013, p. 310) categorize risks to known and unknown risks, which differ in the way they can be treated. Stewart (2020) supplements this categorization by categorizing risks to the known unknowns, knowable unknowns, and unknowable unknowns, referring to risk as "unknown". PMI (2013, p. 317) recommends categorizing risks based on the cause, whereas ODASD(SE) (2014, p. 22) utilizes a combined categorization of cause and effect. The latter categorization includes technical, programmatic, and business risks, where business risk is categorized based on the risk's source, and technical and programmatic risks are categorized based on the effect. The Basel Committee on Banking Supervision (BCBS) (2006) categorizes risks to credit, operational, and market risk. Operational risk can then be sub-categorized into risks arising from internal processes, people, systems, or external events (BCBS, 2006; Jobst, 2007). A similar risk categorization was presented by Javaid and Iqbal (2017) in their People, Process, and Technology (PPT) risk management model, which focused on risks in Information Systems. Marotta (2020) categorizes supply chain risks to internal and external risks. For example, the COVID-19 pandemic could be categorized as an external risk (Alicke et al., 2020; Marotta, 2020). It can also be categorized as an unknowable unknown or disruption risk, depending on the type of categorization (Chen et al., 2013; Stewart, 2020).

2.1.2 Risk management

Risk management is defined as a coordinated set of actions to direct the organization to address its risks (ISO, 2018b). According to the ODASD(SE) (2014), the purpose of the risk management process is to assess the likelihood of a future event and evaluate its consequences. The ISO (2018b) gives a vaguer description for the purpose of risk management as a creator and protector of value. Managing risks helps organizations in strategy setting, decision making, and achieving objectives (ISO, 2018b). Segismundo and Miguel (2008) also highlight risk management as a support for the decision-making process.

Risk management should be conducted as an organization-wide activity. In addition, comprehensive risk management should include collaboration with external stakeholders. (Ho et al., 2015; ISO, 2018b) Risk management should be viewed as an iterative process, which is continually improved (ISO, 2018b).

According to Xu et al. (2017), risk management practises can utilize paradigms like Total Quality Management (TQM), Six Sigma, or Statistical Process Control (SPC). TQM can help in managing risks related to human errors, negligence, or malice. Being more statistical, Sig Sigma and SPC can be used for system monitoring and managing defects. (Xu et al., 2017) Usage of statistical methods for risk management is prevalent in the insurance and financial industries (BCBS, 2006; European Banking Authority, 2017). In fact, according to Pergler (2012), the whole business model of financial institutions relies on risk calculations. Choi et al. (2018) discuss the usage of big data in the context of operations management. The authors claim that utilization of big data would be beneficial for risk analysis. Big data could for example provide quantitative likelihood estimates, which might be biased if performed by humans (Choi et al., 2018; Javaid & Iqbal, 2017).

2.1.3 Risk treatment

Marotta (2020) describes a strategy for treating risks in a supply chain by the Prevention, Preparedness, Response, Recovery (PPRR) risk management model. While not going into details, this model gives an overall view of what aspects should be considered when treating risks. Preventive actions reduce the likelihood of an event with unwanted consequences. Preparedness, response, and recovery are topics to consider in case the unwanted event still takes place. These actions could reduce the risk's consequences if planned and conducted properly (Marotta, 2020).

According to ISO (2018b) risk treatment options include avoiding the risk by not conducting an activity that causes the risk, removing the risk's source, reducing the likelihood or consequences of the risk, sharing the risk responsibility, or deciding to retain the risk. These options are commonly presented in the literature using four possible actions for risk treatment (Javaid & Iqbal, 2017; ODASD(SE), 2014, pp. 35–36; PMI, 2013, pp. 344–345). These actions are elaborated on Figure 2. According to the literature, the risks can be reduced, avoided, transferred, or accepted. The ISO (2018b) also points out that the risk treatment actions are not mutually exclusive, and several actions may need to be conducted before the risk can be accepted. The “reduce” action has been phrased slightly differently depending on the literature source. The ODASD(SE) (2014) uses the term “control”, PMI (2013) uses the term “mitigate”, and Javaid and Iqbal (2017) use the term “reduce”. However, all of these terms represent an action which reduces either the consequences or the likelihood of the unwanted event. The Automotive Industry Action Group (AIAG) (2019, pp. 119–120) recommends a priority of actions for risk treatment. According to AIAG (2019) the first action should be to try to mitigate the risk’s consequences, then to reduce its likelihood, and finally to increase the detectability of the effect. However, according to ODASD(SE) (2014, p. 26) it is more typical to reduce the likelihood than the consequence when mitigating risks. ODASD(SE) (2014, p. 36) also recommends to first evaluate avoidance, transfer, and acceptance actions, before reduction.

Avoidance tackles the cause of the risk by conducting the process in a way where the risk is not present (ODASD(SE), 2014, p. 35). This is done to avoid the factors that cause the risk (Javaid & Iqbal, 2017). However, in complex systems making changes to the process might introduce new risks (AIAG, 2019; Cook, 1998; ISO, 2018b). The PMI (2013, p. 343) also recognizes this phenomenon, and refers to it as secondary risk. Transferring the risk responsibility to another entity can be done for example by outsourcing and taking insurances (Javaid & Iqbal, 2017). Risk acceptance means that the risk is evaluated and the consequences are accepted if the risk is to be realized (ODASD(SE), 2014, p. 35). Acceptance can also be done to the residual risk, that is left after any risk treatment actions have reduced the risk to an acceptable level (Javaid & Iqbal, 2017).

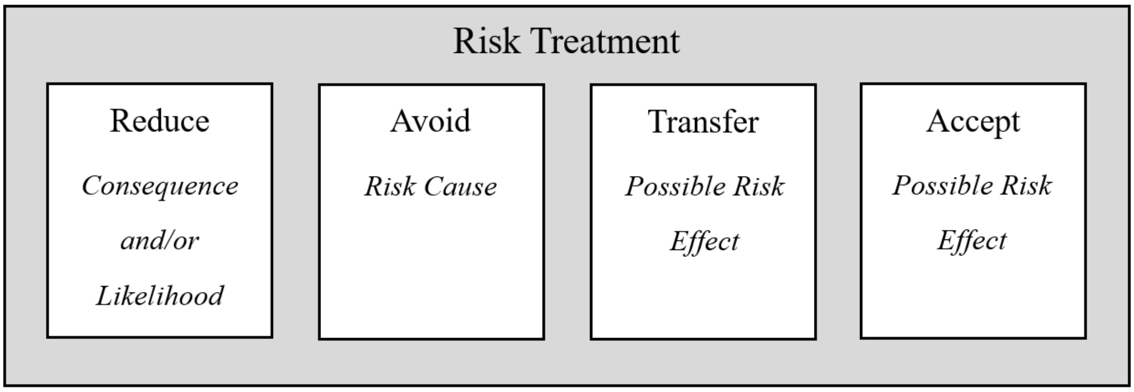

Figure 2. Risk treatment options based on (Javaid & Iqbal, 2017; ODASD(SE), 2014; PMI, 2013).

2.2 Risk management contexts

According to Dvorsky et al. (2021), recent financial and economic crises have caused a more proactive orientation to risk management in both SMEs and larger companies. The authors also highlight the importance of effective risk management in SMEs, as they claim it to be a deciding factor for survival in the competitive market. Falkner and Hiebl (2015) also demonstrate the importance of a risk management process in SMEs. They found that there is a notable difference in the formality of how risk management is conducted in different SMEs. Another finding was that the risk management practises in SMEs tend to evolve over time.

In the SME context, there has been an increase in the relevance of Project risk management, Strategic risk management, and SCRM in the literature (Ferreira de Araújo Lima et al., 2020). De Oliveira et al. (2017) also recognize a growing interest in SCRM among researchers in a more general level. In their systematic literature review, Ferreira de Araújo Lima et al. (2020) indicate that in the risk management literature, case study was a common study method, and operational risk was a commonly studied risk type, especially within the manufacturing industry.

In their risk management application platform for SMEs, Javaid and Iqbal (2017) emphasize that the first and most important step of risk management is to establish the scope and boundaries. An appropriate framework should be selected and tailored to the specific business process in question. (Javaid & Iqbal, 2017) The ISO (2018b) also suggests to establish understanding of the organization's internal and external context when designing the risk management framework. Some factors affecting the organization's internal context can be for example the organization's vision, mission, and values, the organizational structure, adopted standards, information systems, resources and knowledge, internal stakeholders, or contractual relationships. Similarly, the external context is affected for example by contractual relationships and commitments, external stakeholders, and cultural, political, regulatory, financial, and technological factors. In addition to understanding the organization and its context, the ISO 31000 risk management framework recommends articulating risk management commitment, assigning organizational roles and responsibilities, allocating resources, and establishing communication and consultation. (ISO, 2018b)

The internal and external context leads to different organizations having different attitudes towards risk (PMI, 2013, p. 311). According to PMI (2013) these attitudes reflect the degree of risk an organization is willing to take or able to withstand. For example, as the automotive industry is known for its high quality demands, legislative requirements, complexity, and competition, risk management is seen as a requirement for survival (AIAG, 2019; Segismundo & Miguel, 2008). This also affects companies that work as a part of an automotive supply chain, as collaboration within SCRM is widely highlighted in the literature (Alicke et al., 2020; Cavalcante de Souza Feitosa et al., 2021; Chen et al., 2013; Ho et al., 2015). Collaboration with external stakeholders, coupled with the "customer focus" and "risk-based thinking" underlined in the ISO 9001 standard, describes the external pressure for adequate risk management practises in any organization (ISO, 2015a). According to Chiarini (2017), there is a lack of practice on how to implement the risk-based thinking within European manufacturing SMEs.

According to Ferreira de Araújo Lima et al. (2020) SMEs are often driven to adopt different tools and methods compared to larger companies. This can be for example due to the lack of resources. Additionally, the selected tools in SMEs often focus on reacting to realized risks rather than preventing them (Ferreira de Araújo Lima et al., 2020). Grube et al. (2017) highlight the flexibility often needed in the operations of SMEs. According to ben Said et al. (2016) increasing diversity in demand has resulted in the need of HMLV production. The authors claim that HMLV requires quick product development ability, sustainable production capacity, and efficient equipment utilization (ben Said et al., 2016). According to Grube et al. (2017), it is common for manufacturing SMEs to operate in the HMLV context. Mu et al. (2009) claim that this flexibility is needed also in the risk management practises in companies conducting new product development (NPD). The authors highlight that NPD is a problem-solving process where information is created, which in turn reduces uncertainty. For this reason, it can be impossible to specify all issues beforehand, and there should be room for flexibility to handle issues as they arise (Mu et al., 2009).

Falkner and Hiebl (2015) identified different types of risks SMEs face. The identified types were interest rate risk, raw material prices risk, e-business and technological risks, supply chain risks, growth risk, and risk related to management and employees. According to Ferreira de Araújo Lima et al. (2020), financial issues are often one of the biggest concerns for SMEs. Falkner and Hiebl (2015) elaborate this issue by noting that

SMEs are often highly dependent on external finance. The risk categories identified by Falkner and Hiebl (2015) arise for example from rapid technological changes, limited number of suppliers, and knowledge loss due to losing long-term employees, which are typical for SMEs (Falkner & Hiebl, 2015).

Sifumba et al. (2017) claim that managing risks could be a strategy for success for manufacturing SMEs. According to Dvorsky et al. (2021) managing operational risk has the most significant positive effect on future business of SMEs. This effect comes from the effective utilization of corporate resources. Chowdhury et al. (2019) also highlight the optimal usage of SMEs' scarce resources for operational supply risk reduction. Falkner and Hiebl (2015) present networking and cooperative relations as a way to decrease risks SMEs face. This is supported in the SCRM literature, as the importance of collaboration is extensively highlighted (Alicke et al., 2020; Cavalcante de Souza Feitosa et al., 2021; Chen et al., 2013; Ho et al., 2015).

2.2.1 Supply chain and operational risk management

Mentzer et al. (2001) define supply chain as a set of three or more entities that are directly involved in a flow of products, services, finances, or information. With this definition, a supply chain includes at least one upstream and one downstream entity, in addition to the focal company. Ho et al. (2015, p. 5) define SCRM as "*an inter-organizational collaborative endeavour utilizing quantitative and qualitative risk management methodologies to identify, evaluate, mitigate, and monitor unexpected macro and micro level events or conditions, which might adversely impact any part of a supply chain*". So, a company and its own operations should be managed as a part of a supply chain (Ho et al., 2015; Mentzer et al., 2001). SCRM is defined by its field of application, and it is considered it as one of the main risk management streams in SMEs (Ferreira de Araújo Lima et al., 2020).

By contrast, operational risk is defined by its causes, and is considered one of the most common risk types managed in SMEs (Ferreira de Araújo Lima et al., 2020). Dvorsky et al. (2021) describe managing operational risk as the reasonable utilization of corporate resources. Ferreira de Araújo Lima et al. (2020) apply the definition of operational risk as potential human or process mistakes. As mentioned in section 2.1.1, the BCBS (2006) also includes the risks caused by external events in the operational risk definition. Jobst (2007) further appends this definition by including information systems. This cumulative definition matches the risk categorization of the PPT model presented by Javaid and Iqbal (2017). The PPT risk management application platform, directed towards SMEs, categorizes risks based on the source of the risk. The identified sources include people, processes, and technology. (Javaid & Iqbal, 2017)

According to de Oliveira et al. (2017) ruptures and interruptions in supply chains may cause substantial financial and reputational losses. Additionally, Chowdhury et al. (2019) claim that SMEs face greater operational supply risk than larger companies. According to the authors, this is due to the inability to resolve upstream variations in the supply chain within the SMEs own production processes. De Oliveira et al. (2017) state that the ISO 31000 standard can be used as a standardized method to implement SCRM.

SCRM has been widely discussed in the risk management literature (Ho et al., 2015). Cavalcante de Souza Feitosa et al. (2021) categorize Supply Chain Risks in their SCRM Maturity Model. The Supply Chain Risks are defined as:

- supply risk,
- demand risk,
- financial risk,
- production risk,
- information risk,
- transportation risk, and
- disruption risk.

Similar categorization with division to internal and external risks was proposed by Marotta (2020), who categorizes internal risks to business, manufacturing, planning and control, and mitigation and contingency risks. External risks are categorized to supply, demand, business, and environmental risks. Another categorization of risk types studied in the SCRM literature is given by Ho et al. (2015). Ho et al. (2015) categorize supply chain risks into supply, demand, financial, manufacturing, information, transportation, and macro risks. Macro risks are defined similarly to disruption risks (Ho et al., 2015). The categories defined by the forementioned sources are complementary and mostly coherent (Cavalcante de Souza Feitosa et al., 2021; Ho et al., 2015; Marotta, 2020).

Chen et al. (2013) also derive a categorization for supply chain risks from the literature. This definition combines the concepts of SCRM and operational risk, as the authors divide supply chain risks to operational and disruption risks. The operational and disruption risks are defined as before in this section and in section 2.1.1. The operational risk is additionally divided to supply, demand, and process risk. This definition can be conceptually linked to the Mentzer's (2001) definition of supply chain consisting of three entities. According to Chen et al. (2013) process risk stems internally, while supply and demand risks stem externally. The authors also claim that supply risk and demand risk increase process risk. This suggests that the internal and external risks are intertwined. Collaboration within the supply chain was presented as a method to mitigate these risks (Chen et al., 2013). Dietrich and Cudney (2011) also highlight the importance of positive supplier relationship and communication.

2.2.2 Production risk management

Production risk was presented in the previous section as a subcategory of supply chain risk (Cavalcante de Souza Feitosa et al., 2021; Ho et al., 2015; Marotta, 2020). According to AIAG (2019, p. 15), the risks manufacturers face can be categorized into technical, financial, time, and strategy risks. In a similar categorization, ODASD(SE) (2014, p. 23) divides risks to technical, programmatic, and business risks. In this division, production risks are included in the technical risks. Other technical risks include risks related to requirements, technology, engineering, integration, testing, quality, logistics, and training (ODASD(SE), 2014, p. 23). However, some of these technical risks are sometimes included in the definition of production risk. For example, according to Ho et al. (2015) production risk can include risks related to quality, lead time, yield, design, machine failures, or capacity inflexibility.

Chiarini (2017) analysed the main risk categories European manufacturing SMEs face, in accordance with the ISO 9001 standard's risk-based thinking. This produced a comprehensive list with 11 categories of specific risk sources for manufacturing SMEs. The sources are defined as:

- lack of customer requirements,
- technical design nonconformity,
- lack of risk assessment,
- nonconforming delivery from supplier,
- supplier business continuity problems,
- inadequate production planning or control,

- production of nonconforming products,
- failures in Information and Communication Technologies (ICT),
- failures in machines and equipment,
- lack of training, skills, or awareness of workers, and
- disruptions.

According to the author, majority of these categories arise from product design, supply chain processes, and production processes. The production nonconformities, human related issues, supplier nonconformities, and lack of risk assessment are the most commonly managed risks in manufacturing SMEs. (Chiarini, 2017)

Tupa et al. (2017) categorize operational risks in manufacturing organizations to risks associated with manufacturing process management, maintenance, operation methods and tools used, material, human sources, machines and manufacturing technologies, and machine environments. Table 1 presents a consolidation of risk categories presented in the forementioned literature sources. The presented risk categories are divided according to categories presented by Tupa et al. (2017), appended with the "External" category for risks that could not be assigned to the determined categories. Risks in the "External" category can be observed to arise from external sources in the environment or the supply chain.

Table 1. Consolidation of manufacturing risk categories presented in the literature.

Risk categories according to Tupa et al. (2017)	**Risk factors according to other literature sources**
Manufacturing process management	Lack of risk assessment (A) Production planning or control (A; C) Integration (E)
Maintenance	Machine failures (A; C) Quality (C; E) Lead time (C) Yield (A; C)
Operation methods and tools used	Quality (C; E) Lead time (C) Yield (A; C)
Material	Supplier nonconformities (A)

	Inventory issues (C)
Human sources	Worker training, skills, or awareness (A; C; E; F) Occupational Health and Safety (OHS) (B; C) Yield (A; C)
Machines and manufacturing technologies	Machine failures (A; C) Testing (E)
Machine environments	ICT failures (A) Integration (E)
External	Product requirements (A; E) Technology, design, or engineering (A; C; E) Supplier business continuity (A) Logistics (E) Disruptions (A) Demand variations (D)

(A: Chiarini, 2017; B: DAU, 2022a; C: Ho et al., 2015; D: Kenge & Khan, 2020; E: ODASD(SE), 2014; F: Sifumba et al., 2017)

Production of nonconforming products was considered as the most relevant risk among manufacturing SMEs (Chiarini, 2017). Nonconforming production leads to a lower production yield, which was one of the risks presented by Ho et al. (2015). However, as Chiarini (2017) states, it is actually a result of many other risks arising from human sources, lack of instructions or procedures, and poor maintenance. These sources can clearly be connected with the Javaid and Iqbal's (2017) PPT risk management model, presented in section 2.3.3.

According to Sifumba et al. (2017) risk management is considered important and viewed positively in the manufacturing industry. Notwithstanding, the authors claim that in practise there is often room for improvement. According to Chiarini (2017) manufacturing SMEs do not have enough experience of the ISO 9001 risk-based thinking approach, which leads to lacking risk assessment.

Priority and urgency management was recognized as a common challenge in production planning and control (Chiarini, 2017). Falkner and Hiebl (2015) present safety stocks and excess capacity as ways to handle capacity related risks in production. The suitability of enterprise resource management systems to flexible production was also blamed in planning and control related issues. Other ICT related risks in manufacturing include data loss, cybersecurity, and stoppages caused by system updates. Especially the loss of operative data was considered serious. (Chiarini, 2017) The relevance of ICT risks is apparent, as ICT systems are strongly present in the modern manufacturing industry (Chiarini, 2017; Tupa et al., 2017).

Failures in machines and equipment are serious risks, as they may cause production stoppages and delays in deliveries (Chiarini, 2017). Preventive maintenance is presented as an effective reducing strategy for this risk in various literature sources (AIAG, 2019, p. 110; Bailey et al., 2019; ben Said et al., 2016; Chiarini, 2017). The operation methods and tools are also presented as a source for risks in production (Tupa et al., 2017). Kenge and Khan (2020) present Jidoka, Poka-Yoke, and Kaizen as mitigation methods for these risks. Jidoka stands for the automatic detection of defects, Poka-Yoke stands for error proofing, and Kaizen for continual improvement (Kenge & Khan, 2020; Taylor, 1998). The AIAG (2019) also presents controls to avoid risks resulting from operation methods. These include technical error proofing solutions like two-handed machine operation, Poka-Yoke, and form-dependent position, as well as other solutions like visual aids, machine controls, and calibration procedures (AIAG, 2019, pp. 104, 110). According to AIAG (2019, pp. 119–120) the process should be modified to reduce the effect or occurrence of a failure. If this is not possible, the detectability should be increased.

Risks related to suppliers are considered serious among European manufacturing SMEs (Chiarini, 2017). These include supplier business continuity and material nonconformity related problems (Chiarini, 2017; Tupa et al., 2017). At worst these problems might cause production stops or even reach the customer (Chiarini, 2017). However, the mitigation options for these risks are limited, as SMEs usually have low control over their suppliers' processes (Chiarini, 2017; de Oliveira et al., 2017). According to Chiarini (2017), inspection is used to monitor this risk, but it increases product costs. Supplier selection and deeper supplier evaluation are presented as options for SMEs to mitigate supplier related risks (Chiarini, 2017; Falkner & Hiebl, 2015). According to Chowdhury et al. (2019) SMEs may reduce the incentive for opportunistic supplier behaviour by assuring shared values and common language with their key suppliers. Another risk related to material comes from the inventories (Ho et al., 2015). According to Ho et al. (2015) inventories might face risks caused by material obsolescence, disruptions, holding costs, and ownership.

Demand variations may also cause operational risks in production. These risks may cause suboptimal utilization of inventories, machines, and workforce. (Kenge & Khan, 2020) Chiarini (2017) also highlights that customer requirements are not always considered enough, which could cause complaints and unsatisfied customers. Ho et al. (2015), Chiarini (2017), and ODASD(SE) (2014) also highlight the product design related risk. However, according to Chiarini (2017), this risk is not very relevant, as it can be easily detected, and design is sometimes also controlled by the customer. According to Chiarini (2017), design risk is not necessarily considered a risk in NPD, but a natural part of the process.

As introduced in section 2.1.1, Stewart (2020) categorizes risks to known, knowable, and unknowable risks. This categorization adds a dimension of process knowledge to the uncertainty of risk, as process knowledge and risk identification activities might turn some knowable risks to known risks. Unknowable risks, however, remain challenging to address (Bailey et al., 2019; Stewart, 2020). Depending on the source, the unknowable risks are also referred to as disruptions and "Acts of God" (Chen et al., 2013; Chiarini, 2017; Stewart, 2020). Chiarini (2017) gives natural disasters like flood, fire, or earthquakes as examples of such risks. Ho et al. (2015) appends this definition by giving examples like war, terrorism, political instability, economic downturns, and external legal issues. According to Chiarini (2017) developing contingency plans is the only way to address these kinds of risks. However, Falkner and Hiebl (2015) introduce options like taking insurances and investing in weather derivatives, in addition to an emergency plan. Risk transferral by taking insurances is also presented by Javaid and Iqbal (2017). Falkner and Hiebl (2015) also remark that, based on the work of Cioccio and Michael (2007), SMEs are more likely to lack a contingency plan than larger companies.

Bailey et al. (2019) suggests building strong defences and a risk-aware culture to better prepare for unknown risks. The defences can include activities like design quality control, equipment health monitoring, output assurance, risk-informed decision making, operator skills and behaviours, and preparing the organization and equipment for emergencies (Bailey et al., 2019). Having multiple layers of defences against failures requires the occurrence of multiple concurrent failures for any significant event to occur (Bailey et al., 2019; Cook, 1998). Building a risk-aware culture helps the organization in identifying new and previously unknown risks effectively, and responding to realized risks (Bailey et al., 2019). According to Bailey et al. (2019) the culture should be based on acknowledgement, transparency, responsiveness, and respect. The Defense Acquisition University (DAU) (2022b), ODASD(SE) (2014), and PMI (2013) also highlight that the knowledge of all personnel should be utilized for identifying risks. This also connects to the underutilization of people's talents, skills, and knowledge, which in Lean thinking is considered waste (Skhmot, 2017). According to Sifumba et al. (2017) risk management training and communication is not always conducted sufficiently. This should be considered alarming, as communication of risk management activities is highlighted (Hillson, 2014, p. 299; ISO, 2018b). Sifumba et al. (2017) also claim that there might be some problems in the assignment of roles regarding risk management. This is also highlighted by the ISO (2018b).

The ISO (2018b) highlights that the variability of human nature should be considered throughout the risk management process. Risks arising from human sources, like the lack of training, skills, or awareness are presented by Chiarini (2017). According to Chiarini (2017) these risks are considered the second most relevant risk among manufacturing SMEs, after the production of nonconforming products. Chiarini (2017) adds that human sources could result in the production of nonconforming products and even customer dissatisfaction. Especially the lack of training is presented as a risk in various literature sources (Chiarini, 2017; Ho et al., 2015; ODASD(SE), 2014; Sifumba et al., 2017; Tupa et al., 2017). Ho et al. (2015) also provides examples of OHS related risk factors like accidents, absence, job dissatisfaction, strikes, insufficient breaks, and working conditions. DAU (2022a) gives more elaborated examples of factors affecting working conditions and accidents. These include the safe handling of hazardous materials, ergonomics, occupational noise, and the chemical, physical, and biological health of workers (DAU, 2022a).

According to Madsen et al. (2020) OHS related risks can be assessed through the implementation of Occupational Health and Safety Assessment Series (OHSAS) 18001 standard or the newer ISO 45001 standard (ISO, 2018a; Madsen et al., 2020). Madsen et al. (2020) reviewed the OHSAS 18001 standard, and concluded the mechanics and program theories behind it. The program theories are defined as operational, institutional, and compliance. The main mechanics confirming the program theories are identified as integration, learning, motivation, translation, and attention. The OHS performance of the organization can be improved through reinforcing these mechanics. (Madsen et al., 2020) DAU (2022a) also presents a process for identification, assessment, mitigation, and control of OHS risk. The documentation also includes tables for assessing the risk's severity and likelihood. For OHS risk mitigation, DAU (2022a) recommends to avoid or reduce risks through design. After design changes for avoidance and reduction have been assessed, warning devices and signs, trainings and procedures, and protective equipment can be used for further mitigation (DAU, 2022a). Esposito (2007) also gives examples on how the consequences and likelihood of OHS related risks can be reduced. The consequences of an unwanted event can be reduced for example by automation, engineering controls, better tools, and early warnings (Esposito, 2007). These align with the technical error proofing solutions presented by AIAG (2019, p. 104). The probability of an unwanted event can be reduced for example by reducing the amount of people performing the task, improving work practises, and by measuring and addressing trends in processes (Esposito, 2007). Likewise, these align with the visual aids and standard work instructions presented by AIAG (2019, pp. 104, 110).

Madsen et al. (2020) recommend integrating OHS risk management to existing frameworks like Plan-Do-Check-Act (PDCA), TQM, and Lean. The authors also recommend utilizing internal and external audits, certifications, and employee participation through continual improvement (Madsen et al., 2020). Participation and organizational culture are also highlighted by Bailey et al. (2019) and Brocal et al. (2019). Brocal et al. (2019) recommends the frequent discussion of risks, encouraging doubt and different opinions, discussing past behaviour, requesting safety demonstrations, and performing gap analysis between outlooks and observations.

2.2.3 Project risk management

Project risk management practises are utilized when managing risks in NPD (Mu et al., 2009; Ricondo et al., 2006; Segismundo & Miguel, 2008). According to Ferreira de Araújo Lima et al. (2020) project risk management is also considered to be one of the main risk management streams in SMEs.

Risk definition and risk management process in projects do not differ significantly from the general definitions (ISO, 2018b; PMI, 2013). Risk definitions are introduced in section 2.1.1, and risk management processes are introduced in section 2.3. Hillson (2014) argues that for project risk management, a structured process is necessary but not sufficient. In addition to a process, accurate risk concepts need to be defined, the role of people need to be understood, and the project needs to be linked to the wider organization

(Hillson, 2014, p. 281). According to PMI (2013, p. 310) and Hillson (2014, p. 283), risk management in projects should account for both opportunities and threats. PMIS Consulting (2014) agrees with this view, but advocates against combining both opportunities and threats under the definition of risk. For projects, there is a need for evaluating individual risks, but also the risk of the project as a whole (Hillson, 2014, p. 283; PMI, 2013, p. 334). According to the International Electrotechnical Commission (IEC) (2009, p. 17) in a project, risk management can be performed in different life cycle stages. When applied at the beginning of a project, risk assessment can be used to decide whether to proceed with the project or not (IEC, 2009, p. 17). Hillson (2014, pp. 299–300) recommends the use of post-project reviews to capitalize the risk management knowledge gained from the project. This contributes to the organizational learning and the risk management of future projects.

In an exemplary risk breakdown structure, Hillson (2014, p. 291) categorizes project risk to technical risk, management risk, commercial risk, and external risk. According to the author, technical risks can include factors like scope, requirements, processes, design, safety, and security. Management risk can include factors like organization, resourcing, communication, and information. Commercial risk may include factors like contracts, procurement, suppliers, and customers. External risks can include factors like legislation, economics, and geopolitical and business environments. (Hillson, 2014)

2.2.4 Contextual risk management challenges

According to Falkner and Hiebl (2015), the formality of risk management activities varies between SMEs and risk management practises evolve over time. SMEs are prone to many challenges arising from the lack of resources, financing, required flexibility in operations, growth, diverse demand, and supplier relations (ben Said et al., 2016; Chiarini, 2017; de Oliveira et al., 2017; Falkner & Hiebl, 2015; Ferreira de Araújo Lima et al., 2020; Grube et al., 2017). According to Tupa et al. (2017), the new industrial revolution, referred to as Industry 4.0, might also introduce new types of challenges for a manufacturing organization. The Industry 4.0 related challenges arise from cyber security issues, data loss and processing errors, and the new abilities and qualifications required from workers (Tupa et al., 2017). Grube et al. (2017) presented some common challenges in HMLV SMEs. Many of these challenges are related to inadequate long-term planning and unnecessary complexity. These can result for example in complex material flow, too high inventories or work-in-progress, suboptimal production layout, or ill-advised investments. However, SMEs conducting HMLV production also possess some strengths compared to larger institutions. SMEs are for example often closer to their customers, flexible in their operations, and effective in communication inside the company. (Grube et al., 2017)

Additional challenge in risk management activities in any organization arises from people. This is highlighted by AIAG (2019), Hillson (2014), and ISO (2018b). According to ISO (2018b) human behaviour and culture should be considered throughout the risk management process. Hillson (2014, p. 300) underlines that risks are not managed by tools and processes, but by people. Risk management is subjective, as it is dependent on the people conducting it, and how they see the risks (AIAG, 2019, p. 106; Hillson, 2014, p. 300). In addition to opinions, biases, perceptions, and judgements of the people conducting the risk management, it is affected by the quality of information, the limitations of techniques used, and any assumptions made (ISO, 2018b). There is also uncertainty associated with data, methods, and models used to identify and analyse risks (IEC, 2009, p. 15). According to ISO (2018b) these influences should be considered, documented, and communicated. Ben Said et al. (2016) claim that in HMLV production organizations, there is a need for knowledge management and learning loops which integrate technical systems and human actors.

Complexity poses its own challenges to risk management (Cook, 1998). In a complex system, the treatment of any current risk might always introduce completely new risks to assess (AIAG, 2019; Cook, 1998; ISO, 2018b; PMI, 2013). The treatments also tend to increase complexity instead of increasing the safety of the system (Cook, 1998). Complex systems also require multiple failures for significant effects to occur (Bailey et al., 2019; Cook, 1998). According to Cook (1998) this results in difficulty assessing causes for any realized risks. Cook (1998) claims that in a complex system, no root cause for a failure can be assigned as no single cause could result in the failure alone. Especially human judgement is falsely assigned as a cause for a failure, after the failure outcome is known (Cook, 1998). According to Munro et al. (2015, p. 415) 80 % of the time the problem is in the system, not in the people. According to IEC (2009, p. 19), in complex systems, risks need to be managed as a whole rather than individually, ignoring any potential interactions.

2.3 Risk management processes and frameworks

Falkner and Hiebl (2015) demonstrate the importance of a risk management process in SMEs. The importance of the existence of processes is also highlighted in the ISO 9001 process approach (ISO, 2015b, 2015a). This chapter introduces different risk management processes described in the literature. The introduced processes are divided to subchapters according to the literature sources. Some differences and commonalities between the processes are discussed in the literature review synthesis section.

2.3.1 ISO 31000

In the ISO 31000 standard risk management is defined on an organizational level using three entities: principles, framework, and process. The principles define the characteristics required from an organization to be able to manage risks effectively. The purpose of the framework is to assist the integration of risk management into the different functions of the organization. This chapter focuses on the defined risk management process. The ISO also remarks that these entities might exist fully or partially in an organization even before implementation of the ISO 31000 risk management standard. (ISO, 2018b)

The ISO (2018b) describes a general risk management process in their ISO 31000 standard. This process and its subprocesses are illustrated on Figure 3. The risk management process should be iterative, and it can be applied in the organization at strategic, operational, programme, or project levels. The core of the process consists of establishing the context, and the assessment and treatment of risks. This core is then supported by communication, monitoring, and reporting of risk management. Communication and monitoring should happen in all stages of risk management, whereas the frequency of reporting should be considered according to the needs of the subject in hand. (ISO, 2018b)

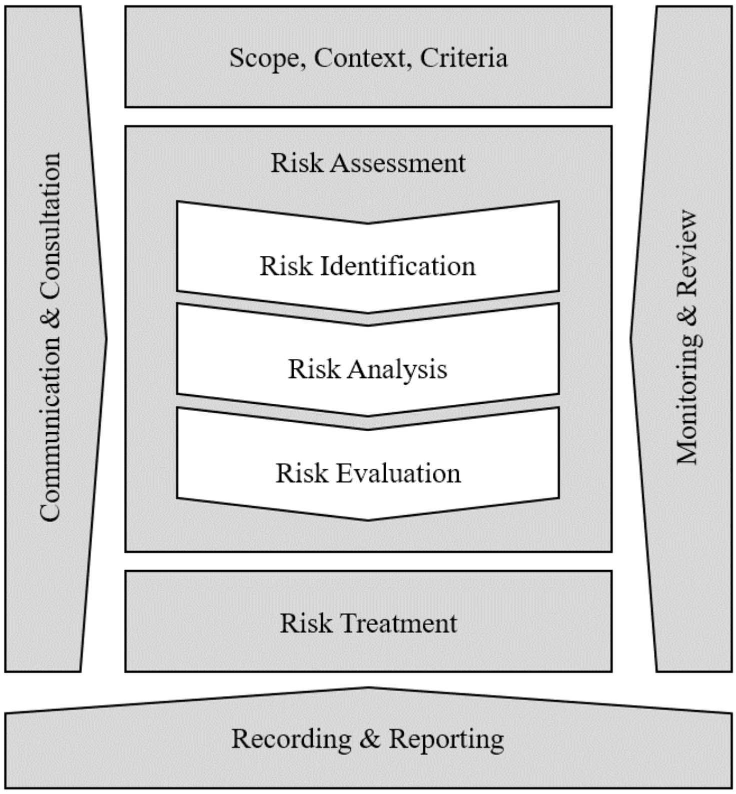

Figure 3. The ISO 31000 risk management process, adapted from ISO (2018b).

First step of the core process is to establish the scope, context, and criteria for risk management. These form the basis for the risk assessment activities and should include considerations for example for the selected risk management tools, allocated resources, and defined risk levels. The second step, risk assessment, includes the identification, analysis, and evaluation of risks. The purpose of the identification phase is to find and describe risks. The analysis phase then focuses on comprehending the sources, consequences, likelihood, and controls for the risks. Analysis can be conducted either qualitatively, quantitatively, or both. Finally, risk evaluation compares the analysed risk to the defined risk criteria to support decision making. This decision making takes place in the third step, risk treatment. The risk treatment phase is a process that consists of selecting how the risk is to be treated, planning and implementing the treatment, assessing the effectiveness of the taken actions, and either accepting or treating the residual risk. (ISO, 2018b)

From the supporting subprocesses, communication and consultation indicate a two-way flow of information between the people responsible for risk management, and appropriate internal and external stakeholders. Taking place at all stages of the risk management process, communication and consultation bring different views together and create a culture of involvement through inclusion. Monitoring and review are also conducted throughout the risk management process. The purpose of this subprocess is to assure the effectiveness of the risk management process. The purpose of the recording and reporting subprocess is to communicate the outcomes of risk management to the whole organization for informed decision-making. (ISO, 2018b)

2.3.2 PMBOK

The PMBOK by PMI (2013) includes a chapter that discusses risk management in projects. Figure 4 depicts a project risk management process derived from the PMBOK. This process includes six phases: risk management planning, risk identification, qualitative risk analysis, quantitative risk analysis, response planning, and risk control. (PMI, 2013, p. 309)

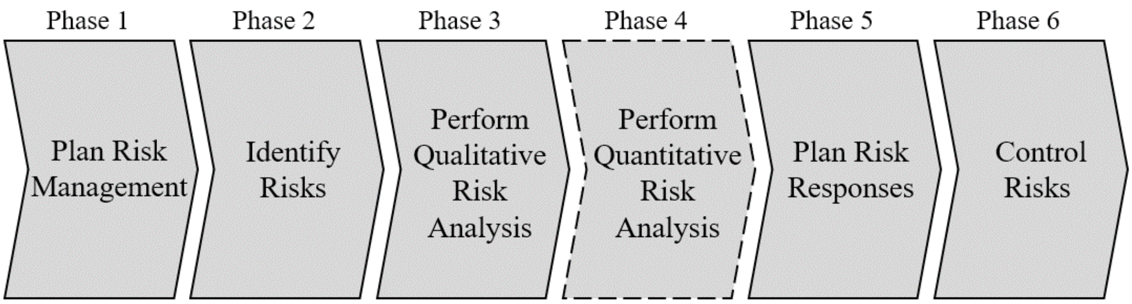

Figure 4. The project risk management process, adapted from PMBOK (PMI, 2013, p. 309).

The purpose of the planning phase is to ensure that sufficient resources are allocated to risk management. This phase also produces the basis for risk evaluation and is vital for successful risk management. (PMI, 2013, p. 314) The risk identification phase aims to recognize and document the applicable risks. This phase is recognized to be iterative as new risks may emerge during the project. (PMI, 2013, p. 321) Qualitative risk analysis is used as a cost-effective tool for prioritizing risks for risk response planning. Quantitative risk analysis can be performed after the qualitative analysis, but it is not always necessary or possible due to availability of sufficient data. Quantitative risk analysis is performed on risks with the highest priority according to the qualitative analysis. The analyses are used to assess the likelihood and consequences for the identified risks and to prioritize the risks accordingly. (PMI, 2013, pp. 328–335) The response planning phase is used to develop actions to address risks by their priority rating. (PMI, 2013, pp. 342–343) In the final phase, the risk responses are conducted, identified risks are monitored, new risks identified, and the effectiveness of risk management is evaluated. (PMI, 2013, p. 349)

2.3.3 PPT-Model

Javaid and Iqbal (2017) present their People, Process and Technology (PPT) risk management application model for information systems risk management in SMEs. Figure 5 presents the PPT risk management application model derived from the article. According to the authors, the model can be applied flexibly and scalably to different types of organizations. The model is built to consider the PPT aspects in every step of its application. (Javaid & Iqbal, 2017)

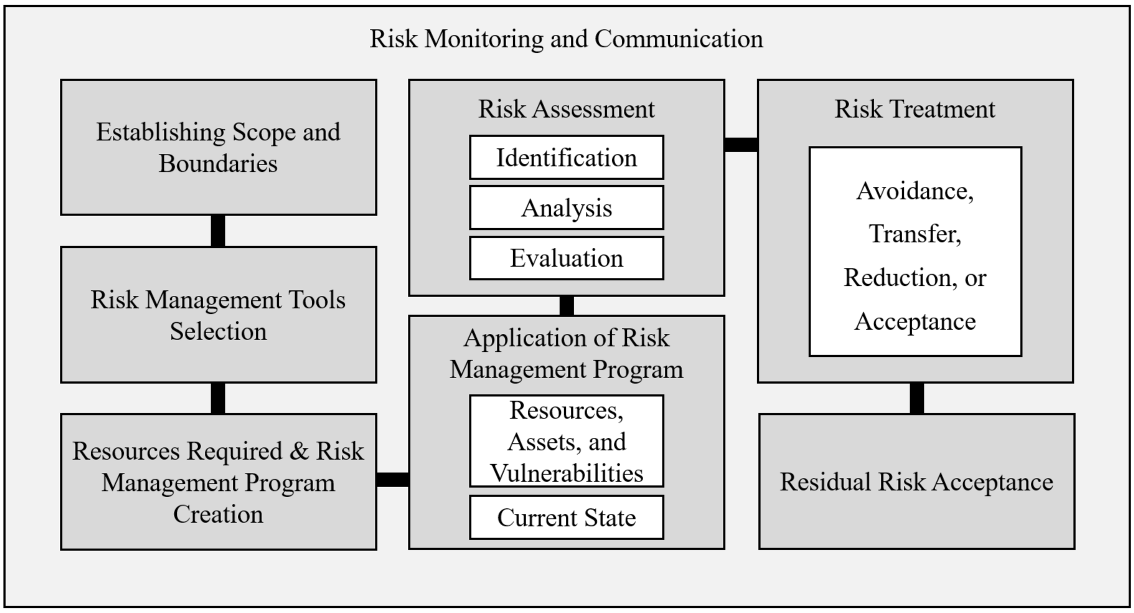

Figure 5. The PPT risk management application process, adapted from Javaid and Iqbal (2017).

The application process starts with establishing the scope of risk management. When defining the scope, the needs of people, processes, and technology should be considered. The importance of this step is highlighted, as mistakes in the scope definition would be difficult to correct later in the process. The second step is to select the applicable framework and tools for risk management. The selection includes the review, prioritization, and approval of the selected framework and tools. This step is also emphasized as the selected tools will facilitate the risk management and assessment. The third step is used to define the resource requirements, schedules, and responsibilities and to specify the finalized risk management tools used. (Javaid & Iqbal, 2017)

The application of risk management program phase includes identifying the PPT related resources, assets, and vulnerabilities. Additionally, the current state of risk management is analysed. First, the people, process, and technology resources are listed, then the criticality of these assets is evaluated. The assets are classified to critical, essential, core, and supporting based on their value to the business. The supporting assets are further categorized to relevant and irrelevant. The vulnerabilities of these assets are then identified. Finally, the current state of risk management and existing risk controls are documented. This step focuses on the problems and shortcomings in the current controls. (Javaid & Iqbal, 2017)

The risk assessment phase includes three steps: the identification, analysis, and evaluation of risks. These risks are associated with the assets identified in the previous phase. This phase utilizes the tools selected in the second phase of the application process. The risk identification step involves identifying the PPT associated risks, and assessing the likelihood and causes on qualitative and quantitative basis. The risk analysis step then connects each risk with its consequences. It is stated, that in this step risks are discussed based on likelihood and consequences without considering any controls. The risk evaluation step evaluates the existing controls, and proposes new controls considering the overall picture of risks. (Javaid & Iqbal, 2017)

The risk treatment phase develops options for treatment of each identified risk. An action plan with priority and cost estimates is produced. The authors present four treatment options: avoidance, transfer, reduction, and acceptance. The definitions for these actions are given in section 2.1.3. The treatment options to be implemented are selected considering their effectiveness and implementation costs. In the final phase, the residual risks are accepted. The purpose of this phase is to document and gain formal approval for all accepted risks. (Javaid & Iqbal, 2017)

The risk monitoring and communication phase, portrayed to cover all other phases in Figure 5, was inconsistently defined in the source article. It was both defined as a final step to be conducted after risk treatment and residual risk acceptance, and as a step covering the whole process. The latter definition was used in Figure 5. The phase involves creating a permanent mechanism for implementing, monitoring, and communicating risk management. This enables continuous evaluation of risk management practises, making required changes, and addressing budget requirements. (Javaid & Iqbal, 2017)

2.3.4 The United States Department of Defense

The ODASD(SE) (2014) has published the United States Department of Defense (DoD) Risk Management Guide for Defense Acquisition Programs. This publication includes a risk management process definition. The process consists of four steps: risk identification, analysis, mitigation, and monitoring. The DoD Defense Acquisition University (DAU) presents a similar process in their Systems Engineering Brainbook (DAU, 2022b). This process includes an additional first step of risk process planning. Since both of these publications are linked to the DoD, they are introduced here as a single DoD risk management process. The process is depicted on Figure 6.

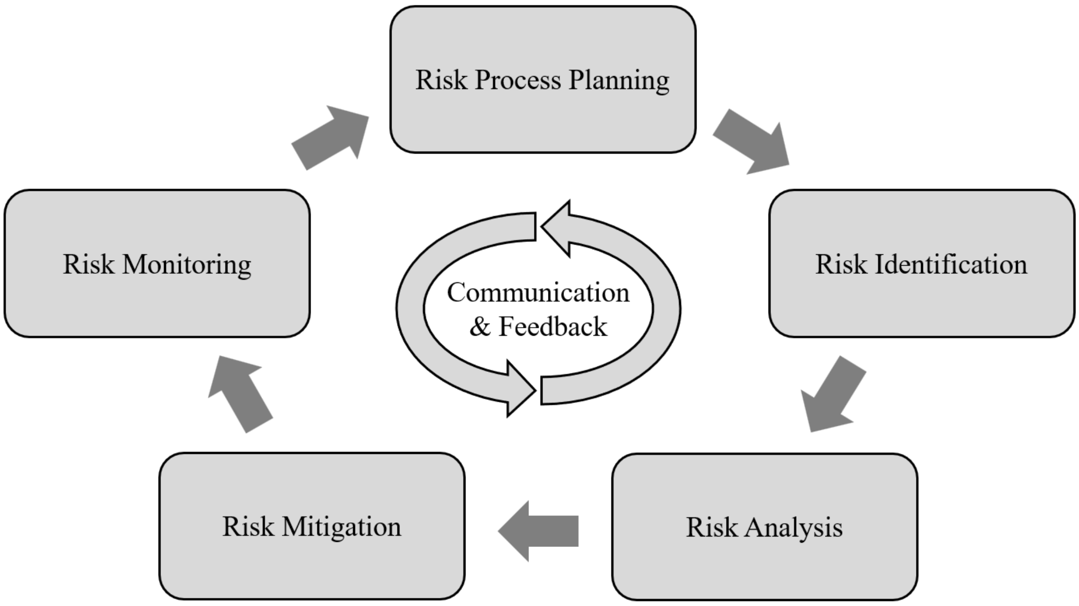

Figure 6. The DoD risk management process, adapted from DAU (2022b) and ODASD(SE) (2014, p. 19).

According to DAU (2022b) the risk process planning phase is used to define the risk management process, tools used, criteria for assessing likelihood and consequence, as well as risk training material tailored to the process. Although the ODASD(SE) (2014) does not include the planning step in the continuous process definition, it is stated that the risk management process should be defined, implemented, and documented so that it follows the defined four-step process.

The risk identification phase aims to define what can go wrong and find the root causes for these identified risks (ODASD(SE), 2014, p. 19). According to DAU (2022b) the risks are stated in this phase using at least the potential event and its consequences.

Additionally, the root cause should be included if known. According to ODASD(SE) (2014, p. 19) the identification phase is essential for the ability to understand the risk's likelihood and mitigation options in subsequent steps of the process.

The risk analysis phase investigates the risk's likelihood and the severity of its consequences (DAU, 2022b). Each identified risk is examined to refine the risk description, isolate the cause, and determine the effects (ODASD(SE), 2014). Predetermined levels of consequence and likelihood are assigned to each risk, and the risks are documenter to a central repository. The consequence and likelihood levels should be determined to suit the needs of the organization. (DAU, 2022b; ODASD(SE), 2014) This phase gives the required information for prioritizing risk mitigation efforts and resource allocation (ODASD(SE), 2014, p. 25).

In the risk mitigation phase the mitigation actions for analysed risks are decided. A decision is made whether the risk should be accepted, avoided, transferred, or controlled. (DAU, 2022b; ODASD(SE), 2014) A schedule for implementing the actions is created and metrics for tracking progress are defined (DAU, 2022b). The plan should include the specifics of the mitigation action to be performed, implementation schedule, responsibilities, impact on objectives, and required resources for each identified risk (ODASD(SE), 2014, p. 33).

In the risk monitoring phase, the decided mitigation actions are tracked, and achieved performance is measured. This provides information on how the risks are evolving continuously. (DAU, 2022b; ODASD(SE), 2014) Communication and feedback are presented as a central ongoing process that is interconnected with all process steps. However, it is not addressed as an individual process in either of the literature sources. (DAU, 2022b; ODASD(SE), 2014) Reporting practises and communication are highlighted especially as a part of the risk monitoring phase. Communication in the monitoring phase includes a regular schedule for risk reviewing to re-evaluate and track the current risks. (ODASD(SE), 2014, pp. 38–39)

2.4 Risk management tools

IEC (2009) presents various tools and techniques for risk assessment, in accordance with the ISO (2018b) 31000 standard. These include simple look-up methods, scenario analyses, function analyses, control assessments, and statistical methods (IEC, 2009, pp. 23–26). For example, simple checklist for risks is categorized as a look-up method. Tools like Root Cause Analysis (RCA) and Fault Tree Analysis (FTA) fall under the scenario analysis category. Reliability Centred Maintenance (RCM) and Failure Mode and Effects Analysis (FMEA) are categorized as function analyses. Bow tie analysis is given as an example of a controls assessment tool, and Monte Carlo simulation as a statistical method. Supporting methods include tools like Delphi technique, interviews, and brainstorming. (IEC, 2009, pp. 23–26) Ferreira de Araújo Lima et al. (2020) also provide a list of the main risk management tools categorized to qualitative and quantitative. For example, tools like FMEA, FTA, and Monte Carlo simulation, are categorized as quantitative, and tools like brainstorming, Delphi technique, and Risk Register (RR), are categorized as qualitative (Ferreira de Araújo Lima et al., 2020). Some of these tools and their usage are further elaborated in this section.

De Oliveira et al. (2017) provide a prioritization of risk management tools in an automotive supply chain. The prioritization was derived from a classification conducted by industry experts as a part of the study. The prioritization placed FMEA as the fifth highest priority, with tools like Cost/benefit analysis, business impact analysis, scenario analysis, and environmental risk assessment on higher priorities. However, as IEC (2009, p. 22) assessed the applicability of different tools to risk assessment, from these tools, only environmental risk assessment achieved as high applicability as FMEA. Strongest applicability ratings were achieved by FMEA, environmental risk assessment, Structured What-if Technique (SWIFT), and RCM (IEC, 2009, p. 22).

He et al. (2002) present some quality tools for continual improvement. The tools presented are SPC, FMEA, Quality Function Deployment (QFD), and Design of Experiments (DOE). The authors recommend the use of QFD, DOE, and FMEA in the design phase of the product or process. SPC an DOE can then be used for continual performance improvement and variance reduction in the manufacturing phase. (He et al., 2002)

Javaid and Iqbal (2017) emphasize the importance of selecting the right tools for risk management. IEC (2009, pp. 18–19) and ODASD(SE) (2014, p. 10) present criteria and considerations for selecting the right risk management tools and techniques. According to ODASD(SE) (2014, p. 10) the support for objectives, recurrence, helpfulness, accessibility, integration, and requirements of a tool should be considered before deployment. ODASD(SE) (2014, pp. 34–35) also highlights that the level of detail used should be dependent on the life cycle phase and the rationale for risk treatment actions should be documented. According to the IEC (2009) the selected tools should be appropriate to the organizational context, they should enhance the understanding of current risks and treatment options, and their usage should be traceable, verifiable, and repeatable. Javaid and Iqbal (2017) propose the potential tools to be prioritized based on organizational goals, costs, available skills, and required time frames. IEC (2009) also highlights the consideration of the objectives and needs, and the needed expertise and other resources. In addition, IEC (2009) raises the requirements arising from regulatory or contractual requirements, types of risks and magnitude of consequences, availability of information, and the potential need for updating risk assessment in the future. According to the IEC (2009, p. 15) there are often uncertainties associated with data, methods, and models used to identify and analyse risk. These uncertainties should be analysed and documented (IEC, 2009, pp. 15–17).

2.4.1 FMEA

FMEA is a risk assessment tool intended to evaluate the technical risks of a product or process, analyse their causes and effects, and recommend and document actions for preventing and detecting them (AIAG, 2019, p. 15). According to Tague (2005, p. 242) and Taylor (1998), many tools are utilized within the FMEA process. These include idea creation tools, process analysis tools, cause analysis tools, and data analysis tools. Some examples given are tables, matrices, checklists, flowcharts, brainstorming, FTA, Pareto analysis, Five Whys, Control charts, DOE, and statistical analysis (Tague, 2005, p. 242). The objective of an FMEA is to improve the design of the product or process (Carlson, 2015). According to Carlson (2015), FMEA can prevent problems, reduce costs, shorten product development times, and increase the safety and reliability of products and processes. FMEA also supports the development of specifications, maintenance and test plans, and process Control Plans (CPs) (Carlson, 2015; IEC, 2009, p. 46).

IEC (2009, p. 20) notes that different project and product life cycle stages require different tools and techniques. According to Carlson (2015) and AIAG (2019, p. 23) FMEA is conducted early in the product development process. A dynamic application of FMEA is briefly described in section 2.4.7. FMEA enables the identification of risks in the design phase, which is substantially less expensive than fixing the problems afterwards (Carlson, 2015; IEC, 2009, p. 48). Segismundo and Miguel (2008) discuss the usage of FMEA in an NPD context. The authors claim that FMEA is fundamental to the technical risk management of an NPD project. It is also stated that FMEA is one of the most widespread methods used for technical risk prioritization in NPD (Segismundo & Miguel, 2008). FMEA is also prioritized as one of the top five risk assessment tools in the automotive industry, according to a survey conducted by de Oliveira et al. (2017) to experts in automotive supply chains. This is likely amplified by the fact that the ISO/TS 16949 technical specification requires the use of FMEA for automotive suppliers (de Aguiar et al., 2015; ISO, 2009, p. 16). FMEA is one of the documents required as a part of Production Part Approval Process (PPAP) (ISO, 2009, p. 6). The purpose of PPAP is to demonstrate the manufacturing process capability and understanding of customer design and specifications (AIAG, 2008, p. 35).

The main types of FMEA are Process FMEA (PFMEA) and Design FMEA (DFMEA), which are used in the manufacturing industry (AIAG, 2019, pp. 21–22). Other FMEA types, used in other industries, include for example System FMEA, Service FMEA, and Software FMEA (IEC, 2009, p. 25). FMEA also has a derivative Failure Mode, Effects, and Criticality Analysis (FMECA), in which a criticality analysis for each failure mode is performed after the initial FMEA (Carlson, 2015; General Motors Corporation, 2008, p. 137; IEC, 2009, p. 25). According to IEC (2009, p. 47) criticality analysis can be applied when quantitative data of the failure effect probability, failure rate for the failure mode, and operating time for the system are available. Carlson (2015) also highlights the need of objective data to be able to conduct the criticality analysis. Nowadays a distinction between FMEA and FMECA is not always made (General Motors Corporation, 2008, p. 137).

According to AIAG (2019, p. 17) FMEA is strictly a qualitative tool, but Ferreira de Araújo Lima et al. (2020) claim it to be quantitative in nature. IEC (2009, p. 46) claims FMEA can provide either qualitative or quantitative information. AIAG (2019, p. 17) argues the use of the tool and the results obtained are subjective and dependent on the team performing the analysis. It is even stated that analyses performed by different teams should not be compared, even if the product or process in question is identical (AIAG, 2019, p. 106).

Carlson (2015) identified six critical success factors for implementing FMEA, which receive support from other literature sources. First, the FMEA project team needs to clearly understand the fundamentals of FMEAs (Carlson, 2015; de Aguiar et al., 2015). Secondly, as conducting FMEAs is time consuming and expensive, the need for conducting an FMEA on a specific project should be carefully considered (AIAG, 2019, p. 18; Carlson, 2015). Thirdly, the importance of planning and preparative steps is highlighted (AIAG, 2019, p. 17; Carlson, 2015). Fourthly, Carlson (2015) highlights applying the lessons learned from previous FMEAs. This knowledge accumulation is also highlighted by AIAG (2019, p. 19) in the form of Foundation FMEAs, which are discussed later in this section. Fifthly, Carlson (2015) highlights the importance of effective facilitation, which is also recognized as one of the key roles in conducting FMEA by AIAG (2019, p. 27). Roles and responsibilities also link to the sixth and final success factor, FMEA process implementation (Carlson, 2015). The FMEA process is also further discussed later in this section.

According to Carlson (2015) and AIAG (2019, p. 25) the team conducting FMEA should be cross-functional and include people from different parts of the organization. Carlson (2015) also highlights that a project team consisting of one or two people is not sufficient, although this is done in some companies. The selection of the FMEA project team links to the FMEA project planning and preparation, which is the third success factor identified by Carlson (2015). Both AIAG (2019, pp. 25–26) and Carlson (2015) give examples of who should participate the project team. AIAG (2019, pp. 26–28) however also presents a wider perception for this issue by determining the roles and responsibilities required in the project team. AIAG (2019, p. 26) highlights that these roles and responsibilities do not necessarily need to be filled by a single person each, but they can be shared. One person may also have multiple roles and responsibilities. The roles presented by AIAG (2019), each having multiple responsibilities, are the project manager, technical lead, facilitator, core team members, and experts. (AIAG, 2019, pp. 26–28)

A similar process for conducting an individual FMEA project is presented by many literature sources (AIAG, 2019, p. 29; Carlson, 2015; General Motors Corporation, 2008, pp. 8–13; IEC, 2009, p. 47). Figure 7 depicts a consolidation of these processes. The AIAG's (2019, p. 29) process includes seven steps: planning and preparation, structure analysis, function analysis, failure analysis, risk analysis, optimization, and results documentation. The IEC's (2009, p. 47) process also has seven steps: defining the scope and objectives, assembling the team, building understanding of the system or process in question, conducting a breakdown of the system into components, defining the function for each component, assessing failures for each component, and identifying design provisions to compensate failures. General Motors Corporation (2008, pp. 8–13) present a ten-step process consisting of identifying the team, defining the scope, defining the customer, identifying functions, requirements and specifications, identifying potential failure modes, identifying potential effects, identifying potential causes, identifying controls, identifying and assessing risk, and proposing recommended actions and results. Carlson's (2015) process is divided to three main steps: preparation, conducting meetings, and follow-up. Preparation includes steps like scope definition, team selection, defining rules and assumptions, and gathering information. Assumptions need to be documented to monitor changes in assumptions, which result in changes in other risk management aspects (IEC, 2009, pp. 11, 17). The meetings phase contains most of the work as it includes all the steps associated with identification and assessment of functions, failures, controls, and risks. The follow-up phase includes steps like implementing corrective actions, reviews and audits, updating test and control plans, and documenting the lessons learned. (Carlson, 2015) According to AIAG (2019, p. 121), The FMEA is only ready when all risks are either accepted or the closure of actions related to them are documented. However, PFMEAs should be reviewed periodically and always if process changes are implemented (General Motors Corporation, 2008, p. 110). Munro et al. (2015, p. 57) highlight that FMEA should be a documented and revision-controlled document, and it should be integrated to the Quality Management System (QMS).

Risks are evaluated in FMEA using severity (S), occurrence (O), and detection (D) (AIAG, 2019, p. 104; Carlson, 2015; General Motors Corporation, 2008, p. 13). These risk attributes are each given a rank on a numerical scale from 1 to 10. This is done using risk-ranking scales with descriptions for each rank. (Carlson, 2015) For example, AIAG (2019, pp. 108–109) presents severity evaluation criteria with descriptions of "*Failure may result in an acute health and/or safety risk for the manufacturing or assembly worker*" for rank 10 and "*No discernible effect*" for rank 1. These ranks are then used for prioritization of treatment actions for individual risks (Carlson, 2015).

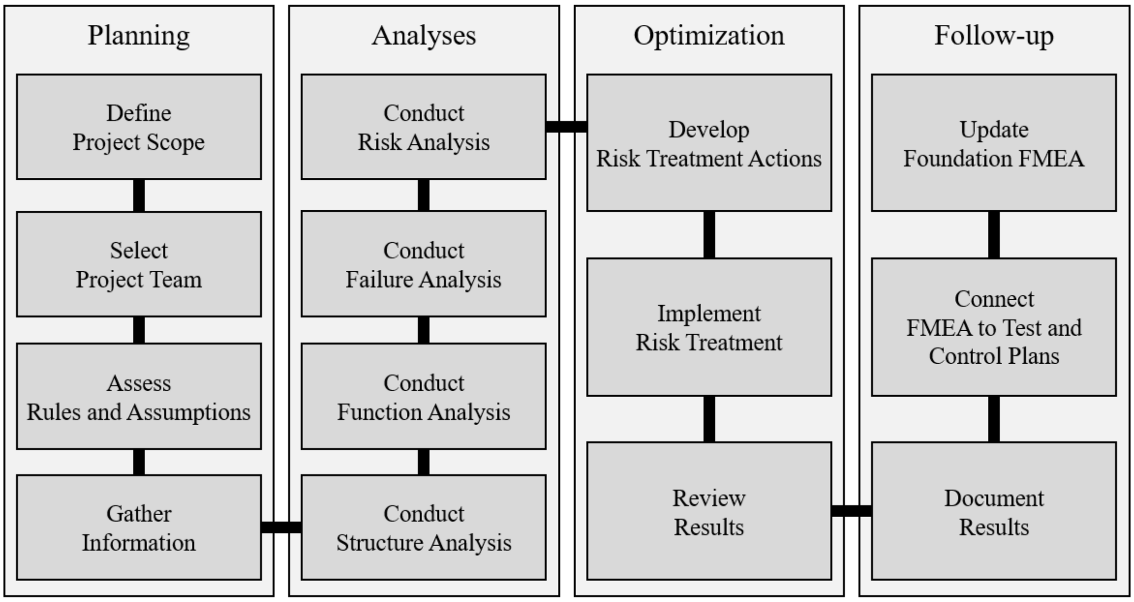

Figure 7. The process for conducting an individual FMEA, consolidated from AIAG (2019, p. 29), Carlson (2015), General Motors Corporation (2008, pp. 8–13), and IEC (2009, p. 47).

According to PMI (2013, p. 321), risks should be stated in a way that supports the ability to compare their relative effects. For example, Risk Priority Number (RPN) can be used for this purpose (General Motors Corporation, 2008, pp. 57, 135). The RPN represents the arithmetic product of the S, O, and D ratings, and is thus calculated as follows (1):

$$RPN_i = S_i \times O_i \times D_i, \qquad (1)$$

where RPN_i refers to the RPN of a risk i, S_i is the severity rating assigned to the risk i, O_i is the occurrence rating assigned to the risk i, and D_i is the detection rating assigned to the risk i (Carlson, 2015; Segismundo & Miguel, 2008). The use of RPN for risk treatment prioritization is widely criticized (AIAG, 2019, p. 114; Carlson, 2015; de Aguiar et al., 2015; General Motors Corporation, 2008, p. 103; Segismundo & Miguel, 2008; Tague, 2005, p. 242). General Motors Corporation (2008, p. 135) and AIAG (2019, p. 114) highlight that, for different risks, different combinations of S, O, and D could result in the same RPN, although the risks should be prioritized unequally. Also, as previously stated, Stewart (2020) advices against the perception of risk as a multiplication of consequence and probability. However, AIAG (2019, p. 115) states that it is not necessarily the risk but the need for actions that is ranked. According to IEC (2009, p. 47), RPN is used in quality assurance applications because low detectability of a failure mode raises its priority.

Some alternatives for RPN are also proposed (AIAG, 2019, p. 114; Carlson, 2015; General Motors Corporation, 2008, p. 136). Carlson (2015) suggests not relying on RPN alone but using both severity and RPN for prioritizing risk treatment. Leaving D out of the equation and prioritizing actions only using S and O is also proposed by AIAG (2019, p. 114) and General Motors Corporation (2008, p. 136). Carlson (2015) proposes the criticality analysis performed in FMECA as an alternative for RPN. However, as stated before, criticality analysis requires objective qualitative data (Carlson, 2015; IEC, 2009, p. 47). In their 2019 FMEA Handbook, AIAG (2019, pp. 114, 218) presents Action Priority (AP) chart to replace RPN. The chart defines an action priority of high, medium, or low for each combination of S, O, and D. The chart is built to put most emphasis on S, then on O, and least emphasis on D. (AIAG, 2019, p. 114) Segismundo and Miguel (2008) recommend the implementation of a monthly PDCA cycle to periodically monitor the high and medium risks, until all risks can be considered acceptable and the FMEA project can be ended.

According to PMI (2013, p. 329) bias can be reduced by establishing definitions for risk severity and occurrence. When assigning levels to particular risks, the justifications and assumptions should also be documented (PMI, 2013, p. 330). Charts for assessing S, O, D, AP, or equivalent properties, are presented by several authors (AIAG, 2019, pp. 185–203; Carlson, 2015; DAU, 2022b; General Motors Corporation, 2008, pp. 88, 93, 100; Hillson, 2014, pp. 290, 294; Munro et al., 2015, pp. 63–65; ODASD(SE), 2014, p. 30; PMI, 2013, pp. 318, 331). Munro et al. (2015, p. 67) advice against copying the S, O, and D rating scales from another company or industry. Customized scales that are only used within the organization are also discouraged (Munro et al., 2015, p. 67). According to AIAG (2019, p. 107) the scales should be agreed between customer and supplier organizations. The ODASD(SE) (2014, p. 26) also advocates seeking for a common risk consequence analysis framework to enhance collaboration between entities.

Carlson (2015) presents an overall process within an organization for conducting FMEA projects. It is stated that management support, well-defined roles and responsibilities, management review of high-risk issues, quality audits, execution of recommended actions, and feedback loop implementation are key elements for a successful FMEA process. On a broad level the process follows the PDCA cycle, as the phases are denoted as Planning, Doing, Reviewing, and Implementing. The Planning phase includes the formation of both strategic and resource plans for conducting FMEAs. The Doing phase consists of creating Foundation FMEAs and program specific FMEAs. (Carlson, 2015) Test and field data may be utilized in forming the Foundation FMEAs, and they are used as a basis for forming the specific FMEAs. The Foundation FMEAs ensure knowledge accumulation and are also sometimes referred to as generic, baseline, template, core, master, and best practise FMEAs. (AIAG, 2019, p. 19; Carlson, 2015; Segismundo & Miguel, 2008) The knowledge accumulation is supported by ben Said et al. (2016) as a requirement for a modern HMLV production organization. The Reviewing phase includes the execution of management reviews, quality audits, and supplier FMEAs. In the Implementing phase, risk treatment actions are executed, and the FMEA project is linked to other processes. All of these phases are preferably managed through integrated software. (Carlson, 2015)

According to AIAG (2019, p. 101), failures presented in DFMEA are failures of product function, and the corresponding failures in PFMEA are failures in manufacturing the designed function. IEC (2009, p. 46) notes that changes can usually be more easily implemented in the design phase. However, risks that are not mitigated in the DFMEA phase should be transferred to PFMEA (General Motors Corporation, 2008, p. 17). According to Carlson (2015), DFMEAs provide important input to PFMEAs, and PFMEAs to process CPs (Carlson, 2015). In addition to DFMEA, process flow diagrams and historical data provide valuable input for conducting PFMEA (Carlson, 2015; General Motors Corporation, 2008, pp. 70, 73). The use of process flow diagram for risk categorization is supported by PMI (2013, p. 332). Figure 8 depicts the linkage and information flow between DFMEA, PFMEA, and CP. CP is discussed further in section 2.4.2. According to Carlson (2015), FMEA can be implemented as a standalone process, but linkages enhance effectiveness.

Johnson and Khan (2003) present some PFMEA-related challenges in the automotive industry in the United Kingdom. The authors report that the cause, effect, and failure mode are sometimes confused between each other. This is linked to the observation that proper training for the people conducting FMEA is not always provided (Johnson & Khan, 2003). AIAG (2019, p. 17) highlights that FMEA is subjective, and relies on the knowledge and skills of the team performing it. Javaid and Iqbal (2017) also point out the role of human judgement in risk quantification. Subjectivity was identified as a common concern also among automotive suppliers (Johnson & Khan, 2003). However, Johnson and Khan (2003) claim that the subjective rating of S, O, and D is sufficient for practical purposes of risk prioritization. Various literature sources state, that conducting FMEAs is time consuming (AIAG, 2019, p. 18; Carlson, 2015; IEC, 2009, p. 48). According to IEC (2009, p. 48), it can also be difficult and tedious in complex systems. Johnson and Khan (2003) also report that the progress or effectiveness of PFMEAs are rarely measured. In addition, FMEA is only capable of considering single-point failures (AIAG, 2019, p. 17; IEC, 2009, p. 48). This is in direct conflict with the claims made by Bailey et al. (2019) and Cook (1998), which state that failures in complex systems are intrinsically multi-point failures.

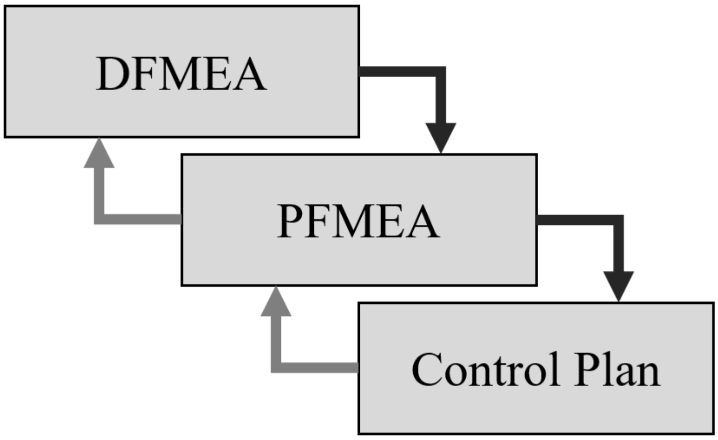

Figure 8. The linkage and information flow between DFMEA, PFMEA, and CP, adapted from General Motors Corporation (2008, p. 111).

2.4.2 Control Plan

AIAG (2008, p. 4) defines CP as a written system description for controlling parts and processes. It provides a structured approach for implementing control methods to manufacture quality products according to customer requirements (AIAG, 2008, p. 43). AIAG (2008, pp. 44–55) provides an exemplary CP sheet with explanations for each section and guidance for use. AIAG (2008, p. 45) recognizes the main benefits of implementing CPs as reduced waste and improved quality, increased customer satisfaction, and effective communication of changes in Special Characteristics (SCs), controls, and measurements.

Process flow diagram, SCs, and FMEAs are utilized in the creation of the CP (AIAG, 2008, p. 45; Carlson, 2015; General Motors Corporation, 2008, p. 111). Taylor (1998) even expresses CP as an end result of conducting an FMEA. SCs are the product or process characteristics arising from regulations, safety considerations, or knowledge of the product or process (AIAG, 2008, p. 104). General Motors Corporation (2008, p. 112) highlights that the current controls defined in PFMEA have to be consistent with controls defined in the CP. The ISO/TS 16949 technical specification requires the use of CP for automotive suppliers (ISO, 2009, p. 16). According to the ISO/TS 16949, CP has to take into account DFMEA and PFMEA outputs, list all manufacturing process controls, include methods for monitoring controls for SCs, initiate reaction plans when process becomes unstable or statistically incapable, and be reviewed and updated when changes are made to product, process, measurement, logistics, suppliers, or FMEA (ISO, 2009, pp. 22–23).

Separate CPs with different purposes are created in Prototype, Pre-launch, and Production phases (AIAG, 2008, pp. 4–5; ISO, 2009, p. 36). The Prototype CP includes descriptions for the dimensional measurements and material and functional tests performed in the prototype phase (AIAG, 2008, p. 20; ISO, 2009, p. 36). Its purpose is to assure that the product meets specifications, establish preliminary process parameters, ensure attention for SCs, and communicate any concerns and deviations (AIAG, 2008, p. 20). According to ISO (2009, p. 17), all SCs should be included in the CP. The Pre-launch CP includes descriptions for the dimensional measurements and material and functional tests performed in the pre-launch phase (AIAG, 2008, p. 20; ISO, 2009, p. 36). The process flow chart and PFMEA assist the creation of the Pre-launch CP (AIAG, 2008, p. 26). Its purpose is to contain potential non-conformities during initial production runs, and, compared to the Prototype CP, it includes more frequent inspection, more checkpoints, more robust statistical evaluations, enhanced audits, and the identification of error-proofing devices (AIAG, 2008, p. 27). The Production CP includes the final written system description for controlling parts and processes, and it should be continuously updated to reflect any changes in controls (AIAG, 2008, p. 35).

2.4.3 FTA

FTA (Fault Tree Analysis) aims to analyse a single potential failure to identify all possible causes for it (General Motors Corporation, 2008, p. 137). The causal factors and their logical relationships for a specific undesired event are identified and presented in the form of a tree diagram (IEC, 2009, p. 49). According to General Motors Corporation (2008, p. 137), FTA considers both interdependent and independent causes, and normally also probabilities for failures. This enables system reliability calculation, but of course requires knowledge of the probabilities of the causal events (General Motors Corporation, 2008, p. 137; IEC, 2009, p. 49). FTA can be used for selecting between design options, evaluating how failures can occur in the operating phase, or diagrammatically analysing an occurred failure (IEC, 2009, p. 49). FTA is a useful tool for displaying causal relationships, analysing top event probability, or inspecting individual pathways to the top event using minimal cut sets (IEC, 2009, p. 50).

The tree diagram is formed starting from the top event, and moving down identifying causes, and causes for these causes, until further analysis becomes unproductive (IEC, 2009, p. 50). The diagram consists of different kinds of gates and events, which are differentiated with symbols (IEC, 2009, p. 49; Tague, 2005, p. 244). IEC (2009, p. 49) introduces two types of gates: "And" gates and "Or" gates. Tague (2005, p. 244) introduces additional gates with priority, exclusivity, inhibiting, and voting properties. The events are differentiated to express the current state of analysis. These can include events that can be analysed into more causes, independent events i.e., root causes, events that will not be analysed further, conditional events, or events that are analysed in a separate diagram. (IEC, 2009, p. 49; Tague, 2005, p. 244)

According to Taylor (1998), FMEA and FTA are closely related, and FTA is a variation of FMEA. FMEA employs a bottom-up analysis strategy, while FTA employs a top-down strategy. FMEA starts with the potential failures, and moves towards the consequences, while FTA starts with the consequence, and moves towards the causes. According to Taylor (1998) FMEA is more detailed, but FTA can be performed earlier in the design process. According to AIAG (2019, p. 17), FTA can be used in quantitative and multi-point failure analysis, while FMEA is only used in quantitative and single-point failure analysis. This is also apparent by the logical relationship expressions and probabilities noted by IEC (2009, p. 49), as well as the cause interdependencies noted by General Motors Corporation (2008, p. 137). As with FMEA, FTA is recommended to be applied as early as possible to save resources (Tague, 2005, p. 246). Tague (2005, p. 247) notes that FMEA can be applied to an entire system or process, while FTA is only capable of analysing one failure at a time. It is also stated that FTA could be used within the FMEA process for understanding causes for the failure modes (Tague, 2005, p. 247). This has been employed before, as for example Peeters et al. (2018) successfully applied FTA and FMEA in a recursive manner.

IEC (2009, p. 51) lists some of the limitations of FTA. According to IEC (2009, p. 51) there may be some uncertainties in the probabilities of base events, which results in high uncertainty on the probability of the top event. However, it is stated that a high degree of confidence can be achieved in a well understood system. Another challenge regarding the execution of FTA is that all important pathways to the top event are not necessarily identified, which could affect the results of the analysis. Challenges related to the characteristics of the tool are that the tool only considers binary states of failure and does not account for time interdependencies. It is also stated that human errors, domino effects, and conditional failures are not easily included in the analysis. (IEC, 2009, p. 51)

2.4.4 RCA

American Society for Quality (ASQ) (n.d.) defines root cause as a factor, which caused a nonconformance. Root Cause Analysis (RCA) is defined as a method for identifying, solving, and preventing reoccurrence of the correct and accurate cause for a problem (ASQ, n.d.). Karjalainen (2023) highlights RCA as a general concept containing all problem-solving methods that are based on analysis. RCA can be conducted reactively or proactively (Karjalainen, 2023). Cook (1998) criticizes the concept of finding a root cause. According to Cook (1998), multiple faults are required for a failure to occur in a complex system, which makes root cause attribution fundamentally wrong.

IEC (2009, p. 45) presents six examples of RCA tools: Five Whys, FMEA, FTA, Fishbone diagrams, Pareto analysis, and Root Cause Mapping. Karjalainen (2023) appends this list with Bayesian deduction, Change analysis, Current Reality Tree, Barrier Analysis, and Rapid Problem Resolution. This section briefly introduces the overlapping tools mentioned by Karjalainen (2023) and IEC (2009), which are not introduced in other sections. These include the Five Whys, Fishbone diagrams, and Pareto analysis. FMEA and FTA are introduced separately in sections 2.4.1 and 2.4.3, respectively.

ODASD(SE) (2014, p. 19) recommends repeating the question “why?” to find the underlying root cause for a particular risk. This is also known as the Five Whys technique (ASQ, n.d.). Tague (2005, p. 513) refers to the Five Whys technique as a why-why diagram. However, compiling a diagram is not necessary (Tague, 2005, p. 513). Carlson (2015) recommends the use of Five Whys for cause determination in FMEA. Tague (2005, p. 247) also remarks that the “why?” question is repeated in each level of a Fault Tree to reveal underlying causes. Same applies to the forming of a Fishbone diagram

(IEC, 2009, p. 57). Tague (2005, p. 516) notes the similarity of a why-why diagram and FTA, and states that FTA is more structured and generates more information about the relationships between causes and effects.

The Fishbone diagram identifies many possible causes for an unwanted event and sorts them into categories (Tague, 2005, p. 247). According to IEC (2009, p. 57) a Fishbone diagram is structured by first creating branches for the cause categories, and then creating sub-branches for the causes and sub-causes for a specific effect. The generic cause categories are methods, machines, manpower, materials, measurement, and environment (Tague, 2005, pp. 247–248). Man, machine, Material, and Environment are commonly referred to as Ishikawa's 4M, and also utilized in the FMEA failure analysis (AIAG, 2019, pp. 97–98). The causes and sub-causes are found by answering the question "why?" repeatedly, like in the Five Whys technique (Tague, 2005, pp. 248, 513). Fishbone diagram is sometimes also called cause-and-effect diagram, Ishikawa diagram, or feather diagram (AIAG, 2008, p. 89; Tague, 2005, p. 247).

IEC (2009, p. 56) presents the use of Fishbone diagram as a way to organize information gathered in a Cause-and-effect analysis. Tague (2005, p. 247) remarks that it can be utilized to structure a brainstorming session. PMI (2013, p. 325) recommends Fishbone diagram for risk identification. In the failure analysis step of conducting an FMEA, AIAG (2019, p. 93) recommends failure cause identification with a Fishbone diagram. AIAG (2008, p. 90) presents the use of Fishbone diagram as a part of a continual improvement loop. According to IEC (IEC, 2009, p. 57), the Fishbone diagram is represented similarly to an FTA, but it cannot be quantified for head event probability calculation, as the causes in Fishbone are not necessarily failures with known probabilities but merely possible contributory factors.

According to Tague (2005, p. 15) Pareto analysis, in addition to Fishbone diagram, is one of the seven basic quality control tools. Pareto analysis is presented in the form of a bar graph, where the bars represent the frequency or cost associated with it and are arranged in an order according to frequencies. This helps in finding and focusing on the most significant problems. (Tague, 2005, p. 376) Focusing on the most frequent problems in the Pareto analysis context is also presented with the 80/20 rule, which states that 80 % of problems are caused by 20 % of causes (Karjalainen, 2023). Tague (2005, pp. 379–380) presents two derivatives for the Pareto chart: weighted Pareto chart and comparative

Pareto charts. These can be used when the bar categories have different relative importance or two or more datasets need to be compared (Tague, 2005, pp. 379–380). Munro et al. (2015, p. 64) recommends utilizing Pareto analysis on graphing FMEA failure modes according to their individual RPN scores.

2.4.5 Maintenance practises

According to Munro et al. (2015, p. 355) maintenance can be used to minimize defects and downtime by removing deficiencies from machines. According to Chiarini (2017), the risk of machine and equipment failures can be significantly reduced using preventive maintenance. Stoppages caused by equipment breakdowns or nonconformities, material waste, scrap, and need for rework can be reduced by maintenance (Munro et al., 2015, p. 355). Maintenance is also one of the layers of defences against unknown risks presented by Bailey et al. (2019). Ben Said et al. (2016) claim that maintenance is a key contributor for improving and sustaining production capacity. Maintenance can be conducted correctively, preventively, or predictively (ben Said et al., 2016; Mili et al., 2009). Munro et al (2015, p. 425) define preventive maintenance as breakdown prevention through scheduled maintenance activities. According to ISO (2009, p. 23), preventive maintenance should at minimum include planned activities, packaging and preservation of equipment, ensuring replacement part availability, and documented objectives. In addition, all tool changes and repairs should be recorded (ISO, 2009, p. 30). Tague (2005, p. 32) presents preventive maintenance as a Lean tool, which reduces waste caused by non-functioning equipment.

Munro et al. (2015, p. 424) present a Lean tool called Total Productive Maintenance (TPM). According to the authors, it has evolved from breakdown maintenance, corrective maintenance, preventive maintenance, and productive maintenance practices (Munro et al., 2015, p. 425). TPM is considered more than a preventive maintenance practise, as it includes also management of people, processes, systems, and environment (Munro et al., 2015, pp. 242–425). TPM integrates engineering, operations, and maintenance, as a portion of the maintenance activities is conducted by the operational workers as a part of their ongoing process activities. This includes for example simple calibrations, inspections, cleaning, lubrication, and adjustments. (Munro et al., 2015, p. 425) In addition to the maintenance performed by operators and scheduled maintenance performed by maintenance personnel, for example RCA, equipment design, and training in TPM are recommended practises (Munro et al., 2015, p. 428). Conducting TPM requires data about the uptime, utilization, and efficiency of equipment (Munro et al., 2015, p. 426). TPM introduces metrics like Overall Equipment Efficiency (OEE), Mean Time to Repair (MTTR), and Mean Time Between Failures (MTBF). OEE represents the efficiency in which the equipment is used, MTTR represents average time it takes to perform a repair, and MTBF represents the average time between successive failures. MTBF thus reflects the overall reliability of equipment and effectiveness of maintenance. (Munro et al., 2015, pp. 426–427)

IEC (2009, p. 66) presents a maintenance practise called RCM. The goal of RCM is to efficiently and effectively achieve the required safety, availability, and economy of equipment operation (IEC, 2009, p. 66). According to IEC (2009, p. 67) it follows the basic steps of FMECA, but requires a maintenance specific approach in the analysis phase. Carlson (2015) introduces a specific type of FMEA, Maintenance FMEA, created to support RCM projects. RCM involves collection of equipment failure and maintenance related data. The required equipment functions and failures, as well as failure occurrence and effects need to be defined. The occurrence should be estimated assuming no maintenance was done. (IEC, 2009, p. 67)

AIAG (2019, p. 110) remarks preventive maintenance as a way to reduce failure occurrence in FMEA. Ben Said et al. (2016) utilized FMECA for maintenance management in a HMLV production facility. The IEC (2009, p. 46) and Carlson (2015) also suggest the use of either FMEA or FMECA for maintenance planning. According to ben Said et al. (2016) preventive maintenance cannot always be performed effectively using historical data, as the equipment failure behaviour could be evolving. Especially in HMLV production, maintenance procedures need to be dynamically updated (ben Said et al., 2016).

2.4.6 Verification and validation practises

Process validation is used to confirm that the process output fulfils requirements consistently (Sidor & Lewus, 2007). Taylor (1998) highlights that validation requires documented evidence of the constant fulfilment of requirements. ISO (2009, pp. 30–31) specifies requirements for monitoring and measurement of products and manufacturing processes for automotive suppliers. This includes verification of capability and fulfilment of requirements when changes are introduced (ISO, 2009, pp. 14, 30–31). Changes should also be reflected and approved on the applicable controlled documents (ISO, 2009, p. 6).

FMEA and FTA are introduced as tools to facilitate the overall validation effort (Taylor, 1998). For example, Sidor and Lewus (2007) utilized FMEA for risk-based process validation. These are then supported by different statistical tools like control charts, capability studies, and DOE (Taylor, 1998).

Control charts can be used to detect changes in the process (Munro et al., 2015, p. 113; Taylor, 1998). Typically control charts are used to display changes in the averages and ranges of process samples (Taylor, 1998). Control limits are defined from historical data, and comparing the current data to these limits reveals whether the process variation is consistent or unpredictable (Munro et al., 2015, p. 113). The correct application and utilization of control charts is referred to as SPC (Munro et al., 2015, p. 374). Control charts are also used in capability studies for demonstration of stability (Taylor, 1998).

According to Taylor (1998) capability studies are done to determine whether a process is stable and capable of producing wanted results. Munro et al. (2015, p. 241) link capability studies to FMEA, CP, and SPC. FMEA is used to identify the characteristics to be included in CP and SPC, which can then be used to verify capability (Munro et al., 2015, p. 241). A preliminary process capability study is conducted as a part of product and process validation to assess their readiness for production (AIAG, 2008, p. 34).

DOE is a structured and organized method to study relationships between factors and process outputs (Munro et al., 2015, p. 316). DOE involves changing the values of process input variables and measuring the effect on one or more output variables (Taylor, 1998). The input variables are adjusted systematically according to a predetermined design matrix (AIAG, 2008, p. 91). He et al. (2002) describe DOE as an active tool for problem solving and continual improvement that can be used for product and process optimization. According to AIAG (2008, p. 91) early application of DOE can improve process yields as well as reduce variability, development time, and overall costs.

Good measurements are needed when studying variation. The measurement system can be verified using Measurement System Analysis (MSA). (Taylor, 1998) MSA compares the variation caused by the measurement system to the total process variation, and ensures the measurement variation is low enough to reflect the true process variation (Tague, 2005, p. 448). According to AIAG (2008, p. 34) MSA should be performed as a part of process validation. MSA is also sometimes referred to as Gage Repeatability and Reproducibility (GRR) study (Tague, 2005, p. 448).

AIAG (2019, p. 110) presents the validation of error proofing and process verification methods as ways to lower risk occurrence rating in FMEA. According to Taylor (1998) mistake proofing is to be used when the failures are caused by human errors. AIAG (2008, pp. 92–93) separates mistake proofing and error proofing, stating that mistake proofing prevents occurred errors reaching the customer, and error proofing prevents the error from happening in the first place. Taylor (1998) combines both of these definitions under mistake proofing.

The use of external and internal audits is proposed widely in the risk management context (AIAG, 2019; Carlson, 2015; ISO, 2009; Madsen et al., 2020; PMI, 2013). Audits are used to independently assess projects or processes against established plans and goals (Munro et al., 2015, p. 104). AIAG (2019, p. 106) recommends auditing the current risk prevention and detection controls to verify their implementation and effectiveness. Carlson (2015) proposes the use of quality audits as a part of an effective overall process for conducting FMEAs. ISO (2009, pp. 29–30) requires internal auditing of the QMS, manufacturing processes, and products. Madsen et al. (2020) highlight the importance of auditing in directing attention to OHS related risks. PMI (2013, p. 351) proposes conducting risk audits as a way to examine and document the effectiveness of risk responses and risk management process.

The Office of the Secretary of Defense Manufacturing Technology Program (OSDMTP) (2022) presents guidelines for assessing Manufacturing Readiness Level (MRL). According to OSDMTP (2022, p. 1) MRL criteria have been designed to identify and manage risks in manufacturing. DAU (2022b) also recommends the use of MRL for manufacturing risk reduction. MRL is assessed to define the current maturity level, identify any shortfalls, and enable manufacturing risk and maturity management (OSDMTP, 2022, p. 1). In addition to the current level, a target level, and a plan for achieving it should be defined (Morgan, 2007). MRL includes ten levels with criteria for nine dimensions, or "threads" (OSDMTP, 2022, pp. 5–13). Each of the dimensions are divided to sub-dimensions, or "sub-threads", which each contain their own criteria (OSDMTP, 2022, pp. 12–13). These form a matrix for assessing the current maturity level. The levels range from identification of basic manufacturing implications to the demonstration of full-rate production and Lean practises (OSDMTP, 2022, p. 6). The evaluated dimensions are technology and industrial base, design, cost and funding, materials, process capability and control, quality, manufacturing workforce, facilities, and manufacturing management (OSDMTP, 2022, pp. 12–13). MRL is designed to complement Technology Readiness Level (TRL) (Morgan, 2007). TRL includes nine levels with criteria for assessing the performance maturity of a technology (Morgan, 2007; OSDMTP, 2022, p. 15). MRL and TRL are used together to assess the capability and risks for an emerging technology (Dietrich & Cudney, 2011). MRL is needed, because TRL does not assess the manufacturability of a technology (Morgan, 2007).

2.4.7 Dynamic tools and continual improvement

According to the ODASD(SE) (2014, p. 39) a management indicator system should be implemented for effective risk monitoring. For this purpose, Hwang (2011, p. 125) proposes the use of Key Risk Indicators (KRIs). Tupa et al. (2017) also perceive KRI as an important management indicator. According to Hwang (2011, p. 132) KRIs are often used in conjunction with other risk identification and management tools. KRIs can be selected among the most significant risks recognized using other tools (Hwang, 2011, p. 135). Other sources for KRIs may be for example benchmarking, company strategy, and regulations (Hwang, 2011, p. 137). Tupa et al. (2017) propose a KRI system with division to strategic and operational KRIs. KRIs can also be divided according to priority or responsibility (Tupa et al., 2017). Hwang (2011, p. 134) highlights that KRIs can be used to monitor operations continually, unlike other tools that are often conducted periodically.

Munro et al. (2015, pp. 418–420) present a dynamic version for a Control Plan. The dynamic CP combines for example PFMEA, CP, and maintenance plan, among other metadata and supporting information for manufacturing. The primary focus is however in CP and PFMEA. One important aspect of a dynamic CP is that the manufacturing operators have the right and responsibility to keep it up to date. Changes made are then communicated to all necessary parties (Munro et al., 2015, pp. 418–420).

Mili et al. (2008) propose a dynamic approach that enables using FMECA as an operational knowledge management tool. This approach integrates the FMECA in an industrial information system in real time. Human intervention is partially replaced with computerized and automated tasks that connect the FMECA with real time production events, which are considered as risks that can reoccur. (Mili et al., 2008) In another article, Mili et al. (2009) demonstrate the utilization of dynamic FMECA approach for managing maintenance activities. In this approach, FMECA is connected to a computerized maintenance management system. The approach utilizes data gathered from the computerized maintenance management system, updates FMECA accordingly, and causes possible updates in maintenance planning. A case study conducted as a part of the article showed this approach helped to identify new frequent risks that had not previously been discovered because of their low impact. (Mili et al., 2009)

Improvement and process approach are highlighted as quality management principles in the ISO 9001 (ISO, 2015a). Continual improvement is also one of the main principles of risk management according to the ISO 31000 (ISO, 2018b, pp. 3–4). Munro et al. (2015, p. 421) describe continual improvement as a process of open-mindedly looking for ways to make things better, cheaper, or faster. The use of FMEA for continual improvement is presented by AIAG (2019, pp. 119, 121) and He et al. (2002). AIAG (2008, p. 90) also presents Fishbone as a part of a continual improvement loop. In addition to FMEA, He et al. (2002) recommend using SPC, QFD, and DOE for continual improvement. Madsen et al. (2020) emphasize the role of continual improvement for employee involvement. Kaizen as a continual improvement method is discussed by Munro et al. (2015, p. 37) as well as Kenge and Khan (2020). According to Munro et al. (2015, pp. 366, 370) Kaizen achieves continual improvement through small incremental changes and enhances employee involvement.

2.4.8 Other tools

PMI (2013, p. 312) recommends the use of analytical techniques, meetings, and expert judgement for risk management planning. Expert judgement was also proposed as a technique for risk identification, analysis, and response planning (PMI, 2013, p. 312). IEC (2009, p. 12) proposes analysis of historical data and use of check-lists for risk identification. These are also proposed by PMI (2013, p. 312), in addition to brainstorming and interviews. Brainstorming and interviews are also recommended by ODASD(SE) (2014, p. 20).

IEC (2009, p. 23) presents brainstorming and interviews, Delphi technique, and SWIFT as supporting methods for risk assessment. Munro et al. (2015, p. 145) describe brainstorming as a process where ideas are generated by a group or a single individual. According to Munro et al. (2015, p. 145), brainstorming consists of a creative phase, where ideas are created, and aa evaluation phase, where the usefulness and applicability of these ideas is evaluated. According to IEC (2009, p. 27) brainstorming may be used in conjunction with another tool, or as a stand-alone technique. Interviews should be conducted as structured or semi-structured (IEC, 2009, p. 28). Compared to brainstorming, interviews might enable involvement of more stakeholders, but may also lack the imagination achieved in brainstorming (IEC, 2009, p. 29). The Delphi technique aims to form a consensus within a group of experts, and it is sometimes used as a synonym for brainstorming. The technique consists of iterative questionnaires independently conducted to experts, until consensus is reached. (IEC, 2009, pp. 29–30). SWIFT is a structured brainstorming technique that is guided by asking "What if…?" questions (Card et al., 2012). The technique is used to investigate how deviations could affect normal operations (IEC, 2009, p. 38). According to Card et al. (2012) SWIFT is flexible and easy to learn. It can also be used as a stand-alone tool or, being faster to implement than FMEA, as a preliminary approach for evaluating the need for FMEA (Card et al., 2012).

PMI (2013, p. 312) proposes the use of a risk probability and impact matrix for qualitative risk analysis. It is also proposed by Hillson (2014, pp. 293–294) and ODASD(SE) (2014, p. 29) with varying naming conventions. In the probability and impact matrix each risk is rated according to its probability (likelihood) and impact (consequence), which places the risk on a matrix scale that categorizes the risk to low, moderate, or high priority (PMI, 2013, p. 331). ODASD(SE) (2014, pp. 25–27) presents tables with criteria for rating likelihood and consequences for each risk. Hillson (2014, p. 294) and PMI (2013, p. 331) also utilize probability and impact matrix with a mirrored extension for assessing opportunities.

According to Hillson (2014, p. 292), after identifying risks, they should all be documented into a RR. This practise is also supported by DAU (2022b), ODASD(SE) (2014, p. 32), and PMI (2013, p. 327). According to Hillson (2014, p. 293), the RR should include data about the project the risk is related to, and about the risk, its assessment, and responses. These include for example risk identifier, source, description, probability and impact ratings, related risks, treatment actions, responsibility, schedule, and status (Hillson, 2014, p. 293). Similar, yet less exhaustive lists for register data are given by ODASD(SE) (2014, p. 32) and PMI (2013, p. 327). Risk statuses should be kept up to date and new risks added when identified (ODASD(SE), 2014, p. 32).

2.5 Risk management capability

Risk management capability is sometimes required externally (ISO, 2018b, p. 6). For example, the ISO/TS 16949 technical specification sets some risk management requirements for automotive suppliers (ISO, 2009, p. 16). This is also amplified by the customer focus highlighted in the ISO 9001 (ISO, 2015a). Johnson and Khan (2003) report that in some organizations the external requirements may even be the main driver when considering the use of some risk management tools, instead of the internal benefits. Hillson (1997) however reports increasing awareness in the benefits of risk management among organizations.

2.5.1 Risk management capability assessment

Risk management maturity models are useful for assessing the stage of risk management in an organization (Wieczorek-Kosmala, 2014). According to Hillson (1997) risk management maturity models could be used to assist in implementing risk management or improving current practises. Bititci et al. (2015) highlight the role of maturity models in organizational learning. According to Bititci et al. (2015) the application of maturity models enables discussion among management, increases criticality towards current practises, and encourages more regular review of practises.

Pergler (2012) presents four maturity levels for risk management. The first level is referred to as the initial transparency stage. At this level, risk management is driven by compliance with basic standards and regulations, and regular surprises are reduced. The second level is referred to as systematic risk reduction. This level includes professionalized management and avoidance of unexpected events with big potential consequences. The third level is referred to as risk-return management. Here, risk management is driven by competitive pressure, requirements for the return on equity of improvements are in place, and trade-offs are considered in decision making. The fourth level is referred to as risk as competitive advantage. Here, risk management activities are driven by the top management’s focus on risk-adjusted performance and strong risk culture. (Pergler, 2012) According to Pergler (2012), companies with exposure to natural resources or important technical or research and development risks, are usually completely or partially on the third level of maturity.

Hillson (1997) also proposes a maturity model with four levels: naive, novice, normalized, and natural. The author provides a matrix for assessing the maturity level based on four dimensions: Culture (A1), Process (A2), Experience (A3), and Application (A4). A summarized table for the Hillson's (1997) maturity model is presented in Appendix 2. In the naive level, the organization does not recognize the need for risk management and does not learn from the past to better prepare for future risks. An organization in the novice level is aware of the benefits of risk management, and is experimenting with risk management through a few individuals. However, a novice organization has not effectively implemented risk management processes, although some formal methods may be utilized as a part of a few major projects. In the normalized level, the benefits of risk management are recognized at all levels of the organization, but not always fully achieved. Risk management is implemented in almost all projects and risk processes are formalized and widespread. In the natural level, similarly to the Pergler's (2012) fourth maturity level, a risk-aware culture is highlighted. Risk management has a proactive approach, both opportunities and threats are managed through risk processes, and risk information is actively used for process improvement and competitive advantage. (Hillson, 1997)

Cavalcante de Souza Feitosa et al. (2021) propose a SCRM maturity model, which classifies a company's ability to manage supply chain risk based on three main dimensions: Organizational Support (B1), Risk Management Process (B2), and Managed Risks (B3). The maturity model includes four levels, similarly to the models proposed by Pergler (2012) and Hillson (1997). A summarized table for the maturity model proposed by Cavalcante de Souza Feitosa et al. (2021) is presented in Appendix 3. Criteria for each level and dimension are provided for assessment of current level. The B1 dimension criteria include properties like communication, culture, and continual improvement, and are derived from ISO (2018b) and ISO (2015a). The B2 dimension criteria include different risk management process stages and tools derived from ISO (2018b) and IEC (2009). The B3 dimension criteria include different SCRM risk categories derived from literature, presented in section 2.2.1.

2.5.2 Risk management capability improvement

According to Hillson (1997) the implementation of risk management needs to be treated as a project with objectives, success criteria, planning, resourcing, and monitoring. According to ODASD(SE) (2014, p. 5) risk management needs to be planned early, resourced well, and implemented aggressively. The ISO 31000 standard also requires the planning of risk management activities including timing, resourcing, and responsibilities (ISO, 2018b, p. 7). Additionally, the ISO 31000 requires continual improvement of risk management practises (ISO, 2018b, p. 8).

Hillson (1997) highlights the use of risk management maturity models for implementing risk management or improving current practises. After assessing the current maturity level, action plans for achieving the next level can be made (Hillson, 1997). According to Wieczorek-Kosmala (2014), higher risk management maturity level leads to higher benefits. However, Pergler (2012) claims there is no robust statistical evidence that more mature risk management would lead into better performance. Instead, Pergler (2012) believes the observed better performance merely reflects the underlying differences between organizations. Nevertheless, the benefits of reaching the next maturity level need to be compared to the costs involved (Hillson, 1997). Pergler (2012) believes there is going to be an increasing shift towards higher maturities in risk management in the future.

The maturity levels provide logical progression for improving practises (Wieczorek-Kosmala, 2014). In addition to the maturity level descriptions Hillson (1997) also provides some exemplary actions for progressing from level to another. For example, to progress from the novice level to the normalized level, an organization could strengthen corporate backing for risk management, provide formal risk training, utilize external expertise, allocate more resources for risk management, promotion, and process formalization. External expertise could be used to support internal skills, introduce outside influence, and possibly to extend risk management practises to new parts of the organization. Resource allocation can be done through training, recruitment or risk management tools and activities. Promotion may include celebrating any successful risk management events, demonstrating the benefits of risk management through selected projects, and implementing regular risk reporting. Process formalization includes the definition of risk management scope, objectives, procedures, and tools. (Hillson, 1997)

2.6 Literature review synthesis

This section provides a short synthesis on the main outcomes of the literature review. The purpose of this section is to provide a short overview of the topics included, as well as guide towards the empirical section of this thesis. An answer to the RQ1 is given in the end of this section.

The section 2.1 gives an introduction to risks, risk management, and risk treatment. The definition of risk is not always consistent among literature sources. As stated by PMIS Consulting (2014), risk management is nowadays often combined to a single process with opportunity management. This is in line with the risk management frameworks proposed by ISO (2018b) and PMI (2013). However, as PMIS Consulting (2014) remarks, including opportunity in the definition of risk is confusing and may lead to misunderstandings. Consequently, this study utilizes the risk definition by ODASD(SE) (2014). In this definition, risks are seen as uncertain negative effects on organization's objectives. Figure 2 in section 2.1.3 depicts the different risk treatment options widely referred to in the literature (Javaid & Iqbal, 2017; ODASD(SE), 2014, pp. 35–36; PMI, 2013, pp. 344–345). These are the reduction, avoidance, transferral, and acceptance of risk.

Risk management contexts are assessed in the section 2.2. Current state of the literature, risk categorizations, as well as some tools and challenges related to SMEs, NPD, HMLV, supply chains, production, and projects are discussed. Risk management is dependent on the context in which it is applied. The ISO (2018b, p. 6) and IEC (2009, p. 9) highlight establishing the internal and external context when planning risk management. This is also backed by Javaid and Iqbal (2017) and PMI (2013, p. 311). Some of the factors affecting the context are introduced in section 2.2. IEC (2009, pp. 9–10) additionally recommends establishing the context of the risk management process and defining risk criteria. Figure 9 compiles some of the supply chain risk categories presented in section 2.2.1. Production risk categories and risk factors related to them are presented on Table 1 in section 2.2.2, which utilized the categorization made by Tupa et al. (2017), appended with the external category. Some of these categories match with the Ishikawa's 4M risk categories utilized in FMEA (AIAG, 2019, pp. 97–98). Especially when appended with the extended 4M categories presented by Tague (2005, pp. 247–248). Comparison between these categories is presented on Table 2. The table also includes the operational risk categorization derived from BCBS (2006), Jobst (2007), and Javaid and Iqbal (2017).

Table 2. Comparison of production and operational risk categorizations according to literature sources.

Tupa et al. (2017)	**AIAG (2019, pp. 97–98)**	**Tague (2005, pp. 247–248)**	**BCBS (2006); Jobst (2007); Javaid and Iqbal (2017)**
Human sources	Man	Manpower	People
Manufacturing process management			
Machines and manufacturing technologies	Machine	Machines	Technology
Maintenance			
Material	Material	Materials	External
Machine environments	Environment	Environment	
Operation methods and tools used	N/A	Methods	Processes
N/A	N/A	Measurement	N/A

The section 2.3 introduces different risk management processes presented in the literature. The sources considered are ISO (2018b), PMI (2013), Javaid and Iqbal (2017), DAU (2022b), and ODASD(SE) (2014). Figure 10 presents a process synthesized from these sources. Figures for individual processes can be found in their respective sections. The synthesized process consists of four main phases: plan, assess, mitigate, and control. These phases are then supplemented with selected features from different processes. The communicate phase is presented as a central ongoing phase, similarly to DAU (2022b), ISO (2018b), Javaid and Iqbal (2017), and ODASD(SE) (2014, p. 19). Differing from other risk management planning phases, the DAU (2022b) risk management process included the creation of training material regarding risk management. Some challenges in the risk management process implementation are presented in the literature. Ferreira de Araújo Lima et al. (2020) note that many companies focus on the initial risk management process phases, applying the process only partially. Falkner and Hiebl

(2015) remark that in SMEs risk management evolves over time, and the formality of risk management practises vary between companies.

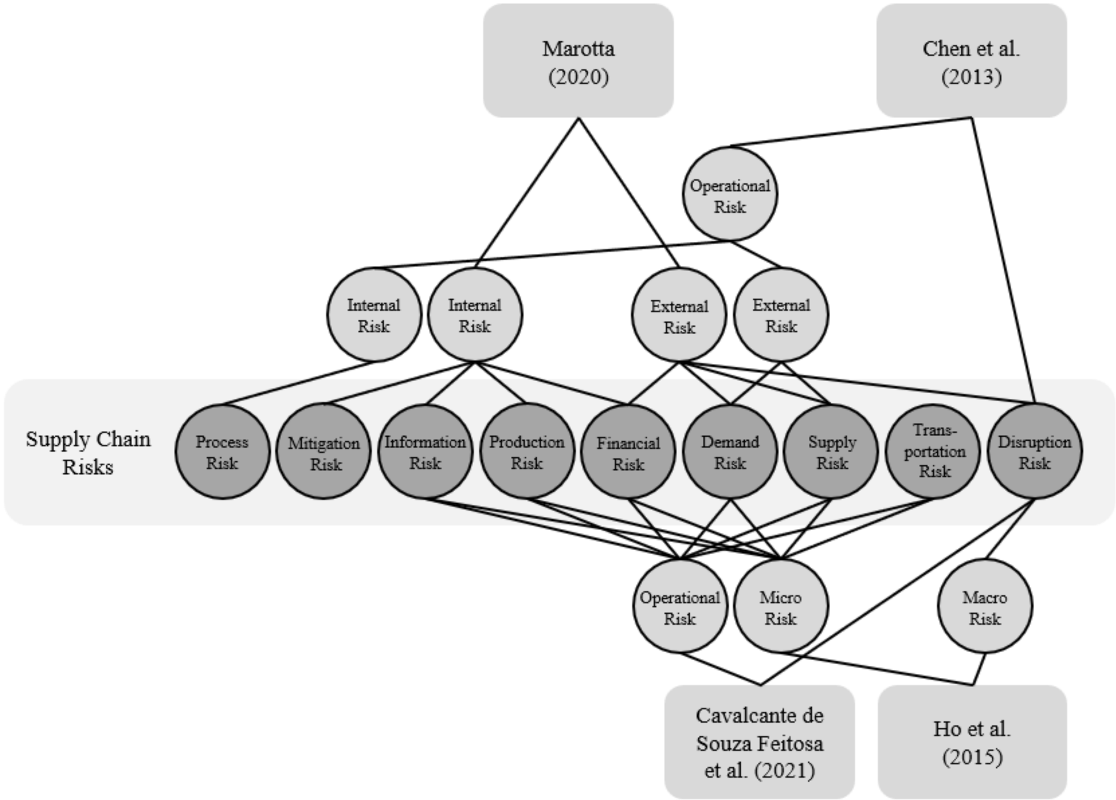

Figure 9. Supply chain risk categorization according to Cavalcante de Souza Feitosa et al. (2021), Chen et al. (2013), Ho et al. (2015), and Marotta (2020).

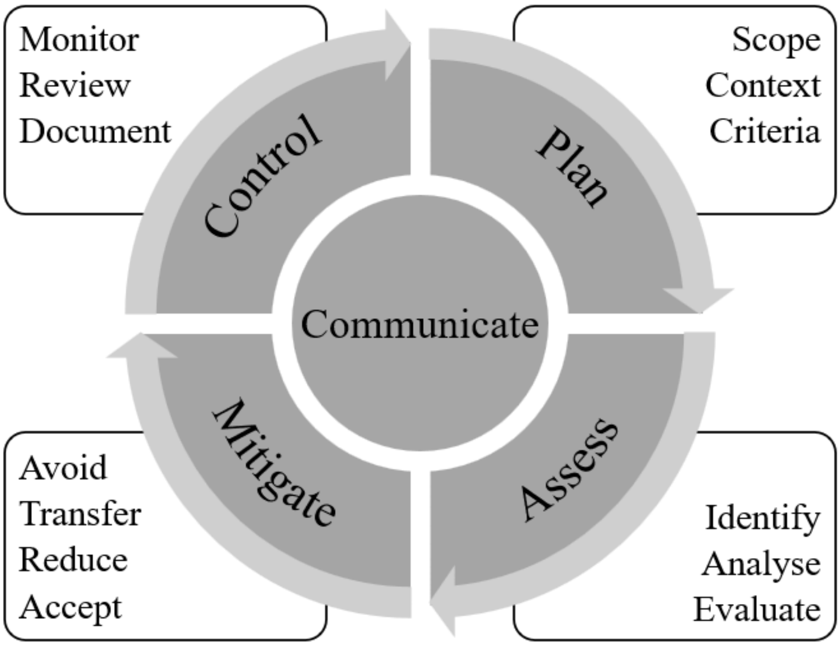

Figure 10. Synthesized risk management process, adapted from DAU (2022b), ISO (2018b), Javaid and Iqbal (2017), ODASD(SE) (2014, p. 19), and PMI (2013, p. 309).

Various risk management tools are assessed in the section 2.4. FMEA and the closely linked CP are discussed in sections 2.4.1 and 2.4.2, respectively. Supporting tools like FTA, RCA, as well as maintenance and verification and validation practises are discussed in sections 2.4.3-2.4.6. The discussed maintenance practises include preventive maintenance, RCM, TPM, and FMECA. A dynamic FMECA was also utilized for managing maintenance activities by Mili et al. (2009). The discussed verification and validation practises include FMEA, FTA, statistical tools, audits, and MRL assessment. Section 2.4.7 discussed risk monitoring using KRIs, the dynamic utilization of FMEA and CP, as well as some tools presented for continual improvement. Finally, the section 2.4.8 introduced other tools like brainstorming, SWIFT, Delphi technique, probability and impact matrix, and RR. Also, the utilization of supplier collaboration and organizational culture for risk reduction are presented in sections 2.2.1 and 2.2.2, respectively.

According to AIAG (2019, pp. 15–16) FMEA can be utilized for managing technical risks. In turn, ODASD(SE) (2014, pp. 22–23) includes production risks and many other operational risk categories under the technical risk definition. As pointed out by AIAG (2019, p. 17) and IEC (2009, p. 48) FMEA is only capable to consider single-point failures. For multi-point failures, AIAG (2019, p. 17) recommends using FTA. The combined usage of FMEA and FTA is presented by Peeters et al. (2018) and Tague (2005, p. 247). He et al. (2002) analyse the relationship between SPC, FMEA, and DOE. According to the authors, DOE and SPC can be used to identify significant factors for failures to be included in the FMEA. DOE can also be used to improve and optimize the product or process identified in the FMEA. FMEA and DOE can be used to identify the quality characteristics to be controlled in SPC. SPC may also be used to identify factors to be optimized using DOE. (He et al., 2002)

The section 2.5 considers the assessment and improvement of risk management capability. As stated, requirements for risk management capability may arise from external sources (ISO, 2009, p. 16, 2018b, p. 6; Johnson & Khan, 2003). However, internal benefits are also recognized (Hillson, 1997). Three frameworks for assessing risk management capability were introduced. This includes two general risk management maturity models, proposed by Pergler (2012) and Hillson (1997), and one maturity model specialized in SCRM, proposed by Cavalcante de Souza Feitosa et al. (2021). According to Wieczorek-Kosmala (2014) it is typical for risk management maturity models to include four or five levels and a matrix for assessing the current level. The maturity levels also function as targets for improving risk management practises (Wieczorek-Kosmala, 2014).

The RQ1 seeks to find out how operational risks should be managed in a HMLV production SME according to literature. The question can be broken down to the context of where and what risks need to be managed and to the “how?” question. The required or pursued capability is dependent on the context (Pergler, 2012; PMI, 2013, pp. 310–311). Pergler (2012) for example generalizes common capabilities according to the industry and size of an organization, placing smaller companies and retail industry lower in the scale, and bigger organizations and energy industry higher in the scale. On the Pergler’s scale, a typical manufacturing SME could then be located in the lower-middle area of the scale. The costs and benefits of higher capability need to be considered (Hillson, 1997). To answer the “how?” question, one needs to consider the managed risks, organizational support, and processes and tools in place, in contrast to the context, forming the risk management capability (Cavalcante de Souza Feitosa et al., 2021).

The managed risks define the comprehensiveness of risk management. Table 2 and Figure 9 consolidate some of the categorizations related to operational and production risks. These should be taken into account when determining the comprehensiveness. Organizational support effectively enables risk management through culture and investment. (Cavalcante de Souza Feitosa et al., 2021) The existence of a risk management process is considered important, regardless of the context (Falkner & Hiebl, 2015; ISO, 2015b, 2015a). The formality and included steps are also important factors when assessing the risk management capability (Cavalcante de Souza Feitosa et al., 2021; Hillson, 1997, p. 39). A synthesized risk management process is depicted in Figure 10.

The selected risk management tools need to be applicable for the context, and they need to be used correctly to gain their full benefits. The context applicability can be evaluated by comparing the context presented in section 2.2 to the risk management tool selection criteria presented in section 2.4. The evolving risk management practises and need for flexibility present in SMEs might pose a potential need for updating the tools and practises in the future. The types of risks and magnitude of consequences present in manufacturing encourage some investment in risk management practises, but the incentives are higher in some other industries (Pergler, 2012). The availability of capital in SMEs for investing in risk management could limit the usage of some heavier tools and information systems. Information systems and data collection also links to integration and the availability of information, which could limit the use of some quantitative risk management tools. While not completely separate from the context, the correct usage of the selected tools relates strongly to how risk management should be conducted. Regulatory and contractual commitments might guide both selection and usage of risk management tools. Similarly, the people resources and expertise available might limit the complexity and comprehensiveness of the selected tools, as well as their full utilization. In addition, the tools should be used in a way that is traceable, verifiable, and repeatable (IEC, 2009, p. 18).

The risk treatment actions, depicted in Figure 2 in section 2.1.3, are reduction, avoidance, transferral, and acceptance of risk. These should all be considered when treating risks, and can be prioritized to first try to avoid, transfer, or accept the risk, and then to reduce it by reducing its consequences or likelihood, or increasing its detectability (AIAG, 2019, pp. 119–120; ODASD(SE), 2014, p. 36).

3 EMPIRICAL STUDY

This section presents the results obtained from the empirical study. The used research methods and materials are introduced in section 3.1 and the case company in question is introduced in section 3.2. The current state, which also answers the RQ2, is presented in section 3.5. Justifications for the current state are provided in sections 3.3 and 3.4, covering the PFMEA project and observations related to different risk management maturity model dimensions.

The risk management maturity models, introduced in section 2.5.1, are utilized in assessing the current state of operational risk management in the company. The selected maturity models were proposed by Hillson (1997) and Cavalcante de Souza Feitosa et al. (2021). Summarized tables for the maturity level descriptions for each dimension in both maturity models are provided in Appendices 2 and 3, respectively. Full descriptions for the maturity levels may be obtained from the original sources. In the original article, Hillson (1997) also provides some guidance on how to proceed from a maturity level to the next one. In the context of this study, proposals for advancing risk management maturity are given in section 4.1.

As two different maturity models are utilized and each dimension is evaluated separately, the observations related to different dimensions have been grouped to sections 3.4.1-3.4.4. These include the observations related to the risk management process, tools, managed risks, and organizational support in the company. The relationship between the grouped observations and the maturity model dimensions is elaborated in Figure 11, in section 3.4. The respective maturity model dimensions are also identified in the beginning of each section, and the current state with assessed maturity levels is summarized in Table 3 in section 3.5.

3.1 Research methods and materials

The overall research process with inputs and outputs and their relation to the RQs are presented as a flowchart in Figure 1, in section 1.2. As can be observed from the figure, the empirical study utilizes interviews, observations, and documentary data to obtain the current state of risk management in the case company.

The researcher was part of a team conducting the observed PFMEA project. Participatory observing was utilized to gather the observations. In participatory observing, the researcher acts actively with the informants of the study (Tuomi & Sarajärvi, 2018, Chapter 3.2). The documentary data included documents of previously conducted and ongoing FMEA projects and MRL and TRL assessments, maintenance plans, audit records, and process descriptions. Eisenhardt (1989) recommends simultaneously conducted but separated data collection and analysis, so this was utilized in this study.

After collecting and analysing the participative observations and documentary data, gaps in the accumulated knowledge were identified. Three semi-structured interviews were then conducted aiming to fill these gaps. The identified gaps were utilized to form the questions for the interviews. The interviews were conducted in Finnish but the questions were provided beforehand to the interviewees in English. This was done to achieve more thorough and exact answers. Sending the questions to the interviewees beforehand is also a recommended practise by Tuomi and Sarajärvi (2018, Chapter 3.1). The interview questions are presented in Appendix 1. Semi-structured interviews are conducted by going through predetermined themes and questions related to them that are central to the subject in hand (Tuomi & Sarajärvi, 2018, Chapter 3.1). Each of the three interviews was concentrated on a different theme related to the empirical study. The questions are divided according to the following themes:

1. Risk management tools and managed risks,
2. Utilization of MRL and TRL assessments, and
3. Risk management process and organizational support.

For each theme, a different interviewee was selected according to their areas of expertise and responsibility to best answer the provided questions. The interviewees were the Director of Product Data and Test Systems (DPDTS), the Vice President of Platforms Industrialization (VPPI), and the Quality Manager (QM) in the case company. The DPDTS was interviewed on the first theme, the VPPI was interviewed on the second theme, and the QM was interviewed on the third theme. The responsibilities of the DPDTS include the supervision and management of the FMEA, CP, and testing processes, the VPPI oversees the technology industrialization projects, utilizing the MRL and TRL frameworks, and the QM is responsible for the operations' and management system's compliance on the adopted standards. The QM also facilitates the company level

RR. The interviews were recorded to enable more thorough analysis and to save time by supporting note taking.

3.2 Case company introduction

The case company is introduced in this section based on the ISO 31000 organizational context. The ISO 31000 divides the organizational context into internal and external contexts, and gives examples of factors affecting them. (ISO, 2018b, p. 6) Some of these factors are listed in section 2.2.

Starting with the internal context; the case company is a technology-driven SME with small production operations, which have characteristics of HMLV and NPD. The company employs around 100 people, with about 10 people working in production, including the researcher. The business is focused in technology development and licensing. For this reason, the manufacturing activities are focused on technology prototyping and verification. The people working in production are highly skilled specialists in their areas of responsibility. The company is capable to both design and manufacture the prototypes inhouse. In addition, flexibility in operations is required due to HMLV characteristics. Being an SME, the company has limited resources in regards of people and capital. However, the company possesses strong intellectual property and considerable amount of expertise and knowledge. As pointed out by Grube et al. (2017) communication is often efficient within SMEs. This is also true in the case company, so information flow can be considered effective due to the size of the company. The limited capital poses some limitations on the adopted information systems. Vast amount of data is created in the production processes, for example regarding the used process parameters, testing, and process capability. However, the usage of this data is somewhat limited due to the lack of proper database structure. Highly varying process parameters also limit some of the conclusions that can be made from analysing the data for example regarding the process capability or failure mode occurrence. The organization has a certified management system, which fulfils the ISO 9001 quality- and the ISO 14001 environmental management system standards. The ISO 9001 includes requirements regarding quality management, process approach, risk-based thinking, and continual improvement (ISO, 2015a). The ISO 9001 does not however require the use of formal risk management methods or a documented process, although a plan for addressing risks is required (ISO, 2015a, p. 22). Customer focus is also highlighted in the ISO 9001 standard (ISO, 2015a, p. 3). While arising from the internally adopted standard, the customer focus also highlights the external context.

Continuing with the external context; the case company is based in Oulu, Finland, and it operates in the B2B sector with companies in various industries. In Finland, the social, economic, environmental, and political environments can be considered relatively stable, and do not pose any significant disruption risks. Of course, the recent global crises have caused instability in supply chains and political environment globally. The local legal and regulatory requirements guide especially the management of risks related to OHS and environment. The objectives of the organization are mainly driven by trends in technology adoption and the needs of selected external stakeholders. Cooperating with companies in different industries and countries pose some challenges and expectations for risk management. This is also related to the forementioned ISO 9001 customer focus. Some industries, like the automotive industry, set certain requirements for risk management capability and even for the tools to be used in risk management. These requirements can be enforced for example through PPAP. Varying geographical locations of cooperative organizations might pose some risks related to supply chains. In addition, it is noted that SMEs usually have low control over their suppliers' processes (Chiarini, 2017; de Oliveira et al., 2017). However, according to the DPDTS, supply risks are not highly relevant in the business.

3.3 PFMEA project

The operational risk management practises in the case company were first studied through participatory observation of a PFMEA project and examining documentary data related to previously conducted FMEAs. The interview of the DPDTS was then utilized to support the findings and fill any gaps in the observations. The subsections follow the consolidated individual FMEA process presented in Figure 7, in section 2.4.1. This section describes the entire PFMEA project, but when a narrower focus is required, a single risk and actions related to it are inspected.

The case company utilizes the FMEA template, scales, and steps presented by AIAG (2019, pp. 29, 163, 195–197, 200–203). FMEA has not yet been implemented extensively in the case company, and only a few FMEA projects have been conducted. Due to the HMLV nature of the business and frequent prototyping, it is not feasible to conduct time consuming FMEAs for every project. The overall process for conducting FMEAs or the roles and responsibilities related to FMEA have not yet been formalized. However, according to the DPDTS, both of these should be formalized in the future. FMEAs are conducted for significant customer projects, and PFMEA is utilized internally as a tool for process improvement. Criteria for FMEA project selection are the size of the project and customer requirements. According to the DPDTS, FMEAs are not expected to be commonly required by the customers in the future, although it has happened in the past. FMEA is however seen as a requirement inside the company for technology development. A non-product specific PFMEA is also going to be provided as supporting material to licensing customers.

FMEA review meetings are conducted with management when needed. The FMEA work is conducted by a small number of individuals, who organize meetings for management review. No regular meeting schedule or agenda have been defined. FMEAs are currently managed in shared spreadsheets, which can be accessed by the company personnel in real time. It has been pointed out that the spreadsheets are somewhat difficult to read by people who are not part of the FMEA team. A formal FMEA training has been conducted by an external organization. However, some of the trained personnel in production operations are no longer working for the company. The actual workflow of conducting a PFMEA did not always follow the steps specified by AIAG (2019, p. 29). Although the PFMEA was conducted according to the steps, on closer observation, the process was rather iterative and some steps were conducted simultaneously. New failure modes, effects, and causes were identified and documented throughout the PFMEA project.

Both DFMEAs and PFMEAs have been conducted in the case company. CPs are also utilized. Unlike FMEAs, specific CPs are constructed for each production run. A general “Master CP”, which is definitionally comparable to the Foundation FMEA in the FMEA process, has been implemented, and is reviewed periodically. Foundation FMEAs have not yet been developed, but the topic of developing them has been brought up in an FMEA review meeting. One supplier FMEA is also currently ongoing, but demanding supplier FMEAs is not a common practise. The product specific PFMEAs are viewed as living documents, utilized in the continual improvement of the process. Some form of revision control has been implemented into the PFMEA spreadsheets, but the need for new revisions and management of revision history are not yet effectively implemented.

It can be observed that the DFMEAs, PFMEAs, and CPs are managed somewhat separately and are thus not always in sync. Some changes implemented through PFMEA have been transferred to CP, but the linkage is not automatic or systematic. This mismatch is partially explained by the different cycles and contexts CPs and PFMEAs are managed. DFMEA is also not directly linked to either CP or PFMEA. However, according to the DPDTS, the information is transferred indirectly. The lack of linkage between the documents is seen as a deficiency in the system, and a need for improvement is recognized. In one case, it was observed that a failure mode which is supposedly detected in the DFMEA, often passes through to production, but is not controlled in the PFMEA. However, through an expert interview, it was noted that an undocumented control was in place. In this case, the DFMEA control should have been reviewed, or the risk should have been transferred to PFMEA.

3.3.1 Planning

Initial FMEA meeting was conducted when the FMEA tool was adopted. On the planning and preparation step, properties related to customer, product, and the FMEA project in question, were identified and documented as metadata for the FMEA spreadsheet. These function as the scope definition. However, the scope for included risks were not fully specified. For example, it was unclear for the FMEA team whether supply related risks should be included in the scope. According to the DPDTS, some supply related risks should be considered. The project related metadata includes the nominated FMEA team. The selected team includes people from different parts of the organization, however most of them are closely related to production operations. Also, there is no representation of supply chain operations in the project team. The DPDTS remarks that in the future the FMEA project team could also include experts from external organizations.

Rules and assumptions related to the FMEA project or individual decisions made were not documented. The product specific process flow diagram was used in the structure analysis phase. Historical data was not gathered to support failure occurrence quantification. DFMEA for the product in question had been conducted previously but was not used as input data for conducting the PFMEA. Foundation FMEA was also not used as an input as it had not yet been implemented.

3.3.2 Analyses

Carlson (2015) refers to the analysis phase as "conducting the meetings", which contains the FMEA steps from structure analysis to risk prioritization. As stated, in the case company, meetings are conducted mostly on review purpose. No specific FMEA brainstorming sessions are held, but expert knowledge is utilized by interviewing individual specialists for specific manufacturing processes.

Process flow diagram was used for identification of process steps and sub-steps in the structure analysis. The 4M categories machine, man, material, and environment, with the additional categories method and measurement, were utilized as work elements in the structure analysis. During the structure analysis, there were some uncertainties regarding the inclusion of some process steps especially related to materials receiving.

For the function analysis, no specific tools were utilized. The result of the structure analysis was used as an input, and common reasoning with process and product knowledge was used to derive the functions for process items, steps, and work elements. Only after conducting further analyses, customer defined product SCs and manufacturing environment conditions were used to expand the analysis.

In the failure analysis phase, failure modes, effects, and causes were identified. The reasoning behind the failure analysis was based on the FMEA team's experience and interviews with process experts. The 4M categories were assigned to the failures, but no Fishbone diagrams were utilized. Standard AIAG (2019) scales were used for the S rating. According to the people conducting the risk analysis, the S scale seems somewhat incompatible with the industry as lower severities cannot be assigned due to the nature of the technology. Customer collaboration was not used to establish customer perspective for failure effects and their severities. However, ship-to plant and end user effects were considered internally among the people conducting the FMEA analyses. The potential need for customer collaboration is understood in the company, but has not yet been necessary. Differentiations between failure modes, effects and causes were sometimes challenging to make. Also, there was some uncertainty present in assigning the correct work element type. However, there was a learning curve along the FMEA project. The failures were made to sync with the identified functions. However, in some cases this proved to be difficult, as there is an intrinsic difference in the levels of detail between the failures and the structure, which was initially used as an input for the function analysis.

This led to some iterative changes made in the defined functions. In the end, there was no certainty of the comprehensiveness of the analyses conducted. No comprehensive data of past things gone wrong or scrap reports were available to be utilized in the analysis. Currently, the nonconforming products are identified and marked, but causes are not always recorded. When the causes are recorded, they are not categorized or otherwise documented in an easily analysable format. Build feedback reports should include failure data, which are considered when revisioning CPs. However, this practise should be reinforced and improved, according to the DPDTS.

In the risk analysis phase, the existing prevention and detection controls were documented and the O and D ratings were given accordingly. In practise, failure and risk analyses were conducted simultaneously. The ratings were based solely on human judgement and approximation. In unclear situations expert judgement was utilized through interviews. Standard scales were used for rating, and actions were prioritized using AP chart instead of RPN. The classifications in the AP chart also follow the template presented by AIAG (2019, pp. 116–117).

3.3.3 Optimization

In the optimization phase, each FMEA row was assessed and any potential prevention or detection actions were discussed among the team and listed to their respective columns, or the risk was accepted. The optimization phase has not yet been used to assign responsibilities or to determine schedules for implementing the discussed actions. Decision making on implementing the proposed prevention and detection actions have also not yet been integrated to the FMEA process. For this purpose, another tool called Production Issues Report (PIR) was used.

As an example, during the PFMEA project, one risk was brought up and evaluated through the PIR tool. A DOE was decided to be conducted to find out the significant factors affecting the risk in question. The DOE was conducted in two rounds: first to study the effect of variables reasoned to be most significant, and second to verify results and further test the effects of other variables. Changes were made to the product design and processing variables according to the DOE results. Currently, FMEA and PIR tools are related, but their relation and synchronized utilization are not defined in the company.

3.3.4 Follow-up

The PFMEA project was kept up to date and documented in the spreadsheet. As the PFMEA is viewed as a “never ready” living document, the project was never closed. New recognized risks are still identified, documented, and optimized. As stated, the CPs and FMEAs are managed somewhat separately. Contents of the CP are not intentionally made to match with the contents of the FMEA, and changes in the FMEA do not automatically trigger changes in the CP. However, as the CP is periodically reviewed partially by the same people conducting the FMEAs, the changes should also be updated to the CP. Nevertheless, currently the link is not defined, systematic or rigorous.

Following up on the DOE performed in the optimization phase, a need for change in the maintenance practises of the machine in question was recognized. This was acknowledged by the person responsible for the machine, but not documented in the maintenance plan. This is linked to the current state of maintenance practises in the company, described in section 3.4.2. A detection control was also added to the CP to confirm the actions taken continue being effective.

3.4 Risk management in case company

This section describes the risk management practises present in the case company. It introduces the processes and tools currently in place as well as the state of organizational support and managed risk types. This section is structured according to the evaluated dimensions in the maturity models presented by Hillson (1997) and Cavalcante de Souza Feitosa et al. (2021). Summarized tables for the maturity models are given in Appendices 2 and 3. As two separate maturity models with overlapping dimensions are utilized, the observations have been grouped to different subsections. These subsections then contain observations related to varying number of dimensions. The relationship between the grouped observations and maturity model dimensions is depicted on Figure 11. The respective dimensions for each maturity model are also stated in the beginning of each subsection.

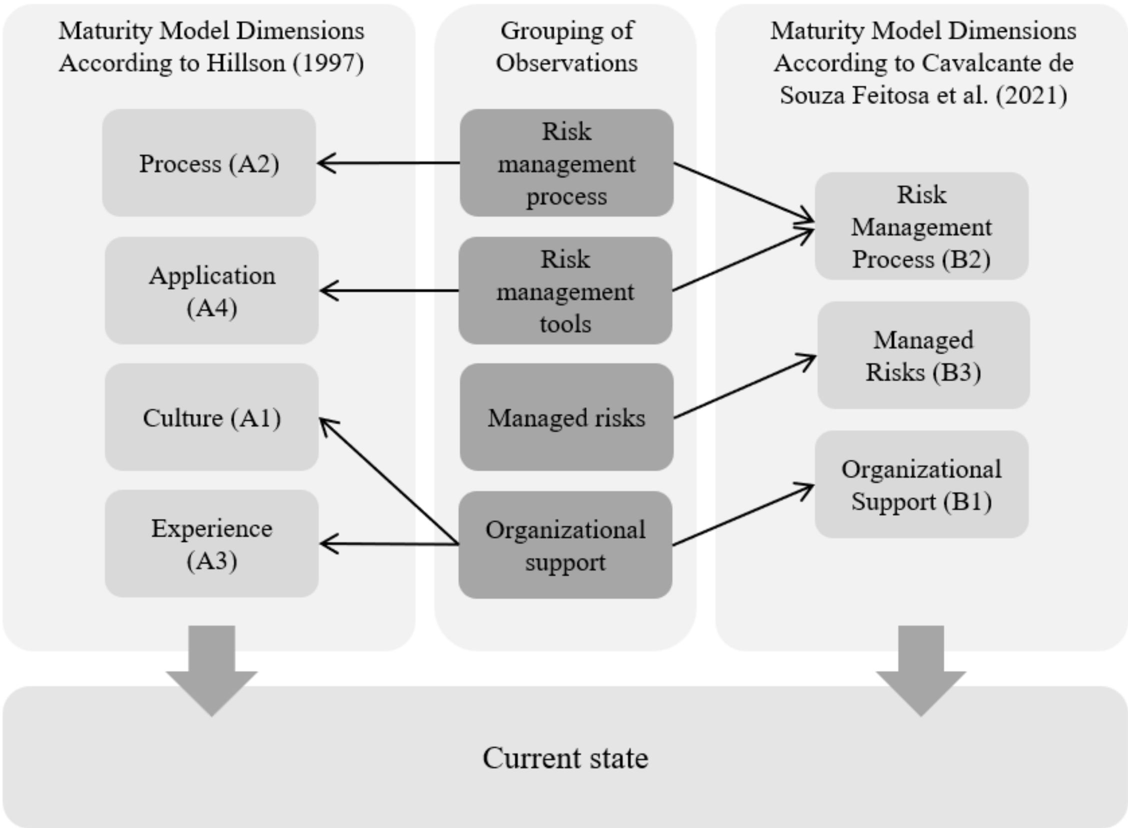

Figure 11. Relationship between the grouped observations, maturity model dimensions, and the current state.

As can be observed from Figure 11, the observations are grouped to four categories, which are then evaluated through the maturity model dimensions. These evaluations are then utilized to form the current state, and eventually the development proposals. The relationship between the maturity model dimensions and observations is depicted in Figure 11 with one-way arrows. From these arrows one may observe for example that the observations on the risk management process, presented in section 3.4.1, are evaluated on the A2 and B2 dimensions, and the observations on the risk management tools, presented in section 3.4.2, are evaluated on the A4 and B2 dimensions. Same logic applies for the observations on managed risks and organizational support, which are presented in sections 3.4.3 and 3.4.4, respectively. The evaluations based on the observations given in sections 3.4.1-3.4.4 are presented in section 3.5. The current state with assigned maturity levels for each dimension is also summarized in Table 3 in section 3.5.

3.4.1 Risk management process

This section includes observations related to the A2 dimension in the Hillson's (1997) maturity model and the B2 dimension of the maturity model proposed by Cavalcante de

Souza Feitosa et al. (2021). The observations are related to the application and formality of a risk management process in the case company.

According to the QM, the case company has a company level risk management process, but it has not been formally documented. Same applies to the production operations. However, some structure and formality are gained from the utilization of FMEA and CP. Project management related risks are managed by the project manager. Although FMEA is not utilized for all projects, CPs are formulated for each production run. Due to the nature of the tool, FMEA is dependent on the skills of the team performing it. Some reliance on the skills of individuals can also be observed from the lack of rigid connection between the FMEAs and CPs. The FMEA is used to assess occurrence and severity of risks, as well as to prioritize risk management actions. However, as reported in section 3.3.2, the comprehensiveness of the risk analyses cannot be ensured and records of risk's previous occurrences are not readily available. The improvement actions are implemented and FMEA is used for documentation. Thus, FMEA can be observed to be utilized in the identification, assessment, mitigation, and monitoring of risks. All processes are reviewed yearly on a company level.

3.4.2 Risk management tools

This section includes observations related to the A4 dimension in the Hillson's (1997) maturity model and the B2 dimension of the maturity model proposed by Cavalcante de Souza Feitosa et al. (2021). The observations are related to the application of risk management tools and risk treatments in the case company.

According to the QM, the company level risks and opportunities have been documented on a RR, in accordance to the ISO 9001 risk-based thinking. The QM also notes that the recent global crises have led to the development of Business Continuity Plans (BCPs), which are utilized to control disruption risks on a company level. For operational risk management, the company utilizes DFMEA, PFMEA, and CP. The utilization of these tools is in elaborated in section 3.3. As stated, FMEAs are not conducted extensively and the integration between DFMEAs, PFMEAs, and CPs is not effective. The CP is structured according to AIAG (2008, p. 44). However, the CP type is not specified and customer related fields are not utilized, as typically the build-specific CPs are related to prototype builds and no customers are involved with the CPs. Within the FMEA process, expert judgement is utilized through interviews. Some error proofing methods like Poka

Yoke jigs are used for selected products. The utilization of product specific error proofing jigs is however limited due to HMLV requirements.

The company also utilizes their own PIR and Corrective Action Request (CAR) tools, which can be accessed by company personnel online through a software called Jira. In some cases, PIR can be compared to Kaizen, as the tool enables the creation, management, and archival of issue reports and improvement recommendations. However, the PIR tool is not actively used by the people working in the production operations and it is not effectively integrated to the use of other tools like FMEAs and CPs. CAR is used to manage changes and disruptions. However, according to documentary data, it is not actively in use, especially on the operational level.

MRL and TRL assessments are also utilized on selected projects. However, they are not conducted regularly and do not have overall ownership. According to the VPPI there are no customer requirements guiding towards the utilization of MRL or TRL assessments. Currently they are utilized as structured frameworks guiding the risk management and actions related to it for large technology development projects. The assessments are divided into six responsibility areas with responsible persons from different parts of the organization. For ongoing assessments, each area is reviewed weekly to determine the status and evidence for fulfilling requirements. As the company is focused on technology development, the assessments are not typically conducted to reach the higher readiness levels. The VPPI would like to see MRL and TRL assessments utilized more to guide the daily work in the organization. However, the current customer needs and business model would need to be accounted for in the process.

Some maintenance plans have been created but the documentation and organizing of maintenance practises are very informal. A production machine maintenance guideline has been constructed and approved several years ago. However, the guideline is not up to date and maintenance activities are not monitored or controlled actively. Maintenance planning is not included in the regular production scheduling activities and maintenance is conducted reactively. However, the requirements for maintenance are not comparable to mass production, as production in the case company is conducted in one shift and the production volumes are low. The current maintenance practises rely on this low volume and the expertise and activeness of individual specialists, who work daily with the machines. The DPDTS highlighted that, although the volumes are low, the nature of the business requires high stability from the production processes and machine functions, to enable reliable comparisons within the high mix of products. This should also set certain requirements for maintenance activities.

The utilization of DOE for process improvement and problem solving is an established practise in the company. RCA tools like Fishbone diagrams, Pareto analysis, and Five Whys are also used occasionally. Control charts are used as a part of regular post-build reporting. However, the utilization does not fulfil the characteristics of SPC. MSA is performed in the company in the form of GRR studies, measurement system calibrations, and “Mini GRR studies”, which involve a single operator measuring single part ten times. Mini GRR studies are conducted as a part of standard operation procedures through the CP process. Calibrations are conducted regularly and full GRR studies when necessary.

The company does not have any risk metrics in use. However, Key Performance Indicators (KPIs) are utilized on both company and process levels. According to the QM, there is no need for adopting the use of KRIs at the moment. The management system’s compliance to the adopted standards is externally audited annually on a three-year cycle. This cycle is replicated on the internal audits. All defined processes are also audited internally at least once a year to evaluate their capabilities and review the KPIs related to them. Audits are performed to maintain the management system certifications and ensure compliance with the adopted standards, but also to find ways to improve current practises. Some external audits have also been performed as a part of customer PPAP.

3.4.3 Managed risks

This section includes observations related to the B3 dimension of the maturity model proposed by Cavalcante de Souza Feitosa et al. (2021). This includes a description of the extent to which different risk categories or factors are assessed in the case company.

Table 2 in section 2.6 presents a comparison of the different production and operational risk categorizations. As stated in section 3.3.2, the extended 4M categories of machine, man, material, environment, method, and measurement were considered when identifying risks in the PFMEA. However, as was also stated, there is no certainty of comprehensiveness of the analysis due to the lack of analysable data for past failures. Process knowledge is utilized to turn knowable risks to known risks through interviewing experts. However, this is not utilized to full extent as the interviews are not conducted systematically.

OHS related risk management is considered important in the company and strongly regulated in Finland. OHS risks are managed through conducting internal and external audits. Training records are kept for all employees, but production operator trainings are not actively considered from a risk management perspective. Plans of conducting trainings to better prepare for unexpected absences have been made, but not yet executed. OHS and training factors are also considered in the MRL assessment. Machine maintenance is not extensively covered in the PFMEA. As stated in section 3.4.2, the documentation and organizing of maintenance practises are lacking. Risks related to operation methods and tools are however included in the PFMEA. However, as stated, the use of error proofing methods is limited due to HMLV characteristics. Material related risks are considered in the PFMEA, but there is no representation from the supply chain in the FMEA team. Supply chain related risks are also considered in the MRL assessment, where the supply chain representative is present. Incoming material quality checks are also performed regularly. Manufacturing environment related risks are considered in both PFMEA and MRL. Outsourced maintenance is utilized to sustain environmental conditions in the manufacturing facilities. Major disruption risks are considered on a company level through BCPs.

3.4.4 Organizational support

This section includes observations related to the A1 and A3 dimensions in the Hillson's (1997) maturity model and the B1 dimension of the maturity model proposed by Cavalcante de Souza Feitosa et al. (2021). The observations describe the level of organizational support and commitment for risk management in the case company.

No formal risk management policy has yet been created. According to the QM this is not required by the currently adopted standards, but could highlight the commitment for risk and opportunity management from the top management. Some tools and processes like PIR and CAR have been specifically developed for the environment. However, for FMEA the standard template, scales, and steps presented by AIAG (2019, pp. 29, 163, 195–197, 200–203) are utilized. As stated in section 3.3, there is also some ambiguity in the definition of roles and ways of communication within the FMEA process. Risk management is conducted for most projects. Project risks are managed by the project manager, RR and BCP are utilized on company level risks, and CPs are formulated for each production run. FMEAs in the other hand are conducted only on selected projects. However, PFMEA has some common aspects regardless of the product in question, so some of the results of PFMEA benefit the production process as a whole. The utilization of the forementioned tools makes the risk management process documented. However, the performance of risk management is not monitored.

The benefits of risk management have been recognized in the company. In addition to FMEAs required by customers, internal FMEAs are conducted. Furthermore, the researcher was hired and this thesis conducted to improve risk management practises in production. Operational risk management is conducted by a small number of individuals, some of which have been formally trained for FMEA. The people working in production are highly knowledgeable of the production processes under their area of responsibility. Due to this expertise and HMLV characteristics, the production operations are relatively risk-aware. However, this risk-awareness is not effectively harnessed due to inefficient input from production workers and observed lack of documentation on some risk controls performed.

3.5 Current state analysis

This section assesses the current state of the risk management practises introduced in section 3.4, according to the maturity models presented by Hillson (1997) and Cavalcante de Souza Feitosa et al. (2021). The evaluation criteria presented in the forementioned maturity models and summarized in Appendices 2 and 3, are utilized in this section to analyse the current state of risk management, and in section 4.1 to form development proposals. According to Wieczorek-Kosmala (2014) the overall risk management maturity should be assigned according to the weakest evaluation area, as risk management can be considered only as strong as the weakest link. An answer to the RQ2 is given in the end of this section.

The maturity models are utilized to the extent they are applicable to the subject, as no credible manufacturing specific risk management maturity model was identified in the literature review. For example, the SCRM maturity model presented by Cavalcante de Souza Feitosa et al. (2021) evaluates the management of different risk categories present in a supply chain. Not all of them are directly applicable to manufacturing, so manufacturing risk categories presented in Table 2 in section 2.6 are used instead. As two separate maturity models are utilized, the observations related to different maturity model dimensions have been grouped to sections 3.4.1-3.4.4. This grouping, depicted in Figure 11 in section 3.4, is also utilized in structuring this section. The following paragraphs present the evaluations of different maturity model dimensions, utilizing this grouping.

The risk management process presented in section 3.4.1 fulfils the second level requirements of the A2 dimension in the Hillson's (1997) maturity model. In the second level there is no formalized generic risk management process, but some formal methods are in use. The effectiveness of the risk management process is also dependent on the skills of the risk management team. However, some requirements of the third and fourth levels are also partially fulfilled. According to the QM, the company level risk management is integrated to the QMS. Also, risk management is applied to most projects through the use of CPs. The regular updating of processes is a requirement on the fourth maturity level. On the maturity model proposed by Cavalcante de Souza Feitosa et al. (2021), the requirements of the second maturity level on the B2 dimension are also fulfilled. These include requirements for the identification, assessment, mitigation, and monitoring of risks. For example, in the second level the organization identifies different types risks, but not comprehensively, has some experience of using more complex risk management tools, some mitigation practises are in use, and records of risk occurrences are not produced. The current risk assessment and prioritization through FMEA also yields partial fulfilment of the third and fourth maturity levels.

The utilized risk management tools presented in section 3.4.2 fulfil the second level also on the A4 dimension of Hillson's (1997) maturity model. In this level, the tools are not yet fully integrated and there is some inconsistency in their application. However, some of the third level requirements are also partially fulfilled, as some of the tools are utilized consistently and the activities show commitment of resources. In the maturity model proposed by Cavalcante de Souza Feitosa et al. (2021), the risk management tools are included in the B2 dimension. The tools are not evaluated separately, but many of the tools utilized in the company are given as examples to be utilized in different process phases.

The managed risks, presented in section 3.4.3, are evaluated on the B3 dimension in the maturity model proposed by Cavalcante de Souza Feitosa et al. (2021). As the maturity model is designed for evaluating SCRM, some of the included risk categories are not evaluated here. The considered risk categories include manufacturing risk categories presented in in Table 2 in section 2.6. The second maturity level requires the action to manage and minimize operational risks, which is fulfilled. The third maturity level requirements however are not fulfilled, as it requires the action to manage and minimize all operational risks. In the fourth maturity level, also disruption risks are managed, which is done on a company level. Partial fulfilment of the third and fourth levels can therefore be assigned.

The organizational support presented in section 3.4.4 can be assessed through Hillson's (1997) A1 and A3 dimensions. On the A1 dimension, the second maturity level requirements are fulfilled. However, some of the requirements of the third maturity level are also fulfilled. On the second level risk management is utilized in selected projects, but there is no accepted risk management policy. On the third level risk management benefits are recognized and expected and the organization is prepared to commit resources to risk management. Likewise, on the A3 dimension, the requirements of the second maturity level are fulfilled, with partial fulfilment of the third level requirements. Although some specific tools like PIR and CAR have been created, which is a requirement on the third level, the operational risk management is limited to individuals with little to no formal training. In the maturity model proposed by Cavalcante de Souza Feitosa et al. (2021) organizational support is evaluated in the B1 dimension. The requirements for the second level of maturity are fulfilled. In this level, there is a growing concern of risk management, but no performance monitoring, and there is room for improvement in the accountability and communication of risk management activities. The third maturity level requirement of recording the risk management process is also fulfilled.

The RQ2 seeks to find out how operational risks are currently managed in the case company. The reached maturities of operational risk management in the case company are utilized to answer this question. The fulfilment of requirements for different maturity levels and dimensions is presented in Table 3. Evaluations for the fulfilments are presented above, and the respective observations are presented as justification in sections 3.4.1-3.4.4. As can be observed from the assessments, the operational risk management in the company can be uniformly assigned between the second and third maturity levels. Partial fulfilment of the third level requirements applies to all dimensions, but none of the evaluation areas completely fulfilled the third level criteria. The observed operational risk management matches also the overall description of the second maturity level by Hillson (1997). According to this description, the organization is experimenting risk management through a small number of individuals, has no generic structured process in place, is aware of the potential benefits of risk management, and has implemented risk management somewhat ineffectively. An overall maturity corresponding to the second maturity level can therefore be assigned to the current operational risk management practises in the case company.

Table 3. Fulfilment of requirements for different maturity levels and dimensions.

Maturity Model	**Dimension**	**Fulfilment of Requirements**			
		1st Level	**2nd Level**	**3rd Level**	**4th Level**
Hillson (1997)	**Overall**	S	F	P	N
	Culture (A1)	S	F	P	N
	Process (A2)	S	F	P	P
	Experience (A3)	S	F	P	N
	Application (A4)	S	F	P	N
Cavalcante de Souza Feitosa et al. (2021)	**Organizational Support (B1)**	S	F	P	N
	Risk Management Process (B2)	S	F	P	P
	Managed Risks (B3)	S	F	P	P

(S: Surpassed; F: Fulfilled; P: Partially fulfilled; N: Not fulfilled)

4 DISCUSSION

This section presents the development proposals and their implementation for operational risk management in the case company. An overview of the proposed improvements is presented in the beginning of section 4.1. The improvements are then discussed in detail in the subsections 4.1.1 and 4.1.2. The section 4.2 then presents a condensed description of the prioritization, sequence, and resource requirements of the proposals, which is given as an answer to the RQ3. Finally, sections 4.3-4.5 assess the managerial and scientific implications as well as the limitations of the study.

4.1 Development proposals

In section 3.5, the case company's operational risk management maturity was assigned in between the second and third levels on the maturity models presented by Hillson (1997) and Cavalcante de Souza Feitosa et al. (2021). The improvements proposed in this section are directed towards obtaining higher maturity ratings. As noted in section 2.5.2, Wieczorek-Kosmala (2014) believes that a higher risk management maturity yields higher benefits, yet Pergler (2012) believes the higher benefits are due to underlying differences between organizations. However, in addition to obtaining a higher maturity rating, implementing the proposed improvements could reinforce the active and correct usage as well as integration of risk management tools and processes.

In the subsections, the development proposals are divided into organizational and operational improvements. These are then further categorized according to Figure 12. The proposed improvements are described in detail within the subsections under headers corresponding to the categorization. The improvement proposals include actions with varying priority and resource requirements, and should thus not all be considered equal. However, when applicable, the proposed actions are linked to the corresponding maturity levels in the detailed descriptions. The proposed changes can be roughly divided into three stages:

1. improve and formalize the existing tools and processes,
2. implement key tools and practises to extend the reach of risk management, and
3. focus on continually improving and investing in risk management.

These stages give a rough perception on the sequence of the proposed improvements. This sequence is affected by the urgency and resource requirements of the actions, as well as the requirements on the higher maturity levels. Based on these three stages and the proposals given in sections 4.1.1 and 4.1.2, a more detailed proposal for priority and estimated resource requirements is provided in section 4.2.

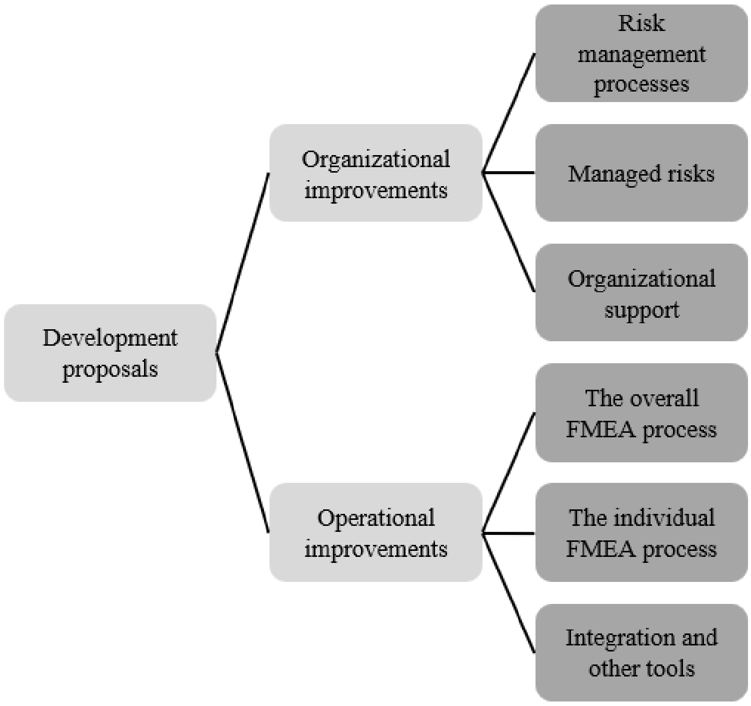

Figure 12. Categorization of the development proposals.

4.1.1 Organizational improvements

The organizational improvements introduced in this section include improvements to the risk management processes, managed risks, and organizational support for risk management. The organizational improvements are closely linked to the operational improvements presented in section 4.1.2.

Risk management processes

Both organizational and operational level risk management processes should be formally defined and described. Although the ISO 9001 standard does not directly require formal definition of risk management processes, it is required by ISO 31000 (ISO, 2018b, p. 14). In addition, a formalized risk management process is a requirement in the higher risk management maturity levels (Hillson, 1997). The synthesized process depicted on Figure

10 in section 2.6 may be utilized when defining the formal description of the process. This process should then be reviewed periodically, which is already done to other processes in the company. Periodic reviews are supported by BCBS (2006, p. 209) and ISO (2018b, p. 7), and are also a fourth level requirement on the A2 dimension of Hillson's (1997) maturity model.

The PFMEA project conducted in the empirical part of the study indicated a focus on the initial phases of the risk management process, as the subsequent phases were not completed or managed within the FMEA tool. This is in line with the observations made by Ferreira de Araújo Lima et al. (2020). Integrating the risk management process into a single tool or defining the relationships between different tools utilized in the process could clarify the process. For example, risk treatment strategies were not managed within the FMEA tool. The effective implementation of treatment strategies is a third level requirement in the B2 dimension in the maturity model proposed by Cavalcante de Souza Feitosa et al. (2021). The preparation and implementation of risk treatment plans is also highlighted by ISO (2018b, p. 14). More emphasis should also be put on the risk monitoring phase, as highlighted by DAU (2022b) and de Oliveira et al. (2017). Risk monitoring is vital for continual improvement, analysing changes, and identifying emerging risks (de Oliveira et al., 2017). The effectiveness of risk management practises should also be monitored. Risk metrics, which provide constant feedback for improvement, are required on the fourth level of the A2 dimension in Hillson's (1997) maturity model. Monitoring the risk management process is also required by ISO (2018b, p. 14). The comprehensiveness of risk management should be confirmed by collecting and analysing records of risk occurrences. Complete risk identification is a third level requirement in the B2 dimension in the maturity model proposed by Cavalcante de Souza Feitosa et al. (2021).

The reliance on the skills of individual employees should also be reduced. This is a requirement to reach the third level on the A2 dimension of Hillson's (1997) maturity model. The reliance may be harmful, as for example some of the people trained for FMEA no longer work for the company. The previously presented actions of simplifying and documenting the risk management process could reduce the effect of this reliance. The reliance itself could be reduced for example by enforcing the risk-aware culture, which is also a fourth level requirement on the A3 dimension of Hillson's (1997) maturity model.

Managed risks

The B3 dimension in the maturity model proposed by Cavalcante de Souza Feitosa et al. (2021) sets requirements for the management of different operational risk categories and disruption risks. As previously stated, recording and analysing previous risk occurrences might increase the comprehensiveness of risk identification. To further increase this comprehensiveness, knowledge could be acquired more systematically from production workers via regular meetings or encouraging engagement and risk-awareness.

Some of the operational risk categories might also require more attention. The already made plans for conducting trainings to production workers to better prepare for unexpected absences should be executed. This requires coordination with a more in-depth planning of who should be trained for which work. The consideration of maintenance related risks should be increased to transform maintenance activities from reactive to proactive. This matter is further discussed in the operational improvements, in section 4.1.2. A need for managing some key supply related risks was identified in the interview of the DPDTS. As stated by Chen et al. (2013) supply risk increases process risk, which makes it important to be managed from the operational perspective too. As highlighted in section 2.2, it is important for SMEs to drive for collaborative risk management in the supply chain (Alicke et al., 2020; Cavalcante de Souza Feitosa et al., 2021; Chen et al., 2013; Ho et al., 2015). Disruption risks are currently managed at the company level. However, their management and actions related to them could be made more visible to the operational level.

Organizational support

The level of organizational support could be increased by systematizing communication, defining responsibilities, continually improving practises, training and encouraging personnel for risk management, and implementing performance monitoring. The usage of specifically developed tools and processes like PIR and CAR should also be further developed and reinforced.

The communication and regular reporting of risk management activities should be made more systematic. This is supported by Hillson (2014, p. 299), ISO (2018b), and PMI (2013, p. 311). Requirements for efficient communication of risk management activities are also given in the higher maturity levels of the B1 dimension in the maturity model proposed by Cavalcante de Souza Feitosa et al. (2021). Encouraging and rewarding proactive risk management is also a higher-level requirement in the A1 dimension of the Hillson's (1997) model. Inclusion of all personnel for risk identification is a widely advocated practise (DAU, 2022b; ODASD(SE), 2014; PMI, 2013, p. 321). Brocal (2019) also recommends frequent discussion of risks and encouraging different opinions. Training for risk management could also be conducted more regularly. In addition to strengthening the in-house expertise on risk management, this would show the commitment of management and enhance risk-awareness. Regular external trainings are a requirement in the fourth level of the A3 dimension in the Hillson's (1997) maturity model. According to Hillson (1997), this exposes the internal staff to outside influences. DAU (2022b) also proposes the creation of internal training material for risk management. The potential of this could also be considered at the later stages of implementation.

A risk management policy could be created to highlight top management commitment on managing risks. Javaid and Iqbal (2017) highlight the need for management support and an accepted risk management policy is required in the third level of the A1 dimension in the Hillson's (1997) model. Culture is included in the B1 dimension in the maturity model proposed by Cavalcante de Souza Feitosa et al. (2021) and a separately evaluated dimension on its own in the Hillson's (1997) model. Enforcing the risk-aware culture was previously proposed as an action to reduce reliance on individuals. It is also supported by Bailey et al. (2019), and a requirement for higher maturity levels on both of the utilized maturity models (Cavalcante de Souza Feitosa et al., 2021; Hillson, 1997). Risk-awareness is also linked to the awareness of roles regarding risk management. However, to enable this awareness, the accountabilities, roles, and responsibilities regarding operational risk management first need to be defined. Higher awareness of roles and responsibilities is required in the third and fourth maturity levels in the B1 dimension of the maturity model proposed by Cavalcante de Souza Feitosa et al. (2021). Sifumba et al. (2017) also recognized a need for improvement in the communication and roles regarding risk management.

Performance monitoring and continual improvement were discussed on the subject of process improvements, but they also relate to the A2, A3, and B1 dimensions. They are included as requirements for the higher maturity levels on both of the utilized maturity models (Cavalcante de Souza Feitosa et al., 2021; Hillson, 1997). According to the QM, there is no need for implementation of KRIs. However, KPIs related to operations should be reviewed and communicated. Performance monitoring for FMEA is discussed in section 4.1.2.

4.1.2 Operational improvements

The operational improvements introduced in this section include improvements to the utilization and processes related to FMEA and CP, as well as suggestions on integration and other tools to implement. FMEA will be discussed in more depth regarding the overall and individual FMEA processes, due to its central role in operational risk management in the company.

The overall FMEA process

The overall FMEA process and responsibilities related to it should be defined. Carlson's (2015) overall FMEA process is briefly described in section 2.4.1. As stated in section 4.1.1, this process, like other processes, should be periodically reviewed. Foundation FMEAs should be created to support conducting specific FMEAs. This is also supported by AIAG (2019, p. 19), as it enables knowledge accumulation through applying the lessons learned from previous FMEAs. Conducting specific FMEAs requires the formulation of specific criteria for selecting which FMEA projects should be conducted. Exemplary selection criteria are provided for example by AIAG (2019, pp. 20, 31–32, 79–80) and Carlson (2015). As PFMEAs are conducted as living documents, effective practises for review and revision control need to be implemented. This is supported by General Motors Corporation (2008, p. 110) and Munro et al. (2015, p. 57). Regular meeting schedule for reviewing and discussing FMEA related matters needs to be determined. The DPDTS agrees that scheduling monthly meetings could be beneficial. This is also linked to the effective facilitation of FMEA activities, which is one of the six critical FMEA success factors proposed by Carlson (2015). In fact, FMEA process implementation, applying lessons learned, and selecting the right FMEA projects are all included in the Carlson's (2015) six critical FMEA success factors.

The integration between DFMEA, PFMEA, and CP should also be reinforced, as the desired relationship between the tools, depicted in Figure 8 in section 2.4.1, is not currently applied. Although PFMEA assumes correct design, any risks that are not mitigated in the DFMEA should be transferred to PFMEA to avoid hidden risks that need to be managed during production. This is supported by General Motors Corporation (2008, p. 17). Also, any controls placed in the PFMEA should be included in the CP. This is also supported by General Motors Corporation (2008, p. 112). The FMEA process integration to other business processes and the QMS could also be considered. This is supported by Munro et al. (2015, p. 57).

The individual FMEA process

The individual FMEA process employed in the company is defined in the AIAG's (2019, p. 29) FMEA template, but it is not utilized to its full extent. This is related to the integration and definition of relationships between different tools. The planning and follow-up phases suffer from the lack of Foundation FMEAs and integration between DFMEA, PFMEA, and CP. In addition, the use of PIR as an input for FMEA is not fully harnessed and the optimization step is not facilitated through FMEA process. A company specific individual FMEA process with described integration of the utilized tools should be defined. This also includes defining the responsibilities and review practises. For example, Segismundo and Miguel (2008) recommend utilizing a monthly PDCA cycle for conducting risk treatment until the end of the FMEA project. The individual FMEA process was identified in the empirical study to be iterative rather than sequential. This is in line with ISO (2018b, p. 9) and ODASD(SE) (2014, p. 5), who claim that risk management process is often iterative in practise. A consolidated process for executing individual FMEAs is depicted in Figure 7 in section 2.4.1. For clarity, the following improvements are presented according to the structure of the consolidated process.

Planning and preparation for each FMEA is stated as one of the six critical FMEA success factors by Carlson (2015). More emphasis should be put to defining the scope of the FMEA project. While the scope of the conducted PFMEA was defined based on the technology development needs, the risk severities were assessed based on delivering goods. This creates a contradiction, which might make the FMEA team focus on irrelevant risks. Rules and assumptions related to the FMEA project should be defined and documented. This enables assessing the validity of the made assumptions in the follow-up phase. Roles and responsibilities need to be defined also for the individual FMEA process. This is supported by IEC (2009, p. 8). For reference, AIAG (2019, pp. 25–28) presents FMEA related roles and responsibilities. These are also discussed in section 2.4.1. As stated by the DPDTS, the FMEA team may also include external team members, which needs to be taken into account when formulating the teams. The inclusion of purchasing or transport and design knowledge in the team should also be considered to elaborate the supply risks and information flow between DFMEA and PFMEA.

A more carefully conducted function analysis could reduce the iterations from the FMEA process. However as stated, iterations are typical for a risk management process (ISO, 2018b, p. 9; ODASD(SE), 2014, p. 5). More supporting tools could be utilized in the failure analysis phase. This could include tools like brainstorming, Delphi technique, SWIFT, FTA, or RCM (Cavalcante de Souza Feitosa et al., 2021). To be able to ensure FMEA completeness, past failure data or scrap reports should be collected. Collecting scrap reports with coded failure modes and causes on selected projects was discussed and gained support in the interview of the DPDTS. If any assumptions are made during the analyses, these should be documented to enable review in the future. This is supported by PMI (2013, p. 330). IEC (2009, pp. 15–17) also recommends documenting any uncertainties present during the analyses.

The Applicability of the S scaling should be evaluated. This is also linked to the contradiction in the scope definition, as the risk evaluation should be done so that it serves the greater scope and purpose of the tool. As previously stated, the utilized S rating was based on delivering goods, even though the scope of the PFMEA focused on technology development. In the case company, the S rating should reflect the ability of getting correct results and having a stable process instead of delivering goods. A similar remark was made in the maintenance context by the DPDTS, presented in section 3.4.2, when the importance of maintenance activities in the company was discussed. As was established in section 2.4.1, the use of RPN is widely criticized in the literature (AIAG, 2019, p. 114; Carlson, 2015; de Aguiar et al., 2015; General Motors Corporation, 2008, p. 103; Segismundo & Miguel, 2008; Tague, 2005, p. 242). Thus, the AP chart presented by AIAG (2019, pp. 116–117) is utilized in the company instead. However, as manually checking the AP rating for each risk was tedious and prone to errors, an automatic lookup function was implemented during the empirical study. Currently the S scaling is defined in a way that limits the possible AP ratings that can be obtained in practise. This in turn leads to more risks having the same AP ratings and makes the prioritization less useful. The DPDTS hesitates changing the S scale, and would rather implement the changes in the AP chart. However, manually recategorizing the AP chart could lead to inconsistencies, so it requires careful consideration. Another option would be to utilize RPN or one of its alternatives, presented in section 2.4.1, to support prioritization within a specific AP rating. Whether the changes are implemented in the AP chart or through supporting prioritization scales, these changes should be assessed in the future. When making changes to any scales, the potential customer perspective needs to be accounted for. AIAG (2019, p. 107) highlights this by stating that the evaluations need to be agreed by the organization and its customer.

According to AIAG (2019, p. 119) "*Actions represent a commitment to take a specific, measurable, and achievable action, not potential actions which may never be implemented.*". Currently in the case company, the optimization columns in the FMEA form are utilized precisely for the latter purpose. This is not the intended way, and is likely caused from the lack of FMEA meetings, where the actions could be discussed. Decision making on actions should be implemented within the FMEA process. This should be clarified through implementing the regular FMEA meetings and defining the combined utilization of different tools within the risk management process.

As the PFMEA is utilized continually, the current prevention controls should be regularly audited. This is supported by AIAG (2019, p. 106). Recording assumptions was highlighted on both planning and analysis phases. In the follow-up phase, the validity of these assumptions needs to be reviewed. IEC (2009, pp. 11, 17) highlights that changes in assumptions require changes in other risk management aspects. FMEA linkage to CP and Foundation FMEAs is highlighted in the follow-up phase (Carlson, 2015). As stated in the context of the overall FMEA process, the Foundation FMEAs should be created. CP linkage has also been discussed previously, and will be discussed further in the context of integration and other tools.

Integration and other tools

The FMEA tool fills a lot of the requirements for a risk management tool from a risk management process point of view. This can also be observed from the applicability rating by IEC (2009, p. 22). The individual FMEA process is heavily linked to the risk management processes introduced in section 2.3. The risk management process is effectively built into the tool, if it is used properly. In addition, the risk expression and treatment planning in FMEA directly comply with ISO 31000 and PMBOK (ISO, 2018b; PMI, 2013, pp. 321, 343). However, in addition to FMEA, some RCA and optimization tools might be necessary for process improvement. FMEA naturally includes aspects from Fishbone diagram, Process flow diagram, risk categorization, as well as Risk Reporting and evaluation matrices. It can also be supplemented by the forementioned tools or tools like SWIFT, FTA, brainstorming, interviews, and various statistical and RCA tools. The utilization of supplementing tools could be increased. This could give the FMEA steps more structure and ensure comprehensiveness, which in turn would reduce iterations and unidentified risks.

In addition to improvements in the individual tools, the integration of tools should be improved and defined. PFMEA, DFMEA, CP, and PIR are currently being used simultaneously but separately. Integrating these tools would make the process more efficient and effective. This is supported by Carlson (2015). CP is currently used routinely, but the consistent and routine application of risk management in all activities could be improved. In addition, reporting and decision making based on risk should be implemented and conducted regularly. These actions are linked to the requirements in the third and fourth levels of the A4 dimension in the Hillson's (1997) maturity model. Support for the actions also comes from the IEC (2009, p. 8), as it highlights that the risk management team should be clear about the used tools and their relation to the risk management process, risk management's integration to organizational processes, and the conducted reporting and reviewing. Cavalcante de Souza Feitosa et al. (2021) recommend including the risk causes and effects, employed treatment plans, and their results in the reports.

At minimum, the relationships between PFMEA, DFMEA, CP, and PIR need to be defined. A weak connection between PFMEA and CP could be achieved by assigning unique identifiers for each risk, which would be matched between the documents. Defining and numbering product-specific SCs could serve a similar purpose. A better solution would be to integrate the tools through a system. This could be achieved through a revision control system, in which a change to a document would automatically require approval of the document and all documents linked to it. A stronger integration could still be achieved through the existing Jira system, where different FMEAs, CPs, and PIRs could be controlled as separate projects with individual common elements and linkages. Taking the FMEA tool to Jira could also make the FMEAs more accessible to the whole organization and increase the readability compared to a spreadsheet. Jira could provide a better user interface compared to a spreadsheet, as investing on a dedicated FMEA software would probably not be justifiable.

The dynamic applications of FMEA and CP, discussed in section 2.4.7, should be considered. The dynamic CP, as proposed by Munro et al. (2015, pp. 418–420), has some common aspects with the practises already in place. If the dynamic approach is pursued, Munro et al. (2015, pp. 418–420) may be used as a reference point. Operator input could be collected through PIR or Jira. The dynamic application of FMEA, as proposed by Mili et al. (2008), might however be less relevant at the time due to the required quantitative failure data. The use of quantitative historical data or capability indices for occurrence rating might not be applicable to a HMLV environment as this data is highly affected by constantly changing parameters. However, the O rating is currently based on human judgement, which could be biased. Some quantitative failure data could be produced through scrap reports. The need for scrap reports was also noted in the context of the individual FMEA process. Scrap reporting could be done in Jira through PIR or a separate scrap reporting platform. The DPDTS agrees that PIR could be utilized for this purpose. The data could then be utilized in an RCM application or evaluating the comprehensiveness and providing input for FMEA and CP.

The utilization of PIR to report machine failures should also be reinforced. These reports could function as an input for planning and conducting maintenance activities. Immediate actions for organizing maintenance activities are required. As stated by the DPDTS, high stability is required from the machines and processes, although sudden production stoppages are not critical from a maintenance perspective. RCM or Maintenance FMEA could be implemented to obtain a risk-based approach for maintenance. This is also supported by the DPDTS. The DPDTS also highlighted that PFMEA and Maintenance FMEA should be managed separately. RCM is one of the recommended practises proposed by Cavalcante de Souza Feitosa et al. (2021). Ben Said et al. (2016) also highlight the need for dynamic maintenance practises in HMLV environments. Regardless of the implementation of new maintenance practises, the existing maintenance guideline should be updated, reinforced, and kept up to date. Maintenance FMEA could be utilized in forming the new versions of the guideline. Maintenance should be incorporated to the daily work due to its indisputable importance. This includes producing records of the conducted maintenance activities. This is supported by ISO (2009, p. 30). IEC (2009, p. 67) also highlights that RCM requires the collection of data related to equipment failures and maintenance activities. Scheduling maintenance activities as a part of regular production planning should also be considered.

In general, PIR should be utilized more extensively. If used extensively, PIR could function as a register for past things gone wrong. The usage could be increased through implementing the recently presented purposes for PIR inputs. To encourage the usage of PIR, the activities made through the tool could be made more visible to the production workers. At some point, PIR could be combined with some sort of rewarding system to reward reporting activity. The DPDTS seconds the proposal of strengthening the utilization of PIR as an input for FMEAs, CPs, and maintenance activities. The DPDTS also proposed going through the PIR findings in the regular FMEA meetings, which could be conducted in the future. As stated, the combined usage of PIR and FMEA should be defined. This is especially important because some of the use cases of the tools are currently overlapping. PIR can be utilized as an input for FMEA, but FMEA should guide the overall risk management process. Any actions should be documented in FMEA, while PIR could be utilized for carrying out the actions as projects. A re-launch of the PIR tool could be performed to highlight the new practises. Regular re-launches are also recommended by Hillson (1997).

Finally, KRI, SPC, and MRL are other tools that could be considered. If, as was established in section 3.4.2, KRI is not to be implemented, some other form of performance metric for operational risk management could be beneficial. Cavalcante de Souza Feitosa et al. (2021) recommend measuring risk management performance in the form of reliability, cost, and responsiveness. Simplified performance metrics could be implemented for example as a dashboard in the FMEA tool. This could provide a quick review of the FMEA progress and total numbers of identified risks in each process phase and action priority rating. Munro et al. (2015, p. 64) recommend forming a Pareto analysis of RPN scores, which could also be presented in the dashboard. ODASD(SE) (2014, p. 39) and Wieczorek-Kosmala (2014) also advocate for a management indicator system. As stated, SPC may have limited applicability in a HMLV environment. However, it could be considered for some of the steadier process parameters. The benefits of the combined usage of DOE, SPC, and FMEA is presented by He et al. (2002), and discussed in section 2.6. The use of MRL for guiding daily work was also proposed by the VPPI. This could be beneficial if there are resources for conducting MRL assessments.

However, it would be somewhat overlapping with the current FMEA practises, which needs to be taken into account.

4.2 Implementation plan for the case company

The purpose of this section is to provide a condensed proposal for the sequence of implementation for the development proposals presented in section 4.1. This proposal is provided as an answer to the RQ3, which aims to determine how the risk management practises in the case company's production operations can be improved. The purpose of this prioritized sequence of actions is to give an overall image and help in carrying out the changes. For an in-depth description of the required actions, see section 4.1.

A proposed sequence of actions with estimated level of required resources is depicted as a Gantt chart in Figure 13. Both time and maturity increase when progressing from left to right in the chart. The sequence is based on the urgency of the matter, required resources, and progression of maturity levels. The respective maturity model dimensions are also specified in the figure after each action. As was stated in section 2.5.2, the costs of a higher maturity need to be compared to the associated benefits (Hillson, 1997). For specific actions, this is discussed in the detailed proposals, presented in sections 4.1.1 and 4.1.2. For example, the urgency of maintenance activities is highlighted, but implementation of Dynamic FMEA is considered less relevant at the time due to its requirements. Some of the more resource intensive proposals might require further discussion on whether they should be pursued or not.

The relative timing of the proposed actions is associated with the three stages of implementation, proposed in section 4.1. The exact timing of these stages should be determined according to the prevailing context of the organization and available resources to implement the proposed actions. However, the first stage should be implemented as soon as possible. The second stage should be pursued after the completion of the first stage, possibly within a few years. The third stage may be pursued after the second stage, according to available resources. The following paragraphs include more detailed descriptions of the three stages.

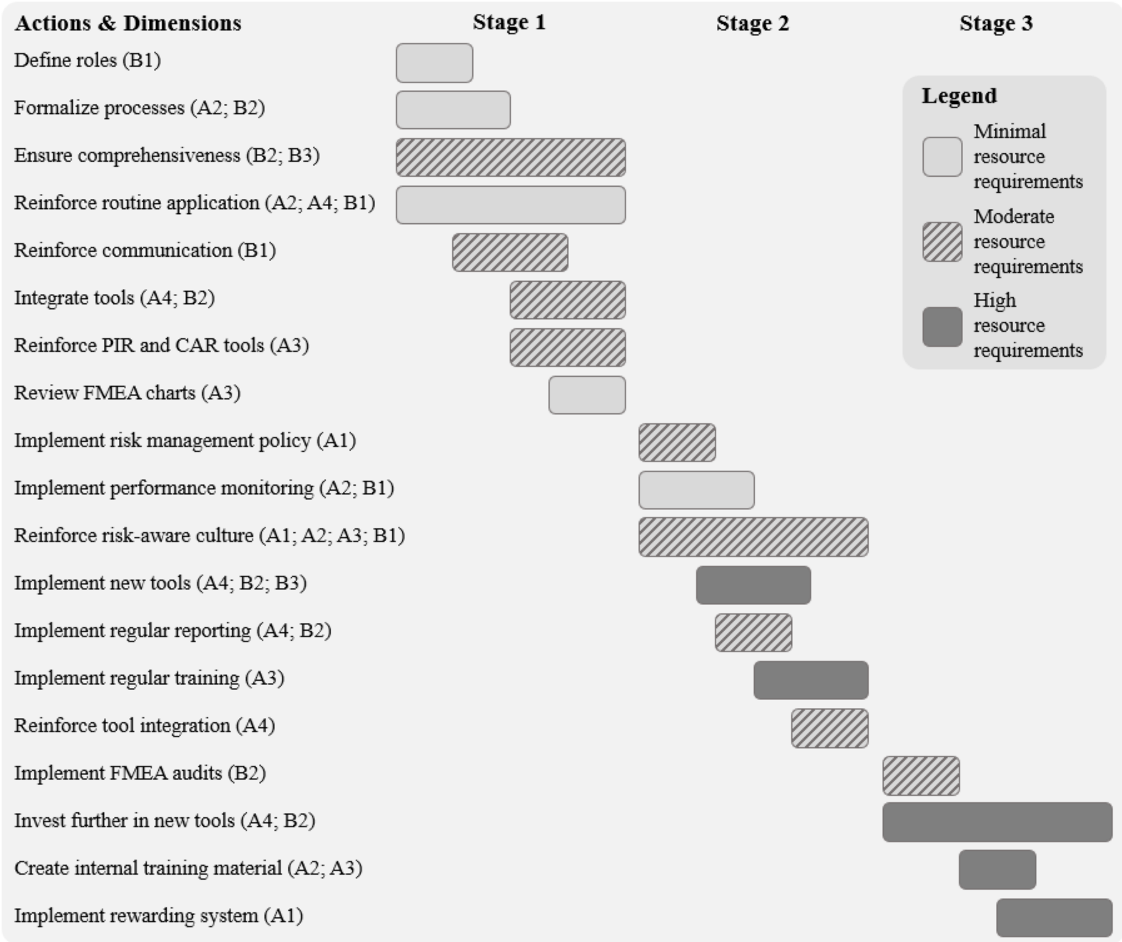

Figure 13. Gantt chart proposing the sequence, estimated level of required resources, and respective maturity model dimensions for the actions.

The stages loosely follow the progression of maturity levels. The first stage includes actions required to progress from the second maturity level to the third. However, some of such actions are also included in the second stage. The second stage actions are directed towards achieving the third and fourth maturity levels, and the third stage actions aim to fulfil the fourth level requirements as well as to maintain the achieved maturity. According to Hillson (1997), the third maturity level requires a formalized, routine application of risk management in most projects. To progress from the second maturity level to the third, Hillson (1997) recommends strengthening the corporate backing, allocating resources, conducting formal trainings, and formalizing the processes. The fourth maturity level requires a risk-aware culture with active utilization of risk information, and opportunity management (Hillson, 1997). To progress from the third maturity level to the fourth, Hillson (1997) recommends regularly reviewing the process, re-launching practises, and conducting external trainings, as well as continually improving and investing in risk management, and encouraging a risk-aware culture. To maintain the fourth level maturity, Hillson (1997) recommends regularly auditing risk management practises, managing both risks and opportunities, as well as involving customers and suppliers and continuously investing in risk management.

The first stage includes the most urgent actions directed towards improving and formalizing the existing tools and processes. The processes, responsibilities, and communication for operational risk management need to be defined. The integration of different tools should be improved and their linkages should be defined. The comprehensiveness should be improved by reinforcing the utilization of the PIR tool, and refining practises for scrap reporting, maintenance, and supply risk management. The FMEA charts should also be reviewed in this stage.

The second stage includes actions that should be performed later when the time and resources allow it. Risk-aware culture, training, and company policy all aim for more collective awareness of risks and less reliance on individuals. New tools, performance monitoring, regular reporting, and stronger tool integration should also be pursued at this stage. The further integration of tools could be achieved for example through Jira. The new tools to implement could include tools like RCM, Dynamic CP, and Foundation FMEA, as well as more supporting tools to be utilized jointly within FMEA.

The third stage includes the least urgent actions that are focused on maintaining the achieved risk management maturity and continually improving practises. These include actions like implementing FMEA audits, creating internal training material, implementing rewarding systems, and further investing in new tools like Dynamic FMEA, KRI, SPC, and MRL assessments.

4.3 Managerial implications

This section describes the managerial implications of this study to give a general overview on how and where the results of this study could be utilized. The managerial implications of this study arise from presenting the central literature and a case study with observations and development proposals related to operational risk management in HMLV production. These may be utilized by managers and process engineers looking to evaluate, improve, or implement practises for operational risk management, especially in HMLV environments.

The literature review provides an overview for risks and risk management. Different contexts for risk management and some important operational risk management tools are also introduced. Some central risk management maturity models are introduced as ways to assess risk management capability. Synthesized processes are also presented for risk management and conducting individual FMEAs. Main results of the literature review for the purpose of this study are presented in section 2.6, which provides a synthesis of the conducted literature review. The results of the literature review may be utilised by companies that are starting to implement formal risk management practises, or want to look for ways to improve or assess the current state of operational risk management. The synthesized processes may be utilized in implementing and evaluating individual and overall FMEA processes or the general risk management process present in a company.

The empirical study introduces a case example of a PFMEA project and observations related to assessing the state of operational risk management using two maturity models, which are summarized in Appendices 2 and 3. The development proposals include both organizational and operational improvements directed towards improving operational risk management capability. Improvements are proposed to processes, management, and the implementation and utilization of risk management tools. Implementation of the changes is divided to three stages to indicate the sequence of implementation for the case company. The development proposals are especially useful for the case company itself, as the results are directly applicable to the environment. However, the development proposals and observations made in the empirical study might also be beneficial for companies who want to conduct similar assessments or have similar environment or needs for improvement. The empirical study also highlights some of the challenges that might be present in any company conducting FMEAs or operational risk management in general.

If a similar study utilizing the same maturity models is to be conducted, the framework depicted in Figure 11 in section 3.4 may be utilized for grouping observations and forming evaluations of the current state. The summarized maturity models, presented in Appendices 2 and 3, may also be utilized in the evaluations. In addition, the current state matrix for representing the assigned maturity levels, presented in Table 3 in section 3.5, may be utilized. The chosen maturity models, although partially overlapping, complement each other. As no manufacturing specific model was identified, utilizing both selected models is recommended to achieve a wider perception and recognize more areas for improvement. As stated, the development proposals obtained in this study are somewhat subject to the evaluated organization, but ideas for improvement and presenting the results may be obtained from sections 4.1 and 4.2.

A general framework for managing operational risks in HMLV production SMEs is obtained by considering the factors contributing to capability. The capability to manage operational risks is assessed through the maturity models, and the contributing factors can be derived from the maturity model dimensions. The dimensions of the utilized maturity models can be combined to processes, tools, managed risks, and organizational support, as depicted in Figure 11 in section 3.4. Higher capability should generally be pursued, but the associated costs and benefits need to be considered. Selected tools and processes should be dynamic to accommodate evolving practises and high mix of products. Available resources might be limited or prone to change, which should also be considered. Comprehensiveness should be ensured by considering the risk categories applicable to production, such as in Table 2 in section 2.6. The statements above are condensed to a general framework in Figure 14.

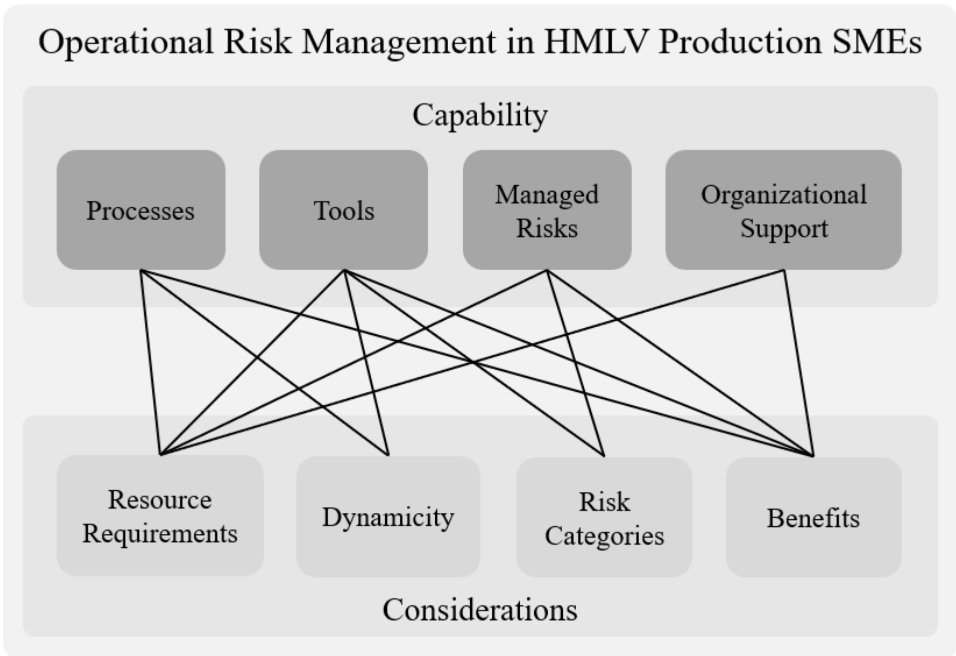

Figure 14. General framework for operational risk management in HMLV production SMEs.

4.4 Scientific implications

ICT and SCRM are common topics in the recent risk management literature and research. However, not a lot of literature exists on risk management in HMLV context or assessing risk management maturity in production operations. Both of these topics are discussed in this study. This study provides a literature review on the topic and a single case study of operational risk management in a HMLV production SME. The literature review contributes new by providing synthetizations for risk management tools, processes, and operational risk definitions. The empirical study contributes new by applying the maturity models constructed by Hillson (1997) and Cavalcante de Souza Feitosa et al. (2021) to operational risk management in a HMLV production SME. A general framework for managing operational risks in HMLV production SMEs is also proposed in section 4.3.

The case company's operational risk management was assigned in between the second and third maturity levels in section 3.5. This is in line with Pergler's (2012) generalization for the risk management maturity of similar organizations. As was stated by the QM, the processes in the company are constantly evolving. Several changes are currently being carried out, which applies to more than just the risk management process in the organization. Thus, Falkner and Hiebl's (2015) remark on evolving risk management practises in SMEs is also supported by this study. The findings of this study also complement the research by Ferreira de Araújo Lima et al. (2020) by identifying a focus on the initial phases of the risk management process. The iterative nature of a risk management process in practise, noted by ISO (2018b, p. 9) and ODASD(SE) (2014, p. 5), was also observed in this study.

Dvorsky et al. (2021), highlight the role of the recent global crises in the attitude towards risk management in both SMEs and larger companies. This is supported by this study, as the crises led to the development of BCPs in the case company, as was pointed out by the QM. The existence of a BCP can be considered contradicting to the remark made by Falkner and Hiebl (2015) on the work of Cioccio and Michael (2007), which deemed such plans less common in SMEs. The lack of practise for implementing the ISO 9001 risk-based thinking within European manufacturing SMEs, reported by Chiarini (2017), also does not apply to the case company. According to the QM, risk-based thinking is implemented in the company through identifying, assessing, and assigning actions to risks and opportunities. The investment and continual improvement of risk management practises present in the company is in line with the remarks made by Sifumba et al. (2017) regarding attitudes towards risk management present in the manufacturing industry. However, the remarks made by Sifumba et al. (2017) about insufficient risk management training, communication, and role assignment in manufacturing SMEs also receives support from this study. Although communication in general is direct and efficient in the company level due to the small size of the company, which is in line with the remarks made by Grube et al. (2017), the communication in risk management could be systematized.

Earlier research by Ben Said et al. (2016) highlights the need for dynamic maintenance practises in HMLV environments. This is supported by this study, as the role of maintenance was highlighted by the DPDTS. This is further linked to the claim made by Mu et al. (2009) on the needed flexibility of risk management practises on companies conducting NPD. Support for this claim can also be identified from this study as a more general approach is preferred in conducting PFMEAs and the use of error proofing methods like Poka Yoke jigs is limited due to high mix of products.

Ferreira de Araújo Lima et al. (2020) claim that SMEs are driven to adopt different tools than larger companies, and that the selected tools in SMEs are reactive, not preventive. Although the first claim could be supported by the resource limitations, the tools utilized by the case company are by no means limited to SMEs. However, the resource limitations may be visible in the extent to which the more resource intensive tools are utilized or systems they are integrated to. For example, in the case company FMEAs are managed in spreadsheets and specific FMEAs are only conducted for a limited number of major projects. This also supports the claims made in various literature sources, that conducting FMEAs is resource intensive (AIAG, 2019, p. 18; Carlson, 2015; IEC, 2009, p. 48). The claim of reactivity in risk management is also contradicted by the use of tools like RR and FMEA. However, reactivity is present in the current maintenance practises, so the claim is partially supported.

Johnson and Khan (2003) studied the use of PFMEA in the automotive industry in the United Kingdom and made several observations. Johnson and Khan (2003) report that the ratings made in the FMEA were subjective. This is supported by this study and linked to the conflicting statements between AIAG (2019, p. 17) and Ferreira de Araújo Lima et al. (2020) on whether the tool is qualitative or quantitative in nature. As stated by IEC

(2009, p. 46), the tool can provide either qualitative or quantitative information. This depends on whether the ratings are subjectively estimated or dynamically calculated, like in the works of Mili et al. (2008). Johnson and Khan (2003) also reported some confusion between the cause, effect, and failure mode in the FMEA tool execution. This was also recognized in this study, although the confusion diminished along the project due to learning. Another claim suggested improper training for the FMEA team (Johnson & Khan, 2003). This is also partially supported, as external FMEA training was conducted, but is not kept up regularly, and some of the trained people no longer work for the company. A lack of FMEA progress and effectiveness measurement, as reported by Johnson and Khan (2003), is also supported by this study. However, contradicting observation was made on the driver of FMEA implementation. According to Johnson and Khan (2003), the main driver seems to be external requirements rather than internal benefits. This does not apply to the case company, where FMEA is seldom conducted solely due to external requirements.

4.5 Research limitations

The limitations of this study are addressed in this section through construct validity, external validity, and reliability, as defined by Yin (2003, pp. 34–39). According to Yin (2003, p. 34) construct validity assesses the operational measures, external validity assesses the generalisability, and reliability assesses the repeatability of the study. A fourth dimension to assess research limitations would be internal validity, which assesses the presented causal relationships. However, Yin (2003, p. 36) states that internal validity is only applicable for causal studies trying to explain a causal relationship between events. Yin (2003, p. 36) also adds that internal validity may be extended to assessing any inferences made from the observations. However, this study does not attempt to propose causal explanations or inferences, so internal validity does not apply to this study.

Construct validity assesses whether correct operational measures were utilized for the studied subject (Yin, 2003, p. 34). To increase construct validity of a study, Yin (2003, p. 36) recommends using multiple sources of evidence, establishing a chain of evidence, and having the study report reviewed by key informants. Multiple sources of evidence were utilized, as the study contains a literature review with versatile sources, and an empirical study with documentary data, participative observations, and three semi-structured interviews. Also, two risk management maturity models were utilized with similar assessment results. However, some inaccuracy could be present in the assessment of the B3 dimension in the maturity model proposed by Cavalcante de Souza Feitosa et al. (2021), as the original SCRM operational risk categories were not utilized. The documentary data utilized in the study has limited accessibility from people external to the company due to privacy reasons. Also, the observations in this study were made by a single researcher, which can be considered as a limitation, as Eisenhardt (1989) advocates for using multiple investigators. According to Yin (2003, p. 94), participative observing could accurately portray the studied phenomenon and enables an internal viewpoint on the studied subject. However, Yin (2003, pp. 94–96) also points out that in participative observing, forming an external view can be difficult, and participation could draw attention from the observing. In this study, literature and maturity models were used to help in making versatile observations. In addition, participatory observing was not used as a sole source of evidence, which could patch some otherwise missed observations. People knowledgeable of the interview theme were selected as the interviewees and the questions were provided for them beforehand. A chain of evidence was built by first conducting the participatory observations and studying documentary data, and then interviewing the applicable people on the findings and gaps in the observations. Some of the development proposals were discussed with the appropriate personnel during the interviews and participative observing. The report draft and the development proposals have also been reviewed by the study supervisor working in the company.

External validity assesses the generalizability of the study results outside the study itself Yin (2003, p. 37). The literature review presented in this study contains generalizable information on operational risk management and risk management in general in different contexts. Some parts of the literature review focus on the SME or HMLV contexts, but those are also generalizable outside this study within the applicable contexts. As briefly discussed in section 4.3, the results of the empirical study have limited generalizability. Only one case is studied as a part of this research, which limits the generalizability of the results. The results are directly applicable to the case company’s environment, but might not all be applicable to another organization having different practises or operating in a dissimilar organizational context. However, some of the results are likely applicable to organizations with either similar practises or organizational context. In addition, support for the recommendations made were presented from previous literature. According to Eisenhardt (1989) discussing similar findings presented in the previous literature strengthens the internal validity, generalisability, and conceptual level of the study.

Similarly, discussing conflicting literature can help defining the limitations of the generalisability, while ignoring conflicting literature reduces the confidence of the findings (Eisenhardt, 1989). Similarities and conflicts between the study and previous literature are discussed in section 4.4.

Reliability assesses if same results would be achieved by repeating the same study with the described procedures by another researcher Yin (2003, p. 37). As Yin (2003, p. 38) points out, this requires documenting and presenting the followed procedures. The research approach and methods utilized in this study are described in sections 1.2 and 3.1. For the literature review, all utilized references are cited and listed in the reference list. In addition, the methods and databases utilized for obtaining the references are described. The references are also saved to a library in Mendeley Reference Manager software. For the empirical study, the data collection consists of documentary data, participatory observations, and semi-structured interviews. The utilized documentary data are named, and are internally available within the company databases. The participatory observing was done in a PFMEA project, presented in section 3.3. In a practical sense, it is not reasonable to expect someone to be able to precisely repeat the participative observing done in this study. However, similar results should be expected if the observations were made by another researcher, as the results were reviewed and discussed within the company without conflicting opinions. The interviewees are named in section 3.1, and the interview questions are presented in Appendix 1. The interviews were recorded and the recordings are stored in a Google Drive folder.

5 CONCLUSIONS

5.1 Key results

The purpose of this research was to study operational risk management in HMLV production SMEs. This was condensed into three RQs, presented in section 1.1. A literature review was conducted to form the theoretical foundation of the study. An empirical study, utilizing documentary data, participatory observations, and interviews, was then performed to study the risk management practises in a case company. The theoretical foundation and empirical observations were then compared to form development proposals for the operational risk management in the case company. The following paragraphs provide condensed answers to the RQs. Comprehensive answers to RQ1, RQ2, and RQ3 can be found in sections 2.6, 3.5, and 4.2, respectively.

The RQ1 aims to establish how operational risks should be managed in HLMV production SMEs according to previous literature. The context dictates the types of risks to manage as well as the required risk management capability. In the context related to this study, the relevant types of risks to be managed are depicted in Table 2 in section 2.6. The capability is formed from the comprehensiveness of managing different risk types the organization is subject to, the level of organizational support, and the processes and tools in place. The manufacturing industry does not have as high requirements for risk management as for example the energy industry. However, the benefits of higher risk management capability need to be compared to the associated costs, to reach a suitable level of capability.

The RQ2 aims to determine the current state of operational risk management in the case company. Risk management maturity models presented in Appendices 2 and 3 were utilized to assess the current state. The achieved maturity is presented as a matrix representing the fulfilment of requirements in different maturity model dimensions in Table 3 in section 3.5. The maturity was uniformly assigned on the second level. However, on some dimensions partial fulfilments were achieved also from the third and fourth maturity levels. The current maturity is on an expected level for the company in question, considering its context. However, areas for improvement could be recognized from the observations.

The RQ3 aims to propose improvements to the risk management practises in the case company's production operations. The proposed sequence of actions, their estimated level of resource requirements, and respective maturity model dimensions are presented in Figure 13 in section 4.2. The improvements are proposed in three stages, which have different level of urgency and resource requirements. The improvements are directed towards obtaining higher maturity levels, but the costs associated need to be considered. The most urgent improvements should target improving and formalizing the existing tools and processes. These include formal definitions of roles, communication, and processes, integrating risk management tools, and increasing the comprehensiveness of managed risks.

5.2 Future research

Some of the future research avenues are linked to the limitations of this study, presented in section 4.5. The main limitations suggesting for future research are the limitation of a single case and the limited accessibility of the case related data due to privacy reasons.

As recognized in the introduction section, more research on risk management in the HMLV context and on operational risk management maturity in production should be conducted. This study provides a single case study and a literature review regarding operational risk management in HMLV production SMEs. Studying more similar cases would help in building theory regarding the subject. The future studies should focus on the risk management processes and tools in place, as well as the managed risk types and the state of organizational support. More remarks on conducting similar studies can be found in section 4.3. Also, developing a maturity model specifically for operational risk management in production would be beneficial especially from the practical viewpoint of companies operating in the manufacturing industry. This new maturity model could be constructed according to the general framework for operational risk management in HMLV production SMEs, presented in section 4.3. The general framework could also be further studied and tested in practise. Finally, the utilization of the FMEA tool could be studied further. This could include observing the usage of the tool compared to recommended practises, as well as the application of the individual and overall FMEA processes in different companies and industries.

REFERENCES

AIAG. (2008). *Advanced Product Quality Planning (APQP) and Control Plan Reference Manual* (Second Edition).

AIAG. (2019). *Failure Mode and Effects Analysis ─ FMEA Handbook* (First Edition).

Alicke, K., Barriball, E., Lund, S., & Swan, D. (2020). Is your supply chain risk blind ─ or risk resilient? *McKinsey & Company*.

ASQ. (n.d.). *Quality Glossary*. Retrieved January 31, 2023, from https://asq.org/quality-resources/quality-glossary

Bailey, T., Barriball, E., Dey, A., & Sankur, A. (2019). A practical approach to supply-chain risk management. *McKinsey & Company – Our Insights*.

BCBS. (2006). *International Convergence of Capital Measurement and Capital Standards: A Revised Framework, Comprehensive Version*. Bank for International Settlements. http://www.bis.org/publ/bcbs128.pdf

ben Said, A., Shahzad, M. K., Zamai, E., Hubac, S., & Tollenaere, M. (2016). Experts' knowledge renewal and maintenance actions effectiveness in high-mix low-volume industries, using Bayesian approach. *Cognition, Technology and Work*, *18*(1), 193–213. https://doi.org/10.1007/s10111-015-0354-y

Bititci, U. S., Garengo, P., Ates, A., & Nudurupati, S. S. (2015). Value of maturity models in performance measurement. *International Journal of Production Research*, *53*(10), 3062–3085.

Brocal, F., González, C., Komljenovic, D., Katina, P. F., Sebastián, M. A., & Garciá-Alcaraz, J. L. (2019). Emerging Risk Management in Industry 4.0: An Approach to Improve Organizational and Human Performance in the Complex Systems. *Complexity*, *2019*. https://doi.org/10.1155/2019/2089763

Card, A. J., Ward, J. R., & Clarkson, P. J. (2012). Beyond FMEA: the structured what-if technique (SWIFT). In *Journal of Healthcare Risk Management* (Vol. 31, Issue 4, pp. 23–29). American Society for Healthcare Risk Management. https://doi.org/10.1002/jhrm.20101

Carlson, C. S. (2015, January). Understanding and Applying the Fundamentals of FMEAs. *2015 Annual Reliability and Maintainability Symposium*.

Cavalcante de Souza Feitosa, I. S., Ribeiro Carpinetti, L. C., & de Almeida-Filho, A. T. (2021). A supply chain risk management maturity model and a multi-criteria classification approach. *Benchmarking*, *28*(9), 2636–2655. https://doi.org/10.1108/BIJ-09-2020-0487

Chen, J., Sohal, A. S., & Prajogo, D. I. (2013). Supply chain operational risk mitigation: A collaborative approach. *International Journal of Production Research*, *51*(7), 2186–2199. https://doi.org/10.1080/00207543.2012.727490

Chiarini, A. (2017). Risk-based thinking according to ISO 9001:2015 standard and the risk sources European manufacturing SMEs intend to manage. *TQM Journal*, *29*(2), 310–323. https://doi.org/10.1108/TQM-04-2016-0038

Choi, T. M., Wallace, S. W., & Wang, Y. (2018). Big Data Analytics in Operations Management. *Production and Operations Management*, *27*(10), 1868–1883. https://doi.org/10.1111/poms.12838

Chowdhury, P., Lau, K. H., & Pittayachawan, S. (2019). Operational supply risk mitigation of SME and its impact on operational performance: A social capital perspective. *International Journal of Operations and Production Management*, *39*(4), 478–502. https://doi.org/10.1108/IJOPM-09-2017-0561

Cioccio, L., & Michael, E. J. (2007). Hazard or disaster: Tourism management for the inevitable in Northeast Victoria. *Tourism Management*, *28*(1), 1–11. https://doi.org/10.1016/j.tourman.2005.07.015

Cook, R. I. (1998). How Complex Systems Fail. *Cognitive Technologies Laboratory, University of Chicago*, 64–118. https://how.complexsystems.fail

DAU. (2022a). *ESOH Risk Assessment*. DAU Systems Engineering Brainbook. https://www.dau.edu/tools/se-brainbook/Pages/Management%20Processes/esoh-risk-assessment.aspx

DAU. (2022b). *Risk Management Overview*. DAU Systems Engineering Brainbook. https://www.dau.edu/tools/se-brainbook/Pages/Management%20Processes/Risk-Management.aspx

de Aguiar, D. C., Salomon, V. A. P., & Mello, C. H. P. (2015). An ISO 9001 based approach for the implementation of process FMEA in the Brazilian automotive industry. *International Journal of Quality and Reliability Management*, *32*(6), 589–602. https://doi.org/10.1108/IJQRM-09-2013-0150

de Oliveira, U. R., Marins, F. A. S., Rocha, H. M., & Salomon, V. A. P. (2017). The ISO 31000 standard in supply chain risk management. *Journal of Cleaner Production*, *151*, 616–633. https://doi.org/10.1016/j.jclepro.2017.03.054

Dietrich, D. M., & Cudney, E. A. (2011). Methods and considerations for the development of emerging manufacturing technologies into a global aerospace supply chain. *International Journal of Production Research*, *49*(10), 2819–2831. https://doi.org/10.1080/00207541003801275

Dvorsky, J., Belas, J., Gavurova, B., & Brabenec, T. (2021). Business risk management in the context of small and medium-sized enterprises. *Economic Research-Ekonomska Istraživanja*, *34*(1), 1690–1708. https://doi.org/10.1080/1331677X.2020.1844588

Eisenhardt, K. M. (1989). Building Theories from Case Study Research. In *The Academy of Management Review* (Vol. 14, Issue 4).

Esposito, P. (2007). Integrating a Balanced Scorecard Approach to Risk Management in an OHSAS 18000/ANSI Z-10 Management System. *Safety 2007*. https://aeasseincludes.assp.org/proceedings/2007/docs/730.pdf

European Banking Authority. (2017). *Guidelines on Credit Institutions' Credit Risk Management Practices and Accounting for Expected Credit Losses*.

https://www.eba.europa.eu/regulation-and-policy/accounting-and-auditing/guidelines-on-accounting-for-expected-credit

Falkner, E. M., & Hiebl, M. R. W. (2015). Risk management in SMEs: a systematic review of available evidence. In *Journal of Risk Finance* (Vol. 16, Issue 2, pp. 122–144). Emerald Group Publishing Ltd. https://doi.org/10.1108/JRF-06-2014-0079

Ferreira de Araújo Lima, P., Crema, M., & Verbano, C. (2020). Risk management in SMEs: A systematic literature review and future directions. *European Management Journal*, *38*(1), 78–94. https://doi.org/10.1016/j.emj.2019.06.005

General Motors Corporation. (2008). *Potential Failure Mode and Effects Analysis (FMEA) Reference Manual* (Fourth Edition). AIAG.

Grube, D., Malik, A. A., & Bilberg, A. (2017). Generic challenges and automation solutions in manufacturing SMEs. *Annals of DAAAM and Proceedings of the International DAAAM Symposium*, 1161–1169. https://doi.org/10.2507/28th.daaam.proceedings.161

He, Z., Qi, E., & Liu, Z. (2002). Continuous Improvement Through Integration of Quality Tools. *International Journal of Quality Innovation*, *3*(2), 38–45.

Hillson, D. (1997). Towards a risk maturity model. *The International Journal of Project & Business Risk Management*, *1*(1), 35–45.

Hillson, D. (2014). Managing risk. In *Gower Handbook of Project Management* (Fifth Edition, pp. 281–304). Gower Publishing, Ltd.

Ho, W., Zheng, T., Yildiz, H., & Talluri, S. (2015). Supply chain risk management: A literature review. *International Journal of Production Research*, *Vol. 53*(No. 16), 5031–5069.

Hwang, S. (2011). Identifying and Communicating Key Risk Indicators. In *Enterprise Risk Management* (pp. 125–140). https://doi.org/10.1002/9781118267080

IEC. (2009). Risk Management — Risk Assessment Techniques. *IEC 31010:2009*. https://www.iso.org/standard/72140.html

ISO. (2009). Quality management systems — Particular requirements for the application of ISO 9001:2008 for automotive production and relevant service part organizations. *ISO/TS 16949:2009*. https://www.iso.org/standard/52844.html

ISO. (2015a). Quality management systems — Requirements. *ISO 9001:2015*. https://www.iso.org/standard/62085.html

ISO. (2015b). The Process Approach in ISO 9001:2015. *ISO 9001:2015*. https://www.iso.org/files/live/sites/isoorg/files/standards/docs/en/iso_9001_2015_process_appr.pdf

ISO. (2018a). Occupational health and safety management systems — Requirements with guidance for use. *ISO 45001:2018*. https://www.iso.org/standard/63787.html

ISO. (2018b). Risk Management — Guidelines. *ISO 31000:2018*. https://www.iso.org/standard/65694.html

Javaid, M. I., & Iqbal, M. M. W. (2017). A Comprehensive People, Process and Technology (PPT) Application Model for Information Systems (IS) Risk Management in Small/ Medium Enterprises (SME). *2017 International Conference on Communication Technologies (ComTech)*, 78–90. https://doi.org/10.1109/COMTECH.2017.8065754

Jobst, A. A. (2007). Operational Risk-The Sting is Still in the Tail but the Poison Depends on the Dose. *Journal of Operational Risk*. http://ssrn.com/abstract=944486

Johnson, K. G., & Khan, M. K. (2003). A study into the use of the process failure mode and effects analysis (PFMEA) in the automotive industry in the UK. *Journal of Materials Processing Technology*, *139*(1-3 SPEC), 348–356. https://doi.org/10.1016/S0924-0136(03)00542-9

Karjalainen, E. (2023, January 5). *Juurisyyanalyysi ja sen kehittyminen*. Quality Knowhow Karjalainen. https://qkk.fi/juurisyyanalyysi-ja-sen-kehittyminen/

Kenge, R., & Khan, Z. (2020). Manufacturing Excellence Model to Solve Operational Risks Due to Product Demand Variations. *Parikalpana: KIIT Journal of Management*, *16*(1 & 2), 138. https://doi.org/10.23862/kiit-parikalpana/2020/v16/i1-2/204565

Madsen, C. U., Kirkegaard, M. L., Dyreborg, J., & Hasle, P. (2020). Making occupational health and safety management systems 'work': A realist review of the OHSAS 18001 standard. *Safety Science*, *129*. https://doi.org/10.1016/j.ssci.2020.104843

Marotta, D. (2020). *Supply Chain Risk Management: 10 Strategies for Success – Hitachi Solutions*. https://global.hitachi-solutions.com/blog/supply-chain-risk-management/

Mentzer, J. T., Dewitt, W., Keebler, J. S., Min, S., Nix, N. W., Smith, C. D., & Zacharia, Z. G. (2001). Defining Supply Chain Management. *Journal of Business Logistics*, *22*(2), 1.

Mili, A., Bassetto, S., Siadat, A., & Tollenaere, M. (2009). Dynamic risk management unveil productivity improvements. *Journal of Loss Prevention in the Process Industries*, *22*(1), 25–34. https://doi.org/10.1016/j.jlp.2008.07.011

Mili, A., Siadat, A., Hubac, S., & Bassetto, S. (2008). Dynamic management of detected factory events and estimated risks using FMECA. *The 4th IEEE International Conference on Management of Innovation & Technology*, 1204–1209.

Morgan, J. (2007). Manufacturing Readiness Levels (MRLs) Manufacturing Readiness Assessments (MRAs). *Air Force Research Laboratory*.

Mu, J., Peng, G., & MacLachlan, D. L. (2009). Effect of risk management strategy on NPD performance. *Technovation*, *29*(3), 170–180. https://doi.org/10.1016/j.technovation.2008.07.006

Munro, R. A., Ramu, G., & Zyrmiak, D. J. (2015). *The Certified Six Sigma Green Belt Handbook* (Second Edition). ASQ Quality Press.

ODASD(SE). (2014). *Department of Defense Risk Management Guide for Defense Acquisition Programs, 7th ed.* https://acqnotes.com/wp-content/uploads/2014/09/DoD-Risk-Mgt-Guide-v7-interim-Dec2014.pdf

OSDMTP. (2022). *Manufacturing Readiness Level (MRL) Deskbook Version 2022*. https://www.dodmrl.com/MRL%20Deskbook%20V2020.pdf

Peeters, J. F. W., Basten, R. J. I., & Tinga, T. (2018). Improving failure analysis efficiency by combining FTA and FMEA in a recursive manner. *Reliability Engineering and System Safety*, *172*, 36–44. https://doi.org/10.1016/j.ress.2017.11.024

Pergler, M. (2012). Enterprise Risk Management ─ What's different in the corporate world and why. *McKinsey & Company*. https://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/risk/working%20papers/40_whats%20different%20in%20the%20corporate%20world.ashx

PMI. (2013). Project Risk Management. In *A Guide to the Project Management Body of Knowledge (PMBOK® guide)* (Fifth Edition, pp. 309–355).

PMIS Consulting. (2014). *Project Risk Management: A Practical Guide*. https://www.pmis-consulting.com/articles/project-risk-management/

Rampini, G. H. S., Takia, H., & Berssaneti, F. T. (2019). Critical Success Factors of Risk Management with the Advent of ISO 31000 2018 - Descriptive and Content Analyzes. *Procedia Manufacturing*, *39*, 894–903. https://doi.org/10.1016/j.promfg.2020.01.400

Ricondo, I., Arrieta, J. A., & Aranguren, N. (2006). NPD Risk Management: Proposed Implementation to Increase New Product Success. *In 2006 IEEE International Technology Management Conference (ICE)*, 1–8. https://www.researchgate.net/publication/228415612

Segismundo, A., & Miguel, P. A. C. (2008). Failure mode and effects analysis (FMEA) in the context of risk management in new product development: A case study in an automotive company. *International Journal of Quality & Reliability Management*, *25*(9), 899–912. https://doi.org/10.1108/02656710810908061

Sidor, L., & Lewus, P. (2007). Using Risk Analysis in Process Validation. *Biopharm International*, *20*(2), 50–57.

Sifumba, C. M., Mothibi, K. B., Ezeonwuka, A., Qeke, S., & Matsoso, M. L. (2017). The risk management practices in the manufacturing SMEs in Cape Town. *Problems and Perspectives in Management*, *15*(2), 386–403. https://doi.org/10.21511/ppm.15(2-2).2017.08

Skhmot, N. (2017, August 5). *The 8 Wastes of Lean*. The Lean Way Blog. https://theleanway.net/The-8-Wastes-of-Lean

Stewart, H. (2020). On the definition of risk. In *Journal of Risk Management in Financial Institutions* (Vol. 13).

Tague, N. R. (2005). *The Quality Toolbox* (Second Edition). ASQ Quality Press.

Taylor, W. A. (1998). *Methods and Tools for Process Validation*. Taylor Enterprises. https://variation.com/methods-and-tools-for-process-validation/

Tuomi, J., & Sarajärvi, A. (2018). *Laadullinen tutkimus ja sisällönanalyysi: Uudistettu laitos*. Tammi.

Tupa, J., Simota, J., & Steiner, F. (2017). Aspects of Risk Management Implementation for Industry 4.0. *Procedia Manufacturing*, *11*, 1223–1230. https://doi.org/10.1016/j.promfg.2017.07.248

University of Oulu. (n.d.). *Industrial Engineering and Management*. Retrieved February 13, 2023, from https://www.oulu.fi/en/university/faculties-and-units/faculty-technology/tuotantotalous

Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. In *Source: MIS Quarterly* (Vol. 26, Issue 2). http://www.jstor.org/stable/4132319

Wieczorek-Kosmala, M. (2014). Risk management practices from risk maturity models perspective. *Journal for East European Management Studies*, 133–159. https://doi.org/10.5771/0949-6181-2014-2-133

Xu, Y., Pinedo, M., & Xue, M. (2017). Operational Risk in Financial Services: A Review and New Research Opportunities. *Production and Operations Management*, *26*(3), 426–445. https://doi.org/10.1111/poms.12652

Yin, R. K. (2003). *Case Study Research – Design and Methods: Vol. Volume 5* (Third Edition). Sage Publications.

1. **Risk management tools and managed risks**
    1.1. Who are you and what is your role in the company?
    1.2. Is there an overall process for conducting FMEAs in the company?
        1.2.1. Has it been documented?
        1.2.2. How are FMEA projects selected? Have selection criteria been determined?
    1.3. Have the roles and responsibilities for conducting FMEAs been determined?
        1.3.1. Have they been documented?
        1.3.2. What are the roles and responsibilities?
    1.4. What is the scope of different types of risks managed through FMEA?
        1.4.1. Are supply related risks included?
    1.5. How has the FMEA team been selected?
        1.5.1. Should the FMEA team include more representation from design and supply operations?
    1.6. Who have received FMEA training?
    1.7. Should FMEA meetings be conducted regularly?
    1.8. Are initial FMEA meetings conducted at the beginning of new FMEA projects?
        1.8.1. What is decided in the meetings?
    1.9. What is the relationship between DFMEAs, PFMEAs, and CPs in the company?
        1.9.1. Are unmitigated risks transferred from DFMEA to PFMEA?
        1.9.2. Could these be more linked in the future?
    1.10. Should PIR be utilized better as an input method for FMEAs, CPs, and maintenance activities?
    1.11. How was communication with the customer conducted during the FMEA project?
        1.11.1. Were FMEA scales and their applicability discussed?
        1.11.2. Has a common understanding of the severity ratings been established?
        1.11.3. Are supplier FMEAs conducted?
    1.12. Should the AIAG scales be modified for the industry?
    1.13. Are scrap reports or failure data collected?
        1.13.1. Is the data analysable for determining failure mode occurrence or ensuring FMEA comprehensiveness?
    1.14. Are any other MSA practises than Mini GRR studies utilized?

1.15. What are your thoughts on the utilization of Foundation FMEAs and Maintenance FMEAs?

2. **Utilization of MRL and TRL assessments**
   - 2.1. Who are you and what is your role in the company?
   - 2.2. When are MRL and TRL assessments conducted?
   - 2.3. How are MRL and TRL assessments conducted in the company?
     - 2.3.1. What is the process?
     - 2.3.2. What departments are represented in the team conducting the assessments?
   - 2.4. How are MRL and TRL assessments utilized from a risk management perspective?
   - 2.5. Has a non-product-specific MRL or TRL assessment been conducted?
     - 2.5.1. If not, would this be feasible?
3. **Risk management process and organizational support**
   - 3.1. Who are you and what is your role in the company?
   - 3.2. Does the company have a formalized risk management process?
     - 3.2.1. Has the process been documented?
   - 3.3. Does the company have a general risk management policy?
     - 3.3.1. If not, would it be feasible to be created?
   - 3.4. What kinds of KPIs are related to production operations?
     - 3.4.1. How are KPIs utilized?
     - 3.4.2. Are any risk metrics like KRIs utilized?
   - 3.5. How is the ISO 9001 risk-based thinking visible in the company?
     - 3.5.1. How are action plans to address risks and opportunities conducted in the company?
   - 3.6. What internal and external audits are regularly conducted?
     - 3.6.1. Why are audits conducted?

Appendix 2. Risk management maturity model summarized from Hillson (1997).

Dimension	**1st Level**	**2nd Level**	**3rd Level**	**4th Level**
Overall	Unaware of the need for risk management, no structured approaches, and no attempt to learn from past or prepare for future.	Experimenting through a small number of individuals, no generic structured process, aware of potential benefits, and ineffective implementation.	Risk management built into routine business processes, formalized process utilized in almost all projects, and benefits understood in all levels.	Risk-aware culture with proactive approach, risk information actively used for process improvement, and emphasis on opportunity management.
Culture (A1)	No risk awareness and resistant to change.	Risk management used on selected projects, and seen as additional overhead with variable benefits.	Accepted risk management policy, benefits recognised and expected, and prepared to commit resources.	Top-down commitment, leadership by example, and proactivity encouraged and rewarded.
Process (A2)	No formal processes.	No generic formal process, some specific formal methods, and dependent on risk team skills.	Generic formal processes incorporated into QMS and applied on most projects, allocation of risk budgets, and less need for support.	Risk-based business processes, Total Risk Management, regular process updates, and routine risk metrics.
Experience (A3)	No understanding of risk principles.	Limited to individuals with little formal training.	Risk management as core expertise, formal training, specifically developed processes and tools.	All staff risk-aware, learning from experience, and regular external training.
Application (A4)	No dedicated risk management resources or tools.	Inconsistent application and ad hoc collection of tools.	Routine application to all projects, committed resources, and integrated tools.	Applied to all activities, reporting and decision making based on risk, and state-of-the-art tools.

Appendix 3. SCRM maturity model summarized from Cavalcante de Souza Feitosa et al. (2021).

Dimension	**1st Level**	**2nd Level**	**3rd Level**	**4th Level**
Organizational Support (B1)	No communication of risk processes or their performance, no commitment from top management, and no awareness of roles and responsibilities.	Growing concern of risk management, lacking commitment and accountability, inefficient communication, and no performance monitoring of risk management.	Risk management partially integrated to organizational routine, process recorded, and more awareness of roles.	Risk management completely integrated to organizational routine, consistent communication, performance monitored, and strong commitment and awareness of roles.
Risk Management Process (B2)	Risks not identified, no tools, no assessment of likelihood and consequence, no mitigation, and no records or reporting of occurred risks.	More risks identified, simple tools applied, advanced tools experimented, likelihood and consequence assessed, mitigation applied, and no records or reporting of occurred risks.	Risks fully identified, simple and advanced tools effectively used, risk prioritization according to assessment, mitigation effectively implemented, and some documentation of occurred and identified risks.	Maintains risk management process documentation and verifies effectiveness of practises.
Managed Risks (B3)	No action to manage any operational risks.	Actions to manage and minimize some operational risks.	Actions to manage and minimize all operational risks.	Actions to manage and minimize all operational and disruption risks.