Carmen E. Castaño R.

Model-Based Risk in MedTech

A Model-Based Approach to Comprehensive Risk Management for Medical Devices

„A Model-Based Approach to Comprehensive Risk Management for Medical Devices“

„Ein modelbasierter Ansatz zur Verwirklichung eines umfassenden Risikomanagements für Medizingeräte“

Von der Fakultät für Maschinenwesen der Rheinisch-Westfälischen Technischen Hochschule Aachen zur Erlangung des akademischen Grades einer Doktorin der Ingenieurwissenschaften genehmigte Dissertation

vorgelegt von

Carmen Elizabeth Castaño Reyes

Berichter: Univ.-Prof. Dr.-Ing. Robert Heinrich Schmitt
Prof. Dr. rer. nat. Elba del Carmen Valderrama Bahamóndez

Tag der mündlichen Prüfung:16 Februar 2021

Carmen Elizabeth Castaño Reyes:

A Model-Based Approach to Comprehensive Risk Management for Medical Devices

1st edition, 2021

Published as e-book, specimen copies printed resp. in Panama and Germany

Carmen E. Castaño R.
Parque Lefèvre c. 9na #45C39
Panama City, Panama, Panama

carmen.castano@rwth-aachen.de

Suggested Citation:

Castaño, C.: A Model-Based Approach to Comprehensive Risk Management for Medical Devices. Dissertation, Faculty of Mechanical Engineering, RWTH Aachen University, Aachen, 2021

This work is made available by RWTH Publications as well as the National Library of Panama (#24899).

DOI: 10.18154/RWTH-2021-04766 doi.org/10.18154/RWTH-2021-04766

ISBN: 978-9962-13-825-9

D 82 (Diss. RWTH Aachen University,2021)

Preface

This dissertation was created during my work as a research associate at the Fraunhofer Institute for Production technology (IPT) as well as a student at the CDS at RWTH Aachen University. I would like to use these lines to thank my dear friends and colleagues, without whose support such work would not have been possible.

First of all, I would like to thank Prof. Schmitt for the given support. It was his backing letting me move – equipped with the tools of IPT – in a little researched cross-section of RM, MBSE and Health, together with the freedom to choose and lead my small, but quite interdisciplinary team, that contributed considerably to the success of the research project.

Also, my thanks go to Prof. Corves as chairman of the examination committee and Prof. Valderrama as the second examiner. Thanks to the former heads of department, Dr.-Ing. Markus Große Böckmann and Dr.-Ing. Eike Permin, who gave me constructive criticism in the development of my research.

I would like to thank my colleagues at IPT for their cooperation. I am grateful that I had the chance to strengthen the friendship to my fellow master student and colleague Beijan. Thank you for our discussions, for mastering the challenges in the dissertation process together, for your laudatory speech and simply for a great time.

The main contribution to the success of any research project is, of course, a skilled team. My thesis students, interns and my student assistant have dedicated their talent, vigor and a great deal of time to the MBR project. In particular, I would like to thank Poornima and Nandakishore for their huge commitment. I wish them all the very best for their careers and their personal lifes.

Furthermore, the project would not have been possible without the collaboration with several other research groups and projects. I would like to express my gratitude for the trusting and friendly cooperation with my fellow researchers in Aachen, Bonn, Lisbon, Munich and elsewhere; special thanks go to Bastian Nießing and Andreas Elanzew of the SCFIII project.

Also, I would like to express my appreciation to the National Secretariat for Science, Technology and Innovation (SENACYT) of my home country Panama, whose scholarship has financed my stay in Germany.

For all your support, heart and mindfulness, thanks to all my friends! Thank you, Michael, Gloria, Ingrid and Rhona, for all your practical and moral support!

Finally, my greatest thanks go to my little family: to my husband Marcel, who was and is always there for me and without whose unconditional support this work would never have come about, and to my daughter Lucía, whose joy and love warm and carry us.

Panama City, August 2021 Carmen E. Castaño R.

Summary

Medical devices are becoming more complex than ever, as do the networks they pertain to. The current trends in MedTech manufacturing complicate the work of a systematical and comprehensive RM process. At present, manufacturers implement many different, but exclusively document-based RM approaches.

The work described in this thesis focuses on conceiving and validating a model-based risk management system that enables RM operators to overcome the endemic deficits of the document-based approaches. This shall be achieved by the formalization of RM steps, the role-based separation of procedures in computation and human action and by providing an RM system that enables an iterative RM process during the entire product lifecycle for all stakeholders. The research approach adopted mainly comprises an extensive study of relevant literature, reasoning and an implementation of applied research, carried out in a case study.

A systematical and comprehensive RM for medical devices can be accomplished with a MBR concept. The iterative system design separates the operational and computational procedures in the MBR Core from the actions of the experts and stakeholders. A universal API processes all changes to and all documents generated from the MBR core. The sequential use of human expertise and computational rigor allows for the integration of document-based RM methods and techniques that are broadly accepted in the industry. A main factor for comprehensive RM results is the computerization of the identification of critical characteristics. The elements of the physical product are tagged with approved industry classifications. A novelty in product modeling is the utilization of an own block class for interactions instead of relational elements; it has proven to be functional and valuable in implementation.

The software implementation of the system is shown on a demonstrator level. The validation of MBR in a case study applying two RM methods on two similar complex medical device systems, advanced prototypes of automated stem cell platforms, has shown the potential to drastically reduce the deficits endemic to document-based approaches. The augmentation of established RM techniques with legacy information can improve identification of critical characteristics. However, the case study also showed that the disposition of the panelists is key to the success of the concept. While proficient users of tools in MBSE explored the full potential in the utility tests, panelists with a basic to intermediate knowledge of MBSE, showed strong reservations against accepting “advise” from the augmented graphical model.

In total, the model-based RM approach can be a significant contribution to the improvement of RM processes for complex medical devices and, in general, to the dissemination of risk-based thinking throughout all lifecycle stages, provided that all stakeholders engage in an open-minded and interdisciplinary process.

Zusammenfassung

Medizingeräte werden immer komplexer und ebenso verhält es sich mit den Netzwerken, zu denen sie zusammengeschlossen werden. Dies erschwert zunehmend – zusammen mit anderen Entwicklungen in der MedTech-Branche – systematische und umfassende RM-Prozesse. Die eingesetzten, ausnahmslos dokument-basierten Herangehensweisen können diese Zielkonflikte nicht lösen.

Diese Schrift beschreibt daher das Konzipieren und Prüfen eines modelbasierten RM-Systems, welches es Anwendern erlaubt, die ureigenen Defizite der dokument-basierten Ansätze zu überwinden. Erreicht werden soll dies durch die Formalisierung der Prozessschritte, die rollenbasierte Trennung der Abläufe in Rechenleistung und menschliche Arbeit sowie die Bereitstellung eines iterativen RM-Prozesses, der durch den gesamten Produktlebenszyklus und für alle Beteiligten trägt. Die gewählte Metoden zur Erforschung umfassen eine ausführliche Auswertung der relevanten Literatur, logische Argumentation und deren Umsetzung in angewandte Forschung, die in einer Fallstudie mündet.

Die Arbeit zeigt, dass die o.g. Forderungen an das RM für Medizingeräte durch ein MBR-Konzept erfüllt werden können. Das iterativ ausgelegte System trennt operative und rechnerische Abläufe im Systemkern von den Einwirkungen durch Experten und Stakeholder. Alle Änderungen am Systemkern und alle erstellten Dokumente werden durch eine API gehandhabt. Dieses Vorgehen erlaubt die Einbindung der in der Industrie verbreiteten Methoden und Techniken in den einzelnen RM-Schritten, ohne die Schwächen ihrer Dokumente zu übernehmen. Ein wesentlicher Faktor für allumfassendes RM ist die hierfür konzipierte Automatisierung der Identifikation von kritischen Produkteigenschaften. Hierzu erkennt erstmals ein Softwarewerkzeug strukturelle und semantische Ähnlichkeiten zwischen dem zu bewertenden Modell und Bestandsdaten und weist die zu erwartenden Interaktionen und deren Kritikalität aus. Eine Klassifizierung aller physischen Elemente nach Industriestandards verbessert die risikotechnische Bewertung der kritischen Eigenschaften. Diese Neuerungen haben sich in Tests als funktional und hilfreich für den Gesamtprozess erwiesen.

Die Implementierung des Systems wird auf dem Niveau eines Software-Demonstrators gezeigt. Die Validierung des MBR-Konzepts erfolgte in einer Fallstudie, in der zwei RM-Methoden an einander ähnlichen, komplexen Medizingerätenetzwerken (einsatzfähige Prototypen von Stem Cell Factories) vergleichend angewandt und bewertet wurden. Hier konnte eine drastische Reduzierung der anvisierten Defizite gezeigt werden. Das Augmentieren von etablierten RM-Techniken mit Informationen aus Bestandsdaten kann die Identifikation von kritischen Produkteigenschaften verbessern. Entscheidend für den Erfolg in der Praxis ist allerdings auch die Einstellung der Teilnehmer zum Konzept. Während jene Nutzer, die MBSE-Werkzeuge schon vorher kompetent verwendeten, die neuen Informationsformen in vollem Umfang nutzten, musste bei unerfahrenen oder wenig erfahrenen oft eine starke Aversion dagegen festgestellt werden, aus einem Modell heraus "Ratschläge anzunehmen".

Insgesamt können modelbasierte Ansätze als signifikanter Beitrag zur Verbesserung von RM-Prozessen für komplexe Medizingeräte im Speziellen und zur Verbreitung von risikobasiertem Denken im gesamten Produktlebenszyklus im Allgemeinen angesehen werden. Voraussetzung dafür ist, dass alle Beteiligten einem interdisziplinären RM-Prozess gegenüber aufgeschlossen sind.

I Content

II List of Abbreviations

Abbreviation	Description
AADL	Architecture Analysis & Design Language
ACQMM	Aachen Quality Management Model
AIMDD	Active Implantable Medical Devices Directive
API	Application Programming Interface
BHWG	Biomedical-Healthcare Working Group
CA	Criticality Evaluation
CAD	Computer-Aided Design
CAE	Computer-Aided Engineering
CAM	Computer-Aided Manufacturing
CAP	Computer-Aided Planning
CAPP	Computer-Aided Process Planning
CAQ	Computer-Aided Quality Assurance
CAx	Set of all (used) computer-aided production tools
CEN	Comité Européen de Normalisation (*French:* European Committee for Standardization)
CNMD	Classification Names for Medical Devices
CRM	Customer Relationship Management
CUI	Concept Unique Identifier

Abbreviation	Description
D	Detection
DB	Database
DIN	Deutsches Institut für Normung (*Germ.:* German Institute for Standardization)
ECMO	Extracorporeal Membrane Oxygenation
EDMA	European Diagnostic Manufacturers Association
EPO	European Patent Office
E-R	Entity-Relationship
ERP	Enterprise Resource Planning
EU	European Union
FDA	Food and Drug Administration
FEM	Finite Element Method
Finc	find in catalog (alliance for bibliographic search engines)
FM	Failure Mode
FMEA	Failure Mode and Effects Analysis
FMECA	Failure Mode, Effects and Criticality Analysis
FTA	Fault Tree Analysis
GEHC	General Electric Health Care
GHTF	Global Harmonization Task Force

Abbreviation	Description
GMDN	Global Medical Device Nomenclature System
GMP	Good Manufacturing Practice
GMT	General Model Theory
HAZOP	Hazard and Operability Studies
HGM	Hierarchy Gap Method
hiPSCs	Human-Induced Pluripotent Stem Cells
HMI	Human-Machine Interface
ICT	Information and Communication Technologies
ID	Identifier
IDDS	Infusion and Drug Delivery System
DIE	Integrated Development Environment
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
iFEM	Innovative Function-Effect Modeling
IMDRF	International Medical Device Regulators Forum
INCOSE	International Council on Systems Engineering
IPT	Institute for Production Technology
ISO	International Standard Organization
IT	Information Technology

Abbreviation	Description
IVD	In-Vitro Diagnostics
IVDMD	In-Vitro Diagnostic Medical Devices Directive
JFMDA	Japanese Medical Device Nomenclature
KB	Knowledge Base
LHU	Liquid Handling Unit
MBR	Model-Based Risk (Management)
MBRA	Model-Based Risk Assessment
MBSE	Model-Based Systems Engineering
MD	Medical Device
MDD, *also:* MEDDEV	Medical Devices Directive(s)
MedTech	Medical Technology
MES	Manufacturing Execution System
MRM	Mission Reliability Method
MTP	Microtiter Plate
NKKN	Norsk Klassifisering Koding and Nomenklatur (*Nw.:* Norwegian Classification, Coding and Nomenclature)
O	Occurrence
OBO	Open Biomedical Ontologies
OCL	Object Constraint Language
OEM	Original Equipment Manufacturer

Abbreviation	Description
OMG	Object Management Group
OOSEM	Object-Oriented Systems Engineering Method
OPM	Object-Process Methodology
OSLC	Open Services for Lifecycle Collaboration
OWL	Web Ontology Language
PBS	Product Breakdown Structure
PDM	Product Data Management
PHP	Hypertext Preprocessor
PLM	Product Lifecycle Management
PMTE	Process, Methods, Tools and Environment
QMS	Quality Management System
QRC	Quick Risk Check
RBAC	Role-Based Access Control
RDF	Resource Description Framework
RM	Risk Management
RMCM	Risk Management Capability Model
RPN	Risk Priority Number
RUPSE	Rational Unified Process for Systems Engineering
RWTH	Rheinisch-Westfälische Technische Hochschule (*also:* RWTH Aachen University)

Abbreviation	Description
S	Severity
SA	State Analysis
SCD	Stem Cell Discovery (Platform in Aachen)
SCFIII	Stem Cell Factory (Platform in Bonn)
SCM	Supply-Chain-Management
SDL	Specification and Description Language
SE	Systems Engineering
SMEs	Small and Middle-Sized Enterprises
SNOMED CT	Systemized Nomenclature of Medicines Clinical Terms
SO	[Severity] * [Occurrence], sts. also PS for [Probability of Occurrence] * [Severity]
SOD	[Severity] * [Occurrence] * [Detection]
SPI	Software Process Improvement
SysML	Systems Modeling Language
TEMA	Themenpaket "Technik und Management" (*Germ.:* topic cluster „Technology and Management“, literature meta-database)
UID	Unique Identifier
UMDNS	Universal Medical Devices Nomenclature System
UML	Unified Modeling Language

Abbreviation	Description
UMLS	Unified Medical Language System
URI	Uniform Resource Identifier
UTF-8	8-Bit Unicode Transformation Format
UTS	→UMLS Terminology Services
VDI	Verein Deutscher Ingenieure
WHO	World Health Organization
XMI	→XML Metadata Interchange
XML	Extended Markup Language

III List of Figures

IV List of Tables

V List of Snippets

1 Introduction

1.1 Current Situation

The European medical technology industry consists of around 27,000 companies, more than 95% of them small and medium-sized enterprises (SMEs), with over 675,000 employees [MEDT17]. In the European Union (EU) alone, medical devices constituted by far the biggest part of the medical technology (MedTech) sector with a market of 95 billion euros in annual sales in 2015 [EURO15].

Like with many high-tech products, the global medical devices market is characterized by trends that complicate the task of systematical and comprehensive risk management (RM) significantly. These are shorter innovation cycles and subsequently shorter expected product life, shorter time to market, more complex devices, device networks and product lifecycles, more stakeholders with different professional backgrounds, customer expectations of low-maintenance high-tech products [BEIH14; SORL09, p.60].

Moreover, stakeholders progressively demand extended functionality, higher reliability, shorter product lifecycles, and lower prices throughout different domains. This leads to considerable levels of complexity and interdependence of system elements as well as cost, schedules and quality demands [BEIH14]. As a result, for manufacturers, all these needs translate to costs in product conception [SORL09, p.60]. Paradoxically, a systematically and comprehensively performed RM process will help SMEs cope with those needs.

In order to raise quality and diminish cost and time of delivery to market, it is advantageous to steer product development and process development with modern information and communication technologies (ICT). It is required to obtain product data from dissimilar companies' computer systems during the entire product lifecycle. However, the trend of growing utilization of information technology (IT) tools in engineering companies requires massive advancement in information and knowledge management tools to approximate the single-source-of-truth paradigm [MA08; NAGY92]. This challenge impedes technological progress and business efficiency. [SAJA13]

Engineers use heterogeneous engineering software tools (mostly provided by different vendors), and customer and vendor toolsets need to interact in extensive supply chains [BAJA16]. This, again, is not limited to MedTech but applies to all fields in manufacturing. For example, flaws in the interchange of product data throughout the supply chain can hinder the innovative design and development process. A study on the interoperability costs in the U.S. automotive supply chain found the compensations to exceed $1 billion per year. Besides, it slowed down the launching of new models by about two months. [BRUN02]

RM has become a key tool for conquering the previously mentioned challenges [OEHM10] and necessitates multidisciplinary expertise for it [RAKI06]. Most of the RM methods utilized in the RM process are document-centric. Document-based RM methods and techniques have some

endemic deficits. First and foremost, almost all of them are based on non-comprehensive approaches. Moreover, the risk identification process is often integrated into other steps and the source of expert knowledge and evaluation are identical (bias by design). Also, many techniques have got an insufficient level of formalization leading to a low reproducibility of RM results. Finally, the uncertainty of the level of coverage cannot be quantified, as document-based approaches will not convey any information a certain document is not designed for and thus discard all information that is not an operational result [CAST16].

These deficits have led to the decision to address the current situation and exploit the field of opportunities for possible design improvements. For this purpose, it is crucial to research superior RM by systematically combining strengths of computation with expert's knowledge and skills as well as the potentials of a methodical approach.

1.2 Objectives

The overall aim of this research is to conceive a model-based risk (MBR) management system that enables RM operators to overcome the endemic deficits of the widely-used document-based approaches. This shall be achieved by the formalization of RM steps, the role-based separation of procedures in computation and human action and providing an RM system and software demonstrators that exemplify an iterative RM process during the entire product lifecycle for all stakeholders.

This approach is elaborated in the following objectives of the research project:

1. Description of a graphical modeling language and database (DB) to comprehensively represent a complex medical device's product lifecycle as a single source of truth for risk management
2. Formulating necessary and sufficient requirements to implement one systematical and comprehensive tool set in different phases of the process chain
3. Conception of an element-wise fragmentation (DB) and vectorization (graphic model) of medical devices to allow for computation
4. Developing rules and finite vocabulary for the data types needed to capture the operational content in the models and DBs focusing on interactions in the breakdown structure and their effects on critical characteristics
5. Developing one iterative RM system for the whole product lifecycle integrating all stakeholders through unified visualization in different professional environments and ubiquitous model access

This work focuses on MedTech companies, where the product is a mixture of mechanical, electronic and software components. Such companies have medium-to-high-volume production and are typically involved in all manufacturing and marketing stages of their products, including stakeholder analysis, product development, marketing, production, sales and distribution.

1.3 Contribution of this Work

The contribution of this research project is a model-based approach for the risk management process to expedite the identification of critical characteristics of medical devices. This approach comprises a framework for MBR, model theory for a general risk modeling and a comprehensive approach for risk identification.

The topic of the thesis is situated in the crossing of risk assessment and model-based systems engineering (MBSE). The concept behind MBR is to utilize all the advantages of human expert panels without adapting its flaws in methodology. Thus, the tool computerizes the identification of critical characteristics which lead to known hazards, so it will deliver comprehensive results which only depend on data quality and not on processing. A universal application programming interface (API) compliant with the rules of the *Open Services for Lifecycle Collaboration* (OSLC) with role-based access control (RBAC) will help feed the results to the stakeholders featuring visualization in their familiar software environments and augmentation of product models with data from the knowledge base (KB). All means of software are to be shown on a demonstrator level.

In a broader context, it may reduce the time to market of the product as it will help avoid the reoccurrence of failures, shorten the time needed to seek for information (reducing costs) and facilitate participation of the stakeholders in the whole product lifecycle (know-how) before rollout. Furthermore, it is suitable as a base to build the procedural RM foundation for an International Standard Organization (ISO) 9001:2015 certification on. Essentially, risk-based thinking is propagated by reusing and processing previously obtained data, which otherwise would be left idle. Also, it can assist coping with marketing conditions where complicated regulatory requirements favor big corporations. In a medium term, MBR might push the internationalization of safety critical systems engineering (SE).

2 Terminology and Definitions

In the following chapter, terms and concepts are defined and explained in the way they are used in this thesis. This is done for a proper understanding of the work done and shall not insinuate that they were per se superior to any differing definitions.

2.1 General Terminology

System

A system is plenty of components (elements) and dependencies (relationships) between them [STEI93, p.163]. According to [ISO16], a system is the association of interacting elements structured to carry out one or more stated purposes, some examples of system element are hardware, software, data, humans, processes (e.g. processes for providing service to users), procedures (e.g. operator instructions), facilities, materials and naturally occurring entities, or any combination.

Complexity

A system is deemed complex if it consists of multiple independently acting components whose local interactions arrange for a nonlinear global outcome. Unlike systems that are just complicated, they show the emergence of properties which do not equal the sum of properties of its parts.

Comprehensiveness

A process is comprehensive if all of its subjects have undergone all applicable steps completely. ISO 31000 accentuates the comprehensiveness of the RM process as one of its principal aims [ISO09a].

Method, Technique & Tool

While definitions of these three terms will overlap in most terminologies, there are certain aspects that are characteristic for the use in risk management: Here, a method is a well-planned set of fix tasks to achieve predetermined goals like calculating an index. In contrast, a technique is the set of practical aspects of skills enabling someone to accomplish a task. By this definition, e.g. brainstorming is a technique that is frequently used in Failure Mode and Effects Analysis (FMEA), but can be used in many other methods, too.

Tools are in the following discriminated from techniques by their instrumental nature. Using a tool, one may perform a task that one otherwise would be unable to due to a missing skill or resource. In risk management, tools are often software.

Data vs. Information vs. Knowledge

Too often, the term data is exchanged for information or in reverse, the same happens to the tuple information & knowledge [BOIS04]. However, distinguishing these terms is key to understanding the premise of the concept underlying this thesis and the whole research project. Data is any account of a finding (such as a diagnostic, a measurement or an observation) that is related to the event (fact, incident, etc.) from which it has been received. In science, it often refers to the physical entities in the bottom abstraction level (e.g. process data or patient data). Information is gained when data is interpreted in the context of the event. Based on that information, an understanding being can use inductive reasoning to create knowledge. [HOLZ14, p.76; BOIS04] Here, the prevalent implicit knowledge of the being is an important factor in the form and scope of the created knowledge (expertise).

Another distinction necessary to point out is the one between standardized data and structured data. Standardized data expedite the likening of data, interoperability of systems, guarantee that the comprehension of the information is the same for all the users and assist the reusability of the data. In contrast, non-standardized data is the larger part of data and hinder data quality, data exchange and interoperability. [HOLZ14, p.67f] Data can be categorized as well-structured data (every data element possess a related determined structure, relational tables, or the resource description framework (RDF), or the Web Ontology Language (OWL) and non-structured data or unstructured data (where only a natural person can give a significant explanation) [HOLZ14, 67-68,207].[1]

Vocabulary

This term may refer to a list of all the words known by a particular person or belonging to a variety (lect) in a language (cluster) or the language itself. Deviating from this, when used in this work, vocabulary means a list of words used by specialists to communicate on a subject. Finite vocabulary lists are common in risk management to avoid ambiguities in documents.

Ontology

An ontology is the understanding of a domain, where the comprised items are common or at least shared by experts of the field.

Nomenclature

A nomenclature is a system of rules forming the names of items by the conventions of a field or science. In some fields, nomenclatures are especially referred to as systems able to term

[1] The determination if and how data is structur**ed** should not be confused with the differentiation between data with structur**al** or content value as made in section 7.3.

new concepts just by applying the building rules, e.g. in chemistry naming a previously unknown molecule.

Vocabulary, Terminology, Ontology and **Nomenclature** are overlapping concepts and – outside of the domains of linguistics and metaphysics – often used synonymously. This is current practice in MedTech and biomedical engineering [BODE08]. For the sole sake of differentiation, this work will refer to self-contained explanatory tables of items of a certain domain as vocabularies, networks of such tables or tables interlinking at least three topically pivotal columns as ontologies and finally to the semiotical building rules for the proposed RM model as nomenclature.

Verification vs. Validation

While both terms refer to the confirmation of the fulfillment of requirements by objective evidence, verification is the examination whether all requirements in the specification are met, whereas a validation detects if the specified requirement and their implementation suit a certain application case. [ISO15b]

2.2 Quality Management

Quality is the extent to which a set of inherent characteristics of an object satisfies requirements. In order to accomplish the expected outcomes, organizations recognize its objectives and define the processes and resources for activities: a quality management system (QMS). An organization's QMS model requires to be adjustable inside the complexities of the organizational context as it acknowledges that no all systems, processes and activities can be predestined. [ISO15b]

This concept is broadened by the Aachen Quality Management Model (ACQMM) as the quality related task. As is depicted in figure 2.1, ACQMM is comprised of three elements: the quality stream (transformation of customer demands into desirable products that are able to bind customers), management (includes classifying tasks, competences and responsibilities for the management, which remains the initiator and driving force for any quality initiatives) and resources & services (preparation and qualification of resources & services). The quality backward chain organizes the reactive and corrective actions for all product groups. Control loops between the quality forward chains of different product groups and the quality backward chain enhance the model with elements of continuous improvements. [SCHM15, 117ff]

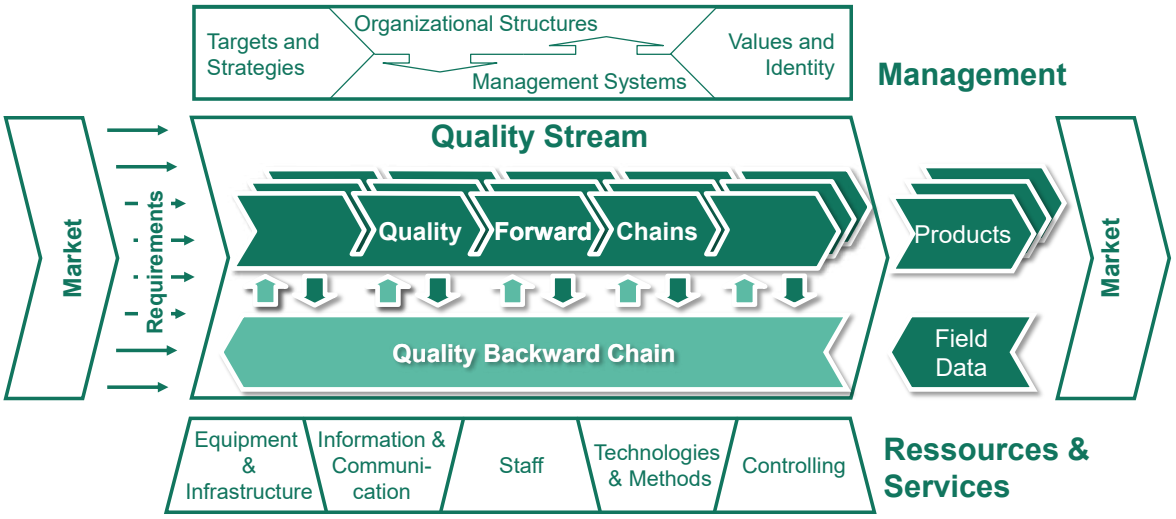


Figure 2.1: Aachen Quality Management Model

In order to achieve an effective QMS, the ISO 9001:2015 has introduced the concept of risk-based thinking. Acting as a preventive tool is a key purpose of a QMS, which uses the concept of risk-based thinking to formulate the QMS requirements. [ISO15c]

2.2.1 Good Manufacturing Practice for Medicinal Products

Good Manufacturing Practice (GMP) is that part of Quality Management which ensures that products are consistently produced and controlled to the quality standards appropriate to their intended use and as required by the Marketing Authorization, Clinical Trial Authorization or product specification. GMP is concerned with both production and quality control. [HEAL12]

2.2.2 Risk Management

Before starting to describe the risk management process, it is very important to define and understand the risk concept. The definition of the risk concept can be derived according to:

- multidisciplinary perspective [ALTH05],
- probability, chance or expected values,
- undesirable events or danger
- uncertainties [AVEN12; ŠOTI15]

A characterization of the different risk definition categories can be found in [AVEN12]. The definition and comprehension of the risk concept can influence the risk analysis; therefore, it can affect the risk management process and the decision-making [AVEN12; ŠOTI15; AVEN16].

Risk

By and large, this thesis will follow the definition of ISO Guide 73 [ISO09b].

A risk is an effect of uncertainty on objectives, where

- an effect is a change of an otherwise expected outcome, be it positive or negative,
- uncertainty is a state of missing information which prohibits a (complete) understanding of an event, its consequence or likelihood and which per se can be measured by the deviation of the existing state from calculable, but impossible states, and
- objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different organizational levels.

This definition is only meaningful if the objectives are dependent on potential events whose outcome carries consequences. If a risk is based on the outcome of two or more independent potential events, the common incidence is called an **interaction**.

Arithmetically, risk is often seen as the product of the costs the consequences of the realized event imply and the probability with which the event (or chain of events) occurs. In risk analysis, these values are usually normalized to indices of **severity** (S) and **occurrence** (O). [ISO09b]

A consensus for a risk definition is that it should fit to either outcome. If it were to be limited to unwanted outcomes, it would be required to distinguish what is when unwanted and for whom, as stakeholders will not always agree on the nature of the outcome. [AVEN09]

Different classifications covering the types of risk are available. For instance, a general classification could utilize physical, social and economic sources or such according to the environment of origin (e.g. physical, social, political, operational, economic, legal, cognitive environment) [TCHA02]. Another possibility is to give a risk an organizational link: project-related (e.g. team skills, novelty of the product) vs. categorizable (e.g. technical properties, communications), internal (e.g. equipment, leadership) vs. external (e.g. regulation, climate change) [KAYI07].

Risk Management Process

RM is a significant element in the design, development and deployment of systems and services [SHAW90] and is used in many disciplines [XIUX10].

The RM process is defined as a “systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing risk” [ISO09b]. As illustrated in figure 2.2, the **risk assessment** comprises **risk identification**, **risk analysis** and **risk evaluation**. The risk identification process shall recognize and find the risks [ŠKEC13]; its results serve as a direct input for the next steps: risk analysis and treatment [TCHA02]. In the **risk analysis**, where risks are analyzed regarding their likelihood of occurrence and seriousness of impact if they occur [KASA07]. The **risk evaluation** prioritizes risk in a comparison of the risk analysis outcomes with the risk criteria, so as to define which risks require treatment. The final step of choosing options to alter risk is called **risk treatment** or **risk control**. [ISO09a].

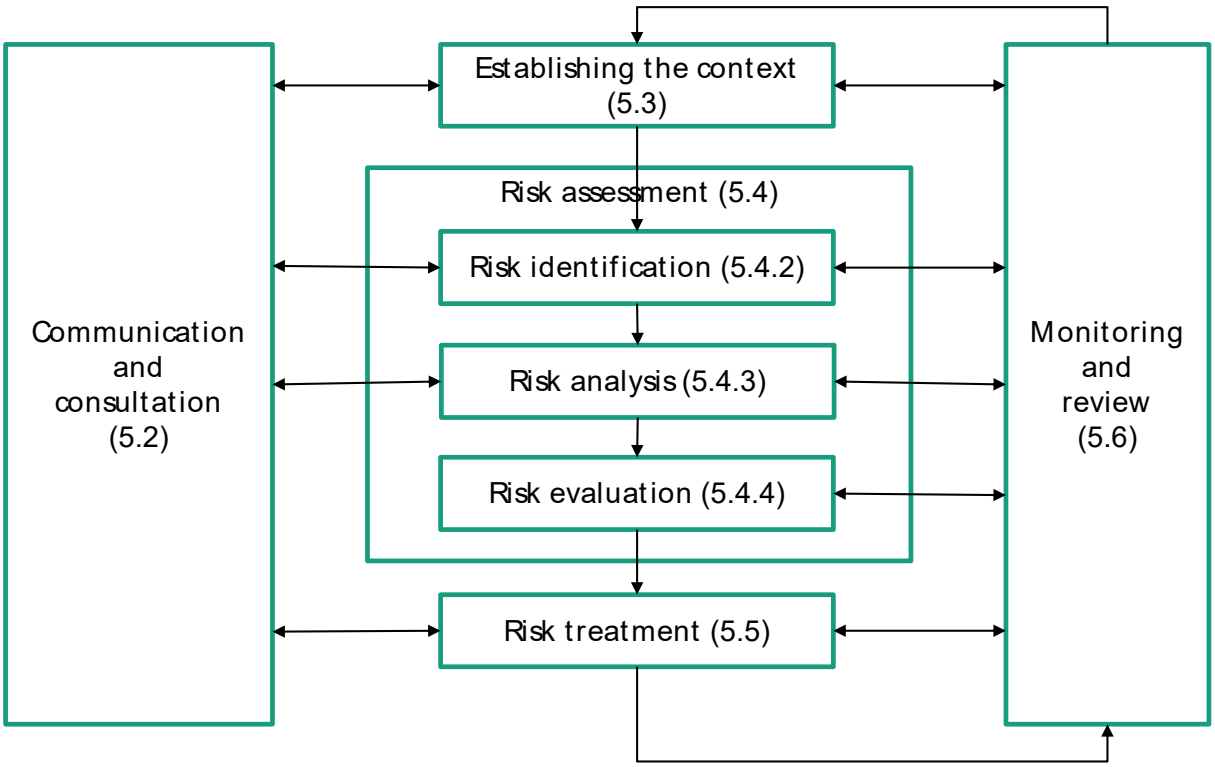


Figure 2.2: Risk management process [ISO09a]

Critical Characteristic

A characteristic is critical if its noncompliance with a safe state or value bears a hazard.

2.3 Medical Technology

Every technology employed to preserve lives or change the fitness of human beings affected by any disease or condition is called medical technology. MedTech covers medical devices (MD) and in-vitro-diagnostic (IVD) medical devices. [MEDT17]

The definition by the Global Harmonization Task Force (GHTF) has been approved by major jurisdictions [WORL17b, p.8] and will be used in this thesis.

Medical Device

"'Medical device' means any instrument, apparatus, implement, machine, appliance, implant, reagent for in vitro use, software, material or other similar or related article, intended by the manufacturer to be used, alone or in combination, for human beings, for one or more of the specific medical purpose(s) of:

- *diagnosis, prevention, monitoring, treatment or alleviation of disease,*
- *diagnosis, monitoring, treatment, alleviation of or compensation for an injury,*

- *investigation, replacement, modification, or support of the anatomy or of a physiological process,*
- *supporting or sustaining life,*
- *control of conception,*
- *disinfection of medical devices,*
- *providing information by means of in vitro examination of specimens derived from the human body;*

and does not achieve its primary intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its intended function by such means." [GLOB12]

In-Vitro-Diagnostic Medical Device

"In-Vitro Diagnostic (IVD) medical device' means a medical device, whether used alone or in combination, intended by the manufacturer for the in-vitro examination of specimens derived from the human body solely or principally to provide information for diagnostic, monitoring or compatibility purposes." [GLOB12]

Medical Classification

The process of converting the characterization of medical diagnoses and procedures into a universal medical classification scheme is named medical classification, sometimes also: coding [HOLZ14, p.129]. A nomenclature system expedites the administration and regulation of MD through the normalization of terms empowering the communication. Several groups of specialists utilize different denominating systems for MD in accordance with their necessities, e.g. maintenance, procurement, adverse medical event reporting or regulatory affairs [WORL17a, p.70]. The latter require a distinct subset of classifications based on the risk MD bear for life and limb of the intended users (including patients).

"[The rules] depend on the features of the device, such as whether it:

• is life supporting or sustaining;

• is invasive and if so, to what extent and for how long;

• incorporates medicinal products;

• incorporates human or animal tissues or cells;

• is an active medical device;

• delivers medicinal products, energy or radiation;

• could modify blood or other body fluids;

• is used in combination with another medical device."

[WORL17b, p.9]

There are different specifications of risk classes; the most common stem from World Health Organization (WHO) (A..D), the U.S. Food and Drug Administration (FDA) (I..III) and the EU's medical devices directives (MEDDEV) (I, IIa, IIb, III). The majority of national regulating authorities around the world uses one of these specifications or a derivative.

2.4 Modeling

2.4.1 Modeling Theory

While there are many different definitions of the next two terms 'subject area' and 'object area', this work will use them in the narrower sense their German counterparts *Gegenstandsbereich* and *Objektbereich* are used in modeling theory[2].

At least since Kant [STAC73, s. 1.1.1], it is a widely accepted notion in metaphysics that the experience of a particle of the world as a delimited object cannot be separated of the ego's perception of it. Assuming to objectify, one always includes their beliefs, intents and consciousness in the realization of any subject. Thus, a model may not exist without built-in purpose, aims and views of the modeler.

Subject Area

A subject area is the field of study in which and from whose perspective an object is examined.

The subject area of the models proposed in this thesis contains, of course, RM, but also involves the mindsets of the stakeholders of MD, or – perhaps more precise in the spirit of this argument – the author's perception of the above.

Object Area

The object area comprises all elements of the reality perceived by the modeler that are relevant to the purpose of a model. As the purpose cannot be separated from the modeler, the object area of the model likewise cannot be separated from its subject area. [STEI93, ch. 3]

The object area of the researched RM models always includes buts is not limited to the RM-relevant aspects of the product lifecycle.

[2] From Marx up to the computer scientists of the turn to the 21st century, the majority of the fundamental literature in modeling theory is published in German. Many further authors use the German terms when referring to the fundamental works. It thus seems advisable to lay out definitions with the German words in mind first and then translate the concepts into English.

Model

Learning is not conceivable without the possibility to make mistakes. However, in many cases an approach by “trial and error” cannot be carried out in real systems; hence, the best solution can only be identified by utilizing a model allowing for simulations and experiments. Indeed, models and simulation are considered the most sophisticated method of information processing. [NIEM07]

The term model is used in two meanings in this work. When talking about the theory behind modeling, the epistemological definition from Stachowiak's General Model Theory (GMT) is applied. It is based on Stachowiak's extensive research on the cognitive theories of the great scientists and philosophers from the 17th to the 20st century. Accordingly, any knowledge — be it scientific findings, technological insight or awareness of the surrounding world — is gained by perception of or through models. Any information is perceived relative to the subject and based on a selective and temporary observation of the original.

Here, a model is any reduced projection or representation of the reality or its particles. It features three main characteristics:

1. **Projection/Representation.** A model must be based on a natural or artificial, preexisting original, which regardless may be a model itself.
2. **Reduction.** A model holds only those attributes of the original that are known and relevant to the subject.
3. **Pragmatism.** A model is not unambiguously assigned to an original, but its assignment is relative to
    a. certain subjects whose use case it is tailored to,
    b. a certain time interval in which it is supposed to be used and
    c. a certain setting enabling the desired operations. [STAC73, s. 2.1.1]

As far away as this definition may seem from a technological view, it is nevertheless very important to justify the reductions a pragmatic modeling approach causes for the sake of the technological feasibility of the model.

Subsequently, the second definition of the term 'model' is established for models that follow this approach. Here, in turn, a model is a system built for the sufficiently faithful reproduction of all necessary aspects of an object class to serve a certain engineering purpose. At the same time, it may refer to instances of such system which reunites this definition with the first characteristic of Stachowiak's pragmatic model.

Steinmüller defines models as a “model system” in itself (and explicates it as a “‘Model’ i.w.S.” – a model in its broader sense) with four sub-systems :

- Model subject (creator and user)
- Model object (instance)
- Original (represented object)
- Addressee (the receiving end that is to be influenced) [STEI93, 178f]

Respecting both definitions then, a complex set of building rules (e.g. weather forecast model or here: a theoretical RM model) is called a model with the same right as a specimen created to resemble the desired aspects of an original (e.g. a model airplane or here: files modeling a certain MD).

2.4.2 Model-Based Systems Engineering

"[Model-Based Systems Engineering (MBSE)] is the formalized application of modeling to support system requirements, design, analysis, verification and validation activities beginning in the conceptual design phase and continuing throughout development and later life cycle phases." [INCO07]

Modeling Language

A modeling language is a semiformal language describing the kinds of elements (allowed to put into your model), allowable relationships between them. In other words, it determines a grammar: a set of rules describing whether a given model is well-formed or ill-formed. [DELL13, p.5] Modeling tools are conceived and carried out to conform to the rules of one or more modeling languages, allowing to create well-formed models in those languages. If you compare diagramming tools (Visio, Schematic, etc.) with a modeling tool, the first ones generate diagrams in one page and the last one conceives a model and optionally a set of diagrams supporting as views of the underlying model. An alteration of an element on a diagram within a modeling tool means modifying the element itself in the underlying model. A modeling method is similar to a road map containing a documented set of design tasks, which a modeling team performs to develop a system model. More precisely, it's a documented set of design tasks that ensures that everyone on the team is building the system model consistently and working toward a common end point. Without such guidance, there will be wide variance in the breadth, depth, and fidelity that each member of the team builds into the system model. [DELL13, p.8]

Utilizing the fitting methods has insufficient attention at the moment of carrying out a process and a set of tools on a project in spite of the fact that utilizing improper methods can direct to inefficacious and likewise occasionally failure [MART97, p.52]. Raising costs, decreasing quality and frustration for engineers and management are the result of an inapt balance between the following elements: process, methods, tools and environment (PMTE) [MART97, p.51]. In fact, the current literature does not provide too much direction about the connection between PMTE elements. This issue can be dealt with a PMTE paradigm. Figure 2.3 shows the existing relations in PMTE [MART97, 3.2]. An individual process determines "what" is to be performed and must be assisted by specific methods successively; a method determines the "how" of each task and can be assisted by one or more tools. Next, a tool – which is an instrument easing the completion of the "hows" – must be assisted inside a certain environment. Further, the introduction of new technology enforces the development of new methods. [MART97, p.66] Methodology is the compilation of the associated process, method and tool [ESTE08].

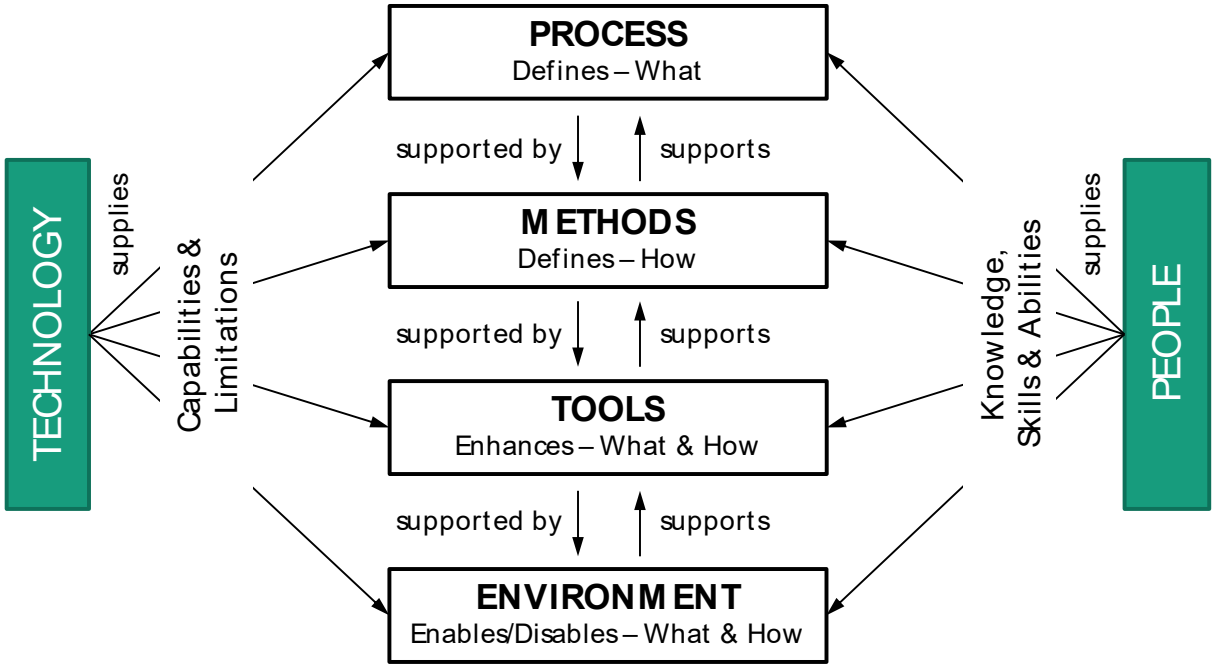


Figure 2.3: The PMTE paradigm (merger based on [MART97, p.67])

2.4.3 Product Modeling

Product model data is the result of product modeling, which has got two interconnected aspects: product models and process chains. It is the key factor in determining the success of various product development strategies and industrial competitiveness in the future. [KRAU93]

Product Model

A product model is the entity of all information that is necessary to define a product according to the postulated model aspect, where

1. a product is an artificially generated object or group of objects – be they material or immaterial – that form a functional unit and
2. the model aspect is the maxim a model adheres to in the informational relation with the subject. Model aspects may be its projection, function or purpose, among others.

A product model is further the logical collection of all pertinent information regarding a given product during the product lifecycle saved in forms of digital product model data and are provided with access and manipulation algorithms.

Process Chain

A process chain (*also:* product development workflow, product modeling process) brings a set of technical and management functions expected to transfer initial ideas to final products.

Some of the most important product models in production belong to the class of computer-aided production tools (CAx), the computer-aided (data) design, analysis and manufacturing systems [VDI16]. Examples are computer-aided design (CAD), ~ engineering (CAE), ~

manufacturing (CAM) or ~ planning (CAP). All product model types with a commercial use relevant to this work may be found in figure 5.2.

Interoperability

Interoperability is defined as the sharing of technical and business information continuously with partners through software tools to encode and decode the associated electronic transmission [RAY06].

3 Risk Management for Medical Devices Today

The task of manufacturing medical devices safe for human use is becoming more complex due to the globalization of the medical device market place and increasing medical device usage [CORC13]. Moreover, there is a necessity to harmonize national standards so as to decrease regulatory hindrances and expedite trade [WHO03]. To obtain access to foreign markets, RM has turned into a valuable competitive tool. To guarantee device usability, safety, and regulatory compliance, an RM process is essential [CORC13]. At the same time, medical devices themselves are becoming more and more complex and interconnected which increases the difficulty of managing risk at satisfactory levels.

The literature review revealed that the reasons for underachieving RM are connected to definable and distinguishable deficits (→ 3.3). Some of those are due to the RM methods and techniques used, others rest with the document-based approach of the chosen RM process. The latter seem to be especially challenging for manufacturers in highly innovative fields as well as to SMEs. The MedTech sector is situated in the intersection of both; this fact makes it an interesting starting point to research the advantages of model-based RM for complex product lifecycles. Hence, this thesis recognizes the possible mitigation of the endemic deficits of document-based RM by shifting to a model-based approach that integrates procedures and results from the former.

The state of the art established in this chapter shall bring the reader to understand the need to research a model-based RM system and the importance of its application in the development of modern medical devices.

3.1 Standards, Guidelines and Rules for Medical Devices

In order to balance the diverging expectations on medical devices from industry, consumer and the public, different rule sets shall guarantee the concurrence of technological progress, continuous improvement in performance as well as product and process safety. In practice, using international industrial standards will facilitate developing innovative products while complying with regulations. [ISO07]

3.1.1 Regulations of Medical Devices

A fast development of medical devices can be achieved using standards while complying with the demands of the public and regulators guaranteeing the safety and performance as intended of medical devices [ISO07].

There are different regulations for medical devices in different countries. In this thesis, the focus is put on the EU and European regulations.

The regulatory framework for medical devices within the EU includes the following three directives:

- Council Directive 90/385/EEC on Active Implantable Medical Devices (AIMDD) (1990)
- Council Directive 93/42/EEC on Medical Devices (MDD) (1993)
- Council Directive 98/79/EC on In Vitro Diagnostic Medical Devices (IVDMD) (1998) [EURO18b]

To solidify the role of the EU as a global leader in the sector and to consider overall technological and scientific advancements in the sector, two new regulations entered in force on 25 May 2017. These regulations replace the existing directives.

- Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC
- Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU [EURO18b]

New to the 2017 regulations is the postulation that, manufacturers shall establish, implement, document and maintain an RM system. [EURO17a; EURO17b]

3.1.2 Standards

ISO 31000

ISO 31000 is based on the Australia/New Zealand risk management standard (AS/NZS 4360:2004). This standard establishes the principles required to perform an effective RM, the framework in where RM takes place and the RM process. Also, it emphasizes a top-down enforcement and a proactive approach. It declares that it can be implemented by any public, private or community enterprise, association, group or individual and it is not restricted to any industry or sector. [GJER11] This standard is not contemplated with the aim of certification [ISO09a].

ISO 14971

ISO 14971 is a standard establishing a framework to estimate the probability of occurrence and consequences of the risks [TEFE17] and helps regulators to qualify the fitness and suitability of RM implementations. This standard is cross-referenced by other standards such as ISO 13485 where RM is a requirement for the QMS for medical device organizations [ISO03]. In IEC 60601-1, ISO 14971 is cited as a prerequisite for the respective certification [PHAR16].

Excursus: Why prefer ISO 31000 over ISO 14971 in MBR even for medical devices?

At this point, it is advisable to explain why the author has chosen the structure of the more general ISO 31000 over DIN EN ISO 14971 even though it actually specifies RM application to medical devices. By no means is it meant to reject the guidelines found in each step, but rather highlight the importance of a self-consistent risk identification, as ISO 31000 does. If RM

alongside the process chain is understood as iterative, the values of contained, consecutive RM steps become clear. Only a risk identification, whose inputs and outputs stay comparable when repeated, makes changes in risk measurable between iterations or set alternatives. Moreover, the question of how comprehensive risk identification has been managed should be answered while concluding risk identification and when RM participants still have the chance to reduce residual risk if the level is insufficient. In the scheme of DIN EN ISO 14971 comprehensiveness is not fully ascertained until entering risk control. Therefore, ISO 31000 is preferred for setting up an explicit formal risk identification step. [CAST16]

ISO 13845

ISO 13485 is an independent QMS standard stemming from the ISO 9000 quality management standard series and adjusting the ISO 9000 process-based model for a regulated medical device manufacturing environment and resting on the ISO 9001 process model concepts of *Plan, Do, Check, Act*. This standard assists medical device manufacturers to devise a QMS to determine and keep the effectiveness of their processes [BSI16]. Annex 3 of the WHO Medical Device Regulations provides a conceptual comparison of ISO 9000 and ISO 13485 [WHO03].

ISO 13022

ISO 13022 gives recommendations for the implementation of RM processes for medical products containing (in our case study more accurately: treating) viable human cells and defines requirements for their handling. While the RM system proposed in this work has no dependency on this standard, it is binding for a compliant documentation of the RM processes analyzed in the case study and the actual treatment based on that. [ISO12]

ISO 16142-1

This standard introduces general principles deemed essential for the development of any safe and performing medical device. Part one lists the general principles for all types of medical devices together with those standards recommend to consult for compliance as well as additional essential principles for non-IVD devices. [ISO16]

3.1.3 Guidelines

Global Harmonization Task Force

GHTF endorses the convergence of standards and regulatory practices regarding the safety, performance and quality of medical devices prompting technological innovation, helping international trade and acting as an information exchange forum. Its members encompass medical device regulatory agencies and the regulated industry representatives of the EU, Canada, Japan, Australia and the United States of America [ISO07; WHO03].

The fulfillment of GHTF goals is mainly done through the publication and distribution of harmonized guidance documents for fundamental regulatory practices [WHO03], which were developed by five different GHTF Study Groups. This study groups were: premarket evaluation

(study group 1), post-market surveillance/vigilance (study group 2), quality systems (study group 3), auditing (study group 4), and clinical safety/performance (study group 5). [WORL16]

The study groups were decommissioned in February 2012 and the GHTF was substituted by the International Medical Device Regulators Forum (IMDRF), having the same goal as GHTF. Conversely the GHTF, IMDRF members are regulators with industry connection, by invitation only. IMDRF consists of the GHTF starting participants and Brazil, China and Russia were asked to enter. The care of the collection of documents beforehand published by the GHTF are guaranteed by IMDRF. [WORL16]

Good Manufacturing Practice

Manufacturing of medicinal products in line with the guidelines for GMP has been happening for several years and it is not ruled by the European Committee for Standardization (CEN)/ISO standards. [HEAL10]

Throughout the lifecycle of a medicinal product, a quality risk management approach should be implemented in which a supported and documented risk assessment of the facilities, equipment, utilities and processes should be the base for all decisions on the scope and extent of qualification and validation. [HEAL15]

3.1.4 Classification of Medical Devices and their Components, Nomenclature

At date, there are more than 100 biomedical classifications in practice. [HOLZ14, p.130] Most of them can be found organized in ontological systems, either with the exact term or a congruent concept. The two most utilized nomenclature systems are the Global Medical Device Nomenclature System (GMDN) and the Universal Medical Devices Nomenclature System (UMDNS). [WORL17a, p.70]

These two systems, however, are rarely used in a complimentary way, but in most countries rival as an implementation for state-regulated medical classification. Many regulating authorities within the reach of CEN (the sponsor of GMDN) who have not switched from UMDNS to GMDN yet, plan do to so as soon as the collection and translation of terms in GMDN has reached a state they deem satisfactory. For example, the German governmental agency entrusted with medical classification, the German Institute of Medical Documentation and Information, takes the collection to be sufficient, but is waiting for an officially translated German DB while – in the meantime – continuing to stipulate the use of UMDNS 1.0 (from 1996) and 1.1 (1998). Our research project thus has chosen GMDN over UMDNS

With this in mind, a short explanation of the two ontologies used in this research project will follow, which are GMDN and the Unified Medical Language System (UMLS).

Table 3.1: Characteristics of some biomedical ontologies [BODE08] based on the information present in the UMLS (2007AC)

Name	Ref.	Scope	# Concepts	# Concept Names				Subs. Hier.	Version/ Notes
				Min	Max	Med	Avg		
SNOMED CT	[DONN06]	Clinical medicine (patient records)	310,314	1	37	2	2.57	●	2007-07-31
LOINC	[HUFF98]	Clinical observations and laboratory tests	46,406	1	3	3	2.85	○	Version 2.21 (no „natural language“ names)
FMA	[MCDO03]	Human anatomical structures	~72,000	1	?	?	~1.50	●	(not yet in the UMLS)
Gene Ontology	[ASHB00]	Functional annotation of gene products	22,546	1	24	1	2.15	●	2007-01-02
RxNorm	[LIU05]	Standard names for prescription drugs	93,426	1	2	1	1.10	○	2007-08-31
NCI Thesaurus	[CORO04; NATI19]	Cancer research, clinical care, public information	58,868	1	100	2	2.68	●	2007_05E
ICD-10	[WORL18]	Diseases and conditions (health statistics)	12,318	1	1	1	1.00	○	1998 (tabular)
MeSH	[U.S.19]	Biomedicine (descriptors for indexing the literature)	24,767	1	208	5	7.47	○	2007-08-27
UMLS Meta.	[BODE04]	Terminology integration in the life sciences	1,4M	1	339	2	3.77	n/a	2007AC (English only)

Unified Medical Language System

As a consequence of the diversity of names utilized to state the identical concept and the lack of a standard structure to disseminate terminologies, the UMLS evolved by the National Library of Medicine. The three knowledge sources included in UMLS are *Metathesaurus*, *Semantic Network* and *SPECIALIST Lexicon*. [BODE08; YOO06, p.13] The first one is the dominant component, Metathesaurus, a huge repository of interrelated biomedical concepts [CHEN05, p.219; BODE04]. It features concepts, concept names and other attributes coming from more than 100 terminologies, classifications, and thesauri, some in multiple editions (like UMDNS) [BETH09]. The second one is composed of a set of broad subject categories, or Semantic Types, which procure a logical categorization of all concepts rendered in the UMLS Metathesaurus. In addition to this, it contains a set of valuable and relevant relationships, or

semantic relations, present between semantic types. [BETH09]. The *SPECIALIST Lexicon* encompasses a set of lexical entries with one entry for each spelling or set of spelling variants in a specific part of speech [BETH09]. Table 3.1 shows some examples of biomedical ontologies present in UMLS [BODE08].[3]

Global Medical Device Nomenclature

There are many players with distinct responsibilities and levels of understanding of the processes in the lifecycle of medical devices but all with the same goal of guaranteeing the availability of medical devices to the public. Thus a general method to define and recognize medical devices in a clear manner is required. GMDN offers to recognize all medical devices on a generic level. [ANAN10]

The standard organizations CEN and ISO generated the ISO 15225, which specifies a nomenclature system to identify medical devices converging the requirements of the global market [WHO03; ANAN10]. This standard gives the rules and guidelines for a medical device nomenclature data structure to expedite the collaboration and interchange of data utilized by regulatory bodies on an international level between interested parties, e.g. regulatory authorities, manufacturers, suppliers, health care providers and end users. [ISO10] GMDN is established on ISO 15225 [ISO10].

The nomenclature comprises four stages, which are device category, collective term, generic device group and device type [ISO10].

The following nomenclature were employed to create GMDN:

- Classification Names for Medical Devices (CNMD) and in vitro Diagnostic Products
- European Diagnostic Manufacturers Association (EDMA) in vitro diagnostic product classification
- ISO 9999 Technical Aids for Disabled Persons Classification
- Japanese Medical Device Nomenclature (JFMDA)
- Norsk Klassifisering Koding and Nomenklatur (NKKN)
- UMDNS. [ANAN10]

IMDRF suggests to use the GMDN, which is already utilized by over 70 national medical device regulators to assist their activities [GMDN18]. Among the 174 countries surveyed by the Baseline Country Survey on MD, 13 % of high-income countries use only GMDN and 6% only UMDNS [WORL17a, p.72]. The GMDN Agency administers and maintain the GMDN [GMDN18].

[3] For more information about the available ontologies see: Open Biomedical Ontologies (OBO), http://www.obofoundry.org/

3.2 Challenges in Medical Technology

The MedTech sector shows a research-and-development share surpassing any other sector limiting the time span to only 18 to 24 months before an upgraded version of the product comes to market [MEDT17]. In 2017, MedTech filed 13,090 patent applications with the European Patent Office (EPO) which make it the top scorer with 7.9% of the total number of applications [EURO18a]. SMEs companies build 95% of the MedTech industry [MEDT17].

Presently, MedTech companies are forced to reduce product development cycles that go in hand with quick technological changes and harsh marketing conditions [DASH10]. Furthermore, the amount of competitors and the complexity of the product lifecycle are augmented notably by the globalization of the marketplace as more companies and partners have to communicate [OEHM10].

In developing countries, the possible market for MD is around five times bigger than in developed nations where a great number of developers and manufacturers of MD are settled [WORL10a]. Some general hindrances to innovation for low- and high-resource settings are restrictions in training the staff how to utilize the new device, rejection from established medical practice and unwillingness to acknowledge the necessity to upgrade skills; however, there are some distinct hindrances for each one [WORL10b]. In the case of low-income countries, some of the hindrances are the habitual costs to operate a new device (e.g. service contracts, spare parts, depreciation, consumables, training and so forth), infrastructure, cultural and social context and extreme regulation. All these hinder the proper utilization of imported MD in developing countries proposing high income countries to re-design technologies adapting to local needs. In the case of high income countries, especially EU members, some impediments are the bargaining of reimbursement for new medical technology to be included in the mainstream package of care and the administrative and regulatory hurdles to innovation. [WORL10b]. Regulatory requirements for the safety of MD play a critical role but inflict additional costs to the designers and manufacturers [WORL10c, p.62].

A vital tool to cope with all these challenges is a satisfactory RM [PALA10]. To assure device usability, safety and regulatory conformity is crucial to RM [CORC13]. In addition, a comprehensive RM is required for a trustworthy supply chain in a globalized production [CHAN10]. There are several other incitements demonstrating the necessity for a constant and cost-effective RM through the entire product lifecycle and beside the complete process chain [CAST16].

Unfortunately, the mentioned challenges collude with several deficits of classic RM approaches in a way that will increasingly lead to shortcomings of current RM in MedTech. The following sections introduce methods, techniques and tools in use today and carve out their deficits in general comparisons and, in particular, for medical devices' lifecycles.

3.3 Risk Management Methods, Techniques and Tools

With around 40 years of existence, risk management is a relatively young scientific field [AVEN16]. The RM process has been adequately standardized but the plenty of methods to choose from in each process step result in very heterogeneous designs [HALL11]. Additionally, there is a growth of methods serving as impediment for companies due to the lack of direction to choose the right method [ŠKEC13].

The grouping of risk assessment techniques can be done in several manners. For example, in IEC/ISO 31010, the techniques and tools are clustered according to their application in every step of the risk assessments process (risk identification, risk analysis-consequence, probability, level of risk, risk evaluation). Moreover, they are sorted by influencing factors (resources and capability, nature and degree of uncertainty, complexity) and quantitative/qualitative output. [IEC09] The choice of technique, again, depends tremendously on the selecting individual and will itself influence the path of the RM process [REDM02a].

FMEA is one of the most used method in risk assessment [ZENT13]. In table VIII.1 of appendix A, an overview of the available risk assessment method and techniques can be found.

3.3.1 Challenges of Technical Risk Management

The Fraunhofer Institute for Production Technology (IPT) performed a study on 180 manufacturing companies considering their products as innovative and complex [ZENT13] in which most of them emphasized the implementation of the RM process in the company and the worth of eluding failures in the beginning steps of the product development. Furthermore, some issues like RM methods lacking clarity and accuracy, high-priced risk assessment methods, inexact methods to define the main risks, and falling short methods of risk analysis to define risk causes are common to them.

Interestingly, the list of motives to run a risk analysis is led by the company's financial security with around 59%, followed by preventing product failure with almost 56% and compliance to laws, standards and guidelines with 49.2%. In this context the implementation of a risk analysis successive to the failure happened had a score of approx. 62% [ZENT11, 25f, 78].

3.3.2 General Deficits of Risk Management Methods

For the purpose of identification, evaluation and treatment of risk, the implementation of a risk management method or technique is required. The following seven deficits were determined through a literature review for the RM methods and techniques in [CAST16]:

- Missing comprehensiveness: failure in the identification of a risk due to the concurrency of complexity and comprehensiveness, transcription and copy errors, bureaucratic loops or simply files missing

- Uncertainty of coverage: missing DB of their previous products, documents are in different format and style lacking a quantitative evaluation. Compensation requires to increase the workload.
- No formalization of risk identification as single step: every step is implemented in several habits regarding its perceived significance and precision.
- Incompatibility of results due to the multitude of techniques and that each one owning procedure, features relating to complexity, expertness required, and so on. Furthermore, they are rooted on human observation, judgment and creativity.
- Human Factor:
    - Bias by design: new information is usually embedded with experts who not just add their expertise not to mention their social skills, creativity, professional background and readiness to judge.
    - Mindsets and value systems: the daily custom utilized in a profession can confuse strangers to the profession.
    - Environmental influence
- Incompatible work environments: panel gatherings with different stakeholders lacking on resources, regulatory constraints, no acquainted routines or missing trained personnel
- Poor Risk Treatment: reluctance to agree to the large investments (time, money, personnel) and exhausting tracking of treatment measures.

3.3.3 Endemism of the Deficits to Document-Based Risk Management

Some deficits are dependent of the risk management method or technique and it is important to differentiate them from those endemic to the document-based approach. Therefore, a literature review was conducted to identify the endemic deficit of the RM methods and techniques which are distinct between each other. The following endemic deficits were found through the literature review:

Closed Fashion of Documents vs Recurring Risk in the Product Lifecycle

An RM method can be applied at different stages of the product lifecycle [IEC09]. Multitude of RM methods and techniques are propagated as suitable for performance at any stage of the product lifecycle, common examples are FMEA or fault tree analysis (FTA) [AHME07]. While this section is not committed to investigate these claims per se, there is one aspect particularly important to complex and interconnected products: Many of the document-based methods/techniques are not qualified for iterative RM – at least not in the fashion that their procedures and documents are standardized today. Once an organization *A* has finished a non-iterative RM process, missed risks are probably not found later on by another RM process in that organization, let alone by any other *B* that is only involved in later lifecycle stages *A* has got no control over. Following professions (in application, maintenance etc.) cannot prove the identification again. Yet, to charge *A* with the responsibility to foresee al implications of *B,C,…* is a rather theoretical possibility, especially as *A* will not even be aware of all following organizations involved. Alternatively, *A* may resort to cast its panel with all further lifecycle

stages in mind, because expertise lost in the first steps cannot be respawned later on. In practice, often representatives of presumably involved types of organizations are invited to the panel to mitigate the effects of this deficit.

Level of Complexity

To comprehend the complexity of an individual risk or of a portfolio of risks of an organization. it is vital to choose the appropriate RM method or techniques. Indeed, treating a single risk and disregarding the interactions may have an overall negative impact. Thus, it is important to understand the effect in the components of the whole system [IEC09]. In the case of a highly complex product lifecycle, the imperative structure of document-based techniques will most certainly render it impossible for human beings to factor all significant interactions in.

Unknown Level of Uncertainty

An understanding of the quality, quantity and integrity of accessible information regarding the concerned risk is demanded for the nature and degree of uncertainty. In this respect, it encompasses the degree to which satisfactory information about the risk, its sources and causes, and its consequences to the accomplishment of objectives is accessible. The origin of uncertainty can be from poor data quality or missing essential and reliable data. [IEC09] Through the uncertainties related to single or organization can be dealt with methods like solid documentation, sensitive analysis and risk communication. However, such methods cannot deal appropriately with uncertainty of coverage.

Missing Comprehensiveness

Methods and processes must be designed comprehensively [MAIE11; ISO09a; GRUB11] as IEC/ISO 31010 states that document-based risk management fails to master the growing demand of complexity and comprehensiveness. The lifecycle of a medical product depends usually on various multi-level manufacturers and many manipulators, the complexity is inferred. This results in a heavy workload and can destroy the comprehensiveness. Another impairment for missing comprehensiveness form transcription and copy errors, bureaucratic loops or simply files getting lost, as most of the document-based approaches drop in comprehensiveness with each step [IEC09; cp. DELL13, pp.2–4]. Not dealing with the complexity of the analyzed system and its interactions in the RM process will eventually lead to residual risk. Such risks will later resurface in the product’s lifecycle and may harm the comprehensiveness. [CAST16]

Incompatibility of Results

A great number of RM techniques and methods are available and often each technique is based on singular procedures and methods [GRUB11]. These techniques are selected on the basis of humans’ judgement, their skills or creativity [REDM02b; REDM02a]. As every technique varies from each other, this leaves an effect on risk identification.

An output of each document-based RM method or technique can be quantitative (e.g. tables, graphs, either worksheets or pictorial representations) or qualitative [IEC09]. For example,

FMEA or FTA provides a quantitative worksheet, whereas the hazard and operability studies (HAZOP) delivers qualitative output. [IEC09] Sometimes users might not be able to compare the results on the respective documents or simply not see the coincidence.

Execution Cost

The document-based approach to SE is expensive as it is necessary to maintain the discrepancies, disconnected and out-of-date artifacts [DELL13, p.2]. Moreover, an expert team is needed at any stage and the project time is lengthened [IEC09].

Human Factors

There are various human factors involved as the RM process is being carried out. These human factors can be bias by design, mindsets and value systems as well as environmental influence. Some methods require the advice and experiences of **various** experts that might differ in certain aspects. Each professional may have a different mindset and work in a manner not according to the ways of the others. Similarly, results can be different once the working environment of these experts is changed. For example, the same experiment can yield very different results if performed at some other time or at some new place. Document-based methods with their definitive appearance deviate advertence from human factors [CAST16]

No Formalization of Risk Identification as a Single Step

Most of the organizations implementing RM processes achieve a reasonable level of standardization. However, examining the individual steps of these processes, it is found that they are being carried out in different manners in relation to their importance and accuracy. Thus, all singular steps like risk identification need to be more formalized as well. [CAST16] It is considered a deficit non-endemic to the document-based approach, meaning this is not healed by shifting to MBR, but by conceiving better tools and techniques in general. MBR may help organizations structure their tool portfolio and improve implementation and transitions yet is not a remedy for this deficit by itself.

All aforementioned deficits are listed in table 9.2, where they are set against the remedies provided in the MBR concept (→ ch. 6).

3.4 Risk Management in Medical Technology

3.4.1 Relevance of Deficits to Medical Devices

The main effects of these deficits on RM for medical devices can be divided into two dimensions: those attributed to the nature of the product (made for medical application) and the product trends in the industrial sector (→ 3.2) and those linked to the distinctive features of the organizations owning the product's RM process, typically the manufacturer.

Comprehensiveness in RM is exceptionally important whenever product lifecycles are likely to bear risks with high severity and low detectability. Among with e.g. means of passenger transportation or pharmaceuticals, medical devices fall into this range. The inability to master

comprehensive RM for complex product lifecycles therefore is the most damaging deficit of document-based RM approaches. If, concurrently, the risk assessment cannot provide satisfying statements about the specificity of risk uncertainties, this methodical weakness may amount to a serious increase in costs for all stakeholders, be it avoidable health hazards or an unnecessary limitation of the range of application.

With the vast amount of document-based RM techniques that are usually catered to a certain professional mindset, the results of preceding RM processes/steps may sometimes be calculatively incompatible to the present RM process, in many cases at least not mergeable at reasonable expense. In the increasingly probable case of a network medical device, those prerequisites are multiplied. Creating the product lifecycle of a medical device is an interdisciplinary effort and gathering the required information for a meaningful RM process is almost always a very cost-intensive step of the manufacturing process chain[4]. In addition, the manufacturer's own RM results again must be readied to the demands of regulators and at times users like hospitals or practice networks.

Besides, innovative medical device manufacturers are in their great majority small and middle-sized enterprises acting in highly regulated markets. The execution of a document-based RM process, the time needed for an expert RM operator which is necessarily curtailing his actual availability as a practitioner or the manual generation of documents may consume a substantial share of the total expenses.

3.4.2 Meaning of Risk Management for the Companies

An empirical study to identify the external factors influencing the decision-making process was realized, which was divided in three parts: literature research to identify the external factors, semi-structured interviews to gain insights and an online survey to quantify the factors.

Literature Research

The most relevant sources identified by the literature review were covering different aspects and backgrounds possibly affecting the decision-making process like RM in general, regulations in medical engineering and the decision-making process with regards to the decision-maker himself. A list of all the factors found in every source was done. Sometimes the factors were explained in different parts of the literature with different names; therefore, they were renamed to be consistent. For instance, in Donelan et al. [DONE15] the factor "time to market" was found, but in the paper referred to "time consideration" or "time pressure". Overall, 74 factors with relevance in risk treatment were compiled, see figure 3.1.

[4] In this regard, the case study for this thesis is a primary example. Considering that its subjects are prototype systems where most of the stakeholders are acquainted scientists, one can imagine the stress of the task for a market-ready medical device.

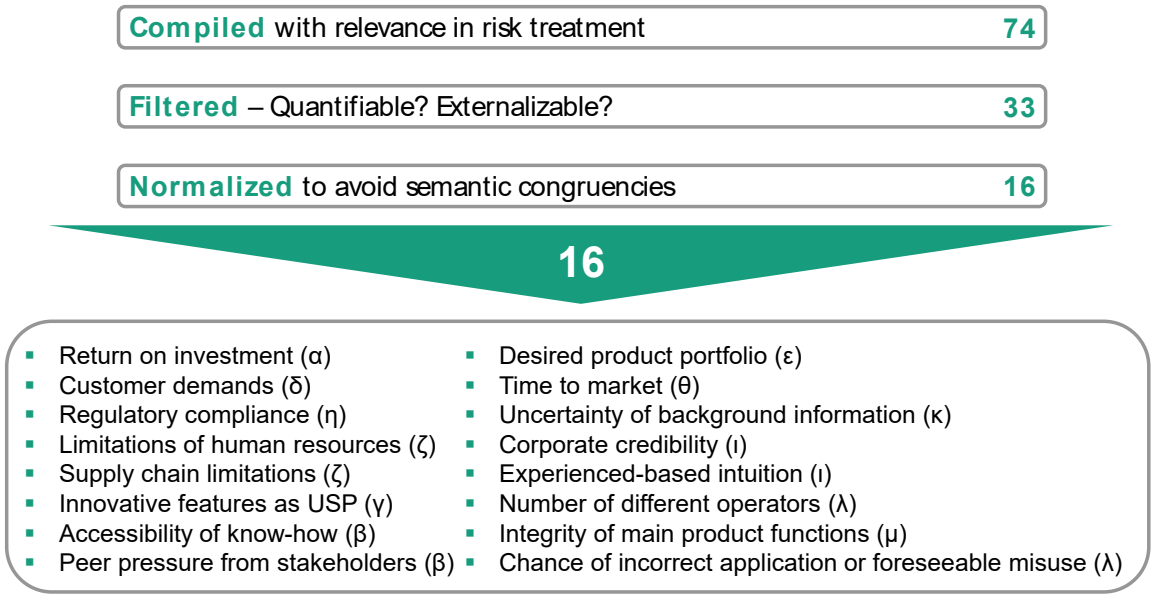


Figure 3.1: External decision-making factors[5]

Two criteria were used to assess all the factors found in the literature review. First, every factor must be quantifiable and expressible by a scale such as ratings, amounts or Boolean. Following the previous example of “time to market”, this factor is without a doubt countable. In the scope of MBR, this criterion allows for computability. Being able to quantify influential factors enables the stakeholders to include them into risk evaluation in an explicit instead of a tacit way. A prominent example of this advantages would be the comparison of different risk treatment options. The second criterion asks for the leverage of the factor on the decision-maker to be externalizable. Meant is the momentum in which the responsible decides to start or stop a risk treatment, which should be external to the decision-maker and leveraged by the treatment decision. Going back to the former example of “time to market”, companies urge to be the first to enter an innovative product into the market; hence, there is a sway during the whole product development process. Thus, this factor is external to the decision-maker and the probable risk treatment options can influence the time required in the product development process. Counterexamples would be any factors based on personal beliefs, bias, interests or considerations, e.g. avoiding conflicts with superiors, negative experiences with a technology or antipathy for the corporate policies of a supplier.

[5] The external decision-making factors listed here were originally found in: α: [EBER13, p.16]; β: [EBER13, 38,90-92,124]; γ: [EBER13, 41-44,124]; δ: [EBER13, 58-59,89], ε: [EBER13, 76f,126]; ζ: [EBER13, 86,92f]; η: [EBER13, 134-141,143]; θ: [DONE15, 319,321]; ι: [DONE15, pp.321–327]; κ: [DONE15, p.323]; λ:[FISC12, p.93]; μ: [FISC12, 95f].

Any factors failing either criterion were eliminated. Finally, the factors with similar meaning were removed from the list or combined. Figure 3.1 lists the results with respective source of origin.

To confirm the external factors found in the literature review, semi-structured interviews were realized.

Semi-Structured Interviews

Five semi-structured interviews, a qualitative method, were conducted to confirm the external factors found in the literature review in practice, in which some of them were confirmed directly and indirectly, as shown in figure 3.2. From the sixteen external factors, eleven factors were directly mentioned by the participant and five were indirectly addressed. The participants came from companies manufacturing a variety of medical products like wheelchairs and equipment for the disabled, surgery and hospital equipment and eye-surgery apparatus. Regarding the participant occupation inside the company, they were:

- Direct RM responsible in own department
- Quality manager/ regulatory affairs responsible (twice)
- Product designer/developer
- Consultant

The questionnaire containing instructions and key questions can be found in section B of the appendix (→ VIII).

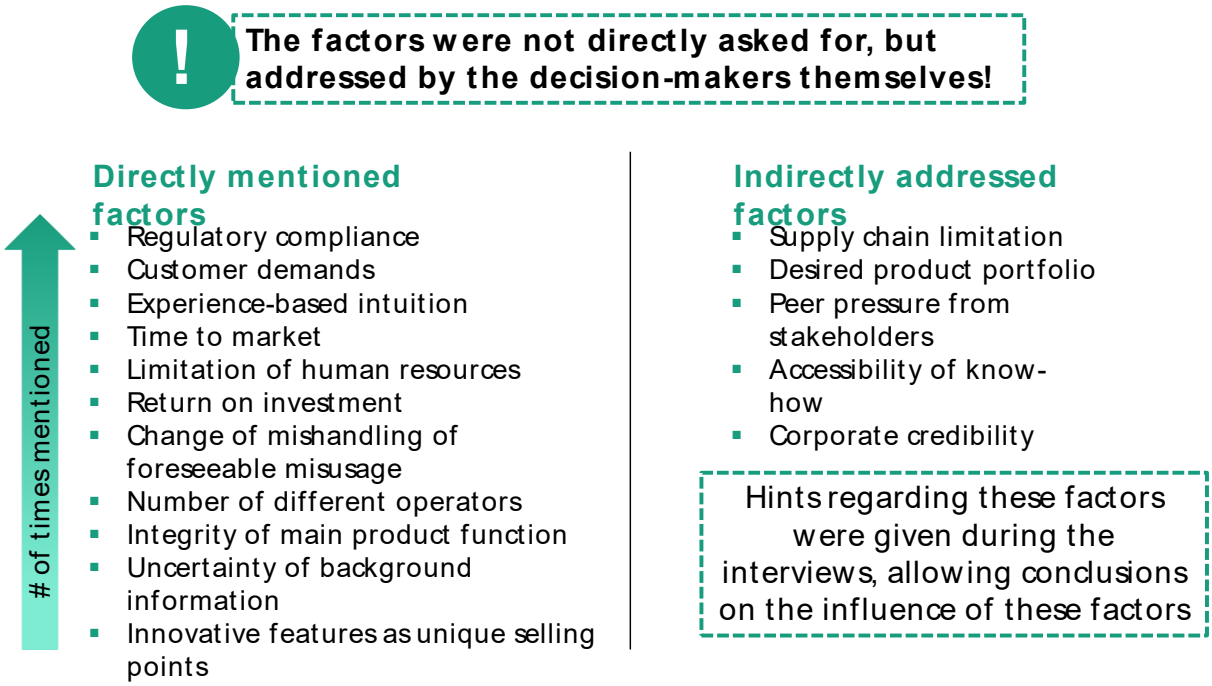


Figure 3.2: Emergence of decision-making factors in the semi-structured interviews

3.5 Model-Based Systems Engineering

MBSE moves the central point from document-centric to model-centric so the system information is collected, handled, and analyzed entirely inside a computer environment. Thus, the congruity of the information during the design process is not burdensome to support. Furthermore, it supports the traceability from requirements to system design, analysis and verification. [STEV12] In order to make different stakeholders during the lifecycle comprehend the model, a domain-specific modeling language and visualization and models must be described clearly and exactly [HASK11]

A computer model emerges from the system bestowing a unique source of truth in where documents, views and artifacts are created by request instead of acquiring system architecture and requirements in immobile and detached documents [BAJA16].

MBSE is valuable for different industries like healthcare [SCHN14]. The significance of implementing MBSE in the biomedical-healthcare systems is increasing. Proof of that is that the International Council on Systems Engineering (INCOSE) created a Biomedical-Healthcare Working Group (BHWG) to make evident the value and benefit of MBSE in those systems. Some of the challenges of these systems are to diminish the adoption time, guarantee regulatory, compliance and risk management requirements are fulfilled, reduce the cost, have consistency during the device design. [CORN14]

Delligatti refers to modeling language, modeling method and modeling tool as the three pillars of MBSE [DELL13, p.4]. Based on that, the following subchapter will be divided by those three pillars of MBSE.

3.5.1 MBSE Methodology

At the present, several MBSE methodologies are utilized:

INCOSE Object-Oriented Systems Engineering Method (OOSEM)

It offers a framework unifying object-oriented techniques, a model-based design approach and traditional top-down waterfall-style SE practices. In the beginning, it was founded on the Unified Modeling Language (UML) modeling, then was adjusted with Systems Modeling Language (SysML) in 2006. [PEAR12]

IBM Rational Unified Process for Systems Engineering (RUPSE)

This is an architecture framework established on four principles: separation of concerns (permit designers to tackle every set of stakeholder concerns alone), integration (accomplished by needing the utilization of a general set of design elements over various set of concerns), system decomposition (break down the system by structure) and scalability (accomplished by utilizing an identical framework). [BALM06]

IBM Telelogic Harmony–SE

The language employed is UML and variants. A combined group of workflows leads the developer to utilize the complete benefit of UML, this is defined in the Harmony process. [DOUG14, p.35] Moreover, the Harmony process copies the “Vee” lifecycle development model of system design. [ESTE08]

Vitech MBSE Methodology

This is founded on four primary concurrent SE activities connected and supported by a general system design repository, which are behavior analysis, source requirement analysis, architecture analysis, design V & V. [OMG11a]

JPL State Analysis (SA)

This methodology is grounded on a control architecture having the notion of state in its core generating requirements on system and software design expressed on models of system behavior. A common language shall convey thoughts between system and software engineers. [INGH05]

Object-Process Methodology (OPM)

This holistic approach makes it possible to model the system’s structural, behavioral, functional, and architectural features all in one framework [REIN04]. Formal mathematical grounds of graph grammars and a subset of natural language are the foundations of OPM [DORI11].

3.5.2 Graphical Modeling Languages

To describe and specify a system, graphical languages have been utilized for software development since the initial years of computer science as a good way to envision concepts. Entities of a system are represented as nodes and relationships as arcs in a graph. Keywords and the semantics of the association are conveyed by sentences [DICK13]. Next, a short review of the available graphical modeling languages is discussed.

Object Constraint Language

Text-based modeling languages like Object Constraint Language (OCL) were originally built to tackle the shortcomings of visual notation systems and today can either substitute or be combined with graphical notations. Started as add-on for UML, OCL has become a valuable textual constraint language associated with many more text-based languages. [BALA12]

Entity-Relationship (E-R) Diagram

The concepts of semantic modeling (depict the meaning of words) and object-oriented modeling are combined through E-R, which is a data modeling notation. Entities represented by rectangles, relations depicted by diamonds and attributes represented by circles are the three fundamental elements for a diagram. [DICK13]

Unified Modeling Language

Visualization, specification, construction, and documentation of the artifacts of a software-intensive system are the possible purposes to utilize the UML. Furthermore, it is adequate to model systems like enterprise information systems, distributed web-based applications and hard real-time embedded systems. Best utilized for a process, which is use-case-driven, architecture-centric, iterative, and incremental, but itself is process-free. [BOOC05, ch. 2] While being a very useful languages for highly abstract problems, UML's inner complexity and the laborious interoperability of bigger models can be cumbersome if tackling problems clos to the tech level [VARA12].

Attributes are defined by its formal name, type and multiplicity and may be detailed with a textual explanation to their purpose or meaning. [OMG11b]

Systems Modeling Language

SysML is derived from UML for depict systems and product architectures, behavior and functionalities [BALM07] and assists in the analysis, specification, design, verification and validation of complex systems [FRIE12, p.29]. SysML allows to stipulate requirements, structure, behavior, allocations, and constraints on system attributes associating in the exactly same view working as an open standard to assist engineering evaluation. [ISO17; BAJA16].

3.5.3 MBSE Tools

Some of the available commercial tools are:

- *IBM Rational Rhapsody* (IBM) is a tool that supports modeling and design activities, offer a collaborative design, development and test environment for systems and software engineers. This tool supports UML, SysML and AUTOSAR. [IBM18]
- *MagicDraw* (NoMagic) is a business process, architecture, software and systems modeling tool allowing several developers to work all at once on the same model. The language UML 2.0, XML[6] Metadata Interchange (XMI) standard for data storage is supported by this tool. [NO M18]
- *Enterprise Architect* (Sparx Systems) in combination with *MDG for SysML 1.5* offers an integrated modeling environment for systems engineer. It is recommended especially for complex system models. [SPAR18]

Several commercial and open source tools are accessible in the market such as Papyrus, Modelio, and so on.

[6] XML stands for Extended Markup Language, but is written as acronym within XMI

3.5.4 Issues in MBSE Adoption

Enforcing MBSE in existing organizations bears some challenges as modern systems utilize several models like CAD models, simulation models, product lifecycle management (PLM) part structures, software code and so on; the ideal of a unique source of truth becomes blurred [BAJA16].

Important reasons for an insufficient adoption of MBSE are missing interoperability and standardization in available tools, innovation lags in the organization's IT and immatureness of the product. In addition, stakeholders might present an aversion to change which acts as a psychological hindrance to MBSE and might lead to the product being out of date. [HASK11]

There are three main approaches to reach interoperability:

- Point-to-point: Every partner creates a customized solution. The outcome is a fragile integration (proprietary APIs, discordance version), which is complex to manage and where jobs are worked on in silos. This is costly because each pair of software system requires a committed solution giving a larger cost to user, consultant and vendor. When a software upgrade is released by a system provider, it is very likely that the APIs require modification. [RAY06; MATT10]
- Conform to a particular solution: each original equipment manufacturer (OEM) forces all partners to comply with a particular, commonly proprietary solution. This is very common in the automotive sector. This is a cost-effective solution for the OEM, but the partners are pressured to purchase and maintain multiple, redundant systems if they want to do business with some major OEM.
- Neutral, open standards establish the foundation of the infrastructure. This approach eliminates the problem of the first approach and reduces the issue of the second approach as partners can buy any software assuming the vendors implement the standards. Moreover, it gives uniformity in the representation of information, a fundamental property for long-term data retention, which is frequently acknowledged as a costly and critical problem for industries with long product lifecycles, e.g. aerospace. [RAY06]

There are also examples of mixed concepts. E.g. Model Bus is a tool integration platform developed by the team at System Quality Center at Fraunhofer FOKUS. A basic set of open source software are brought following the HTTP, HTTPS, XMPP, CXF, JMS, SOAP, OSLC standards for transportation. [FRAU14]

OSLC boosts free accessible joined integration utilizing a web style architecture and grounded in linked data [MATT10] . This group of specifications denotes the least number of protocols to permit tools functioning unitedly almost continuously but it does not standardized the performance of the tool [ELAA13].

3.5.5 Risk Management Models

Risk Management Capability Model

Risk Management Capability Model (RMCM) attempts to enhance medical regulations and their enforcement in software for MD by disciplining all risk management practices to conform to a software process improvement (SPI) model. It is aimed at supporting safe and effective software production. [BURT06; BURT08]

Multi-Criteria Decision-Making Model

The multi-criteria decision-making model ranks medical devices in relation to their criticality, in which ones with larger criticality ranking are allocated with the top superiority in the maintenance and management programs. This is achieved through a computerized medical management system. [CORC13]

MBSE for risk management in medical devices

There are some examples for MBSE implementation for MD. The first one is the INCOSE-BHWG challenge team, which developed an infusion and drug delivery system (IDDS) model to utilize as reference architecture during the device lifecycle in the biomedical industry [CORN14]. This generic model is useful to plan, develop and receive regulatory approbation of medical device [MAHE15]. The second one is the General Electric Health Care (GEHC) that uses MBSE techniques to execute behavioral analysis of fundamental system features and functions with the purpose of detecting and confirming system requirements, recognizing and itemizing subsystem functions and interfaces as well as seeding FMEA and develop system test scenarios. Some of the challenges faced are the shortfall of customer focus, issues of late integration or poor requirement leveling [UNGE14]. Another example is the Extracorporeal Membrane Oxygenation (ECMO) which provides a heart and/or lung bypass. ECMO is utilized in cases that the habitual course of action fails and the survival likelihood is between 20-25%. Very complex and dissimilar systems need constant observation from highly specialized personnel. MBSE aids by modeling stakeholders and their obligations at distinct places to discover similarities and dissimilarities. Furthermore, modeling assists in discovering places where human personnel is reduced by automatization of data acquisition. [PIHE14]

4 A Model-Based Approach for Risk Management and its Context

In this chapter, the research question, the research methods as well as the strategies and tools for validation are explained.

The interconnected objectives of this thesis under the context of model-based RM were presented in chapter 1.2. The relevant aspect shaping the methodological necessities for this research work is driven by objective five:

“Developing one iterative RM system for the whole product lifecycle integrating all stakeholders through unified visualization in different professional environments and ubiquitous model access”

Many of the conceptual benefits applying MBSE to the RM process such as enhancing communication between development stakeholders, enlargement of the capability to handle system complexity, improved knowledge acquirement and so on [JULI12] are linked directly to that notion. The chance to conceive one model-based RM system will contribute not only to the RM process in general but to the integration of all stakeholders through unified visualization and ubiquitous[7] access. These issues are explicated in chapter 3, where the gap in existing research is recognized.

This chapter will specify the research design chosen to illustrate which

- means of collecting and analyzing data,
- study cases including their surroundings,
- analysis approach and interpretation techniques

were selected.

Moreover, the potential limitations and problems with the selected research design and its implementation will be discussed.

4.1 Research Question

The scientific objective focused on developing a system.

As explained in the previous chapter, there is a research gap which has been addressed within the scope of the research project *Model Based Risk Management in MedTech.* Mastering the concurrence of complexity and comprehensiveness seems by far the most pressing issue in RM for future medical devices (→ 3.2, 3.3), resulting in the formulation of the following central research question:

[7] The access is ubiquitous (technical availability), but not universal (authorization).

Can a systematical and comprehensive RM on the whole product lifecycle of medical devices be accomplished through Model-Based Risk Management Processes?

This research question carries four more detailed subordinate questions which define tasks:

- How to vectorize all RM-relevant elements of medical devices' product lifecycles to allow computation?
- Can intangible influencers – here in particular: interactions – be modeled as elements of the device's system?
- What are the necessary and sufficient requirements for the implementation?
- Will augmenting established RM techniques with legacy information improve identification of critical characteristics and interactions?

Answering all four questions is considered necessary and sufficient to verify the thesis. The first question will be answered in chapter 7. Then, in chapter 8, the second and third question will be addressed. Finally, the fourth question will be tackled in chapter 5 and chapter 9.

4.2 Research Approach and Methodology

Based on the previous introduction to the problem statement of this work, it is placed in the science category as it is stated the goals (understanding, prediction and control), assumptions (determinism, in other words: cause-effect relationship and lawfulness is discoverable), scientific method (empirical referent, repeatability, self-correcting, systematic) [LAMM05, pp.3–6].

This work can be located according to the Ulrich [ULRI76] classification of science, shown in figure 4.1, under empirical sciences[8]. Formal sciences endeavor the development of languages that is sign systems with controls for the utilization of the signs. Conversely, empirical sciences strive for the description, explanation and configuration of experiential, observable real detail. [ULRI76]

[8] Nevertheless, the strategy for applied science proposed by Ulrich [ULRI84, bk. II s. 4.4] explicitly includes the methods from formal science in the inventory of its methodology box. This means that in this work, the step from recognizing the deficits in current RM (practical | empirical) to the conceived solution (practical | inferential) would not be explicable without fundamental modeling theory and metaphysics (theoretical | inferential).

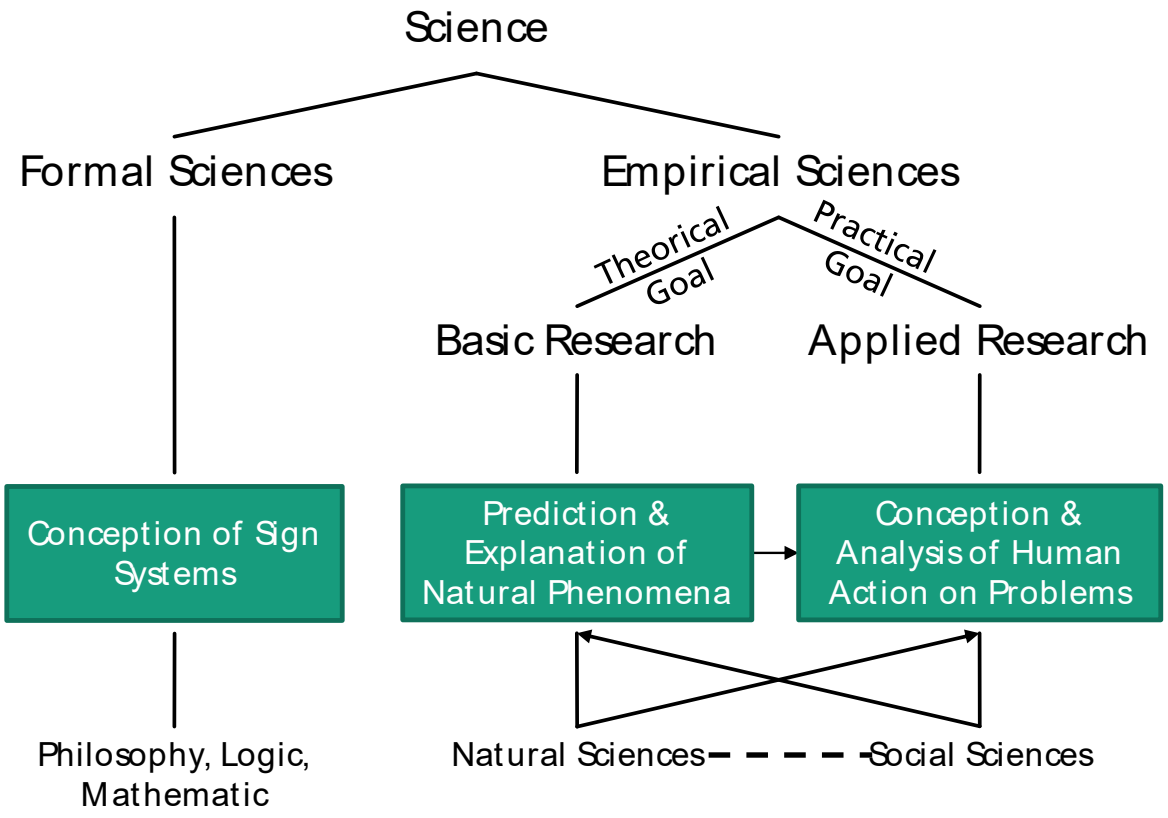


Figure 4.1: Taxonomy of science (own translation of fig. 1 "Wissenschaftssystematik" in [ULRI76])

The problem statement in the case under consideration is based on the insights in the entrepreneurial practice "applied". For this reason, this work is located in applied research and it follows Ulrich's strategical proposal [ULRI81; ULRI84] (→ fig. 4.2, left side). Applied research strives to discover an explanation for a pressing matter in the society or an industrial/business association [KOTH04, p.3]. In addition, it does not describe the validation of the theory of the examined problem but rather the practicability of models and rules for the behavior of scientific fields in the praxis [ULRI84]. The model and its respective requirements and testing are organized in the MBR research project. Following Eden's idea of the three paradigms, the verification of the system through the implementation and application of a software demonstrator is part of the technocratic paradigm [EDEN07]. The practical validation of the thesis would since be located in the realm of social sciences.

As it is depicted in figure 4.2, the first chapter attends to give an introduction into the subject. Chapter 3 collects the challenges facing RM and MedTech companies. The essential scientific roots, the orientation and the modus operandi of the work are described in this chapter. Research questions are introduced in the next chapter and it is described how it will be attempted to answer them; also, the selected research methods are listed in this chapter 4. The foundation of the model is presented in chapter 5. The results are presented in chapters 6, 7 and 8 and validated in chapter 9. Finally, the discussion of the results and an outlook on future research opportunities in chapter 10 conclude the main part of this dissertation paper.

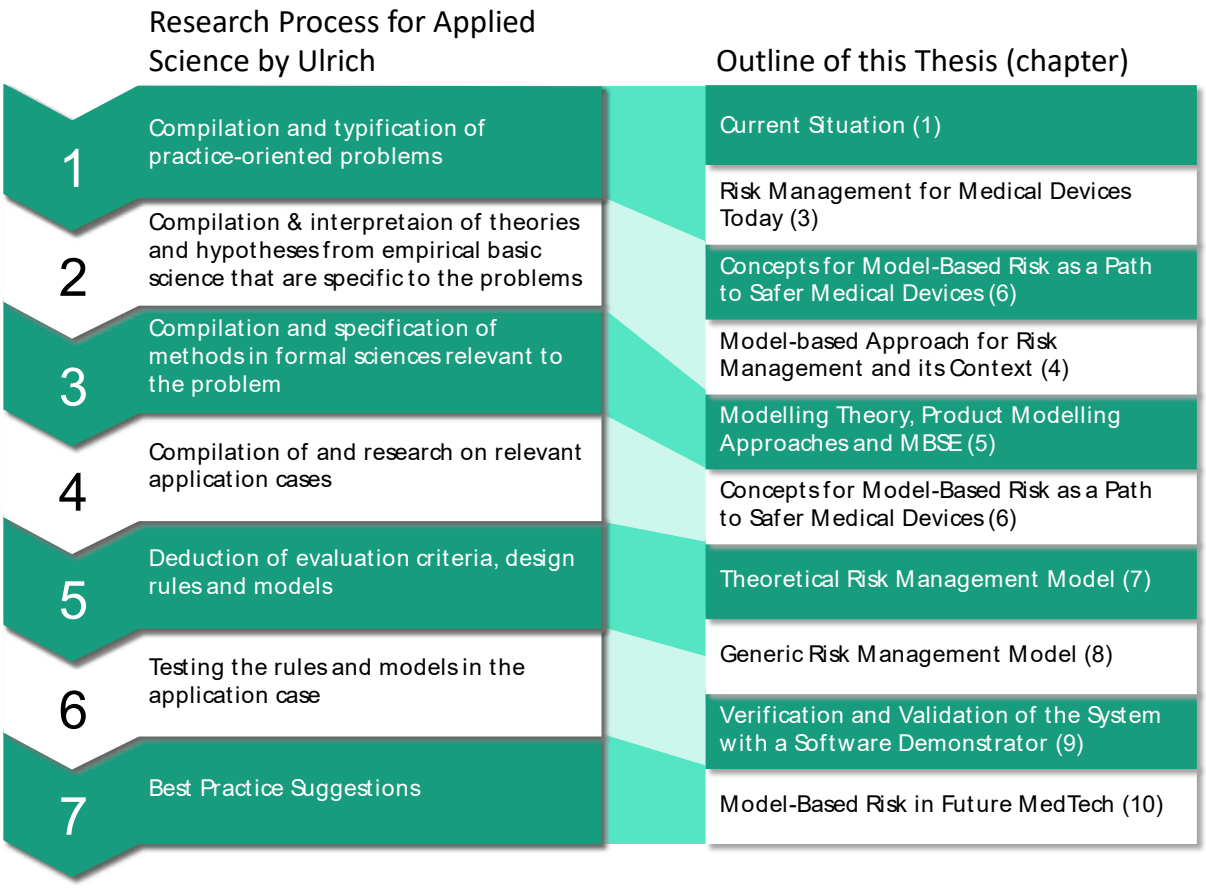


Figure 4.2: Structure of the thesis

In order to select the appropriate research method, it is necessary to find the suitable type of research design according to the objectives of the research project. Research design shall offer a framework for the gathering and analysis of the data produced by the investigation and afterwards point out the apt research method [WALL11, p.13]. Three conditions were suggested by Yin [YIN18, p.9] to differentiate the various research methods: the form of research question set forth, the control a research worker owns over actual behavioral events and the degree of focus on contemporary contrary to historical events. Five research methods are connected to these conditions (→ table 4.1), each of which aligns with certain types of research questions that can be reduced to interrogatives.

Here, the research question that fits the focus of the MBR research project best is “how, why?”. Moreover, there is no manipulation of the behaviors of the events and it is concerned with different evidences from the past and present (contemporary events) [YIN18, p.9]. Taking all these conditions into account, the most suitable research method for the validation of the main thesis is the case study.

Table 4.1: Relevant situations for different research methods, from [YIN18, p.9]

Method	(a) Form of Research Question	(b) Requires Control Over Behavioral Events?	(c) Focuses on Contemporary Events?
Experiment	how, why?	Yes	Yes
Survey	who, what, where, how many, how much?	No	Yes
Archival Analysis	who, what, where, how many, how much?	No	Yes/No
History	how, why?	No	No
Case Study	how, why?	No	Yes

Qualitative research may bring a particular analysis of a relevant theme using the information gathered by case studies, ethnographic work, interviews, and so forth. Furthermore, a researcher can create theories or hypotheses, explanations and conceptualizations from specifics contributed by the participator; hence, it is considered inductive [HARW11]. Quantitative research tests statistical hypotheses in order to generalize the found characteristics and so is defined as deductive in nature [HARW11].

Essentially, this research is mostly of a qualitative nature, though efforts to quantify some parts of the results are made. The main thesis is formulated as a closed question in a way that a successful implementation of the RM system that satisfies all set requirements will suffice as answer. Its incorporated goal is to find an active solution to a real-life problem; an empirical evaluation of the statistical superiority of the solution could only be achieved in future field test of a near-commercial or commercially released version of the system.

The theoretical concept for MBR is deducted by reasoning from the shortcomings of its logical opponent: risk assessed, evaluated and controlled with document-based approaches which forms the state of the art in most of the manufacturing world, including the MedTech sector. At this point, it is critical to discriminate clearly between risk and RM. Model-Based RM cannot exist in opposition to document-based RM, but rather is an advancement to it. Consequently, the conception thrives to integrate approved document-based approaches into the system, albeit it does not embed any specific method in its theory. This set-up shall also provide for a sustainable development of consecutive concepts in the predominance of document-based RM approaches.

The primary goal of the practical part of this work is to implement MBR in a fashion that increases the comprehensiveness and systematicness of the RM process in the product lifecycle of a MD. Here, an RM process using prevalent document-based RM techniques is set up against one embedding the same techniques in a model-based approach. This provides

the basis for a qualified comparison and allows for the execution of a case study without the need to extensively train the participants (avoiding ungovernable level of effort). To apprehend instances of the product lifecycle of a MD and to understand the influent aspects of the stakeholders involved, a thorough examination of the study objects is at place. It is necessary to gather data from many origins, like the type of stakeholders involved, type of data existing to feed the model and DB, functional and procedural designs and so forth. At the same time, the state of the prototypes and the user interaction must be documented.

While carrying out the case study, all changes to the model and supplied documents and the creation of new documents must be protocolled. Any noteworthy observation regarding the execution and the linked behavior of participants and the staff needs to be recorded.

The research project *MBR in MedTech* in its entirety is an interdisciplinary endeavor. The technical disciplines of production technology and quality management are the main subject areas for the evaluation of the results. Preparative works in the research project are also using methods from empirical social research and organizational psychology. Besides computer science and software engineering, the development of the software prototypes involved applied linguistics and biomedical engineering.

4.2.1 Literature Research Methodology

The literature backing up the research concerning the first two objectives in section 1.2 (MBR core, iterative RM system) is mostly related to document-based RM methods and techniques, the RM process, external factors influencing the decision-making in RM as well as graphical modeling languages. The remainder of the objectives is satisfied either as follow-up on the first two (and thus relies on the same literature) or based on literature from MedTech or Health-&-Life science background.

Conclusions mainly drawn from the literature research include: the deficits of document-based RM methods and techniques, gathering factors inhibiting the decision-making in risk treatment, available graphical modeling languages and their suitability to describe a complex medical device's product lifecycle and of course statistics and figures highlighting the state of the art and the scope of the problem.

The literature research was structured according to the following steps indicated in [COOP09, 80ff]. The topics for the search process included RM methods and techniques, fundamental standards and guidelines for medical devices, literature recommending or regulating the medical devices, linguistic works about the use of verbs in English, modeling theory, standards concerning product modeling, influences on decision-making processes.

To reduce false negatives (relevant sources not identified), a keyword mapping clustering the terms by topic including all known synonyms and appropriate related terms was created (→ annex A, fig. VII.1). Then, search profiles containing combinations of these search terms and if necessary additional fix query terms were built; table VII.1 gives an example. The search was conducted in the e-Lib DB from Fraunhofer, which includes around 100 million datasets (from WTI Themenpaket "Technik und Management" (TEMA), Scopus, Web of Science,

Institute of Electrical and Electronics Engineers (IEEE), Springer, Elsevier, etc.) as well as with the tools of the main library of the Rheinisch-Westfälische Technische Hochschule (RWTH) main library, which searches the inventory, subscriptions and literature lists of the central and decentral libraries of universities and other educational institutions in Northrhine-Westfalia, Bavaria and various other German states[9]. In all cases, the mode was set to searches in subject indexes with specific reference to the last 30 years (1987-2017)[10].

The resulting lists for each search profile were merged eliminating obviously implausible hits and duplicates. Then, title and abstract were evaluated to determine if the document has some relevance.[11] If the document appeared relevant, the document was examined. Moreover, a hand search of the examined literature was done using footnote chasing, which retrieves the preceding items. Intermittently, the previously conducted searches were revisited using only the most recent year in order to not miss any recent developments.

4.2.2 Standards and Guidelines

Apart from the literature research, a profound understanding of the industrial standards, the regulations including some of their legal implications, the organizational structure of regulators and guidelines regarding medical products is a prerequisite to this work. However, a planned search process like in subsection 4.2.1 would most probably not lead to an adequate orientation and training in this area. Instead, a strategy similar to that of a web crawler was used, searching for references in corresponding literature and a basic set of standards and guidelines[12], crawling link-to-link until looping back to already crawled documents. While this method is certainly slower and not as efficient as the one above, it is effectively more thorough[13].

4.2.3 Theoretical Framework

The theoretical conclusions the MBR approach is based on ought to be grouped in the realm of technological research which differs from the classical theoretical research (e.g. in natural sciences) in the indispensability of an artifact to render innovation, cp. figure 4.3. Without the development of the MBR system, the thesis question could absolutely not be scrutinized.

---

[9] The *finc* architecture alone claims 120 million datasets. Find the members here: https://finc.info/de/anwender

[10] Older documents will still show up if sufficiently referenced in newer ones.

[11] Usually, these two steps brought results down by one to two magnitudes.

[12] It was either already established in the author's education and continuous training (QM/RM, some MD) or had itself been built using Cooper's search strategy (MD, product modeling).

[13] Of course, it would draw a lot of duplicates to the similar, but laxer footnote chase.

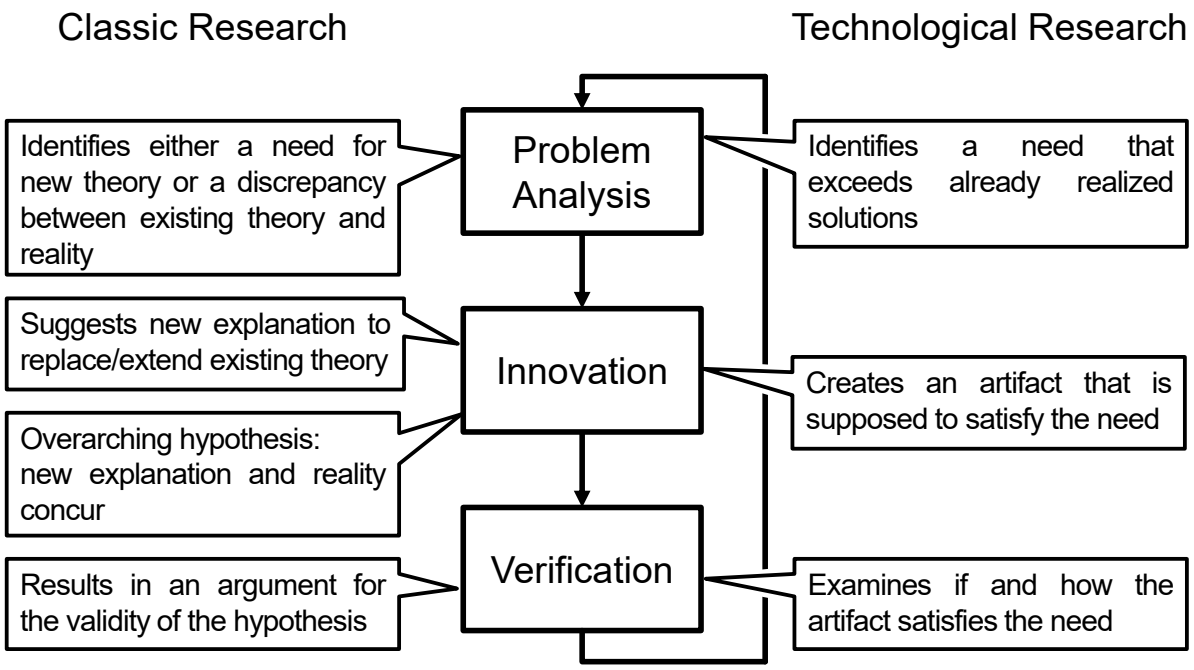


Figure 4.3: Comparison of the main steps in classical research vs. technological research, based on [SOLH07]

The data compiled from the literature research was subjected to a qualitative analysis in order to extract and classify the information on

- deficits in RM in general and RM for medical devices in particular,
  - whether those deficits are endemic to document-based approaches,
- strength and weaknesses of all common RM methods and techniques,
  - how these behave in the conflicted concurrence of complexity and comprehensiveness as well as
- which advances to the former issues had been achieved with MBSE in other areas.

After discovering that there was not enough empirical groundwork as to how those issues interacted with decision-making in risk treatment, thus which starting points would be promising to mitigate the effects on the RM process, a study including semi-structured interviews with MedTech decision-makers was scheduled.[14] After analyzing the findings (→ 3.4.2), an online

[14] The results of a literature review conducted by Bryman about research methods and research design reported that 71.1% of the articles carry out a semi-structured interview or unstructured interviews for qualitative interviews. Moreover, the unification of survey instrument and qualitative interviews was found in 57.3% of the articles [BRYM16].

survey focusing on more details concerning the occurrence of the factors and the relations with organizational aspects was set as second stage.[15]

The conception of the theoretical RM system was largely achieved through logical reasoning. After identifying the unsatisfied needs through abductive reasoning from the key features and deficits in which known RM methods and techniques vary, possible design improvements and design conclusion were deducted from the comparison of those needs with the rules and objectives from standards and guidelines (gap/opportunity for innovation). The RM system was conceived to render a probable solution to fill the gap (inductive reasoning). The three types of logical reasoning are depicted in figure 4.4.

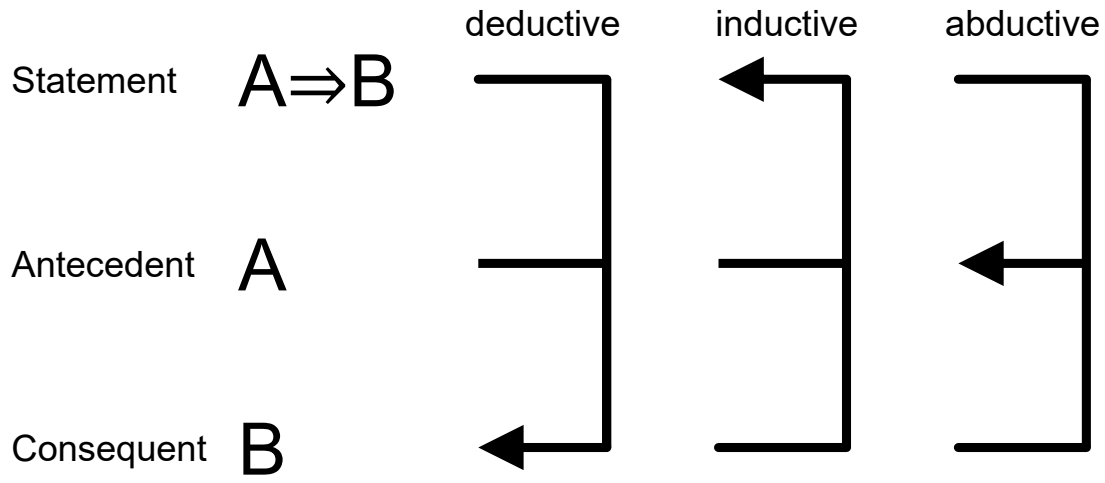


Figure 4.4: Types of logical reasoning

4.2.4 Conception and Creation of the Technical Solution

The innovation was linked to the idea that it would be instrumental for a superior system to combine the strengths of human experts and computation. As the research question is based on a model-based RM approach and all relevant product (lifecycle) models used by MedTech manufacturers (at times: unwittingly) follow the pragmatic modeling approach (→ 5.1), it is consequential to follow the MBSE principles in the de-facto standards agreed on by INCOSE and Object Management Group (OMG) (e.g. [OMG11b; BEIH14; ISO17]). Hence, modeling language and model structure were selected by eliminating and recombining the common

[15] The results of this survey are not subject of this dissertation, though, as the outcome in German-speaking Europe was too low to deliver significant results. However, the author and her research partners are preparing to expand the survey to other regions.

choices. This way, a maximum of compatibility with the technical environments as well as the mindsets of the stakeholders in MedTech was pursued.

The details of the selection process are described in section 5.3.

4.2.5 Implementation

As a proof of concept, a demonstrator of the MBR system was built, then subjected to different stages of examination, as described in the next subsection. Before designing the original software though, decision regarding the ready-to-use software[16] had to be made. As it was foreseeable that there would not be any abundance of software solutions in any of the touched engineering and design areas, morphological methods could not be used. With few to choose from, options were evaluated for functional suitability instead. The ISO 25000 family thereunto names three subcharacteristics [ISO11]. The functional completeness was ranked by comparing features qualitatively with specification sheets. Functional correctness was tested with a dummy model (→ fig. VII.6). As there was no reliable way to test the functional appropriateness of the ready-to-use components without interacting with the prototypes, the step was initially replaced with an ad-hoc assessment and later on integrated into the user tests – which in one case led to a replacement.[17]

Following, the main methods used in software design and prototyping will be introduced. If not otherwise referenced, descriptions of the methods can be found in [LAZA17b].

Use Case Analysis

To further the technical requirements on a role-based level, target users and according use case scenarios are specified. Preconditions and postconditions are identified and the scenario is sequenced into steps so that each step is definable independently of the scenario's context. From the emerging use case diagrams, the steps can be developed into routines to be implemented.

Paper Prototyping

Using paper-based techniques is a flexible way to create prototypes of low fidelity. Typically, different diagrams and displays framing the components, functionalities and interfaces will be sketched (printed or drawn by hand), then presented in briefings where all common creativity techniques (like brainstorming, mind mapping, TRIZ) may be applied to modify the prototype. The high communicative value of paper prototypes also reduces the risk of missing key information in interdisciplinary teams.

---

[16] that is all software used without major code base changes, so to say "bought-in" software

[17] Despite a lower ranking in functional correctness, Modelio replaced Eclipse/Papyrus due to the sheer number of issues raised concerning the API connection (→ 8.1).

Software Mock-Up

Next, medium-fidelity prototypes were built based on so-called software mock-ups, that is pieces of interfaces and network sequences that pretend to satisfy use cases but bear no backend functionality. The mock-ups helped to clear dependencies between the tools and the model core and were the medium on which the first usability tests with externals were based. In addition, they aided in evaluating the choices in ready-to-use background technologies.

Functional Prototyping

Finally, the MBR core and successively the tools from the software layer were set into high-fidelity prototypes which were developed gradually in functionality and behavior to meet prioritized intermediate targets. As computational speed and security were not emphasized for the case study, functional prototypes that satisfied the expectations were directly adopted for the software demonstrator, only modifying them to serve certain experimental aspects (e.g. replacing actual functions and displays with fixed output).

4.2.6 Validation and Verification of the Model

Before explaining the methodology for validation and verification, it is necessary to understand the difference between them. The first one refers to the accomplishments of the requirements for a predetermined utilization or application by objective proof. The second one, verification, proves the accomplishment of indicated requirement by supplying objective proof. [ISO15a]

Usability Testing

The basic outline of the testing methods and techniques described in this subsection can be found in [LAZA17a]. The verification process included various stages of usability testing. Early on, the author and her team applied heuristic evaluation on the use cases to discover errors in reasoning. In the next step, inexperienced users were confronted with simple data handling and modeling tasks to detect flaws in basic usability.

Think-Aloud Evaluation Technique

This technique is a strong instrument for checking user interfaces with inexperienced end users. The technique is aimed at gaining a clear image about the thinking process of the end user. This is very advantageous for insights on true levels of information or confusion about the interface, the usefulness of system feedback or any impediments performing given tasks. Adversely, the nature of this technique impedes tracking progress among a fix user group.

Participants are instructed to speak out loudly any thoughts about the tested software while they perform an appointed task. The examiner remains silent after the initial instructions. The sessions are recorded, observed and protocolled.

Focus Group Workshops

Aiming at more sophisticated testing, working with focus groups featuring well-experienced users of common skills or professional background is a very productive method to provide insight into advanced aspects of usability like expected behavior, cross-application user conduct and ergonomics. In the MBR software demonstrator, these were no criteria per se, but rather elements to facilitate acceptance for the augmented RM process among future participants.

Beside testing with appointed tasks, the users were encouraged to voice more holistic criticism, draw comparisons to commercially used tools and suggest improvements based on their experience. The participants were free to interact with the investigator, first performing one part of the test individually, then in open exchange. The sessions were filmed for analysis; both the investigator and the users took notes which were labelled with pseudonyms and collected.

Requirement Compliance Testing

The final tests before service were conducted by the author, two software developers of the research team and five externals with proficiency in the use of product modeling software and engineering background. After informally evaluating the compliance in this group of eight, a formal validation was carried out checking each requirement within the specification individually.

A summary of the whole validation can be found in table VII.2 of annex B.

Case Study

In order to test the superiority of the conceived RM system and verify the developed tools, a comparative case study was conducted.

A case study is a particular example of a limited system, often intended to instance a more common principle. One of the advantages is that it allows to observe consequences in actual contexts determining cause and effects. [COHE09, p.253] In this research, a case study examines the advantages of a model-based RM for an automated stem cell platform delivering all necessary premises: a safety-critical system, a complex medical device system, a network of self-contained interacting medical devices and the presence of various professional mindsets due to an interdisciplinary group of stakeholders. Also, this work shall compare the results of the case study to the endemic deficits of RM methods and techniques found in the literature review and in the antecedent practice-oriented studies in the same research project.

The main disadvantages implied in the use of case studies include concerns about the strictness of implementation, difficulties to generalize the findings, the unpredictability of the workload and the level of effort needed, the unclear benefits over empirical trials as well as the risk of an unfavorable reception by the scientific audience based on their bias built on the exposure to popular-science case studies which do not meet standards. [YIN18, p.18]

The RM methods implemented to do the risk assessment process in the automated stem cell factory (SCFIII) in Bonn were QuickRiskCheck (QRC) and Failure Mode, Effects and Criticality Analysis (FMECA). Workshops were done for both methods where the participants were introduced to the respective method and trained with examples and a short exercise run.

Quick Risk Check

QRC is a method to identify the most critical process steps of project or products. It is suitable for entry-level RM in interdisciplinary panels with relatively short introduction. The steps followed were: process definition, process segmentation, process prioritization (by pairwise comparison), detailing the process steps (with the 6M), risk assessment and definition of the measures. [ZENT12]

This method was chosen because of its time efficiency in amounting analyzed risk if measured by impact. In this way, QRC helps to voice the most important risks as seen by stakeholders of the different professional mindsets and to then agree on a ranked list of the most urgent risks to treat. Comparing QRC scenarios with and without MBR backing would give a good impression on whether RM panelists would per se accept input from the MBR system when they could not control the provenience of the information.

Failure Mode, Effects and Criticality Analysis

FMEA is used widely in the industry to define, identify and eliminate errors or issues from the device, process or design before it reaches the end user. [STAM03] FMEA aims to identify all known and potential failure modes (FMs) as well as their causes and effects, prioritize them based on how critical or relevant it is and plan corrective action. Prioritization of risks is done using a metric known as risk priority number (RPN) which is a product of frequency of occurrence, severity and detection (D).

The steps followed were: plan the FMECA, identification of the functions and performance standards of item or process, identification of FMs, identification of local and final effects of FM, identification of failure causes, identification of detection methods and existing controls, determination of severity of failure final effect, estimation of the likelihood of FM, identification of actions. Then, it was decided whether a criticality evaluation (CA) was required. For the SCFIII, it was necessary to do the CA as the RPN as mere product was deemed not reliable on its own, because different combinations of SOD can yield the same number of RPN. Therefore, a ranking of the FM according to the values of RPN was shown to the experts. They were asked to choose the last critical FM in the RPN ranking. Then, the name of that FM was located in the SO ranking and that FM and any above would need to undergo the qualitative CA. The evaluation of the criticality was done with the help of a matrix where every FM was assessed according the occurrence and severity. Afterwards, every FM was located in the matrix with the input of O and S. The matrix has the following levels of criticality categorization: 1 (unacceptable), 2 (undesirable), 3 (acceptable), 4 (minor). [DIN15] This methodology was followed for the System FMECA and the Process FMECA.

5 Modeling Theory, Product Modeling Approaches and MBSE

In the beginning of this chapter, an explanation of the modeling theory will be given. Then, an overview of the product modeling follows. A detailed definition of ‘model’ is laid out in section 2.4. Finally, a description of the available modeling languages, methods and tools will be given.

5.1 Modeling Theory

Because models cannot exist on their own terms, but only as a result of the creator’s definition of the original, it is wise to discuss the different modeling concepts before analyzing which might be the best modeling approach. Schlitt [SCHL04] has compiled five major aspects from Steinmüller’s model concept and applied them on Stachowiak’s GMT (→ fig. 5.1), amongst others. Answering the following central questions shall clear the epistemological positions behind the preset background the model will rest upon – alas recover the modeling aspects of the product models our meta model is based on – and lead to the preferable modeling approach:

(A) Functional aspects. What is the relationship between the model (as the modeler's output) and its object area (as the input provided by the task set)? How are potential intermediate outcomes relevant to the relationship?
(B) Methodical aspects. Which methods and techniques will be used in the construction of the model? Can it be divided into independent partial procedures? If so, how to integrate the partial solutions into a fully functional model?
(C) User aspects. How does the specification of the user affect the modeling objectives as input for the construction? What is the relationship between the model creator and the user and how does their interaction influence the modeling process?
(D) Objectives. Which conclusions can be drawn regarding the modeling objectives? How does the model’s purpose resonate in the use case and how important are the several objectives individually and in concurrence therefor?
(E) Contextual aspects. Besides the modeling objectives, usually there will be also non-purpose-led restrictions, given e.g. by the choice of components in the realization of the original or unchangeable organizational workflows. These build a framework whose influence on the model needs to be respected as part of the task in order to keep it purposeful. [SCHL04]

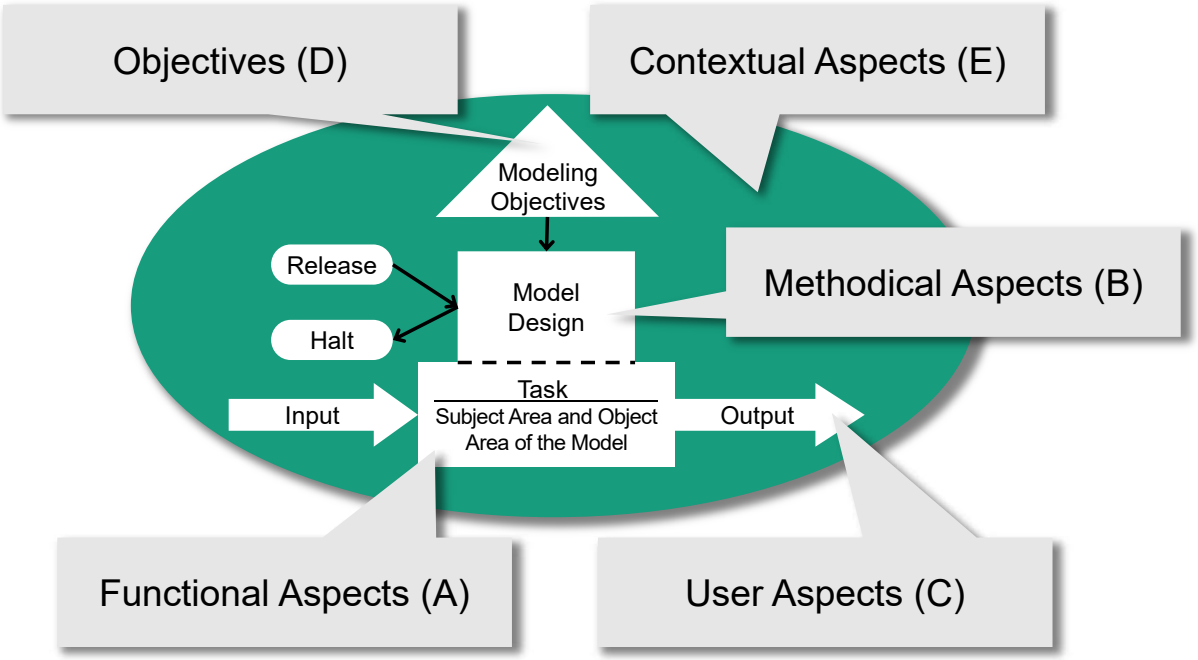


Figure 5.1: Modeling aspects and their influence on model building, based on [SCHL04]

Schlitt acknowledges that these five questions are not answered by the concept of a model the theory of reflection[18] provides. In particular, the methodology behind a modeling process cannot be abstracted from the imaging process[19]; herein, the conscious act of selecting model elements and their properties remains unheeded by a purely materialistic view – missing out in what Stachowiak calls the model's operationality. The functional aspects can only be acknowledged through their correspondence. By methodical aspects, the imaging process is regarded as being the algorithmic solution itself. The remaining three aspect are not even in the scope of the imaging theory. [SCHL04]

5.2 Product Modeling Approaches

A whole lifecycle of a system may be divided into fundamental stages depicting the superior advancement and accomplishment of milestones. In many instances, the following seven are found: ideation/market analysis, concept, development, production/manufacturing, utilization/application, support/maintenance and retirement. [ISO16]

[18] The theory of reflection is also known as reflection theory or imaging theory, not to be confused with the image theory, that is the theory behind image processing.

[19] E.g. Lenin defines an image as our reflection of a thing that „exists outside us“. By this theory, those images are verified by confirming predications in the practice of the original, thereby building a reality. [LENI08].

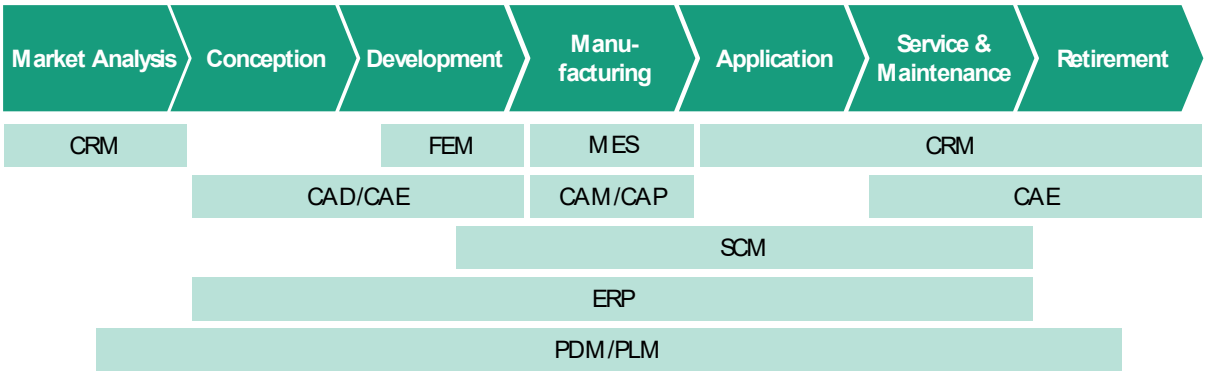


Figure 5.2: Product models throughout lifecycle, modified from [VDI16][20]

Typical product models and their positioning in the product lifecycle are shown in figure 5.2. All of them are feasible inputs for an RM model; as a whole, they cover relevant RM information from all organizational units. Just as well, they are all pragmatic models sacrificing quality of the projection for fitness for purpose. Which structural and content information can be expected from which product model type is elaborated in section 7.3.

5.3 Engineering Decisions

The results of the literature research on the available graphical modeling languages, shown in appendix C, table VIII.2, were used to categorize the modeling languages according to its field of application:

- Systems modeling – models for describing systems either software or hardware or both.
- Software modeling – models for describing software
- Process modeling – models for describing a process for e.g., business process, project process.
- Conceptual modeling – models describe design or software concepts
- Data modeling – models describe data and its relationship

Though all the categories are in a way addressing a whole system, systems modeling as a common category overlaps the rest, see figure 5.3. Since the model diagrams represent medical systems and their components, the best suited category of modeling, among the five mentioned above, is systems modeling. Thus, all the remaining categories and the modeling languages that come under them were eliminated. The search was continued to get the evidence of application of each modeling language, by looking for the literature concerning these modeling languages – to get an in depth idea about the area of application of these modeling languages and their relevance to the topic of interest, (→ table VIII.2).

[20] Please refer to the list of abbreviations (→ II) for the full names.

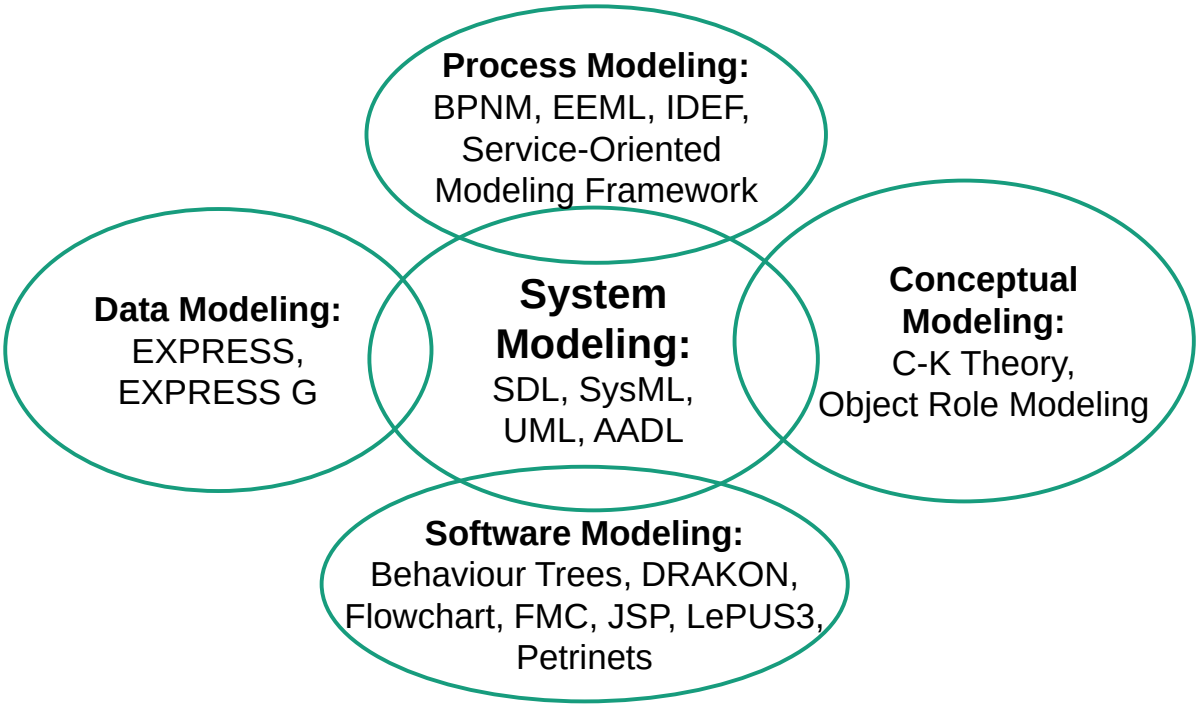


Figure 5.3: Relationship of the shortlisted modeling languages and their categories

After choosing the application category of the modeling language, still four different modeling languages were left: Architecture Analysis & Design Language (AADL), Specification and Description Language (SDL), SysML and UML. In a following list, along with the aspects that would help in representing a system, the focus was set on learnability, documentation, ease of understanding, among others.

Following, the reasons for omitting a modeling language were:

- The chosen modeling language should have specific type of diagrams/ elements to describe a system and its complexity.
- It should not be ambiguous in giving out the information associated to the model elements.
- Should be well developed, so that enough documentation and online help is available to learn the language and its constructs.
- Should have modeling tool support, to build the models/ diagrams.
- Should be less complicated, for smaller learning curve.

Respecting the conditions mentioned above, UML and SysML were evaluated as appropriate. More, documentation and online help for UML and SysML are far superior in comparison to the other two.

The above two modeling languages were chosen because the modeling components and the models they offer fit perfectly the mode of operation of this RM system. The modeling language chosen is SysML, complemented with some elements of UML 2 in order to aid the purpose of clustering the components using the class.

Both UML and SysML provide structural decomposition and interconnection of a system via ports, parts and connectors [ROQU11], behavioral decomposition via sequence and activity states. But the vocabulary of UML-2.0 remains too software oriented, e.g.: objects, classes etc., SysML offers systems engineers the following advantages over UML for specifying systems and systems of systems. It describes SE semantics better than UML. It reduces UML's software bias and adds two new diagram types for requirements management and performance analysis. Requirement diagrams and Parametric diagrams respectively. SysML is smaller and easier to learn than UML, since it removes many software centric constructs [RUMP02].

The block definition diagram from the SysML was used to depict the medical system chosen. The language specification used at the end is not proper SysML, but inherits UML 2 elements, that are not allowed in SysML due to the will to reduce the element types to just blocks, packages and composites. The sub-classification of block elements and the way it is used composites is valid UML 2, but SysML elements specs are strictly based on UML 1.

5.3.1 Selecting a Modeling Tool

While looking up for the available modeling tools, open source tools as well as proprietary tools came across. Proprietary tools were decided to be excluded in this research for the following advantages that the open source tool offers:

- Open source developers choose to make the source code of their software publicly available for other developers to try it out and contribute to the software. They make the software customizable. The developed API will be interacting with the files in the tool – extract information from it and manipulate the information in the file. The intention is to modify and adapt the available software according to requirements. In the line-up needed for this work, it is deemed not to be possible with the proprietary tools because of the permission and license issues [HERO13].
- As developers, there will be freedom to use the tool the way it is needed. There would be no obligation to upgrade the versions with the software updates – any version of the available software may be used, unlike the proprietary tools that would make the older versions obsolete after upgrading the tool and make the update mandatory.
- Since open source tools are free, the number of people using them would be higher compared to the proprietary tools. That means, the tools would be popular and the amount of support online and tutorials on using the tool would be higher [HERO13].

After deciding on the modeling language, choosing an appropriate modeling tool was a throughout logical task as there were two important criteria to be met:

- The modeling tool should be compatible with the UML and SysML modeling languages.
- The modeling tool selected, should be an open source software.

The above two criteria were a great influence in filtering out most of the tools that were available in the market. A shortlist of tools was made, owing to the criteria mentioned above is given in table 5.1.

Table 5.1: Shortlisted MSBE software

Tool Name	Description
Modelio	Supports UML and SysML standards among others. Easily extendible modules XMI import/export
Papyrus	Based on UML and SysML standards Addresses specific domain, every part of the papyrus can be customized
SysML Designer	Based on eclipse Sirius and UML Designer module. Open source software, Install SysML Designer Module in UML Designer project
Topcased	Developed by eclipse working group. No clear documentation available Version support of eclipse not mentioned.

New conditions were added to choose the right tool as it follows:

- The tool's interface should be simple
- The model file should be easy to understand, so that it can be manipulated easily
- The tool should be easy to use with a steep learning curve in the beginning.
- The tool should support importing exporting of model files

Each tool was tested by first trying to replicate a model template as shown in figure 5.4.

5.3.2 Explanation of the Template of Hemodialysis System Model with Datatypes

Figure 5.4 shows an extract of the product breakdown structure of a hemodialysis system model. This was used to generate a template for choosing the modeling tool as can be seen in annex B, figure VII.6. This template was built in all the modeling tools available and checked for the tool's functionalities with it

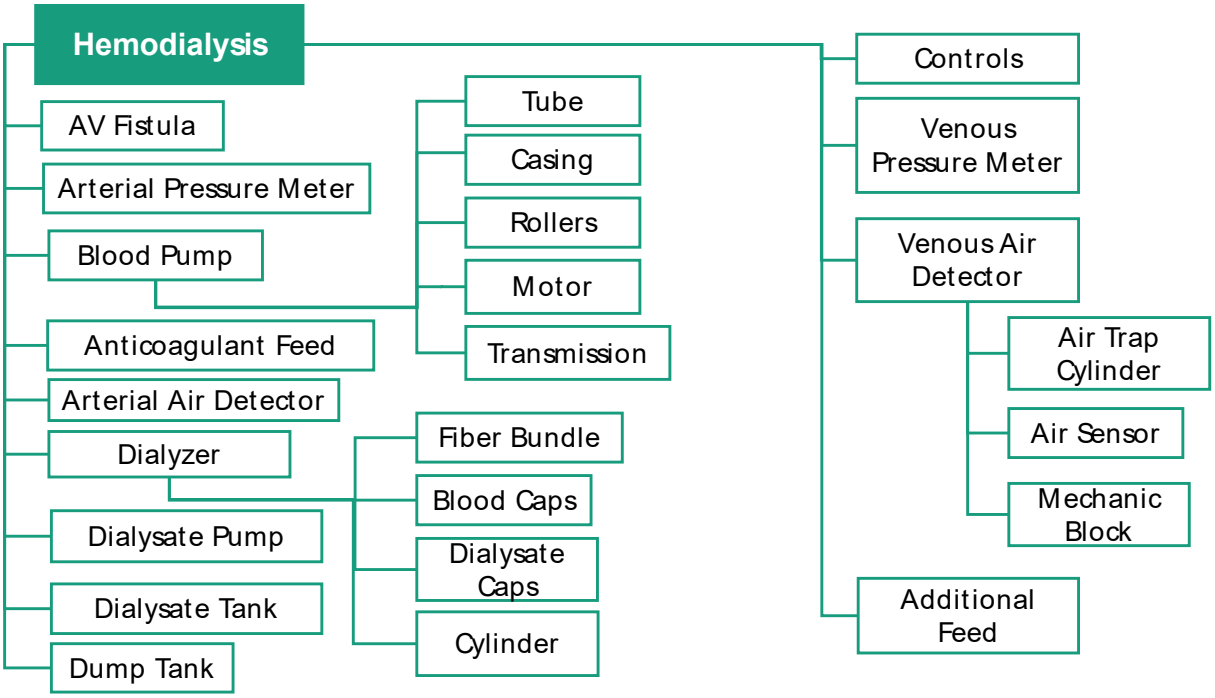


Figure 5.4: Product breakdown structure of the hemodialysis system

GMDN DB was used to select the class names for the assemblies. All the components in annex B, figure VII.6 were looked up in the DB, to find the standard names and the corresponding standard names were chosen as the class names. The attributes were also chosen similarly.

The parent class is the Hemodialysis System (HS). The components of the hemodialysis system form the remaining 9 classes: Fistula Needle, Additional feed, Controls, Pressure Meter, HS Blood Pump, Anticoagulant Feed, Air Detector, HS Dialyzer, HS Dump Tank with the composition association form the children of Hemodialysis System Class. The parts of the component classes form their respective children with the composition relation. Here, the main datatypes are the basic UML datatypes: string, integer, float, Boolean.

5.3.3 Conclusion derived after testing the tools

Based on table 5.1, product models for four tools were finalized and compared for different aspects like usability, completeness, interoperability etc. Out of the four tools chosen, three are based on Eclipse. Overall, one of the main points at issue with the tools based on Eclipse has been the too complicated deployment of SysML, which is supported as a UML derivate but not in the spotlight of the platform developers. Given our enhanced demands, it was not possible to create the whole template in Topcased or SysML Designer. Along with this, there is one more important factor related to eclipse and that is: it keeps updating its versions comparatively fast. This could be a major drawback because the support or the documentation is available only for the latest version of the tool.

Among the remaining tools: Papyrus and Modelio, Papyrus is more popular and there is a lot of documentation that is provided online for this tool. On the other hand, it is much more

complicated than Modelio. The interface of Modelio is straightforward and the learning curve is steeper. Overall, it is easier to use. The most important criteria remained to be able to access the model file, manipulate it, and view it back in the tool. When exporting the model, Modelio creates an XMI file which can be imported back into the model with all diagrams still intact. In Papyrus, there are many associated files that are created when a model diagram is drawn which makes it confusing to understand how the files are connected to one another and whether/how the associated files reflect changes. In the end, both formal and practical criteria indicated the use of Modelio.

In conclusion, the modeling language chosen in an exhaustive literature research is SysML supplemented with some UML specifications. The corresponding modeling tool chosen is Modelio.

6 Concepts for Model-Based Risk as a Path to Safer Medical Devices

The MBR construct was first presented in a concept paper by Schmitt and the author in 2016 [CAST16] and provides operators, participants and other stakeholders with an RM system that shall combine the strength of human risk assessment and the technical reliability of computational data processing. The proposed structured risk model would be apt for any product lifecycle (with minor administrative variations), but here it shall be described according to its implementation for medical product lifecycles as this is the focus of this dissertation. Nevertheless, it is this broad approach that makes the concept work independently of the type or classification of medical devices.

MBR will support the risk management process by formalization and give systematic guidelines to all the stakeholders during the whole product lifecycle. The system follows two fundamental design principles. First, it introduces iteration into RM for MedTech, which is more approximate to today's product design environments and – more importantly – allows for versioning which again facilitates the deployment of legacy product data. Second, MBR features a strict division between its computational core and the “human side” where the outer RM process takes place, including the RM methods and techniques used by the participants (panel) and the stakeholders.

A project funded by the EU named CORAS developed a model-based risk assessment (MBRA), which uses success-oriented models to define every planned system feature comprising functional, operational and organizational features of the objective. In addition, the CORAS framework consists of the following principle constituents: terminology, library, methodology and computerized tool. [GRAN04] Indeed, CORAS focusses in the documentation and communication of the results from RM methods such as HAZOP, FTA, FMECA, Markov and Event tree analysis (ETA) [GRAN04; STAM03]. This approach is then a mixture of a new methodology for the risk assessment step and a tool to improve the divulgation of the results of complementary designed methods. It is not an approach for a model-based risk system by itself, but very well might function as an RM method within such.

Bajaj et al. propose extended MBSE across system lifecycle (MBSE++), which they demonstrate in their own MBSE platform *Syndeia*, linking a powerful SysML model of the system's architecture with product models, libraries and customer repositories. A sophisticated authentication management allows to feed and push information from all linked models [BAJA16]. Albeit *Syndeia* can assist in MBR, its SysML core is designed to suit what they call a Total System Model that focuses on the junction of all software and hardware implementations. This approach does not fit the demands for analytical computation in complex RM models [CAST16]. Versioned models of different origin are kept in repositories which are interlinked on element level. This way, organizations may use the most suitable model for each tool whilst keeping the representations of the product elements interconnected. The entity of all models, the so-called TSM federation, evolves in a controllable and

collaborative fashion. Models of complex systems especially benefit from the advantages in traceability and impact assessment, among others. [BAJA17]

MBR as a concept provides a structured model, supporting and formalizing the risk management process during the whole product lifecycle. The RM system works for all medical devices, independent of their type or classification. As all RM documents are generated in real time, MBR shifts responsibility from stakeholders and panel members to a computational system, vastly reducing human error and red tape. This requires a software layer between DB, model and tools on one side and human decision processes on the other. Figure 6.1 shows the information flow in this iterative RM approach. As the process chain is continuous, a servicing point marks a virtual halt for the iterative RM process at a certain status quo. Between servicing points, all input is strictly separated from the actual changes in model and DB; all tools in the software layer must adhere to this policy. And while the potential for conflict and refusal to cooperate was acknowledged because of the perceived loss of control, the implementation of the concept relies on the estimate that the advantages of ubiquitous access, an environment-sensitive display (a universal API for the tools already in use at the stakeholder's workplace) and the bias-reducing uncoupling of content and contributor will by far outweigh the potential for conflict and refusal to cooperate because of the perceived loss of control. Experience from transformation in other engineering areas and also the INCOSE SE Visions support that estimate [INCO07; JULI12].

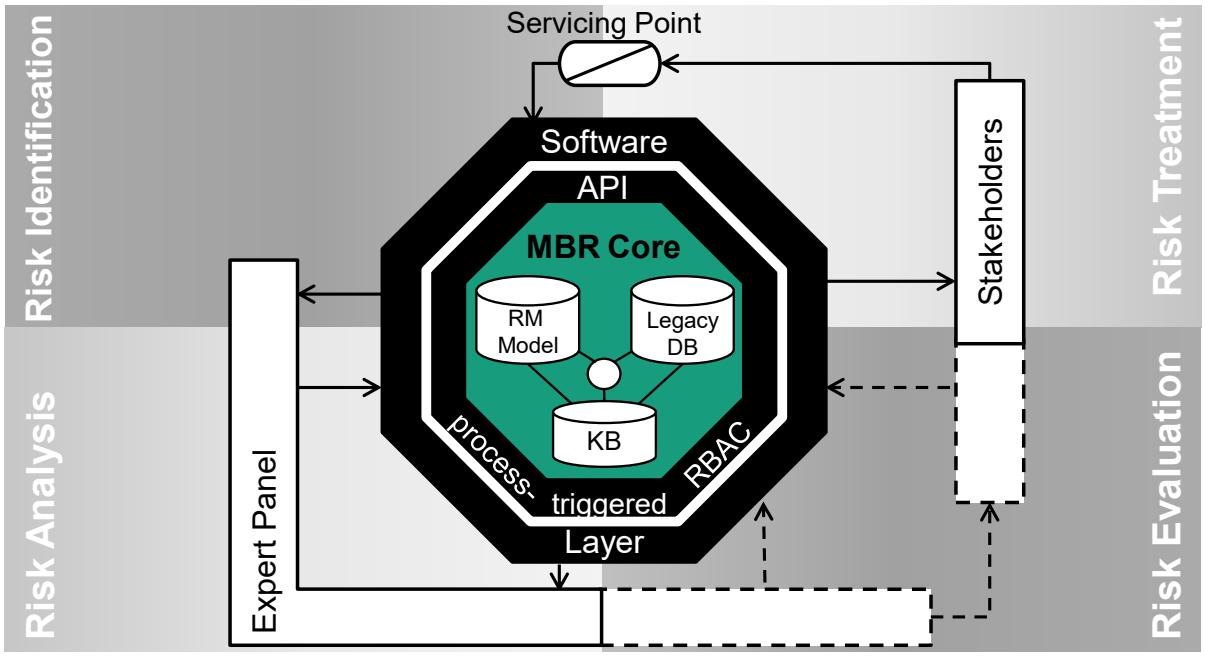


Figure 6.1: Flow of an iteration in the MBR system

RM alongside process chain necessarily involves treating RM stages as a sequence of events in an iterative process. At each start, all risk treatment from the last iteration must be concluded, so a newly redacted instance of the risk model is in place and the former version now becomes legacy. As SysML seems to be most adequate in specification and documentation but lacks certain formal capabilities and some functionalities needed for the

human-machine interfaces (HMIs), a new specification expanding SysML with parts from UML 2 was built. It also allows to connect the MBR tools to innovative function-effect modeling (iFEM), an in-house technique of IPT. These techniques currently do not hold an underlying modeling language, but were planned with a possible SysML implementation in mind [SCHM11].

With MBR, the deficits mentioned earlier (→ 3.3.3) of a document-based approach can be addressed or at least be dramatically improved. The areas of opportunity span through all stages of an RM process and are be tackled with software tools.

6.1 Comprehensive Risk Identification

This section describes how the MBR approach strives to accomplish comprehensive risk identification with the help of MBSE principles. Outer and inner formalization are essential to this.

The risk identification step must be clearly defined and well-limited. All stakeholders shall be aware of its beginning and ending and trust that the same input conveys the same output[21]. Likewise, all entries within the RM methods & techniques used in the step must be recorded in a form that the results are fit for computation.

If an organization is already using MBSE, it might only need some support to provide a finite model of the whole product lifecycle, the main requirement to start an MBR process. Others can transform their document-based information about the product lifecycle into a valid model through data inquiry.

As this development shall suit any kind of medical device, all points of view of all stakeholders and all guidelines they follow must be considered. At the same time, software engineering needs to exclude unnecessary data sets as early as possible. Metaphorically, no more and no less than every question necessary to complete the model must be asked.

6.1.1 Nomenclature and Syntax for Human-Machine Knowledge Transfer

The diverging approaches and terminologies used by the different technical disciplines may result in (partially) incompatible descriptions of the very same product. Regarding the known critical characteristics, these descriptions shall be reunited in a common terminology that reduces the inconsistencies of language comparable to be accessible for search engines. The presented concept defines the following five demands as necessary:

1. "A finite vocabulary of interactions. In this context, interactions are all actions occurring between one or more active components and any number of components influenced by

[21] The expertise the stakeholders provide and how they perform the tasks, counts as part of the input. Otherwise, it would be absurd to expect repeatability.

this action." [CAST16] To enable semantic search queries, the matrix is limited to verbs describing physical action and holds a distance value for any two items. The list may be extended with suitable items from literature as long as the new entries do not show too much congruency to any existing one.

2. "A set of adpositions clearing relation, location, direction, orientation etc. This set needs to describe each one-to-one correspondence between all physically and logically existing instances of components of the product lifecycle in a clear way that states how the instance pointed affects the reference (one component can have many logical instances, even pointing to each other)." [CAST16] Because adpositions build a closed class in linguistics, their amount in a human language can be estimated fairly confidently.
3. A finite list of possible element types within medical devices. The combined implementation of GMDN generic terms[1] and the UMLS metathesaurus provides element nomenclature, while the building rules of the generic model clear the placement. Together, they ensure the unambiguous identification of each model element. [CAST16]
4. "A hierarchic classification of MedTech products by function and application. GMDN's collective terms cover, among others, sorting by medical condition, application background or special features and by that allow us to classify assemblies in hierarchies from general to specific." [CAST16] While this is not directly mirrored in the structure or nomenclature of the model, it helps to cut off ramifications irrelevant to RM and clear element-wise dependencies where the cross-section information is not delivered when using only generic terms, e.g. application constraints that are meant to mitigate risk in a specific use case of a component.
5. "A classification of possible application and maintenance cases. Advocating RM alongside process chain, the whole product lifecycle needs to be classified, hierarchically organized and fed to the product breakdown structure." [CAST16] While design and production phases are usually well-documented through CAx which can be integrated into the model through the product breakdown structure (PBS), the use of GMDN's collective terms in the further packages of the model shall help to broaden the coverage to all lifecycle stages up to and including obsolescence and disposal which play a more important role in MedTech RM than in other sectors (think: tissue removal, nuclear waste). [CAST16]

6.1.2 Identification of Critical Characteristics

Data input to the MBR core may come from CAD/CAM, guidelines, field data, whitelists, RM documentation from legacy products, etc. The automated input can be complemented or substituted by manual entry through a wizard that offers a graphical interface to create and edit PBS and has scripts querying the user directly for additional information. In this processes, characteristics of the model elements can be flagged as critical and then end up as known critical characteristics in the legacy DB. In the risk identification tool, a highly customizable search engine will compare these with similar structures in the PBS and semantically similar characteristics of the current model. This way, known hazards can be connected to interactions in the current model, suggesting the triggering characteristics to be marked as critical as well. The results can be grouped on multiple levels, e.g. by risk assessment data, priority or

according to the potential sources of harm, and are then prepared for display, as seen in figure 6.2. Modeling interactions as new elements within the PBS allows for them to be processed in the same way as actual components. Technically, the identification tool delivers comprehensive results which only depend on data quality and not on the thoroughness of panelists and operator. The representation of the current model is augmented with the sampled information on known critical characteristics for discussion in the expert panel. Just as important, the display will alert the panel of all loose ends, where interactions are expected, but no positives were found in the current model. Up to here, the results are reproducible and comparable; data reliability can be traced in input/output tests. Operational cost can be reduced because all documents are generated in real time from the underlying model and substantial parts of the risk identification shift from man-hours to more cost-effective compute-time. Investing in the preprocessing of collected data will increase that effect. From a controlling perspective, compute-time is much easier to estimate than panel sessions, reducing delays and time pressure on the experts.

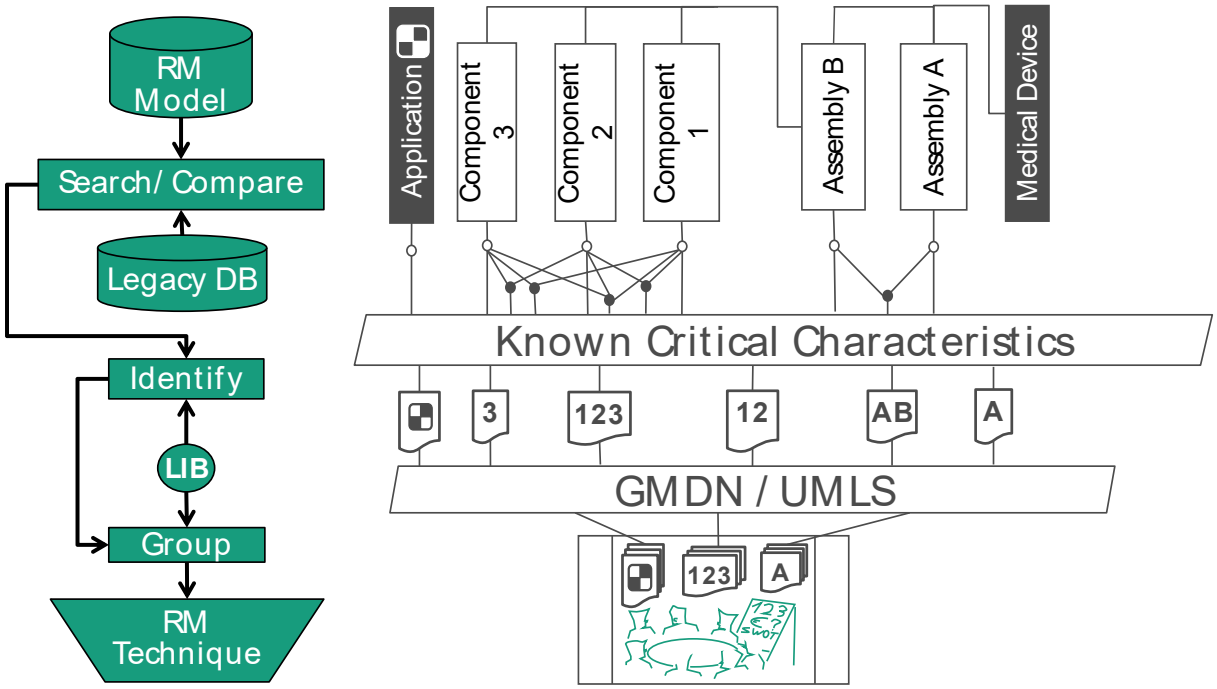


Figure 6.2: Scheme of the risk identification tool

6.2 Formalization of Individual Risk Management Steps

Here, the choice of the more general ISO 31000 over DIN EN ISO 14971 must be explained. Certainly, the latter would appear as the obvious pick as it actually specifies RM application to medical devices. This work by no means rejects its principles and emphasizes to follow the guidelines found in each step. However, formalizing risk identification as an individual process step, as ISO 31000 does, is crucial for the mitigation of the deficits in RM described earlier (→ 3.3f). The importance of contained, consecutive RM steps becomes evident if one takes the iterative nature of RM alongside process chain into account. The changes in risk between iterations or set alternatives must be kept measurable in order to interpret the overall course

of RM. Moreover, the level of coverage should be calculable while concluding risk identification and before entering analysis, when participants still have the chance to reduce residual risk. In the scheme of DIN EN ISO 14971, though, coverage is not fully predictable until entering risk control. Finally, the collaboration with practitioners researching and developing medical devices has shown that the structure proposed in ISO 31000 also yields advantages in transitioning RM results for processes from the ISO 9000 family.

In the proposed RM system, all events are constantly decoupled from the MBR core through a software layer. RM participants are never to change the model directly, but only through software tools; their entries can be traced back. As long as compliance with the API is provided, risk identification and analysis may be carried out by the panelists with any RM technique desired.

6.3 Vectorization of Risk Management Data

The XMI specification is the first to reach portability not only on model level, but on code level between different modeling environments. Albeit this is still limited to certain aspects, exchanging most properties of model components can be standardized in XMI by directly emulating the buildings rules which makes APIs easier to create and safer to run. Even though the API implementation of the software demonstrator (→ 8.1.3) serves for various (more immediate) data input formats, the use of XMI in any further prototype is strongly encouraged.

To avoid accruing inconsistencies over RM iterations[22], the transformation needs to be persistent linear. Any number of different, but congruent entries must automatically trigger the identical change to the model and vice versa. Thus, the demands from subsection 6.1.1 must resound in the API specifications.

6.3.1 Comparability of Panel Results

No matter which information gathering technique is applied, mode and motive of the experts' decisions will always be intrinsically tied to the resulting protocol. No approach for an RM system could change that without inflicting the autonomy of the decision-making which in itself then would be an adverse effect of bias. However, a model-based approach can (and hence MBR necessarily must by its own requirements) detach the decision’s implications from the decision-making’s documentation. The former are they are changes to the model itself, the latter are documented in the KB. The vectorized model is thus not influenced by the methods used and the free choice of information gathering techniques is ensured.

[22] One may compare the sequence of copy errors to Chinese whispers. Although the sequence would be an echo effect off the two representations, the error would stem from the API not channeling the changes correctly. Here, as above, keeping the emulation of data transition parallel to the model building rules as far as technically possible also helps.

Any changes to the actual product or its lifecycle – the “hard” facts from the RM process –will automatically be carried in any newly generated document. The meta data changes – the “soft” circumstances that portrait the evolution – are traceable, but separate; depending on the use case, the software layer could emphasize or withhold that information from the panel.

Moreover, the MBR core concept facilitates comparing the impact of potential treatments in sum or individually without losing track. The UML component and composite structure diagrams can help to visualize the differences. However, modeling interactions as own blocks offers a way in SysML, too.

6.3.2 Statistic Control

Comprehensiveness of the recognition of known critical characteristics can be achieved by simple multipass runs of the model calculating the coverage of the tree structure. For highly complex product lifecycles, statistical tools will then show level of coverage, coverage probabilities or numeric error. Even though the volume will grow steadily, the time consumption will stay predictable because all computational processes may be applied to the fragmented form of the models in the legacy DB where all correlations are linear. Also, a company may compare RM data of similar projects with the given tools, so RM stakeholders get an idea where to invest in RM activities for new projects. With each RM iteration finished, the organization will likely gain more statistical knowledge about its products in the next iteration.

6.3.3 Human Factor: Capturing Implicit Results

A stakeholder's disposition to contribute to an RM process may be negatively affected by bias-driven behavior, be it their own or others. MBR proposes to separate generation and evaluation of RM material in the panel from its reorganization and display. The urge for panelists to examine RM tasks for inhibiting consequences to their or others' roles as stakeholders may be reduced. For instance, engineers might more easily accept changes to their own designs or medics more openly discuss application errors mentioned by medical laymen. With a visualization focusing on the circumstances of the risk rather than the origin of its claim, a more objective view to complete data sets could lead to better risk assessment. Overall, unified visualization and access should decrease subjectivity and deliver clear and limited assignments. The same mechanisms within MBR that help balance human bias can be used to integrate the different professional mindsets of stakeholders into an interdisciplinary RM process. The high level of formalization proposed for the modeling syntax should assist participants in understanding what fellow panelists from other backgrounds want to communicate, while the possibility for raw descriptions assures each expert can express his thoughts as detailed as desired. Nevertheless, not all connotations can be saved in the procedure, as non-document-based RM still is text-based. For that reason, it is still important to choose the RM techniques wisely according to the mindsets and work history of the participants.

A strictly formalized modeling syntax should also help to integrate different professional mindsets into an interdisciplinary RM process. At the same time, any stakeholder may express

any additional content in a raw description for the KB as detailed as desired. Binary documents can be complemented with additional information. Nevertheless, it is still advisable to choose techniques according to the mindsets and work history of the participants.

„Eventually, MBR will not eliminate all circumstantial effects on the RM process, but its ability to separate automate workflow from task design can support and enable RM to achieve better results, where the special faculties of human minds are needed, may help to spare paperwork and factor out human distortion wherever a computer can do the better job. The MBR software layer should not be viewed as means to replace human experts, but rather a front desk assisting them and letting them focus on their expert work.“ [CAST16]

7 Theoretical Risk Management System

This chapter begins with a description of the requirements for and the features and benefits of the RM model. Then, a depiction of the components of the system will be given. Some overarching challenges interweave the problems described in the next section. They cannot be expressed in individual needs, but rather justify the employment of pragmatic models in engineering in general and MBSE in particular.

Model-based approaches in engineering should always be designed for relying on a single source of truth, that is every fact provided by the information in the model should be traceable to one data structure; all other data structures should link and be updated from this one. This premise stands and falls with the actual compatibility of used data structures and the acceptance of HMIs. Wherever one of these points of transfer fails to satisfy, human beings (developers as much as users) will choose a work-around (copy, skipping data maintenance and incorporation, making a note on a printout etc.). Any change will then create a new source of truth and updating from the original source will be futile.

Points of transfer constantly should be checked for their right to exist, that is only when one side has lost their operational superiority to the other, competence should shift and the workflow should be substituted by a corresponding one in the superior side. Translated to RM criteria, the underlying concept of this work strives to identify where humans perform worse in transferring RM-related information and tries to substitute this transfer with an algorithm. However, keeping humans out of transferring might invoke them to withhold implicit knowledge from the process which results in relevant information missing in the model. This concerns active retention as well as unconscious omissions.

Aspects of this general challenges that are not covered in the following section, are addressed in the description of the MBR core in section 7.2.

7.1 Requirements, Features and Benefits

Following, the procedural and functional requirements for the theoretical built of the risk model are listed. For clarity, all requirements are grouped with the indicated feature and resulting benefit. More detailed information about the features can be found in the technical specification in chapter 8.

It should be mentioned that the description of features and benefits partly reflect an ex-post point of view, as there naturally was no way to know if objectives would have been achieved after implementation and testing.

7.1.1 Procedural Requirements

PR1: Concurrency of Comprehensiveness and Complexity

Problem: Document-based RM systems lack the ability to master the concurrency of comprehensiveness and complexity (factors driving complexity in medical devices → 3.2). This is often a cause for delay in RM processes, errors in RM methods and consequently documents and – most importantly – non-identified risks (e.g. from complex interaction scenarios). Additionally, for many RM operators, RM method is synonymously with RM system, which leads to the wrong conclusion that the RM process would be concluded once the method had finished.

Need: Technically, the handling of this concurrency is already given by switching to model-based RM systems (→ 6). However, comprehensiveness on a technical level will not suffice for real-life RM systems, as it hinges on the question of practicability. Very complex products will impede comprehensive processing by overload (exponentially rising processing times, human motivational bias, organizational flaws etc.). Hence, an eligible RM system will have to include conceptual measures against such overload. Wherever a lossless transition is possible, processes whose time spans grow faster than the complexity factor need to be computerized.

Requirement: The most important requirement is, of course, implementing the RM system with a model-based approach. As redundant as this remark may sound, it is in fact imaginable to impose some of the following requirements without this premise. Albeit they still might work in favor of comprehensiveness, it is not the matter of this paper to discuss their individual benefits, but to show their sufficiency in this model-based system and its theoretical model.

The computing time of all processes must be calculable with linear effort. No computerized process shall overarch RM steps or stakeholder accesses. Conversely, stakeholders may not access the system in any follow-up sequence of computational processes[23].

The risk model must be limited to structural data only and any data that is needed for non-computerized processes only – for the sake of reducing computing time – may not be part of it; however, it must be retrievable for the stakeholders at any time they are granted access. All relational information must be transitioned into hierarchies in the model to avoid sunk information[24] and loops.

---

[23] If you think of a computational risk model as taking workload out of the stakeholders' hands, this then is the equivalent of an undisturbed workflow.

[24] Relational data may include information that provides truthful statements in its context but leads to contradiction in hierarchical contexts. E.g., two relational data sets may be pointing vice versa onto each other, which, transitioned into composite associations, is strictly not

Features: The MBR Core is designed with a clear division between KB and risk model, which resembles the rules in input data processing (structural/content data). All data sets from the KB are linked with the corresponding model elements. The generic model has been reduced to three different model elements: package[25], block and composite association[26]. Interactions are shown as model elements of their own right; they are children of the interacting physical model elements, e.g. from the PBS or users.

Benefit: The division in the MBR core keeps the risk model lean. The amount of content information will not influence the computing time of the risk model, which stays calculable at any time. All requests to the model come about with certainty of coverage, which is especially important for the risk identification tool.

PR2: Comprehensiveness in Risk Identification

Problem: As it is pointed out in subsection 3.3.3, document-based methods miss comprehensiveness in the risk identification process. This is fatal in MedTech as a failure to identify a risk can result in a risk not evaluated and not treated [CAST16]. Residual risk can emerge from that, this could arise in an RM iteration in the product lifecycle, reappearing as failure. Document/based RM does neither manage the complexity of the system nor the complex interactions. In MedTech accordingly, this frequently implies humans being harmed. [RADE04]

Need: As explained in section 6.1, a finite design of the risk model is gotten moving to model-based RM system. Besides, a legacy DB with known critical characteristics and a KB storing critical characteristics and risk management information are required in order to compare current model with the database through a search engine.

Requirement: In order to cope with the missing comprehensiveness of the document-based methods, it is necessary to recognize critical characteristics that are already known from legacy product lifecycles. In addition, the expert panel should get a visualization of the legacy critical characteristics with the estimated point of occurrence in current model.

Feature: The MBR Core is designed with a clear division between KB and risk model. The identification of critical characteristics will be done with a highly customizable search engine

---

logical as it would imply them reciprocally being parents and children, the hierarchical information from the structural data would be sunk.

[25] The number of packages is fix to the amount of lifecycle stages plus one (PBS).

[26] Composite associations in SysML/UML 2 have got hierarchical ends, as in a parent-child relation of their owners. Therefore, an interaction is not considered a loop regardless of the amount 1..n of its parents.

leading to known hazards, which can be clustered on multiple levels, e.g. by risk classes. The risk identification results are prepared for visualization.

Benefit: The risk identification results obtained by means of computerization are reproducible and comparable giving a certainty of coverage. The tool will deliver to the panelists the risk identification results and alert them of all lose ends.

PR3: Generality of Model Building Rules

Problem: More interconnected devices and shorter product lifecycles and development time targets result in more changes to the product in less time. Also, new products often cannot be compared directly to their predecessors because they are bound in a broader device context. All this might make for shallower RM and reduced product quality.

Need: Red tape associated with RM needs to be cut; human beings should be excluded from document generation as widely as possible. Current RM process must profit from legacy RM not only via expert knowledge, but also systemically.

Requirement: The RM model must be based on a generic model providing building rules that facilitate computer-based as well as intuitive comparison of current and legacy products. All documents must be generated real-time and with the form and timing intended by the RM process, using only structural information from the model. Content information must be available at any time in a standardized way of request.

Feature: The MBR Core is designed with a clear division between KB and risk model. RBAC and a standardized interface enable the operator to pair any compliant module that may request the documents needed for the chosen RM method or technique[27]. The fragmentation of legacy risk models in an own DB increases the traceability of modifications.

Benefit: The experts involved in the RM process can generate and view up-to-date documents in their individual professional environment. The workload preparing and communicating the panels is drastically reduced. Panelist will identify more risk and can assess risk in less time.

PR4: Indifference to Origin of RM-Relevant Information

Problem: RM results are impacted negatively by human factors like bias or motivational conflicts (→ 6.3.3). Differing professional mindsets of the panelists may impede the apprehension of certain decisions taken.

Need: The RM system must avoid bias by design and level acceptance of risk information independent of its origin.

---

[27] Then, stakeholders can plug in the document creation into their professional environments. At this point, it is not feasible to think theoretical solution and technical implications separately.

Requirement: RM participants' roles (e.g. operator, expert, and stakeholder) should be mirrored in the system. Rules should be made to allow access or deny access based on the process. All actual RM information must be available outside of the documents they originate from. Interfaces shall be standardized in a way that prevents discrimination of professional mindsets as possible.

Feature: A control layer separates the MBR Core from all user interfaces. RBAC rules on when and how users may interfere with the process or change the model. All RM information is pulled from the MBR core and may be displayed equally in the form the user's environment is supposed to rather than in a document stemming from another environment.

Benefit: The user[28] does not need to care in where the data is being displayed or is stored. While they need to add their own relevant information through the interfaces once, they profit from not having to incorporate all the data from the other professional environments (multiple workload). At the same time, the acceptance of RM material may be better when displaying it their own environment will obscure the origin (at least at a glance).

PR5: Compatibility

Problem: The multitude of accessible RM methods and techniques produces incompatible RM results (→ 3.3.3).

Need: The RM system must separate treatment from documentation as it means change to the model itself. Thus, the vectorized model is not impacted by the method utilized.

Requirement: There must be a gate keeper deciding which information goes into which part. A unique and unambiguous nomenclature for the model should be independent of the recordings of the different stakeholders which should be embedded in their original form of writing.

Feature: The MBR core consists of different types of information storage (model, legacy DB and KB) which work in different ways and whose elements linked to each other. In the DB, very specific descriptions and protocols can be kept in raw text and be linked with the regarding element's unique identifier, maintaining the model lightweight.

Benefits: As long as the RM operator accepts and fulfills their role for the RM system[29] virtually any RM method or technique that respects the steps in ISO 31000 may be used in the RM process. Stakeholders are able to trace model changes by comparison of legacy models,

---

[28] This is true for all users but the operator, of course.

[29] This is a substantial concern with any operator who needs to conform to another role. As a preliminary analysis of the survey on decision-makers shows, in MedTech manufacturers, RM operators often double as panelists, product safety officers or even C-level officer.

instance generation of documents, KB. Moreover, a comparison of the interchangeable elements concerning to their impact on risk is possible.

PR6: Continuity of RM through the Lifecycle Stages

Problem: Most document-based RM is designed to take place at one point in the development process. Often, the whole of observations may be premature and obsolete at the same time, but the workload of common RM systems does not allow for them being applied several times, or a second employment would even impede the observation quality.

Need: The RM system must be available alongside process chain; the RM process must be iterative where operators can choose servicing points freely in the continuous product lifecycle.

Requirement: The system design needs to enable the handling and storing of several legacy models in a manner that all their elements can be compared with the current model in one operation. There must be a facility to transfer a current model to this storage that can be used by the operator without having to take any additional procedural decisions.

Feature: The design of the MBR core permits versioning risk models not only for legacy products, but also for different versions of one product. At the same time, the iterative system design ensures the complete and consecutive execution of all RM steps. The separation of KB and legacy models makes it possible to link content information to model elements in various status. The fragmentation of the legacy models into blocks and relations makes computing requests economical and offers sensible options for logging and back up.

Benefit: “Hard” RM data and “soft” context[30] are presented as interlinked for the panelists, but strictly separated at the backend. This allows to choose RM techniques independently while keeping the changes in the model comparable. Forking risk models and implementing RM methods in parallel become conceivable.

PR7: Unambiguousness of the Nomenclature

Problem: RM documentation is often ambiguous due to humans using different vocabulary to put the same information into writing. This can mislead panelists interpreting the information as well as impede recognition of similarities.

Need: A unique and unambiguous nomenclature for the model must be composed. This nomenclature needs to be computable as well as informative to human beings.

---

[30] “Hard” data is the one which may be directly converted into RM results through arithmetic or logical processing. “Soft” data will impact the RM result only by being interpreted by the experts.

Requirement: The semantic settings shall be computable and logical to humans at the same time. A finite set of vocabulary for the interactions is required, adpositions shall be limited to directional prepositions.

Features/Benefits: A verb matrix limits the vocabulary for the interactions and provides fixed semantic distances between the items. The use of a unique identifier for each model element allows for informative, repetitive and variable element names. A classification of all structural elements via GMDN or UMLS facilitates computation of the similarity of elements or model fragments while linking more detailed information on the element for the user without actually keeping it in the model. The model element nomenclature follows ideas of object-oriented programming making it easy for humans to retrace relations in the code and the visualization parallelly. These features qualify the system to use semantic search technology on which the potential advantage of the risk identification tool over the current document-based techniques is based.

PR8: Separability of RM Steps

Problem: Many current RM methods and techniques do not formalize risk identification as a single step. The mixing of identifying and analytic properties hinders the comprehensiveness of risk identification and brings uncertainty of coverage to the whole RM process.

Need: Beginning and ending of the risk identification step must be clearly perceptible (methodically) and technically separated and secured (procedurally). Inputs and output of the computational part risk identification need to be comparable; its results must be repeatable (pass a black box test). Changes in risk between iterations or set alternatives shall be measurable.

Requirement: A software tool shall check the model for known critical characteristics and proceed a preliminary risk identification run before the panelist get in touch with the current model. The suggested risks, their localization and related human-readable knowledge shall be visualized prior to opening the step in the panel. The panel shall be forced to revisit the risk identification run before transitioning to risk analysis.

Feature: The API with its RBAC divides the MBR core from the software layer and third-party applications, hence, separates the computational tasks from the panel work and guides the stakeholders reliably through the individual steps. Inputs are requested and outputs displayed at predetermined points in the process, while surrounding information is always available augmenting the visualized model. Any changes can be traced back, altered and reversed. The risk identification tool recognizes semantic and structural patterns comparing current to legacy models and highlights kind and location of a probable occurrence of known critical characteristics. These functions are tunable to refine and prioritize search results.

Benefit: Risk identification is made more comprehensive in two ways: First, highlighting and augmenting potential risk by a source that is accepted as neutral increases the chances for better procedural instructions, RM segmented clearly, certainty of coverage, risk identification and analysis may be carried out by the panelists with any RM technique desired.

PR9: Comparability of Treatments

Problem: Various negative incentives lead to a disinterest in evaluating the impact of competing risk treatment options (→ 3.4.2).

Need: Decision-makers must be informed on comparisons of all treatment scenarios and their impact.

Requirement: The RM system shall be designed to allow version forking to compare different treatments with a control. It must be possible to sustain several future scenarios of the current model within one installation of the system.

Feature: When finishing one RM iteration, the current model is fragmented and stored in the legacy DB. This act may be reversed and repeated many times without erasing the afore-transferred versions, thus creating as many “legacy” scenarios of a current model as desired.[31]

Benefit: Comparing different forks might help in complex products to specify the impact related to a certain treatment.[32] Making information about treatment alternatives accessible would then depend on computing time rather than project man-hours and back office load, thus allowing better estimates on ROI, diminishing investments.

7.1.2 Functional Requirements

FR1: Integration of Structural Information from Existing Product Models

Problem: Manufacturers use a multitude of product models in the process chain. RM-relevant information does not enter the RM process because not all data of the product models is incorporated.

Need: The RM system must integrate all relevant information into one single source of truth before starting the RM process.

Requirement: The data input tools shall vectorize the PBS by automatically selecting structural data from given product models. There shall be a facility to correct and complement via HMI.

Feature: The software layer allows to create a model baseline loading PBS data through the standardized API into Extended Markup Language (XML) code. In the model wizard, the

---

[31] A sensible implementation of this feature would call for additional software that was not devised for this work. Subsequently, this feature cannot be found in the specifications of chapter 8. Nevertheless, a similar feature was implemented for testing purposes by keeping multiple (unfragmented) current models in a DB.

[32] This a solely logical claim and an interesting field for future work as the author could not find any actual research on this.

structure can be controlled and changed. The RM operator can save in XML to use it as a current model or store the structure in the legacy DB. The user may also edit structures in a graphic modeling environment and load it back to the model wizard, e.g. for merging PBS from two product models.

Benefit: The RM operator does not have to take decisions which structural information may be gained from which product model. The workload and error rate for data input is reduced, therefore, the chances that all structural information from all product model is used will improve.

FR2: Compliance of Product Model Data

Problem: Data in RM processes is often not exchanged in a formalized way. Information is lost due to transitioning errors or user distress. Data loses informational value because the exchange is only partially executed.

Need: Industrial standards whose implementations are widely available for the common product models in manufacturing must be used to exchange data.

Requirement: Data entry to the model should be OSLC-compliant. The RM operator shall be able to add all data that is non-compliant, but can be put into computable attributes, through a software tool.

Feature: All automated data exchange runs through the OSLC-compliant API. The RM operator may enter any non-compliant, but computable data in the model wizard.

Benefit: Most common product models can exchange information in ways that allow to create OSLC-compliant input with relatively low effort. The reduced workload enables organizations to include more relevant information in the RM process in less time. Motivational barriers for RM operators (overtaxing tasks, bias against certain product models) may be reduced if they are aware of a downstream option to correct and complement the automated input.

FR3: Autonomy of Interaction Elements

Problem: Many product models in manufacturing build the product lifecycle around the PBS. However, many times the hazards cannot be traced back to characteristics of a single component or similar element but lie within an interaction of two or more elements. Following only PBS, it is immensely difficult to attach the precise critical characteristic to the interaction.

Need: Within the RM system, interactions must be managed as an element of their own right without losing their existential dependency of the interacting elements.

Requirement: Interactions shall be modeled as new elements within the product breakdown structure instead of relational elements. It shall be possible to equip them with classifiable attributes. They must be distinguishable as their own element class by syntax. Their nomenclature shall convey the nature of the interaction for human beings.

Feature: Interactions are established as an own block class with all attributes required. Their nomenclature follows the human concept of interaction (1..n elements act upon each other with an effect on at least one of them). The parent-child style integrates seamlessly in the PBS.

Benefit: Critical characteristics can be located precisely in the model. Safe states for critical characteristics can be substantiated directly in the risk model. The improvement on risk identification can diminish residual risk.

7.2 MBR Core

The technical RM system consist of the MBR Core and the software layer as shown in figure 7.1.

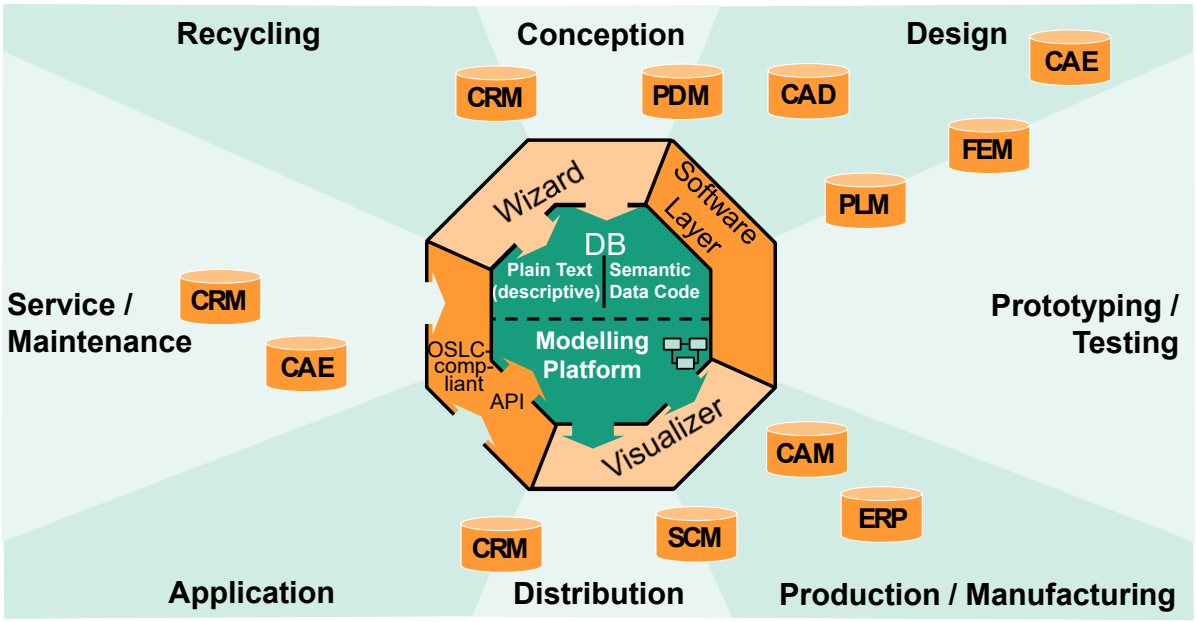


Figure 7.1: Model data input (MBR with software assistance)

As previously explained, the MBR Core has an explicit separation from KB and risk model. Following, an explanation of the elements comprising the MBR Core will be given.

7.2.1 Risk Model as a Hierarchical Product Model

The MBR approach is founded on Stachowiak's GMT. This means that the more the models resemble each other respecting the key criteria of GMT, the more attuned are they relating to the interchanging structure-related information. [CAST17]

Product Breakdown Structure in the Nomenclature

The generic model of the device encompasses three different model elements: package, block and composite association.

The number of packages is fix, they build the top level of any hierarchical tree and bear no further attributes beyond name, class and associations. Their relations are handled the same as those of blocks.

The relation between the blocks is always described as a parent-child relation of their owners. They may get any attribute assigned that is of a structural nature to the RM process. Any information on them that is considered non-structural (knowledge), is stored in the KB and linked to their unique identifier. Examples for typical block classes are device, assembly, component, subcomponent, user or interaction.

Interactions as New Elements

Interactions are shown as model elements of their own right; they are children of the interacting physical model elements, e.g. from the PBS or users.

The first challenge while adding interactions was that unlike the other tags, interactions can be between two elements at any level of the hierarchy. While this is unproblematic on the graphical level (in SysML), this proved to be an issue in UML syntax. The first approach to define the parents in a likewise-named tag in the initialization of the interaction block showed that it works well within the MBR core and theoretically fulfills all XML specifications, but that it is hindering the processing of XMI model files, which are needed as one kind of OSLC-compliant output, most importantly for the major graphic modeling platforms. This was solved by adding the interaction twice in the XML, united by the unique identifier, but distinguishable by a ‘status’ tag that can carry ‘agent’ or ‘patient’. The computation in the MBR core will only rely on those tags with agent status, while graphic modeling platforms may also use the one with patient status to draw associations.[33]

Secondly, interactions may have more than one parent element, usually two or more. SysML does, however, not allow associations to be connected to more than two other elements (here: the interaction and one parent). This led to the decision to expand the model’s language specifications to UML 2 which does allow for this kind of constructs. To avoid issues with adapting to the much wider definitions in UML 2, a mixed SysML/UML 2 specification was adopted.

Nomenclature of Product Specification

Numerous examples of nomenclature for medical devices have been developed without having a common structure, approach and applying to dissimilar goals. A universal platform to identify medical devices and interchange unharmed related data cannot be achieved by different nomenclature systems. [GMDN10]

[33] The existence of independent MBR, XML and XMI identifiers proved very convenient in the actual implementation of this.

The product breakdown structure used to model the medical device has only four levels: device, assembly, component and subcomponent. The components were given generic descriptor tags using either the GMDN or the Unified Medical Language System (UMLS) standard. These DBs are extremely vast and manually looking up the terms is cumbersome. On the other hand, it cannot be fully automated as some elements in the model can have multiple suitable GMDN or UMLS descriptors and the most suitable one can only be selected by the user. There is also the possibility that certain elements do not have any suitable descriptors in either DB.[34]

GMDN

The hierarchical classification of the medical device by function and application was done using the GMDN. For this purpose, the GMDN term code (non-repeating unique values), term name and term definition corresponding were used as shown in figure 7.2. The termID (unique identifiers (IDs) for individual objects) is connected to the collective term IDs.

As of June 2017, the GMDN nomenclature has got over 25,000 entries in the main sheet (term sheet). Each element in the list is a unique category of medical with a unique term code, name, definition etc. The terms are also grouped and classified in a hierarchical tree structure based on their properties. Such terms used to group the individual device terms are called collective terms which are listed on a separate sheet complete with an ID, name, definition and status whether active or obsolete; examples are given in figure 7.3. Two separate sheets show the grouping of individual term IDs into collective term groups as well as the linkage of collective terms to form a hierarchical tree.

[34] This, later on, did not turn out as a quality issue, as there has not been a single case in the user tests where a specific medical component could not be classified. Assigning user-generated terms was only necessary for those elements that portray very general fields of application, e.g. screws or seals. Most of the time, they are found at a subcomponent level.

termCode	termIsIVD	termName	termDefinition	termStatus	modifiedDate	createdDate	obsoletedDate
10943	IVD	Sputum specimen container IVD	A sterile covered plastic receptacle (	Active	9/15/2012	5/17/2004	
12542	IVD	Midstream urine specimen cont	A covered plastic receptacle with no	Active	9/12/2012	5/17/2004	
15015	IVD	Oxygen breath analyser	A mains electricity (AC-powered) lab	Active	10/9/2012	5/17/2004	
15110	IVD	Microscope slide maker IVD	An automated mains electricity (AC-	Active	9/11/2012	5/17/2004	
15126	IVD	Colony counter IVD, manual	A device designed to provide a lighte	Active	7/25/2013	5/17/2004	
15132	IVD	Cell morphology analyser IVD, m	A mains electricity (AC-powered) ma	Active	12/15/2015	5/17/2004	
15155	IVD	Inoculating loop IVD	A hand-held device intended to be u	Active	9/3/2012	5/17/2004	
15163	IVD	Nephelometry/turbidimetry ana	A mains electricity (AC-powered) ma	Active	10/17/2016	5/17/2004	
15164	IVD	pH meter IVD	A manual, semi-automated, or auto	Active	10/12/2012	5/17/2004	
15599	IVD	Microscope slide stainer IVD	An automated mains electricity (AC-	Active	9/11/2012	5/17/2004	
16291	IVD	Sweat specimen container IVD	A non-sterile, covered plastic recept	Active	1/2/2013	5/17/2004	
16384	IVD	Blood tube mixer IVD	A mains electricity (AC-powered) lab	Active	9/16/2012	6/12/2007	
16865	IVD	Radioimmunoassay analyser IVI	A mains electricity (AC-powered) lab	Active	9/14/2012	5/17/2004	
16877	IVD	High performance liquid chroma	A device consisting of a barrel (cylin	Active	9/17/2012	5/17/2004	
17474	IVD	Infrared spectrometry breath an	A mains electricity (AC-powered) ins	Active	5/17/2017	5/17/2004	
17476	IVD	Hydrogen breath analyser IVD, p	A portable battery-powered instrum	Active	5/17/2017	5/17/2004	
17477	IVD	Methane breath analyser IVD	A mains electricity (AC-powered) lab	Active	1/17/2013	5/17/2004	
17489	IVD	Microplate washer IVD, automa	A mains electricity (AC-powered) lab	Active	9/9/2012	10/26/2006	
17742	IVD	Haematological cell analyser IVI	A mains electricity (AC-powered) lab	Active	9/17/2012	5/17/2004	
30194	IVD	Ammonia IVD, kit, ion-selective	A collection of reagents and other a	Active	3/5/2010	5/17/2004	
30197	IVD	Lithium electrode	An electrochemical sensor that pref	Active	10/19/2012	5/17/2004	
30202	IVD	Carbon dioxide electrode	An electrochemical sensor that pref	Active	3/4/2013	5/17/2004	
30203	IVD	Laboratory pH electrode	A clinical chemistry, electrolyte, elec	Active	10/19/2012	5/17/2004	

Figure 7.2: Examples of individual terms from the GMDN database

collectivetermID	code	name	definition	ctStatus
1	1	Clinical Specialties	Collective terms that describe various clinical specialties.	Active
2	2	Device Attribute Assortment	Collective terms that describe many different device characteristics.	Active
3	3	By Name	Collective terms for device names above the level of the preferred term.	Active
4	4	By Use	Collective terms for device names above the level of the preferred term arranged by clinical panel o	Active
5	5	Device Materials	Collective terms that describe various materials from which devices are manufactured.	Active
6	6	Device Power/Operation	Collective terms that describe various types of energy or methods used to power and operate devic	Active
7	7	Device Sterility	Collective terms that describe various device sterility characteristics.	Active
8	8	Device Use Frequency	Collective terms that describe various types of frequencies of device use.	Active
9	9	Device Invasiveness	Collective terms that describe various types and degrees of device invasion into the body.	Active
10	10	Obsolete Collective Terms	Collective terms that have been permanently taken out of use.	Active
101	101	Hearing	Devices intended to aid, restore, or test a patient's hearing, and other associated devices.	Active
102	102	Beds and associated devices	Structures typically comprised of a mattress and support platform designed to sustain a patient's re	Active
103	103	Personal mobility assistive products	Devices designed to provide a person with a disability the ability to move, or be moved, from one pc	Active
104	104	Diagnostic radiological systems and associ	Device assemblies designed to use very high-frequency electromagnetic energy (i.e., ionizing radiatic	Active
105	105	Magnetic resonance imaging (MRI) system	Device assemblies that use strong magnetic fields and computer-controlled pulsed radio-frequency	Active
106	106	Nuclear medicine systems and associated c	Device assemblies designed to locate, record, quantify, and analyse radioactive emissions from the l	Active
107	107	Diagnostic ultrasound/ultrasound imaging s	Device assemblies designed to generate ultrasound pulses, direct them to a body target area, detect	Active
108	108	Radiation protection/limiting devices	Devices/materials designed to protect persons or objects from unnecessary or excessive radiation e	Active
109	109	Therapeutic radiological systems and assoc	Device assemblies designed to use very high-frequency electromagnetic energy (i.e., ionizing radiatic	Active
110	110	Obsolete CT (Implantable electrical stimulators/stimulation systems)		Active
111	111	General-purpose infusion/syringe pumps	Devices designed to exert a positive pressure greater than that produced by gravity to maintain cont	Active
112	112	Application program software	Software programs, routines or algorithms that add specific computer assisted display, processing a	Active
113	113	Manual dental	Non-powered dental instruments and equipment operated by the healthcare professional.	Active
114	114	Powered dental	Powered (e.g., electrically, pneumatically) dental instruments and systems operated by the healthca	Active

Figure 7.3: Examples of collective terms from the GMDN database

UMLS

For the components and subcomponents of the medical devices, the following terminology has been used as classifier: UMLS ID, Concepts and Concept Unique Identifiers (CUI); UMLS term name and source DB name are returned as classes.

UMLS contains over 2 million names for around 900000 concepts from over 60 medical vocabulary families. Moreover, it also contains 12 million pairs of inter-concept relational data [BODE04]. UMLS services can be accessed on UMLS Terminology Services (UTS), the one used here is called the Metathesaurus. Each element in the UMLS DB has a unique CUI which can also be used for searching in the Metathesaurus tool.

Creating the Verb Matrix

Like GMDN/UMLS descriptors that may connect differently named yet actually similar components, the semantic spacing of verbs is difficult to capture. For a human being, it is comparatively easy to grasp the congruences in the concepts of verbs. In how far an action is described accordingly by two verbs (synonymy), is understood on a very intuitive level. A computer needs more tangible properties to rate this. To solve this issue, an extensive similarity matrix is created for all common verbs.

There is a very large number of verbs in the English dictionary and theoretically, all of them can be used to describe how a component interacts with another. The most elaborate work for this matter so far has been done by Levin [LEVI93] who assumes that a verb's morphological behavior is mostly determined by its meaning regarding expression and interpretation. It uses this idea to delimit and systematize verb behavior in order to create several categories of verbs depending on use cases to generate a classified verb tree. Closeness in this tree and multiple occurrences make two verbs more similar than others. An extensive verb matrix was created extracting the complete verb list in the appropriate tree structure. Before proceeding, the list was limited to those verbs whose meaning may produce physical impact (e.g. *(to) punch*, unlike *(to) love*). Since the categories have a tree structure, the lowest category level (the level closest to the individual verbs) was chosen. Now once the basic matrix V is set, a full matrix is generated with 1 as the value where the verb belongs to a particular category and 0 where it does not. As the aim is to understand how many verbs belong in multiple groups together, a matrix Verbmatrix was created:

Verbmatrix = V*V'

It is, hence, a matrix of verbs vs verbs. It has values from 0 to 4 indicating that at best, there are combinations of verbs occurring in 4 groups simultaneously. The whole path is illustrated in annex B.

There are 3200 verbs in the list. Of the 10236800 possible combinations between two different verbs, there are:

- 249342 instances of two verbs belonging to one group together
- 3428 instances of two verbs belonging in two groups together
- 258 instances of two verbs belonging in three groups together
- 8 instances of two groups belonging in four groups together

There are no cases of any combination of verbs being in more than four groups together.

Now a distance matrix was generated with each element of the matrix being 1/[corresponding element]. This is used to find the semantic similarity between verbs. The shorter the distance, the more similar the verbs.

Nomenclature of Critical Characteristics

Attributes of model elements that require a quantitative value (number, Boolean, etc.) are embraced by the tag ‘characteristic’, complete with a name as a short description of the type of the characteristics and a unit in which that characteristic is measured. To differentiate which characteristics are critical, a tag ‘cc’ within was implemented.

7.2.2 Legacy Model Database

To define the records of this DB, an exemplary legacy model was conceived with a focus on preparing and processing the data to a format that allows easy search with the defined parameters. The creation of a well-defined legacy model is complicated by the fact that the data will not necessarily come from transitioned RM models but may originate from all kind of sources and the nature of the data may vary considerably. Hence, it was decided that any legacy model would have to comply with all building rules for the current model, in order to then fragment it with the same procedures.

All records of the DB are derived from the building rules for packages and blocks in the RM model. Associations are translated in relations between the records, pointing to the unique identifier as record ID. Any attributes are stored in the columns, including the links to the items in the KB.

7.2.3 Knowledge Base

The KB stores critical characteristics and RM information in order to compare the current model with the legacy DB. All data sets from the KB are linked with the corresponding model elements’ unique identifier (UID). Each record consists at least of an ID, name, description and the URI where the content may be found.

7.3 Software Layer

In this section, only those modules shall be described that are strictly necessary derivatives for the RM system to function in theory. The software layer tools in the deployed demonstrator are more numerous (cp. ch. 8,9).

7.3.1 Data Input Module

As mentioned above, Stachowiak’s pragmatic modeling approach [STAC73] was considered as the best option to conceive RM models of complex product lifecycles. His reduction principle sacrifices a model’s refinement in projection wherever it would depreciate its fitness for purpose unreasonably. In terms of RM data selection then, attributes are rendered unnecessary wherever their computational deadweight is not outperformed by their informational value to the RM process. All generic RM models will have to adhere to this policy by implementing respective selection criteria.

The principle data selection strategy of the MBR Core follows the division principle of the RM model. In complex product lifecycles, all "unnecessary weight" added to the model will increase computing time in multiples, slowing down all queries; tuning searches for semantic similarity with legacy model fragments will be complicated by bloating results with false positives that show similarity, but have no effect on critical characteristics.

Data that helps to locate, describe and (mathematically) evaluate critical characteristics, hazards and risk is integrated in the RM model, while all remaining information may be brought into the descriptive KB at the discretion of the user, provided it can be linked to a model block element. The former criterion can be subdivided in four categories defining the data on a modeling level (→ fig. 7.4):

- Structural Data
  - hierarchical data shaping the physical product and product lifecycle, e.g. product breakdown structure, topology, application scenarios
  - relational data shaping the interactions in product and lifecycle, e.g. use cases, process parameters, supply chain meta-data
- Content Data
  - attributes influencing the critical parameters, e.g. dimensions, material properties, quality criteria
  - medical classifications, e.g. GMDN codes and terms, UMLS terms

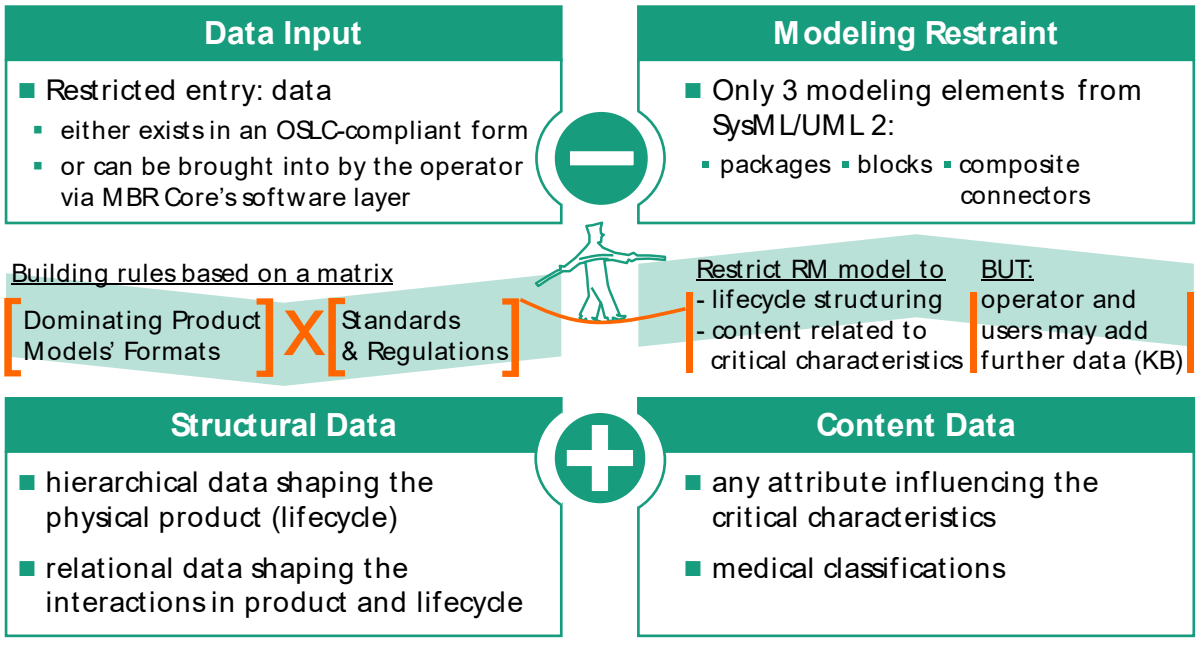


Figure 7.4: Data selection criteria

A matrix crossing the dominating product models and current data interchange standards with inclusion criteria and data types and formats is the base to develop building rules (→ fig. VIII.7). Besides the informational criteria, there are also technical restrictions that act as exclusion criteria which – while sometimes acting as a barrier for actually desired data – are intentional to keep the model lean and tidy. There is restricted entry to the model to data that either exists

in an OSLC-compliant form or can be brought into by the operator via the model wizard. Here, OSLC secures comprehensiveness by making sure that all selected information from compliant product models is echoed in the RM model. The self-restriction to only three modeling elements from SysML/UML 2 – packages, blocks and composite connectors – simplifies the model fragmentation. Technically, it operates as an exclusion criterion, too, as no data can enter the model that cannot be expressed as an attribute of said elements (→fig. 7.5). Virtually, the implications will be minor; it is expected that the affected portions of product model data will be minimal.

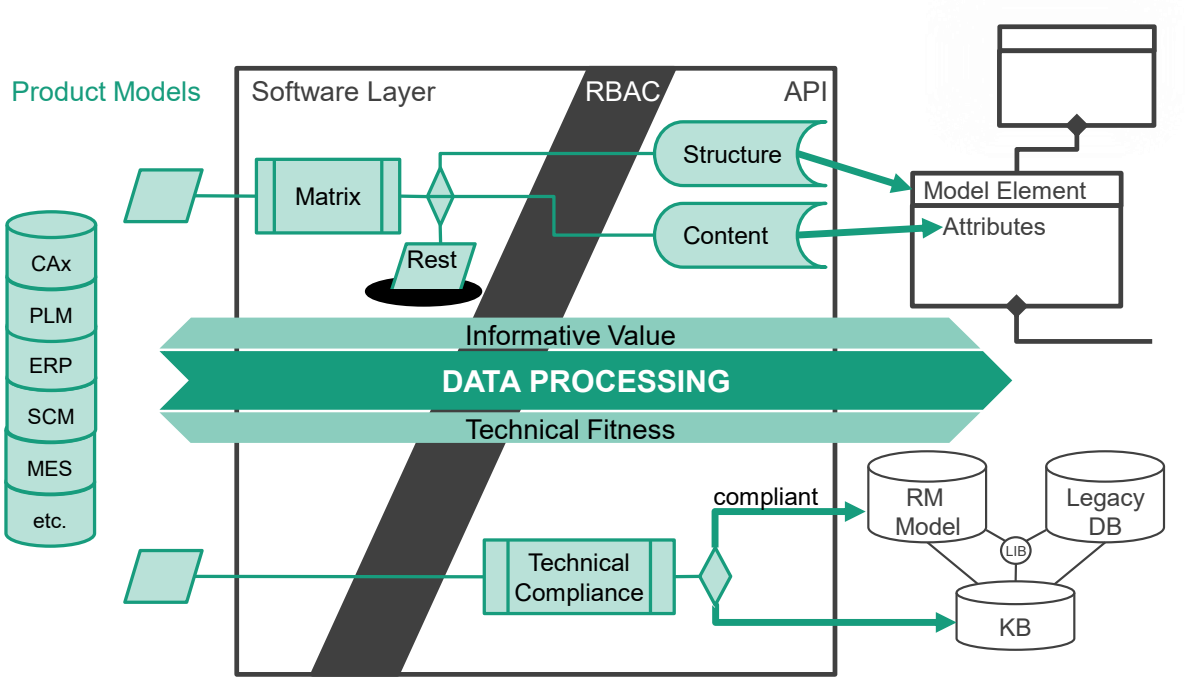


Figure 7.5: Data selection flow

As already stated in chapter 3, a literature review was done to research the available structured product models in the product lifecycle, their penetration in MedTech and the value they carry for the risk management process. To comprehend which kind of information is coming from which model, which output (format), location of that information in the model in which way, a matrix was created underpinned by the literature review done. The data coming from the product models were grouped in the following categories: geometry and design, production planning, process control, data integration, logistics, service, data type, extracted data format, modeling languages (→ VIII.E). Then, each category was clustered into structural, content and none according the extracting types of information from the product models. An example can be found in appendix E, figure VIII.7, too. Finally, the suitability for SysML/UML 2 and the compliance with OSLC must be determined for all structural and content information.

Search Engine and Risk Identification Tool

For the purpose of describing the theoretical system, the search engine and the risk identification tool can be seen as a functional unit. In the demonstrator, they form two individual pieces of software.

Since all files are saved locally or on a local server for this particular use, this search engine resembles a desktop search engine from an input point of view. As size and structure of the data resources are well known, computational costs and response time were not as important benchmarks in the development as usual for search engines. Regarding output, the tunable semantic search and the ranking of the results are the most important perspectives. The design of the search routine and queries was focused on delivering comprehensive identification of similarities. The process needs to be highly customizable, both in the combination and sequence of queries (tuning) and the weighing of the hits (ranking). Adjusting these parameters is the crucial step to obtain a comprehensive identification of the critical characteristics.

To make it comparable, a copy of the current model is fragmented in the same way as the legacy models.[35] The search engine runs comparisons between each fragment of the current model and a chosen subset of the legacy base. Which combination of subsets in which order is chosen for the search routine, can have a strong influence on the results. Subsets that have proven promising are e.g.

- all model elements which carry a characteristic that is linked as critical in an interaction,
- accumulation of similarities in agent and patient names and verb of interactions or
- GMDN/UMLS terms for parent elements of interactions.

There is no such thing as a perfect search routine for all medical devices. If anything, it should be configured and tuned based on the quality and detail the current model provides at that point in time.

After the search has ended, the results are compiled (e.g. multiple occurrences of one element summed up) and ranked based on their cumulative scores. The risk-prone interactions are then tabulated based on the assessments of their probable legacy predecessors (if values are available) and the (original) current model is augmented with the RM-relevant knowledge linked to the former.

Model Wizard

In the theoretical system, the model wizard comprises all means for the users to manipulate the MBR core beyond the formalized ways in the RM process. The operator may user all frontend functions at any time, while all other users have restricted access. As the functions are bundled in one frontend, the user is informed which changes their role is permitted to make rather than just being confronted with a blocked function. The functions accessible in the frontend include initiating and elaborating model builds, incorporating data into and editing in the MBR core, saving backups and images of models in various formats, inserting and editing RM forms, among others.

---

[35] In the implementation for the case study, it is also possible to compare two models in the XML form (coded SysML/UML 2).

7.4 Application Programming Interface

The only necessary deliberation for the theoretical side of the API concern its role as the gatekeeper restricting the data stream to compliant intake. OSLC defines eight domains that may be chosen. They declare rights and obligations directed both at the API provider and the clients.

Domain Specification for the Application Programming Interface

With respect to the technical restrictions, a comparison of the 8 domain specifications was made. While the core specifications are mandatory for compliance in any scenario, software providers may choose which domain(s) they would like to adhere to in order to create a software that is functional and at the same time as open as possible to desired pairs.

In the basic requirements, statements are listed whose fulfillment can be required as ‘may’, ‘must’ or ‘should’. These statements are always of the same kind and verbalism but can be made in different depth (e.g. if the statement is fulfilled in one domain with a ‘must’ clause, but in another one requires ‘must’/’must’ or ‘must’/’may’ due to a subclause detailing the main statement). In the six cases where the basic requirements at max differ in a subclause of the statement, they are from here on called ‘similar’, the remaining ‘dissimilar’. The latter are again divided into those whose fulfillment is desirable for the RM functionality and the rest, as outlined in table 7.1.

Considering the data displayed in table 7.1, four of the domains were shortlisted: *Requirement Management*, *Change Management*, *Quality Management* and *Asset Management*. Further in-depth analysis marked the domains Requirement Management and Quality Management as most favorable.[36]

[36] This is a purely technical evaluation of domain requirements vs. fitness for purpose, even though the choice sounds obvious in the end.

Table 7.1: Alignment of OSLC domain specifications with MBR system requirements

Domain Specification	Requirements		
	Similar	Dissimilar, Desirable	Dissimilar, Not Required
Requirement Management	6	10	3
Change Management	5	11	3
Quality Management	5	11	3
Architecture Management	4	5	13
Asset Management	6	11	3
Performance Monitoring	4	10	3
Automation	5	10	3
Reconciliation	5	10	3
Σ	6	11	14

8 Generic Risk Management Model and Implementation

In chapter 7, the requirements needed for a theoretical model-based RM system were outlined. The theoretical model featured there will be the base for the following technical requirements. The specification explained here in section one conforms with software demonstrator used in the trials and case study. It was conceived catering the needs of scientific analysis and stand-alone qualities and is not considered superior in terms of application. Some technical requirements were not specified at all, as their implementation would have conflicted with research goals. However, the software demonstrator has been designed in a way that the missing bits could have been included and put to work without major changes to it.

In section two, the model building and algorithm structure will be described.

8.1 Technical Requirements and Specification

This section deducts technical requirements from the design and listed features in chapter 7 and describes the specification of the software demonstrator to fulfill the former. As the tested software is tailored to the case study, differences to an ideal build for application are noted as well.

8.1.1 MBR Core

Risk Management Model

Requirements. The risk model is laid out in SysML/UML 2. The lifecycle stages are represented by SysML packages, all hierarchical elements beneath by SysML blocks. Relations are built in composite associations where interactions may have more than one connector on each end. [37] Characteristics that may have structural information – most importantly when they may become critical in a certain interaction – need to be included in a way that system and users expect the right corresponding units and values. All aspects need to be implemented in text while respecting all aspects of the graphic modeling language.

Specification/Implementation. The backend language used is XML 1.0 (encoded in UTF-8). All modeling is realized using customized XML tags that will not be overwritten by the targeted integrated development environment (IDE), here: Modelio 3.5. Critical characteristics bring the expected value type as attribute in parentheses and are allocated to the interactions with pointers called ‘ccLocators’ that have a parent-child syntax known from object-oriented

[37] This is not SysML-compliant but allowed in UML 2. In SysML, interactions and their allocation are designed in a more sequential way which fits narratives based on messaging or signaling, but not so much on interactions of physical components.

languages. Details are explained in section 8.2, as they would else have to be repeated here in too many paragraphs.

Legacy Database

Requirements. Legacy product models, be they products different from or former versions of the current product, shall be fragmented into their model elements so they can be stored in one DB. Also, already fragmented legacy models may be uploaded directly to the DB. The connection to the content data in the KB must be maintained. The structure must be upheld insofar as it suffices to rebuild the model from the fragments. The DB needs to be versionable an updatable to allow exchanging it without breaking MBR core functionality.

Specification/Implementation. This versioned mySQL DB comprises of at least four tables as depicted in table 8.1. The main information on current and legacy models is kept in two separated tables. In theory, there would be no need for a fragmentation of the current model as it used for all RM procedures in its XML form, but for practical reasons, an option to fragment them was implemented so different current test versions could be kept in the software layer at once. This may also prove helpful when managing forked RM models to compare treatment and control of certain risks. Another add-on for practicability is the backup table locating XMI files already generated by the API which mostly contains those directed at visualization in Modelio. In end use, every user application would generate the files in real time from the API which would discard them afterwards. For the usability tests and the case study however, it would have been excess workload to write, test and approve a Modelio plugin just for a software demonstrator. The largest table then contains all model elements from all fragmented models. It is not necessary to directly link it to the models' tables because the structure to build each model is given from the DOM information and the model elements are individually traceable by the UID. Beside the self-referential and RM information, there is also an item listing all related IDs from the KB.

Table 8.1: Chart of the legacy database

Table	Description	Most Important Items
Legacy Models	Legacy RM models and information about their origin, access and associations.	File name, file type, description and user
Current Models	Fragmented instances of current RM models and information about the associated model elements.**	File name, file type, description and user
XMI files	Backup of XMI files generated by API calls.**	File name, Modelio file name
Model Elements	Model elements of all types and classes from all fragmented models	UID, element type, element name, parent, <GMDN>, <UML>, <characteristics>, <RM results>, <KB>, pointers for critical characteristics (ccLocator)

Knowledge Base

Requirements. All RM-relevant content data shall be stored here. Operators and stakeholders can add documents and link them from the software layer or through the API, they may do so based on RBAC. Operators can also upload records with documents in bloc, e.g. stemming from links with added legacy models or technical libraries. The internal DB handling must not corrupt any structural information connected to the current models or the legacy DB. The DB needs to be versionable an updatable to allow exchanging it without breaking MBR core functionality. Storage locations for the actual documents must be editable per record.

Specification/Implementation. This versioned mySQL DB comprises of a table including content data, information valuable for the RM participants in non-computable attributes. The most important items are ID, name, classification, description, URI. Every record is interlinked with the related model element. The information in the KB can be edited or deleted through hypertext preprocessor (PHP) tools at any given point of time by the RM operator; stakeholders have limited rights in the software layer (RBAC). To avoid that changes in the KB would corrupt model structure, the storage location is isolated from the KB ID of the document[38]. As there is no significant difference in the tools, the software demonstrators do not have gotten any implementation in the API.

[38] While this is very helpful in test case scenarios, there should be some kind of fallback option later on. Direct interlinking would most probably bring along versioning issues if e.g. two models use the same document whose record is then being changed. Checking the integrity via encrypted hash functions might be more feasible – or a combination of both.

Software Services

Software that is not part of the three core constituents but is mediately needed for the MBR core to function, will be described here. To some extent, it may be also necessary for the software layer, in which case it will not be explained again later on. To keep the demonstrator utilizable in stand-alone mode, all queries for third-party DBs were realized off version-controlled libraries that were regularly generated from the actual DBs. This applies as well for the verb matrix utilized in the interactions' nomenclature.

GMDN Library

Requirements. GMDN terms shall be available in a versioned DB that allows the user to classify model elements in the model wizard frontend. The terms shall be integrated directly in the model elements attributes in a way that is qualified for semantic search technology.

Specification/Implementation. The library is implemented as a versioned SQL DB which contains three tables (generic terms, collective terms, relations) in CSV format which are based on the respective GMDN tables and cropped to purpose, see table 8.2.

GMDN nomenclature is typically defined and tabulated in SQL or spreadsheet. Each element in the list is a unique category of medical devices and does not have any company specific names. The device is marked as either IVD or non-IVD. Each entry as a unique term code, name, definition, status (active or obsolete), and date when it was added to the DB, and if relevant, date when it was last modified or made obsolete. The terms are also grouped and classified in a hierarchical tree structure based on their properties. Such terms used to group the individual device terms are called collective terms which are listed on a separate sheet complete with an ID, name, definition and status whether active or obsolete. Two separate sheets show the grouping of individual term IDs into collective term groups as well as the linkage of collective terms to form a hierarchical tree.

The frontend conducts Python-driven queries that allow the user to first narrow down the options, then choose a certain GMDN term. The term is parsed into the model element as class by ID and – for human comprehension – as a name tag.

Table 8.2: Chart of the GMDN library

Tables	Selected Items
Collectiveterm	Collective term ID, name and definition
Term	Generic term code, name and definition of each record
Termcollectiveterm	Relation between the generic term code and collective term ID

UMLS Library

Requirements. ULMS terms shall be retrievable from a versioned DB for the user to classify model elements in the model wizard frontend. The terms shall be integrated analogously to the GMDN terms.

Specification/Implementation. A Python-based API connects to the UMLS online DB searching in the Metathesaurus DB to retrieve all corresponding results. This table contains CUI, UMLS term name and source DB name, see figure 8.1.

The user is guided through the selection procedure in the frontend. When a certain UMLS term is chosen, it is parsed into the model element's attributes as class (CUI) and as tag name.

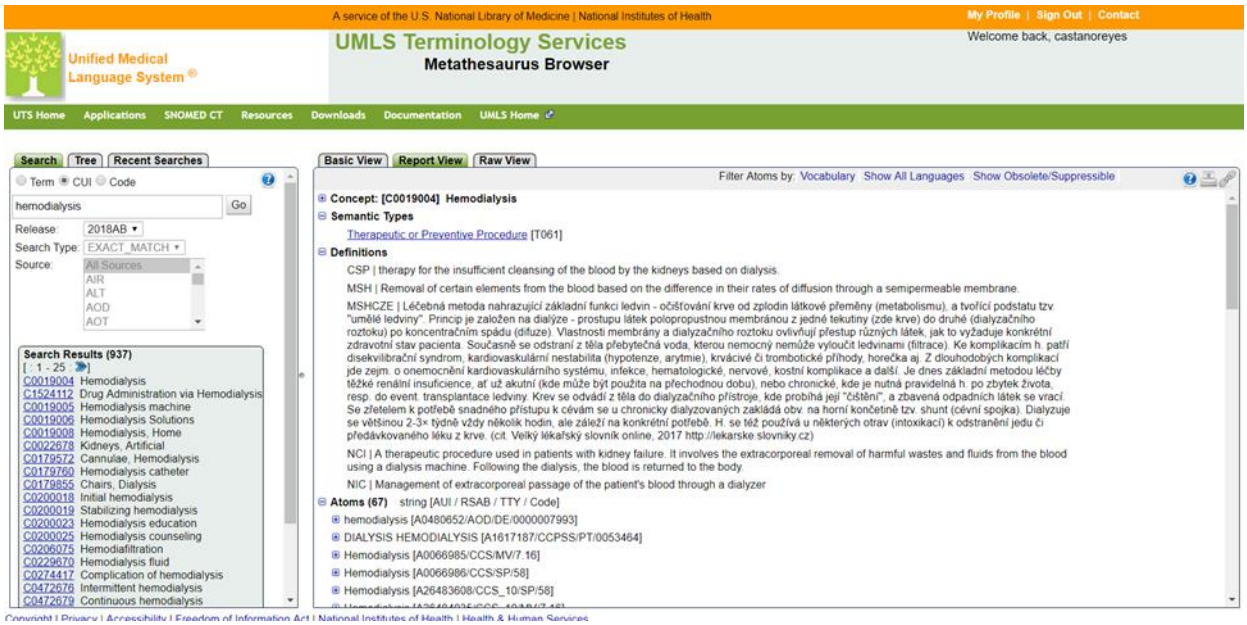


Figure 8.1: UMLS metathesaurus tool showing the results for the sample search query 'hemodialysis'

Of the source DBs in UMLS, the most important for most of our use cases has been the Systemized Nomenclature of Medicines Clinical Terms (SNOMED CT) DB. It has over 300,000 concepts in areas such as diseases, findings, procedures, devices and physical objects [WHIT13]. If a search tool needs to be limited to one DB, SNOMED CT is the clear favorite. In order to classify the components of the medical devices, the UMLS was implemented using the following terminology: UMLS ID, Concepts and CUIs; UMLS term name and source DB name are returned, see figure 8.2.

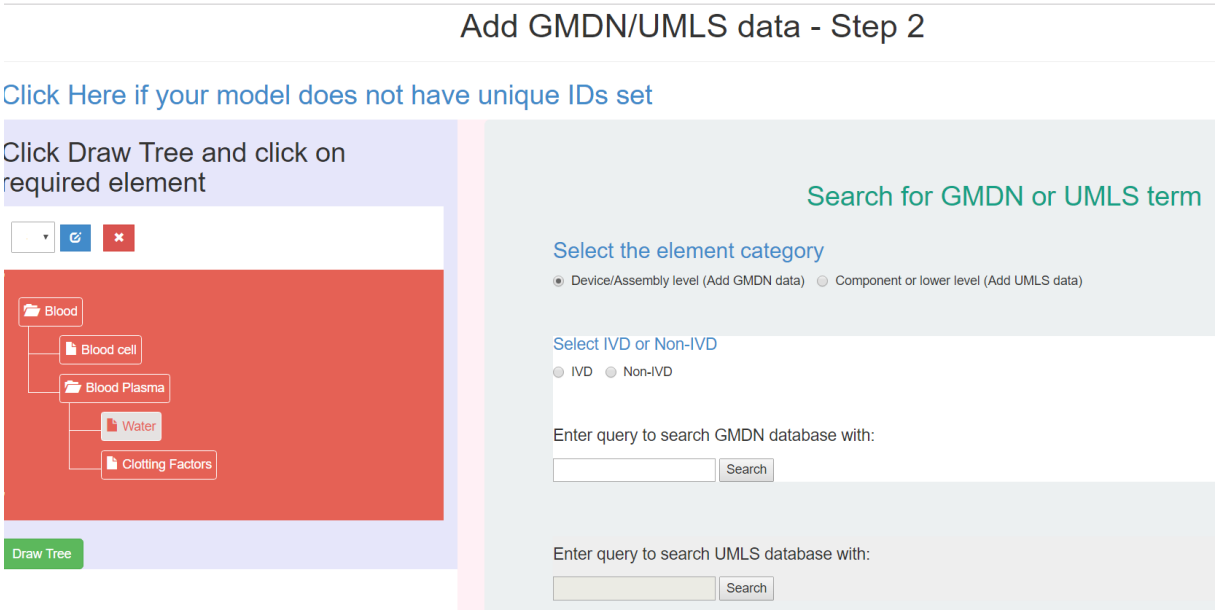


Figure 8.2: Searching for medical classification to add to the model elements

Unique Identifier Assignment

Requirements. To link the selfsame model element through between the core constituents, a unique identifier must be introduced that is robust against code changes and time shifts outside of the API. A set of building rules must be implemented in such way that unique identifiers emerge whose structure is sufficiently dissimilar from any ID commonly used in XML, graphical modeling platforms or product models while being intelligible and – as a matter of principle – resolvable for humans to keep documents usable in case of system failure.

Specification/Implementation. The UID is a 19-to-21-character string consisting of an alphanumeric section of 4 characters for the product name, separated by a hyphen-minus (U+002D) from a 4-char decimal version number and, after another separator, concluded with the elements' serial of two letters indicating the class and seven to nine numeric digits. None of the sections is case-sensitive. Whenever possible, the serials in the case study were chosen to reflect the hierarchies in the models and help orientation for humans. Interactions are the most prominent example where this is not feasible, since they can appear anywhere with parents differing in both dimensions. All hierarchies can be identified from the XML/XMI using DOM elements, though. Snippet 8.1 is an example of a UID from the case study:

```
<uid>bonn-0003-pa1000000</uid><package>StemCellPlatform</package>
```

Snippet 8.1: Implementation of the UID in XML for the package-class element 'StemCellPlatform'

Verb Matrix

Requirements. In order to name interactions in a manner that humans as well as computers could interpret, process and reproduce, the vocabulary must be limited and usable without a complicated grammar. To identify where and when different stakeholders use differing wording to describe an identical interaction, all records of the verb list need to be related to each other

based on their semantic similarity. An index value needs to be assigned to vectorize semantic distances in a way a search engine can accept to tune the queries for critical characteristics.

Specification/Implementation. A verb list is generated modifying the syntax trees from [LEVI93] selecting all verbs where one of the meanings carries a possible physical impact on the object (e.g. as in ‘to hammer’, not as in ‘to love’). The verbs remain in the given syntax groups. Their semantic distance is weighted based on the number of times they appear together in any syntax group. A matrix is generated as described in figure VII.10 and saved as CSV. A determined version may be read through PHP in the modeling procedure of the model wizard or directly through the API.

8.1.2 Software Layer

The WebApp runs on Apache server and utilize phpMyAdmin (software tool to handle MySQL DB). XAMPP 3.2.1 is used to run the local Apache server in the machine. The coding is done using Netbeans IDE version 8.0.2.

User Frontend and Modeling Wizard

The model wizard tool, the front-end application, is composed of Javascript and Ajax for running client -side scripts and sending and receiving the data from the backend. The front-end programming languages are HTML5, Javascript, JQuery 3.0.0, Bootstrap 3.1.1 employed to display the data or information on the screen of the user. The template engine for PHP is TWIG 1.32.0. A detailed explanation of the tools can be found in appendix D.

Semantic Search Engine

Requirements. The search engine needs to be highly customizable in order to fit in with a wide range of models with different qualities and levels of detail. The operator shall have the option to combine and balance the available queries to adapt the search routine. Semantic similarity should predicate a cumulative score for the list of results.

Specification 1 (general): The current model is copied and fragmented (see below) to level the initial representation with the legacy DB. A self-developed PHP tool coordinates the search routine and sends SQL queries to run the search. The hits and parameters are stored preliminary in MySQL, ranked with the operator’s desired scoring and saved in HTML.

Specification 2 (testing): Here, only data from two specific models is compared. The user determines a current and a legacy model at their own discretion by loading the respective XML files from the XML backup DB. A PHP tool checks all the model elements individually against their corresponding counterparts, moving along the tree structure in the XML files using DOM elements. The specification of the risk management model and the legacy DB were previously given. This search routine specifically focusses on interactions that need to be checked for critical characteristic. The results are then treated as above. This second specification is not meant as a productive part of the demonstrator but was used for testing the search routines

with real operating data and to produce the search results from the previously manipulated models from the case study[39].

Risk Identification Tool

Requirements. The ranked search results shall be individually placed in the local interactions and block elements carrying the critical characteristics. Loose ends, that is interactions or ccLocators where no correspondent has been found, shall be highlighted as such. All edited elements need to be marked in order to provide certainty of coverage.

Specification. The PHP tool receives the search results in HTML. This facilitates a table structure while still keeping the tagged elements in original syntax without masking them, which simplifies the further processing in the two directions: to the current model (XML) and to the source files augmenting the visualization (HTML). With the UID, any available RM values are pulled from legacy, RM content (like hazard or FM descriptions) are compiled into single HTML files with a UID-based URI pattern, and links to the respective KBID are included. At the interaction location of any hit, the 'cc'-Tag is set to true and all inherited locations of critical characteristics (via '[UID].[ccLocator]) are flagged[40]. For the user test, a mapped web page with the block elements as div-layers was distilled from the XMI in Modelio and then linked with the HTML files generated.

Modeling Fragmenting

Requirements. Every legacy RM data and so, too, each RM model that is transitioned from current to legacy at the end of an iteration, shall be fragmented from a hierarchical (like the SysML/UML 2 model) to a relational form to be incorporated in the legacy DB. All association (e.g. parent-child) and connections (e.g. KB links) must be retained as shown in figure 8.3.

Specification. In the case of legacy material coming from outside in XMI, the data is transformed into a clean XML representation of the SysML/UML 2 equivalent. The XMI is stored in the backup DB section for reference. A PHP tool parses all structural information from XML to the SQL DB line by line; all association are turned into attributes pointing to the UID of associated element and indicating parent/child status. All content tags (including naming, classification and links) are traced back to the propertied UID and written in the respective attribute column.

---

[39] This was done to integrate treatment and control data in one search result, because the task design would not allow to test them separately (as there naturally was only one panel for each stage).

[40] This was done using a designated XML flag in Modelio whose actual purpose is unrelated to the project's SysML use case. Thus, it was assured Modelio would not eradicate the flag importing the XMI, as it does with unknown flags in some XML tags.

8.1.3 Application Programming Interface

The API was built using PHP Version 5.6.3 as the server-side scripting language. The client-side scripting language is Javascript, asynchronous client-server exchange is handled in AJAX. Created content is displayed to the user in HTML5 assisted with Bootstrap 3.1, a framework made up of HTML, Javascript and CSS sheets written in Less (→ fig. 8.4). The local server machine is run on XAMPP, version 3.2.2. The tool employed to develop the application was Netbeans IDE, version 8.1.

Data Preprocessing

As this software demonstrator consist of in-house prototypes, there is no official documentation of the test-stage API and, hence, no possibility for the participants to deliver compliant data. Generally, assessing data quality within a preprocessing owned by the members of the research team, will avoid dragging along errors that would deflect focus from errors in the original content in an unknown way. In a future application case, this would be a client-side job and most probably solved by offering plugins for major product model software rendering compliant XMI.

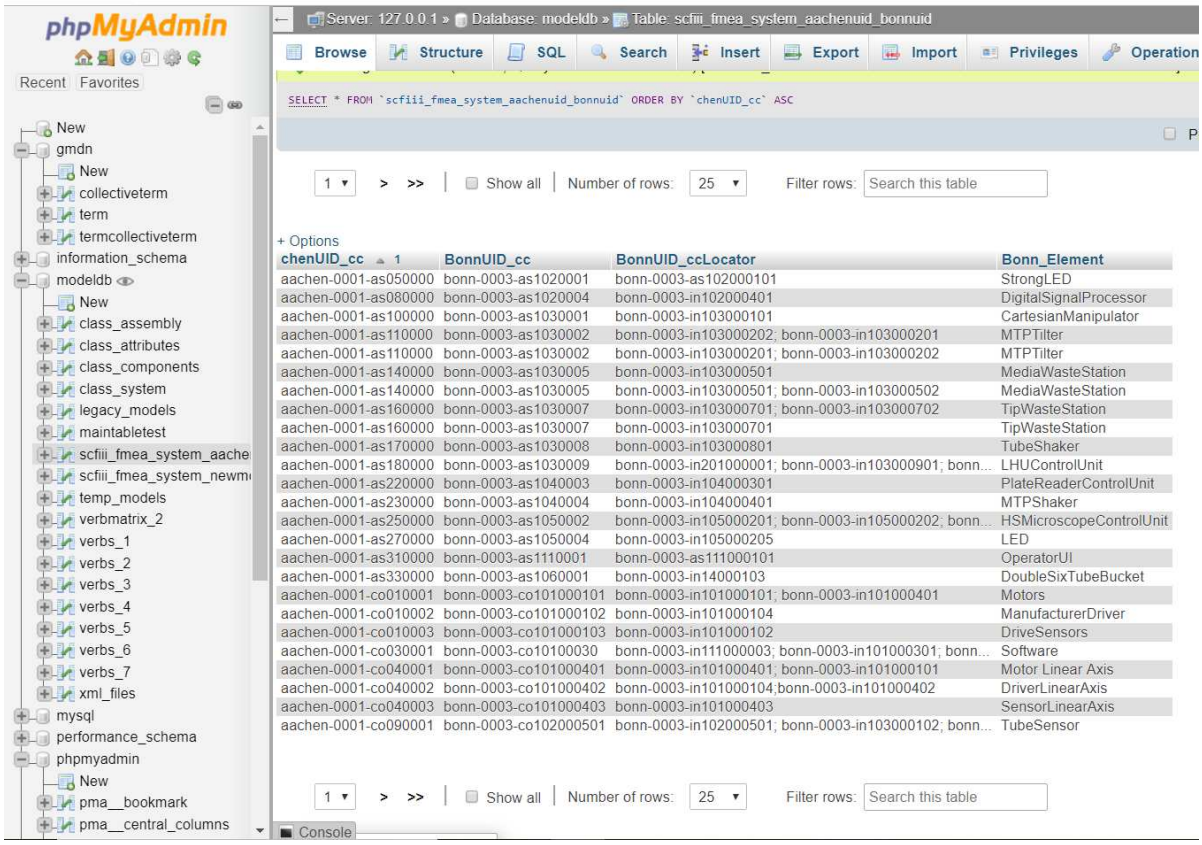


Figure 8.3: Database extract from a query comparing critical characteristics of two models in the case study, screenshot from phpMyAdmin

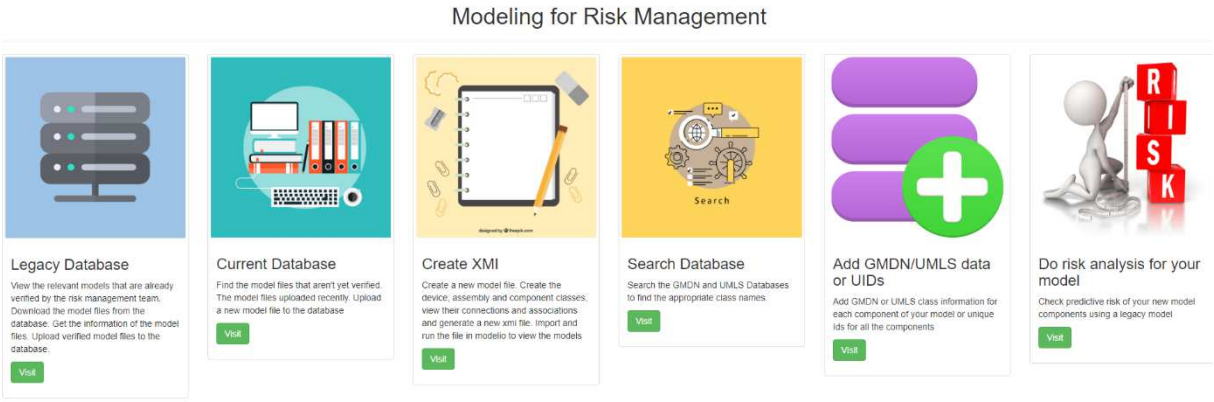


Figure 8.4: Homepage of the software layer's frontend showing some applications

Requirements. Structural data shall be recognized in and extracted from STEP-file format and Modelio's SysML and UML tools. It shall be possible to render XML code in two outputs: a raw product model (XML) that fulfills all requirements to serve as the skeleton for completion in the model wizard as well as a more refined OSLC-compliant XMI to be swapped between software environments without losing any risk-relevant information. Placeholders for all tags necessary for the model fragmentation must be included wherever the tags are not available at the time of conversion.

Specification/Implementation. To extract the structural information, a script for the FreeCAD Python console runs through the PBS and assigns SysML blocks in classes from top to bottom (device --> assembly --> component --> subcomponent[41]). This tree structure was then converted to the XML format used for model creation in the model wizard, so the rest of the RM-relevant data from the STEP file could be transferred and tagged using the existing tools in PHP. To stay flexible for all kinds of legacy STEP files, all non-hierarchical information was extracted manually by running corresponding queries in the open-source console of FreeCAD.[42]

To reach interoperability and OSLC compliance, the XMI file must contain all structural data in both hierarchical and relational description. This is done by connecting the XML ID tags to our ID system based on SysML composite connectors and UIDs. As long as the right SysML or UML 2 elements are used, the API is now able to convert new model elements directly from

[41] The tree structure below this level had to be ignored to reduce data volume. The value for the RM process was considered neglectable. Most elements at this level are standard production parts like screws, washers or cables.

[42] It would have been possible to extract this information in a similar manner, but always only for code generated completely in a single CAx environment. STEP files are thought as container formats to allow editing in multiple applications that may not destroy code meant for the tools they do not feature.

Modelio and to mask changes made in the software layer so that Modelio will accept the resulting model and render it correctly without losing any of the customized XML tags carrying the RM-relevant data, see code comparison in figure 8.5.

Figure 8.5: Comparing model and model interchange; left: „clean“ PBS tree as per MBR specification (XML), right: same tree with all necessary add-ons for OSLC-compliant interchange (XMI)

Data Selecting

Requirements. The API shall select RM-relevant data from the input and divide it into two streams: structural data flows to the RM model directly, content data flows to the KB where it is linked to the respective element(s) in the RM model. Decisions are based on a matrix ruling on the usefulness for RM. The description of this matrix can be found in 7.3.

Specification/Implementation. In the software demonstrator, the selection process is implemented in a very limited fashion. As the executors control all inputs before the test scenarios anyway, there was no need to consider all possible kinds of product models and their data. Hence, all rules were hardcoded into the API, so they could be tested within the API tests[43]. After summoning and preparing all technical files for the test cases from the involved institutions (→ 9.2.2), the necessary changes were applied to the API code accordingly and again tested.

[43] Application case software should source the rules from a database based on the data selection matrix. Only then, the rules could be upgraded and versioned. In the test case however, this would have made programming and testing considerably more complicated and thus error-prone.

8.2 Model Building

Extracting PBS to a Graphical Model through XML

As the basis for the construction of the PBS in the case study was mainly found in CAD/CAE files, the extraction of the structural information was exercised for STEP files, the underlying format for most of the common modern CAx software. The theoretical idea for the extraction would be fundamentally the same for other formats, but the practical implementation up to the generation of the RDF may be very different. Once an RDF/XMI representation that is compliant with the API is reached, the internal procedure leading to the MBR core, however, is identical.

The components of the STEP file are extracted into an XML format which can be viewed in a web browser. The intermediate steps can be found in the long description in annex B. But in order to observe them in a clear tree fashion, they needed to be converted to a block diagram. This allows to visualize the parent-child relationships in the model as well as how they could potentially interact at various levels. To achieve this, the XML file needed to be manually coded in to an XMI file format and visualized using Modelio software. Figure 8.6 compares the tree view in a typical CAD environment with the block diagram after conversion.

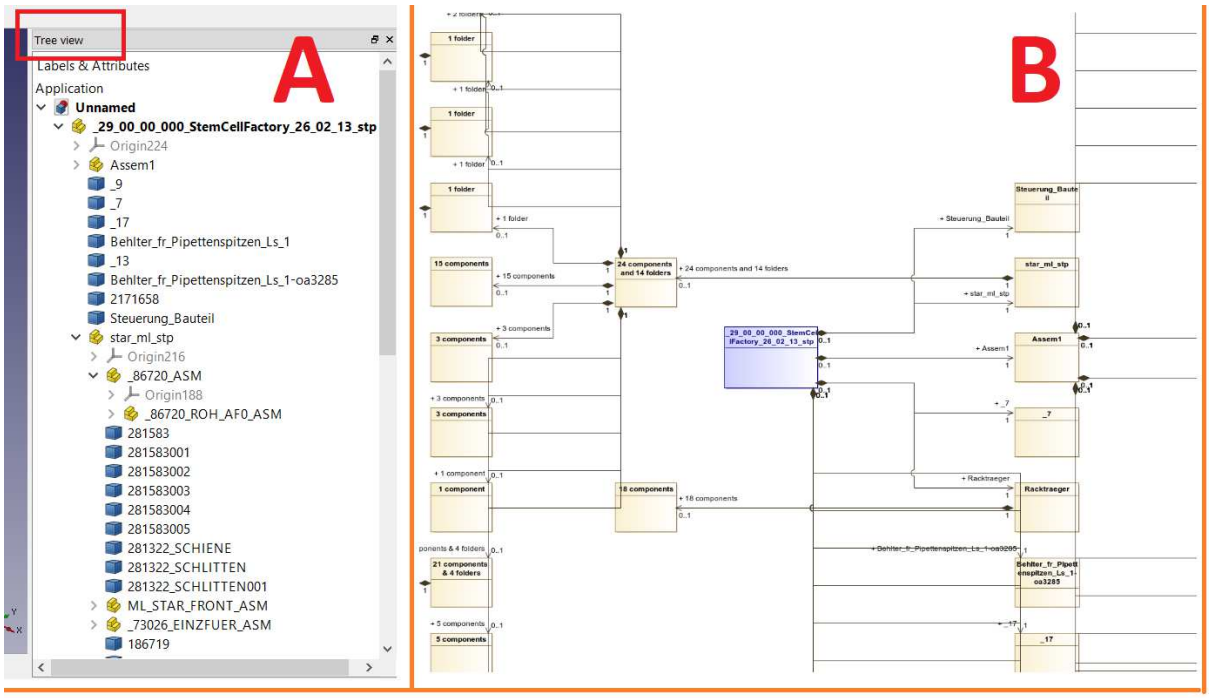


Figure 8.6: (A) Tree view in FreeCAD; (B) Section of the same tree visualized as a block diagram in Modelio

Generating a Current Model from the Generic Model

Instances of the generic model are implemented by a central composer tool in the backend written in PHP. This composer controls the generation and editing of all files in the model building at any time to ensure that there is exactly one interpretation of the source material.

Among those files, the XML and XMI model files are the most important and most commonly used ones and therefore covered as examples here. Then, the implementation is illustrated following a similar description as the theoretical RM model.

While both templates are written in the same language, they fulfill different purposes that are in parts so contrary that a single representation of the model would not suffice. Nevertheless, the generic model behind them is the same.

The XML template is the base for the actual risk model for all computational tasks in the RM process. It is structured in a strictly hierarchical manner and its outline resembles the SysML block diagrams. To keep it lean, all data that is not absolutely necessary for its functionality is outsourced to the corresponding DBs in the MBR core. The tree structure is coded as unsorted lists, where the highest level declares packages standing for the product lifecycle like PBS, application or maintenance. From here on, all lower levels are declared as blocks of different classes, e.g. a user would be a block of the class ‘device’ in the package ‘application’. All other attributes can be found in tags within the list items. Model elements are identified based on the UID except for the composite associations whose existence is implied in the structure.

The XMI template uses a mix of hierarchical and relational structure and is needed to produce the model in UML-compliant modeling platforms and alike. Hence, the syntax was in large part no free choice, but was determined by the desired compatibility with IDE, platforms and tools. It is much more complicated and extensive, but a good starting point for OSLC-compliant interchange. All instances of classes are enclosed as ‘packagedElements’, while all attributes can be found within ‘ownedAttribute’ tags. The depiction of the structure, however, is not linear as in the XML template, but follows no general rule. This makes it easier in terms of compatibility, because any software may add code where it is needed internally with all the extras intended without destroying any relations. At the same time, several diverse entries are necessary to safely identify and relate all elements. XMI type and XMI ID had to be fused with the UID and also e.g. with the element’s ID Modelio uses additionally.

9 Verification and Validation of the System with a Software Demonstrator

This chapter starts with a description of the functional testing that took place before the case study, then explains the setup and execution of the very.

9.1 Practical Software Tests

To evaluate the software prototypes building the demonstrator, several evaluation techniques were used, partly involving test users, which will be laid out following the software engineering process, from concept to functional demonstrator. The software was validated assuring its single functional aspects (white box) as well as verifying predetermined expected outcomes (black box); all modules were tested on their own and regarding their contribution to system integrity. In summary, the following levels of validation were achieved:

- Single function test of the modules
- Frontend design tests
- Use-case test based on the theoretical RM system (in/out)
- GUI-based functionality tests
- Usability testing

All tests that required multiple functions and were executed by the developers themselves, were based on the dummy product ‘Hemodialysis System’ (→ 5.3.2).

9.1.1 Module Testing

The first piece of software implemented was a rudimentary prototype of the Modeling Wizard and a respective early version of the frontend using web technologies (→ 8.1.2). From here on, all implemented functions were tested individually after each change and, regularly, in its procedural context (cp. 7.1). E.g. creating a new block element in the model was tested comparing the user action on the frontend and the subsequent code change, then assigning an element class was checked the same way; later on, the functions were tested together creating a new device or adding a component element to an existing assembly.

9.1.2 API Testing

The functionality of the API was tested using the aforementioned dummy. Unit testing similar to 9.1.1 was run for newly implemented functionality. On every procedural milestone, the use case(s) were applied on the dummy and the output was then audited by the developer for regularity and compliance. Before releasing the prototype for the case study, a bidirectional black box test was executed. More complex dummy files from real product models were fed back and forth and the response compared with the primary input. This was repeated until all

relevant bugs were fixed. A more rigorous testing of the API including penetration test and fault injection is advised for future production trials.[44]

9.1.3 Frontend Design and Ergonomics

The GUI and task design of the frontend were checked on a basic level. Here, the main goal was to reach an acceptable state assuring the frontend quality would not negatively impact the usability test and the case study. A small number of experienced users of CAx and modeling environments were invited for feedback twice: in an early stage evaluating mockups (both on paper and clickable) and again later on testing a working prototype of the modeling wizard. Their opinion was captured from protocolled joint discussion and also on written and graphical feedback sheets.

9.1.4 Provisional Use-Case Tests

Based on the flow of one RM process iteration described in chapter 6, recently achieved or changed use cases were validated for every stage and subprocess with in/out checks. After performing typical tasks on the dummy material, the appropriate documents were generated. Model and documents were compared to the expected outcome by the developer and the state of implementation was communicated to the other team members.

9.1.5 Joint Functionality and Use-Case Test with End Users

In the interest of a more stable verification of the software layer tools, a group of end users was assigned a set of simple tasks to be performed under surveillance. All participants had no previous knowledge of the tools. This test was aimed at functionality (finding bugs and exploits) and usability (GUI, user navigation, articulateness of procedures) at the same time.

Three tasks from typical use cases were designed:

- **Data Handling:** upload a sample file to the DB and check if the upload was successful, view the files in the DB and download a file from the DB.
- **Model Creation I:** create a tree structure for different parts of a medical device, then view the corresponding class diagram in Modelio
- **Model Creation II:** upload a file to the wizard and view the converted output file in Modelio

Beforehand, participants received the required files and the information for creating the tree structure. After thoroughly explaining the tasks to the users, they were instructed on the think-

[44] For the sake of this research project however, safety and security measures are not an issue as the software demonstrators were simply kept isolated from any software used in production. All files were handled as copies and never fed back directly to the research partners' software environments.

aloud evaluation technique they were supposed to use during the session. With the consent of all attendees, the session was filmed and recorded.

The test brought valuable results in both key aspects. Among them, severe bugs regarding file handling were detected (and subsequently fixed). The user navigation was changed to make the experience more straightforward and system feedback was added where users were unsure or unable to finish a task without it. The general observations were also transferred as helpful design policies to the further use cases.

9.1.6 Target Group Workshop

In order to gain superior insights into the system's functionalities, a workshop was carried out with six users possessing prior knowledge and experience in RM and MBSE. The group consisted of research assistants from IPT as well as third-party professionals chosen for their proficiency with established MBSE tools. In the beginning, a short explanation of the systems and its functionalities was given. Then, the participants were requested to execute the tasks from the antecedent section and one extra task:

- **Model Creation III:** utilize the Modelio tool to construct an example model, export it and save it in the DB

The group was encouraged to discuss their opinions on the system. The test took about 90 minutes and was documented as well as recorded for future reference. The participants performed all the tasks and gave valuable advises for improving the system, of which some were implemented afterwards and the remaining considered as future work. E.g. the placement of the data entry and file upload forms in the legacy DB was reconsidered because the original layout might have become confusing with larger real-life tables. Observed difficulties with the handling of Modelio could be traced to varying practical knowledge of the users and were most likely not connected to the design of the generic model the tasks were based on. Overall, the records suggest that the choice of Modelio as the design reference for the graphical modeling is justified.

9.1.7 Survey on Usability and Learnability among Selected Attendees

Ten participants from 9.1.5 and 9.1.6 were provided with questionnaires to be responded succeeding the end of the sessions. The form gave open ended and Likert scale questions. The Likert scale questions, five-point scale, evaluated the usability and learnability of the application. In appendix F, a sample of the questionnaire applied to the participants can be found. The objective of this questionnaire was to analyze if it was easy for the user to utilize the tool or if they encountered inconveniences. In case, the last option happens, if the user performed better while executing the second task – analyze the learnability.

In table 9.1, the results from the user study are shown. The columns represent the Likert scale used and the rows are the questions and their respective answers. On the whole, it was found that the usability of the API was satisfying.

Table 9.1: Ratings cluster from user study, mean value calculation for Likert-scale data

	# Participants					
Statement	**Strongly disagree (1)**	**Disagree (2)**	**Neutral (3)**	**Agree (4)**	**Strongly agree (5)**	**Mean Value**
The app allowed you to upload the file to the database easily.	0	0	3	2	5	4.2
The app allowed you to locate the uploaded files in the database tables easily.	1	2	3	4	0	3
The app allowed you to download the files in the database easily.	0	1	2	3	4	4
The app allowed you to create the tree with all its component classes easily.	1	1	2	3	3	3.6
The app was easy to navigate and understand.	0	0	3	4	3	4
Overall Rating	0	0	2	5	3	4.1

9.2 Case Study

To verify the main research question of this thesis – whether a systematical and comprehensive RM on the whole product lifecycle of medical devices could be accomplished through a model-based approach – a case study comparing selected RM steps on two similar medical device systems was conducted. The study cases, two highly advanced prototypes of automated stem cell platforms, were chosen because they convey all major characteristics the problem statements premises for RM on complex medical devices:

9.2.1 Description of the Automated Stem Cell Platforms

Automated Stem Cell Platform in Bonn

The SCFIII in Bonn consists of medical apparatus in a housing with the external dimensions of 5.4 m x 2.6 m x 2.750 m, in where the inner side is kept sterile by a laminar flow system filtering and tempering the air flow from the ceiling downwards. An electronically locked door only allows access to the housing when no manipulator operating.

The medical apparatus of the SCFIII is composed of the following devices, as depicted in figure 9.1:

- A manipulator mounted on a linear axis moving linearly. It has got a robot arm moving the end effector, gripper, in order to reach the desired kinematic state (position, velocity, acceleration) given by the controllers. The end effector grasp and release the different tubes, microtiter plates (MTP) and disposable tips. Then, the manipulator transport them to the different positions.
- A decapper-barcode scanner allowing to scan the barcode of the MTP and tubes. The decapper removes the lid of the tube and close the tube.
- A liquid handling unit (LHU) where all the handling liquid tasks are performed. The LHU consists of a cartesian manipulator, an MTP tilter module, a tube magazine with a cooling and heating module, a media handling station, a media waste station, tip storage, tip waste, shaker and a control unit. The cartesian manipulator is in charge of refilling the media, opening and closing the MTP, pipetting medium, add medium to the tube and the MTP, transporting volume from the tube to the MTP, resuspendation and processing the source well.
- A plate reader utilized to scan, measure the pH and turbidity.
- A high-speed microscope assessing the development of the cell colonies. In addition, it measures the confluence.
- An automated centrifuge for centrifugation of the cell culture before it leaves the platform.
- A hotel to storage tip, MTP and tube.
- An incubator for incubation, tempering, aeration (CO_2, O_2), and humidity control.

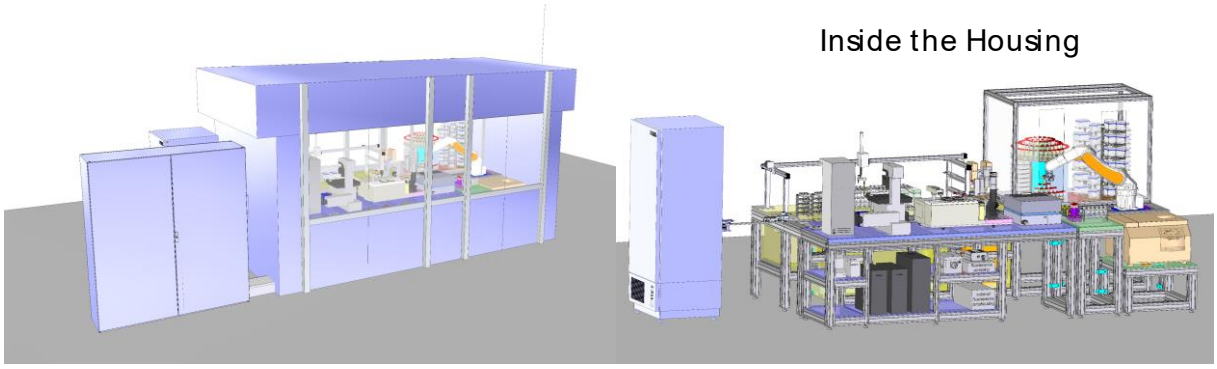


Figure 9.1: 3D views on a CAD model of the automated stem cell factory in Bonn

Automated Stem Cell Platform in Aachen

The equipment in the automated stem cell platform “stem cell discovery” (SCD) in Aachen is organizationally and functionally quite similar to the SCFIII. Some of the devices differ in brand and performance. The most important organizational difference is the existence of two storage units for the material (MTP, tubes, tips) in SCD instead of one, see figure 9.2.

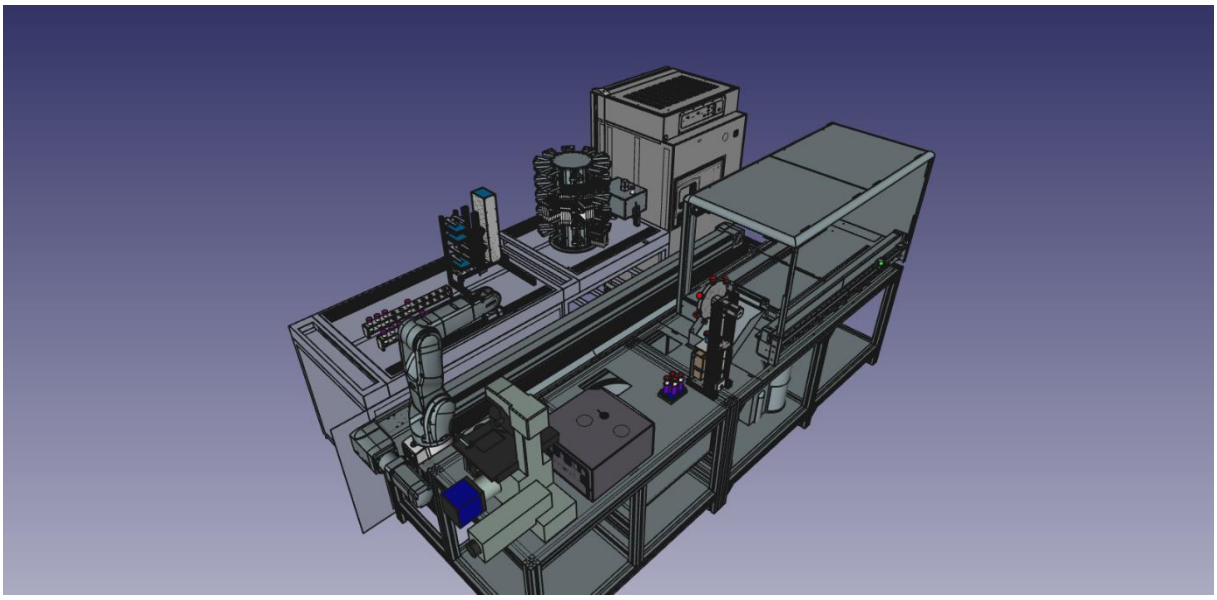


Figure 9.2: 3D view on a CAD model of the automated stem cell platform in Aachen (no housing)

Production Process: Enzyme Free Expansion

The production process analyzed was the enzyme free expansion of human induced pluripotent stem cells (hiPSCs). It is realized in both automated stem cell platforms described above. First, the cells are planted in a 6-well-MTP in the LHU and afterwards they are transported to the incubator by the manipulator. After 12 hours, it is required to control the quality, measuring the pH and the turbidity in the plate reader and the confluence in the high-speed microscope. In the case of the plate reader, if the measurement of turbidity is not in the range desired, a contamination is assumed and the MTP is transported to the waste station. Else, it is transported to the incubator where it is kept until the LHU and high-speed microscope are available. If the measurement of confluence is bigger than 80%, meaning that the cells need more space for growth and should be split, the medium is changed and the MTP is sent to the incubator. If a confluence of less than 80% is measured, the cells are harvested, see figure 9.3.

Different from the SCFIII, the SCD's production process regarded in the case study is set up for mesenchymal stem cells (MSC). From a general point of view, however, the production process similarly consists of planting, growing, quality control and harvesting. Therefore, it will not be explained in detail.

9.2.2 Preparative Work

Before starting the study with the workshops, information from resources belonging to the stakeholders of the two observed research facilities was requested, such as drawings, specifications, product/process requirements, current test plans or process control plans, reliability block diagrams and failure characteristic DBs, previous FMEA on the same or similar system/process and human resources (personnel acquainted with the system/process being analyzed).

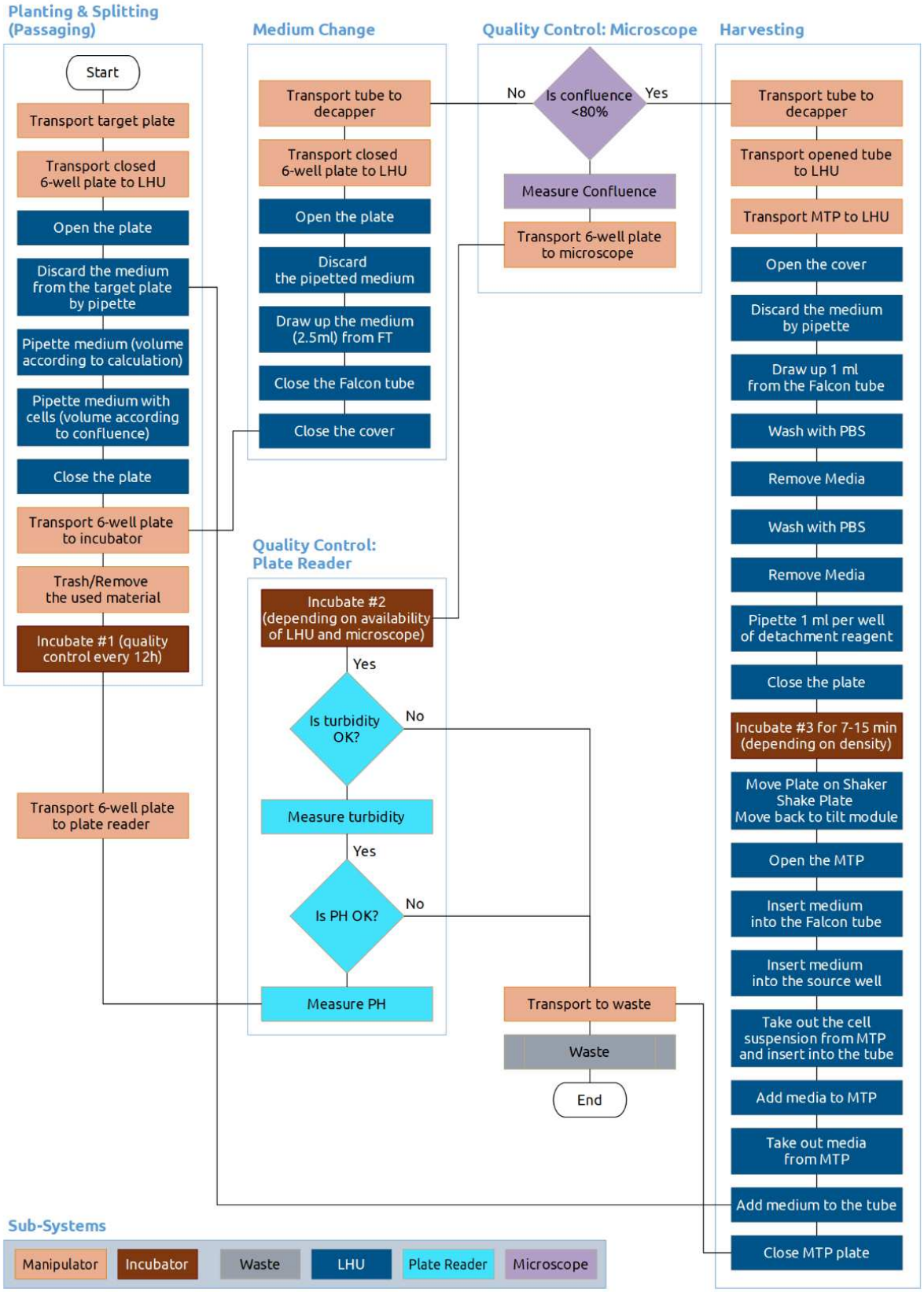


Figure 9.3: Production Process: Enzyme Free Expansion of hiPSCs, flow as conceived by the participants

This information was used to build a preliminary model of the product lifecycle via manual generation of SysML documents. The result was fed back to the responsible persons in either research facility and reworked accordingly.

For the identification of the systems and their boundaries, the investigator asked for the physical and/or functional breakdown structure of the system and the process flow diagram; the characteristics, performances, roles and functions at each level in the hierarchy; inputs and outputs of the system and process; the interfaces with other related systems or processes; the environment in which the system operates or the process is handled; any changes in the system structure for varying operational modes. The presented documentation was then analyzed and transformed into RM-relevant documents, including a general flow chart, flow charts and sequence diagrams of the subprocesses, a functional block diagram, technical comparisons etc. These were also revisited with the responsible parties.

With the insight from this provisions and personal visits of the facilities by the author, the primary models for the case study were built (→ 8.2).

9.2.3 Execution

Each test panel was composed of three experts for the respective automated stem cell platform, two of them with engineering background and one expert for the biological process. Apart from them, the author acting as the study facilitator and personnel for documentation were present in the sessions. Workshop were done for both methods where the participants were introduced to the respective method and trained with examples and a short exercise run. Both methods were executed as explained in section 4.2.6. The course of action can be seen in figure 9.4. Quick Risk Check (QRC) is in a way, a precursor to FMEA as it lists all the risks along with the probability of occurrence and the impact of the error. This allows the panel to identify all situations of high risk and take appropriate measures. These countermeasures are also noted down during study.

The whole process took two days until completion of the QRC template. The second workshop (System & Process FMECA) took around five days.

A third workshop was performed for the SCD in Aachen utilizing the QRC method and the risk identification tool developed. The MBR system was fed with a sample of 49 interactions generated from the results of the SCFIII workshops and complemented with information and material on 5 fictitious interactions which were integrated in the augmented model on code level by hand, so that there would be no way for the participants to tell them apart. To keep the panel on focus with their actual task, the augmented model was presented on a HTML page similar to the software layer frontend where they could click through to obtain more detailed information, rather than allowing them to access the MBR core via API from third-party applications.

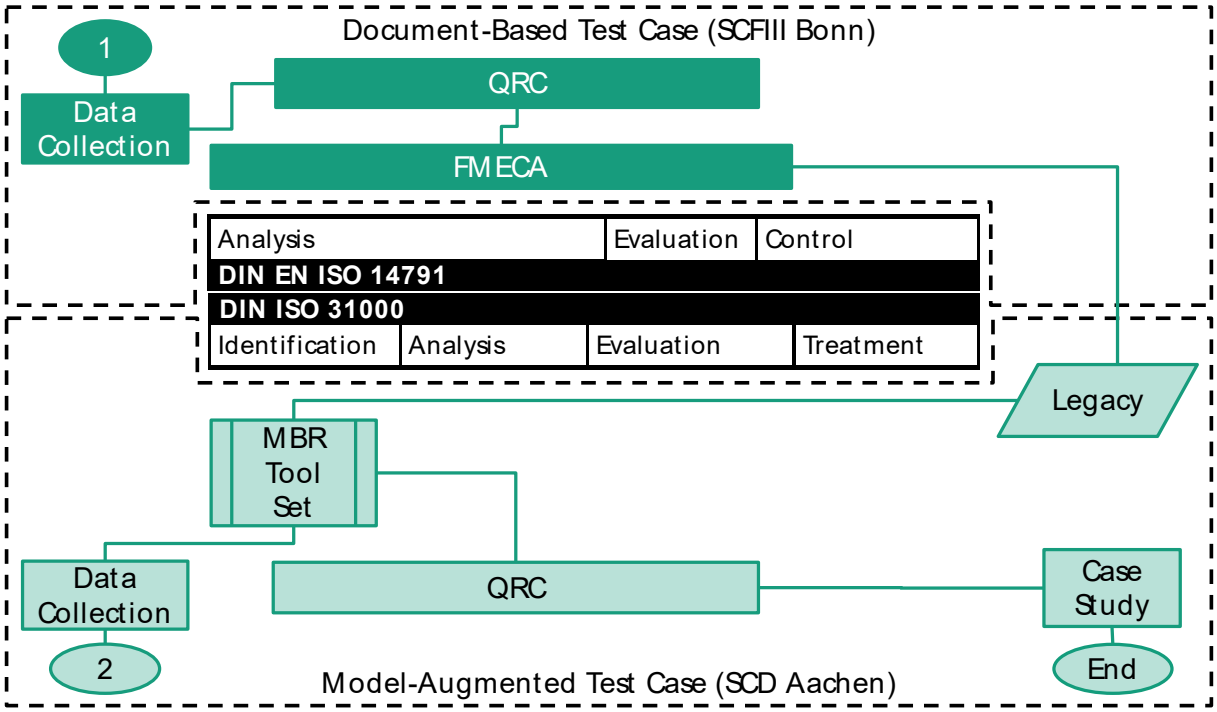


Figure 9.4: Flow of the case study in accordance with the RM process

An introduction to the so-called *MBR tool* was done and the panel was encouraged to use it as a support identifying the possible failures. They were not informed previously on the type of information they would find in the augmented model nor how exactly this information was supposed to help them. Similar to workshop 1, the panel took two working days to reach completion of the QRC template.

9.2.4 Results and Interpretation

The first workshop comprised the risk assessment for the SCFIII using QRC. Here, the most important results are listed:

- The process steps ranking results of the pairwise comparison were: planting, growing, harvesting and controlling. The subprocess were identified as: planting (material preparation), planting (inoculation), growing (medium change), growing (incubation), controlling (plate reader), controlling (microscope), harvesting (material preparation), harvesting (detachment). The panel agreed that all the processes were critical, hence all the sub-processes were analyzed.
- 49 failures were identified from which 44 failures were assessed as high and 5 failures were assessed as medium (→annex C, fig. VII.15).
- 34 measures were identified; among them two stood out with very high benefits (QRC utility function scores of 323 and 318) which both propose providing additional standard operation procedure manuals.

During this workshop, the following observations on the panel were obtained:

- QRC calls for defining linear processes which proved to be challenging for the panel because of the many ways the process loops back to the quality controlling.
- Some of the descriptions of the possible failures were kept really short and from an outsider perspective, more specific information would have been needed to capture the meaning. This led to the research team having to inquire afterwards for more details in order to be able to write the RM report. In the mindset of the panel's experts, there had been no need to elaborate; they were obviously not aware of the communication issue.

In the second workshop concerning SCFIII, the same panel executed the FMECA method whose results can be summed up as follows:

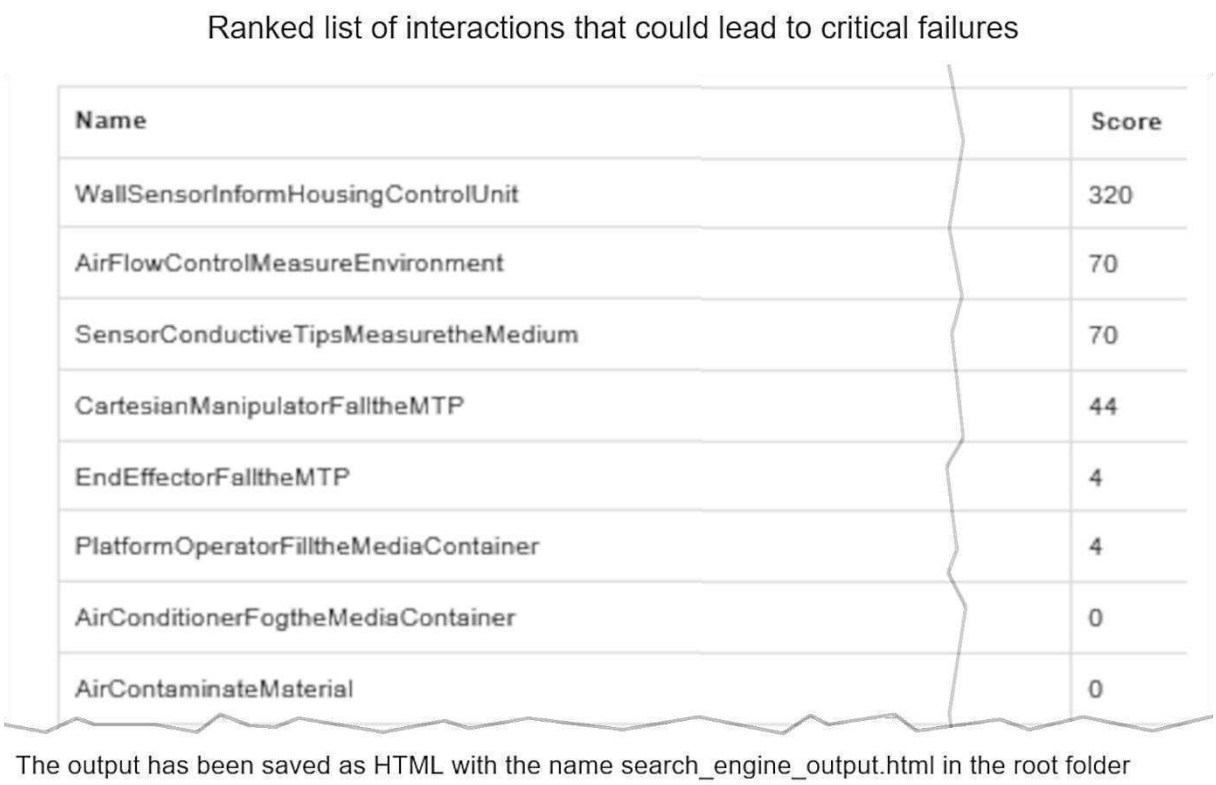
- 95 FM, 56 end effects, and 47 recommended actions were identified in the System FMECA. The Process FMECA came up with 44 FM, 28 end effects, and 28 recommended actions.
- The criticality analysis for the System FMECA identified 67 failures as acceptable, 19 failures as minor and 1 failure as undesirable. The last one describes the collision of the manipulator with any other device inside the housing (→ annex C, fig. VII.16).
- The Process FMECA showed 15 acceptable failures, 1 minor failure and 21 undesirable failures (→ annex C, fig. VII.17).

The protocol notes as special observations on the panel:

- The panel complained that it was very time-consuming filling the whole FMECA template.[45]
- Some descriptions were phrased very vague. This would happen either when the panel was not clear or would not agree on the exact element causing the FM or when they thought that the origin would be so obvious that describing it would have been redundant. Some of the terminology used by the participants emerged so deeply from within their professional mindset that none of the executing staff (with diverse academic background) would have knowledge of it. In both cases, it was necessary to meet with the experts some days after the workshops was done to obtain more details.
- The FMEA terms *current design controls (prevention)* and *current design controls (detection)* confused the panel as they did not always understand how to differentiate them. This complicated the task to allocate events to the FMEA terms, but has not led to any subsequent errors, because the study facilitator was able to clarify the meaning whenever necessary.

The third workshop (treatment) was performed with other panelists utilizing the QRC method on the SCD.

[45] It has to be mentioned, though, that none of the panelists had any previous experience with FME(C)A.



Ranked list of interactions that could lead to critical failures

Name	Score
WallSensorInformHousingControlUnit	320
AirFlowControlMeasureEnvironment	70
SensorConductiveTipsMeasuretheMedium	70
CartesianManipulatorFalltheMTP	44
EndEffectorFalltheMTP	4
PlatformOperatorFilltheMediaContainer	4
AirConditionerFogtheMediaContainer	0
AirContaminateMaterial	0

The output has been saved as HTML with the name search_engine_output.html in the root folder

Figure 9.5: Example of an assumedly critical interaction found in risk identification tool

Besides the augmented model view, the MBR tool returned a ranked list of interactions displayed in descending order of their total risk score as shown in figure 9.5. This list allows for identifying the riskiest interactions in the new model based on comparative analysis with the legacy model and taking appropriate mitigation measures.

In the beginning, the experts started to get familiar with the tool so they first looked at the SCD model. Unfortunately, the participants initially did not make any efforts to use the tool but stuck to discussing potential risk between them without referring to the identified critical characteristics. When this behavior continued in the second day of the workshop, it became necessary for the study facilitator to engage and strongly point to the recommendation to use the MBR tool. The panelists then incorporated the tool into their workflow and, once accustomed, quickly recognized the capabilities. Exemplary, some utilizations shall be described below.

The subcomponent *RobotArm.Motors* bears only one known interaction, as it may be observed on the right side of figure 9.6. The experts checked the information on FMs, severity, RPN etc. as well as the additional KB information provided, as they would do with every hit, see figure 9.7. In this case, they commented that the robot design from the SCD model was very similar to the SCFIII model and hence the FMs as suggested by the tool was “a perfect match”.

The element *Decapper Barcode Scanner* showed one hit: *DecapperBarcodeScannerIdentifytheMediaContainer*. After checking the information on the

FM, the experts concluded that the described failure was unlikely to appear in the SCD where the barcode scanner is webcam-based and separated from the decapper.

Exploring *LHU.MTPTiltModule*, they found the interaction element *MTPTilterInclinetheMTP*. They checked the information on FM, severity, RPN etc. as well as the additional KB information provided and derived the assertion that the failure was linked to properties that are unique to tube shakers. The experts commented that the LHU in SCD has only got an MTP shaker and no tube shaker. Moreover, the media dispenser with tubes from under the table is absent. Logically, they did not adopt the risk.

The last example here features the interaction *PlateReaderControlUnitDirectMTPShaker* within the plate reader control unit. The FM headline revealed the failure was directly linked to speeding. The experts commented that the plate reader controller unit is a purchased object and hence chances of failure would be low. Moreover, they said that due to the configuration in the SCD's plate reader the FM would be inexistent. According to them, in SCD the technical speed limit control would render it impossible select the wrong speed. Therefore, they did agree to not transfer the risk.

In total, 63 failures were found where 1 is connected to a higher risk, 42 to medium risk as well as 17 to low risk.

It was observed that the MBR tool can be easily used to identify FM. The users who are experts in the device design confirmed that the tool returns the list of failures in most cases. But there were also a couple of cases where the list did not show all relevant failures or showed one too many. This is acceptable as both models are not identical. The comparative search engine thus gives the user at any stage of the product lifecycle the ability to assess the risks of failure in the device and take appropriate measures to address and mitigate it.

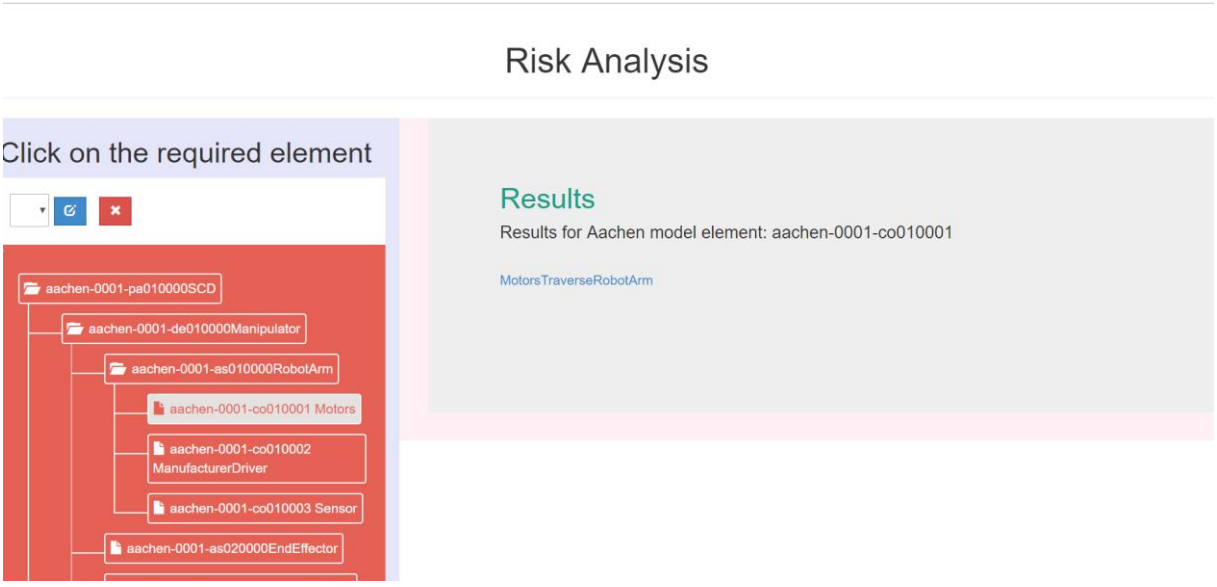


Figure 9.6: Interaction MotorsTraverseRobotArm

recordNo	79
UID	bonn-0003-in101000101
elementType	block
Class	interaction
elementName	MotorsTraverseRobotArm
Parent	bonn-0003-co101000101; bonn-0003-as1010001
GMDNname	
GMDNDefinition	
GMDNCollectiveterms	
UMLSterm	
UMLSdefinition	
UMLSrelations	
criticalCharacteristics	
ccLocator	RobotArm.Motors.DriveResponse (Boolean)
otherCharacteristics	
KBlink	
Failure mode	3.1.1.1; 3.1.2.1; 3.1.2.2
FMHeadline	Wrong position of robot arm; One of the six axis no moving; Motors are too fast.
Severity	8; 8; 8
Occurence	4; 2; 2
Detection	8; 8; 8
RPN	256; 128; 128
CriticalitySeverity	4; 4; 4
CriticalityOccurence	D; D; D
Criticality	3; 3; 3
CriticalityAccessment	Acceptable; Acceptable; Acceptable
KBID	bonn_0003_FM_3111_0001 bonn_0003_FM_3121_0001 bonn_0003_FM_3122_0001 bonn_0003_EE_1_0001 bonn_0003_TR_AA_0001 bonn_0003_TR_AB_0001 bonn_0003_TR_AD_0001

Figure 9.7: Legacy record of the interaction 'MotorsTraverseRobotArm', example with structural information from FMEA, cropped for legibility

However, it became quite clear that the quality of the collaboration between MBR core computation and RM panel depends a great deal on the skills of the RM operator to motivate the panelists to use the given information to its full extent as the experts tend to prefer an open pear discussion over exploring documentation in written and graphical form. It is believed that preponing the first contact with the legacy RM information to their familiar working environments – as it would be the case in a real-life use case of the MBR system – would have a positive effect on this issue. Yet, this would make for a very complex test case that would be difficult to control.

9.3 Effectiveness of the Demonstrator in Mitigating RM Deficits

The aggregate of the results in practical testing of the software prototypes and the experiences from the case study allows for a qualitative assessment of the system's potential to mitigate the deficits listed in section 3.3. The nature of the research project limits the conclusions to qualitative aspects and direct effects, so, whilst the underlying concept has been validated, any measures that would need long-term observations or full-scale implementations could not be verified.

Table 9.2 shows a summary that contrasts the deficits with the concept's remedy and the system's technical requirements. The concept as an entity is valid, as is the case for its individual solutions. As the second device system in the case study is an evolution to the first, but no successor, the potentials of forking models for risk treatment could not be evaluated here. Reducing the negative influences of human factors on RM results could only be shown for participants with certain preconditions (especially professional qualification); general conclusions might be achieved with more granular studies with well bigger samples.

Table 9.2: Evaluation Deficits vs. Remedies

Deficit	Endemic to Document-Based Approaches	Relevant for Problem Statement	Addressed by Concept	Requirement	Remedy	Valid?	Verified?
Missing Comprehensiveness	●	●	●	PR1, PR2, PR7, FR1, FR3	- Software Layer (Data Input Tool, Model Wizard) - Computational Identification of Critical Characteristics - Risk Identification Tool - Augmented Visualization	●	●
Uncertainty of Coverage	●	●	●	PR1, FR3	- MBR Core (RM Model) - Universal API - Augmented Visualization	●	●
No Formalization of Risk Identification as Single Step	○	●	●	PR8	- Process-Triggered RBAC - Risk Identification Tool	●	●
Incompatibility of Results	●	●	●	PR5, PR7, PR8, FR3	- MBR Core	●	●
Human Factors	◐	●	●	PR4, PR9	- Software Layer - Process-Triggered RBAC - MBR Core (Legacy DB, KB)	●	◐
Incompatible Work Environments	●	●	●	PR3, PR4, FR1, FR2	- Software Layer (Model Wizard) - Universal API - MBR Core	●	●
Poor Risk Treatment	○	●	●	PR3, PR9, FR3	- Iterative RM System - MBR Core (RM Model, Legacy DB)	●	○
Closed Fashion/No Iteration Possible	●	●	●	PR6, PR9, FR2	- Iterative RM System - MBR Core (RM Model, Legacy DB) - Universal API	●	●
Insufficiency for High Level of Complexity/Interactions	●	●	●	PR1, PR3, PR7, FR1, FR3	- Computational Identification of Critical Characteristics - Risk Identification Tool - MBR Core (Data Selection and Separation) - Augmented XXXXXX	●	●
Unacceptable Execution Cost	●	●	●	PR3, FR1, FR2	- Software Layer (- MBSE per se)	●	○

● yes/fulfilled ○ no/unfulfilled ◐ partially applicable/fulfilled

10 Model-Based Risk in Future MedTech

Risk management plays a crucial role to overcome the challenges of fast technological changes, competitive time-to-market, shorter innovation cycles, more stakeholders with different professional backgrounds and more complex devices and device networks. Ever more complex product lifecycles reduce the probability of a comprehensive RM process significantly due to the fact that most RM methods do no adjust well to this concurrency which leads to exponentially growing workload. Furthermore, complexity impedes risk identification resulting in residual risk resurfacing as failure later on. This is directly correlated to higher number of stakeholders and data sources for product information.

Technical and formal barriers for interdisciplinary exchange, complicated interoperability, uncertain congruence and co-dependency and high software adaptation cost are the main reasons engineers use many different MBSE tools implying many data sources and provoking transcription and copy errors. All those issues weigh down the advantage of using MBSE because they ultimately violate its most important principle: drawing conclusions from one single source of truth. Therefore, it will become vital to comprehend the development of the coexisting data structures in order to dominate risk in future medical devices.

The result of the research for this work lead to two major beneficial changes in RM for medical devices evolving in the way described above:

As nearly all product models pursue a purpose-driven design which is represented best by Stachowiak's pragmatic modeling approach, risk models in future RM systems should, too. It enhances the chances to incorporate risk-based thinking with all stakeholders and keeps the organizational demands of RM for very complex products manageable. The MBR approach shows that it is feasible and advantageous to shift certain tasks within the RM process to computation, especially in the risk identification step. While the technical implementation is most likely a profitable investment, the case study has shown that it is the human beings that need to adapt to the interdependencies and must be led to trust both the processes that they feel are no longer entirely in their hands and the legacy data that they cannot (at least: not always) trace back completely to its origins.[46] The key to vanquishing these adversaries is a low-threshold embedding of the RM system into the professional environments of the stakeholders. Here, comparative studies on how this can be achieved in various professional settings (medical staff, production engineer, maintenance personnel, etc.) with demonstrator plugins would be a promising continuation of the research.

[46] These allegations are, of course, biased, as both conditions already exist without the new approach. They would only be absent in a scenario with perfect information, which is utterly inconceivable in RM. The bias, though, is real and influences the effectiveness of the implementation.

Second, the trends in MedTech will further blur the lines between product rollout and upgrade. Device networks will evolve in versions rather than being totally replaced; software has become a critical part of the products faster than the industry's RM activities reckon with. An iterative approach alongside process chain like the one proposed in this work allows for a better integration of data sources from third parties in the device network and the versioning of RM processes. It provides the RM operator with the possibility to fork the RM model based on diverging treatments in order to compare impacts and costs. The real implications of this feature should be examined in future research, though.

The MBR approach has shown to deal with the deficits in comprehensiveness and cognitive uncertainties of common document-based RM systems. Its API permits integrating already existing, valuable data to RM that otherwise might have been futile as well as augmenting product lifecycles with information on critical characteristics. As a result, it may help to keep cost on software, training and IT maintenance low and increment the ability to reply to changes and to raise productivity. The following three rules will help to capitalize on the advantages of MBR:

- RM models should follow the same design than the dominating product models in the industrial sector.
- Deliberate data selection criteria keep models lean and allow for budget computing.
- Productive data interchange is facilitated by using open standards like OSLC and interfaces that can be integrated into different professional environments.

As literature and earlier research projects at IPT suggested, SysML and UML have indeed proven to be the modeling language that fit the requirements for complex RM models the best. However, they are exclusively graphical; hence, they do not have a text-based syntax. Complementing them with XML/XMI in order to suit computerization turned out to be a good choice. In this work, the testing of this approach has been limited to functionality and functional usability. In future research, it would be desirable to build a production prototype solely based on own and open source code to fully test all usability and security aspects.

The development of a closed nomenclature in conjunction with the integration of the medical classification systems of GMDN and UMLS has shown to benefit both lean computation and human comprehension. The identification of known critical characteristics from legacy data subsequently has presented sound and consistent results. It is, though, recommended to broaden the examination of the nomenclature off the PBS to structures that influence more heavily later stages of the product lifecycle, like personas or procedures.

VI Bibliography

[AHME07] Ahmed, A.; Kayis, B.; Amornsawadwatana, S.: A review of techniques for risk management in projects. In: Benchmarking: An international journal 14/2007, Nr. 1, p. 22–36

[ALTH05] Althaus, C.: A Disciplinary Perspective on the Epistemological Status of Risk. In: Risk Analysis 25/2005, Nr. 3, p. 567–588

[ANAN10] Anand, K.; Saini, S.; Singh, B.; Veermaram, C.: Global Medical Device Nomenclature: The Concept for Reducing Device-Related Medical Errors. In: Journal of Young Pharmacists : JYP 2/2010, Nr. 4, p. 403–409

[ASHB00] Ashburner, M.; Ball, C.; Blake, J.; Botstein, D.; Butler, H.; Cherry, J.; Davis, A.; Dolinski, K.; Dwight, S.; Eppig, J.; Harris, M.; Hill, D.; Issel-Tarver, L.; Kasarskis, A.; Lewis, S.; Matese, J.; Richardson, J.; Ringwald, M.; Rubin, G.; Sherlock, G.: Gene ontology: tool for the unification of biology. The Gene Ontology Consortium. In: Nature genetics 25/2000, Nr. 1, p. 25–29

[AUER90] Auer, J.; Gokal, R.; Stout, J.; Hillier, V.; Kincey, J.; Simon, L.; Oliver, D.: The Oxford-Manchester study of dialysis patients. Age, risk factors and treatment method in relation to quality of life. In: Scandinavian journal of urology and nephrology. Supplementum 131/1990, p. 31–37

[AVEN09] Aven, T.; Renn, O.: On risk defined as an event where the outcome is uncertain. In: Journal of Risk Research 12/2009, Nr. 1, p. 1–11

[AVEN12] Aven, T.: The risk concept—historical and recent development trends. In: Reliability Engineering & System Safety 99/2012, Supplement C, p. 33–44

[AVEN16] Aven, T.: Risk assessment and risk management: Review of recent advances on their foundation. In: European Journal of Operational Research 253/2016, Nr. 1, p. 1–13

[BADR13] Badreddine, A.; Ben Amor, N.; Badreddine, A.; Amor, N.: A Bayesian approach to construct bow tie diagrams for risk evaluation. In: Process Safety And Environmental Protection 91/2013, Nr. 3, p. 159–171

[BAHI15] Bahill, A.; Smith, E.: An Industry Standard Risk Analysis Technique. In: Engineering Management Journal 21/2015, Nr. 4, p. 16–29

[BAIH09] Baihly, J.; Grant, D.; Fan, L.; Bodwadkar, S.; Baihly, J.; Grant, D.; Fan, L.; Bodwadkar, S.: Horizontal Wells in Tight Gas Sands--A Method for Risk Management to Maximize Success. In: Spe Production & Operations 24/2009, Nr. 02, p. 277–292

[BAJA16] Bajaj, M.; Zwemer, D.; Yntema, R.; Phung, A.; Kumar, A.; Dwivedi, A.; Waikar, M.: MBSE++ - Foundations for Extended Model-Based Systems Engineering Across System Lifecycle. In: INCOSE International Symposium 26/2016, Nr. 1, p. 2429–2445

[BAJA17] Bajaj, M.; Backhaus, J.; Walden, T.; Waikar, M.; Zwemer, D.; Schreiber, C.; Issa, G.; Martin, L.: Graph-Based Digital Blueprint for Model Based Engineering of Complex Systems. In: INCOSE International Symposium 27/2017, Nr. 1, p. 151–169

[BALA12] Balaban, M.; Cabot, J.; Gogolla, M.; Wilke, C.: Workshop on OCL and textual modeling. In: the 12th Workshop. Innsbruck, Austria, 9/30/2012 - 9/30/2012. New York, New York, USA: ACM Press, 2012, p. 5–6

[BALM06] Balmelli, L.; Brown, D.; Cantor, M.; Mott, M.; Balmelli, L.; Brown, D.; Cantor, M.; Mott, M.: Model-driven systems development. In: IBM Systems Journal 45/2006, Nr. 3, p. 569–585

[BALM07] Balmelli, L.: The Systems Modeling Language for Products and Systems Development. In: Journal of Object Technology 6/2007, Nr. 6, p. 149–177

[BALZ15] Balzekiene, A.; Gaule, E.; Jasinevicius, R.; Kazanavicius, E.; Petrauskas, V.: Risk Evaluation: The Paradigm and Tools. In: International Conference on Information and Software Technologies. Druskininkai, Lithuania, October 15-16. Cham: Springer International Publishing, 2015, p. 330–342

[BEIH14] Beihoff, B.; Oster, C.; Friedenthal, S.; Paredis, C.; Kemp, D.; Stoewer, H.; Nichols, D.; Wade, J.: A World in Motion – Systems Engineering Vision 2025. 2014

[BETH09] Bethesda (MD): National Library of Medicine (US): UMLS® Reference Manual [Internet]. September 2009

[BODE04] Bodenreider, O.: The Unified Medical Language System (UMLS): integrating biomedical terminology. In: Nucleic Acids Research 32/2004, Database issue, D267-D270

[BODE08] Bodenreider, O.: Biomedical Ontologies in Action: Role in Knowledge Management, Data Integration and Decision Support. In: Yearbook of medical informatics2008, p. 67–79

[BOIS04] Boisot, M.; Canals, A.: Data, information and knowledge: have we got it right? In: Journal of Evolutionary Economics 14/2004, Nr. 1, p. 43–67

[BOOC05] Booch, G.; Rumbaugh, J.; Jacobson, I.: The unified modeling language user guide. 2nd ed. Upper Saddle River, NJ: Addison-Wesley, 2005

[BRON16] Bronkhorst, E.; Leask, E.: Business process management as a tax risk identification and management method. In: eJournal of Tax Research 14/2016, p. 567–586

[BRUN02] Brunnermeier, S.; Martin, S.: Interoperability costs in the US automotive supply chain. In: Supply Chain Management: An International Journal 7/2002, Nr. 2, p. 71–82

[BRYM16] Bryman, A.: Integrating quantitative and qualitative research. How is it done? In: Qualitative Research 6/2016, Nr. 1, p. 97–113

[BSI16] BSI: Understanding Quality Management System (QMS) certification. URL: https://www.bsigroup.com/meddev/LocalFiles/en-GB/Services/BSI-md-iso-13485-qms-brochure-UK-EN.pdf [Last access: 09.02.2016]

[BURT06] Burton, J.; McCaffery, F.; Richardson, I.: A risk management capability model for use in medical device companies. In: the 2006 international workshop. Shanghai, China, 21-05-2006 - 21-05-2006. New York, New York, USA: ACM Press, 2006, p. 3

[BURT08] Burton, J.: A Software Risk Management Capability Model for Medical Device Software. Doktorarbeit The Irish Software Engineering Research Centre, University of Limerick, Limerick, Ireland, 2008 [Last access: 10.11.2014]

[CAST16] Castaño, C.; Schmitt, R.: Model-Based Risk as a Path to Safer Medical Devices. In: Proceedings of the Twenty-fourth Safety-critical Systems Symposium.

Brighton, UK,, 2nd-4th February 2016: CreateSpace Independent Publishing Platform, 2016, p. 365–381

[CAST17] Castano Reyes, C.; Kiesel, R.; Schmitt, R.: First-class risk management from second-use data sources: How intelligent data processing could make risk management more efficient and affordable for SMEs. In: 3rd Annual IEEE International Symposium on Systems Engineering. Vienna, Austria, October 11-13,. Piscataway, NJ: IEEE, 2017, p. 1–7

[CERN15] Cerniglia-Lowensen, J.: Learning From Mistakes and Near Mistakes:. Using Root Cause Analysis as a Risk Management Tool. In: Journal of Radiology Nursing 34/2015, Nr. 1, p. 4–7

[CHAN10] Chan, S.; Larsen, G.: A Framework for Supplier-Supply Chain Risk Management. Tradespace Factors to Achieve Risk Reduction – Return on Investment. In: IEEE International Conference on Technologies for Homeland Security (HST). Waltham, MA, USA, 8 - 10 Nov. 2010. Piscataway, NJ: IEEE, 2010, p. 29–34

[CHAP98] Chapman, R.: The Effectiveness of Working Group Risk Identification and Assessment Techniques. In: International Journal of Project Management 16/1998, Nr. 6, p. 333–343

[CHEN05] Chen, H.; Friedman, C.; Fuller, S.; Hersh, W.: Medical Informatics. Knowledge Management and Data Mining in Biomedicine. (Series: Integrated Series in Information Systems, vol. 8). Boston, MA: Springer Science+Business Media Inc, 2005

[CHEN11] Chen, T.; Lai, H.; Chen, T.-Y.: A risk management method for enhancing patient safety based on interval- valued fuzzy numbers. In: African Journal Of Business Management 5/2011, Nr. 30, p. 11925–11945

[CHIC89] Chicken, J.; Hayns, M.: The Risk Ranking Technique in Decision Making. 1st ed. Oxford: Pergamon Pr, 1989

[COHE09] Cohen, L.; Manion, L.; Morrison, K.: Research methods in education. 6th ed. London: Routledge, 2009

[COOP09] Cooper, H.: Handbook of Research Synthesis and Meta-Analysis, The. New York: Russell Sage Foundation, 2009

[CORC13] Corciovă, C.; Turnea, M.; Ciorap, R.: Risk Management for Medical Devices. In: Marascu-Klein, V. (ed.): Advances in Biomedicine and Health Science.

Proceedings of the 2nd International Conference on Biomedicine and Health Engineering (BIHE '13), Proceedings of the 2nd International Conference on Health Science and Biomedical Systems (HSBS '13). Athens: WSEAS Press, 2013, p. 51–56

[CORN14] Corns, S.; Thukral, A.; Stein, J.: INCOSE Biomedical-Healthcare Working Group (BHWG) (Model-Based Systems Engineering (MBSE) Challenge Team Meeting). January 27, 2014. – upated: 2014-01-27

[CORO04] Coronado, S. de; Haber, M.; Sioutos, N.; Tuttle, M.; Wright, L.: NCI Thesaurus: using science-based terminology to integrate cancer research results. In: Studies in health technology and informatics 107/2004, Pt 1, p. 33–37

[DASH10] DashWu, D.; Kefan, X.; Gang, C.; Ping, G.: A Risk Analysis Model in Concurrent Engineering Product Development. In: Risk Analysis 30/2010, Nr. 9, p. 1440–1453

[DELL13] Delligatti, L.: SysML distilled. A brief guide to the systems modeling language. Upper Saddle River, NJ: Addison-Wesley, 2013

[DÍAZ16] Díaz-Garduño, B.; Rueda-Márquez, J.; Manzano, M.; Garrido-Pérez, C.; Martín-Díaz, M.: Are combined AOPs effective for toxicity reduction in receiving marine environment? Suitability of battery of bioassays for wastewater treatment plant (WWTP) effluent as an ecotoxicological assessment. In: Marine Environmental Research 114/2016, p. 1–11

[DICK13] Dickerson, C.; Mavris, D.: A Brief History of Models and Model Based Systems Engineering and the Case for Relational Orientation. In: IEEE Systems Journal 7/2013, Nr. 4, p. 581–592

[DIN15] Standard ,DIN EN 60812 (August 2015). Failure Mode and Effects analysis (FMEA)

[DONE15] Donelan, R.; Walker, S.; Salek, S.: Factors influencing quality decision-making. Regulatory and pharmaceutical industry perspectives. In: Pharmacoepidemiology and drug safety 24/2015, Nr. 3, p. 319–328

[DONN06] Donnelly, K.: SNOMED-CT: The advanced terminology and coding system for eHealth. In: Studies in health technology and informatics 121/2006, p. 279–290

[DORI11] Dori, D.: Object-Process Methodology for Structure-Behavior Co-Design. In: Embley, D.; Thalheim, B. (ed.): Handbook of Conceptual Modeling. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, p. 209–258

[DOUG14] Douglass, B.; Douglass, B.: Real-Time UML Workshop for Embedded Systems. The Harmony Process. Newnes: Elsevier, 2014

[DRIG15] Drigo, E.; Filho, S.; Sousa, C.: Operator discourse analysis as a tool for risk management. In: 25th European Safety and Reliability Conference, ESREL 2015. Zürich, Switzerland, 7-10 September 2015. Boca Raton, London, New York: CRC Press; CRC Press Taylor & Francis Group a Balkema book, 2015, p. 416

[DULC91] Dulcos, R.; Shepherd, N.: Automated Logistics Support Analysis Tool, Version I. 0, User's Manual - Functional Requirements Risk Identification (LSA Subtask 301.2.3). Ridgefield, N.J., May 1991

[EBER13] Ebert, C.: Risikomanagement kompakt. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013

[EDEN07] Eden, A.: Three Paradigms of Computer Science. In: Minds and Machines 17/2007, Nr. 2, p. 135–167

[ELAA13] Elaasar, M.; Neal, A.: Integrating Modeling Tools in the Development Lifecycle with OSLC: A Case Study. In: Moreira, A.; Schätz, B.; Gray, J.; Vallecillo, A. (ed.): Model-Driven Engineering Languages and Systems. 16th International Conference, Models 2013, Miami, Fl, USA, September/October 2013, Proceedings. (Series: Lecture Notes in Computer Science / Programming and Software Engineering, v.8107). Berlin/Heidelberg: Springer Berlin Heidelberg, 2013, p. 154–169

[EOM06] Eom, J.-H.; Lee, S.-H.; Lim, H.-J.; Chung, T.-M.: Qualitative Method-Based the Effective Risk Mitigation Method in the Risk Management. In: Computational Science and Its Applications - ICCSA 2006. Glasgow, UK,, 8-11 May. Berlin, Heidelberg: Springer Berlin Heidelberg; Springer-Verlag GmbH, 2006, p. 239–248

[ERIC05] Ericson, C.: Preliminary Hazard Analysis. In: Ericson, C. (ed.): Hazard Analysis Techniques for System Safety. Hoboken, NJ, USA: John Wiley & Sons, Inc, 2005, p. 73–93

[ESTE08] Estefan, J.: Survey of Model-Based Systems Engineering (MBSE) Methodologies ,INCOSE-TD-2007-003-02. 2008

[EURO15] European Commission: Medical devices in EU. URL: https://ec.europa.eu/growth/content/medical-devices-eu-infographic-0_en [Last access: 06.02.2018]

[EURO17a], European Parliament and the Council of the European Union: REGULATION (EU) 2017/745 of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC, 5 April 2017

[EURO17b], European Parliament and the Council of the European Union: REGULATION (EU) 2017/746 of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU, 5 April 2017

[EURO18a]European Patent Office: European Patent Applications 2008-2017 per Field of Technology. URL: http://www.epo.org/about-us/annual-reports-statistics/statistics.html#applications [Last access: 03.04.2018]

[EURO18b]European Commission: Regulatory framework. URL: http://ec.europa.eu/growth/sectors/medical-devices/regulatory-framework_en [Last access: 06.02.2018]

[FALA11] Falahah: Risk management assessment using SERIM method. In: e-Education, Entertainment and e-Management (ICEEE), 2011 International Conference on2011, p. 340–343

[FISC12] FIscher, B.: Risikomanagement. In: mt-medizintechnik 78/2012, Nr. 3, p. 91–98

[FLEM99] Fleming, M.; Manwell, L.: Brief intervention in primary care settings. A primary treatment method for at-risk, problem, and dependent drinkers. In: Alcohol research & health : the journal of the National Institute on Alcohol Abuse and Alcoholism 23/1999, Nr. 2, p. 128–137

[FRAN93] François, B.; Dujardin, B.; Kegels, G.: To screen or systematically treat a population at risk? A method based on the analysis of costs applicable at the level of district health. In: Bulletin Of The World Health Organization 71/1993, Nr. 5, p. 587–594

[FRAU14] Fraunhofer FOKUS: ModelBus Overview. URL: https://www.modelbus.org/en/modelbusoverview.html [Last access: 25.04.2019]

[FRIE12] Friedenthal, S.; Moore, A.; Steiner, R.: A practical guide to SysML. The systems modeling language. 2nd ed. Waltham, MA: Morgan Kaufmann, 2012

[FRIS16] Frischer, J.; Fraller, A.; Mallouhi, A.; Vogl, U.; Baier, F.; Ertl, A.; Preusser, M.; Knosp, E.; Kitz, K.; Gatterbauer, B.: Evaluation of Dose-Staged Gamma Knife Radiosurgical Treatment Method for High-Risk Brain Metastases. In: World Neurosurgery 94/2016, p. 352–359

[GARR90] Garrabrants, W.; Ellis, A.; Hoffman, L.; Kamel, M.: CERTS: a comparative evaluation method for risk management methodologies and tools. In: Computer Security Applications Conference, 1990., Proceedings of the Sixth Annual1990, p. 251–257

[GAYE94] Gayet, B.; Briand, L.: METRIX: a tool for software-risk analysis and management. Proceedings of Annual Reliability and Maintainability Symposium, 0 1994, pp.310-314. In: Reliability and Maintainability Symposium, 1994. Proceedings., Annual1994, p. 310–314

[GJER11] Gjerdrum, D.; Peter, M.: The New International Standard on the Practice of Risk Management – A Comparison of ISO 31000:2009 and the COSO ERM Framework. In: Risk Management2011, Nr. 21, p. 8–12

[GLOB12] Global Harmonization Task Force, Study Group 1: Definition of the Terms ‘Medical Device’ and ‘In Vitro Diagnostic (IVD) Medical Device’. N071:2012. May 16th/2012

[GMDN10] GMDN Agency: GMDN User Guide. Version 2010. 2010

[GMDN18] GMDN Agency: GMDN Database. URL: https://www.gmdnagency.org/About/Database [Last access: 21.02.2018]

[GRAN04] Gran, B.; Fredriksen, R.; Thunem, A.: An Approach for Model-Based Risk Assessment. In: Hutchison, D.; Kanade, T.; Kittler, J.; Kleinberg, J.; Mattern, F.; Mitchell, J.; Naor, M.; Nierstrasz, O.; Pandu Rangan, C.; Steffen, B.; Sudan, M.; Terzopoulos, D.; Tygar, D.; Vardi, M.; Weikum, G.; Heisel, M.; Liggesmeyer, P.; Wittmann, S. (ed.): Computer Safety, Reliability, and Security. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, p. 311–324

[GRUB11] Grubisic, V.; Ogliari, A.; Gidel, T.: Recommendations for risk identification method selection according to product design and project management maturity, product innovation degree and project team. In: 18th International Conference on

Engineering Design. Copenhagen, 15 - 18 August 2011. København: Design Society; Technical University of Denmark, 2011, p. 187–198

[GUI15] GUI, Z.; ZHANG, C.; Li, M.; GUO, P.: Risk analysis methods of the water resources system under uncertainty. In: Frontiers of Agricultural Science and Engineering 2/2015, Nr. 3, p. 205

[GUPT16] Gupta, N.; Charan, H.: Hazard operability analysis (HAZOP): A quality risk management tool. In: International Journal of PharmTech Research 9/2016, p. 366–373

[HACU01] Hacura, A.; Jadamus-Hacura, M.; Kocot, A.: Risk analysis in investment appraisal based on the Monte Carlo simulation technique. In: The European Physical Journal B - Condensed Matter and Complex Systems 20/2001, Nr. 4, p. 551–553

[HALL11] Hall, D.: Making risk assessments more comparable and repeatable. In: Systems Engineering 14/2011, Nr. 2, p. 173–179

[HAO13] Hao, R.; Liu, F.; Ren, H.; Cheng, S.; Hao, R.; Ren, H.; Cheng, S.: Study on a comprehensive evaluation method for the assessment of the operational efficiency of wastewater treatment plants. In: Stochastic Environmental Research and Risk Assessment 27/2013, Nr. 3, p. 747–756

[HARW11] Harwell, M.: Research Design in Qualitative/Quantitative/Mixed Methods. In: Conrad, C. (ed.): The Sage handbook for research in education. Pursuing ideas as the keystone of exemplary inquiry. 2. ed. Los Angeles, Calif.: SAGE Publ, 2011, p. 147–164

[HASK11] Haskins, C.: A Historical Perspective of MBSE with a View to the Future. In: INCOSE International Symposium 21/2011, Nr. 1, p. 493–509

[HEAL10], Health and Consumers Directorate-General of the European Commission: EU Guidelines to Good Manufacturing Practice for Medicinal Products for Human and Veterinary Use - Introduction. In: EudraLex, December 2010

[HEAL12], Health and Consumers Directorate-General of the European Commission: EU Guidelines for Good Manufacturing Practice for Medicinal Products for Human and Veterinary Use - Chapter 1. Pharmaceutical Quality System. In: EudraLex, June 2012

[HEAL15], Health and Consumers Directorate-General of the European Commission: EU Guidelines for Good Manufacturing Practice for Medicinal Products for Human and Veterinary Use - Annex 15. Qualification and Validation. In: EudraLex, March 2015

[HEND08a] Henden, J.: Preventing Suicide. Oxford, UK: John Wiley & Sons, Ltd, 2008

[HEND08b] Henden, J.: Current Service Provision: Risk Assessment, Management and Medication. In: Henden, J. (ed.): Preventing Suicide. Oxford, UK: John Wiley & Sons, Ltd, 2008, p. 31–46

[HERO13] Heron, M.; Hanson, V.; Ricketts, I.: Open source and accessibility: advantages and limitations. In: Journal of Interaction Science 1/2013, Nr. 1, p. 2

[HOLZ14] Holzinger, A.: Biomedical Informatics. Discovering Knowledge in Big Data. Cham, s.l.: Springer International Publishing, 2014

[HUFF98] Huff, S.; Rocha, R.; McDonald, C.; Moor, G. de; Fiers, T.; Bidgood, W.; Forrey, A.; Francis, W.; Tracy, W.; Leavelle, D.; Stalling, F.; Griffin, B.; Maloney, P.; Leland, D.; Charles, L.; Hutchins, K.; Baenziger, J.: Development of the Logical Observation Identifier Names and Codes (LOINC) vocabulary. In: Journal of the American Medical Informatics Association : JAMIA 5/1998, Nr. 3, p. 276–292

[IBM18] IBM: Rational Rhapsody. URL: https://www.ibm.com/uk-en/marketplace/rational-rhapsody [Last access: 01.05.2018]

[IEC09] Standard ,IEC/ISO 31010 (November 2009). Risk management - Risk assessment techniques

[INCO07] INCOSE Technical Operations: Systems Engineering Vision 2020 ,INCOSE-TP-2004-004-02ed. 2.03. September 2007

[INGH05] Ingham, M.; Rasmussen, R.; Bennett, M.; Moncada, A.: Engineering Complex Embedded Systems with State Analysis and the Mission Data System. In: Journal of Aerospace Computing Information and Communication 2/2005, Nr. 12, p. 507–536

[ISO03] Standard ,ISO 13485 (July 2003). Medical devices - Quality management systems -Requirements for regulatory purposes

[ISO07] ISO; IEC: Using and referencing ISO and IEC standards for technical regulations. September 2007

[ISO09a] Standard ,ISO 31000 (November 2009). Risk management — Principles and guidelines

[ISO09b] Guide ,ISO Guide 73 (2009). Risk management — Vocabulary

[ISO10] Standard ,ISO 15225 (May 2010). Medical devices — Quality management — Medical device nomenclature data structure

[ISO11] Standard ,ISO/IEC 25010 (March 2011). Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models

[ISO12] standard ,ISO 13022 (April 2012). Medical products containing viable human cells - Application of risk management and requirements for processing practices

[ISO15a] Standard ,ISO/IEC/IEEE 15288 (May 2015). Systems and software engineering - System life cycle processes

[ISO15b] Standard ,ISO 9000 (November 2015). Quality management systems – Fundamentals and vocabulary

[ISO15c] Standard ,ISO 9001 (November 2015). Quality management systems – Requirements

[ISO16] Standard ,ISO/IEC TS 24748-1 (May 2016). Systems and software engineering -- Life cycle management --Part 1: Guidelines for life cycle management

[ISO17] ,ISO/IEC 19514 (March 2017). Information technology — Object management group systems modeling language (OMG SysML)

[JASE92] Jaselskis, E.; Russell, J.; Jaselskis, E.; Russell, J.: Risk Analysis Approach to Selection of Contractor Evaluation Method. In: Journal Of Construction Engineering And Management-Asce 118/1992, Nr. 4, p. 814–821

[JIAN10] Jiang, J.; Huang, A.; Liu, Y.: Risk Evaluation of Generation-Load System Based on Monte Carlo Method and Fast Clustering Analysis Method. In: Electrical and Control Engineering (ICECE), 2010 International Conference on2010, p. 4185–4188

[JULI12] Julia Murray: Model Based Systems Engineering (MBSE) Media Study - Julia Almond-Murray. May 2, 2012

[KASA07] Kasap, D.; Kaymak, M.: Risk Identification Step of the Project Risk Management. In: PICMET '07 - 2007 Portland International Conference on Management of Engineering & Technology. Portland, OR, USA, 5-9 August. Piscataway, NJ: IEEE, 2007, p. 2116–2120

[KAYI07] Kayis, B.; Zhou, M.; Savci, S.; Khoo, Y.; Ahmed, A.; Kusumo, R.; Rispler, A.: IRMAS – development of a risk management tool for collaborative multi-site, multi-partner new product development projects. In: Journal of Manufacturing Technology 18/2007, Nr. 4, p. 387–414

[KIRO16] Kirova, M.; Velikova, P.; Kirova, M.; Velikova, P.: Risk management method for small photovoltaic plants. In: Management and Marketing 11/2016, Nr. 3, p. 498–512

[KOTH04] Kothari, C.: Research methodology. Methods & techniques. 2nd ed. New Delhi: New Age International (P) Ltd. Publishers, 2004

[KRAU93] Krause, F.-L.; Kimura, F.; Kjellberg, T.; Lu, S.-Y.; van der Wolf; Alting, L.; ElMaraghy, H.; Eversheim, W.; Iwata, K.; Suh, N.; Tipnis, V.; Week, M.; A.C.H.: Product Modelling. In: CIRP Annals - Manufacturing Technology 42/1993, Nr. 2, p. 695–706

[KREI04] Kreinovich, V.; Ferson, S.: A new Cauchy-based black-box technique for uncertainty in risk analysis. In: Reliability Engineering and System Safety 85/2004, 1-3, p. 267–279

[KURT85] Kurth, R.: Development and application of a new probabilistic analysis technique for nuclear risk calculations. [RASCAL technique]. Dissertation Department of Nuclear Engineering, The Ohio State University, Ohio, 1985. URL: https://etd.ohiolink.edu/!etd.send_file?accession=osu148725958026113&disposition=inline [Last access: 05.01.2020]

[LAMM05] Lammers, W.; Badia, P.: Fundamentals of behavioral research. Belmont, Calif.: Thomson/Wadsworth, 2005

[LAZA17a] Lazar, J.; Feng, J.; Hochheiser, H.: Chapter 10 - Usability testing. In: Lazar, J.; Feng, J.; Hochheiser, H. (ed.): Research Methods in Human Computer Interaction (Second Edition). Second Edition. Boston: Morgan Kaufmann, 2017, p. 263–298

[LAZA17b] Lazar, J.; Feng, J.; Hochheiser, H.: Research Methods in Human Computer Interaction (Second Edition). Boston: Morgan Kaufmann, 2017

[LENI08] Lenin, V.: Materialism and Empirio-criticism. (Series: Collected Works, vol. 14). Moscow: Progress Publishers, 1908

[LEVI93] Levin, B.: English Verb Classes and Alternations. A Preliminary Investigation: The University of Chicago Press, 1993

[LI10a] Li, Y.-P.; Wang, W.; Leng, X.-M.; Li, Y.-P.; Leng, X.-M.: A Hierarchy Gap Method (HGM) for Risk Identification. In: Industrial Engineering and Engineering Management (IE&EM), 2010 IEEE 17Th International Conference on2010, p. 995–999

[LI10b] Li, Y.-P.; Wang, W.; Leng, X.-M.: A Mission Reliability Method (MRM) for Risk Management in the Development of Materiel System. In: Industrial Engineering and Engineering Management (IE&EM), 2010 IEEE 17Th International Conference on2010, p. 1000–1004

[LI13] Li, F.; Du, X.; Zhang, M.; Phoon, K.: Improved AHP method and its application in risk identification // Improved AHP Method and Its Application in Risk Identification. In: Journal of Construction Engineering and Management 139/2013, Nr. 3, p. 312–320

[LIU05] Liu, S.; Ma, W.; Moore, R.; Ganesan, V.; Nelson, S.: RxNorm. Prescription for electronic drug information exchange. In: IT Professional 7/2005, Nr. 5, p. 17–23

[LIU08] Liu, R.-H.; Zhai, F.-Y.: Model Identification of Risk Management System. In: International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 2008). Dalian, China, 12-14 Oct. 2008. NJ: IEEE Conference, 2008, p. 1–4

[LIU15] Liu, G.; Yokoyama, S.-I.: Proposal for a Quantitative Skill Risk Evaluation Method Using Fault Tree Analysis. In: Engineering Management, IEEE Transactions on 62/2015, Nr. 2, p. 266–279

[LIZI15] Liziński, T.; Wróblewska, A.; Rauba, K.: Application of CVM method in the evaluation of flood control and water and sewage management projects. In: Journal of Water and Land Development 24/2015, Nr. 1, p. 41–49

[LODI10] Lodi, C.; Vasta, A.; Hegbrant, M.; Bosch, J.; Paolini, F.; Garzotto, F.; Ronco, C.: Multidisciplinary evaluation for severity of hazards applied to hemodialysis devices: an original risk analysis method. In: Clinical journal of the American Society of Nephrology: CJASN 5/2010, Nr. 11, p. 2004–2017

[LOGA11] Logan, C.; Nathan, R.; Brown, A.: Formulation in Clinical Risk Assessment and Management. In: Whittington, R.; Logan, C.; Whittington, R. (ed.): Self-Harm and Violence. Towards best practice in managing risk in mental health services. Chichester, UK: John Wiley & Sons, Ltd; Wiley-Blackwell, 2011, p. 187–204

[LYYT98] Lyytinen, K.; Mathiassen, L.; Ropponen, J.; Lyytinen, K.; Mathiassen, L.; Ropponen, J.: Attention Shaping and Software Risk—A Categorical Analysis of Four Classical Risk Management Approaches. In: Information Systems Research 9/1998, Nr. 3, p. 233–255

[MA08] Ma, Y.-S.; Chen, G.; Thimm, G.: Paradigm shift. Unified and associative feature-based concurrent and collaborative engineering. In: Journal of Intelligent Manufacturing 19/2008, Nr. 6, p. 625–641

[MACD03] Macdiarmid, S.; Pharo, H.: Risk analysis: assessment, management and communication. In: Revue scientifique et technique (International Office of Epizootics) 22/2003, Nr. 2, p. 397–408

[MAHE15] Maheshwari, A.: Application of SE in to Regulatory Compliance Activities for Medical Devices. December 21, 2015. – upated: 2015-12-21

[MAIE11] Maier, A.; Mougaard, K.; Howard, T.; McAloone, T. (ed.): Proceedings of the 18th International Conference on Engineering Design (ICED 11), 15 - 18 August 2011. Impacting Society Through Engineering Design. At: 18th International Conference on Engineering Design Copenhagen, 15 - 18 August 2011. København: Design Society; Technical University of Denmark, 2011

[MANG02] Manganelli, S.; Ceci, V.; Vecchiato, W.: Sensitivity analysis of volatility a new tool for risk management. In: Working Paper Series2002, Nr. 194

[MARL14] Marle, F.; Gidel, T.: Assisting project risk management method selection. In: Int. J. of Project Organisation and Management 6/2014, Nr. 3, p. 254

[MART97] Martin, J.: Systems engineering guidebook. A process for developing systems and products. Boca Raton: CRC Press, 1997

[MART99] Martin, F.; Murphy, M.; Stubbs, B.; Uszynski, B.; Hardage, B.; Kendall, R.; Whitney, E.; Weiss, W.; Martin, F.; Uszynski, B.; Kendall, R.; Whitney, E.; Weiss, W.: Reservoir Characterization as a Risk-Reduction Tool at the Nash Draw Pool. In: Spe Reservoir Evaluation & Engineering 2/1999, Nr. 2, p. 169–179

[MATT10] Matthews, S.: Integration & Interoperability:Lessons Learned from ALM and OSLC. URL: http://docplayer.net/41366461-Integration-interoperability-lessons-learned-from-alm-and-oslc.html [Last access: 11.05.2018]

[MCDO03] McDonald, C.; Huff, S.; Suico, J.; Hill, G.; Leavelle, D.; Aller, R.; Forrey, A.; Mercer, K.; DeMoor, G.; Hook, J.; Williams, W.; Case, J.; Maloney, P.: LOINC, a universal standard for identifying laboratory observations: a 5-year update. In: Clinical chemistry 49/2003, Nr. 4, p. 624–633

[MEDT17] MedTech Europe (ed.): The European Medical Technology Industry. - in figures / 2018. 2017

[MEND14] Mendes, E.: Applying a Knowledge Management Technique to Improve Risk Assessment and Effort Estimation of Healthcare Software Projects. In: International Conference on Software Technologies. Reykjavic, Iceland, 29-31 July. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, p. 40–56

[METZ10] Metzroth, K.; Denning, R.; Aldemir, T.: Dynamic event tree analysis as a risk management tool. In: International Congress on Advances in Nuclear Power Plants 2010, ICAPP 2010 2/2010, p. 979–986

[MEYE15] Meyer, A.; Vaquer, G.; Birebent, B.; Gautier, E.; Segier, J.-M.; Gouby, J.; Basch, B.; Khadri, H.; Doucet, J.; Bierling, P.; Rouard, H.: The Failure Mode, Effects and Criticality Analysis (FMECA) Method:. A Useful Approach for Risk Management Plan in Advanced Therapy Medicinal Products Manufacturing. In: Cytotherapy 17/2015, Nr. 6, S11

[MILO10] Milosevic, D.; Wayahuni, F.; Rao, M.; Riddle, J.: Project Risk Management. In: Milosevic, D.; Patanakul, P.; Srivannaboon, S. (ed.): Case Studies in Project, Program, and Organizational Project Management. Hoboken, NJ, USA: John Wiley & Sons, Inc, 2010, p. 229–246

[MIWA12] Miwa, T.; Aoyama, H.; MIWA, T.; AOYAMA, H.: Evaluation Method of Product Development Process with Technology Risk Using Product Worth Flow Analysis. In: Nihon Kikai Gakkai Ronbunshu, C Hen/Transactions of the Japan Society of Mechanical Engineers, Part C 78/2012, Nr. 785, p. 312–326

[NAGY92] Nagy, R.; Ullman, D.; Dietterich, T.: A data representation for collaborative mechanical design. In: Research in Engineering Design 3/1992, Nr. 4, p. 233–242

[NATI19] National Cancer Institute: NCI thesaurus. URL: https://ncit.nci.nih.gov/ncitbrowser/ [Last access: 01.05.2019]

[NIDD14] Nidd, P.; Thorn, T.; Porter, M.: Back to the Future Using Root Cause Analysis as a Proactive Risk Management Tool. In: 2014 10th International Pipeline Conference. Calgary, Alberta, Canada, September 29 - October 3. New York, NY: ASME, 2014

[NIEM07] Niemeyer, K.: A Contribution to Model Theory. In: Kounchev, O. (ed.): Scientific support for the decision making in the security sector. (Series: NATO science for peace and security series. D, Information and communication security, v. 12). Amsterdam, Washington, DC: IOS Press, 2007, p. 25–40

[NO M18] No Magic: MagicDraw. URL: https://www.nomagic.com/products/magicdraw [Last access: 03.05.2018]

[NOBL12] Noble, P.: Applying fault tree analysis (FTA) as a top level risk management tool in software development. In: Pharmaceutical Engineering 32/2012, Nr. 1, p. 1–6

[OEHM10] Oehmen, J.; Ben-Daya, M.; Seering, W.; Al-Salamah, M.: Risk Management in Product Design: Current State, Conceptual Model and Future Research. In: ASME 2010 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference. Montreal, Quebec, Canada, August 15–18, 2010: ASME, 2010, p. 1033–1041

[OMG11a] OMG: Vitech Model-Based Systems Engineering (MBSE) Methodology [Last access: 18.04.2018]

[OMG11b] OMG: OMG Unified Modeling LanguageTM (OMG UML), Superstructure ,formal/2011-08-06. August 2011

[OSTR12a] Ostrom, L.; Wilhelmsen, C.: Vulnerability Analysis Technique. In: Ostrom, L.; Wilhelmsen, C. (ed.): Risk Assessment. Hoboken, NJ, USA: John Wiley & Sons, Inc, 2012, p. 249–276

[OSTR12b] Ostrom, L.; Wilhelmsen, C.: Basic Fault Tree Analysis Technique. In: Ostrom, L.; Wilhelmsen, C. (ed.): Risk Assessment. Hoboken, NJ, USA: John Wiley & Sons, Inc, 2012, p. 203–222

[PADY17] Padyab, A.: Towards More Structured Information Asset Identification Approach for Risk Assessment Methods: Using Genre Based Method. Master Thesis Department of Computer Science, Electrical and Space Engineering, Luleâ University of Technology, Luleâ, 05.06.2017. URL: https://www.essays.se/essay/7ba990ae2c/

[PALA10] Palanichamy, G.: Basic Principles of Risk Management for Medical Device Design. 2010

[PEAR12] Pearce, P.; Hause, M.: ISO-15288, OOSEM and Model-Based Submarine Design. In: SETE APCOSE 2012. Brisbane, May 2012. Canberra: Systems Engineering Society of Australia, 2012

[PERC13] Percival, V.; Horton, B.: Use of a threshold of flystrike risk as a method for treatment intervention in the management of flystrike in sheep. In: Animal Production Science 54/2013, Nr. 3, p. 308–318

[PHAR16] Pharmout: White paper: Medical device risk management using ISO14971. February 2016

[PHIF10] Phifer, M.: SRS Composite Analysis: A Risk Management Tool. EM Waste Processing Technical Exchange 2010,. In: EM Waste Processing Technical Exchange 20102010

[PIHE14] Pihera, D.; Paden, M.: Application of Systems Engineering to Improve ECMO Therapy (Summit on Model Based Systems Engineering in Healthcare). Boston MA, 2014. URL: http://www.omg.org/news/meetings/tc/agendas/ma-14/mbse/Applying_MBSE_to_ECMO_OMG_FINAL.pdf. – upated: 2014 [Last access: 05.05.2018]

[RADE04] Radermacher, K.; Zimolong, A.; Stockheim, M.; Rau, G.: Analysing reliability of surgical planning and navigation systems. In: International Congress Series 1268/2004, p. 824–829

[RAKI06] Rakitin, S.: Coping with Defective Software in Medical Devices. In: Computer 39/2006, Nr. 4, p. 40–45

[RAY06] Ray, S.; Jones, A.: Manufacturing interoperability. In: Journal of Intelligent Manufacturing 17/2006, Nr. 6, p. 681–688

[REDM02a] Redmill, F.: Risk Analysis - a Subjective Process. In: Engineering Management Journal 12/2002, Nr. 2, p. 91–96

[REDM02b] Redmill, F.: Exploring subjectivity in hazard analysis - Engineering Management Journal. In: Engineering Management Journal 12/2002, Nr. 3, p. 139–144

[REIN04] Reinhartz-berger, I.; Dori, D.: Object-Process Methodology (OPM) vs. UML: a Code Generation Perspective. In: Grundspenkis, J.; Kirikova, M. (ed.): CAiSE'04 Workshops in connection with The 16th Conference on Advanced Information Systems Engineering, Riga, Latvia, 7-11 June, 2004, Knowledge and Model Driven Information Systems Engineering for Networked Organisations, Proceedings,: Faculty of Computer Science and Information Technology, Riga Technical, 2004

[REZA07] Rezaie, K.; Amalnik, M.; Gereie, A.; Ostadi, B.; Shakhseniaee, M.: Using extended Monte Carlo simulation method for the improvement of risk management:. Consideration of relationships between uncertainties. In: Applied Mathematics and Computation 190/2007, Nr. 2, p. 1492–1501

[ROQU11] Roques, P.: SysML vs. UML 2: A Detailed Comparison. New Zealand, October, 2011. URL: https://ecs.victoria.ac.nz/foswiki/pub/Events/MODELS2011/Material/MODELS_2011_T2-Roques-SysML_UML2.pdf. – upated: October, 2011 [Last access: 25.04.2019]

[RUIJ16] Ruijter, A. de; Guldenmund, F.: The bowtie method: A review // The bowtie method. Safety Science, 2016 Oct, Vol.88, pp.211-218 // A review. In: Safety Science 88/2016, p. 211–218

[RUMP02] Rumpe, B.: Executable Modeling with UML. A vision or a Nightmare. In: Khosrowpour, M. (ed.): Issues and Trends of Information Technology Management in Contemporary Organizations. 2002 Information Resources Management Association International Conference Seattle Washington USA May 19 - 22 2002. Hershey: Idea Group Publishing, 2002, p. 697–701

[RYAN13] Ryan, P.; Madigan, D.; Stang, P.; Marc Overhage, J.; Racoosin, J.; Hartzema, A.: Response to Comment on ‘Empirical assessment of methods for risk identification in healthcare data’ // Response to comment on 'empirical assessment of methods for risk identification in healthcare data'. In: Statistics in Medicine 32/2013, Nr. 6, p. 1075–1077

[SAJA13] Sajadfar, N.; Xie, Y.; Liu, H.; Ma, Y.-S.: Introduction to Engineering Informatics. In: Ma, Y. (ed.): Semantic Modeling and Interoperability in Product and Process Engineering. A Technology for Engineering Informatics. London: Springer London, 2013, p. 1–29

[SCHL04] Schlitt, M.: Grundlagen und Methoden für Interpretation und Konstruktion von Informationssystemmodellen. Dissertation Fakultät für Wirtschaftsinformatik und Angewandte Informatik, Universität Bamberg, Bamberg, 2004. URL: http://www.ub.uni-bamberg.de/elib/volltexte/2004/9.html

[SCHM11] Schmitt, R.; Zentis, T.: New approach for risk analysis and management in medical engineering. In: Annual Reliability and Maintainability Symposium (RAMS),. Lake Buena Vista, FL, 24-27 Jan. Piscataway, NJ: IEEE, 2011, p. 1–6

[SCHM15] Schmitt, R.; Pfeifer, T.: Qualitätsmanagement. Strategien - Methoden - Techniken. 5th ed. München: Hanser, 2015

[SCHN14] Schneider, S.: Real-World Applications of OMG Technology in Medicine (Model Based Systems Engineering (MBSE) in Healthcare Summit). Boston, MA, 2014. URL: http://www.omg.org/news/meetings/tc/ma-14/special-events/MBSE_Summit-agenda.htm. – upated: 2014 [Last access: 05.05.2018]

[SHAH10] Shahzad, B.; Al-Mudimigh, A.; Ullah, Z.: Statistical methods for sustainable risk identification methodologies. In: Information Management and Engineering (ICIME), 2010 The 2nd IEEE International Conference on2010, p. 523–528

[SHAW90] Shaw, T.: An overview of risk management techniques, methods and application. In: AIAA Space Programs and Technologies Conference. Huntsville, Alabama, September 25-28: American Institute of Aeronautics and Astronautics, 1990

[ŠKEC13] Škec, S.; Štorga, M.; Marjanović, D.: Mapping Risk Analysis Methods on Product Development Process. In: International Conference on Integration of Design, Engineering & Management for Innovation, (IDEMi 2013). Porto, Portugal, 4-6 September 2013: (self-published), 2013

[SMOL11] Smolarkiewicz, M.; Smolarkiewicz, M.; Biedugnis, S.; Podwojci, P.; Czapczuk, A.: Matrix Methods for Risk Management - Associated Matrices Theory. In: Rocznik Ochrona Srodowiska 13/2011, p. 241–252

[SOLH07] Solheim, I.; Stølen, K.: Teknologiforskning – hva er det? as: SINTEF Rapport ,STF90 A06035. Trondheim, March 2007

[SORL09] Sorli, Mikel, Stokic, Dragan: Innovating in Product/Process Development: Gaining Pace in New Product Development. London: Springer London, 2009

[ŠOTI15] Šotić, A.; Rajić, R.: The Review of the Definition of Risk Aleksandar. In: Online Journal of Applied Knowledge Management 3/2015, Nr. 3

[SPAR18] Sparx Systems: Enterprise Architect. URL: https://www.sparxsystems.com/products/mdg/tech/sysml/index.html [Last access: 03.05.2018]

[STAC73] Stachowiak, H.: Allgemeine Modelltheorie. Wien: Springer-Verlag, 1973

[STAM03] Stamatiou, Y.; Skipenes, E.; Henriksen, E.; Stathiakis, N.; Sikianakis, A.; Charalambous, E.; Antonakis, N.; Stølen, K.; Braber, F.; Lund, M.; Papadaki, K.; Valvis, G.: The CORAS approach for model-based risk management applied to a telemedicine service. In: Baud, R. (ed.): The new navigators. From professionals to patients ; proceedings of MIE2003 ; [XVIIIth international conference of the European Federation for Medical Informatics]. (Series: Studies in health technology and informatics, 95). Amsterdam, Toyko: IOS Press; Ohmsha, 2003, p. 206–211

[STEI93] Steinmüller, W.: Informationstechnologie und Gesellschaft. Einführung in die angewandte Informatik. Darmstadt: Wissenschaftliche Buchgesellschaft, 1993

[STEV12] Steven, C.; Chad, G.: A Model-based Reference Architecture for Medical Device Development. In: INCOSE International Symposium 22/2012, Nr. 1, p. 2066–2075

[STRE14] Strelnik, M.: Approving the ISDWIR Method of Risk Measurement in Making Risk Management Decision. In: Revista de métodos cuantitativos para la economía y la empresa 17/2014, p. 42–59

[SU12] Su, X.; Deng, Y.; Mahadevan, S.; Bao, Q.: An improved method for risk evaluation in failure modes and effects analysis of aircraft engine rotor blades. In: Engineering Failure Analysis 26/2012, p. 164–174

[SUHA16] Suhardi, B.; Estianto, A.; Laksono, P.: Analysis of potential work accidents using hazard identification, risk assessment and risk control (HIRARC) method. In: Industrial, Mechanical, Electrical, and Chemical Engineering (ICIMECE), International Conference of2016

[SUPC15] Supciller, A.; Abali, N.: Occupational Health and Safety Within the Scope of Risk Analysis with Fuzzy Proportional Risk Assessment Technique (Fuzzy Prat). In: Quality and Reliability Engineering International 31/2015, Nr. 7, p. 1137–1150

[TCHA02] Tchankova, L.: Risk identification – basic stage in risk management. In: Environmental Management and Health 13/2002, Nr. 3, p. 290–297

[TEFE17] Teferra, M.: ISO 14971-Medical Device Risk Management Standard. In: International Journal of Latest Research in Engineering and Technology (IJLRET) 3/2017, Nr. 3, p. 83–87

[TSYB81] Tsybakov, A.: The method of minimization of the empirical risk in identification problems. In: Automation And Remote Control 42/1981, Nr. 9, p. 1196–1203

[U.S.19] U.S. National Library of Medicine: Medical Subject Headings. URL: https://www.nlm.nih.gov/mesh/meshhome.html [Last access: 01.05.19]

[ULRI76] Ulrich, P.; Hill, W.: Wissenschaftstheoretische Grundlagen der Betriebswirtschaftslehre. In: Wirtschaftswissenschaftliches Studium : Zeitschrift für Ausbildung und Hochschulkontakt 5/1976, 304--309

[ULRI81] Ulrich, H.: Die Betriebswirtschaftslehre als anwendungsorientierte Sozialwissenschaft. In: Geist, M.; Köhler, R. (ed.): Die Führung des Betriebes. Curt Sandig zu seinem 80. Geburtstag gewidmet. Stuttgart: Poeschel, 1981, p. 1–25

[ULRI84] Ulrich, H.; Dyllick, T.; Probst, Gilbert J. B.: Management. (Series: Schriftenreihe Unternehmung und Unternehmungsführung, vol. 13). Bern: Haupt, 1984

[UNGE14] Unger, C.: Current Approaches to System Design and Modelling at GE Healthcare (OMG MBSE and Healthcare Day). June 2014. URL: http://www.omg.org/news/meetings/tc/agendas/ma-14/mbse/Current_Approaches_to_System_Design_and_Modelling_at_GE_Healthcare.pdf. – upated: June 2014 [Last access: 05.05.2018]

[VALÁ15] Valášková, K.; Spuchľáková, E.; Adamko, P.: Non-parametric Bootstrap Method in Risk Management. In: Procedia Economics and Finance 24/2015, p. 701–709

[VAN 96] van der Schaaf, T.: PRISMA: a risk management tool based on incident analysis. International Conference and Workshop on Process Safety Management and

Inherently Safer Processes, 1996, 1996, pp.242-251. In: International Conference And Workshop On Process Safety Management And Inherently Safer Processes, 19961996

[VARA12] Vara, J.; Marcos, E.: A framework for model-driven development of information systems. Technical decisions and lessons learned. In: Journal of Systems and Software 85/2012, Nr. 10, p. 2368–2384

[VDI16] Standard ,VDI 2219 (September 2016). Information technology in product development, Introduction and usage of PDM systems

[WALL11] Walliman, N.: Research methods. The basics. 1st ed. London [u.a.]: Routledge, 2011

[WEDD89] Weddington, W.; Brown, B.; Weddington, W.: Counseling regarding human immunodeficiency virus-antibody testing: An international method of knowledge and risk assessment // Counseling regarding human immunodeficiency virus-antibody testing. An international method of knowledge and risk assessment. In: Journal of Substance Abuse Treatment 6/1989, Nr. 2, p. 77–82

[WEHB14] Wehbe, F.; Hamzeh, F.: Failure mode and effect analysis as a tool for risk management in construction planning. In: International Group for Lean Construction; Annual conference of the International Group for Lean Construction; IGLC (ed.): 21st annual conference of the International Group for Lean Construction 2013. (IGLC 21) ; Fortaleza, Brazil, 29 July - 2 August 2013. Red Hook, NY: Curran, 2014

[WHIT13] White, J.; Carolan-Rees, G.: Current state of medical device nomenclature and taxonomy systems in the UK: spotlight on GMDN and SNOMED CT. In: JRSM short reports 4/2013, Nr. 7, p. 1–7

[WHO03] WHO: Medical Device Regulations. Global overview and guiding principles. 2003

[WILL07] Willis, K.: Trane ECM risk evaluation tool. In: World Energy Engineering Congress (WEEC). Georgia, USA, 15 - 17, August. Lilburn: The Fairmont Press, Inc., 2007, p. 977–981

[WORL10a] World Health Organization: Trends in medical technology and expected impact on public health: Background paper 7 ,WHO/HSS/EHT/DIM/10.7. Geneva, August 2010

[WORL10b] World Health Organization (ed.): Barriers to innovation in the field of medical devices. Background paper 6 ,WHO/HSS/EHT/DIM/10.6. Geneva, August 2010

[WORL10c] World Health Organization; ebrary, Inc (ed.): Medical devices. Managing the mismatch ; An outcome of the priority medical devices project. Geneva, Switzerland: World Health Organization, 2010

[WORL16] World Health Organization, Regional Office for the Eastern Mediterranean: Regulation of medical devices. A step-by-step guide as: Eastern Mediterranean Series ,38. Cairo, Egypt, 2016

[WORL17a] World Health Organization (ed.): Global atlas of medical devices. Geneva, Switzerland: World Health Organization, 2017

[WORL17b] World Health Organization (ed.): WHO Global Model Regulatory Framework for Medical Devices including in vitro diagnostic medical devices. WHO Medical device technical series. Geneva, Switzerland: World Health Organization, 2017

[WORL18] World Health Organization: Classifications. URL: https://www.who.int/classifications/icd/en/ [Last access: 01.05.2019]

[XIUX10] Xiuxu, Z.; Xiaoli, B.: The Application of FMEA method in the risk management of medical device during the lifecycle. In: 2nd International Conference on e-Business and Information System Security (EBISS),. Wuhan, China, 22-23 May. NY: IEEE, 2010, p. 1–4

[YIN18] Yin, R.: Case study research and applications. Design and methods. Los Angeles: SAGE, 2018

[YOO06] Yoo, I.: Semantic Text Mining and its Application in Biomedical Domain. Dissertation College of Information Science and Technology, Drexel University, Philadelphia, PA, 2006

[YU12] Yu, K.; Li, J.; Jia, X.; Li, J.: The equipment supportability risk identification and analysis method. In: Quality, Reliability, Risk, Maintenance, and Safety Engineering (ICQR2MSE), 2012 International Conference on2012, p. 1384–1386

[ZARG13] Zarghami, A.; Vriezekolk, E.; Eslami, M.; van Sinderen, M.; Wieringa, R.: Assumption-based risk identification method (ARM) in dynamic service

provisioning. In: Requirements Engineering Conference (RE), 2013 21st IEEE International2013, p. 175–184

[ZENT11] Zentis, T.: Technisches Risikomanagement in produzierenden Unternehmen. Eine Untersuchung des Fraunhofer-Instituts für Produktionstechnologie IPT und der P3 Ingenieurgesellschaft. 1st ed. Aachen: Apprimus-Verl., 2011

[ZENT12] Zentis, T.; Schmitt, R.: Risk Minimized Procurement in Low Wage Countries. In: 22nd CIRP Design Conference (CIRP Design 2012). Bangalore, India, 28–31 March. London: Springer London, 2012, p. 217–226

[ZENT13] Zentis, T.; Schmitt, R.: Technical Risk Management for an Ensured and Efficient Product Development on the Example of Medical Engineering. In: Abramovici, M.; Stark, R. (ed.): Smart Product Engineering. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, p. 387–398

Student Theses

The present results are partially built on findings obtained within the research team led by the author. The following student theses have contributed to the MBR research project and were elaborated under the guidance of the author:

Belavadi, P.: Data Input and Processing in Model Based Risk Management for Medical Devices. Master Thesis, Faculty of Mathematics, Computer Science and Natural Sciences, RWTH Aachen University, Aachen 2017

Hanschke, M. C.: Factors of influence Impacting the Enforcement of Risk Management in MedTech Companies. Bachelor Thesis, Faculty of Mechanical Engineering, RWTH Aachen University, Aachen 2017

Saad, L. A.: Comparative Studies on Endemic Deficits of Document-Based Risk Management Techniques and their Specific Improvements in Model-Based Risk Management. Bachelor Thesis, Faculty 1, University of Applied Sciences Bremerhaven, Bremerhaven 2018

Nachimuthu, G.: OSLC-Standardized Data Processing of Product Models in Risk Management for Medical Devices. Master Thesis, Faculty of Medicine, Martin Luther University of Halle-Wittenberg, Halle 2019

VII Annex

A Literature Review

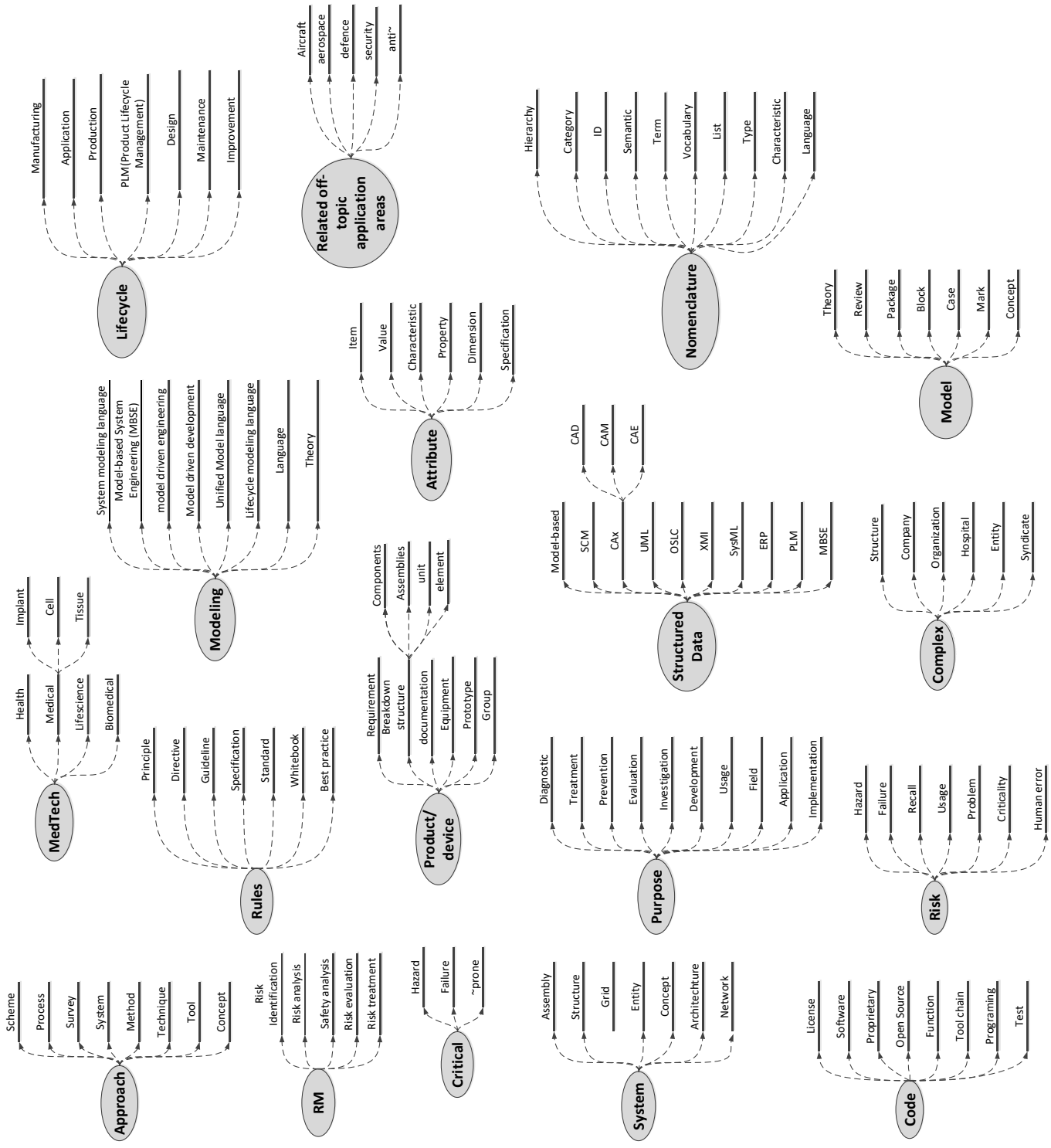


Figure VII.1: Visualization of search terms for the literature review

All literature researches were executed using the search terms from figure VII.1 or a combination thereof. The search terms were queried in groups in all available DBs, the results validated and all positive hits recorded in a group-vs-group matrix. Table VII.1 shows an example crossing the groups [RM] and [Approach] searching for RM methods & techniques. This example is chosen for its simplicity in display; nevertheless, all queries (also crossing more than two groups) followed the same rules. Combinations of search terms from the same group as 'Analysis Evaluation' were used to bring more relevant results to the top. In theory, the hits of any search with this term should build a strict subset of the corresponding searches with 'Analysis' and 'Evaluation'. In real-life literature search engines that run on web protocols and through indexes with tens of millions of publications, the outcome can differ drastically, as the example shows.

Table VII.1: Excerpt from a literature research matrix, here: positive hits for RM methods & techniques from the queries [RM] X [Approach]

Search Terms	Approach	Process	Method	Technique	Tool
Risk Management					
Risk Management			|20| γ	|2| η	
Risk Identification		|1| α	|11| δ		|2| ι
Risk Analysis				|11| θ	
Risk Evaluation					|3| κ
Risk Treatment			|11| ε		|2| λ
Risk Management Analysis		|2| β			|14| μ
Risk Analysis Evaluation			|7| ζ		

Numbers in pipes show the amount of validated positive hits, the Greek letters indicate the references as follows:
α: [BRON16]
β: [LYYT98; VAN 96]
γ: [BAIH09; BRON16; CHEN11; EOM06; FALA11; GARR90; JASE92; KIRO16; LI10a; LI10b; LI13; LIU15; LOGA11; MARL14; MEYE15; PERC13; REZA07; SMOL11; STRE14; VALÁ15]
δ: [BRON16; LI10a; LI13; LIU08; PADY17; RYAN13; SHAH10; SUHA16; TSYB81; YU12; ZARG13]

ε: [AUER90; DÍAZ16; FLEM99; FRAN93; FRIS16; HAO13; HEND08b; LIZI15; LOGA11; PERC13; WEDD89]
ζ: [GUI15; JASE92; JIAN10; LIU15; LODI10; MIWA12; SU12]
η: [MACD03; MEND14]
θ: [BAHI15; CHAP98; CHIC89; ERIC05; HACU01; KREI04; KURT85; LYYT98; SUPC15; OSTR12a; OSTR12b]
ι: [BADR13; DULC91]
κ: [DULC91; MART99; WILL07]
λ: [BADR13; BALZ15]
μ: [CERN15; DRIG15; GAYE94; GUPT16; HEND08a; MANG02; METZ10; MILO10; NIDD14; NOBL12; PHIF10; RUIJ16; VAN 96; WEHB14]

B General Implementation

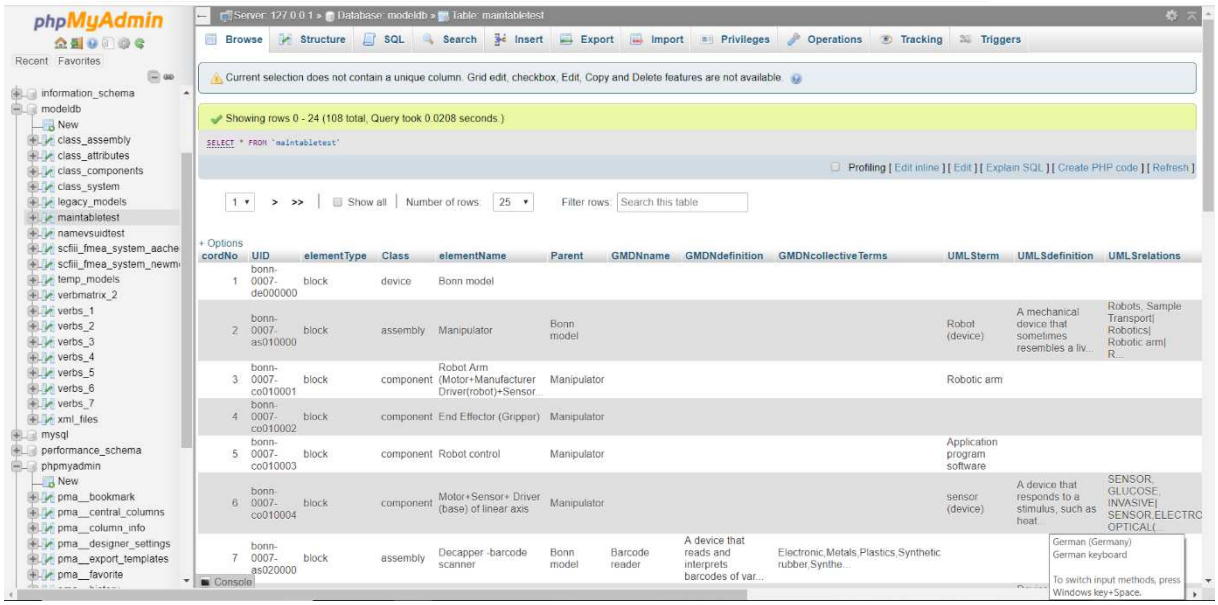


Figure VII.2: Example from a legacy database in the case study, screenshot from phpMyAdmin

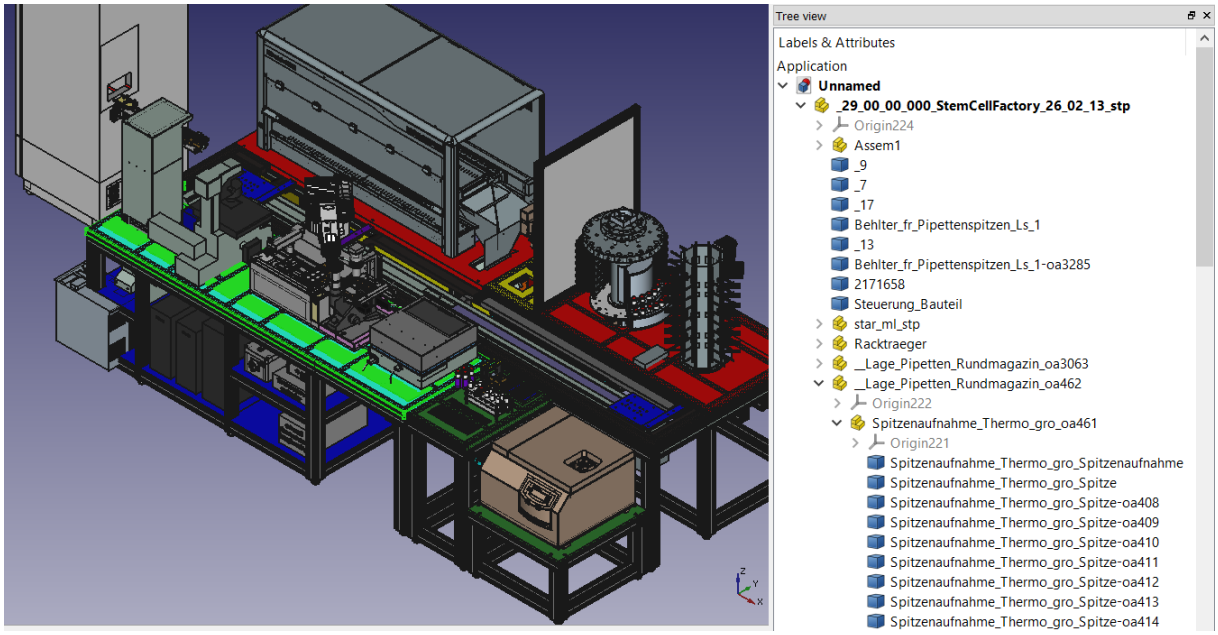


Figure VII.3: 3D model of Bonn Stem Cell Factory device (visualized in FreeCAD)

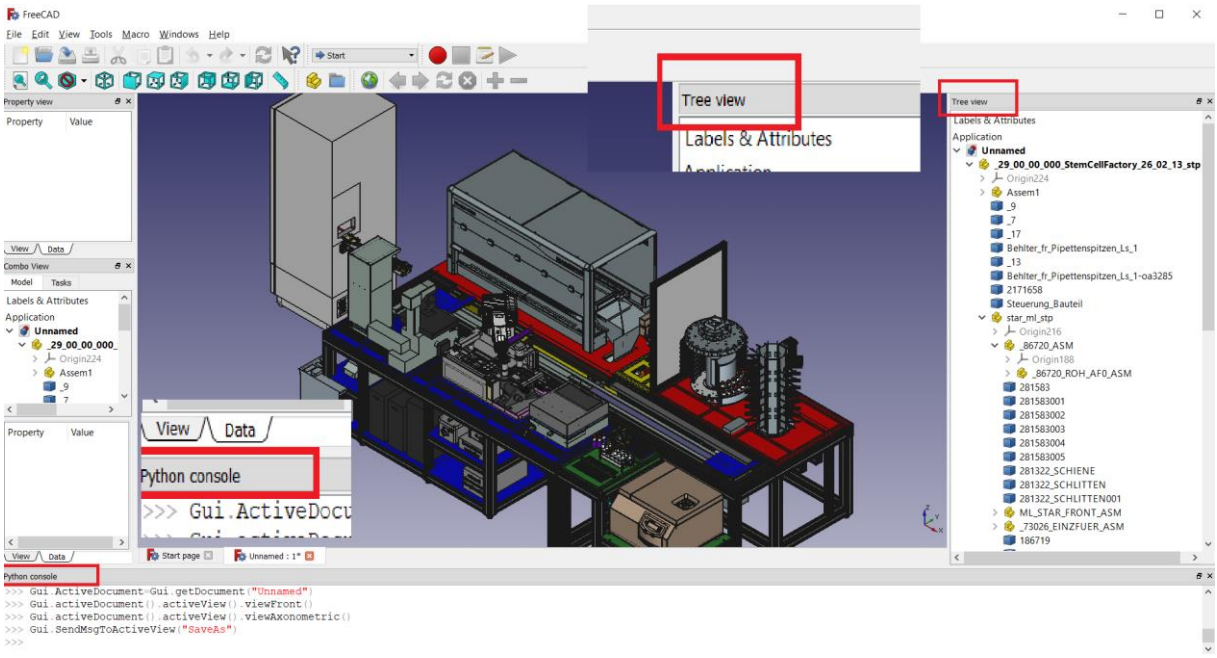


Figure VII.4: FreeCAD representation of the STEP file showing Tree View and Python Console

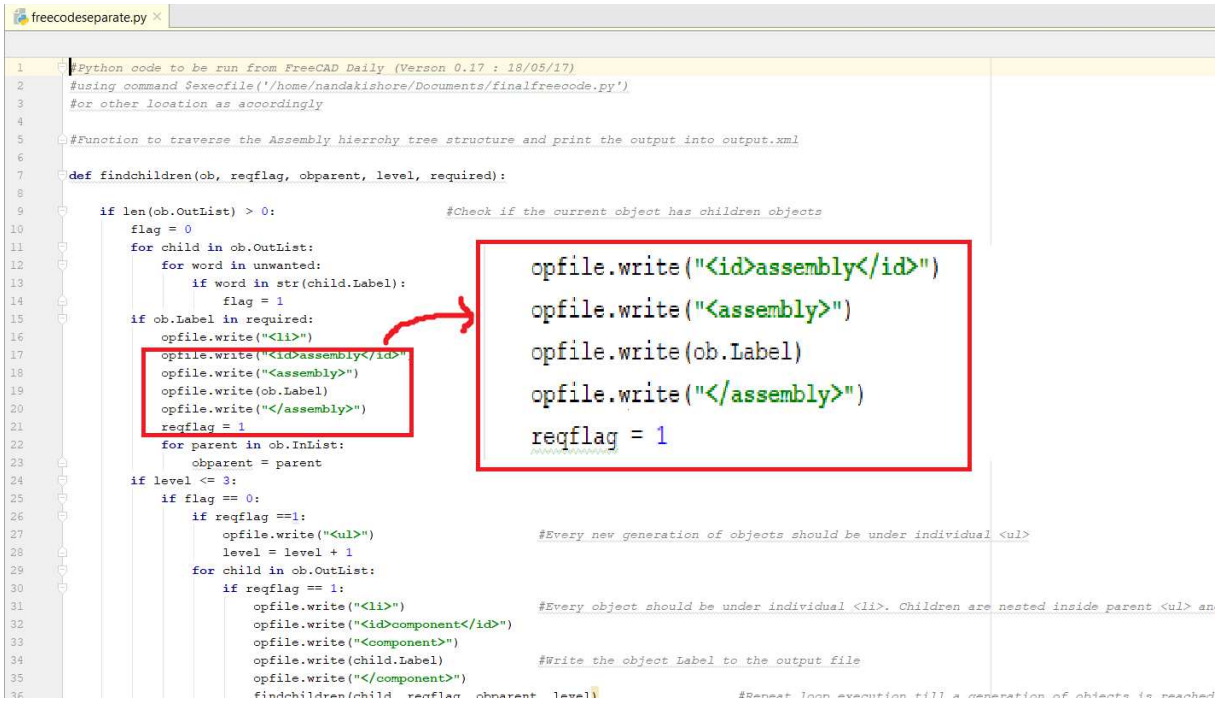


Figure VII.5: Python code used to extract the tree structure to an XML file. It was written and debugged in PyCharm software and executed at the FreeCAD python console. The red rectangle shows how the tree data is written into the file in the standard XML format.

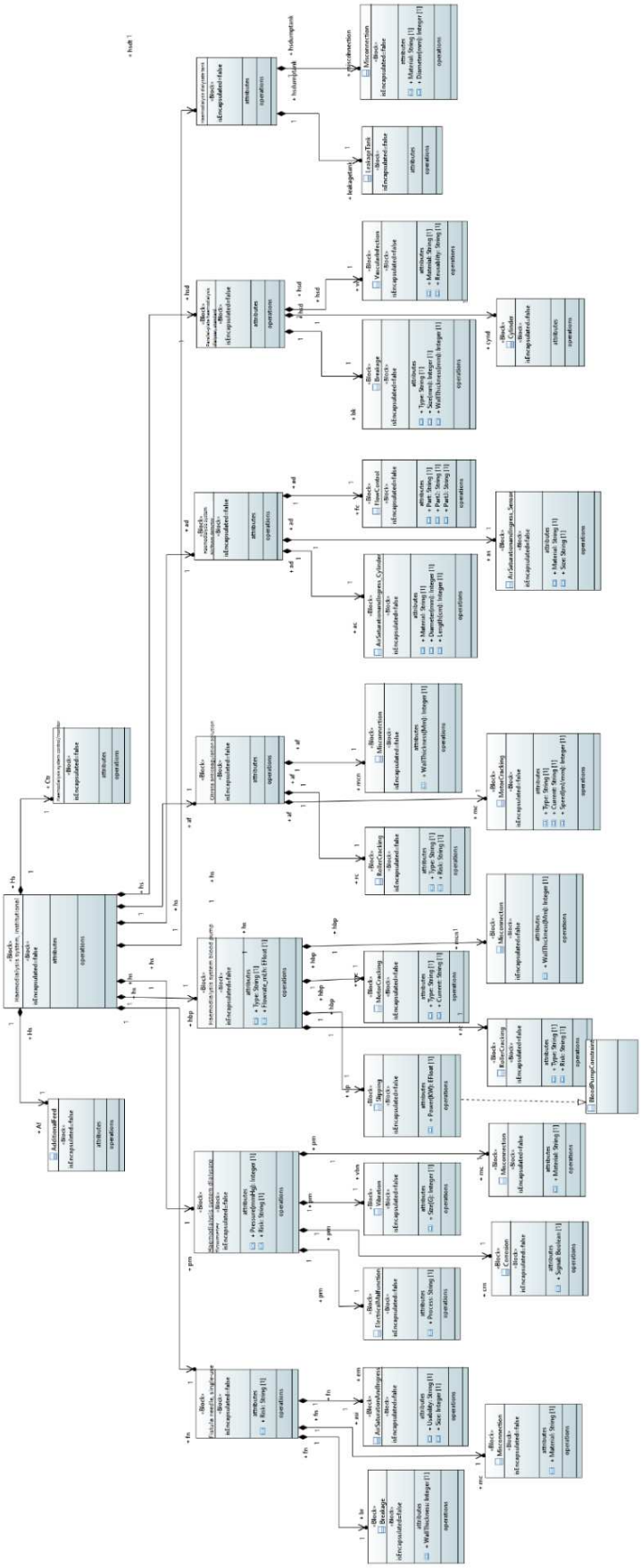
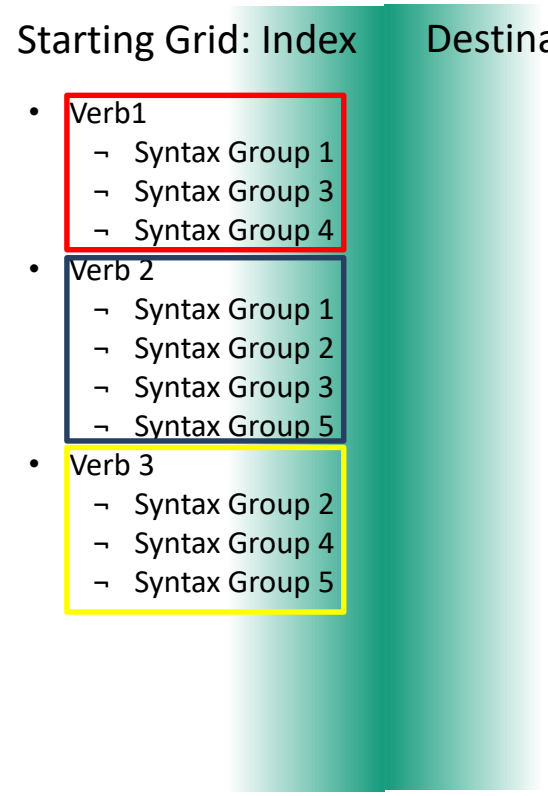


Figure VII.6: Template of the dummy used for testing the functional suitability of modeling platform and tool, based on the PBS in figure 5.4.

Table VII.2: Summary of the software evaluation

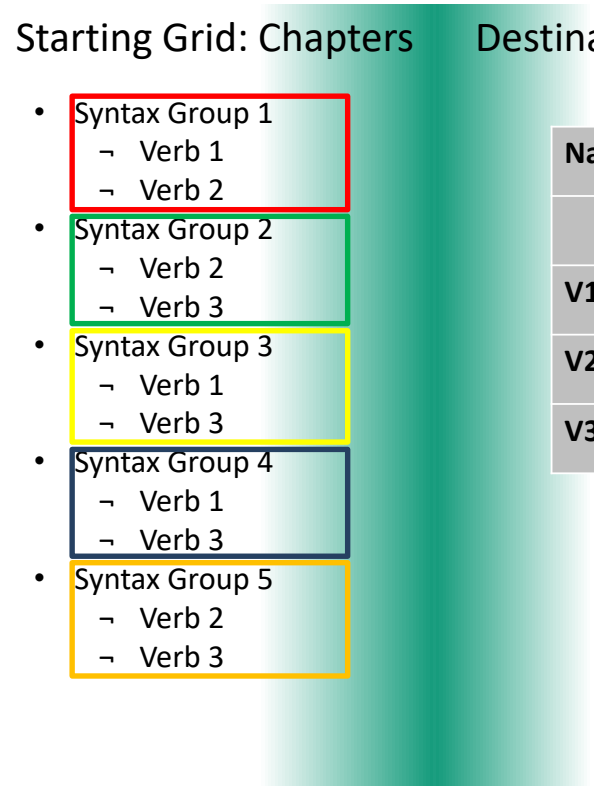
Phase of Analysis	Prototype	Evaluation	Result
Requirement Analysis	Low fidelity – Paper prototype	An understanding of the system description is accomplished Requirements are analyzed	Functional requirements
Functional Analysis	Medium fidelity – PPT mockups	Design of the user interface is analyzed More requirements are gathered	Evaluate user interface
Heuristic Evaluation	High fidelity – Software application	Bugs and errors in the application are identified It is checked whether requirements are met	Evaluation of the system for design errors or other bugs
Think aloud	Final System	Bugs are identified Usability of the system is evaluated	General User feedback
Target group workshop	Final System	Feedback from the experts in the field is gathered Suggestions to improve the system are collected	Target user feedback
Final testing	Final System	System is checked for the compliance with the functional requirements. All the newly implemented software after the previous feedback is also evaluated	

Procedural Steps to Generate a Matrix of Semantic Similarity from Syntax Trees



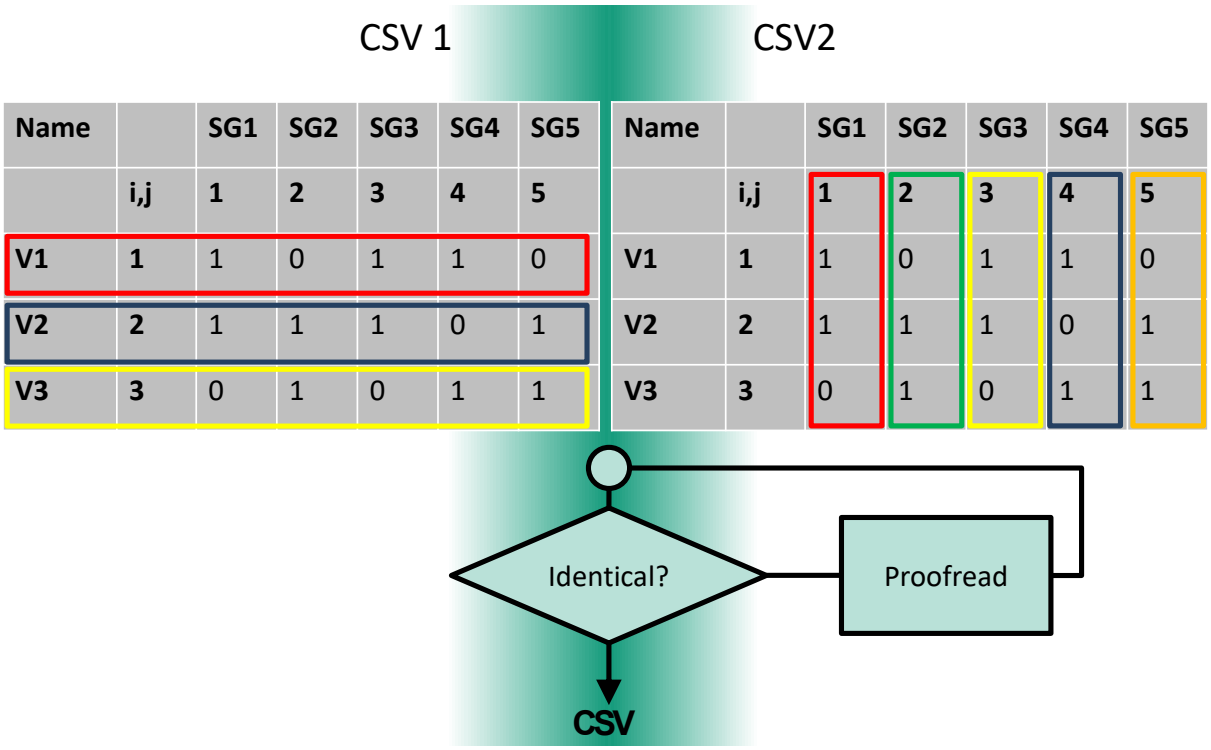
Name		SG1	SG2	SG3	SG4	SG5
	i,j	1	2	3	4	5
V1	1	1	0	1	1	0
V2	2	1	1	1	0	1
V3	3	0	1	0	1	1

Figure VII.7: Semantic verb matrix, step I: transform verb index



Name		SG1	SG2	SG3	SG4	SG5
	i,j	1	2	3	4	5
V1	1	1	0	1	1	0
V2	2	1	1	1	0	1
V3	3	0	1	0	1	1

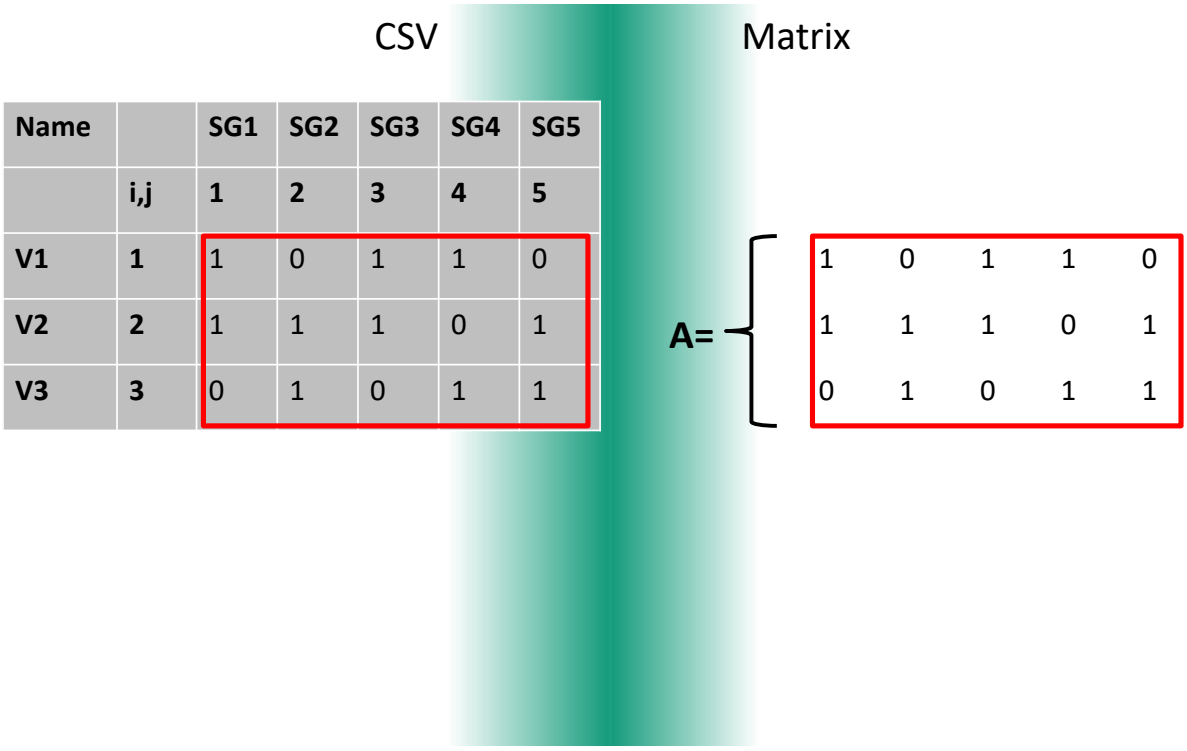
Figure VII.8: Semantic verb matrix, step II: transform verb list



Name		SG1	SG2	SG3	SG4	SG5
	i,j	1	2	3	4	5
V1	1	1	0	1	1	0
V2	2	1	1	1	0	1
V3	3	0	1	0	1	1

Name		SG1	SG2	SG3	SG4	SG5
	i,j	1	2	3	4	5
V1	1	1	0	1	1	0
V2	2	1	1	1	0	1
V3	3	0	1	0	1	1

Figure VII.9: Semantic verb matrix, step III: compare tables



Name		SG1	SG2	SG3	SG4	SG5
	i,j	1	2	3	4	5
V1	1	1	0	1	1	0
V2	2	1	1	1	0	1
V3	3	0	1	0	1	1

1	0	1	1	0
1	1	1	0	1
0	1	0	1	1

Figure VII.10: Semantic verb matrix, step IV: read matrix

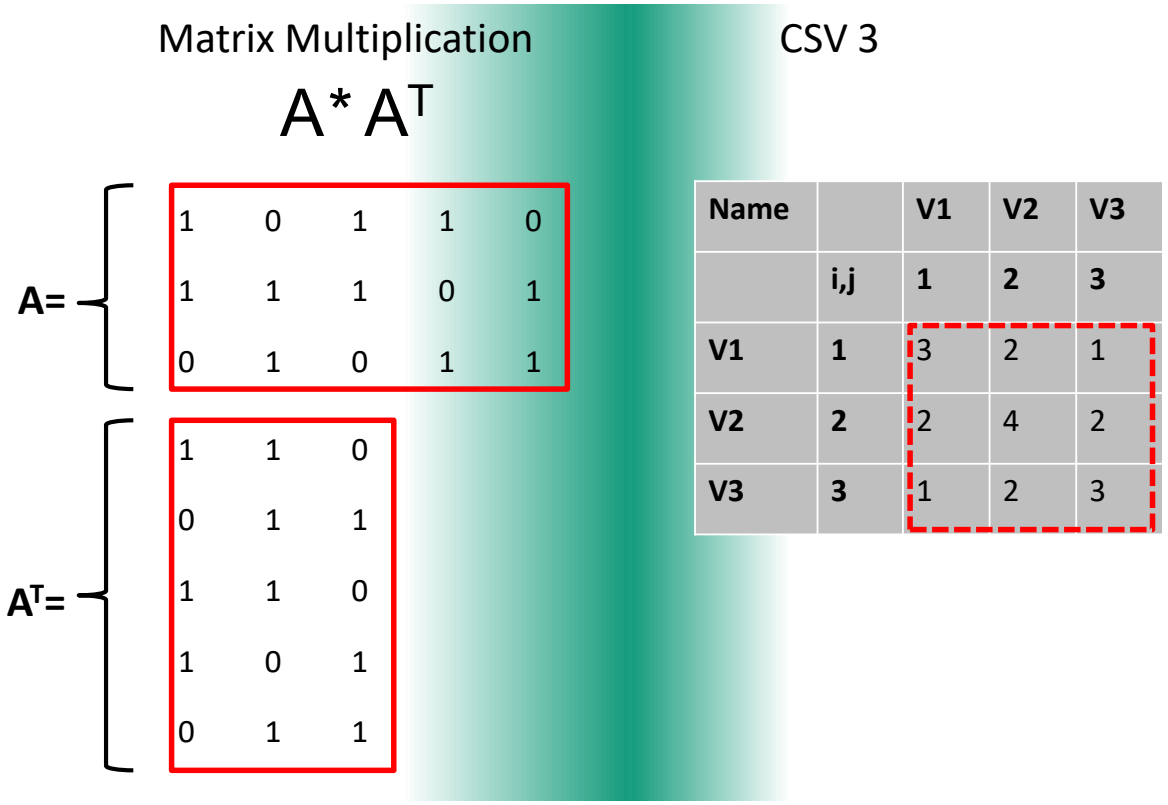


Figure VII.11: Semantic verb matrix, step V: cross matrix

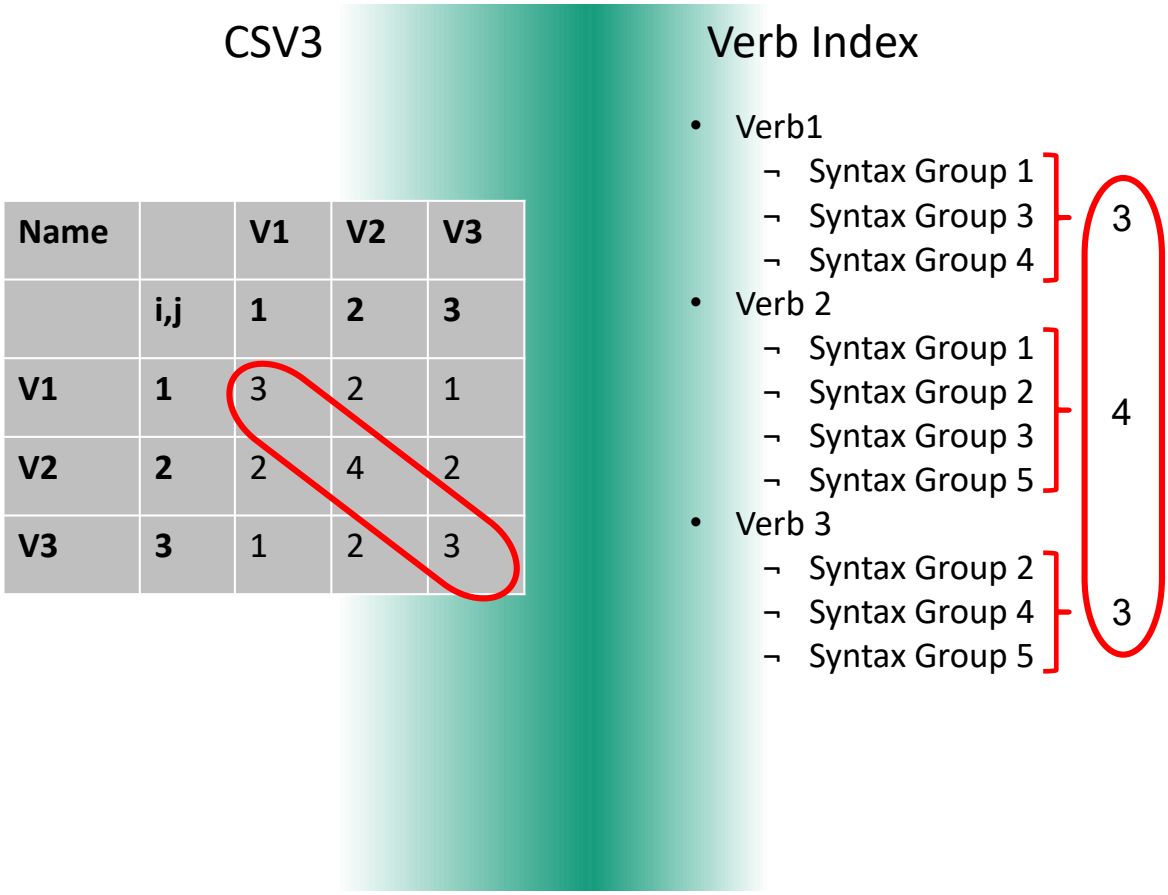


Figure VII.12: Semantic verb matrix, step VI: proofread CSV3

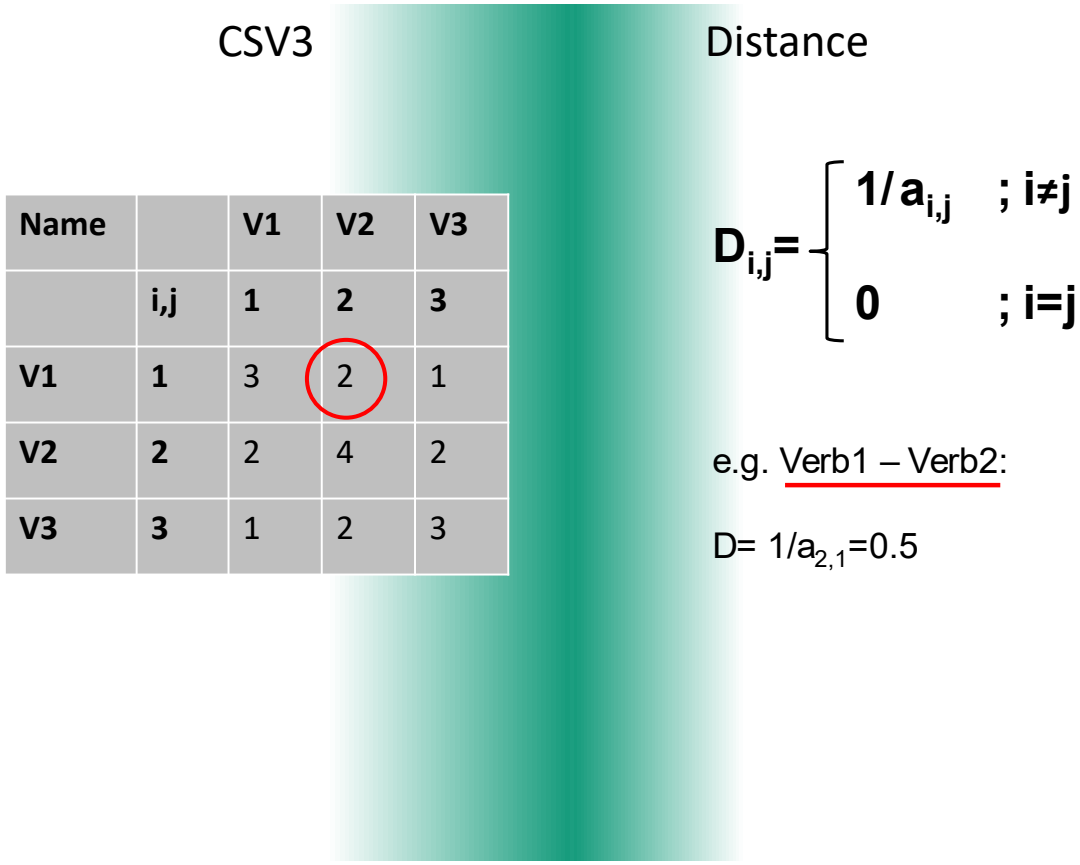


Figure VII.13: Semantic verb matrix, step VII: call $D_{i,j}$ from CSV3

Example of a Search Engine Test

The following section gives an example of a functionality test of the second search engine specification (testing) in 8.1.2.

The search engine, once accessed using the last option in the main menu shown in figure 8.4, takes the user to a model selection page where they can select the legacy model and new model. The legacy model is by default set to a Bonn legacy model but if other models are prepared later as legacy, they can be used as well for this purpose. The user then uploads an XML file for the new model and hits the submit button upon which the App assesses the two files using the comparative search engine and returns the right results.

In the menu seen in figure VII.14, the user can select the legacy and new model XML files to compare.

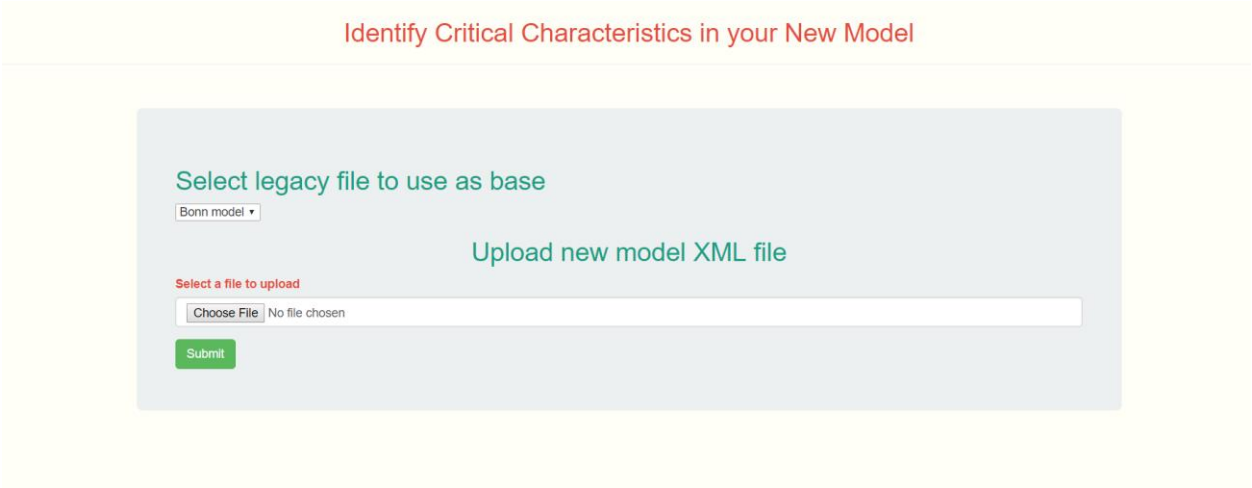


Figure VII.14: First menu in the search engine user interface

As mentioned in the implementation section, each interaction in the Aachen model is examined one by one. For each interaction, the entire legacy model file is read through and points are allocated based on identified similar interactions. If the legacy model has an interaction with the same name, 100 points are added to the score tally for the new model interaction. Having the same verb is a good indicator that the interaction is very similar and could have similar risks. 10 points are added to the tally for every verb in the legacy file that is the same as what we are looking up. The interactions could also be very similar but using a different synonymous verb. To ascertain this, the verb is extracted from the new interaction name and all its synonyms are noted using the verb matrix. The verb matrix also has information on the degree of similarity between verbs as mentioned in the previous sections. For each similar verb identified in the legacy model, twice the verb similarity score is added the tally. Finally, if the interactions have the same parents, that is same agent (actor) and patient (acted upon), then it is an interaction between two similar structural elements in the same directed way and 20 points are added to the tally.

The final result is a ranked list of interactions displayed in descending order of their total risk score, see figure 9.5. This list allows to identify the riskiest interactions in the new model based on comparative analysis with the legacy model and take appropriate mitigation measures.

Whether or not steps are taken to mitigate the identified risks depend on the risk score, components involved and use case. The designer may set a criterion that only identified risks greater than say 50 needs to be addressed in the design phase. This will provide three interactions to reassess in the test example. The riskiest interaction by far in the current example is where the wall sensor informs the housing control unit. If the designer deems this interaction as non-critical in the specific use case, it can be ignored which usually does not happen. The comparative search engine thus gives the designer or a user at any stage of the Product Lifecycle the ability to assess the risks of failure in the device and take appropriate measures to address and mitigate it.

C Panel Results from the Case Study

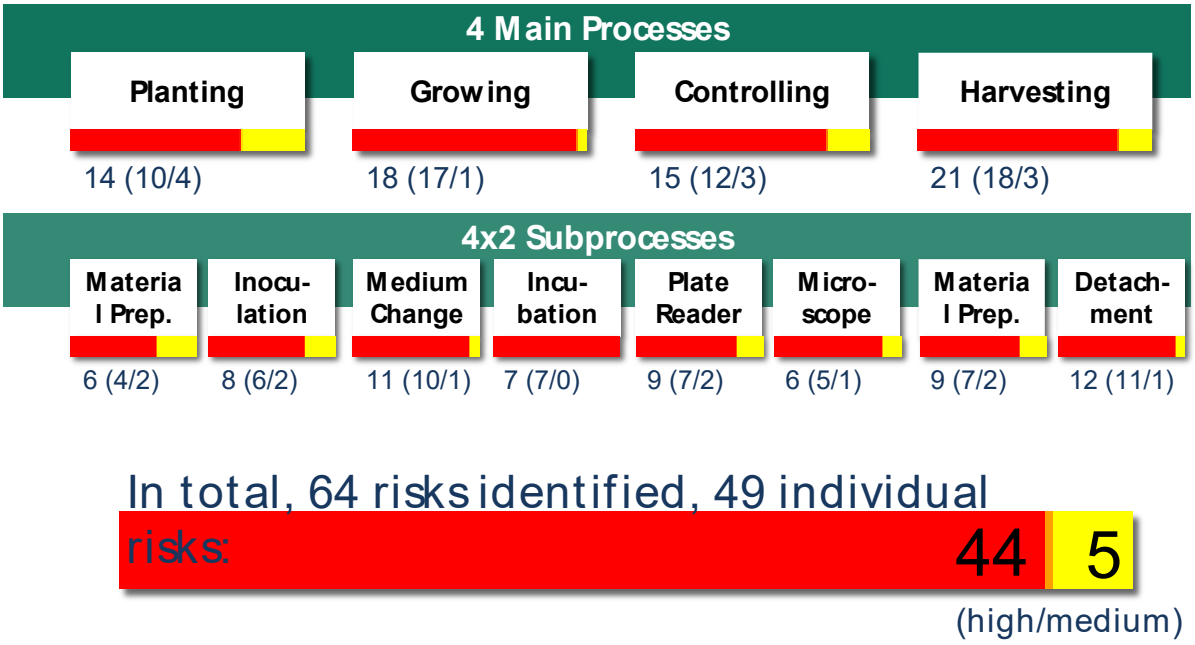


Figure VII.15: Results of the risk assessment for SCFIII, QRC

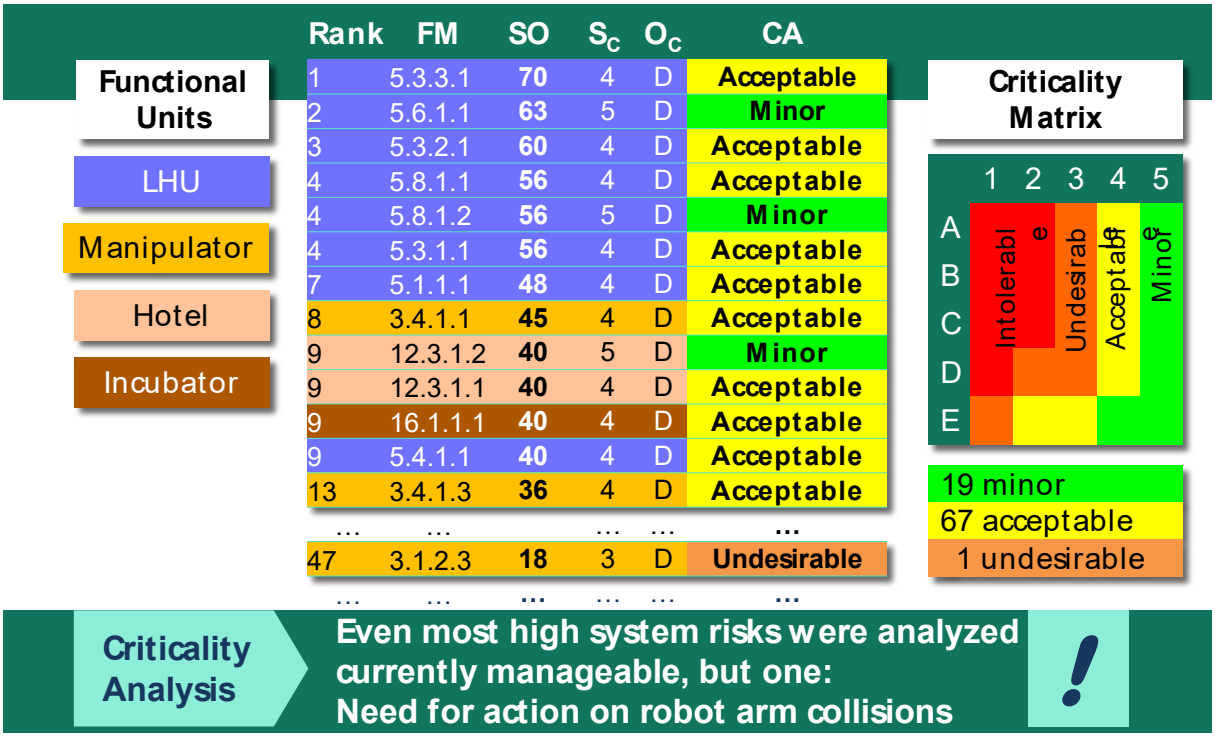


Figure VII.16: Results of the system FMECA for SCFIII

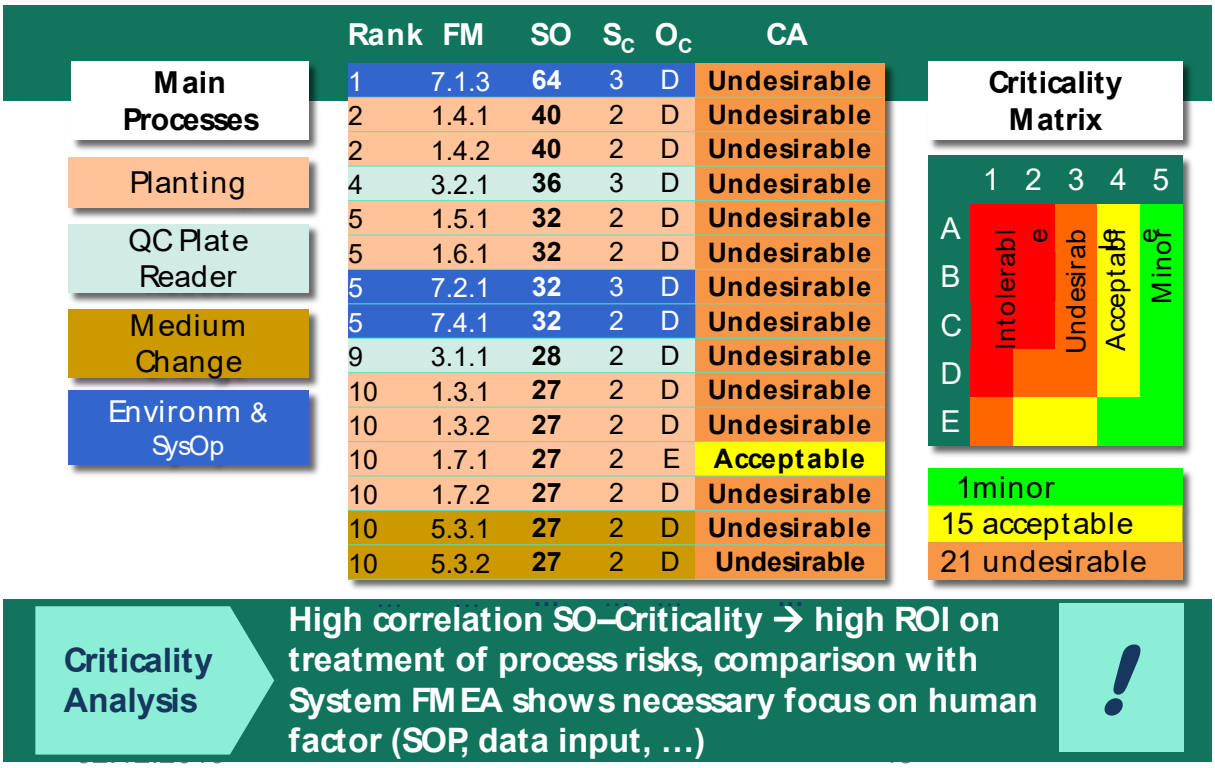


Figure VII.17: Results of the process FMECA for SCFIII

VIII Appendix

A RM Methods and Techniques

Table VIII.1: Comparison of common RM methods and techniques

RM Methods & Techniques	RM Steps	Purpose	Procedure	Field of Application
FMEA [IEC09; MEYE15]	Risk Identification, Risk Analysis and Risk Evaluation	To identify and prioritize potential failures.	The experts analyze each single failure and its resulting effects are documented.	Manufacturing of Medical Products, Auto Manufacturers, Nuclear plants or Aerospace etc.
FTA [IEC09]	Risk Analysis	To identify potential faults, its modes and causes and to quantify their contribution to system unreliability in the course of product design	By constructing Boolean logical gates and create relationship btw components, failures and causes	Aerospace, nuclear power, Process manufacturing, Petrochemical, Pharmaceuticals and other high-hazard industries.
HAZOP [IEC09]	Risk Identification	to identify hazards and operating problems in a process plant	There are 4 steps involved: 1. Definition 2. Preparation 3. Examination 4. Documentation and Follow-up.	Chemical process industry or Pharmaceutical Industries
PHA [IEC09]	Risk Analysis, Assessment and Identification	1. To analyze hazard and risks involved with the handling and transporting of hazardous material 2. To identity opportunities for risk reduction and make recommendations	The experts analyze each single failure and its resulting effects are documented.	Gas supply pipeline power plant

RM Methods & Techniques	RM Steps	Purpose	Procedure	Field of Application
Mission Reliability Method (MRM) [LI10b]	Risk Identification, control and evaluation	To manage the risk in development materiel risk management	With help of both mission reliability block diagram (MRBD) and probabilistic technique, MRM can define the effect of risk events strictly.	Material development material Project ,for example aviation.
Bowtie [IEC09]	Risk evaluation and assessment	To systematically analyze and assess risks	1. Quantitative bowties use a fault tree together with an event tree to calculate risk. 2. Qualitative bowties use simpler cause–effect scenarios with barriers to communicate the risk.	High hazard industries like oil & gas, aviation and mining.
Monte Carlo [IEC09]	Risk Analysis and Assessment	Evaluation of investment projects to analyze and assess risk.	Generates random numbers, calculates the individual components of a project and determines their impact.	IT
Hierarchy Gap Method (HGM) [LI10a]	Risk Identification and risk evaluation	To make out the strategies for risk identification.	HGM transforms the indexes of events into indexes of gap events so system risk can be evaluated efficiently.	Field of Astronautics and Aeronautics.

RM Methods & Techniques	RM Steps	Purpose	Procedure	Field of Application
ETA [IEC09]	Risk Analysis and Assessment	To analyze the risk associated with industrial accident sequences.	1. construct a decision tree that shows accident sequences and defines chronological relationships between initiating and subsequent events. 2. rank the accidents to determine the most important risk.	Nuclear power plants and other hazardous industries.
RCA [IEC09]	Risk Analysis	To improve of quality of care in healthcare .To consider and analyze serious adverse events in a structural manner.	1. Define the problem 2. Gathering data and evidence. 3. identify all the failures. 4. Proper documentation.	Numerous Industries like commercial aviation including Health care.
PRISMA [VAN 96]	Risk Analysis, Risk Monitoring and Prevention	It looks not only at errors but also at recoveries. It provides tools to not only describe and analyze but also give countermeasures.	Consists of sets of tool to monitor and analyze incidents and process. 1. Casual tree incident description method. 2. Eindhoven classification of model system failure. 3. Countermeasures are given.	Originally developed to manage Human error in the chemical process industry. Now applied widely in steel industries, energy Productions and Hospitals.

RM Methods & Techniques	RM Steps	Purpose	Procedure	Field of Application
Delphi Method [IEC09]	Risk Identification	To combine expert opinions on likelihood and expected development time, of the particular technology, in a single indicator.	The experts answer questionnaires in two or more rounds. After every round a document summary is made.	Previously used in weather forecasting. It's now used in topics like automation, space programs, weapons in wars.
HIRARC [SUHA16]	Risk Identification, Risk Assessment and risk control	To analyze potential hazards at workplace.	Analyze risks or hazards using FTA	At any work or occupational place.
Brainstorming [IEC09]	Risk identification	Used in support with other RM methods. Used for high level discussions where issues are identified or at a detailed level for particular problems.	A team of people with knowledge of organizations, system or process being assessed.	Can be implemented at any Engineering sector.
Checklists [IEC09]	Risk identification and analysis	Used to identify hazards and risks or to assess the effectiveness of controls	A check-list is selected which adequately covers the scope.	Numerous industries like aviation or health care.

B Semi-Structured Interview Questionnaire

Interview Questionnaire

Notes for Introduction:

- Fraunhofer IPT, which was founded in 1980 is located in Aachen, working together closely with the WZL of the RWTH Aachen and partners worldwide. In the Project of MBR, we are collaborating with ISCTE IUL in Lisbon
- Carmen E. Castaño Reyes: With Fraunhofer for four years, team lead of the MBR project
- Matthias Hanschke: Student at the RWTH (industrial engineering) and at the Fraunhofer IPT, student responsible for the Study
- Model Based Risk in MedTech is a current project that aims to develop a predesign of the risk along the product lifecycle
- The study support the risk analysis and treatment with insights into preferred treatment option which are used in MedTech today

Consent Form:

Send to participants beforehand, signed by all participants.

!!! Ask participants for audio-recording of the interviews before starting !!!

Guideline questions including follow up questions:

1. **Please give a general description of your current Risk Management process and the respective goals you have by implementing RM. (ISO Part 5+6.1+3)**
    a. Do you have different RM processes for different products?
    b. How often do you have meetings to address RM issues?
    c. For what parts of the Product lifecycle do you use/implement RM?

        - Get overview of current implementation
        - Insights into motivation for RM
        - Check if processes are standardized
        - Responsibility/Structure of RM

2. **How do you initiate a Risk treatment? (ISO Part 6.3+4)**
    a. Do you evaluate the risk of every new product?

b. Do you re-evaluate the risk in cases of complains etc.?
c. How often are you reviewing your RM processes?
d. Who is responsible to address RM issues?
e. How fast are newly identified risks treated?

- Insights into motivation and standing of RM in the company
- Knowledge about triggers of new Risk treatments
- Factors of influence (such as externals, employees, new products…)

3. Explain how you decide whether to treat a risk or not. Is there a fix set of rules for this decision?

a. IF YES, what is this set of rules based on?
b. IF YES, what are typical scenarios when you need to deviate from those rules?
c. IF NO, elaborate on your decision-making procedure, please.
d. Interactions may render it inevitable to exclusively treat only either one of two or more certain risks. How do you decide in such a conflict?
e. Say, instead of concurring risks you have concurring treatments that differ in type of revenue, that is one treatment largely increases that type of cost (man hours, time-to-market, patient wellbeing) the other would litigate and vice versa. How do you decide in such a conflict?

4. Please tell us how you manage the influence of external sources, like other stakeholders, regulations and guidelines, on your decision-making? (ISO Part 6.4+5)

a. Do you follow any specific DIN/ISO standards in your RM processes?
b. IF YES, how detailed do you implement the different parts of the norms?
c. How many different people are involved in the RM decision?
d. How do you incorporate customers in your RM?
e. Do you collect data from past risk treatments? How are you using it?
f. Do you have internal categories to cluster the different risks?

- Overview of involved people and positions in decision making
- Insights into Factors of influence regarding laws/norms
- Possible collection of data to support decision-making from past experiences
- Risk-assessment and rating / internal risk categories to cluster risks

5. **What are the biggest challenges you face in the risk treatment? (ISO Part 6.4+5)**
    a. What methods are you using for RM – decisions? Do you feel you have enough knowledge on the methods?
    b. Would you say that most of the issues date back to deficiencies in risk analysis OR do you see the epicenter somewhere else?
    c. What are typical issues that slow down the decision-making?
    d. Is there (if only sometimes) a point of no return, where you would not convince your peers to stop a treatment already begun?

        - Collection of problems and obstacles
        - Possible communication and standing problems of RM inside the company
        - Recheck of methods and their understanding
        - Collection of first factor of influence (e.g. financial aspects…)
        - Evaluation of RM methods and procedures

6. **How do you communicate treatment measures in your company? (ISO Part 6.2)**
    a. Do you have a communication plan for risk treatment?
    b. Do you feel that communication is happening fast enough?
    c. How fast are you able to get approval and information from different stakeholders?
    d. Do you have regular meetings to control and assess the measures?

        - Check if a communication plan is in place
        - Distribution of responsibility of RM in company
        - Usage+ storage of old RM data for future risk treatment
        - Identify challenges in communication of RM inside the company

7. **How do you evaluate the effectiveness your risk treatment? (ISO Part 6.6+7)**
    a. How do you evaluate if you reached your goals?
    b. Do you conduct empiric control of risk treatment? (Fewer reclamations etc.)

        - Insights into review process of RM methods/procedures
        - Info on implementation of risk treatment
        - Re-check of Goals from question 1

C Selecting a Modeling Language

Table VIII.2: List of graphical modeling languages with their application specifications

Modeling Language	Type	Represent	Application
Behavior Tree	Graphical modeling language	Natural language requirements	Large scale software integrated system
Business Process Modeling Notation	Process modeling language	Business processes	Concepts of modeling applicable to business process
C-K theory	Modeling language for design process	Define design situation	Industrial contexts for design solutions
DRAKON	General purpose algorithmic modeling	Algorithm or family of programing languages	Developing software
EXPRESS and EXPRESS-G	Data modeling language	Define data objects and their relationships	Product data
Extended Enterprise Modeling Language	Business process modeling	Bridge gap between goal modeling and other models	Business enterprise
Flowchart	Diagram	Algorithms	Software development
Fundamental Modeling Concepts	Graphical notation	3 perspectives of a software system	Software intensive systems
IDEF	Family of modeling languages	Functional, object oriented, business process modeling etc.	Software development and business enterprise
Jackson Structured Programming	Structured programming	Data stream and its structure	Software development
LePUS3	Object oriented and visual design description language	Modeling large object oriented programs and design patterns	Software development

Modeling Language	Type	Represent	Application
Object-Role Modeling	Conceptual modeling	Information and rules analysis	Software development
Petri nets	Graphical notation	Model checking, graphical oriented simulation and software verification	Software intensive systems development
Specification and Description Language	Specification language	To depict unambiguous specification and behavior	Reactive and distributed systems
SysML - Systems Modeling Language	Domain specific modeling language	Used in systems engineering	Systems development
Unified Modeling Language	General purpose modeling language	Specify software intense systems	Systems development
Service-oriented modeling framework	Modeling language employed by 'problem domain organization'	Modeling business and software systems	Service oriented business systems
Architecture description language	Software description language	Describe software/systems architecture	Systems development
AADL	Architecture description language	Model software and hardware architecture of embedded/ real-time systems	Systems development

D XML Code Implementation

The following explanations are excerpts from chapter 7 of the master thesis *Data Input and Processing in Model-Based Risk Management for Medical Devices* by Poornima Belavadi and are presented here to help understand the implementation in detail, shall one wish to reproduce the software demonstrator utilized in the case study.

XMI Template Explanation

XMI is recommended use of XML with the intention of providing a standard way for exchanging metadata – information about the set of data and their organization. The intention of XMI is to assist the programmers using UML and its components, to communicate the models with other tools. XMI basically standardizes the description of metadata, that makes the users across the industries look at the data in the same way.

```
<?xml version="1.0" encoding="UTF-8"?>
<xmi:XMI xmi:version="2.1" xmlns:xmi="http://schema.omg.org/spec/XMI/2.1" xmlns:xsi="http://www.w3.org
  <uml:Model xmi:id="_OCzHIDATEeeqWpTJbdqFrA" name="hemodialysissystem">
    <eAnnotations xmi:id="_OCzHITATEeeqWpTJbdqFrA" source="Objing">
      <contents xmi:type="uml:Property" xmi:id="_OCzuMDATEeeqWpTJbdqFrA" name="exporterVersion">
        <defaultValue xmi:type="uml:LiteralString" xmi:id="_OCzuMTATEeeqWpTJbdqFrA" value="3.0.0"/>
      </contents>
    </eAnnotations>
    <packagedElement xmi:type="uml:Class" xmi:id="_OCzuMjATEeeqWpTJbdqFrA" name="HemodialysisSystem">
      <ownedAttribute xmi:id="_OCzuMzATEeeqWpTJbdqFrA" name="av_fistula" visibility="public" type="_OC
    </packagedElement>
    <packagedElement xmi:type="uml:Association" xmi:id="_OCzuNDATEeeqWpTJbdqFrA" memberEnd="_OCzuMzATE
      <ownedEnd xmi:id="_OCzuNTATEeeqWpTJbdqFrA" visibility="public" type="_OCzuMjATEeeqWpTJbdqFrA" as
        <lowerValue xmi:type="uml:LiteralInteger" xmi:id="_OCzuNjATEeeqWpTJbdqFrA"/>
      </ownedEnd>
    </packagedElement>
    <packagedElement xmi:type="uml:Class" xmi:id="_OCzuNzATEeeqWpTJbdqFrA" name="AV_Fistula">
      <ownedAttribute xmi:id="_OCzuODATEeeqWpTJbdqFrA" name="needle" visibility="public" type="_OCzuRD
      <ownedAttribute xmi:id="_OCzuOTATEeeqWpTJbdqFrA" name="pipesandtubes" visibility="public" type="
      <ownedAttribute xmi:id="_OCzuOjATEeeqWpTJbdqFrA" name="dialysatecaps" visibility="public" type="
    </packagedElement>
    <packagedElement xmi:type="uml:Association" xmi:id="_OCzuOzATEeeqWpTJbdqFrA" memberEnd="_OCzuODATE
      <ownedEnd xmi:id="_OCzuPDATEeeqWpTJbdqFrA" visibility="public" type="_OCzuNzATEeeqWpTJbdqFrA" as
        <lowerValue xmi:type="uml:LiteralInteger" xmi:id="_OCzuPTATEeeqWpTJbdqFrA"/>
      </ownedEnd>
    </packagedElement>
    <packagedElement xmi:type="uml:Association" xmi:id="_OCzuPjATEeeqWpTJbdqFrA" memberEnd="_OCzuOTATE
```

Figure VIII.1: Representation of a tree structure using the XMI format

To make it simpler to understand, we have considered the XMI file of the diagram shown in the figure VIII.2. (The diagram is a rough representation of the final SysML block diagram, the standard class names haven't been used here). We explain XMI code showing the relationship between the system and assembly class and then the relationship between the assembly and its component class.

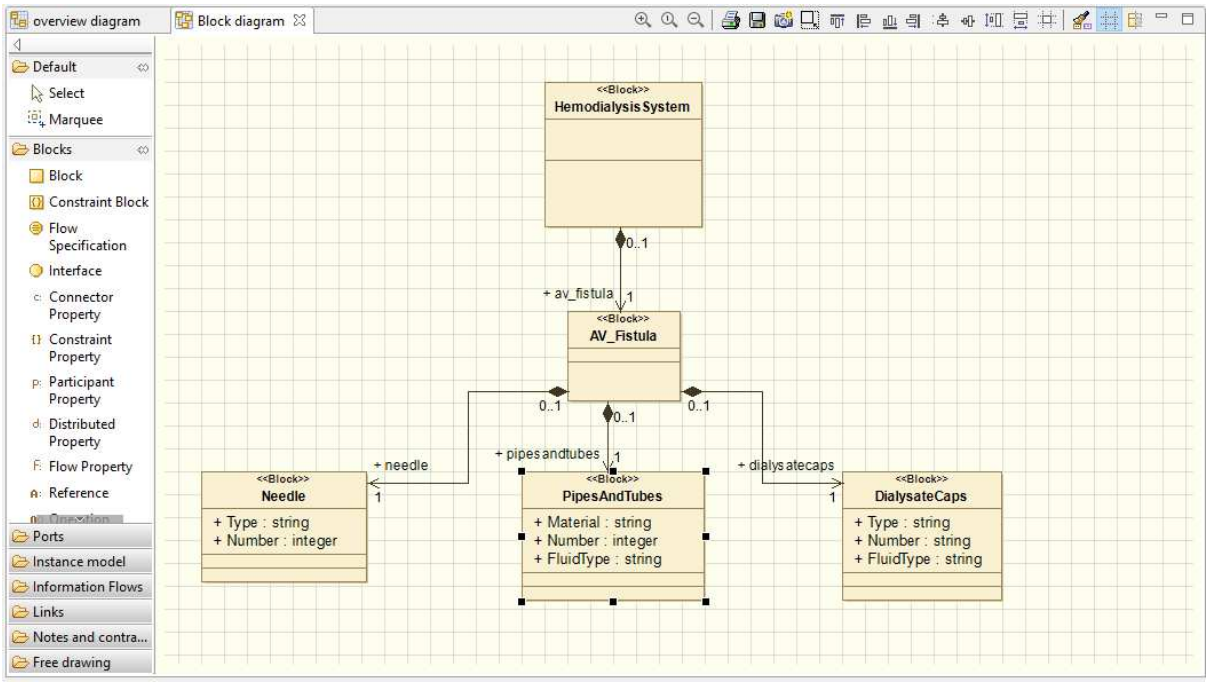


Figure VIII.2: Drawing the block definition diagram.

XML document starts with the XML declaration with the version of XML to which the document confirms.

```
<?xml version="1.0" encoding="UTF-8"?>
```

Snippet VIII.1: XML declaration

In the template the version is 1.0, followed by the encoding type. The name given to the model was “hemodialysissystem”, which is mentioned within the <uml:Model> tag:

```
<uml:Model xmi:id="_OCzHIDATEeeqWpTJbdqFrA" name="hemodialysissystem">
```

Snippet VIII.2: UML tag initializing the model

The first block is the root class, which is the Hemodialysis System. An owned attribute of the Hemodialysis System is ‘AVFistula’ and it forms one assembly class. Each of the assembly classes is related to the parent class ‘hemodialysissystem’ by a composite association, where the association type is handled independent from the pointer, compare figure VIII.3.

The XML code for the template is shown below:

```
<packagedElement xmi:type="uml:Class" xmi:id="_WrmI8DATEeeqWpTJbdqFrA"
name="HemodialysisSystem">
      <ownedAttribute xmi:id="_WrmI8TATEeeqWpTJbdqFrA" name="av_fistula"
      visibility="public" type="_WrmI9TATEeeqWpTJbdqFrA"
      aggregation="composite" association="_WrmI8jATEeeqWpTJbdqFrA"/>
</packagedElement>
```

Snippet VIII.3: An assembly element is initialized beneath its device element

Code Explanation

The class and its attributes are enclosed within the <packagedElement></packagedElement> tags. Each class has a type defining the type of the block, id and a name. The name would be the one given by the user; in this case it is “Hemodialysis System”. The attributes of the class are enclosed within the <ownedAttribute></ownedAttribute> tags within its parent class. Each attribute is defined by xmi:type, xmi:id, name, type, aggregation, association. Out of these, name and aggregation would be user defined. In this case, av_fistula and composite aggregation. The xmi:type and :id defines the type of the property, e.g. ‘uml’ or ‘ecore’, ‘xmi id’ gives the auto generated id for that property element. Type gives the id of the design block. Association gives the id of the association that connects the parent and the child class.

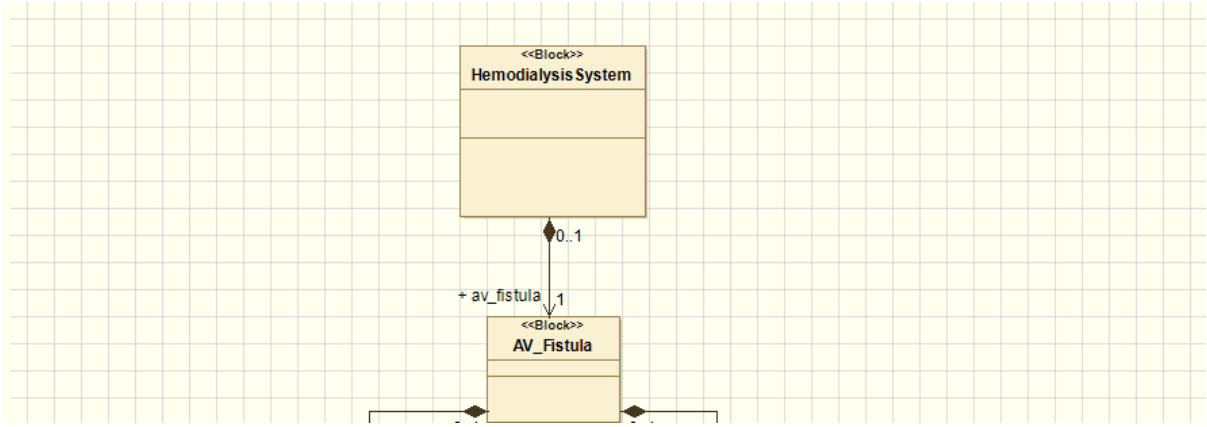


Figure VIII.3: Relationship between the system class and assembly class.

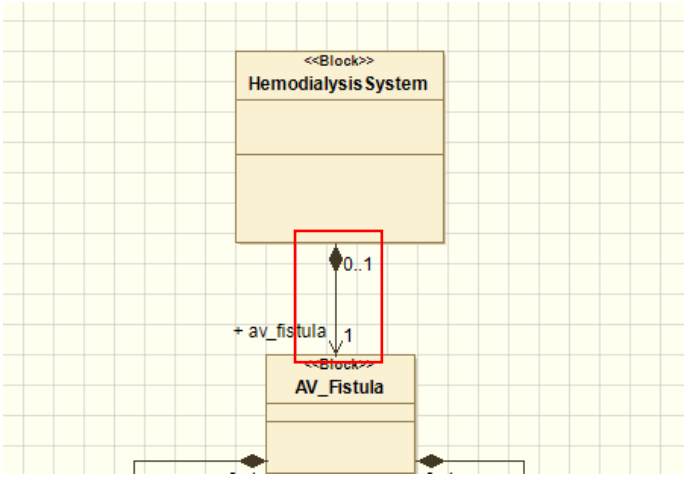


Figure VIII.4: Composition relation between the system class and the assembly class

The line connecting the HemodialysisSystem and the child AV Fistula is the association between the two blocks. In this case it is composition association. This association is represented by the following code block:

```
<packagedElement xmi:type="uml:Association"
xmi:id="_WrmI8jATEeeqWpTJbdqFrA" memberEnd="_WrmI8TATEeeqWpTJbdqFrA
_WrmI8zATEeeqWpTJbdqFrA">
      <ownedEnd xmi:id="_WrmI8zATEeeqWpTJbdqFrA" visibility="public"
      type="_WrmI8DATEeeqWpTJbdqFrA" association="_WrmI8jATEeeqWpTJbdqFrA">
            <lowerValue xmi:type="uml:LiteralInteger"
            xmi:id="_WrmI9DATEeeqWpTJbdqFrA"/>
      </ownedEnd>
</packagedElement>
```

Snippet VIII.4 The actual association between 'hemodialysissystem' and 'AVFistula'

The association is also enclosed in <packagedElement></packagedElement> tags but the XMI type is UML Association. Id will be again auto generated. The owned end of the association refers to the end which has the arrowhead in the diagram.

Important aspect to be noted here is that the two blocks – Hemodialysis System and AV Fistula are connected in the code by their auto generated IDs. This connection between the blocks through their IDs is explained in the end of this section.

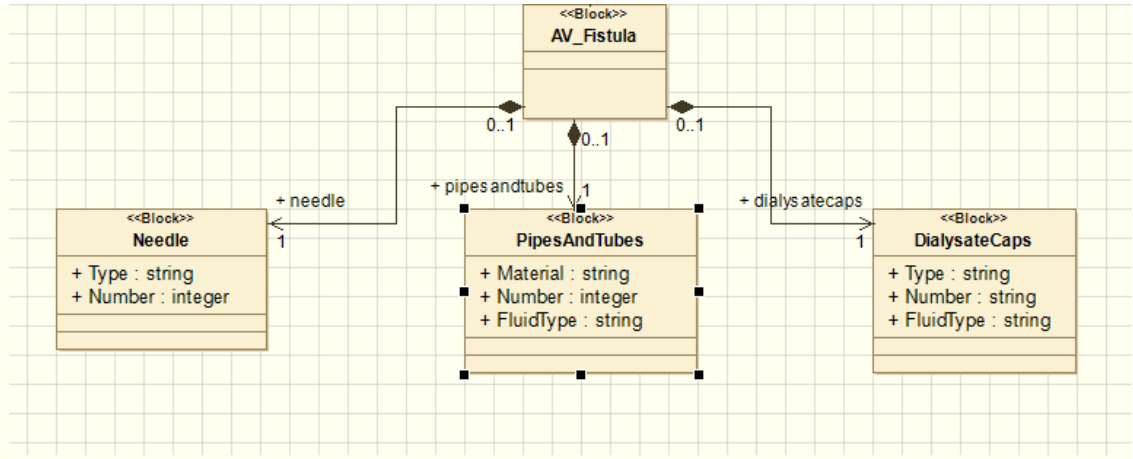


Figure VIII.5 : Relationship between the assembly class and its component classes

The assembly class along with its components is explained here. To avoid redundancy in explanation we have explained just one assembly class and its corresponding component classes. All the remaining classes follow the same pattern.

The assembly class is the AV Fistula class. The component classes that are connected to it are: Needle, PipesAndTubes, DialysateCaps. The association is composite. The following code snippet represents their relationship:

```
<packagedElement xmi:type="uml:Class" xmi:id="_WrmI9TATEeeqWpTJbdqFrA"
name="AV_Fistula">
      <ownedAttribute xmi:id="_WrmI9jATEeeqWpTJbdqFrA" name="needle"
      visibility="public" type="_WrmJAjATEeeqWpTJbdqFrA"
      aggregation="composite" association="_WrmI-TATEeeqWpTJbdqFrA"/>
      <ownedAttribute xmi:id="_WrmI9zATEeeqWpTJbdqFrA" name="pipesandtubes"
      visibility="public" type="_WrmJBjATEeeqWpTJbdqFrA"
      aggregation="composite" association="_WrmI_DATEeeqWpTJbdqFrA"/>
      <ownedAttribute xmi:id="_WrmI-DATEeeqWpTJbdqFrA" name="dialysatecaps"
      visibility="public" type="_WrmJCzATEeeqWpTJbdqFrA"
      aggregation="composite" association="_WrmI_zATEeeqWpTJbdqFrA"/>
</packagedElement>
<packagedElement xmi:type="uml:Association" xmi:id="_WrmI-
TATEeeqWpTJbdqFrA" memberEnd="_WrmI9jATEeeqWpTJbdqFrA _WrmI-
jATEeeqWpTJbdqFrA">
      <ownedEnd xmi:id="_WrmI-jATEeeqWpTJbdqFrA" visibility="public"
      type="_WrmI9TATEeeqWpTJbdqFrA" association="_WrmI-TATEeeqWpTJbdqFrA">
            <lowerValue xmi:type="uml:LiteralInteger" xmi:id="_WrmI-
zATEeeqWpTJbdqFrA"/>
      </ownedEnd>
</packagedElement>
```

Snippet VIII.5: Relationship between component elements and their parent assembly element

The class AV_Fistula is again enclosed within <packagedElement> </packagedElement> tags. All its components form its children class - component class. Each of the component block is defined within the <ownedAttribute></ownedAttribute> tags. Each attribute is defined by xmi type, xmi id, name, type, aggregation, association. Out of these, name and aggregation would be user defined. In this case, needles, pipesandtubes, dialysatecaps and composite aggregation. The xmi type and id defines the type of the property for e.g., uml or ecore, xmi id gives the auto generated id for that property element. Type gives the id of the design block. Association gives the id of the association that connects the parent and the child class.

The first component class for the AV Fistula Class - Needle and its attributes are now defined:

```
<packagedElement xmi:type="uml:Class" xmi:id="_WrmJAjATEeeqWpTJbdqFrA"
name="Needle">
      <ownedComment xmi:id="_WrmJAzATEeeqWpTJbdqFrA">
      <body></body>
      </ownedComment>
      <ownedAttribute xmi:id="_WrmJBDATEeeqWpTJbdqFrA" name="Type"
      visibility="public" isUnique="false">
            <type xmi:type="uml:PrimitiveType"
            href="pathmap://UML_LIBRARIES/UMLPrimitiveTypes.library.
            uml#String"/>
      </ownedAttribute>
      <ownedAttribute xmi:id="_WrmJBTATEeeqWpTJbdqFrA" name="Number"
      visibility="public" isUnique="false">
            <type xmi:type="uml:PrimitiveType"
            href="pathmap://UML_LIBRARIES/UMLPrimitiveTypes.library.
            uml#Integer"/>
      </ownedAttribute>
</packagedElement>
```

Snippet VIII.6: Initializing a component element as UML class

The definition of the component class is like any other class described before. Each class is enclosed in <packagedElement> tag. The user defined attributes are defined within the <ownedAttribute> tag. The associations are defined similarly as explained before between the AV Fistula class and Needle class.

Relationship between Code Blocks and their Connection through IDs

Each code block – the code within the <packagedElement> tag is connected with another through the IDs that are auto generated by the tool, when a block is created. Here we describe these connections in brief, refer the code snippets that are posted above. We use "=" sign to denote that the two IDs are same.

System and Assembly class along with its association.

Assembly class and the first Component class along with its association.

System class here is Hemodialysis System, the Assembly class is the AV Fistula class and Component class is Needle

- ID of System class = type of ownedEnd of the Association.
- ID of ownedAttribute of System Class = first part of memberEnd of Association.
- ID of Association = association of ownedAttribute of SystemClass and association of ownedEnd of Association.
- ID of ownedEnd of Association = second part of memberEnd of Association.
- ID of Assembly class = type of ownedAttribute of System class and type of ownedEnd of Association (Assembly and Component).
- ID of ownedAttribute of Assembly Class = first part of memberEnd of Association (Assembly and Component).
- ID of Component Class = type of ownedAttribute of AssemblyClass.

We make use of this relationship in our API to create the Modelio files. The process of doing that is explained in the next section.

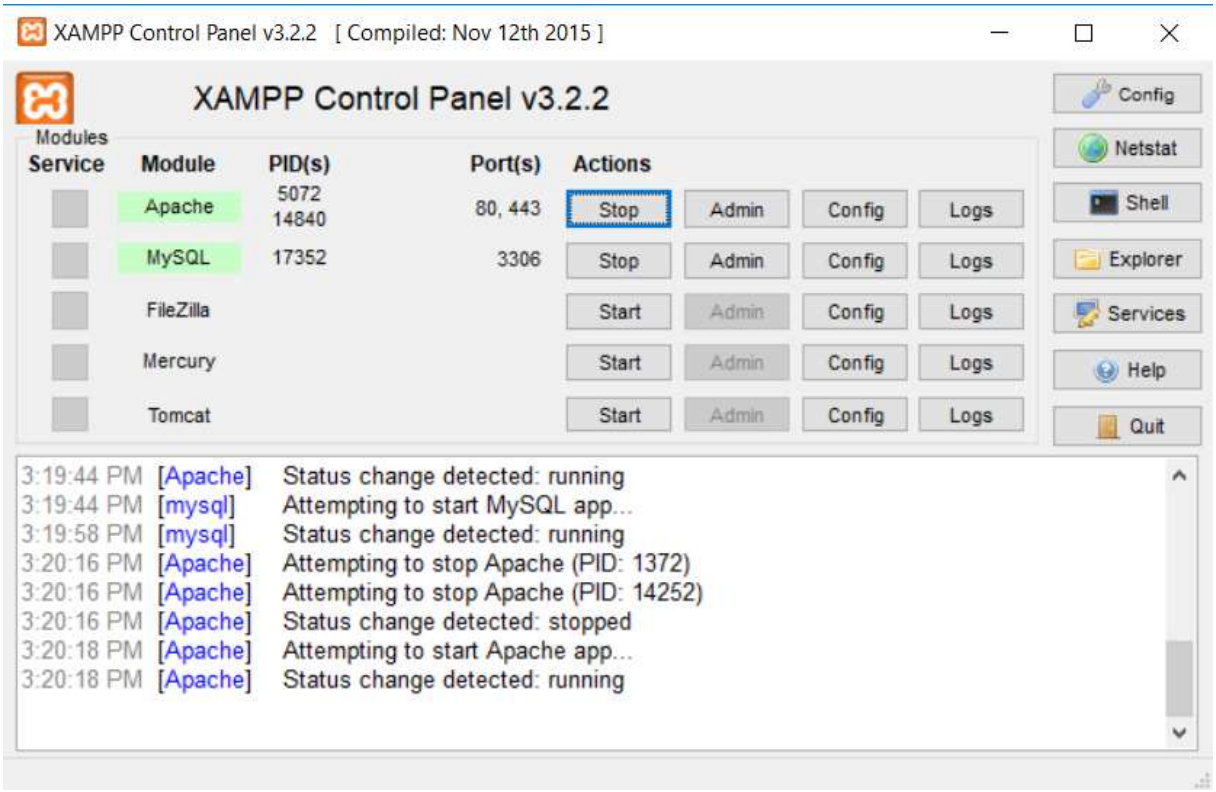


Figure VIII.6: Basic settings in the Apache control panel showing Apache server and MySQL started. Apache is necessary to run the project and access any file in PHPMyAdmin. MySQL is needed to run any SQL query used in various parts of the project.

E Data Selection

The following example is based on the description in chapter 5 of the Master Thesis *OSLC-Standardized Data Processing of Product Models in Risk Management for Medical Devices* by Gowthaam Nachimuthu.

Example: Determining Data Input Destination with the Data Selection Matrix

To better understand the decision if the data is structural/content or none, the reader may consider the datatype ‘geometry and design’. In this example, the information is coming from a CAD model. Almost all the elements inside that source represent structural data. But it also contains information about the dimension of the product and properties of it which is considered content data. Any parts of the underlying STEP file that the data input tool recognizes as belonging to ‘geometry and design’, has already passed as RM-relevant. The number and identity of components in an assembly is architectural information, a group within ‘geometry and design’ and therefore relevant. The hierarchical relation of the components is structural information that will be translated into blocks and associations. Names, sizes and positions are content information which will form part of the blocks’ attributes.

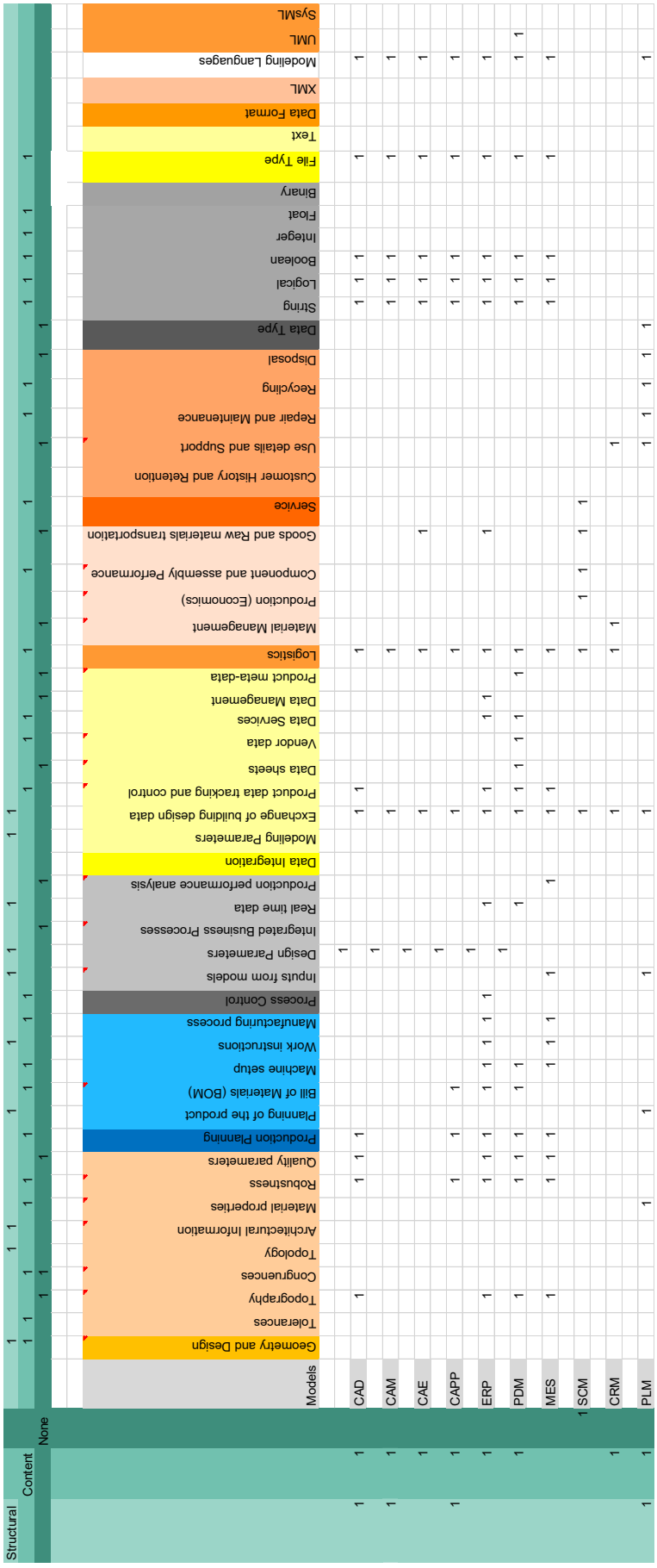


Figure VIII.7: Data selection matrix

F Example of a Questionnaire from the Usability Tests

Feedback form

Questionnaire - During the experiment

User code: _____

The data gathered will only be used for research purposes. We will keep all the information anonymous.

Task 1: Upload a sample file to the database and check if the upload was successful, view the files in the database and download it.

1 The task mentioned was easy to perform

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree

2 Did you experience any discomfort while performing the task?

3 List positive or negative aspect in the system you noticed while performing the task

Task 2: Create a tree structure for different components, view the corresponding class diagram in Modelio OR upload a file to the wizard and view the converted output file in Modelio

1 The task mentioned was easy to perform

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree

2 Did you experience any discomfort while performing the task?

3 List positive or negative aspect in the system you noticed while performing the task

Task 3: Create a class diagram in the Modelio and view its tree structure in the wizard

1 The task mentioned was easy to perform

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree

2 Did you experience any discomfort while performing the task?

3 List positive or negative aspect in the system you noticed while performing the task

4 I like the application overall

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree

Carmen E. Castaño R.

is a lecturer at the Technological University of Panama (UTP). After graduating in Mechanical and Industrial Engineering at UTP and Production Systems Engineering at RWTH Aachen University, she went on to teach at UTP before starting her doctorate in Aachen in 2013, working as a research assistant at the Fraunhofer Institute for Production Technology (IPT).

Her research focuses on improving risk management through systematization and modeling; it is aimed at increasing product safety and sustainability.

ISBN 978-9962-13-825-9