



Lukas Strohmaier, BSc

Unterschiede und daraus resultierende Synergiemöglichkeiten zwischen der Automobil- und Medizingeräteentwicklung

MASTER'S THESIS

to achieve the university degree of

Diplom-Ingenieur

Master's degree programme: Biomedical Engineering

submitted to

Graz University of Technology

Supervisor

Univ.-Prof. Dipl.-Ing. Dr.techn. Christian Baumgartner

Institute of Health Care Engineering

Assoc.Prof. Dipl.-Ing. Dr.techn. Christian Landschützer
Institut für Technische Logistik

Graz, August 2022

EIDESSTATTLICHE ERKLÄRUNG

AFFIDAVIT

Ich erkläre an Eides statt, dass ich die vorliegende Arbeit selbstständig verfasst, andere als die angegebenen Quellen/Hilfsmittel nicht benutzt, und die den benutzten Quellen wörtlich und inhaltlich entnommenen Stellen als solche kenntlich gemacht habe. Das in TUGRAZonline hochgeladene Textdokument ist mit der vorliegenden Masterarbeit/Diplomarbeit/Dissertation identisch.

I declare that I have authored this thesis independently, that I have not used other than the declared sources/resources, and that I have explicitly indicated all material which has been quoted either literally or by content from the sources used. The text document uploaded to TUGRAZonline is identical to the present master's thesis/diploma thesis/doctoral dissertation.

Datum / Date

Unterschrift / Signature

Die Technische Universität Graz übernimmt mit der Betreuung und Bewertung einer Masterarbeit keine Haftung für die erarbeiteten Ergebnisse: Eine positive Bewertung und Anerkennung (Approbation) einer Arbeit bescheinigt nicht notwendigerweise die vollständige Richtigkeit der Ergebnisse.

Danksagung

Zu Beginn möchte ich mich bei meinen beiden Betreuern Univ.-Prof. Baumgartner und Assoc.Prof. Landschützer herzlichst bedanken. Sie haben mich im Vorfeld dieser Arbeit und bei der Themenfindung und -eingrenzung massiv unterstützt und es mir somit ermöglicht, in dieser Arbeit mein berufliches und privates Interesse zu verbinden.

Ein weiterer großer Dank gilt der Firma Tyromotion GmbH, im Speziellen Herrn Alexander K. und Armin H.. Ich habe in diversen Meetings beziehungsweise bei einem Besuch in ihrer Grazer Wirkungsstätte einen beeindruckenden Einblick in die Entwicklung und Produktion ihrer Rehabilitationstechnik bekommen.

Der größte Dank gebührt einerseits meinen Eltern und meinem Bruder, die mir nicht nur dieses Studium ermöglichten, sondern mich auch jeden Tag darin bestärkten und mich selbst in den schwierigsten Stunden dazu ermutigten, mein Ziel nicht aus den Augen zu verlieren.

Andererseits danke ich meiner besseren Hälfte Stephanie, die mich durch ihre selbstlose Art in allen Belangen unterstützte und für mich auch in den stürmischsten Momenten der rettende Anker war. Des weiteren möchte ich unsere treue Wegbegleiterin Suki erwähnen, die durch einen Blick Gewitterwolken in Sonnenschein verwandeln kann.

Zuletzt möchte ich einen speziellen Dank an meinen Freund Lukas aussprechen, der mich in unzähligen Fragen unterstützt hat und der immer für mich da ist.

Danke für eure Unterstützung - ohne euch wäre ich nicht dort, wo ich jetzt bin.

Zusammenfassung

Unterschiede und daraus resultierende Synergiemöglichkeiten zwischen der Automobil- und Medizingeräteentwicklung

Durch den immer schnelleren Fortschritt in der Wissenschaft und Technik ist es nötig, über den eigenen branchenspezifischen Tellerrand zu blicken und etwaige Unterschiede in einzelnen Entwicklungsaspekten beziehungsweise -herangehensweisen zu entdecken. Diese Unterschiede müssen je nach Gebiet bewertet und können falls möglich, in die eigene Branche übertragen werden. Dadurch können selbst völlig verschiedene Bereiche, wie die der Medizin- beziehungsweise Automobiltechnik, von einander profitieren. Dies steigert die Qualität eines Produktes und senkt den eigenen Entwicklungsbedarf und somit die entstehenden Kosten.

-Entwicklungsunterschiede -Synergiemöglichkeiten -Transferinnovation -Änderungen
-Funktionale Sicherheit

Abstract

Differences and resulting synergy opportunities between automotive and medical device development

Due to the ever faster progress in science and technology, it is necessary to look beyond one's own industry-specific horizon and explore possible differences in individual developmental aspects or approaches. These differences have to be evaluated depending on the field and can be transferred to one's own industry if possible. As a consequence, even completely different industries, such as medical or automotive engineering, can benefit from each other. This can increase the quality of a product and consequently reduces developmental needs and incurred costs.

-Differences in development -Synergy opportunities -Transfer innovation -Changes
-Functional safety

Inhaltsverzeichnis

| | | |
|----------|--|-----------|
| 1 | Einleitung | 1 |
| 1.1 | Definitionen | 1 |
| 1.2 | Produktlebenszyklus | 1 |
| 1.2.1 | Produktentstehungsprozess / Beginning of life | 2 |
| 1.2.1.1 | Entwicklungs- und Konstruktionsphase | 3 |
| 1.2.1.2 | Vorgehensmodelle | 6 |
| 1.2.2 | Technische Änderungen | 17 |
| 1.2.2.1 | Eigenschaften einer technischen Änderung | 18 |
| 1.2.2.2 | Auswirkungen von Änderungen | 21 |
| 1.2.2.3 | Änderungsmanagement | 23 |
| 1.3 | Transferinnovation | 27 |
| 1.3.1 | Cross-Industry-Innovation | 28 |
| 1.4 | Eingrenzung der Branche | 30 |
| 2 | Aufgabenstellung | 31 |
| 3 | Methoden | 32 |
| 4 | Ergebnisse | 33 |
| 4.1 | Forderung des Einsatzes von Analysen | 33 |
| 4.2 | Modell der funktionalen Sicherheit im Kraftfahrzeug | 35 |
| 4.2.1 | Unterschiede in der Klassifizierung | 37 |
| 4.2.2 | Verwendung des W-Modells | 41 |
| 4.2.3 | Möglichkeit zur Dekomposition | 43 |
| 4.2.4 | Hardware-Metriken | 44 |
| 4.3 | Überwachung nach dem Inverkehrbringen | 47 |
| 5 | Diskussion | 51 |
| 5.1 | Einsatz von Analysen | 51 |
| 5.1.1 | Vorteile des frühen Einsatzes einer Analyse | 51 |
| 5.1.2 | Nachteile einer FMEA | 53 |
| 5.2 | Aspekte der funktionalen Sicherheit | 54 |
| 5.2.1 | Die funktionale Sicherheit bei Einsatz von agilen Methoden | 54 |

| | | |
|----------|---|-----------|
| 5.2.2 | Einheitliche Klassifizierung und deren Auswirkung | 55 |
| 5.2.3 | Dekomposition | 57 |
| 5.2.4 | W-Modell | 58 |
| 5.2.5 | Metriken der Hardware | 59 |
| 5.3 | Gesetzlich geforderte Marktüberwachung | 60 |
| 6 | Schlussfolgerung | 63 |

Abbildungsverzeichnis

| | | |
|----|---|----|
| 1 | Produktlebenszyklus | 2 |
| 2 | Produktentstehungsprozess | 3 |
| 3 | Phasen der Entwicklung | 4 |
| 4 | Stacey-Matrix | 6 |
| 5 | Vorgehensmodelle in der Stacey-Matrix | 7 |
| 6 | Charakterisierung der klassischen Herangehensweise | 8 |
| 7 | Fünfstufiges Wasserfallmodell | 8 |
| 8 | V-Modell | 10 |
| 9 | Charakterisierung der agilen Herangehensweise | 13 |
| 10 | Kanban-Board | 14 |
| 11 | Scrum | 15 |
| 12 | Product-Backlock vs. Sprint-Backlock in Scrum | 17 |
| 13 | Externe und interne Ursachen einer Änderung | 20 |
| 14 | Produktarchitektur | 22 |
| 15 | Zehnerregel | 25 |
| 16 | Zyklus des Änderungsmanagement | 26 |
| 17 | Möglichkeiten der Transferinnovation | 28 |
| 18 | Schraubendreher WORX & Go mit Revolverdesign | 29 |
| 19 | Mechatronik | 30 |
| 20 | Branchenspezifische Ableitungen der IEC 61508 | 36 |
| 21 | Bestandteile eines Systems | 36 |
| 22 | Ablaufdiagramm der Klassifizierung von Medizinprodukten | 37 |
| 23 | ASIL-Klassen abhängige Risikoreduktion | 40 |
| 24 | In ISO 26262 dargestelltes W-Modell | 42 |
| 25 | Aufteilung der Anforderungen im W-Modell | 42 |
| 26 | Beispiel zur Aufteilung eines Sicherheitszieles in funktionale und technische Sicherheitsanforderungen | 43 |
| 27 | Möglichkeiten zur Dekomposition von Sicherheitsklassen der ISO 26262 . . | 44 |
| 28 | Geforderte Formen der Überwachung von Medizingeräten | 47 |
| 29 | Ablaufdiagramm der Post-Market Surveillance | 48 |
| 30 | Einfluss der FMEA auf den Entdeckungszeitpunkt eines Fehlers | 52 |
| 31 | Klassifizierung von Medizintechnik anhand der ASIL-Stufen | 56 |

| | | |
|----|---|----|
| 32 | Mögliche Dekomposition der MedSIL-Klassen | 57 |
|----|---|----|

Tabellenverzeichnis

| | | |
|---|--|----|
| 1 | Vergleich der verwendeten QM-Normen beider Branchen | 35 |
| 2 | Risiko- beziehungsweise Sicherheitsklassen in der Medizintechnik | 38 |
| 3 | ASIL-Stufen | 39 |
| 4 | Nach ISO 26262:2018 empfohlene Analysen der Systemarchitektur | 41 |
| 5 | Beispielswerte für die Ausfallrate und deren Wahrscheinlichkeit eines $1k\Omega$ Widerstandes | 46 |
| 6 | Zielwerte der Hardware-Metrik in der ISO 26262 | 46 |
| 7 | Mögliche Zielwerte der HW-Metriken der MedSIL-Klassen | 59 |

Abkürzungsverzeichnis

| | |
|---------|---|
| % | Prozent |
| § | Paragraph |
| Abs. | Absatz |
| ASIL | Automotive Safety Integrity Level |
| DFA | Dependent Failure Analysis |
| DIN | Deutsche Industrienorm |
| EN | Europäische Norm |
| EUDAMED | Europäische Datenbank für Medizinprodukte |
| FMEA | Failure mode and effects analysis (Fehlermöglichkeits- und -einflussanalyse) |
| FMEDA | Failure modes, effects, and diagnostic analysis (Fehlermöglichkeits-, -einfluss- und -diagnoseanalyse) |
| FTA | Fault Tree Analysis (Fehlerbaumanalyse) |
| HARA | Hazard Analysis and Risk Assessment |
| IEC | International Electrotechnical Commission |
| ISO | International Organization for Standardization |
| IVDR | In-vitro-Diagnostic Device Regulation |
| KFZ | Kraftfahrzeug |
| MDR | Medical Device Regulation |
| PDCA | Plan, Do, Check, Act |
| PMS | Post-Market Surveillance |
| QM | Qualitätsmanagement |
| VDA | Verband der Automobilindustrie |

1 Einleitung

1.1 Definitionen

Bevor man sich mit dem Entwicklungsprozess von der Idee bis zu einem serienreifen Produkt und den daraus resultierenden einzelnen Prozessschritten beschäftigt, bedarf es einer grundsätzlichen Erklärung der wichtigsten Begriffe.

Zur marktreifen Entwicklung eines Produktes ist es branchenunabhängig nötig, klar definierte Arbeitsabläufe oder Prozesse zu implementieren. Wie im Gabler Wirtschaftslexikon angeführt, wird ein Prozess als „[...] die Gesamtheit aufeinander einwirkender Vorgänge innerhalb eines Systems“[1] verstanden. Auf den Produktentwicklungsprozess konkretisiert bedeutet dies das Zusammenspiel und gegenseitige Beeinflussen aller Teilbereiche einer Produktentwicklung. Unter Produktentwicklung versteht man „die Möglichkeit durch neue Produkte oder Verbesserung bestehender Produkte auf bestehenden Märkten Wachstum zu realisieren[sic!]“[2]. [3]

1.2 Produktlebenszyklus

Jedes neu auf den Markt kommende Produkt durchlebt einen sogenannten Produktlebenszyklus. Dieser beginnt mit der Idee eines neuen Produktes und endet mit dessen Außerdienststellung und Entsorgung (Deproduktion). Grob kann dieser Zyklus, wie in Abbildung 1 ersichtlich, in drei verschiedene Phasen unterteilt werden.

Weitere Aspekte dieses Kreislaufes sind sogenannte unterstützende Prozesse, wie beispielsweise das Projekt-, Risiko- und Qualitätsmanagement (QM). Des Weiteren zählt zu dieser Aufzählung das Änderungsmanagement, das neben der Produktentwicklung für diese Arbeit von Wichtigkeit ist. [4]

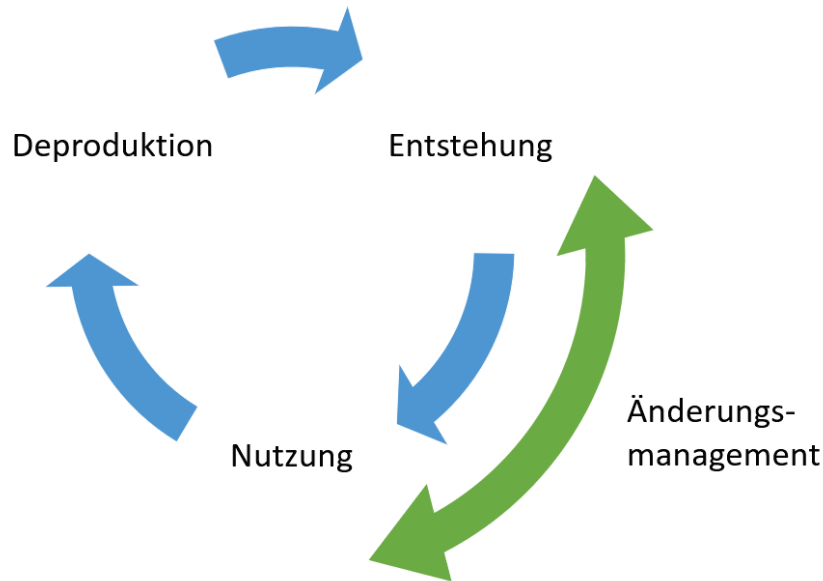


Abbildung 1: Produktlebenszyklus, bestehend aus den Phasen der Entstehung, Nutzung und Deproduktion samt begleitendem Prozess des Änderungsmanagements. Eigene Darstellung, angelehnt an [4] und [5]

Im Englischen ist eine Unterteilung in die folgenden drei Phasen üblich:

- Beginning of life (BoL)
- Middle of life (MoL)
- End of life (EoL) [6]

Diese Bezeichnungen können synonym für die oben genannten deutschsprachigen Begriffe Entstehung, Nutzung und Deproduktion verwendet werden.

1.2.1 Produktentstehungsprozess / Beginning of life

Am Anfang eines jeden Produktes steht der sogenannte Produktentstehungsprozess. Dieser beinhaltet den gesamten Weg von den ersten Ideen bis hin zu einem fertigen, in Serienproduktion übergegangenen Produkt. Innerhalb dieses Prozesses spielt der, in Abbildung 2 ersichtliche Entwicklungs- und Konstruktionsprozess die Hauptrolle. In diesem werden in etwa 80% der Gesamtkosten sowie die Auswirkungen auf die Umwelt festgelegt. Somit hat er auch den größten Einfluss auf das entstehende Endprodukt. [7]

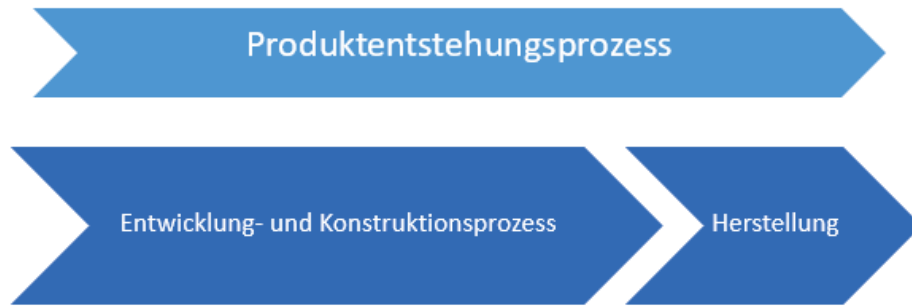


Abbildung 2: Aufteilung des Produktentstehungsprozesses in Entwicklung- und Konstruktionsprozess und Herstellung. Eigene Darstellung, angelehnt an [8]

Aufgrund dieser Tatsache ist ein näheres Eingehen auf die Thematik der Entwicklung und Konstruktion von großer Bedeutung. Gerade hier ist ein Lernen sowie Übernehmen von Prozessen beziehungsweise Denkweisen aus anderen Branchen sinnvoll, wodurch großes Potential zur Einsparung von Ressourcen und Kosten besteht.

Der zweite Teil des Produktentstehungsprozesses, die Phase der Herstellung, wird in dieser Arbeit nur am Rande betrachtet.

1.2.1.1 Entwicklungs- und Konstruktionsphase

Die Produktentwicklung kann, wie in Abbildung 3 ersichtlich, grob in die unten stehenden Phasen eingeteilt werden. Dieser Ablauf ist in den meisten Fällen iterativ. Somit können in einer Phase vorangegangene Arbeitsprodukte wieder geändert und, falls nötig, korrigiert werden.

- Planungsphase
- Konzeptphase
- Realisierungsphase
- Freigabe [4][9]



Abbildung 3: Phasen der Entwicklung. Eigene Darstellung, angelehnt an [9]

Planungsphase

Das übergeordnete Ziel der Planungsphase ist die Erstellung eines Lastenhefts. Diese Anforderungsspezifikation beschreibt die vom Auftraggeber (Kunde) gestellten Forderungen, die durch den Auftragnehmer (Lieferant) im Zuge eines Projektes zu erbringen sind. Es ist teilweise gelebte Praxis, den Inhalt dieses Lastenhefts in Abstimmung mit dem Lieferanten zu erstellen. Generell gilt, dass die gestellten Anforderungen so allgemein wie möglich und so restriktiv wie nötig sein sollten. Dadurch kann eine Einschränkung der Lösungsansätze und Möglichkeiten des Auftragnehmers vermieden werden.

Im Allgemeinen besteht ein Lastenheft aus den folgenden Unterpunkten:

- Einleitung (Zweck und Umfang des Projektes)
- Beschreibung des geforderten Produktes
- Anforderungen (Schnittstellen, funktional und nicht funktional)
- Lieferumfang
- Zeitliche Planung des Projektes
- Qualitätsanforderungen

Aus diesem vom Auftraggeber formulierten Lastenheft, wird vom Auftragnehmer das Pflichtenheft erstellt, in dem beschrieben wird, wie der Lieferant die gestellten Anforderungen lösen will. [10]

Konzeptphase

In dieser Phase werden Lösungsansätze und -varianten erarbeitet und entwickelt. Diese Ansätze münden in die Entscheidung für eine Variante zur Lösung des Projektes. Es wer-

den genaue Pläne zur Ausführung beziehungsweise Lösungsmöglichkeiten zur Umsetzung von gestellten Anforderungen erstellt. [9]

Realisierungsphase

Wie sich aus dem Namen bereits schließen lässt, werden in der Realisierungsphase die in der vorangegangenen Phase erstellten Pläne in die Tat umgesetzt. Diese Tätigkeiten bestehen unter anderem aus:

- Programmierung der Software
- Herstellung einzelner Geräte
- Erstellung der Dokumentation
- Ausarbeitung von Konzepten der Wartung und Instandhaltung
- Festlegung des Umgangs mit Störungen
- Durchführung von sowohl mechanischen als auch gegebenenfalls elektronischen und softwarebezogenen Tests

In dieser Phase eingegangene und gewünschte Änderungen werden über einen Change-Prozess abgewickelt. [9]

Freigabe

Nach der Realisierung des Projektes müssen etwaige Prototypen verifiziert und validiert werden. Diese Schritte münden nach positiver Bewertung in eine Produktfreigabe, die eine Grundvoraussetzung für einen Produktionsstart ist. [11]

Der Unterschied zwischen Verifizierung und Validierung kann in diesem Zusammenhang durch Stellen der folgenden Fragen am besten erklärt werden.

- Verifizierung: mache ich die Dinge richtig?
- Validierung: mache ich die richtigen Dinge?

Um diese soeben beschriebenen Phasen der Entwicklung geordnet und fachgerecht zu durchlaufen, werden verschiedene Vorgehensmodelle verwendet.

1.2.1.2 Vorgehensmodelle

Der Nutzen von Vorgehensmodellen liegt in der Beschreibung des Ablaufs der einzelnen Aktivitäten des Entwicklungsprozesses. Da zurzeit mehr als 50 verschiedene Modelle anerkannt und angewandt werden, muss am Beginn eines Projektes die Frage des am besten geeigneten Vorgehensmodells gestellt werden.

Um diese Frage zu beantworten und somit die Auswahl zu erleichtern, lohnt es sich, einen Blick auf die sogenannte Stacey-Matrix zu werfen. Der britische Professor für Management Ralph Stacey (*1942) entwickelte diese Matrix als Entscheidungshilfe in komplexen Situationen. Wie in Abbildung 4 ersichtlich, wird auf der y-Achse die Klarheit beziehungsweise Unklarheit der gegebenen Anforderungen aufgetragen. Anders ausgedrückt, wird die Menge der zum Startzeitpunkt bekannten Anforderungen sowie die Wahrscheinlichkeit der Änderung dieses Zustandes im weiteren Projektverlauf dargestellt. Auf der x-Achse wird die Neuheit respektive Originalität eines Lösungsansatzes aufgetragen. Dadurch lässt sich bestimmen, wie bekannt beziehungsweise unbekannt eine mögliche Lösung oder deren Technologie ist. Durch diese Tatsachen lässt sich nun auf der Winkelhalbierenden der Charakter eines Projektes von einfach bis chaotisch beziehungsweise die Unterscheidung zwischen traditionell, auch klassisch genannt, und agil ablesen.

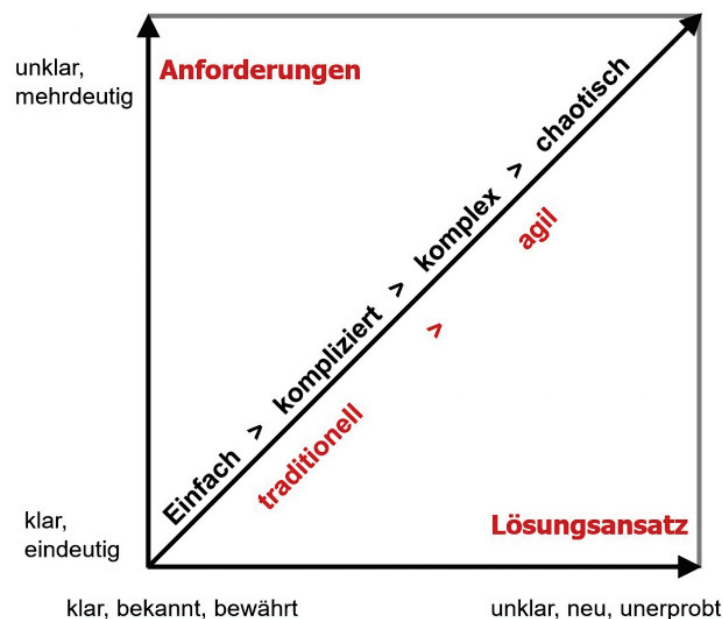


Abbildung 4: Stacey-Matrix. Charakterisierung eines Projektes durch Gegenüberstellung von Bekanntheit des Lösungsansatzes zur Klarheit der gestellten Anforderungen [12]

Dieser Unterteilung können, wie in Abbildung 5 zu sehen ist, verschiedene Vorgehensmodelle zugewiesen werden. In den folgenden Kapiteln werden die bekanntesten und für diese Arbeit relevanten Modelle in klassisch und agil unterschieden und näher dargestellt und erläutert. [12][13]

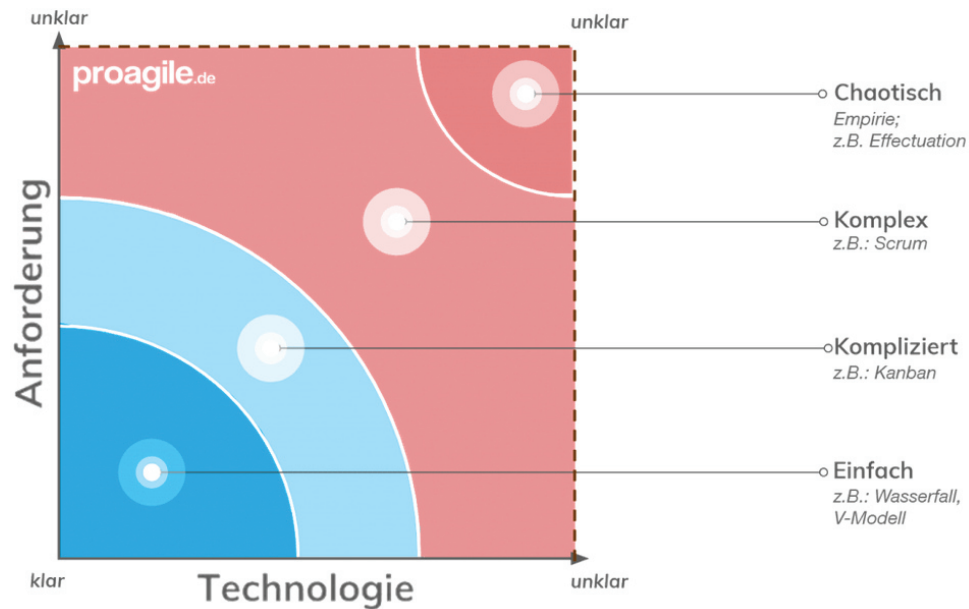


Abbildung 5: Vorgehensmodelle in der Stacey-Matrix. Die wichtigsten klassischen und agilen Vorgehensmodelle werden je nach Grad der Klarheit von Anforderung beziehungsweise der verwendeten Technologie aufgelistet. [13]

Klassische Vorgehensmodelle

In der klassischen Herangehensweise legt ein Projektleiter sowohl die zu erledigenden Arbeitspakete, als auch die involvierten Personen beziehungsweise Teammitglieder am Anfang eines Projektes fest. Das Projekt ist in mehrere, voneinander getrennte Meilensteine gegliedert, die das Projekt in einzelne Phasen unterteilt. Das Auftreten von etwaigen Änderungen wird möglichst vermieden, da dies einen aufwendigen und dadurch möglicherweise kostspieligen Änderungsprozess zur Folge hat.

Typisch für das klassische Vorgehensmodell ist, wie in Abbildung 6 dargestellt, dass die Projektumfänge klar definiert, einzuhaltende Termine und entstehende Kosten allerdings flexibel sind. Das bedeutet, dass diese Parameter in einem solchen Maß angepasst werden, dass diese Umfänge erreicht werden können. [14][15]

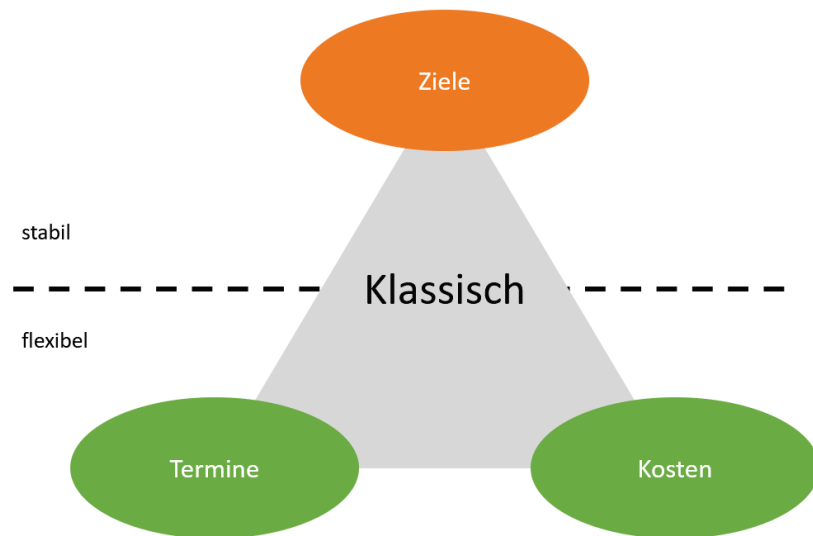


Abbildung 6: Charakterisierung der klassischen Herangehensweise. Die Abbildung zeigt die Auftrennung der flexiblen (grüne Ellipse) und stabilen (orange Ellipse) Merkmale der klassischen Herangehensweise. Eigene Darstellung, angelehnt an [14]

Wasserfallmodell

Das Wasserfallmodell ist, wie in Abbildung 7 ersichtlich, ein lineares Planungsmodell und in aufeinanderfolgende Phasen gegliedert. Es wird unter anderem in der Entwicklung von Software angewandt. Ein neues Projekt startet in der ersten Phase und durchläuft ohne Iterationen strikt den definierten Ablauf. Dadurch gilt grundsätzlich, dass jede dieser Phasen nur einmal durchlaufen wird.

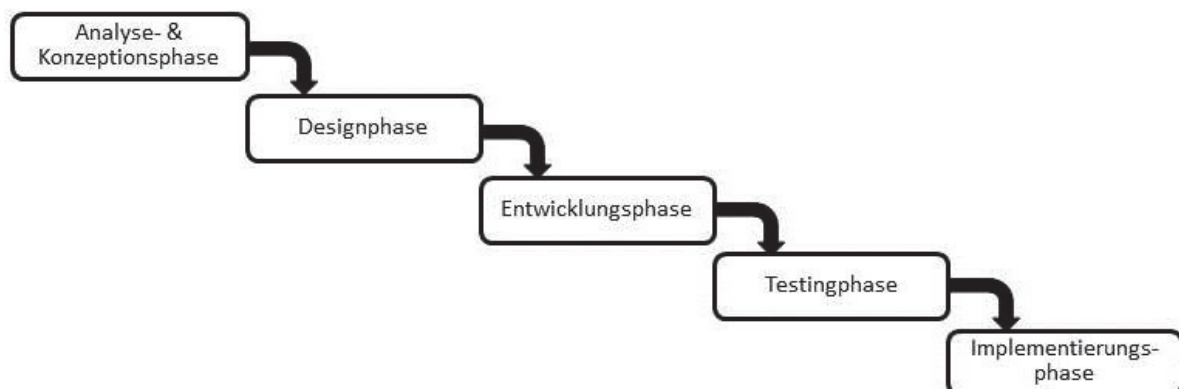


Abbildung 7: Fünfstufiges Wasserfallmodell [16]

Die Phasen können wie folgt gegliedert werden:

Analyse

Jedes Projekt beginnt damit, die einzelnen Anforderungen an das Projekt mit dem Kunden zu definieren und festzulegen, diese zu analysieren und ein Soll-Konzept zu entwickeln (Lastenheft).

Design

In dieser Phase wird durch die zuvor gestellten Anforderung ein Lösungskonzept erarbeitet. Das Ergebnis dieser Phase ist die Erstellung eines Entwurfsdokumentes, in dem die vorherige Planung festgehalten wird.

Entwicklung

In der Entwicklungsphase steht die eigentliche Arbeit, beispielsweise das Programmieren und Implementieren der gewünschten Software, im Mittelpunkt. Zur Vereinfachung und Arbeitserleichterung werden komplexe Programme in einzelne Komponenten zerlegt, die durch Modultests überprüft und danach in ein Gesamtkonstrukt integriert werden.

Test

In dieser Phase werden die zuvor separat entwickelten Programmteile als Gesamtprodukt getestet und in die Zielumgebung integriert. Ziel ist es, zu überprüfen, ob die gestellten Anforderungen erfüllt werden und etwaige Fehler aufzudecken und zu beheben. Am Ende dieser Phase ist das Produkt bereit für den Release respektive die Freigabe.

Betrieb

Nach erfolgreicher Beendigung der Testphase wird das Produkt an den Kunden ausgeliefert und kann in Betrieb genommen werden. Des Weiteren schließt diese Phase auch die Aktualisierung, Wartung und Verbesserung des Produktes ein.

Dieses Modell wird vor allem bei Projekten mit von Anfang an bestehenden Anforderungen und Abläufen eingesetzt. Dies sind meistens kleine, nicht allzu komplexe Projekte der Software. Des Weiteren ist es oft nicht möglich, einzelnen Phasen klar voneinander abzugrenzen, da der Übergang zwischen ihnen fließend ist. Teile eines Gesamtsystems können sich schon im Gebrauch befinden, während andere noch in der Designphase sind. [16][17]

Eine Weiterentwicklung des soeben beschriebenen Wasserfallmodells ist das weit verbreitete, ebenso linear verlaufende V-Modell. Es wurde ursprünglich in der Softwareentwicklung verwendet, findet aber mittlerweile auch in der Entwicklung mechatronischer Systeme immer mehr Anwendung. [18]

Das Diagramm stellt das V-Modell dar, ein etabliertes Modell für die Softwareentwicklung und -prüfung. Es ist durch zwei Achsen strukturiert:

- Zeitachse (horizontal):** Ein Pfeil nach rechts oben mit der Beschriftung "Zeit".
- Detaillierungsachse (vertikal):** Ein Pfeil nach unten links mit der Beschriftung "Detaillierung".

Die Entwicklungspfade (links) und Testpfade (rechts) sind wie folgt gegliedert:

- Entwicklungspfad (linke Seite):** System-anforderung → Systementwurf → Architektur → Komponenten-Spezifikation → Implementierung.
- Testpfad (rechte Seite):** Abnahmetest ← Systemtest ← Integrationstest ← Komponententest.

Die Phasen sind durch diagonale Linien verbunden, die den Rückkopplungsprozess verdeutlichen:

- Systementwurf ↔ Abnahmetest (Validieren)
- Architektur ↔ Systemtest (Verifizieren)
- Komponenten-Spezifikation ↔ Integrationstest (Verifizieren)
- Implementierung ↔ Komponententest

Zusätzlich zeigt eine gestrichelte Linie am oberen Rand einen direkten Pfad von der Systemanforderung zum Abnahmetest.

Es werden nicht nur Anforderungen an das System beziehungsweise eine Systemarchitektur, sondern auch die entsprechenden Tests und Testfälle erstellt. Dies dient der Sicherstellung, dass sowohl das Gesamtsystem als auch die einzelnen Teile und Komponenten abgetestet werden und somit den gestellten Anforderungen entsprechend funktionieren.

Im Großen und Ganzen kann dieses Modell in drei Teile gegliedert werden:

Entwurfsphase

In dem absteigenden Teil des V-Modells (linke Seite) werden die einzelnen Anforderungen nach dem Top-Down-Prinzip, zuerst grob, danach immer detaillierter beschrieben. Hierbei steht die Tatsache, dass eine Änderung auf einer Ebene Anpassungen auf darunterliegenden Ebenen zur Folge hat, im Vordergrund.

Diese Ebenen sind:

- Anforderungen an das System

Die erste Phase beschäftigt sich, ähnlich dem Wasserfallmodell, damit, Anforderungen an das Produkt zu stellen und somit ein Lastenheft zu erstellen.

- Systementwurf

Hier wird das Gesamtsystem entworfen beziehungsweise designend und beschrieben, wie die gestellten Anforderungen umgesetzt werden können. Dies mündet, wie zuvor beschrieben, in einem Pflichtenheft.

- Architektur

In dieser Ebene wird das Gesamtsystem in Komponenten, Module oder Subsysteme unterteilt. Die Abhängigkeiten und Schnittstellen untereinander können mittels Analysemethoden, wie beispielsweise einer Fehlermöglichkeits- und -einflussanalyse, kurz FMEA, beschrieben werden.

- Spezifikation der Komponenten

Zuletzt wird die Umsetzung dieser Module und Komponenten spezifiziert.

Implementierung

An der Spitze des V's steht die eigentliche Produktentwicklung oder Implementierung im Mittelpunkt. In dieser Phase entsteht das zuvor definierte Produkt. Diese Implementierung wird nicht näher durch das V-Modell beschrieben.

Validierungsphase

Im rechten Teil, der auch als Validierungsphase bekannt ist, wird beschrieben, wie die gegenüberliegenden Entwurfsebenen, von der Komponenten- bis Systemebene, mittels Bottom-Up-Prinzip getestet und dadurch validiert und verifiziert werden.

- Komponententest

In dieser tiefsten Testebene werden einzelne Funktionen oder Module getestet.

- Integrationstest

Der nächste Schritt ist das Absichern und Testen des Zusammenwirkens einzelner Komponenten und beispielsweise deren Kommunikation.

- Systemtest

Wie aus der Bezeichnung schließen lässt, wird hier das System als Ganzes abgetestet.

- Abnahmetest

In der finalen Testphase wird das Produkt möglichst in der späteren Anwendungsumgebung von den Endnutzern validiert. [19] [20]

Vor und Nachteile

Durch diese Vorgehensweise ist eine hohe Testabdeckung einzelner Komponenten und des Gesamtsystems möglich. Da Testfälle am Anfang konzipiert und geplant werden beziehungsweise es zu einem frühen Einbinden der Tester kommt, können unvollständige Spezifikationen im Lasten- oder Pflichtenheft früh erkannt werden.

Aufgrund dieser Tatsachen ist dieses Modell jedoch starr und wenig flexibel und somit für eine agile Herangehensweise wenig geeignet. [19]

Agile Vorgehensmodelle

Im Allgemeinen werden agile Vorgehensmodelle durch eine iterative Entwicklung, einen regen Austausch mit dem Kunden und der Forderung nach einem frühen Kundenfeedback charakterisiert. Dies soll den Entwicklungsprozess flexibler gestalten und die Vorabplanung reduzieren. Da sich das Team im Projekt überwiegend selbst organisiert und die Arbeitspakete untereinander aufteilt, wird die Rolle eines Projektmanagers oder -leiters im traditionellen Sinne obsolet. Dieser nimmt dafür eine Moderatorenrolle im Team ein. Die Grundideen dieses Ansatzes für die Software-Entwicklung ist im „Agilen Manifest“ niedergeschrieben, welches in dieser Arbeit nicht näher erläutert oder beschrieben wird.

Wie in Abbildung 9 ersichtlich, sind sowohl Termine als auch die entstehenden Kosten und der Aufwand klar definiert und abgesteckt. Da sich der Umfang und die Umset-

zung der Anforderungen jedoch kontinuierlich ändert, ist diese Größe variabel gestaltet. Dieser Umstand lässt eine Berücksichtigung von Änderungen ohne weitere Probleme zu. [14][15][21][22][23]

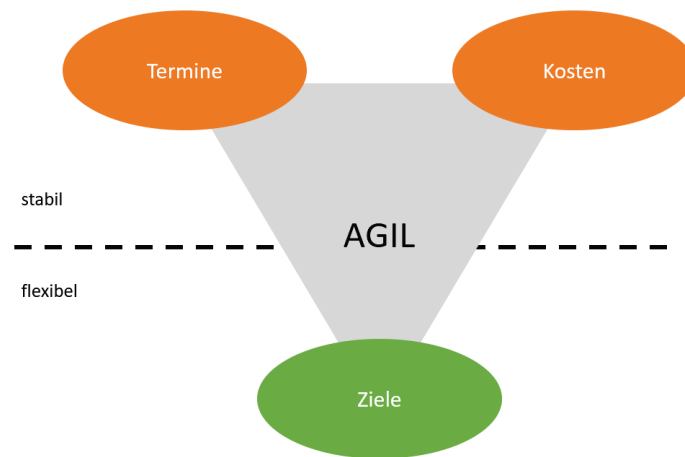


Abbildung 9: Charakterisierung der agilen Herangehensweise. Die Abbildung zeigt die Auftrennung der flexiblen (grüne Ellipse) und stabilen (orange Ellipse) Merkmale der agilen Herangehensweise. Eigene Darstellung, angelehnt an [14]

Kanban

Kanban wurde ursprünglich von dem japanischen Automobilhersteller Toyota entwickelt und kann in etwa mit dem Wort „Signalkarte“ übersetzt werden. Diese Methode diente anfangs zur Optimierung von Materialflüssen in der Produktion, in dem sie die sogenannte Pull-Methode (Güter werden erst angefordert wenn der Vorrat zur Neige geht) einführte.

Heute findet diese Methode nicht nur in der Produktion sondern auch beispielsweise in der Software-Entwicklung Anwendung. Durch den Einsatz dieses Modells werden Aufgaben nach der Pull-Methode zugeteilt. Erst nach Abschluss einer Aufgabe beziehungsweise eines Tasks wird mit einem Neuen begonnen. Dies dient primär zur Verbesserung des Workflows, da nach dem Motto „stop starting - start finishing“ gearbeitet wird. Zu erledigende Aufgaben werden in einzelne Subaufgaben unterteilt, die nacheinander erledigt werden. [24][25]

Das in Abbildung 10 gezeigte Kanban-Board ist das Zentrum dieser Methode und dient zur Darstellung der Arbeitsschritte. Als Board wird in den meisten Fällen entweder eine

Pinnwand, ein Whiteboard oder eine digitale Lösung gewählt. Auf dieser Tafel können einzelne Aufgaben als farbige Karten oder Pins angebracht werden, wobei der Aufbau und die Farben keinerlei Rolle spielen. Wichtig ist nur, dass die Tafel übersichtlich gestaltet ist.

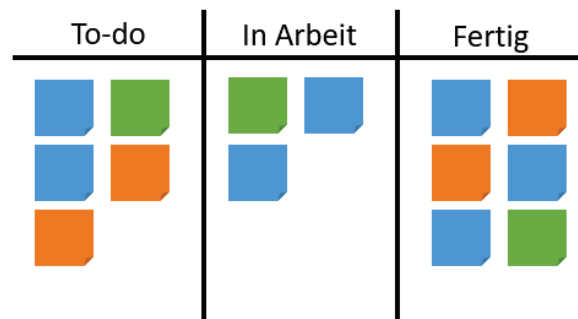


Abbildung 10: Kanban-Board mit einzelnen Arbeitspaketen, aufgeteilt in die Bereiche „To-Do“, „In Arbeit“ und „Fertig“. Die verwendeten Farben können hier beispielsweise ein gewisses Projekt widerspiegeln. Eigene Darstellung, angelehnt an [26]

Generell wird Kanban in die folgenden drei verschiedenen Bereiche gegliedert:

- To-do

In dieser Spalte werden alle noch zu erledigenden Aufgaben beziehungsweise Tasks gesammelt. Dies entspricht dem im folgendem Kapitel „Scrum“ beschriebenen Backlog.

- In Arbeit

In der Mitte befinden sich die Aufgaben, die derzeit bearbeitet werden. Falls eine Aufgabe mehrere Phasen durchläuft, kann diese Spalte auch noch weiter unterteilt werden.

- Fertig

Erst nach vollständiger Abarbeitung einer Aufgabe wird sie in die letzte Spalte verschoben.

Es können durchaus mehr als die genannten Phasen, beispielsweise eine Spalte für Tests oder Reviews, vorhanden sein. Durch die Tatsache, dass nicht alle Aufgaben gleich wichtig beziehungsweise dringend oder von allen Mitgliedern zu erledigend sind, ist es möglich, neben den vertikalen auch horizontale Linien in das Board einzufügen, die unter anderem die einzelnen Teammitglieder oder auch die Wichtigkeit abbilden. [24][25]

Scrum

Wenn man sich mit agilem Projektmanagement beschäftigt, führt nahezu kein Weg an Scrum vorbei. Der Ursprung dieses Modells liegt in der Software-Entwicklung, da diese in der Vergangenheit oft nicht von Anfang bis Ende durchgeplant werden konnte. Der Name Scrum kommt aus dem Rugby-Sport und beschreibt einen taktischen Spielzug. Dies soll, übertragen auf das Projektmanagement, die dynamische und flexible Situation auf der Spielfläche beschreiben.

Der Grundgedanke ist, dass ein Projekt in kleinen Schritten durchgeführt und nicht von Anfang an durchgeplant wird. Dies bringt den immensen Vorteil mit sich, dass binnen kurzer Zeit und ohne großen Aufwand auf Probleme oder Änderungen reagiert werden kann. Eine weitere nennenswerte Eigenschaft von Scrum ist, ähnlich wie bei Kanban, das Nichtvorhandensein eines klassischen Projektleiters, da die Grundlage auf einer Selbstorganisation der Teammitglieder beruht. [23][27][28]

Wie in Abbildung 11 ersichtlich, kann Scrum in mehrere Unterpunkte gegliedert werden.

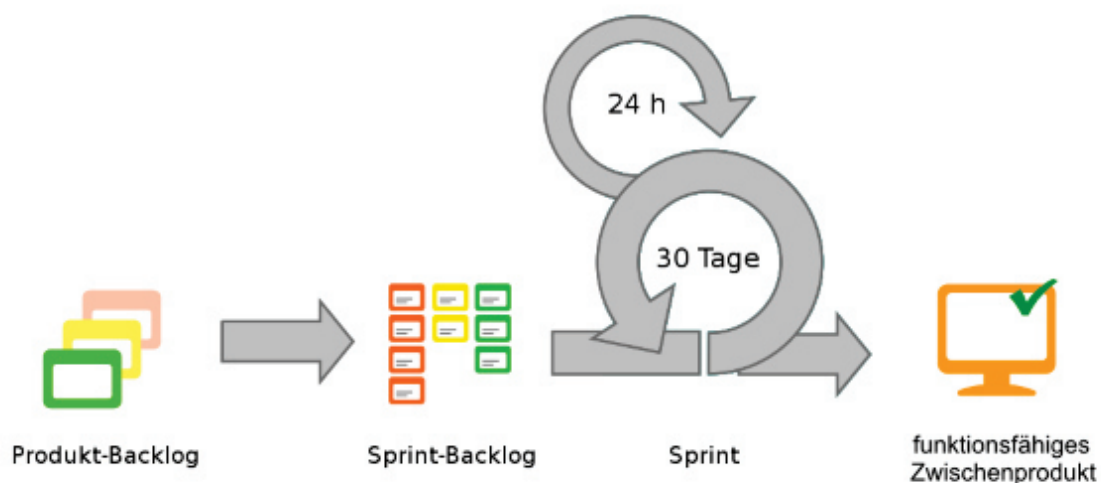


Abbildung 11: Scrum. Alle Anforderungen werden in dem Product-Backlock gesammelt und danach in, in einzelnen Sprints zu erledigenden Aufgaben getrennt und in ein Sprint-Backlock verschoben. Ziel ist es, nach jedem, zwischen 24 Stunden und 30 Tage lang andauernden Sprint ein funktionsfähiges Zwischenprodukt zu erhalten. [27]

Sprint

Bei Scrum wird ein Projekt in verschiedenen Etappen, sogenannte Sprints aufgeteilt. Diese Sprints dauern jeweils maximal 30 Tage, wobei der Trend jedoch in Richtung von ein- bis zweiwöchigen Sprints geht. In dieser Zeit werden sowohl neue Anforderungen als auch etwaige Verbesserungen oder Änderungen realisiert und eingebaut. Sollte eine Änderung während eines Sprints auftreten und sich somit eine Anforderung ändern, kann dieser auch abgebrochen werden. Ziel ist es, am Ende jedes Sprints ein funktionsfähiges Zwischenprodukt (Produktinkrement) zu erhalten, das dem Kunden zur Begutachtung präsentiert wird und etwaige Verbesserungsmaßnahmen weiter in das Produkt einzuarbeiten. Somit baut ein Sprint auf den Vorherigen auf, wobei auch die Möglichkeit besteht, das Resultat eines Sprints im darauf folgenden Durchlauf zu verwerfen. Durch diese kurzen Entwicklungsphasen ist es nötig, sich auf die wichtigsten Funktionen eines Zwischenproduktes zu konzentrieren.

Eine Besonderheit ist das jeden Tag abgehaltene Scrum-Meeting (Daily Scrum). Hier wird im Sinne einer Teambesprechung in kurzer Zeit Feedback über die eigenen Tätigkeiten und deren Fortschritt gegeben. Das Ziel ist, einen Überblick über den Progress der gestellten Aufgaben zu erhalten. [23][27][28]

Backlog

Grundsätzlich werden im Backlog die noch zu erledigenden projektbezogenen Aufgaben gesammelt. Bei Scrum wird zwischen Product- und Sprint-Backlog unterschieden.

- **Product-Backlog**

Im Product-Backlog werden alle Anforderungen an ein Produkt gesammelt, die priorisiert und schrittweise in Sprints bearbeitet werden. Diese können beispielsweise Anforderungen an die zu erstellende Hardware oder Software sein. Es handelt sich um eine dynamische Liste und darf somit nicht mit einem starren Lastenheft im klassischen Sinne verwechselt werden. Durch diese Tatsache ist es einfach, Anforderungen einzufügen, zu ändern oder sogar zu entfernen. [23][27][28]

- **Sprint-Backlog**

In der Sprint-Planung wird entschieden, welche dieser Anforderungen im nächsten Sprint bearbeitet und somit in das Sprint-Backlog verschoben werden sollen. Diese Anforderungen werden, wie in Abbildung 12 ersichtlich, in innerhalb eines Tages

zu erledigende Aufgaben unterteilt. Nach Ende des Sprints wird überprüft, welche Anforderungen erfüllt wurden und welche wieder zurück in das Product-Backlog aufgenommen werden müssen. [23][27][28]

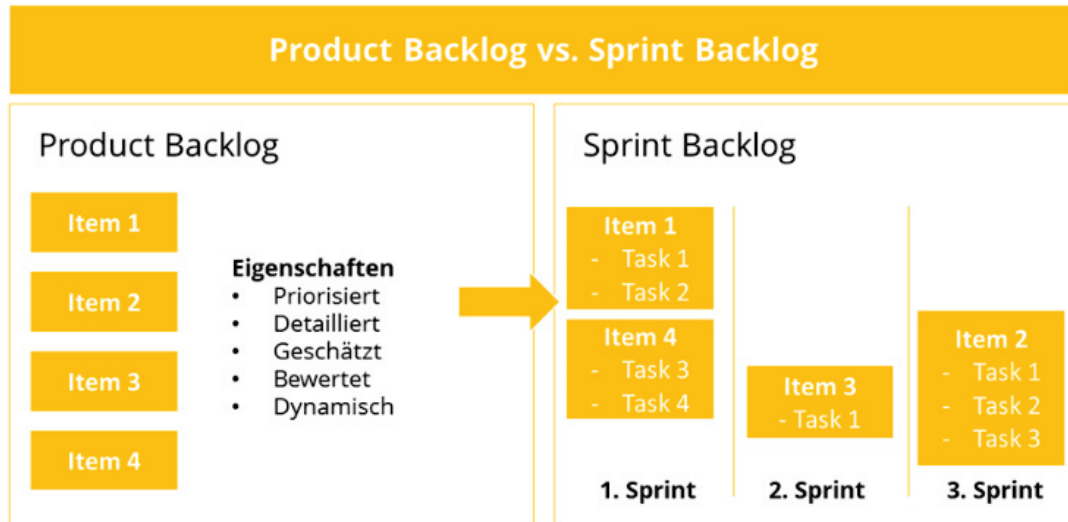


Abbildung 12: Product-Backlog vs. Sprint-Backlog in Scrum. Aufteilung einzelner Items in Tasks, die in einem Sprint zu erledigen sind. [23]

1.2.2 Technische Änderungen

Wie in der Beschreibung der einzelnen Vorgehensmodelle in der Entwicklung in den vorigen Kapiteln ersichtlich, sind Änderungen ein häufiger Vorgang. Diese können während der laufenden Entwicklung oder auch in der Serienbetreuung und somit über den gesamten Produktlebenszyklus hinweg auftreten. Da Management und Einbringung von Änderungen nicht immer einfach ist, wird des Öfteren der Versuch gewagt, durch genaues Projektmanagement ein nahezu perfektes Produkt zu entwickeln, welches keine Änderungen oder Verbesserungen braucht.[29] Dies ist jedoch nicht möglich, da auch bei einfachen und simplen Projekten der unten stehende Leitsatz von Publilius Syrus [30] gilt.

„Nur ein schlechter Plan erlaubt keine Änderung.“

Die Definition einer technischen Änderung ist in der Literatur nicht einheitlich geregelt und unterscheidet sich in Bezug auf das Objekt und den Umfang der Änderung. Sie können auf ein einziges Teil eines Produktes beschränkt sein oder dessen Pläne und sogar Teile wie die Software einschließen. Des Weiteren wird nach dem Auftreten in gewissen Phasen des Lebenszyklus unterschieden. Hierbei kommen je nach Autor Änderungen erst ab

Beginn der Produktionsphase vor, wobei die Phase der Entwicklung außer Acht gelassen wird. Oder aber es wird die Abgrenzung ab einem sogenannten Design-Freeze, in dem eine endgültige Vorlage für die Serienproduktion gebildet wird, vollzogen. Es werden auch verschiedene Bezeichnungen, wie Änderung oder technische Änderung verwendet, die in dieser Arbeit als Synonym betrachtet werden.

Auf jeden Fall ist eine Differenzierung zwischen Änderungen und Iterationen erforderlich, wie sie unter anderem bei kreativen Prozessen der Entwicklung nötig sind. Diese Unterscheidung wird durch den Status einer Freigabe von beispielsweise Prototypen oder der Dokumentation erreicht.

In der Literatur wird jedoch kein Bezug auf die Herkunft oder die Ausmaße einer Änderung genommen. Somit beinhalten technische Änderungen alle möglichen Anpassungen, von kleinen Korrekturen einer technischen Zeichnung bis hin zur vollständigen Überarbeitung eines Produktes. [31][32][33]

Eine weitere Form der Überarbeitung beziehungsweise Abwandlung ist die organisatorische Änderung, die die Veränderung von Prozessen oder Betriebsstrukturen und somit die Organisation des Ablaufs eines Unternehmens adressiert. Diese Form kann auch durch eine technische Änderung an einem Produkt auftreten, wird jedoch in dieser Arbeit nicht näher behandelt. [31]

1.2.2.1 Eigenschaften einer technischen Änderung

Da Änderungen durch verschiedene Eigenschaften charakterisierbar sind, wird in den folgenden Punkten auf die, für diese Arbeit relevanten, näher eingegangen.

Änderungsauslöser

Eine Änderung hat meist eine Korrektur oder Überarbeitung einer Anforderung und somit einen Unterschied zwischen Soll- und Ist-Zustand zum Ursprung. Diese Abweichungen können prinzipiell in zwei verschiedenen Phasen des Produktlebenszyklus auftreten:

- Entwicklung

Diese Änderungen treten in der Entwicklungsphase eines Produktes auf und haben

beispielsweise eine Überschreitung der Kosten oder ein Problem in der Fertigung und somit eine unzureichende Erfüllung einer Anforderung oder einen Fehler als Auslöser.

- Serienbetreuung

Die zweite Möglichkeit ist, dass eine Änderung nach der Freigabe auftritt und somit der Soll-Zustand nicht mehr den anfänglich gestellten Anforderungen entspricht. Dies kann unter anderem eine Gesetzesänderung oder eine neue Anforderung eines Kunden als Auslöser haben. [31][34]

Eine weitere Unterscheidungsmöglichkeit ist die Trennung in Änderungen, die entweder durch neue Anforderungen eines Kunden initiiert, oder durch vorhandene Produktfehler hervorgerufen werden. [35]

Eine Änderung selbst kann als Folge vorhergehender Änderungen auftreten in dem sie den Ist-Zustand soweit verändern, dass dieser mit dem Soll-Zustand nicht mehr übereinstimmt. [31]

Änderungsgrund

Da eine Abweichung des Ist- und Soll-Zustandes ein alltägliches Vorkommnis und ein Änderungsprozess mit finanziellen Belastungen verbunden ist, muss ein ausreichender Grund für eine Änderung vorhanden sein. Generell kann dieser zwei verschiedene Hintergründe haben:

- Zwingender Grund / Muss-Änderung

Um einen weiteren Verkauf oder Betrieb eines Produktes möglich zu machen, müssen diese Änderungen eingepflegt werden. Gründe hierfür können Änderungen etwaiger Sicherheits- oder Gesetzesvorgaben sein.

- Wirtschaftlicher Grund / Kann-Änderung

Wie aus dem Namen schließen lässt, sind diese Änderungen nicht verpflichtend, sondern dienen dem Steigern des Umsatzes oder Gewinnes eines Produktes. Diese Steigerung kann beispielsweise durch eine Verringerung der Herstellungs- beziehungsweise Zulieferungskosten oder einer Verbesserung des Produktes und somit einer Erhöhung der Verkaufszahlen erzielt werden. [34][36][37]

Änderungsursachen

Die Ursache einer Änderung beschreibt den kausalen Grund einer Abweichung des Ist- und Soll-Zustandes. Diese Ursachen reichen von Flüchtigkeitsfehlern bis hin zu Verbesserungen eines Produktes oder Einsparungen der entstehenden Kosten. Oft auftretende Ursachen können die Verlegung eines Produktionsstandortes, ein neuer Lieferant oder neue Anforderungen eines Kunden oder des Gesetzgebers sein. [38]

Abweichungen des Ist- und Soll-Zustandes können somit, wie in Abbildung 13 dargestellt, sowohl externe als auch interne Ursachen haben.



Abbildung 13: Externe und interne Ursachen einer Änderung. Eigene Darstellung, angelehnt an [36]

Interne Ursachen beruhen beispielsweise auf einem Änderungswunsch durch das Management bei zu hohen Kosten, durch das Qualitätsmanagement bei entstehenden Fehlern oder auch bei auftretenden Innovationen durch die Forschungs- und Entwicklungsabteilung, im englischen mit R&D abgekürzt. Weit verbreitete externe Ursachen einer Änderung können Veränderungen der Markt- oder Kundenanforderungen sein. Somit kann selbstverständlich ein Wandel des Verkaufstrends von Produkten oder das Auftreten eines besseren Konkurrenzproduktes zu Änderungen im eigenen Betrieb führen. Auch Zulieferer können Ursa-

chen für Änderungen sein, falls beispielsweise gelieferte Teile nicht mehr in gewünschter Form oder Qualität vorhanden sind. Selbstverständlich können auch Anpassungen von Gesetzen, Normen oder Sicherheitsbestimmungen zu Änderungen führen. [36][39][40]

Des Weiteren kann in Änderungen beruhend auf Fehlern und Änderungen aufgrund von Neuerungen unterschieden werden. Die Zuordnung in eine dieser Klassen gestaltet sich jedoch teilweise schwierig, da genaues Wissen über den wahren Ursprung vorhanden sein muss. Es ist durchaus möglich, dass sich eine durch einen Kunden eingebrachte Änderung von einer fehlerhaften oder nicht vollständigen Anforderung herleiten lässt. [34]

1.2.2.2 Auswirkungen von Änderungen

Die Auswirkungen von Änderungen können auf verschiedene Bereiche oder Kategorien einen Einfluss haben. Diese können das Produkt selbst, umschließende Prozesse oder auch allgemeine Ressourcen betreffen.

Produktauswirkungen

Da technische Änderungen immer eine Veränderung oder Abwandlung eines Produktes zur Folge haben, werden die Auswirkungen von dessen Architektur beeinflusst. Die wichtigsten Faktoren der Architektur sind, wie in Abbildung 14 ersichtlich, der Zusammenhang von funktionalen Eigenschaften und den dazugehörigen Bauteilen beziehungsweise Komponenten und deren Schnittstellen.

Durch diesen Zusammenhang ist es möglich, dass eine Änderung eines Bauteils gleichzeitig zu Änderungen in einer anderen Komponente führt. Aufgrund dieser Tatsache kann der Umfang einer Änderung ein nicht vorhergesehenes Ausmaß annehmen. Dies ist allgemein als Änderungsausbreitung oder -fortpflanzung bekannt. Daraus resultiert, dass mit steigender Komplexität eines Produktes auch die Wahrscheinlichkeit zunimmt, im Vorhinein ungewollte und nicht beachtete Änderungen einer anderen Komponente herbeizuführen.

Falls eine Modulbauweise Einsatz findet, hat möglicherweise eine kleine Änderung Auswirkungen auf viele verschiedene Produkte. [31][35][39]

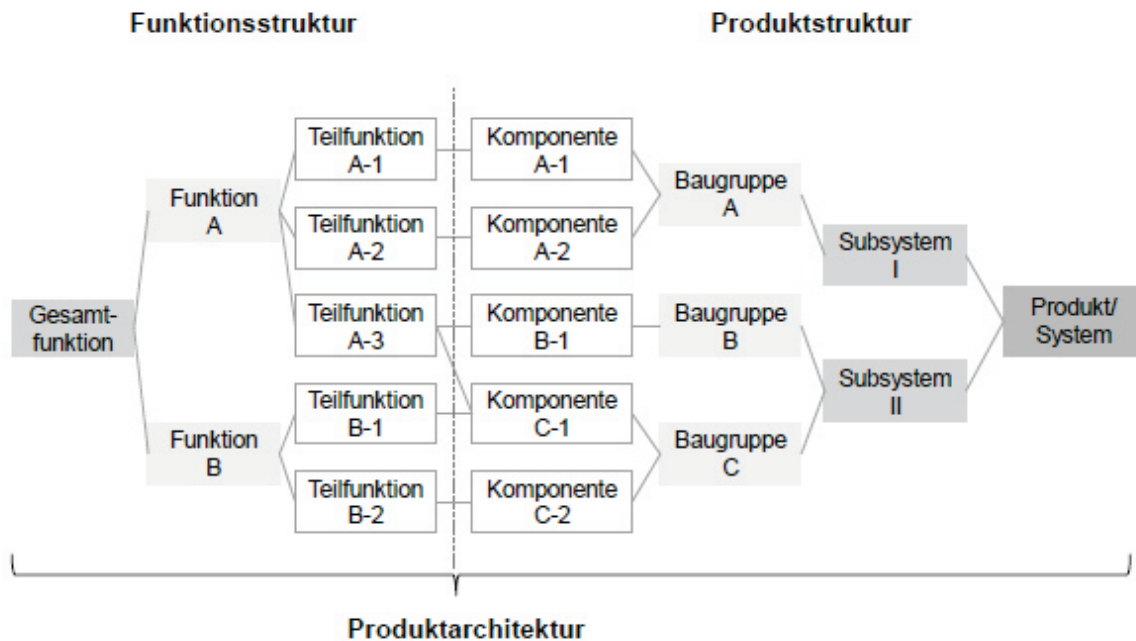


Abbildung 14: Produktarchitektur. In dieser Abbildung wird die Aufteilung und der Zusammenhang von Funktionsstruktur und Projektstruktur dargestellt. [31]

Prozessauswirkungen

Eine technische Änderung kann über den gesamten Produktlebenszyklus hinweg und somit auf nahezu alle Prozesse und Bereiche eines Unternehmens Auswirkungen haben. Des Weiteren können diese Änderungen nicht nur den eigenen Betrieb, sondern auch die Kunden und Lieferanten betreffen. [31][34]

Auswirkungen auf Ressourcen

Im Allgemeinen haben Änderungen eines Produktes positive Auswirkungen auf die Qualität. Dies beruht auf einer eventuellen Verbesserung durch genaueres Erfüllen von Anforderungen oder durch Beheben eventuell aufgetretener Fehler. Bei einem sehr komplexen Produkt können aber auch negative Folgen auftreten, da durch Ausbreitung einer Änderung möglicherweise neue Fehler entstehen, die erst in der Nutzungsphase bekannt werden.

Einen weiteren, sehr essenziellen Einfluss haben Änderungen auf die Dauer der Entwicklung und somit auf die Kosten. Wie in der Beschreibung der einzelnen Vorgehensmodelle

der Entwicklung ersichtlich, ist durch eine Änderung ein neues Durchlaufen, beispielsweise des V-Modells, nötig. Selbst die Durchsicht und Prüfung des Antrags einer Änderung kann zu einer Verzögerung führen. All dies kann eine Verlängerung der Entwicklungsdauer und somit der Zeit zur Markteinführung zur Folge haben. Dies führt unweigerlich zu einer finanziellen Belastung, da während der Entwicklung zwar Kosten entstehen aber keine Einnahmen erzielt werden können. Aber auch das Gegenteil ist möglich, da durch eine Änderung eine Neuentwicklung eines Produktes eventuell obsolet wird und somit der benötigte Zeitbedarf sinkt und dadurch die Kosten vermindert werden können. [31][34][41][42][43]

1.2.2.3 Änderungsmanagement

Da die Umsetzung einer Änderung diverse Komplikationen im Projektmanagement, wie oben genannt beispielsweise eine Verlängerung der Entwicklungszeit oder eine Erhöhung der geplanten Kosten verursachen kann, muss dieser Prozess genau strukturiert und gut geplant erfolgen. Aus diesem Grund, wird in den meisten Betrieben ein Änderungsmanagement implementiert. Diese Abteilung hat die Aufgabe, Prozesse und betriebsinterne Strukturen zu bilden und zu bedienen, um Änderungen organisiert und transparent in den Entwicklungs- und Produktionsprozess einbringen zu können.

Der englische Begriff Change-Management kann hier nicht als Synonym verwendet werden, da er in der Regel das Ändern von Prozessen und Abläufen beschreibt. [29]

Das neben dem Änderungswesen ebenso für das Änderungsmanagement wichtige Konfigurationsmanagement wird in dieser Arbeit nicht näher betrachtet.

Strategien

Um die Anzahl von Änderungen gering zu halten, werden verschiedene Strategien im Änderungsmanagement angewandt. Diese können als Vermeidung, Vorverlagerung oder Steigerung der Effizienz beschrieben werden. Dies trifft hauptsächlich in der klassischen Herangehensweise zu, da hier, wie zuvor beschrieben, Änderungen nicht wünschenswert sind. Im Gegensatz dazu, spielen diese Strategien im agilen Ansatz nahezu keine Rolle, da die gewünschte Agilität durch das Auftreten von Änderungen erreicht wird. [31][44]

- Vermeidung

Diese Strategie zielt auf das Vermeiden von unnötigen Änderungen und somit auf

eine Reduktion der Gesamtanzahl von Änderungen im Betrieb ab. Laut einer Studie sind mehr als 20% aller technischen Änderungen vermeidbar. Als unnötig werden Änderungen bezeichnet, die beispielsweise aufgrund eines Fehlers oder mangelnder Kommunikation im Projektteam und daraus resultierender zu spät kommender oder gar falscher Information entstehen. Nicht alle dieser Fehler sind vermeidbar, es ist jedoch möglich, aus bereits bekannten Fehlern oder Problemen zu lernen und diese nicht zu wiederholen.

Um die Anzahl, dieser meist im Entwicklungsprozess auftretenden Fehler zu minimieren, ist es sinnvoll, geeignete Analysen und Methoden des Qualitätsmanagements zu etablieren und zu benützen. Zu diesen Analysen zählt beispielsweise eine Fehlermöglichkeits- und Einflussanalyse (FMEA), die sowohl auf Produkt-, als auch Prozessebene durchgeführt werden kann. Um bekannte Fehler nicht erneut zu begehen, ist es möglich, gewonnene Erkenntnisse mit Ansätzen des Wissensmanagements wie beispielsweise der sogenannten „Lessons Learned“ zu verwalten.

Es kann aber auch das Produkt selbst so konstruiert werden, dass es gegenüber äußeren Einflüssen oder Veränderungen unempfindlich wird. Dies kann als „Design for robustness“ bezeichnet werden. [31][34][45][46][47]

- Vorverlagerung

Da, wie vorhin näher erläutert, Änderungen immer mit Kosten und Zeitaufwand verbunden sind, wird in den meisten Betrieben versucht, die Anzahl der Änderungen so gering wie möglich zu halten und diese so früh wie möglich zu implementieren.

Dies wird durch Betrachtung der in Abbildung 15 dargestellten sogenannten Zehnerrregel ersichtlich. Diese auch als „Rule-of-ten“ bekannte Regel besagt, dass sich die Kosten zur Behebung eines Fehlers und somit die einer notwendigen Änderung von Schritt zu Schritt des Produktlebenszyklus verzehnfachen. Somit ist es von großer finanzieller Bedeutung, einen Fehler zum frühestmöglichen Zeitpunkt zu entdecken und die daraus nötig gewordene Änderung so früh wie möglich zu implementieren. [45][48]

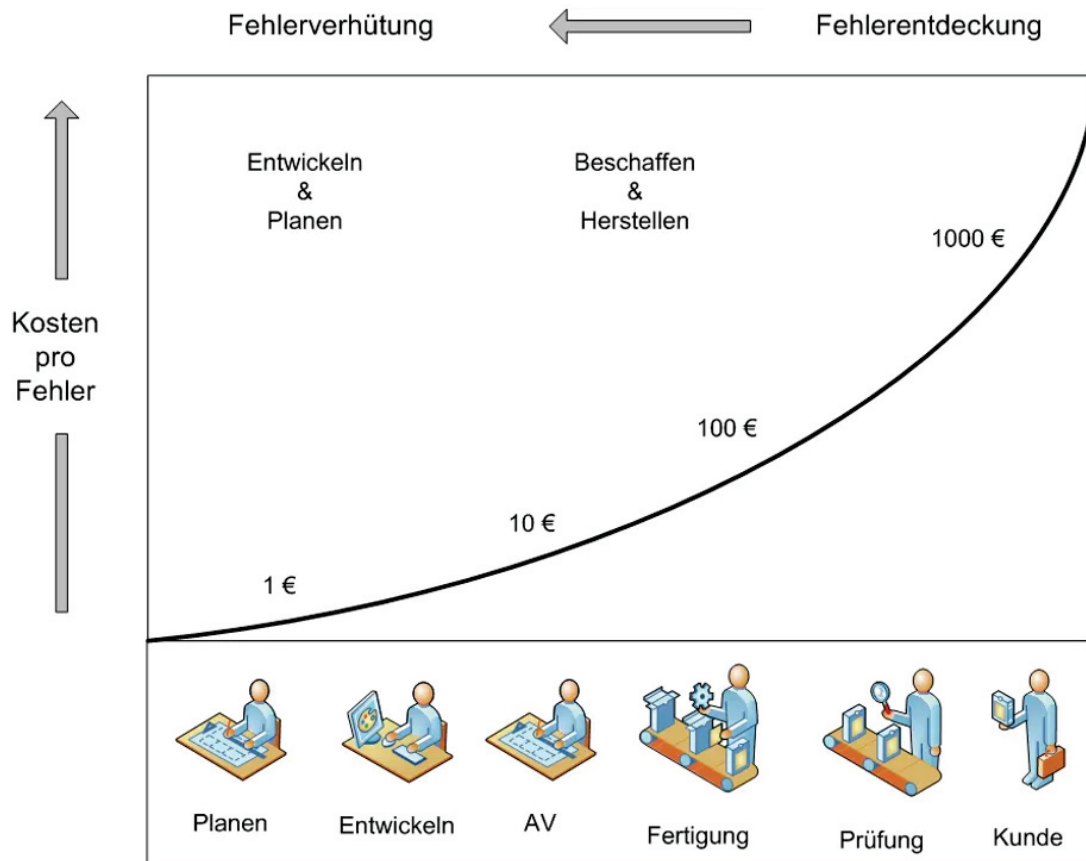


Abbildung 15: Zehnerregel. Anhand der dargestellten Kurve ist ersichtlich, dass die finanziellen Auswirkungen eines Fehlers mit dem Fortschritt eines Projektes zunehmen. Von der Planung über die Arbeitsvorbereitung (AV) bis hin zur Auslieferung an den Kunden findet ein exponentielles Wachstum der Kosten statt. [48]

Gleich wie bei der Strategie der Vermeidung spielt hier auch das Nutzen von bereits gemachten Erfahrungen in ähnlichen Projekten eine große Rolle. Es ist jedoch nicht sinnvoll, alle entstehenden Änderungen so rasch wie möglich umzusetzen, da beispielsweise in der Anfangsphase der Entwicklung meist zu wenig Wissen über die tatsächlichen Eigenschaften des Produktes herrschen. Dadurch kann es durch eine zu strikte Vorverlegung der Änderungen auch zu einer Nichterfüllung von Kundenwünschen und somit zu einem Nachteil kommen. [31][45][47][49]

- Steigerung der Effizienz

Diese Strategie dient dazu, Änderungen ohne wirtschaftlichen Nutzen (Kann-Änderungen) früh abzulehnen. Rund 23% aller Änderungen sind für die Erfüllung der gestellten Anforderungen nicht nötig und dadurch optional. Bei den Muss-Änderungen entfällt zwar die Entscheidung ob man sie durchführt, es kann jedoch bei Bestehen

von verschiedenen Möglichkeiten auf die beste Variante zurückgegriffen werden.

Des Weiteren ist es nötig, Änderungen schnell und ohne großen Aufwand umzusetzen. Dies schont vorhandene Ressourcen und führt deshalb auch zu einer Senkung der entstehenden Kosten. Hierbei empfiehlt es sich, einen standardisierten Änderungsprozess einzusetzen. [31][39][45][47]

Änderungsprozess

Wie in Abbildung 16 dargestellt, durchläuft eine Änderung einen vom weit verbreiteten PDCA-Zyklus (Plan, Do, Check, Act) abgeleiteten Kreislauf.

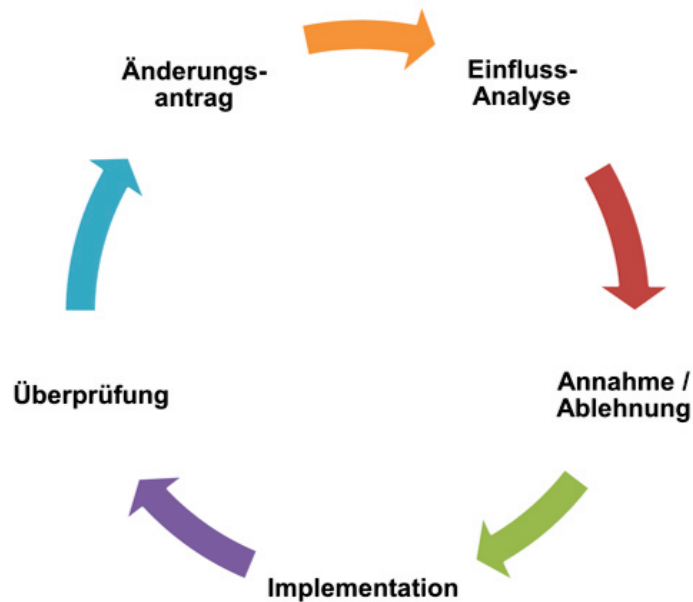


Abbildung 16: Zyklus des Änderungsmanagement. Eigene Darstellung, angelehnt an [50]

Am Beginn des Zyklus steht die Identifikation des Wunsches oder Bedarfes einer Änderung. Dies mündet in einem standardisierten Änderungsantrag, der, wie oben beschrieben, von verschiedenen Stellen eingebracht werden kann. Danach werden im Zuge der Einflussanalyse (im englischen auch als impact analysis bekannt) die technischen und wirtschaftlichen Auswirkungen der gewünschten Änderung eruiert und bewertet. Es können auch verschiedene Alternativen gegeneinander abgewogen und somit die günstigste ausgewählt werden. Diese erste Einschätzung der entstehenden Kosten und Auswirkungen wird von allen beteiligten Abteilungen, wie beispielsweise Entwicklung, Vertrieb, Einkauf und Produktion

abgegeben. Aufgrund dieser Stellungnahmen trifft in den meisten Fällen die Projektleitung zusammen mit den Auftraggebern die Entscheidung, ob die Änderung umgesetzt werden soll. Falls es zu einer negativen Entscheidung kommt, wird der Zyklus automatisch abgebrochen und es kommt zu keinem Umsetzen der Änderung. Bei positivem Ausgang wird mit der Umsetzung und Implementierung der Änderung begonnen. Dies kann beispielsweise nach dem Schema eines V-Modells ablaufen. Als letzte Phase wird die Änderung, ihre Umsetzung sowie deren Auswirkungen analysiert und mit dem Soll-Zustand verglichen. Dies dient primär zur Feststellung der positiven Abwicklung und dem Lernen aus der Änderung. [31][51]

Durch die immer komplexer werdenden Anforderungen an die Industrie und Forschung, egal ob es sich beispielsweise um die Textil-, Automobil-, Flugzeug- oder Medizinproduktebranche beziehungsweise Forschung handelt, wird es immer wichtiger, über den eigenen Tellerrand zu blicken und möglicherweise bereits angewandte oder verbreitete Forschungs-, Entwicklungs- oder Produktionstechniken und Know-How zu nutzen und für den eigenen Bedarf zu adaptieren [52]. Diese Vorgehensweise ist als Transferinnovation bekannt und spart sowohl Arbeitszeit und -aufwände, als auch in weiterer Folge Geld.

1.3 Transferinnovation

Bereits in den 30er Jahren des vorigen Jahrhunderts stellte der 1883 in Triesch, Mähren geborene Joseph Schumpeter [53] fest, dass die meisten Innovationen eine Kombination aus bereits bestehendem und verbreitetem Wissen sind [54].

In Abbildung 17 sind die einzelnen Kombinationsmöglichkeiten der Transferinnovation zwischen Wissenschaft und Industrie ersichtlich. Es ist sowohl ein Wissenstransfer zwischen rein wissenschaftlich tätigen Unternehmen und Institutionen wie beispielsweise Universitäten oder Forschungseinrichtungen, als auch eine Zusammenarbeit von Forschung und Industrie möglich. Hierbei kann eine auf den Ursprung des Know-Hows hinweisende Unterscheidung getroffen werden.

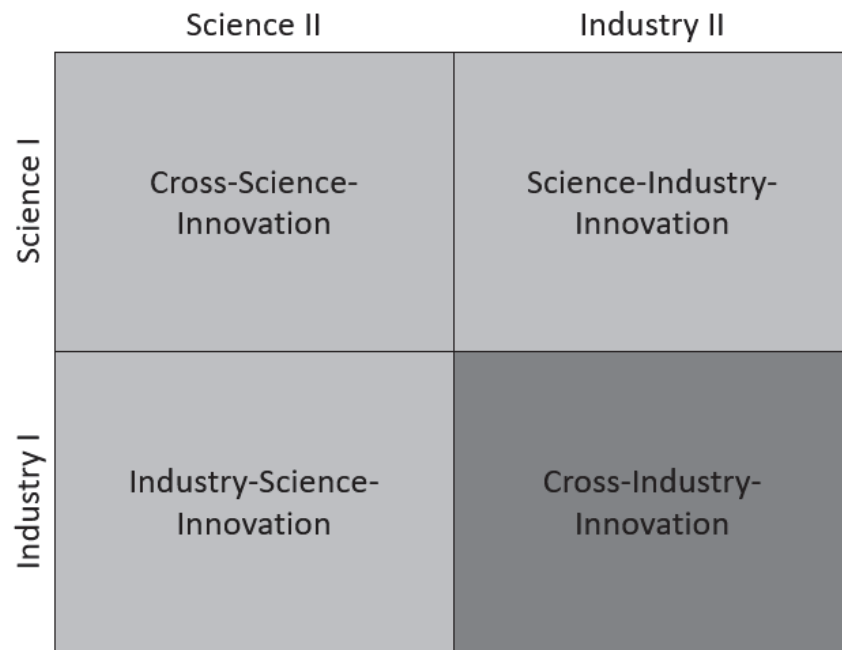


Abbildung 17: Möglichkeiten der Transferinnovation. Eigene Darstellung, angelehnt an [55]

Der Transfer zwischen Forschungseinrichtungen, auch Cross-Science-Innovation genannt, ist allgemein bekannt. Ein Beispiel hierfür ist die durch Wissen der klassischen Physik unterstützte Astronomie. Der Wissenstransfer von der Forschung in die Industrie wird weit häufiger als der umgekehrte Austausch beobachtet. Dies ist der Tatsache geschuldet, dass die in der Wirtschaft tätigen Unternehmen meist einer Geheimhaltung unterliegen. Ein weiterer Grund hierfür ist eine mangelnde Übertragbarkeit von wirtschaftlich nutzbaren Innovationen zurück in den Forschungsbereich. [55]

Die vierte Möglichkeit ist Transfer zwischen einzelnen Industrieunternehmen. Diese Möglichkeit, auch unter Cross-Industry-Innovation bekannt, ist der Hintergrund für diese Arbeit.

1.3.1 Cross-Industry-Innovation

„Die größte Chance, einen Durchbruch zu erreichen, besteht, indem man Ideen aus verschiedenen Branchen miteinander kombiniert“ [56].

Somit bedarf es weniger einer Grundlagenforschung als der Möglichkeit, bereits vorhandenes Wissen aus anderen Branchen für sich selbst und die eigene Produktentwicklung zu

nutzen. Als Beispiele für so einen Wissenstransfer können hier der Einsatz eines, für die Formel Eins entwickelten Stoßdämpfers, dessen Technologie von der Schuhindustrie (Nike Shox) weiterentwickelt und so als Schockabsorber in Laufschuhe eingebaut und verwendet wird und der Schraubendreher WORX Twist & Go, der, wie in Abbildung 18 ersichtlich, in seinem Design und seiner Funktion einem Revolver ähnelt, genannt werden. [57][58][59]

Dieser Wissenstransfer muss nicht nur einzelne Produkte oder Technologien betreffen, es ist auch ein Austausch oder eine Wiederbenützung von einzelnen Prozessen und Prozessschritten bis hin zu Denkweisen und Konzepten möglich. Dies kann der Überwindung etwaiger entstandener Denkbarrieren und zu einem Beschleunigen einzelner Entwicklungsschritte oder der gesamten Entwicklung eines Produktes dienen. [60]



Abbildung 18: Schraubendreher WORX & Go mit Revolverdesign [61]

1.4 Eingrenzung der Branche

Diese in den vorhergehenden Kapiteln beschriebenen Methoden ermöglichen eine Vielzahl von Möglichkeiten und Herangehensweisen in der Entwicklung. Somit ist auch selbstverständlich klar, dass es zu diversen Unterschieden in der Entwicklung kommen kann. Diese Tatsache kann sowohl branchenintern als auch branchenübergreifend auftreten und ist somit auch zwischen der Medizintechnik- und der Automobilbranche möglich.

In dieser Arbeit wird auf die Entwicklung eines sogenannten mechatronischen Systems eingegangen. Darunter versteht man, wie in Abbildung 19 ersichtlich, das Zusammenspiel und die Mischung aus Mechanik, Elektronik und Informatik. [62]

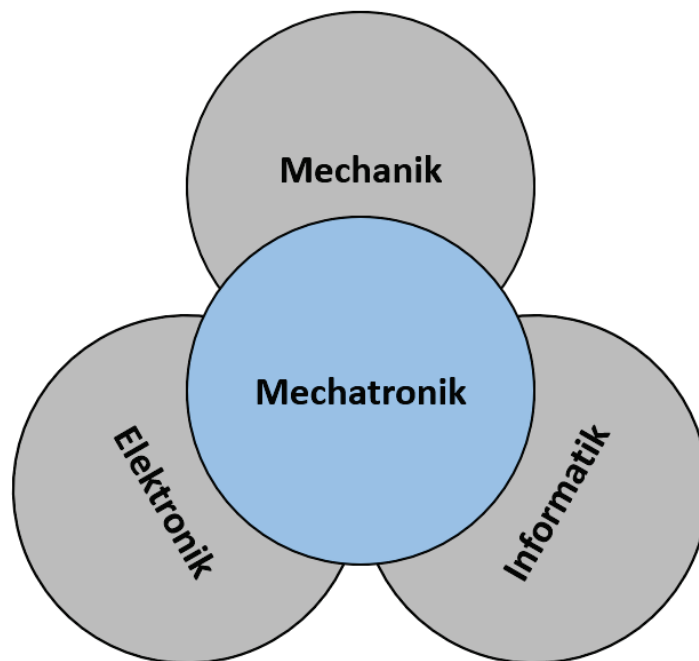


Abbildung 19: Mechatronik, bestehend aus Mechanik, Elektronik und Informatik. Eigene Darstellung, angelehnt an [62]

2 Aufgabenstellung

Ziel dieser Diplomarbeit ist es, den Entwicklungszyklus sowohl im Bereich der Medizintechnik als auch der Automobilbranche zu analysieren und darin bestehende Unterschiede zu beschreiben. Es sind einzelne Aspekte der Entwicklung miteinander zu vergleichen und daraus etwaige Synergiemöglichkeit abzuleiten. Vor- und Nachteile sind nach Gegenüberstellung und Vergleich abzuschätzen.

Das Hauptaugenmerk wird hierbei auf Standpunkte der funktionalen Sicherheit und der Beobachtung nach Inverkehrbringen (PMS - Post-Market Surveillance) in der Automobil- und Medizintechnikbranche gelegt, wobei Synergien für die jeweilige andere Branche untersucht und bewertet werden.

3 Methoden

Um die zuvor genannten Themen zu erarbeiten und die Fragen zu beantworten, wurde eine Literaturrecherche durchgeführt.

Diese Recherche fand mit Unterbrechungen im Zeitraum von Juni 2021 bis Mai 2022 statt. Diese Form der Informationserhebung wurde sowohl in der Bibliothek der Technischen Universität Graz, der Karl-Franzens-Universität, sowie der Medizinischen Universität Graz durchgeführt. Neben den soeben erwähnten Orten wurden auch online Datenbanken, wie beispielsweise der Springer Verlag oder Google Scholar zur Recherche herangezogen.

Es wurde nach sämtlichen, den Entwicklungszyklus von Medizintechnik als auch Kraftfahrzeugen betreffenden Begriffen wie beispielsweise Produktlebenszyklus, Vorgehensmodelle, Änderungsmanagement, Agilität und jeglichen Kombinationen aus diesen Ausdrücken gesucht.

Neben dieser Literaturrecherche bestand zusätzlich die Möglichkeit, einen Einblick in die Entwicklungstätigkeit des Grazer Medizintechnikherstellers Tyromotion GmbH zu bekommen. Hier wurde beispielsweise durch ein sehr informatives Gespräch im Februar 2022 die aktuelle Herangehensweise und Prozesse der Entwicklung besprochen und die möglichen Verbesserungsmaßnahmen erörtert. Diese Maßnahmen sind ein Teil der Arbeit.

Zusätzlich fand ein Großteil des Austausches mit Experten der Entwicklung der Magna Powertrain GmbH & Co KG in Lannach statt.

Diese rein mündlich geführten Gespräche mit adäquaten Quellen zu versehen war eine der Schwierigkeiten dieser Arbeit.

4 Ergebnisse

Der Umfang dieser Arbeit erlaubt es nicht, jeden möglichen Unterschied zwischen der Entwicklung von Medizingeräten und Kraftfahrzeugen darzustellen. Durch die, von dem Medizintechnikhersteller Tyromotion GmbH eingeräumten Möglichkeit, einen Einblick in die Entwicklung und Herstellung von Medizinprodukten zu bekommen, wird der Fokus unter anderem auf einen, für dieses Unternehmen wichtigen Unterschied gelegt. Dieser Unterschied beschreibt insbesondere den Einsatz von Analysen während der Entwicklung und deren Einfluss auf die Reduktion von fehlerbedingten Ausfällen bei bereits verkauften oder in Serienproduktion übergegangenen Produkten. Diese Ausfälle und deren Behebung sind durch das späte Auftreten im Produktlebenszyklus sehr kostenintensiv. Die Ursachen für diese technischen Probleme könnten durch die in den Normen der Automobilindustrie geforderten Analyse-Methoden früh erkannt und behoben werden.

4.1 Forderung des Einsatzes von Analysen

Obwohl die Entwicklung von Medizingeräten durch etliche Normen und Vorschriften geregelt ist, wird in diesen nicht explizit die Anwendung beziehungsweise der Einsatz einer bestimmten Analysemethode gefordert. In der Norm für Risikio management bei Medizinprodukten (ISO 14971) ist zwar der Satz

„Risk analysis shall be performed for the particular medical device as described in 4.2 to 4.4. The implementation of the planned risk analysis activities and the results of the risk analysis shall be recorded in the risk management file.“ [63]

zu finden, es ist aber keine explizite Aufzählung der durchzuführenden Analysemethoden vorhanden. [63]

In der Automobilbranche hingegen ist es seit einigen Jahren per Standard erforderlich, Analysen durchzuführen. Eine dieser geforderten Methoden ist die der FMEA. An dieser Stelle sei besonders der Band 4 des Verbandes der Automobilindustrie (VDA) erwähnt, in dem unter anderem die explizite Forderung einer FMEA verankert ist. [64]

FMEA

Die Fehlermöglichkeits- und Einflussanalyse ist eine der gängigsten Methoden, um Einzelfehler und deren Risiken zu entdecken und zu analysieren. Unter einem Einzelfehler oder auch „Single Point of Failure“ genannt, versteht man den Ausfall oder die Inkorrektheit einer einzelnen technischen Komponente wie beispielsweise eines Signals, das zu einem Ausfall des gesamten Systems führt. Fehler, die auf Kombinationen von Ausfällen zurückzuführen sind, werden in anderen Analysen, wie beispielsweise einer Fehlerbaumanalyse (FTA) betrachtet. Um Schwerpunkte der Vermeidung festlegen zu können, ist es möglich und üblich, Risiken dieser Fehler zu priorisieren. [64][65]

Ein extremes Beispiel hierfür ist die FMEA-Methode der Norm für funktionale Sicherheit im KFZ-Bereich (ISO 26262). Hier wird nicht die allgemein genutzte Einteilung mittels Risikoprioritätsszahl (RPZ) verwendet, sondern es findet eine einfache Trennung in sicherheitskritische und nicht sicherheitskritische Fehlerfolgen statt. [66]

Aufgrund der Tatsache, dass eine FMEA branchenübergreifend einen nahezu gleichen, in der ISO 60812 festgelegten, Prozess durchläuft, wird in dieser Arbeit auf den Ablauf und die Herangehensweise nicht näher eingegangen. [67]

4.2 Modell der funktionalen Sicherheit im Kraftfahrzeug

Die zweite in dieser Arbeit beschriebene Gruppe von Unterschieden betrifft die Möglichkeit zur Übernahme einzelner Aspekte und Herangehensweisen aus der Norm für funktionale Sicherheit im Automobilbereich (ISO 26262). Wobei die grundsätzliche Definition für Sicherheit in beiden Branchen sehr ähnlich ist und in den Normen mit „Abwesenheit unververtretbaren Risikos“ beschrieben wird. [63][66]

Ein Auszug und Vergleich der auf Qualität bezogenen, in den beiden Branchen eingesetzten und verwendeten Normen ist in Tabelle 1 zu finden. [68]

| Bereich | Automobilbranche | Medizintechnik |
|---|------------------|-------------------|
| Qualitätsmanagement System (branchenübergreifend) | ISO 9001 | ISO 9001 |
| Qualitätsmanagement System (branchenspezifisch) | IATF 16949 | ISO 13485 |
| Lebenszyklus-Management | ISO 26262 | EN 62304 (für SW) |
| Sicherheits - / Risikomanagement | ISO 26262 | ISO 14971 |

Tabelle 1: Vergleich der verwendeten QM-Normen beider Branchen. Eigene Darstellung, angelehnt an [68]

Anforderungen an das generelle Qualitätsmanagement aus der ISO 9001 oder den branchenspezifischen Normen sind nicht Teil dieser Betrachtung.

Die funktionale Sicherheit, kurz FuSi genannt, beschäftigt sich mit der Sicherheit eines Systems, die von der korrekten und fehlerfreien Funktion und deren Risiko minimierenden Schritten und Maßnahmen abhängt. Im Unterschied zum Qualitätsmanagement werden hier nicht Fehlfunktionen die zum Ausfall des Gerätes führen können, sondern Fehler, die möglicherweise einen schwerwiegenden, wenn nicht sogar tödlichen Schaden zur Folge haben können, betrachtet. [66]

Die Norm stammt von der allgemeinen und branchenunspezifischen IEC 61508 ab, von der sich, wie in Abbildung 20 ersichtlich, einige anwendungs- und branchenspezifische Normen abgeleitet haben. [66][69]

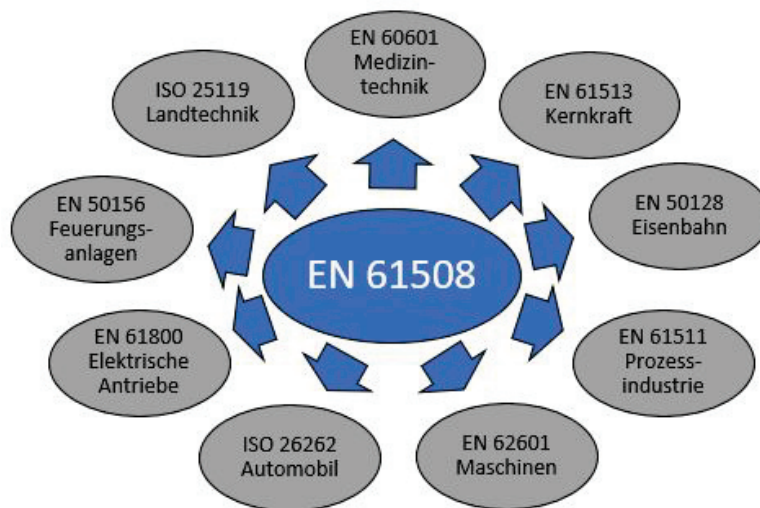


Abbildung 20: Branchenspezifische Ableitungen der IEC 61508. Eigene Darstellung, angelehnt an [69]

Die daraus abgeleitete Norm für Medizintechnik EN 60601 ist weniger eine Verfahrensnorm, als eine Norm für Forderungen an Sicherheit und Ergometrie. Dies ist ein fundamentaler Unterschied zur ISO 26262, die nicht nur einzelne Schritte, sondern den gesamten Lebenszyklus und ein eigenes Vorgehensmodell zur Entwicklung eines als sicherheitsrelevant eingestuften Systems oder Teiles davon beschreibt. [66][70]

Die Norm für Kraftfahrzeuge ISO 26262 grenzt hierbei die rein mechanisch wirkenden Teile, wie beispielsweise Wellen oder Zahnräder aus. Es handelt sich somit um eine Norm für elektronische und elektrische und damit auch programmierbare Systeme oder Teile davon. Diese werden in der Literatur allgemein als E/E-Systeme bezeichnet.

Unter einem System versteht man in diesem Zusammenhang, wie in Abbildung 21 dargestellt, den Zusammenschluss aus mindestens einem Sensor, einem Steuergerät und einem Aktuator. [66][68][70]

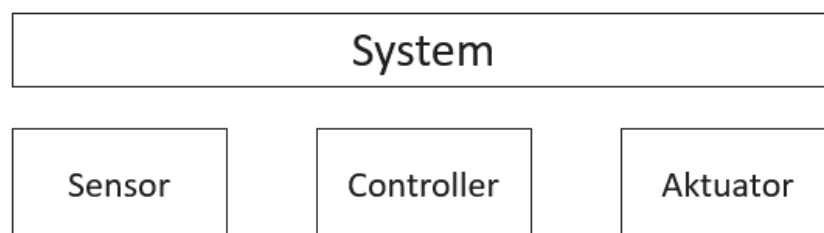


Abbildung 21: Bestandteile eines Systems. Eigene Darstellung, angelehnt an [66]

4.2.1 Unterschiede in der Klassifizierung

In der Medizintechnik sind mehrere, von der Art des Gerätes und Systems abhängige Risiko- beziehungsweise Sicherheitsklassen zu finden, wobei die Sicherheitsklassen nur die Software betreffen. Es wird in klassische Medizinprodukte (MDR), Medizinprodukte für In-vitro-Diagnostik (IVDR) und Software als Medizinprodukt (SW) unterschieden. Die Einteilung der SW wird unabhängig von der Risikoklasse eines Medizinproduktes getroffen und hat größtenteils Einfluss auf die Form der Dokumentation. Ein Ablaufdiagramm hierzu ist in Abbildung 22 dargestellt. [20][71][72][73]

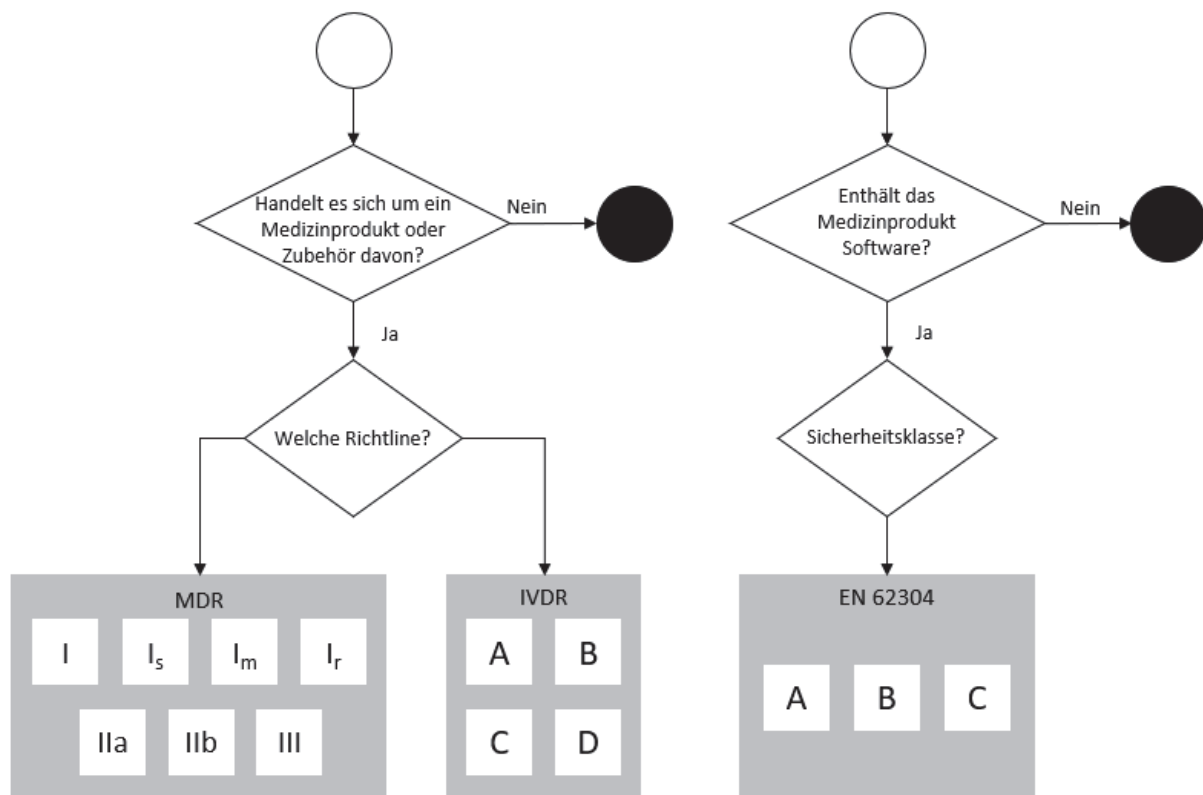


Abbildung 22: Ablaufdiagramm der Klassifizierung von Medizinprodukten, eigene Darstellung, angelehnt an [71]

Für diese drei Bereiche gibt es jeweils von den anderen Bereichen unabhängige und in ihrem Schweregrad unterschiedlich zu bewertende Risiko- beziehungsweise Sicherheitsklassen. An dieser Stelle ist anzumerken, dass die Sicherheitsklassen der Software hauptsächlich einen Einfluss auf deren Dokumentation sowie Architektur hat. Ein Versuch, diese verschiedenen Stufen gegenüber zu stellen und gemeinsam in einer Darstellung abzubilden, ist in Tabelle 2 zu finden. [20][72][73]

| Risiko | MDR | IVDR | SW |
|---------|-----|------|----|
| minimal | I | A | A |
| Niedrig | IIa | | B |
| Mittel | IIa | B | |
| Erhöht | IIb | C | C |
| Hoch | III | D | |

Tabelle 2: Risiko- beziehungsweise Sicherheitsklassen in der Medizintechnik. Eigene Darstellung, angelehnt an [20][72][73]

Im Gegensatz hierzu ist im Automobilbereich ein einheitliches System der Klassifizierung zu finden. Mit Hilfe der ISO 26262 werden einzelne Systeme oder Teile davon in Sicherheitsklassen, die sogenannten „Automotive Safety Integrity Level“, kurz ASIL genannt, eingeteilt. Diese Level geben den Grad der zu erreichenden Makellosigkeit gegenüber Fehlern an und können in die Klassen A (niedrig) bis D (höchste Sicherheitsklasse) unterteilt werden. Diese Einteilung wird im Zuge einer Gefahren- und Risikoanalyse getroffen und dient dazu, Maßnahmen zu setzen um schwerwiegende Fehler zu vermeiden oder diese zumindest zu entdecken und bei Auftreten einen sogenannten sicheren Zustand einzunehmen. In diesem ist zwar ein Teil der Funktion nicht mehr möglich, es kann durch diese Art der kontrollierten Abschaltung aber eine Gefahr vermieden werden. [66]

Als Beispiel hierfür könnte eine, in dem bei jedem Motorenstart durchgeführten Startup-Tests festgestellte Fehlfunktion des Antiblockiersystems (ABS) angeführt werden. Durch den erst ab einer gewissen Geschwindigkeit relevanten Einfluss des Bremsens ohne blockierende Räder, kann beispielsweise die maximale Geschwindigkeit bis zum Beheben des Fehlers in einer Werkstatt auf einen gewissen Wert reduziert werden.

Gefahren- und Risikoanalyse (HARA)

Im Zuge einer sogenannten Gefahren- und Risikoanalyse, auch HARA (Hazard Assessment and Risk Analysis) genannt, werden einzelne Systeme auf ihr Risiko untersucht und dadurch die ASIL-Stufe und ihre Sicherheitsziele bestimmt. Diese Einteilung ist, wie in Tabelle 3 ersichtlich, nach der Bestimmung der drei Parameter „Schwere des Schadens (S für Severity)“, „Häufigkeit der Fahrsituation (E für Exposure)“ und „Beherrschbarkeit durch die lenkende Person (C für Controllability)“ möglich. Diese Einteilung ähnelt in der Form zwar der Software-Sicherheitsklassifizierung der EN 62304 in die Klassen A bis C, ist aber im Gegensatz zur Medizintechnik nicht nur für Software sondern auch für Hardware und somit Elektronik anwendbar. [66][74]

Unter einem Sicherheitsziel versteht man eine Sicherheitsanforderung der obersten Betrachtungsebene eines Systems. [66]

| Severity | Exposure | Controllability | | |
|----------|----------|-----------------|--------|--------|
| | | C1 | C2 | C3 |
| S1 | E1 | QM | QM | QM |
| | E2 | QM | QM | QM |
| | E3 | QM | QM | ASIL A |
| | E4 | QM | ASIL A | ASIL B |
| S2 | E1 | QM | QM | QM |
| | E2 | QM | QM | ASIL A |
| | E3 | QM | ASIL A | ASIL B |
| | E4 | ASIL A | ASIL B | ASIL C |
| S3 | E1 | QM | QM | ASIL A |
| | E2 | QM | ASIL A | ASIL B |
| | E3 | ASIL A | ASIL B | ASIL C |
| | E4 | ASIL B | ASIL C | ASIL D |

Tabelle 3: ASIL-Stufen. Eigene Darstellung, angelehnt an [66]

Dieses System erinnert des Weiteren auch an die Risikoabschätzung in der ISO 14971, benutzt aber einen FMEA-Ansatz. So werden die einzelnen Werte durch Aufteilen des Systems in die einzelnen Funktionen beziehungsweise Fahrsituationen und Bewerten von FMEA-Phrasen wie „Situation tritt ein obwohl nicht gewünscht“ oder ähnlichen, bestimmt. [63][66]

Einfluss der ASIL-Stufe auf die Entwicklung

Die ASIL-Klassifizierung hat einen Einfluss auf die zur Erfüllung dieser Norm notwendigen Arbeitspakete. Dies wird besonders bei Betrachtung von Abbildung 23 ersichtlich, in der die notwendige Risikoreduktion dargestellt wird. So ist der zu setzende Aufwand bei ASIL D um etliches höher, als bei ASIL A.

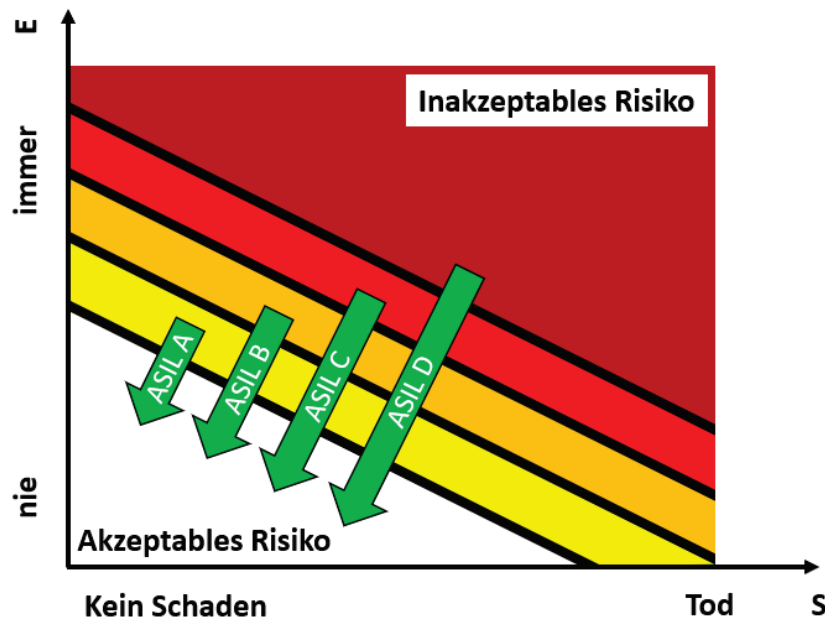


Abbildung 23: ASIL-Klassen abhängige Risikoreduktion. Um ein inakzeptables Risiko zu reduzieren, ist mit steigender ASIL-Klasse ein größerer Aufwand zu betreiben. Eigene Darstellung, angelehnt an [75]

Dieser Umstand kann beispielsweise bei der Wahl der Analysen beobachtet werden. So wird, wie in Tabelle 4 ersichtlich, bei den verschiedenen ASIL-Klassen eine unterschiedliche oder zusätzliche Analyse-Methode empfohlen. Der Grad der Empfehlung eines dieser Arbeitspakete wird wie folgt beschrieben:

- „o“ zeigt an, dass es keine Empfehlung für oder gegen ihre Verwendung für diese ASIL-Stufe gibt.
- „+“ zeigt an, dass diese Methode empfohlen wird.
- „++“ zeigt an, dass diese Methode sehr empfohlen wird.

| Methoden | | ASIL | | | |
|----------|--------------------|------|----|----|----|
| | | A | B | C | D |
| 1 | Deduktive Analysen | o | + | ++ | ++ |
| 2 | Induktive Analysen | ++ | ++ | ++ | ++ |

Tabelle 4: Nach ISO 26262:2018 empfohlene Analysen der Systemarchitektur. Eigene Darstellung, angelehnt an [66]

In diesem gezeigten Fall handelt es sich um die Analysen der Systemarchitektur, die sich in deduktive, wie beispielsweise die Fehlerbaumanalyse (FTA) oder das Ishikawa-Diagramm und den induktiven Analysen, wie die FMEA, aufteilen. [66]

4.2.2 Verwendung des W-Modells

Die ISO 26262 fordert ein eigenes Vorgehensmodell in der Entwicklung. Dies baut auf dem in vielen Branchen mit Softwareentwicklungsanteilen und somit auch der Medizintechnik implementierten und im Kapitel 1.2.1.2 Vorgehensmodelle beschriebenen V-Modell auf.

Zum Unterschied hierzu besteht es aber, wie in Abbildung 24 ersichtlich, aus einem V-Modell, das sich später in zwei verschiedene, den Hardware- und Softwareentwicklungsprozess betreffende V-Modelle aufteilt und somit als W-Modell beschrieben werden kann. Dies lässt die Rückführung von Hardware- und Softwareanforderungen auf Anforderungen an das Gesamtsystem zu. [66][76]

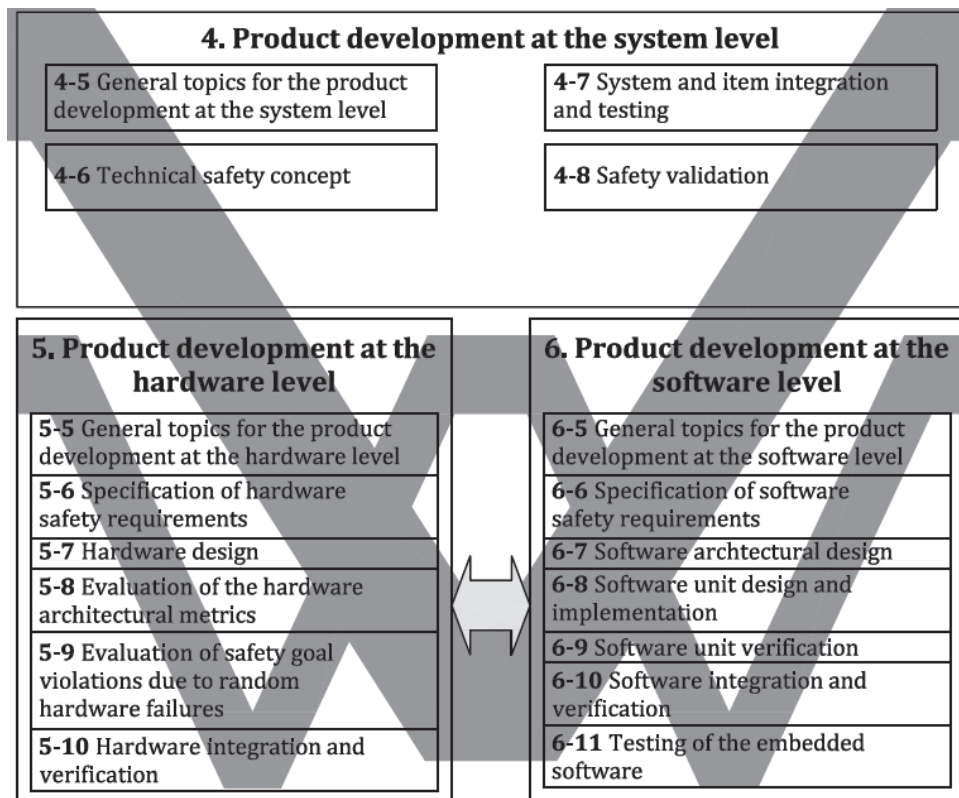


Abbildung 24: In ISO 26262 dargestelltes W-Modell [66]

Diese Aufteilung erfolgt nach dem in Abbildung 25 gezeigten Schema. [66][77]

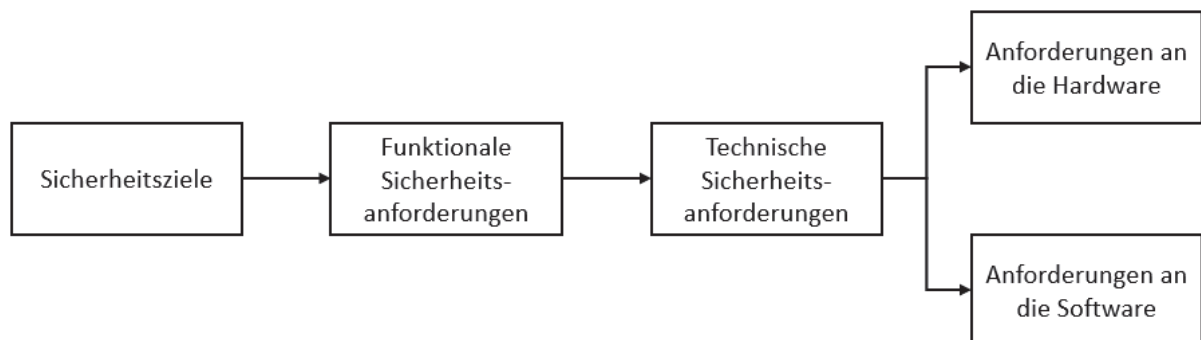


Abbildung 25: Aufteilung der Anforderungen im W-Modell. Eigene Darstellung, angelehnt an [75]

Nach Festlegung der einzelnen Sicherheitsziele in der HARA, werden daraus funktionale Sicherheitsanforderungen abgeleitet. Diese Anforderungen beschreiben, welche zur Erreichung der Sicherheitsziele nötigen Sicherheitsmechanismen umgesetzt werden müssen. Aus diesen werden im nächsten Schritt die sogenannten technischen Sicherheitsanforderungen gebildet, die festlegen, wie die einzelnen Anforderungen umzusetzen sind. Ein Beispiel

hierfür ist in der folgenden Abbildung 26 zu finden. [66][77]

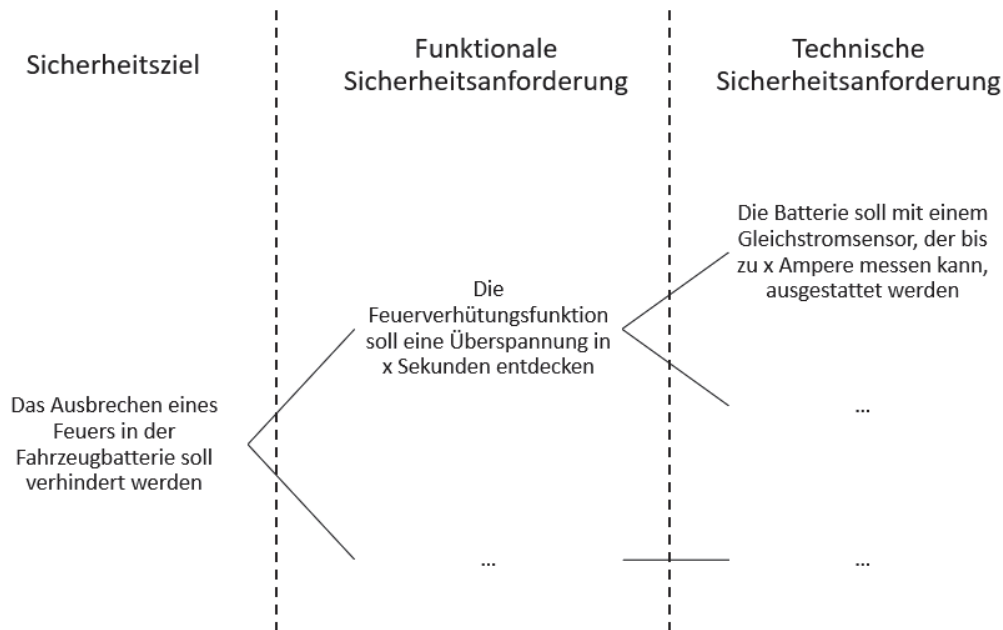


Abbildung 26: Beispiel zur Aufteilung eines Sicherheitszieles in funktionale und technische Sicherheitsanforderungen [77]

4.2.3 Möglichkeit zur Dekomposition

In der Medizintechnik und deren Regularien wird die Dekomposition, auch Dekomponierung genannt, von Risiko- beziehungsweise Sicherheitsklassen in zwei verschiedenen Bereichen angesprochen. Die EN 60601-1 spricht im Abschnitt 14.8 von Themen wie Partitionierung und Redundanz, eine klare Aussage zur Machbarkeit und Anwendung ist aber nicht vorhanden. Des Weiteren wird in der Norm für Medizingeräte-Software EN 62304, Kapitel 4.3 von einer Reduzierung der Sicherheitsklasse durch beispielsweise Hardware-Maßnahmen gesprochen. [70][74]

Die Norm für funktionale Sicherheit im Kraftfahrzeug ermöglicht nicht nur eine Dekomponierung von Software, sondern auch ausdrücklich die von Hardware. Es können, wie in Abbildung 27 dargestellt, alle Sicherheitsklassen in niedrigere Stufen aufgeteilt werden. Es ist durchaus möglich, eine mit ASIL D eingestufte Hardware in einen Teil der höchsten Klasse und einen Teil der niedrigsten Sicherheitseinstufung aufzuteilen. Dies findet vor allem bei als Plattform aufgebauten Systemen Anwendung. So kann beispielsweise ein

System, welches mit ASIL A eingestuft ist und die vorgeschriebenen Werte von ASIL D nicht erfüllt, durch einen redundanten und ausreichend unabhängigen ASIL D-fähigen Sensor-Pfad auf die gewünschte Sicherheitsklasse gehoben werden. In diesem Fall wäre die Schreibweise ASIL A(D) und ASIL D(D). Die Dekomponierung ist auch rekursiv möglich. Dies bedeutet, dass ein ASIL B(D) System weiter in zwei redundante und unabhängige ASIL A(B) aufgeteilt werden kann. [66]

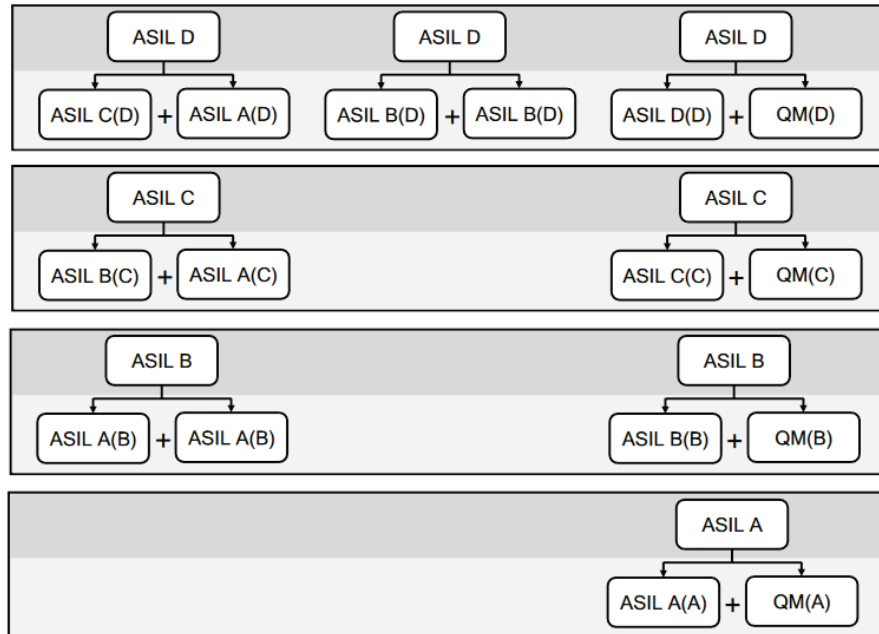


Abbildung 27: Möglichkeiten zur Dekomposition von Sicherheitsklassen der ISO 26262 [78]

Diese geforderte Unabhängigkeit kann mit einer „Dependent Failure Analysis“ (DFA) nachgewiesen werden, in der voneinander abhängige Ausfälle analysiert und somit einzelne Komponenten oder Ereignisse, die eine Verletzung der Unabhängigkeit darstellen, identifiziert und gefunden werden. Dies kann beispielsweise bei der Auswertung einer FTA festgestellt werden, in dem ein und der selbe Fehler an zwei Seiten eines UND-Gatters auftritt und in Folge dessen durch eine einzige Fehlfunktion das gesamte Sicherheitskonzept ausgehebelt werden kann. [66][76]

4.2.4 Hardware-Metriken

Die ISO 26262 stellt ab der ASIL-Stufe B die Anforderung zur quantitativen Bewertung der Zuverlässigkeit von Hardwareelementen. Dieser Begriff ist zwar in den Normen der

Medizintechnik, wie beispielsweise der ISO 14971 und der EN 60601 vorhanden, es gibt jedoch diesbezüglich weder Anforderungen, noch Definitionen von Grenzwerten und quantitativen Zielen.

In der Automobilbranche wird zwischen einzelnen Metriken und Fehlern unterschieden. Aufgrund der komplexen Berechnung der einzelnen Werte wird auf die Anführung und Beschreibung der Formeln verzichtet und auf die ISO 26262-5 verwiesen. [66]

- Single-Point Fault Metric (SPFM)

Diese Metrik gibt einen Wert für die Robustheit eines System gegenüber Einfachfehlern an. Der Wert berechnet sich aus den „Single Point Faults“ oder Einfachfehlern und den, auch unter Restfehler bekannten „Residual Faults“. Das Ergebnis gibt an, wie viel Prozent der möglichen Einfachfehler keinen sicherheitskritischen Einfluss haben.

- Single Point Faults

Diese Fehler führen zu einer sofortigen Sicherheitszielverletzung, da sie durch keinen Mechanismus abgesichert sind.

- Residual Faults

Unter „Residual Faults“ versteht man Fehler, die zu einer Verletzung des Sicherheitsziels führen, aber durch keinerlei Maßnahmen abgesichert werden können.

- Latent Fault Metric (LFM)

Hierbei wird die Empfindlichkeit der Architektur einer Hardware auf schlafende oder latente Fehler betrachtet. Das Ergebnis ist gleich wie das der SPFM zu interpretieren.

- Latent Multiple Point Faults (MPFL)

Diese nicht durch Maßnahmen abgesicherten Fehler führen in Zusammenhang mit anderen, hiervon unabhängigen Abweichungen oder Fehlern zu einer Sicherheitszielverletzung.

- Probability Metric for Random Hardware Failures (PMHF)

Dieser Wert legt quantitativ die Grenzwerte für zufällige, ein Sicherheitsziel verletzende Fehler der Hardware fest. [66][79]

Da die Berechnung dieser Werte die gesamte Hardware berücksichtigen, muss die Ausfallrate beziehungsweise Zuverlässigkeit für jedes einzelne Bauteil bekannt sein. Diese Werte werden in „Failure in Time“ (FIT) angegeben und beschreiben, wie oft ein Bauteil in 10^9 (= eine Milliarde) Betriebsstunden ausfällt. Sie können in Katalogen, wie beispielsweise den von Siemens erstellten SN 29500 gefunden werden. Neben den Ausfallraten muss auch deren Verteilung auf einzelne bauteilspezifische Fehler, wie etwa „Veränderung des Widerstandes“ oder „Kurzschluss“, bekannt sein, deren Summe immer 100% ergibt. Ein Beispiel hierfür ist in der unten angeführten Tabelle 5 ersichtlich. [66]

| Bauelement | Ausfallrate | Ausfallart | Anteil |
|------------------|-------------|------------------|--------|
| R100 (1 kOhm) | 3,0 FIT | Kurzschluss | 80% |
| | | zu klein (Drift) | 5% |
| | | zu gross (Drift) | 5% |
| | | offen | 10% |

Tabelle 5: Beispielswerte für die Ausfallrate und deren Wahrscheinlichkeit eines $1k\Omega$ Widerstandes [79]

Durch Verwendung der in der Norm angeführten Formeln können durch diese Werte die Hardware-Metriken (HW) und somit die Zuverlässigkeit einer gesamten Schaltung ausgerechnet werden. Die Grenzwerte der einzelnen ASIL-Stufen werden in Tabelle 6 dargestellt. [66]

| | ASIL A | ASIL B | ASIL C | ASIL D |
|--|--------|--------------|--------------|-------------|
| Single-Point Fault Metric (SPFM) | - | > 90% | > 97% | > 99% |
| Latent Fault Metric (LFM) | - | > 60% | > 80% | > 90% |
| Probability Metric for Random Hardware Failures (PMHF) | - | < 100 FIT | < 100 FIT | < 10 FIT |

Tabelle 6: Zielwerte der HW-Metrik in der ISO 26262 [66]

So dürfen beispielsweise für Geräte der höchsten Klasse (ASIL D) mehr als 99% aller Einzelfehler und 90% der latenten Fehler keinen sicherheitskritischen Einfluss haben. Des Weiteren darf die gesamte Schaltung maximal zehn mal in einer Milliarde Betriebsstunden ausfallen. [66][79]

Eine Methode zur Berechnung dieser Metriken ist die „Failure Modes Effects and Diagnostic Analysis“, kurz FMEDA. Diese Analyse ähnelt der FMEA, nimmt jedoch Bezug auf die Hardware des Systems. [79]

4.3 Überwachung nach dem Inverkehrbringen

Ein weiterer signifikanter Unterschied zwischen den beiden Branchen ist die in nahezu sämtlichen, die Qualität eines Medizinproduktes betreffenden Normen und Regularien verpflichtende Forderung einer Überwachung von bereits in Verkehr gebrachten Produkten an alle Hersteller von Medizinprodukten. [63][72][73][80]

Diese Forderung ist im Automobilbereich in der „EU-Verordnung über die Genehmigung und die Marktüberwachung von Kraftfahrzeugen“ Artikel 13 (7) vorhanden, in der die Forderung an die Hersteller zur Dokumentation von Vorkommnissen, Beschwerden über Risiken und Problemen bei der Nichterfüllung der gesetzlichen Vorschriften und der Unterrichtung der Händler ihrer Produkte vorhanden ist. Dies entspricht jedoch bei Weitem nicht dem Umfang der Richtlinien in der Medizintechnik. [81]

Ein Beispiel für die Komplexität dieser Maßnahmen ist in Abbildung 28 ersichtlich, in dem die einzelnen zu treffenden Maßnahmen dargestellt sind. Diese teilen sich in Überwachung beziehungsweise erarbeitete Maßnahmen durch den Hersteller und durch die Behörden auf. [72]

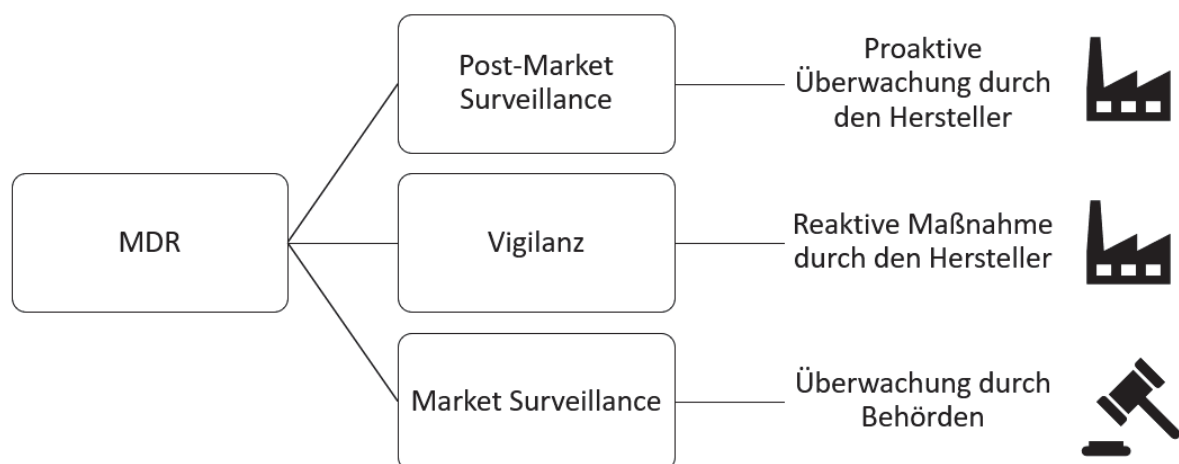


Abbildung 28: Geforderte Formen der Überwachung von Medizingeräten. Eigene Darstellung, angelehnt an [72]

Post-Market Surveillance (PMS)

Unter Post-Market Surveillance versteht man einen proaktiven Qualitätsmanagementprozess, um Informationen über Qualität und ähnliche Parameter von bereits in Verkehr gebrachten und somit benutzten Medizingeräten zu erhalten und daraus notwendige Änderungs- beziehungsweise Präventivmaßnahmen ableiten zu können. Zwar sind Risiken bereits vor dem Inverkehrbringen zu minimieren, es können jedoch einige Risiken erst im alltäglichen Gebrauch sichtbar werden.

Die Ziele der PMS können wie folgt definiert werden:

- Systematische Identifikation von Risiken im alltäglichen Gebrauch
- Überprüfung der tatsächlichen Leistungsfähigkeit des Produktes
- Auffinden von Fehlern und Aktualisierung der Nutzen-Risiko-Bewertung
- Schnelles Einleiten von Maßnahmen

Generell führt dieser Prozess, wie in Abbildung 29 dargestellt, bei entdeckten Fehlern oder Ähnlichem zu einer Änderung am Produkt oder seiner Dokumentation, wie beispielsweise der klinischen Bewertung. Nur durch diesen systematischen und kontinuierlichen Überwachungsprozess ist es den Herstellern möglich, die Abwesenheit von unvertretbaren Risiken und den erwarteten Nutzen der Funktion zu gewährleisten. [82]

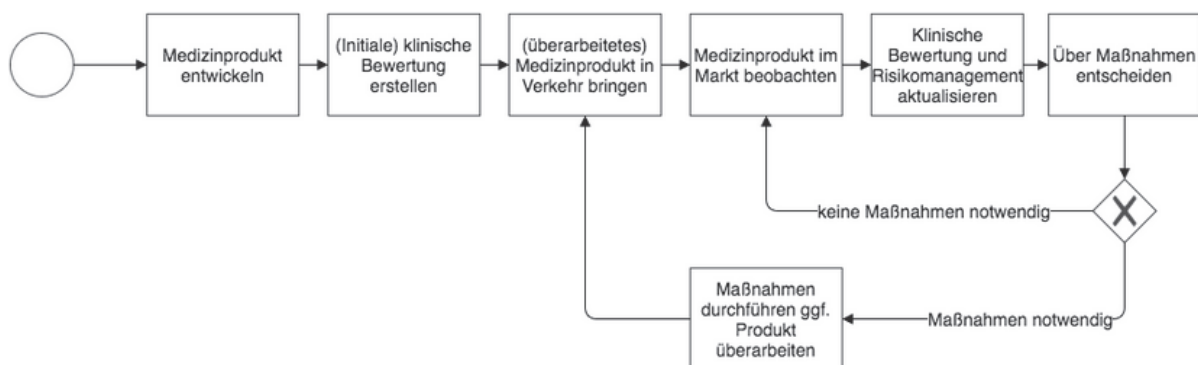


Abbildung 29: Ablaufdiagramm der Post-Market Surveillance [82]

Post-Market Clinical Follow-up (PMCF)

Wenn bei der Durchführung einer PMS eine etwaige Änderung der klinischen Bewertung notwendig wird, können durch sogenannte Post-Market Clinical Follow-up Studien klinische beziehungsweise wissenschaftliche Daten systematisch gesammelt werden. Somit kann die Verbesserung der bereits vorhandenen klinischen Bewertung eines Medizinproduktes als Ziel dieser PMCF-Studien angeführt werden. [82]

Vigilanz

Im Gegensatz zur PMS versteht man unter Vigilanz ein reaktives Meldesystem, mit dem auf Zwischenfälle reagiert werden kann. Die hier verwendeten Vorschriften und Gesetze, wie die Medizinprodukte-Sicherheitsverordnung (MPSV), lassen einen relativ geringen Freiheitsgrad bei der Erstellung des Meldesystems der einzelnen Hersteller zu. [83]

Behördliche Marktüberwachung

Neben den oben beschriebenen, von Herstellern der Produkte zu implementierenden Systemen, gibt es auch noch die vom Gesetzgeber beziehungsweise den Behörden ausgehende Marktüberwachung (Market Surveillance). Durch eine Verordnung wurden alle EU-Mitgliedstaaten dazu verpflichtet, eine Marktüberwachung durch Behörden zu garantieren und damit zur Sicherstellung der Sicherheit von bereits am Markt befindlichen Produkten beizutragen. Diese Überwachung erstreckt sich auf den gesamten Lebenszyklus eines Medizinproduktes. Als Beispiel hierfür kann die Überwachung von Herstellern und Betreibern genannt werden.

In Österreich wird dies durch das Bundesamt für Sicherheit im Gesundheitswesen geregelt. Dieses Institut ist neben der Überwachung auch für die Erfassung einzelner Vorkommnisse und deren Bewertung beziehungsweise die Definition geeigneter Änderungsmaßnahmen und deren überwachte Umsetzung verantwortlich. [20][84]

Meldepflicht

Des Weiteren besteht, bei einer durch ein Medizinprodukt ausgelöste Verschlechterung des Gesundheitszustandes oder sogar Todes, eine Meldepflicht durch den Hersteller. Dies ist der Fall bei beispielsweise einer bisher unbekannten Nebenwirkung, etwaiger auftretender Qualitätsmängel oder einer Fehlfunktion des Gerätes. Eine solche Meldung an die Europäische Datenbank für Medizinprodukte, kurz EUDAMED, muss binnen einer gewissen Frist stattfinden. Die geforderte Zeitspanne beträgt zwischen 15 Tagen bei schwerwiegenden Vorkommnissen und maximal zwei Tagen bei erheblichen Gefahren für die Allgemeinheit. Diese Meldepflicht betrifft neben allen in medizinischen Berufen tätigen Personen, wie Ärzten oder Apothekern beziehungsweise Ärztinnen und Apothekerinnen, unter anderem auch technische Sicherheitsbeauftragte in diversen Krankenanstalten, sowie Prüfstellen medizinischen Gerätes. Neben der Anzeigepflicht für Vorkommnisse, müssen auch die getroffenen Sicherheitskorrekturmaßnahmen im Feld gemeldet werden.

Nach Eingang einer solchen Meldung hat der Hersteller die Untersuchungen dieses Vorkommnisses sofort durchzuführen und eine Riskobewertung und die nötigen Sicherheitskorrekturmaßnahmen zu erarbeiten. Dies geschieht unter Überwachung durch eine Behörde.

Keine Meldepflicht besteht hingegen bei missbräuchlichem oder nicht bestimmungsgemäßem Gebrauch und bei erwartbaren und in Kauf genommenen Risiken. [20][72]

5 Diskussion

Sowohl die Literaturrecherche als auch die Gespräche mit diversen Fachleuten haben gezeigt, dass es einige, teilweise bedeutende Unterschiede zwischen der Automobil- und der Medizintechnikbranche gibt. In den folgenden Kapiteln werden die in den Ergebnissen dieser Arbeit aufgelisteten Unterschiede diskutiert.

5.1 Einsatz von Analysen

Die hier gestellte Frage, warum in einer solch komplexen und sicherheitsrelevanten Branche wie jene der Medizintechnik, keine explizite Forderung zur Anwendung einer bestimmten Analyse vorhanden ist, ist schwer zu beantworten. In diversen Ratgebern und Beschreibungen zur Entwicklung eines medizinischen Systems werden die Anwendung von Analysen, wie die der FMEA, strengstens empfohlen und detailliert beschrieben. [20]

Obwohl es bei den meisten Herstellern von Medizinprodukten ohnehin zu der Anwendung einer Analyse, wie beispielsweise einer FMEA kommt und somit der Profit für die Entwicklung offensichtlich weithin bekannt ist, werden aus gegebenem Anlass in den folgenden Punkten die meist branchenübergreifenden Vor- und Nachteile einer solchen Analyse beschrieben.

5.1.1 Vorteile des frühen Einsatzes einer Analyse

- Minimierung von Fehlern und Senkung der Kosten

Um den Nutzen einer solchen Analyse erzielen zu können, ist es nötig, sie so früh wie möglich in der Entwicklung zu erstellen und die Ergebnisse alsbaldig in den Entstehungsprozess des Produktes (PEP) einfließen zu lassen. Dies führt, wie in Abbildung 30 gezeigt, dazu, dass Fehler frühzeitig und somit noch in der Entwicklungsphase entdeckt und sofort behoben werden können und infolgedessen keine oder nur wenige Störungen in der Serienproduktion und schließlich beim Kunden auftreten. Somit kann ein langwieriger und kostenintensiver Änderungsprozess eingespart werden. Dies ist wie im Kapitel Änderungsmanagement beschrieben der Tatsache geschuldet, dass es in den klassischen frühen Entwicklungsphasen noch keine formalen Änderungen gibt. Auch eine im schlimmsten Fall auftretende, extrem kostenintensive, Image-schädigende und von allen Unternehmen der Welt gefürchtete

Rückrufaktion kann dadurch eventuell vermieden werden. [64][65]

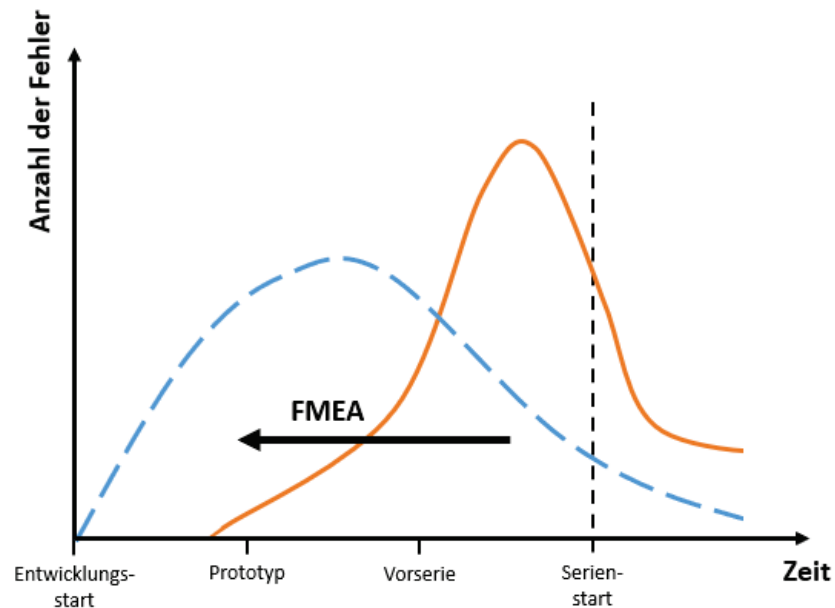


Abbildung 30: Einfluss der FMEA auf den Entdeckungszeitpunkt eines Fehlers. Die blaue Kurve beschreibt die Anzahl der entdeckten Fehler unter Anwendung einer FMEA, die orange Kurve die Anzahl bei fehlender Anwendung einer solchen Analyse. Eigene Darstellung, angelehnt an [85]

Als ein weiteres Beispiel zur Senkung der Kosten und des Aufwandes sei die bei einer Änderung von Medizinprodukten, wie beispielsweise medizinischer Software nötige Vergabe eines neuen „Unique Device Identifiers (UDI)“ erwähnt. Hierbei reichen schon kleine Änderungen, wie etwa Bugfixes von Software aus, um einen neuen Produktions-Identifizier (UDI-PI) beantragen zu müssen. Dieser Identifizier kennzeichnet jede einzelne Instanz beziehungsweise jedes einzelnen Patch eines Produktes. Bei weitschichtigen Änderungen, wie unter anderem einer Änderung der Performance oder der Sicherheit durch Anpassungen an der Softwarearchitektur oder dem Betriebssystem selbst, ist sogar eine neue Device-Identifikation (UDI-DI) nötig. Diese ist für alle Instanzen eines Produktes übereinstimmender Bauart gleich und dient als Schlüssel in der UDI-Datenbank. Durch frühzeitige Erkennung von Fehlern in der Software kann ein Großteil dieser Schritte vermieden werden. [86]

- Steigerung der Robustheit

Durch die Tatsache, dass bei richtiger Durchführung einer FMEA ein Großteil der

möglichen Fehler entdeckt wird, steigt die Zuverlässigkeit und somit auch die Sicherheit von Produkten. Dies wird auch bei Betrachtung des V-Modells sichtbar, in dem die Abhängigkeiten der einzelnen Module und Funktionseinheiten mit Hilfe einer solchen Analyse abgebildet und überprüft werden können. [20][64][65]

- **Schaffung einer Wissensbasis**

Ein weiterer Vorteil ist der Aufbau einer allgemeinen Wissensbasis im Unternehmen durch ein frühzeitiges Einbinden und Abgleichen aller wichtigen Information aus allen Bereichen des Projektteams. So führt die Anwendung einer FMEA zu einem Mit- und auch Vorausdenken der einzelnen Beteiligten, um eventuelle Schwachstellen oder Fehlerquellen frühzeitig zu erkennen oder erst gar nicht auftreten zu lassen. [64][65]

- **Rechtlicher Aspekt**

Bei korrekter Anwendung kann im Falle einer Produkthaftung durch solch eine Analyse ein Entlastungsnachweis erbracht werden. Des Weiteren ist durch solch eine dem Stand der Technik entsprechende Risikoanalyse eine Art Zusatzqualifikation in einer eventuellen Auftragsvergabe vorhanden. [64][65]

5.1.2 Nachteile einer FMEA

Es wäre falsch zu sagen, dass die Anwendung einer solchen Analyse keine Nachteile mit sich bringt.

- **Hoher Zeitaufwand**

Die Planung und Umsetzung einer FMEA bringt einen hohen Personal- und Zeitaufwand mit sich. Laut Quellenangaben kann es sich hierbei um mehrere 100 Personenstunden handeln. [65][85][87]

- **Subjektive Bewertung**

Eine FMEA ist gleich wie alle Analysen nur so gut wie das Team, welches bei der Erstellung involviert ist. Durch die Tatsache, dass in diesem Prozess beinahe die gesamte Arbeit auf Kommunikation beruht, wird Teamfähigkeit von allen Personen vorausgesetzt. Des Weiteren kann der Einsatz eines FMEA-erfahrenen Moderators nötig sein, um sowohl die Mitglieder zu schulen, als auch die richtigen Fragen in der Analyse stellen zu können. [65][85][87]

- Zeitpunkt der Erstellung

Um den größten Nutzen einer FMEA zu erreichen, sollte sie so früh wie möglich in den Entwicklungsprozess eingegliedert werden. Falls es nachträglich in einer späteren Phase des Lebenszyklus zu einer Entdeckung von Fehlern kommt, bietet sich der Einsatz einer sogenannten korrektiven FMEA an. Hierbei sind der entstehende Zeitaufwand und somit die Kosten jedoch um ein Vielfaches höher, als bei frühzeitigem Einsatz. [65][85][87]

5.2 Aspekte der funktionalen Sicherheit

Die Tatsache, dass die Entwicklung von Medizintechnik je nach Anwendungsgebiet des Systems und Gerätes durch verschiedene Normen und Richtlinien reglementiert ist, lässt je nach Betrachtungsweise unterschiedliche Interpretationen der geforderten Sicherheit zu. Dies ist dem Faktum geschuldet, dass die Definition der Klassifizierung eines Medizinproduktes mehrfach belegt ist. [71]

5.2.1 Die funktionale Sicherheit bei Einsatz von agilen Methoden

Durch die Tatsache, dass in einem heutigen Auto teilweise insgesamt mehr als 100 Millionen Zeilen von Softwarecode vorhanden sind, werden Methoden und Vorgehensmodelle gefordert, die sowohl die Effizienz steigern, als auch die Entwicklungszeit verkürzen und dadurch die Kosten senken. Diese Forderung kann durch den Einsatz einer agilen Entwicklung realisiert werden. Die in den Normen und vor allem der ISO 26262 geforderte Dokumentation legt fest, dass adäquate Prozesse zu verwenden und diese auch zu dokumentieren sind. Des Weiteren wird eine lückenlose Historie aller Änderungen, die dadurch eine Rückverfolgbarkeit gewährleistet, benötigt.

Durch den agilen Ansatz wird einer funktionstüchtigen Software mehr Wert zugemessen, als einer ausführlichen und umfangreichen Dokumentation. Des Weiteren kann es durch die unterschiedlichen Ziele zu Widersprüchen und Diskrepanzen kommen. Das Ziel der funktionalen Sicherheit und somit der ISO 26262 ist die Abwesenheit unververtretbaren Risikos, die der agilen Methoden ist die Zufriedenheit des Kunden. Eine mögliche Herangehensweise, agile Methoden trotz der Forderung einer umfassenden Dokumentation zu verwenden ist, Mischformen aus beiden Modellen zu finden. So können durch

Beiziehen eines Sicherheitsexperten beispielsweise bei dem, in der Einleitung beschrieben Daily-Scrum, die Auswirkungen auf die Sicherheit des täglichen Fortschrittes ermittelt und beurteilt werden.

Aufgrund dieser Tatsachen ist es möglich, trotz der oben genannten grundlegenden Unterschiede, den Prozess der funktionalen Sicherheit mit einem, durch benutzerdefinierte Prozesse angepassten und dadurch vom agilen Manifest abweichenden System zu kombinieren. Durch diese Fusion wird nicht nur eine kürzere Entwicklungsdauer und dadurch eine Senkung der entstehenden Kosten, sondern auch eine Unterstützung des eingesetzten W- beziehungsweise V-Modells ermöglicht. [88]

5.2.2 Einheitliche Klassifizierung und deren Auswirkung

Um ein klares Verständnis des Gefährdungspotentials von medizinischen Geräten, egal ob es sich um Software oder beispielsweise einen Defibrillator handelt, zu erhalten, wäre es sinnvoll, eine einheitliche, geräteübergreifende Form der Klassifizierung einzuführen. Hier könnte eine Mischung der Klassifizierungsmethoden und -systeme der ISO 26262 sowie der EN 62304 verwendet werden. Genau wie bei der Software, würde hier in drei verschiedene Sicherheitsklassen eingeteilt werden. Um den Bezug zu den in der Automobilbranche verwendeten ASIL-Klassen herzustellen, wird hier die Bezeichnung „Medical Safety Integrity Level“ (MedSIL) gewählt. Somit würde ein System aufgrund des erwarteten Potentials, Schäden zu verursachen, auf Systemebene klassifiziert werden. Der Unterschied, dass beispielsweise ein medizinisches Gerät Klasse IIb ist, die enthaltene Software aber Klasse A, wäre somit nicht mehr möglich. Eine Zuordnung der einzelnen ASIL-Klassen in MedSIL-Stufen ist in Abbildung 31 dargestellt. [76][89]

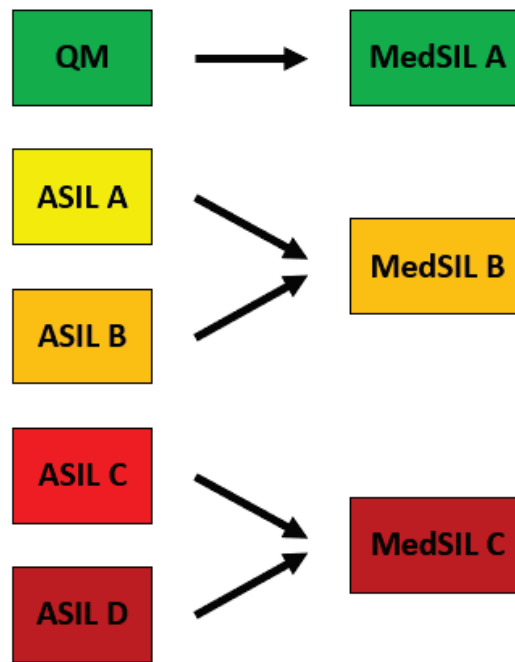


Abbildung 31: Klassifizierung von Medizintechnik anhand der ASIL-Stufen. Eigene Darstellung, angelehnt an [76]

Eine mögliche Definition der einzelnen Stufen könnte wie folgt lauten:

- **MedSIL A**
Das medizinische System kann keinen Beitrag zu einer gefährlichen und somit sicherheitskritischen Situation leisten.
- **MedSIL B**
Das medizinische System kann einen Beitrag zu einer gefährlichen und somit sicherheitskritischen Situation leisten. Der daraus resultierende mögliche Schaden ist als leichte Verletzung oder geringer einzustufen.
- **MedSIL C**
Das medizinische System kann einen Beitrag zu einer gefährlichen und somit sicherheitskritischen Situation leisten. Der daraus resultierende mögliche Schaden ist als schwere Verletzung einzustufen oder führt gar zum Tod.

Die Bestimmung dieser MedSIL-Stufen könnte ähnlich der zuvor beschriebenen HARA im Automobilbereich stattfinden. So würde das mögliche Schadensrisiko durch den Einsatz einer FMEA auf Systemebene ermittelt und daraus die entsprechende Klasse bestimmt und abgeleitet werden. Die in der ISO 14971 geforderte Risikoanalyse und Risikobewertung würde somit mittels der System-FMEA abgedeckt werden, deren Ergebnisse dann

wieder als Beitrag zu einer Konstruktions-FMEA dienen können. Diese im Laufe des Entwicklungsprozesses eingesetzten Analysen erweitern sich gegenseitig. So fließen Ergebnisse der einen FMEA in den Prozess der anderen mit ein und vice versa.

Die MedSIL-Stufen könnten, ähnlich wie im Automobilbereich, den Einsatz von verschiedenen Methoden, Ansätzen und Verfahren zur Entwicklung, Bewertung sowie der Verifizierung von Medizingeräten empfehlen beziehungsweise vorschreiben. So könnte beispielsweise als deduktive Analyse ab Klasse C die Durchführung einer Fehlerbaumanalyse deutlich empfohlen werden.[76]

Dies würde beispielsweise den zuvor beschriebenen Unterschied in der Forderung des Einsatzes von Analysen obsolet machen.

5.2.3 Dekomposition

Die im Automobilbereich in vielen Projekten gelebte Dekomposition von Sicherheitsklassen könnte, unter Einsatz der zuvor beschriebenen MedSIL-Klassen, auch im medizinischen Bereich Anwendung finden. Wie in Abbildung 32 dargestellt, bestehen, durch die Verwendung von drei, statt der vier Sicherheitsklassen im Automobilbereich, weniger Möglichkeiten zur Dekomposition. Es wäre aber genauso möglich, die Sicherheitslast auf unabhängige Systeme niedrigerer Klassen aufzuteilen. Diese Unabhängigkeit muss gleich wie im KFZ-Bereich durch eine dementsprechende Analyse überprüft werden. Ebenso wie im Automobilbereich könnte eine rekursive Aufteilung stattfinden.



Abbildung 32: Mögliche Dekomposition der MedSIL-Klassen. Eigene Darstellung, angelehnt an [66][76]

Die Vorteile einer solchen Aufteilung sind vielfältig und wären in beiden Branchen gleich. So können im Automobilbereich sowohl technische, als auch wirtschaftliche Vorteile beobachtet werden. Bei sichergestellter Unabhängigkeit der einzelnen Teilsysteme wird die

Sicherheit durch die Verwendung von redundanter Architektur gesteigert. Des Weiteren verringert sich durch die Reduktion der Sicherheitsklassen der Entwicklungsaufwand und somit die Kosten um ein Vielfaches, obwohl ein zweites, unabhängiges System entwickelt und erstellt werden muss. Um diese Kosteneinsparungen erzielen zu können, ist es wichtig, den Großteil der verwendeten Software und auch Hardware in den niedrigen Klassen, wie QM oder ASIL A zu entwickeln und nur einen kleinen, beispielsweise zur Überwachung des Systems dienenden Teil in einer hohen Sicherheitsklasse zu realisieren. Falls Teile der Software, die häufigen Änderungen ausgesetzt sind, ebenso mit einem niedrigen ASIL entwickelt werden, können hierbei weitere Entwicklungszeit und somit Kosten eingespart werden. Dies ist der Tatsache geschuldet, dass Änderungen an einem mit ASIL eingestuften Teiles der Software oder auch Hardware automatisch zu einem, in der ISO 26262 beschriebenen Änderungsprozess führen. So müssen in einer sogenannten „Impact Analyse“ alle Querverwirkungen und Einflüsse einer Änderung identifiziert und durch Festlegen einzelner geeigneter Verifikationsmaßnahmen, wie beispielsweise Tests oder Codereviews abgesichert werden.

Falls es zu einer isolierten, nur einzelne Anforderungen der Software betreffenden Aufteilung kommt, wird keine Verbesserung des Systems und somit Erhöhung der Sicherheit erzielt. Dies kann auch zu einer Erhöhung der Kosten führen, da bei einer zu geringen Betrachtungstiefe sowohl häufig alle Anforderungen in der höheren Sicherheitsklasse entwickelt werden, als auch durch die geforderte Redundanz der Arbeitsaufwand massiv steigt. Des Weiteren kann es durch zu rigoroses Dekomponieren zu einer Fehlinterpretation des Sicherheitsprozesses seitens des Entwicklungsteams und somit zu einem Sinken des Verständnisses und der Sympathie für die funktionale Sicherheit kommen. [76][90]

5.2.4 W-Modell

Die Vorteile des Einsatzes eines solchen Vorgehensmodells in der Entwicklung sind für Branchen mit E/E-Systemen (Hardware und Software) gleich. So lassen sich beispielsweise die in der Konzeptphase definierten Dekompositionen einzelner Systeme oder Funktionen ohne weitere Schwierigkeiten auf die Architektur der Hardware beziehungsweise Software übertragen. Durch den iterativen Ansatz eines solchen Modells kann beispielsweise eine Änderung an einem Softwaremodul, die eine Änderung einer Systemanforderung bedingt, ohne nennenswerte Komplikationen umgesetzt werden. Aufgrund dieser Tatsachen ist eine klare Aufteilung einzelner Anforderung in die zwei Teilbereiche und somit eine

konstruktive und unkomplizierte Entwicklungsumgebung möglich. Dies führt neben einer strukturierten Arbeitsweise auch zu einer Steigerung der Sicherheit des entwickelten Produktes. [76]

5.2.5 Metriken der Hardware

Ähnlich wie in der Automobilbranche, wäre es ein sinnvoller Ansatz, für die MedSIL-Klassen B und C alle möglichen und denkbaren Einzelfehler und ebenso latente Fehler der Hardware zu ermitteln und zu bewerten. Dies dient dazu, um die in Tabelle 7 angeführten und aus der ISO26262 übernommenen Grenzwerte einzuhalten. Für die niedrigste MedSIL-Klasse A sind, ähnlich wie für ASIL A, keine Grenzwerte vorhanden. [76]

| | MedSIL A | MedSIL B | MedSIL C |
|----------------------------------|----------|----------|----------|
| Single-Point Fault Metric (SPFM) | - | > 90% | > 97% |
| Latent Fault Metric (LFM) | - | > 60% | > 80% |

Tabelle 7: Mögliche Zielwerte der HW-Metriken der MedSIL-Klassen. Eigene Darstellung, angelehnt an [76]

Aufgrund der Tatsache, dass in beiden Branchen die gleichen Hardware-Bauteile, wie Widerstände oder μ -Controller verwendet werden, könnten die gleichen Fehlerkataloge beziehungsweise die einzelnen Ausfallraten und Grenzwerte der elektronischen Bauteile verwendet werden. Ebenso wäre es aufgrund dieser Grenzwerte für Hersteller dieser Bauteile möglich, einzelne Komponenten in beziehungsweise für verschiedene Sicherheitsklassen zu erzeugen. Diese Tatsache ist in der Automobilindustrie ebenso zu beobachten, da beispielsweise μ -Controller als ASIL B-fähig eingestuft werden. Dadurch reduziert sich der Aufwand für die Auswahl und die Entwicklung der geeigneten Komponenten einer Schaltung. [76][91]

Ein weiterer Vorteil ist, dass durch bereits bekannte Fehlerraten einzelner Komponenten etwaige Fehler oder Verbesserungsmaßnahmen bereits frühzeitig in der Entwicklung identifiziert und behoben beziehungsweise umgesetzt werden können. Somit ist auch hier eine Einsparung der Kosten aufgrund der hinfälligen Verfolgung eines komplizierten und somit zeit- und kostenintensiven Änderungsprozesses möglich. [92]

Ein klarer Nachteil dieser Metriken ist, dass alle nötigen Fehlerzustände und Ausfallraten aller verwendeten Bauteile bekannt sein müssen. Zwar ist es möglich, unbekannte Komponenten in die Analyse mit einer geschätzten Fehlerrate einfließen zu lassen, bei Mikroprozessoren ist es aufgrund ihrer Komplexität jedoch in der Praxis nahezu ausgeschlossen und nicht realisierbar. [92]

5.3 Gesetzlich geforderte Marktüberwachung

Der Unterschied in der Marktüberwachung ist einer der nennenswertesten in dieser Arbeit aufgezeigten Abweichungen beziehungsweise Unterschiede in beiden Branchen. Im Automobilbereich findet zwar neben der „EU-Verordnung über die Genehmigung und die Marktüberwachung von Kraftfahrzeugen“ auch das branchenunspezifische und in Österreich geltenden Produktsicherheitsgesetz Anwendung, es ist aber bei weitem nicht die gesetzliche Strenge aus dem Bereich der Medizintechnik vorhanden.

Dieses Produktsicherheitsgesetz regelt, wie in §1 beschrieben, „[...] Sicherheitsanforderungen an Produkte, Verpflichtungen für In-Verkehr-Bringer/innen sowie behördliche Maßnahmen mit dem Ziel, insbesondere Leben und Gesundheit von Menschen vor Gefährdungen durch gefährliche Produkte zu schützen.“. [93]

Die in der Medizintechnik geforderte Post-Market Surveillance birgt aus Sicht der Automobilbranche einige wirtschaftliche Vorteile, die aber auch für andere Branchen gelten können.

- Steigerung der Kundenzufriedenheit

Die Beobachtung der am Markt befindlichen Geräte beruht auf einer Kommunikation mit den Kunden. Dies führt zu einer Steigerung der Kundenzufriedenheit, da sichergestellt werden kann, dass die Erkennung und Behebung etwaiger Risiken im Sinne des Herstellers ist.

- Möglichkeit zur Risikovermeidung

Durch den Einsatz der Post-Market Surveillance können beziehungsweise sollen, wie zuvor beschrieben, unerwünschte Vorkommnisse identifiziert und daraus Maßnahmen zur Vermeidung des Risikos ermittelt werden. Dies führt automatisch zu einer Verringerung der Wahrscheinlichkeit des Auftretens eines solchen Fehlers und somit auch zu einer Senkung des Risikos daraus resultierender Folgen. Diese reichen von entstandenen Personen- und Sachschäden bis hin zu Produktrückrufen. Somit kann, mit Einsatz dieser Überwachung, die Wahrscheinlichkeit eines Imageschadens und auch eines wirtschaftlichen Schadens verringert werden.

- Raum für Innovationen

Diese Form der Marktüberwachung bildet eine zusätzliche Form des Marketing und der Marktforschung. Durch diese Marktbeobachtung besteht die Möglichkeit, Kundenwünsche zu erkennen und in die Entwicklung neuer Produkte beziehungsweise Geräte einfließen zu lassen. Ebenso können durch diese Erkenntnisse bereits auf dem Markt erhältliche Produkte weiter verbessert werden. Dies kann zu einer Steigerung der Wettbewerbsfähigkeit des Betriebes führen.

- Gesteigerte Qualitätssicherung

Neben der Vermeidung von Risiken besteht auch die Möglichkeit, aus den durch die Beobachtung gewonnen Daten, Produktfehler frühzeitig zu erkennen und vor Entstehung eines Schadens zu beheben. [94]

Vorteile, die nur im Bereich der Medizintechnik zu finden sind, sind in der Aufzählung nicht enthalten. Ein Beispiel hierfür wäre die Erfüllung der Anforderung an Medizingerätehersteller, ihre Produkte am Markt zu beobachten.

Die Tatsache, dass in der Automobilbranche nicht striktere Maßnahmen zur Marktbeobachtung gefunden werden konnten, ist schwer zu verstehen. Alleine in den Jahren 2011 bis 2020 mussten in den USA über 331 Millionen Kraftfahrzeuge aufgrund von sicherheitstechnischen Mängeln zurückgerufen werden. Diese Anzahl ist mehr als doppelt so hoch, wie die Zahl der im gleichen Zeitraum verkauften Neuwagen. Aus diesen Werten ist die heutige Problematik für Hersteller im Automobilbereich klar ersichtlich. Es muss mehr Energie und Zeit und somit Geld für die Änderung von Mängeln der Sicherheit von bereits verkauften Produkten, als in die Entwicklung neuer Systeme investiert werden. Dies führt

unweigerlich zu einer Stagnation der Innovation.

Der Grund für diese enorme Anzahl an Rückrufen ist mitunter die durch mangelnde globale Sicherheitsanforderungen an das Produkt mögliche Gewinnmaximierung auf Kosten der Sicherheit. Dies ist durch den Einsatz von reaktiven Qualitätsmanagementsystemen realisierbar. Somit wird die kostspielige Entwicklungsdauer reduziert und gegen eine mögliche Änderung im Nachgang unter Inkaufnahme von Verletzungen und Unfällen ersetzt. Ein Beispiel hierfür kann der 2020 notwendig gewordene Rückruf von knapp drei Millionen Fahrzeugen der Marke Toyota aufgrund von Fehlfunktionen der elektronischen Airbag-Kontrolleinheit genannt werden.

Die in der Zukunft des Automobilbaues stehende Elektromobilität und Ermöglichung autonomer Fahrfunktionen stellt weitere Anforderungen an die Marktüberwachung. So müssen einzelne Komponenten sowie das gesamte Fahrzeug vor Cyber-Angriffen geschützt werden. [94][95]

6 Schlussfolgerung

Die vorangegangenen Kapitel dieser Arbeit haben gezeigt, dass es deutliche Unterschiede in den beiden Branchen gibt. Der hauptsächliche Unterschied liegt darin, dass die Sicherheit von Produkten beziehungsweise das von ihnen ausgehende Risiko auf unterschiedliche Weise bewertet wird. Zusätzlich hierzu gibt es in der Medizintechnikbranche eine gesetzlich vorgeschriebene Marktüberwachung (Post-Market Surveillance), die so in der Branche der Automobiltechnik nicht vorhanden ist.

Dies wurde beispielsweise bei der seit zwei Jahren die gesamte Welt umfassenden und beeinträchtigenden Coronavirus-Erkrankungen sichtbar. Gleich zu Beginn haben viele Automobilhersteller die Gelegenheit genutzt, durch Erzeugung einzelner medizinischer Geräte und Utensilien wie beispielsweise Masken, die Engpässe dieser Waren zu lindern. Dabei wurden sie beispielsweise mit der für sie branchenfremden aber in diesem Fall verpflichtenden Post-Market Surveillance konfrontiert.

Somit ist es wichtig, auf diese Unterschiede hinzuweisen. Abweichungen einzelner Schritte der Entwicklungsprozesse verhindern beispielsweise die Vereinheitlichung und somit eine leichtere und verständlichere Klassifizierung von Medizintechnik. Zudem wäre auch die oben bereits erwähnte gesetzlich vorgeschriebenen Marktüberwachung zu nennen. Das Fehlen dieser Vorschrift in anderen Branchen erschwert es fachfremden Herstellern und Betrieben, in solchen Notsituationen schnell und gesetzeskonform auf Engpässe der kritischen Versorgung reagieren zu können. [96]

Um hier für die Zukunft etwaige Differenzen zu beseitigen und eine einwandfreie Sicherheit auch nach Inbetriebnahme zu gewährleisten, wäre die Einführung eines solchen verpflichtenden branchenübergreifenden Überwachungssystems sinnvoll.

Bei Betrachtung des Entwicklungszyklus wird sofort klar, dass eine Darlegung aller Unterschiede (des Entwicklungszyklus) den Rahmen einer Diplomarbeit sprengen würde. Somit wäre es in Zukunft durchaus sinnvoll, alle weiteren Aspekte und Phasen der Entwicklung zu beleuchten und miteinander zu vergleichen. Selbstverständlich besteht hierbei auch die Möglichkeit, andere Branchen beziehungsweise die in anderen Ländern geltenden Vorschriften in diese Gegenüberstellung miteinzubeziehen.

Weiterhin bleibt jedoch die Frage offen, ob das bestehende Set an Normen und Vorschriften der einen oder anderen Branche zu sichereren Produkten führt. Sollte dieser Beweis erbracht werden, wären natürlich andere Branchen dazu aufgefordert, die allgemeine Sicherheit erhöhenden Aspekte in ihre eigenen Normen zu integrieren.

Literatur

- [1] *Gabler Wirtschaftslexikon.* – <https://wirtschaftslexikon.gabler.de/definition/prozess-45614/version-383782> aufgerufen am 08.10.2021
- [2] *Gabler Wirtschaftslexikon.* – <https://wirtschaftslexikon.gabler.de/definition/produktentwicklung-45031/version-268331> aufgerufen am 08.10.2021
- [3] LEISTNER, Bastian: *Fahrwerkentwicklung und produktionstechnische Integration ab der frühen Produktentstehungsphase.* Springer Vieweg, 2019. – 3f S.
- [4] PAHL, Gerhard ; BEITZ, Wolfgang ; FELDHUSEN, Jörg ; GROTE, Karl-Heinrich: *Pahl/Beitz Konstruktionslehre.* Springer Berlin Heidelberg New York, 2019
- [5] MEYER, Helga ; REHER, Heinz-Josef: *Projektmanagement, Von der Definition über die Projektplanung zum erfolgreichen Abschluss, 2., überarbeitete Auflage.* 2019
- [6] *LOGISTIK KNOWHOW - Product Lifecycle Management (PLM).* – <https://logistikknowhow.com/supply-chain-management/product-lifecycle-management-plm/> aufgerufen am 12.01.2022
- [7] EIGNER, Martin ; ROUBANOV, Daniil ; ZAFIROV, Radoslav: Modellbasierte virtuelle Produktentwicklung. In: *Springer Vieweg* (2014)
- [8] REIMER, Lars: Systematische Auslegung von Karosseriekonzepten hinsichtlich minimaler Umweltwirkungen in einer frühen Konzeptphase. In: *AutoUni – Schriftenreihe* (2021)
- [9] KUSTNER, Jürg ; BACHMANN, Christian ; HUBER, Eugen ; HUBMANN, Mike ; LIPPMANN, Robert ; SCHNEIDER, Emil ; SCHNEIDER, Patrick ; WITSCHI, Urs ; WÜST, Roger: *Handbuch Projektmanagement, 4. Auflage.* Springer Gabler, 2019
- [10] *projektmagazin - Lastenheft.* – <https://www.projektmagazin.de/glossarterm/lastenheft> aufgerufen am 09.10.2021
- [11] BAUERNHANSL, Thomas: *Fabrikbetriebslehre 1.* Springer Vieweg, 2020. – 67f S.
- [12] *projektmagazin - Stacey-Matrix.* – <https://www.projektmagazin.de/glossarterm/stacey-matrix> aufgerufen am 13.01.2022

- [13] *proagile - Unterschiede zwischen klassischen und agilen Projekten.* – <https://proagile.de/unterschied-klassisch-agil/> aufgerufen am 13.01.2022
- [14] *The project group - Projektmanagement-Methoden Vergleich: Agil, klassisch oder hybrid?.* – <https://www.theprojectgroup.com/blog/agile-klassische-oder-hybrid-projektmanagement-methoden/#Kapitel3> aufgerufen am 14.01.2022
- [15] *fischer BLOG - Agiles Projektmanagement – Fischer goes agile.* – <https://blog.fischer-information.com/agiles-projektmanagement> aufgerufen am 14.01.2022
- [16] *Online Projektmanagemen - Wasserfallmodell.* – <https://www.online-projektmanagement.info/agiles-projektmanagement-scrum-methode/scrum-versus-wasserfallmodell/das-wasserfallmodell/> aufgerufen am 09.11.2021
- [17] *Digital Guide Ionos - Wasserfallmodell.* – <https://www.ionos.at/digitalguide/websites/web-entwicklung/wasserfallmodell/> aufgerufen am 09.11.2021
- [18] GAUSEMEIER, Jürgen ; MOEHRINGER, Stefan: NEW GUIDELINE VDI 2206 – A FLEXIBLE PROCEDURE MODEL FOR THE DESIGN OF MECHATRONIC SYSTEMS. In: *INTERNATIONAL CONFERENCE ON ENGINEERING DESIGN* (2003)
- [19] *Projekte leicht gemacht - Das V-Modell.* – <https://projekte-leicht-gemacht.de/blog/projektmanagement/klassisch/v-modell/> aufgerufen am 17.01.2022
- [20] HARER, Johann ; BAUMGARTNER, Christian: Anforderungen an Medizinprodukte. In: *Carl Hanser Verlag GmbH & Co. KG* (2021)
- [21] *projektmagazin - Agiles Manifest (Agile Manifesto).* – <https://www.projektmagazin.de/glossarterm/agiles-manifest-agile-manifesto> aufgerufen am 13.04.2022
- [22] *Science Soft - 8 Vorgehensmodelle der Softwareentwicklung: mit Grafiken erklärt.* – <https://www.scnsoft.de/blog/vorgehensmodelle-der-softwareentwicklung> aufgerufen am 12.01.2022
- [23] Scrum Grundlagen einfach erklärt, 2. Auflage. In: *InLoox* (2021)
- [24] *IONOS - Kanban.* – <https://www.ionos.at/digitalguide/websites/web-entwicklung/kanban/> aufgerufen am 19.01.2022

- [25] BURROWS, Mike: Kanban. In: *dpunkt* (2015)
- [26] *SCRUMschau - Kanban-Board - so wie es richtig sein sollte.* – <https://scrumschau.wordpress.com/2019/07/16/kanban-board-so-wie-es-richtig-sein-sollte/> aufgerufen am 19.01.2022
- [27] *Projektmanagement: Definitionen, Einführungen und Vorlagen - Scrum.* – <http://projektmanagement-definitionen.de/glossar/scrum/> aufgerufen am 18.01.2022
- [28] *projektmagazin - Scrum.* – <https://www.projektmagazin.de/glossarterm/scrum> aufgerufen am 19.01.2022
- [29] GRANDE, Marcus: *100 Minuten für Konfigurationsmanagement.* 2013
- [30] Publilius Syrus, römischer Mimen-Autor, 1. Jhdt. v. Chr.
- [31] WICKEL, Martina C.: *Änderungen besser managen - Eine datenbasierte Methodik zur Analyse technischer Änderungen.* 2016
- [32] JARRATT, T. A. W. ; ECKERT, C. M. ; CALDWELL, N. H. M. ; CLARKSON, P. J.: Engineering change: an overview and perspective on the literature. In: *Research in Engineering Design* 22 (2011), S. 103–124
- [33] HUANG, G.Q ; YEE, W.Y ; MAK, K.L: Current practice of engineering change management in Hong Kong manufacturing industries. In: *Journal of Materials Processing Technology* 139 (2003), Nr. 1, S. 481–487
- [34] NIEMERG, Conrat: *Änderungskosten in der Produktentwicklung.* (1997)
- [35] ECKERT, Claudia ; CLARKSON, P. J. ; ZANKER, Winfried: Change and customisation in complex engineering domains. In: *Research in Engineering Design* 15 (2004), 01, S. 1–21
- [36] DIN 6789-3:2011, Dokumentationssystematik – Änderungen von Dokumenten und Gegenständen, Allgemeine Anforderungen.
- [37] GILLE, Christian: *Gestaltung Von Produktänderungen Im Kontext Hybrider Produkte.* In: *Springer Fachmedien Wiesbaden GmbH* (2013)
- [38] FELDHOUSEN, Jörg ; GROTE, Karl-Heinrich: *Pahl/Beitz Konstruktionslehre, Methoden und Anwendung erfolgreicher Produktentwicklung.* In: *Springer-Verlag Berlin Heidelberg* 8. Auflage (2013), S. 111f

- [39] KÖHLER, Christan M.: Technische Produktänderungen - Analyse und Beurteilung von Lösungsmöglichkeiten auf Basis einer Erweiterung des CPM/PDD-Ansatzes. (2009)
- [40] EHRENSPIEL, Klaus: *Integrierte Produktentwicklung. Denkabläufe, Methodeneinsatz, Zusammenarbeit, 4. Auflage.* Carl Hanser Verlag GmbH & Co. KG, 2009
- [41] WILDEMAN, Horst: Die modulare Fabrik: Kundennahe Produktion durch Fertigungssegmentierung. In: *München: TCW-Transfer-Centrum* 5. Auflage (1998)
- [42] GILLE, Christan: Gestaltung von Produktänderungen im Kontext hybrider Produkte. (2013)
- [43] GEMMERICH, Marcus: Technische Produktänderungen - betriebswirtschaftliche und empirische Modellanalyse. (1995)
- [44] HAMRAZ, Bahram: Engineering change modelling using a function-behaviour-structure scheme. (2013)
- [45] LINDEMANN, Udo ; REICHWALD, Ralf: *Integriertes Änderungsmanagement.* Springer-Verlag Berlin Heidelberg, 1998
- [46] FRICKE, Ernst ; SCHULZ, Armin P.: Design for changeability (DfC): Principles to enable changes in systems throughout their entire lifecycle. In: *System Engineering* 8 (2005)
- [47] FRICKE, Ernst ; GEBHARD, Bernd ; NEGELE, Herbert ; IGENBERGS, Eduard: Coping with changes: Causes, findings, and strategies. In: *System Engineering* 3(4) (2000)
- [48] *Sixsigmablackbelt - Fehlerkosten 10er Regel Zehnerregel (Rule of ten).* – <https://www.sixsigmablackbelt.de/fehlerkosten-10er-regel-zehnerregel-rule-of-ten/> aufgerufen am 28.01.2022
- [49] ULLMAN, David G.: *The mechanical design process, 3. Auflage.* McGraw Hill Higher Education, 2003
- [50] *Smartsheet - 8 Elements of an Effective Change Management Process.* – <https://www.smartsheet.com/8-elements-effective-change-management-process> aufgerufen am 06.12.2021

- [51] HAB, Gerhard ; WAGNER, Reinhard: *Projektmanagement in der Automobilindustrie*, 4. Auflage. Springer Gabler, 2012
- [52] BADER, Karoline ; ENKEL, Ellen ; BUCHHOLZ, Charlotte ; BOHN, Lorenz: A view beyond the horizon: cross-industry innovation in the health care sector. In: *Journal Performance* 5(2): 10 (2013)
- [53] HAGEMANN, Harald: *Neue Deutsche Biographie* 23. 2007. – 755–756 S.
- [54] SCHUMPETER, Joseph A.: *BUSINESS CYCLES. A Theoretical, Historical and Statistical Analysis of the Capitalist Process*. 1939
- [55] KASCHNY, Martin ; NOLDEN, Matthias ; SCHREUDER, Siegfried: *Innovationsmanagement im Mittelstand*. Springer Gabler, 2015
- [56] Frans Johansson, Autor von „The Medici Effect“
- [57] VULLINGS, Ramon ; HELEVEN, Marc: *Not invented here : cross-industry-innovation ; die Kunst, quer zu denken*. Carl Hanser Verlag GmbH Co. KG, 2016
- [58] ENKEL, Ellen ; GASSMANN, Oliver: Creative Imitation: Exploring the Case of Cross-Industry Innovation. In: *R&D Management* (2010)
- [59] CIEŚLIK, Jerzy: Entrepreneurship in Emerging Economies. (2017), S. 157–193
- [60] KASCHNY, Martin: Cross-Industry-Innovationen: Einordnung und Potenziale. In: *Ideenmanagement: Zeitschrift für Vorschlagswesen und Verbesserungsprozesse. Band 37, Heft 2. Schmidt, Berlin, Bielefeld, München* (2011), S. 62 ff
- [61] *WORX TWIST & GO.* – <https://www.worx.com/sd-driver-screw-holder-wx2551.html> aufgerufen am 06.10.2021
- [62] In: BÖGE, Alfred ; BÖGE, Wolfgang: *Handbuch Maschinenbau: Grundlagen und Anwendungen der Maschinenbau-Technik*. Springer Fachmedien Wiesbaden, 2017, S. 643–653
- [63] *DIN EN ISO 14971:2019 Medizinprodukte – Anwendung des Risikomanagements auf Medizinprodukte*. Europäisches Komitee für Normung
- [64] *VDA Band 4, Qualitätsmanagement in der Automobilindustrie - Produkt- und Prozess FMEA*. Verband der Automobilindustrie, 2012

- [65] *Qualitätsmanagement in der Bosch-Gruppe - 14. Fehler-Möglichkeiten- und Einfluss-Analyse FMEA*. Robert Bosch GmbH, 2012
- [66] *ISO26262:2018 – Road vehicles – Functional safety*. ISO - International Organization for Standardization
- [67] *ISO60812:2018 – Failure modes and effects analysis (FMEA and FMECA)*. ISO - International Organization for Standardization
- [68] KRAMER, Anne: Automotive and medical: can we learn from each other? In: *Journal of Software: Evolution and Process* 25 (2013), Nr. 4, S. 373–379
- [69] WEKA - IEC 61508: Sicherheitsgrundnorm für funktionale Sicherheit. – <https://www.weka-manager-ce.de/funktionale-sicherheit/iec-61508-sicherheit-sgrundnorm-funktionale-sicherheit/> aufgerufen am 03.03.2022
- [70] *EN 60601-1:2006+A1:2013 Medizinische elektrische Geräte*. Europäisches Komitee für elektrotechnische Normung
- [71] *Johner Institut - Schlagwort: Klassifizierung von Medizinprodukten*. – <https://www.johner-institut.de/blog/tag/klassifizierung/> aufgerufen am 20.03.2022
- [72] *EU-Verordnung über Medizinprodukte*. – <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32017R0745&from=DE> aufgerufen am 20.03.2022
- [73] *EU-Verordnung über In-vitro-Diagnostika*. – <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32017R0746&from=DE> aufgerufen am 20.03.2022
- [74] *EN IEC 62304:2006+A1:2015 Medical device software – Software life cycle processes*. International Electrotechnical Commission
- [75] SCHNELLBACH, Adam: *Fail-operational automotive systems*. Dissertation - Technische Universität Graz, 2016
- [76] WALKER, Alastair: Functional safety certification from automotive to medical. In: *Software Quality Professional Magazine* 18 (2016), Nr. 4
- [77] *BTC embedded systems – ISO 26262 Functional Safety Requirement Types*. – <https://www.btc-es.de/en/blog/iso-26262-requirement-types.html> aufgerufen am 10.03.2022

- [78] FRIGERIO, Alessandro ; VERMEULEN, Bart ; GOOSSENS, Kees: A Generic Method for a Bottom-Up ASIL Decomposition. In: *Computer Safety, Reliability, and Security*, Springer International Publishing, 2018, S. 12–26
- [79] ZIELKE, Nico ; HÖLLE, Bernd: FMEDA - Failure Mode Effect and Diagnostic Analysis. In: *Ingenieurbüro Bernd Hölle GmbH* (2014)
- [80] *EN ISO 13485:2016 Medical devices – Quality management systems – Requirements for regulatory purposes*. Europäisches Komitee für Normung
- [81] *EU-Verordnung über die Genehmigung und die Marktüberwachung von Kraftfahrzeugen*. – <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32018R0858&from=DE> aufgerufen am 20.03.2022
- [82] *Johner Institut - Post-Market Surveillance und Überwachung der Produkte im Markt*. – <https://www.johner-institut.de/blog/regulatory-affairs/post-market-surveillance/> aufgerufen am 20.03.2022
- [83] *Johner Institut - Vigilanz-System*. – <https://www.johner-institut.de/blog/regulatory-affairs/vigilanz-system/> aufgerufen am 20.03.2022
- [84] *Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über die Vorschriften für die Akkreditierung und Marktüberwachung im Zusammenhang mit der Vermarktung von Produkten und zur Aufhebung der Verordnung (EWG) Nr. 339/93 des Rates*. – <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32008R0765&qid=1625654798846> aufgerufen am 20.03.2022
- [85] WERDICH, Martin: *FMEA – Einführung und Moderation*. Vieweg+Teubner Verlag, 2011
- [86] *Johner Institut - Unique Device Identification (UDI)*. – <https://www.johner-institut.de/blog/regulatory-affairs/unique-device-identification-udi/> aufgerufen am 20.03.2022
- [87] *ICV - Internationaler Controller Verein - Risikoanalyse FMEA*. – https://www.controllering-wiki.com/de/index.php/Risikoanalyse_FMEA#:~:text=Der%20Zeitaufwand%20f%C3%BCr%20eine%20FMEA,Teilnehmer%20produktiver%20verbracht%20werden%20kann. aufgerufen am 02.03.2022

- [88] *embitel - Can AGILE Methodology and ISO 26262 Based Functional Safety Go Hand in Hand?*. – <https://www.embitel.com/blog/embedded-blog/can-agile-methodology-and-iso-26262-based-functional-safety-go-hand-in-hand> aufgerufen am 13.04.2022
- [89] *Johner Institut - Sicherheitsklassen gemäß IEC 62304*. – <https://www.johner-institut.de/blog/iec-62304-medizinische-software/sicherheitsklassen-iec-62304/> aufgerufen am 20.03.2022
- [90] *Heicon Global Engineering - ISO 26262 ASIL Dekomposition – Chancen und Risiken!*. – <https://heicon-ulm.de/iso26262-asil-dekomposition-chancen-und-risiken/> aufgerufen am 10.03.2022
- [91] *Product Brief - XC2300 and CIC61508 Cost-Optimized Safety Computing Platform*. – <https://www.infineon.com/dgdl/Safety-Computing-Platform-XC2300-CIC61508-Product-Brief.pdf?fileId=db3a3043353fdc16013543303497315d> aufgerufen am 13.04.2022
- [92] HAPPEL, Michael ; LUX, Patrick ; SCHWARZ, David: Werkzeuge zur systematischen Durchführung einer Failure Modes Effects & Diagnostic Coverage Analysis (FME-DA). In: *Studienarbeit - Institut für Softwaretechnologie, Universität Stuttgart* (2014)
- [93] *Produktsicherheitsgesetz*. – <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20004009> aufgerufen am 13.04.2022
- [94] ZIPPEL, Claus: *Die Bedeutung von Post Market-Management in der Medizintechnik*. Springer Fachmedien Wiesbaden, 2016
- [95] *Rückruf-Trends der globalen Automobilhersteller im Langfristvergleich (2011-2021) Referenzmarkt USA*. – <https://auto-institut.de/automotiveperformance/rueckruf-trends-der-globalen-automobilhersteller-im-langfristvergleich-2011-2021-referenzmarkt-usa/> aufgerufen am 13.04.2022
- [96] *sepp.med - An alle Hersteller in der Automobilindustrie*. – <https://www.seppmed.de/an-alle-hersteller-in-der-automobilindustrie/> aufgerufen am 13.04.2022