Jürgen Malin, Bakk. techn.

Automatisierte Generierung von Zuverlässigkeitskennwerten aus elektronischen Schaltplandaten

Masterarbeit

zur Erlagung des akademischen Grades

Diplom-Ingenieur

Masterstudium Telematik

eingereicht an der

Technischen Universität Graz

Betreuer

DI Dr. Kreiner Christian
Ao.Univ.-Prof. DI Dr. Eugen Brenner

Institut für Technische Informatik
Institutsvorstand: Univ.-Prof. Dipl.-Inform. Dr. sc. ETH, Kay Uwe Römer

Graz, August 2018

Eidesstattliche Erklärung

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 identisch.

Datum	Unterschrift

Danke

. . . für die Geduld!

Allen, die viele Jahre auf diesen Abschluss warteten, mich dabei begleiteten und nicht den Glauben daran verloren.

Ich widme diese Arbeit DI Dr. Christian Kreiner, den ich als engagierten Lehrer und Mentor kennenlernen durfte. Als mein Betreuer verlor er niemals das Interesse, war geduldig und neugierig. Leider durfte er den Abschluss dieser Arbeit nicht mehr erleben.

Besonderer Dank gilt Prof. Eugen Brenner für die kurzfristige Übernahme der Betreuung und dem Institut für Technische Informatik, welches die Arbeit ermöglicht und unterstützt hat.

Vor allem danke ich meiner Frau Gabi und meinen Kindern Anna und Luca, die mich während der Umsetzung ertragen mussten.
. . . noch viiieeeel mehhh!

Zusammenfassung

Basierend auf einer adaptierten Version des *4+1 View Models* von Philippe Kruchten, befasst sich diese Masterarbeit mit der praktischen Umsetzung einer verbesserten, möglichst frühen Zuverlässigkeitsbewertung von elektronischen Baugruppen in der Entwicklung.

Nach Einführung in die Zuverlässigkeitstheorie wird der Stand der Technik für die Sammlung von Zuverlässigkeitsdaten festgestellt und eine Auswahl kommerziell verfügbarer Werkzeuge evaluiert. Die Entwicklungs- und Qualitätsprozesse eines mittelständischen Elektronikbetriebs werden im Detail untersucht und bewertet. Dieser stellt auch die Realdaten zu Instandhaltung und Reparatur ausgesuchter Baugruppen zur Verfügung, welche gemeinsam mit den vorhandenen Prozessen aus technischer und wirtschaftlicher Sicht geprüft werden. Während des gesamten Vorgangs werden Anforderungen und Empfehlungen für den Umsetzungsteil gesammelt.

Die Resultate der Untersuchungen bilden den Ausgangspunkt für zwei Umsetzungsvarianten. Der konkret ausgearbeitete Vorschlag zu einem komplett überarbeiteten, qualitätszentrierten Hardware-Etwicklungsprozess ist die erste Variante. Die zweite Umsetzung ist in Form eines computergestützten Werkzeugs realisiert. Dieses extrahiert direkt aus dem vorgegebenen Schaltplan-Entwicklungstool die notwendigen Daten, um die Zuverlässigkeitskennwerte für Standard- und auch Sicherheitsbaugruppen automatisch zu berechnen.

Abstract

Based on an adapted version of the *4+1 View Model* from Philippe Kruchten this Master's Thesis inspects and implements an as early as possible estimation of reliabilty of electronic hardware components during their development.

After a solid introduction of reliability theory, the state of the art on gathering reliability values and professional tools for reliability calculation are evaluated. The R&D and quality environment of a mid sized company is examined in detail and is the source for real life maintenance and repair data. The data and processes are reviewed from a technical and also commercial perspective. During the whole process, several requirements and suggestions for improvements are gathered and used as inputs for the implementation part.

The results are implemented in two practically usable ways. First into a recommendation of a completely overworked, quality centric R&D process. Second into the realization of a computer based tool which is capable to extract automatically required data out of a computer aided hardware design tool to predict reliability characteristics for standard and also safety environments.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1. Einführung

> For a successful technology, reality must take precedence over public relations, for nature cannot be fooled.
>
> *(Richard P. Feynman)*

Die nachfolgende Arbeit beschäftigt sich mit der Problemstellung eines qualitätsorientierten Hardware-Entwicklungsprozesses für elektronische Baugruppen. Ziel ist, auf Basis der Verfügbarkeitstheorie, ein computergestütztes Werkzeug zu entwickeln. Dieses soll dem Entwicklungsingenieur jederzeit, ohne nennenwerten Zusatzaufwand und spezielles Wissen, die Berechnung von Ausfallkennwerten auf Basis eines elektronisch erfassten Schalplans ermöglichen.

Die praktische Umsetzung erfolgt für einen konkreten Entwicklungsbetrieb und macht es notwendig, die Aufgabenstellung aus weiteren Blickwinkeln zu betrachten. Wirtschaftlichkeit und Prozesskompatibilität werden dabei im Detail untersucht.

Eine spezielle qualitative Anforderung an das Berechnungswerkzeug ist der geplante Einsatz für sicherheitstechnische Komponenten nach IEC 61508.

Der Effekt dieser Umsetzung soll sein, dass gezielt hochqualitative, langlebige Schaltungen entwickelt werden, welche trotz höchster Umgebungsanforderungen kostenoptimiert sind und gleichzeitig höchste Garantieansprüche erfüllen.

1.1. Motivation

Die Idee zu dieser Arbeit entstand während der Entwicklung und Umsetzung dreier elektronischer Baugruppen für den Einsatz im Arbeitsschutzbereich (entsprechend der Normen zur Funktionalen Sicherheit [IEC10]). Als Teil dieses Projekts waren die sicherheitstechnischen Kennwerte für die drei Baugruppen als ein notwendiger Nachweis zur Eignung zu berechnen. Auf Empfehlung der zertifizierenden Stelle wurde die Methode *Parts count* gemeinsam mit der FMEA (*Failure Modes and Effects Analysis*) gewählt und manuell auf die Baugruppen angewandt. In wochenlanger Kleinarbeit wurden die Kennwerte von insgesamt mehr als tausend Bauteilen von einem sehr geduldigen Hardware-Mitarbeiter in eine

Excel-Tabelle übertragen, die Fehlermodelle manuell in diese Tabelle eingefügt und dann durch eine zweite Person geprüft und weiter zu den Gesamtkennwerten verarbeitet.

Diese recht mühsame Vorgehensweise musste jedesmal wenn eine Änderung im Schaltplan gemacht wurde, für die entsprechenden Teile wiederholt werden. Dabei galt es besonders zu beachten, dass durch die Änderungen keine unabsichtlichen Fehler in die Tabelle übernommen, bzw. dass Lösch- und Einfügeoperationen hundertprozentig nachvollziehbar wurden. Da die Tabelle, entsprechend der Anzahl an Bauteilen, mehrere tausend Zeilen umfasste, war dies äußerst aufwändig.

Nichts desto trotz war die FMEA an sich sehr wertvoll. Es lagen erstmals bereits sehr früh in der Entwicklungsphase schlüssige Kennwerte für die MTTF (*Mittlere ausfallsfreie Arbeitszeit bis zu einem Fehler*) bzw. MTTF_D (*Mittlere Zeit bis zu einem gefährlichen Ausfall*) vor. Zusätzlich brachte der iterative Prozess der zu diesen Ergebnissen geführt hatte, neue Erkenntnisse im Schaltungsdesign und der Einschätzung von kritischen Bauteilen und Teilmodulen der Endprodukte. Aus dieser Sicht entstand die Idee einer generellen Einführung der Kennwertbestimmung als Zwischenschritt in der Hardware-Entwicklung. Dem gegenüber stand allerdings die allzu zeitaufwändige und somit schlußendlich auch zu kostenintensive Vorgangsweise.

Eine Marktrecherche im Rahmen des ursprünglichen Sicherheitsprojekts ergab, dass am Markt kein Tool verfügbar ist, welches sowohl finanziell für ein KMU leistbar und gleichzeitig recht einfach, sowohl was den Zeit- als auch den Lernaufwand betrifft, in den etablierten Prozess der Produktumsetzung und des Schaltungsdesigns integrierbar ist. Dies waren allerdings wichtige Voraussetzungen dafür, dass ein entsprechendes Tool in der täglichen Arbeit die notwendige Akzeptanz erreichen konnte. In Kapitel 3.2 auf Seite 55 wird die, für diese Arbeit erweiterte, Marktrecherche dargestellt.

Die grundsätzliche Aufgabenstellung ist damit umrissen. Die bestehende, manuelle Vorgehensweise zur Kennwertgenerierung ist dahingehend zu überarbeiten, dass zumindest folgende Ziele erreicht werden:

Zeitersparnis … bei der Entwicklung zukünftiger Sicherheitsbaugruppen bei gleichbleibender oder verringerter Fehlerquote.

Zuverlässigkeits-Verfahren Einen Rahmen zur Einführung als generelles Vorgehensmodell während der Hardware-Entwicklung schaffen, um ein frühes qualitatives Feedback für eine qualitätszentrierte Entwicklung nutzbar zu machen.

Die Vorgehensweise zur Erreichung dieser Ziele liegt in einer **Kombination** aus **Prozessänderung** und **computergestütztem Werkzeug**. Die Prozessänderun-

gen sollen die Entwickler unterstützen und nicht stören und notwendiges Spezialwissen auf einzelne Personen und Aufgaben konzentrieren. Das Werkzeug muss möglichst direkt auf der eingeführten Schaltungs-Design Software, im untersuchten Fall auf den *DxDesigner* von *Mentor Graphics*, aufbauen und so viel als möglich fehlerträchtige, manuelle Wiederholungsarbeit dem Entwickler abnehmen.

Maß für den Erfolg der Umsetzung ist der Grad der Erfüllung der folgenden Anforderungen an Werkzeug und Prozess:

Automationsgrad Manuelle Arbeiten wo möglich automatisieren und damit die Fehlerquote minimieren. Gleichzeitig den Anreiz zur täglichen Anwendung erhöhen.

Effizienz und Effektivität Den Zeitverlust durch die Kennwertgenerierung minimieren, im Idealfall sogar negieren.

Simplifikation Die Anwendung der Methode soll ohne Detailkenntnisse der Verfügbarkeitstheorie und ohne langwierige Einschulungen einfach und natürlich in den momentanen Arbeitsablauf integrierbar sein.

Dies sind gleichzeitig die Grundrequirements an diese Arbeit. Deren Erfüllungsgrad wird in Kapitel 9 auf Seite 161 bewertet.

1.2. Vorgehensmodell

Neben dem praxisorientierten Zugang zur Umsetzung des sogenannten *Prediktionswerkzeugs*, wird in dieser Arbeit eine geordnete Vorgehensweise zur Aufarbeitung der vielschichtigen Aufgabenstellung gewählt.

Die Anwendung von Vorgehensmodellen ist der Versuch einer strukturierten Herangehensweise zur Lösung (großer) Problemstellungen und Umsetzung von Prozessen. Standardisiert unter ISO/IEC/IEEE 42010 (vormals IEEE 1471) sind in der Praxis oft das V-Modell, Spice oder CMMI (*Capability Maturity Model Integration*), vor allem durch Beratungsunternehmen favorisiert, anzutreffen. Ein deutlich weniger schwergewichtiges Modell ist das *4+1 Sichten Modell* von Philippe Kruchten [Kru95], welches hauptsächlich in der Software-Architektur angewendet wird (Verwendung im Rational Unified Process).

Das Modell, wie in Abbildung 1.1 auf der nächsten Seite dargestellt, versucht, eine Problemstellung oder ein Projekt durch die Einnahme verschiedener Perspektiven möglichst vollständig zu beschreiben und damit die Basis für ein optimales Software Architektur Modell zu schaffen. In der vorliegenden Arbeit wird

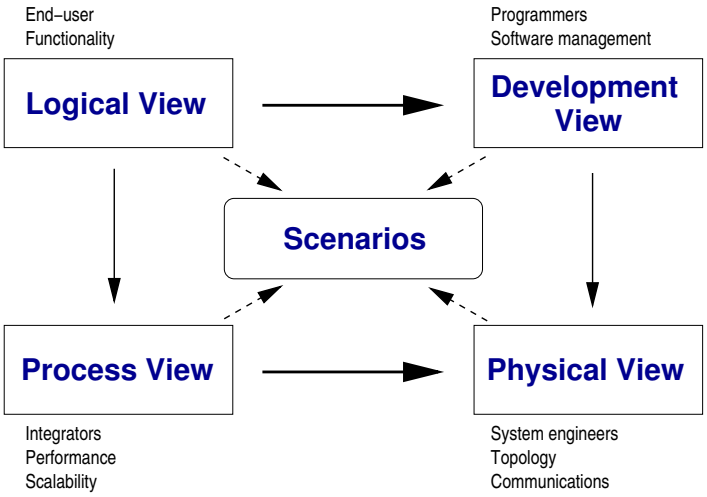


Abbildung 1.1.: Das *4+1 View Model* von Philippe Kruchten [Kru95]

die Grundidee Kruchtens aufgenommen und so adaptiert, dass das Augenmerk nicht allein auf einer sauberen Umsetzung einer Softwarelösung besteht, sondern einem gesamtheitlichen Lösungsraum Platz geschaffen wird: Einen softwaregestützten Prozess, innerhalb eines wirtschaftlich orientierten Betriebs zu etablieren (siehe Tabelle 1.1 auf der nächsten Seite).

Die Anwendung des Vorgehensmodells auf den dabei anfallenden praktischen Teil, die Definition und Implementierung des Anwendungsprogramms, wäre möglich, aufgrund der geringen Komplexität jedoch zu wenig nutzbringend. Viel mehr wird in dieser Arbeit versucht, das softwarezentrierte Modell auf die *multidisziplinäre Problemlösung der Optimierung eines Hardware Entwicklungsprozesses* unter Berücksichtigung von sämtlichen praktischen Anforderungen anzuwenden.

Perspektive	ursprüngliche Anwendung	Adaptierung
Logische Sicht	Endanwender (der SW)	Endanwender (des veränderten Entwicklungsprozess)
Entwurfs-/Entwicklungssicht	Programmierung, Wartung	Programmierung, Anwendung, Wartung, HW-Entwicklungsprozess
Prozess-/Ablaufsicht	System-Integratoren Performanz, Skalierbarkeit, Durchsatz, . . .	Entwicklungsleiter; Wirtschaftlichkeit, Erfüllung von Normen und Vorschriften, Zeitaufwand/-ersparnis, Lernaufwand, Leistungsfähigkeit

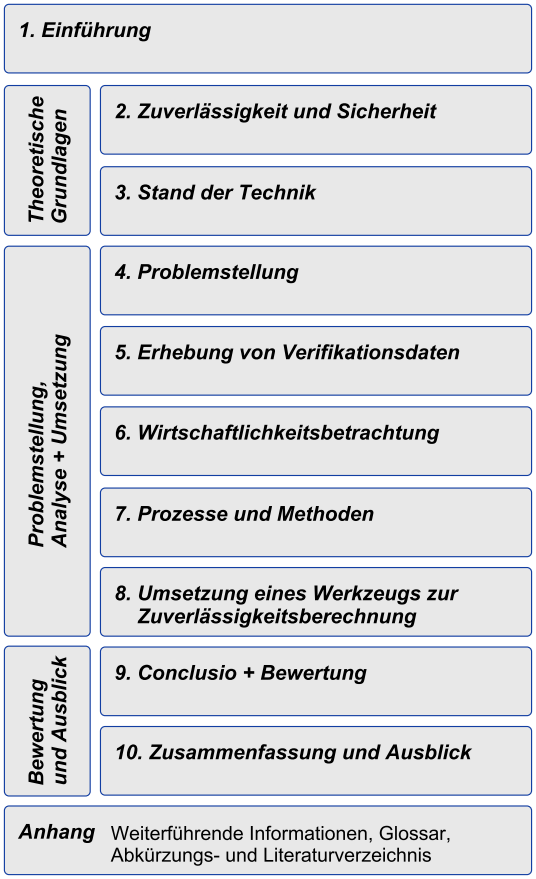
Physikalische Sicht	System- und Applikations-fachmann, Kommunikation, Verteilung, Installation, ...	zu den ursprünglichen Punkten kommt noch die Qualitätssicherung

Tabelle 1.1.: Adaptierung des 4+1 Modells - Zielgruppen und Aufgaben der vier Perspektiven

All die dargestellten Perspektiven führen im Ergebnis zu den maßgeblichen *Szenarien*, in Form von *Anforderungen (Requirements)* und *Anwendungsfallbeschreibungen (Use-Cases)*. Dabei erfolgt keine Adaptierung, wenngleich die Anwendungsfälle die Problemstellung auf unterschiedlichen Prozessebenen beschreiben.

1.3. Strukturierung

Die Masterarbeit ist wie folgt gegliedert:



Nach diesem Abschnitt, der *Einführung*, ist der Inhalt in drei Hauptabschnitte eingeteilt:

Theoretische Grundlagen

In *Zuverlässigkeit und Sicherheit* wird die notwendige theoretische und mathematische Basis zu Verfügbarkeitstheorie und Sicherheitstechnik geschaffen.
In Kapitel *Stand der Technik* werden standardisierte und in der Praxis angewendete Methoden, sowie kommerzielle und nicht kommerzielle Hilfen zur Umsetzung dieser Methoden zur Kennwertermittlung beschrieben.

Problemstellung, Analyse und Umsetzung

Im Kern dieser Arbeit wird zuerst auf die *Problemstellung* im Detail eingegangen. Praktische Anforderungen aus dem Entwicklungsalltag werden gegen die Theorie und den Stand der Technik geprüft. In Kapitel *Erhebung von Verifikationsdaten konkreter Baugruppen* werden unterschiedliche Baugruppen-Untersuchungen, über mehrere Jahre gesammelt, evaluiert und auf Korrektheit überprüft.
Im nächsten Kapitel - *Wirtschaftlichkeitsbetrachtung* - werden Anforderungen gesammelt, welche sich aus der vorgegebenen Einsatzumgebung des wirtschaftlich orientierten Betriebs ergeben.
In Kapitel *Prozesse und Methoden* wird der bestehende Produkt-Lebenszyklus im Detail studiert und entsprechend der Vision eines zuverlässigkeitsorientierten Schaltungsentwicklungsprozesses adaptiert und erweitert.
Den Abschluss dieses Abschnitts bildet die *Umsetzung des Werkzeugs zur Zuverlässigkeitsberechnung*. Konzentriert auf die wichtigsten Anwendungsfälle, wird das umgesetzte, computergestützte Hilfsprogramm anhand eines konkreten Berechnungsablaufs beschrieben. Im Anschluss an die Korrektheitsprüfung sind Informationen zur Benutzerdokumentation und weitere Funktionen, welche während der Umsetzung als zukünftig nützlich bewertet wurden, aufgeführt.

Bewertung und Ausblick

In Kapitel *Conclusio - Bewertung* wird die geleistete Arbeit zusammengefasst und bewertet. Auf Basis der Diskussion erreichter und nicht erreichter Ziele, wird ein Gesamtresümee gezogen. Der *Ausblick* schließt den letzten Hauptabschnitt mit Beispielen für weiterführende Arbeiten ab.

In *Anhang A* werden zusätzliche Hintergrundinformationen zur Verfügbarkeits- und Sicherheitstheorie angeführt.
Anhang B stellt neben einer Übersicht sämtlicher gesammelter Anforderungen, zusätzliche Beschreibungen zur Umsetzung und Inbetriebnahme des Berechnungswerkzeugs zur Verfügung.

1.4. Hinweise für den Leser

Prozess- und Tool-Anforderungen

Anforderungen die in den nachfolgenden Kapiteln identifiziert werden, sind direkt entsprechend gekennzeichnet. Dabei wird folgende Konvention verwendet:

PR 0 **Prozess-Anforderung**
Beschreibt ein *Prozess-Requirement*, welches als Vorschlag für Anpassungen des eingeführten Produktrealisierungs-Prozesses in Kapitel 7 auf Seite 101 näher betrachtet wird.

TR 0 **Tool-Anforderung**
Beschreibt ein *Tool-Requirement*, welches in Form eines Business-Requirements als Vorgabe für die Prediktions-Tool Entwicklung dient (siehe Kapitel 8 auf Seite 137).

Anforderungen die nach diesen Textmarken beschrieben werden, entsprechen Vorschlägen zur Prozess-Verbesserung bzw. konkreten Funktionsvorgaben für das Prediktions-Werkzeug. Sie beinhalten Schlussfolgerungen aus Interviews und der Untersuchung von Prozessabläufen, Fehlerdatenbanken und früheren Ansätzen zur Kennwert-Generierung.

Einzelne Anforderungen scheinen mehrfach im Text auf. Dies kommt daher, dass die Untersuchungsergebnisse in den unterschiedlichen Kapiteln und in unterschiedlichen Untersuchungsphasen, gleiche Lösungsansätze als Schlußfolgerung zulassen. In diesen Fällen erfolgt eine detaillierte Beschreibung nur beim ersten Auftauchen.

2. Zuverlässigkeit und Sicherheit

Die theoretische und mathematische Basis zur Verfügbarkeitstheorie, die Unterschiede zwischen der Betrachtung von Standard- und Sicherheitsbaugruppen und verfügbare Kennwertermittlungsmethoden werden in den nachfolgenden Abschnitten aufgearbeitet.

Neben der Vermittlung der Theorie wird auch versucht, wo möglich, ein Zusammenhang mit und durch Praxisbeispiele zu schaffen.

Da es dabei um den Unterbau bezüglich der Erfüllung von internen und externen Vorschriften und Normen geht, ist das Wissen Voraussetzung für die korrekte Formulierung von Anforderungen aus der *Prozess* und *physikalischen Sicht* entsprechend dem vorgestellten *4+1 Vorgehensmodell* (Abschnitt 1.2 auf Seite 3).

Das nachfolgende Kapitel gibt einen Überblick über die Begriffe und Definitionen der Zuverlässigkeits- und Sicherheitstechnik auf Basis von [Pau03] und [Bir07]. Eine vollständige Übersicht kann in diesen Standardwerken nachgelesen werden. Auf die anzuwendenden Normen wird direkt im Text verwiesen.

2.1. Historische Entwicklung

Die geschichtliche Entwicklung der Zuverlässigkeitstheorie begann mit der immer wichtiger werdenden *Kommunikationsvernetzung* in den 50er Jahren bei Bell. Boeing befasste sich ungefähr gleichzeitig mit der Einführung von methodischen Sicherheitsprognosen und -analysen in der *Luftfahrt*.

Das *Raumfahrtprogramm* in Amerika ist bis heute eine der wichtigsten Quellen für Informationen und betreibt den Großteil der Grundlagenforschung auf dem Gebiet der Zuverlässigkeits- und Sicherheitstechnik (z.B. *Nancy Leveson* am MIT). Die technische und personelle Verflechtung des Raumfahrtprogramms mit den militärischen Stellen des Landes ist wohl der Grund, weshalb viele Standards in diesem Bereich entstanden.

Ursprung	Disziplin/Methode	Jahr
Kommunikationstechnik (Bell)	Redundanz, Zuverlässigkeit	50er Jahre

Flugzeugindustrie (Boeing)	Sicherheit	50er Jahre
Raumfahrt (NASA)	Zuverlässigkeit, Sicherheit	60er Jahre
Armee (US)	Zuverlässigkeit	60er Jahre
Atomindustrie	Sicherheit, Redundanz	50er Jahre
Chemische und petrochemische Industrie	Sicherheit	70er Jahre
Medizintechnik	Sicherheit	
Automobilindustrie (JPN)	Qualitätsmethoden	80er/90er
Maschinenindustrie (DE)	Sicherheit	90er

Tabelle 2.1.: Historische Entwicklung verschiedener Disziplinen und Methoden der Zuverlässigkeitstheorie

Eine Übersicht zur zeitlichen Entwicklung der wichtigsten Methoden und Disziplinen in der Zuverlässigkeitstheorie gibt Tabelle 2.1.

Die *moderne Sicherheitstechnik*, gemeint ist die Personensicherheit, wurde in den 70er Jahren durch die Unfälle der Chemie-Industrie von Seveso in Italien und Bhopal in Indien neu definiert. In Folge dieser Katastrophen wurde die *Maschinenrichtlinie* als Regelwerk für jede in Europa in Betrieb zu nehmende Maschine eingeführt. Gemeinsam mit anderen Richtlinien führte dies zur CE-Kennzeichnung.

Tabelle A.1 auf Seite 169 im Anhang stellt den ursprünglichen Anwendungsgebieten der Zuverlässigkeits- und Sicherheitstechnik, historische Unfälle und Katastrophen gegenüber. Gerade der Absturz des Space Shuttles Challenger zeigt dabei den wiederkehrenden Konflikt zwischen ernsthaften Zuverlässigkeitserhebungen und wirtschaftlichen Interessen. Laut *Richard Feynman*, Mitglied der Untersuchungskommission des Unfalls, waren die folgenden unterschiedlichen Ansichten zur Ausfallwahrscheinlichkeit des Space Shuttles innerhalb der beteiligten Organisationen zu finden [Fey86]:

- Das *NASA-Management* behauptete, dass nur auf einem von 100 000 Flügen ein fataler Abbruch erfolgen könne.
- Die *Konstrukteure des Haupttriebwerks* gingen von einem Versagen bei einem von 100 bis 200 Flügen aus.
- Die *Air Force* ging von Ausfallraten von 1:50 aus.

Untersuchungen zu einem späteren Zeitpunkt ergaben eine *mathematische Versagenswahrscheinlichkeit* von *1:438*. Die Aufteilung dieser Ausfallswahrscheinlichkeit auf die verschiedenen Shuttlekomponenten ist in Bild 2.1 auf der nächsten Seite dargestellt.

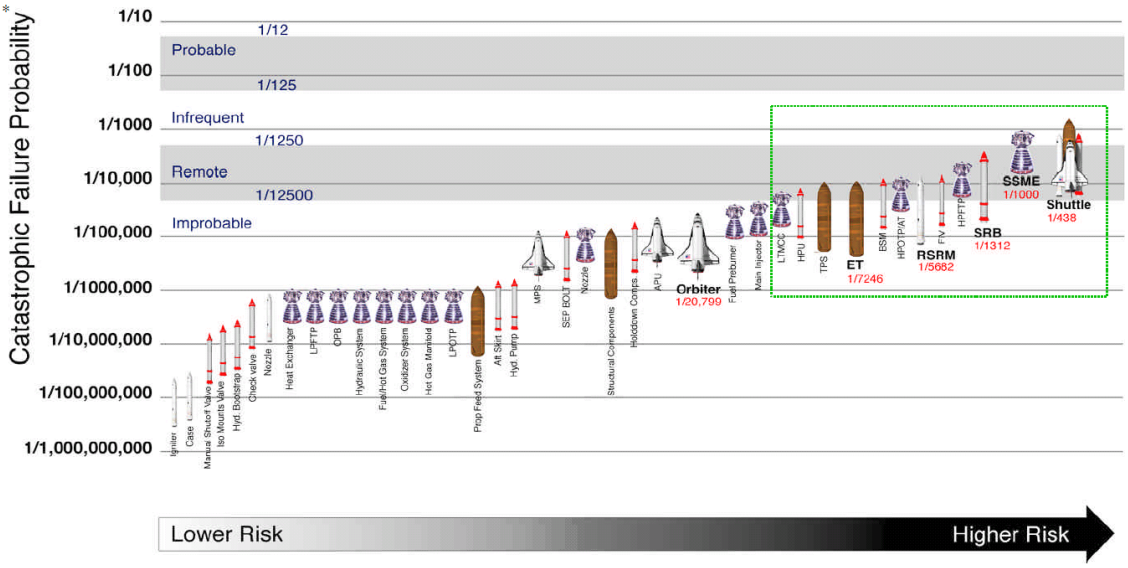


Abbildung 2.1.: Aufteilung der System-Zuverlässigkeit eines Space-Shuttles [Mic00]

Es lag nicht an fehlender Erfahrung der Ingenieure oder mangelnden Berechnungsmethoden, dass deren Zahlen um Magnituden von denen des Managements abwichen. Es gab viel mehr die Befürchtung, dass Investitionen gestoppt werden könnten, sollten die tatsächlichen Risiken bekannt werden.

Durch dieses Beispiel wird bereits klar, dass *menschliches Versagen*, sowohl direkt als auch indirekt, wichtige Ursache für Unfälle und Katastrophen abseits der Natur ist. Diesen Faktor gilt es also möglichst auszuschalten oder zumindest zu minimieren. Weitere Einflussgrößen auf die Zuverlässigkeit sind:

Komplexität Komplexe Systeme unterliegen einem höheren Ausfallsrisiko als einfache Systeme. (Raumfahrt, Luftfahrt, Automobilindustrie)

Häufigkeit der Anwendung Vervielfachung der Anwendung bedeutet Erhöhung der tatsächlichen Ausfälle im Feld. (Maschinenbau, Automobilindustrie)

Einsatzdauer Die Wahrscheinlichkeit eines Ausfalls steigt mit dem Alter und dabei vor allem mit der Zeitdauer im bestimmungsgemäßen Einsatz einer Komponente. In welcher Form, linear oder nicht linear, hängt von der Art der Komponente ab (Elektronik, Mechanik, . . .).

Art der geforderten Zuverlässigkeit Die *Verfügbarkeit auf Anforderung* stellt im Gegensatz zur *kontinuierlichen Verfügbarkeit* andere Anforderungen bei der Umsetzung von Systemen. (Militär, Raumfahrt vs. Maschinenbau, Automobilindustrie)

Sicherheitsanforderungen Forderung nach der Erfüllung von Standards und Richtlinien zum Schutz von Leib und Leben, wie beispielsweise im Bereich des Arbeitsschutzes durch die Maschinenrichtlinie.

Die Risiken und die daraus resultierenden Anforderungen sind für unterschiedliche Anwendungen vorgegeben. So kann eine katastrophale Kernschmelze in einem Atomreaktor nur entdeckt und unterbunden werden, wenn alle Mess- und Notvorrichtungen kontinuierlich arbeiten. Im Gegensatz dazu ist bei der militärischen Anwendung der Steuerelektronik in einer Rakete keine kontinuierliche Überwachung möglich. Trotzdem muss möglichst weitgehend sichergestellt werden, dass diese bei Anforderung *[en: on demand]* erwartungsgemäß funktioniert. In Tabelle 2.2 sind Beispiele zu unterschiedlichen Anforderungen an Zuverlässigkeit und Verfügbarkeit den möglichen Auswirkungen bei Nichterfüllung gegenübergestellt.

Anwendung	Einsatzdauer	Einsatzphase	Fehlerauswirkung
Raumfahrzeug	Tage	kontinuierlich	*katastrophal:* Absturz
Flugzeug	Jahre	kontinuierlich	*katastrophal:* Absturz
Rakete	Sekunden	auf Anforderung	*katastrophal:* falsches Ziel, Fehlzündung
Atomkraftwerk	Jahrzehnte	kontinuierlich	*katastrophal:* Kernschmelze
Raffinerie	Jahrzehnte	kontinuierlich	*katastrophal:* Explosion
Röntgengerät	Sekunden/ Minuten	auf Anforderung	*hoch:* Tod einzelner Personen
Auto	Jahre	kontinuierlich	*hoch:* Tod einzelner Personen

Tabelle 2.2.: Unterschiedliche Anforderungen und Ziele hinsichtlich Zuverlässigkeit und Qualität in Abhängigkeit des Anwendungsgebiets

In der Tabelle ist nicht ersichtlich, dass auch die *Fehlerreaktion*, also das Verhalten bei Detektierung einer Fehlfunktion, sehr unterschiedlich sein kann. So ist bei einer Fertigungsmaschine vorgeschrieben, einen *sicheren Zustand* einzunehmen. Dieser statische, nur durch Quittierung reversible Zustand zeichnet sich beispielsweise dadurch aus, dass Kraftübertragungen momentenlos und Energieübertragungen stromlos geschaltet werden. Bei einer Anlage zum Brandschutz oder dem Sicherheitssystem eines Flugzeugs wären die selben statischen Maßnahmen fatal.

Die aktivsten Forschungen auf dem Gebiet der *Zuverlässigkeitstheorie* findet man dort wo Fehleinschätzungen *hohen wirtschaftlichen Schaden* verursachen oder wo *hohe Gefährdungen für Leib und Leben* (vieler) Menschen gegeben sind. Dabei ist wichtig zu bemerken, dass ein wirtschaftlicher Schaden nicht zwingend als Folge eines Unfalls entstehen muss. Wie in der *Automobilindustrie* ver-

folgbar, ist hohe Qualität ein Grund für den Kaufentscheid. Im Gegensatz dazu können (sicherheits-)technisch sinnvolle Rückholaktionen den Ruf einer Automarke und somit deren wirtschaftlichen Erfolge nachhaltig schädigen.

2.2. Begriffe, Definitionen und Kennwerte

Die Beschäftigung mit der Zuverlässigkeitstheorie erfordert eine klare Definition der fachspezifischen Nomenklatur. Viele Bezeichnungen sind im Alltag verankert, werden aber nicht klar voneinenander abgegrenzt oder missverständlich angewendet.

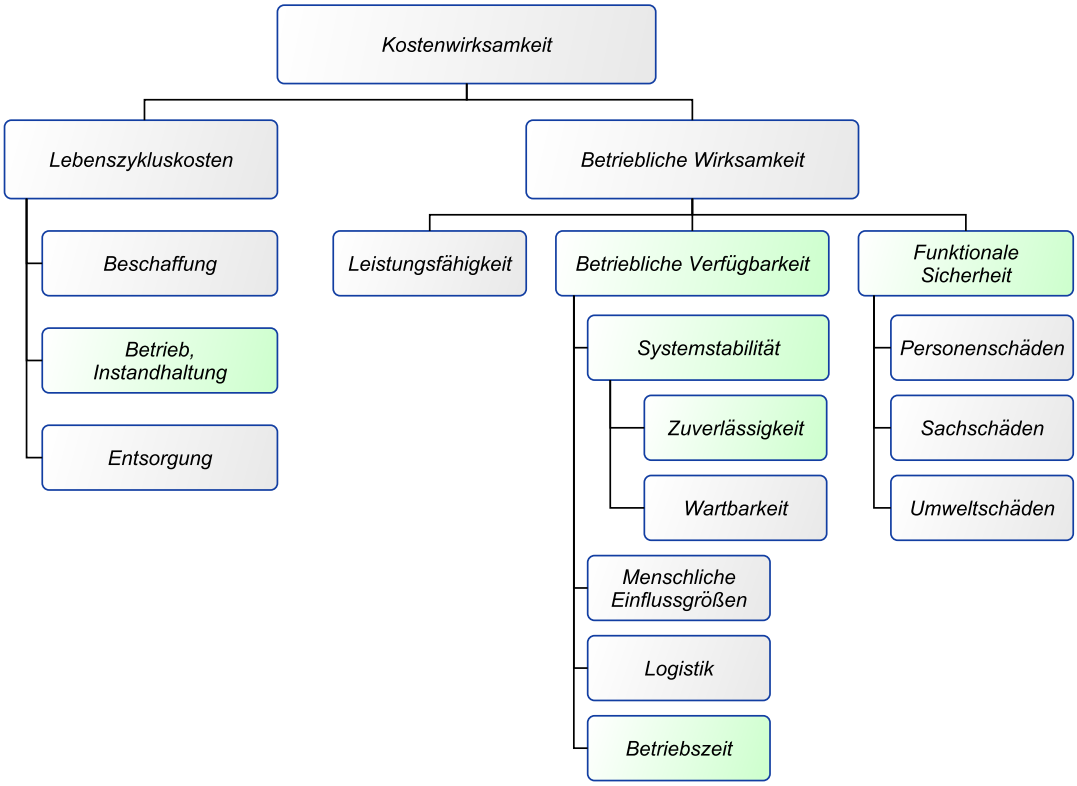


Abbildung 2.2.: Beziehung wichtiger Begriffe und Definitionen der Zuverlässigkeitstheorie, ausgehend von der Kostenwirksamkeit [Bir07]

Um einen Überblick zu schaffen, wird der Zusammenhang der zuverlässigkeitsorientierten Begriffe in Abbildung 2.2 entsprechend der wirtschaftlich orientierten Aufteilung von Birolini [Bir07, Anhang A1] dargestellt. Methoden zur Unterstützung und Absicherung dieser Eigenschaften sind in Abbildung 6.1 auf Seite 92 dargestellt.

Diese Arbeit konzentriert sich in der Folge auf die Zweige der *Betrieblichen Verfügbarkeit* und *(Funktionalen) Sicherheit*. Im Rahmen der Analyse bestehender Prozesse werden die grün hervorgehobenen Bereiche genauer betrachtet. Dabei werden besonders Ansatzpunkte für neue Methoden gesucht, welche während früher Phasen die Entwicklung eines Systems beeinflussen bzw. früh fixiert werden und somit die Gesamtqualität maßgeblich mitbestimmen.

Die wichtigsten Begriffe in diesem Zusammenhang sind in Folge kurz erklärt. Weiterführende und ergänzende Definitionen sind im Glossar zu finden.

Überlebenswahrscheinlichkeit [en: (operational) reliability/dependability]	Ausdruck zur Beschreibung der Leistung bezüglich Verfügbarkeit und ihrer Einflussfaktoren: Funktionsfähigkeit, Instandhaltbarkeit und Instandhaltungsbereitschaft. *Synonyme: Zuverlässigkeit*, Ausfallsicherheit, Systemzuverlässigkeit, Betriebssicherheit
Verfügbarkeit [en: availability]	Die Fähigkeit einer Betrachtungseinheit, innerhalb eines gegebenen Zeitintervalls (*Verfügbarkeit*) bzw. zu einem gegebenen Zeitpunkt (*Punkt-Verfügbarkeit*) die geforderte Funktion unter gegebenen Bedingungen zu erfüllen (*Quelle:* [Bör09]).
Instandhaltbarkeit bzw. Wartbarkeit [en: maintainability]	Beschreibt die Fähigkeit einer Einheit bzw. eines Systems durch vorgeschriebene Verfahren, Methoden und Hilfsmittel entweder den operationsfähigen Zustand zu erhalten oder wieder in einen operationsfähigen Zustand gebracht werden zu können (*Quelle:* [Bör09]).
Sicherheit [en: safety]	Sicherheit beschreibt das *Nichtvorhandensein von unakzeptablen Risiken*. Sicherheit ist ein Zustand in dem das (Rest-)Risiko nicht größer als ein definiertes Grenzrisiko ist (siehe dazu Abbildung 2.9 auf Seite 30). Definition zur *Funktionalen Sicherheit* laut Sicherheitsnorm IEC61508 [IEC10] im Glossar.
Risiko [en: risk] $R = H \cdot S$	R. . . Risiko (→ Abb. 2.9 auf Seite 30) H. . . erwartete Eintrittshäufigkeit eines Schadensereignisses S. . . Schadensausmaß

Tabelle 2.3.: Wichtige Begriffe der Zuverlässigkeitstheorie

In direkt kausalem Zusammenhang mit *Überlebenswahrscheinlichkeit, Verfügbarkeit* und *Risiko* stehen die Begriffe *Fehler* und *Ausfall*:

Ausfall bzw. Versagen [en: failure]

	... tritt auf, wenn ein System die erwartete Funktion nicht mehr erfüllt. Zum Zeitpunkt $t = 0$ wird angenommen, dass ein System frei von *Defekten* und *systematischen Ausfällen* ist.
Systematischer Ausfall [en: systematic failure]	
	Im Gegensatz zum *zufälligen Ausfall*, per Analyse eindeutig auf Ursache zurückzuführen. Durch entsprechende Änderungen im Entwurf, beim Fertigungsprozess usw. behebbar. Fehler in Software führen immer zu systematischen Ausfällen.
Defekt, Fehler bzw. Fehlaussage [en: defect, error]	
	... beschreibt die Diskrepanz zwischen erwartetem und vorliegendem Wert oder Zustand. Unter den Fehlerursachen finden sich auch sämtliche Arten des *menschlichen Versagens*, wie Bedienfehler aber auch Konzept-, Spezifikations-, Herstellungs-, Implementierungs- und Dokumentationsfehler.
Fehlzustand [en: fault]	
	Beschreibt den Zustand eines Systems in dem die erwartete Funktion nicht oder nur eingeschränkt zur Verfügung steht. Ein Fehlzustand eines Systems ist oft die Folge eines Ausfalls des Systems selbst.

Tabelle 2.4.: Definitionen zur klaren Abgrenzung von Fehlern und Ausfällen

Ein *Ausfall* verursacht somit den Übergang vom Status *fehlerfreier Betrieb* zu *Fehlzustand*. Dieser kann dabei durch die Diagnose von *Fehlern* festgestellt werden.

2.2.1. Grundgrößen der Zuverlässigkeit

Tabelle 2.5 auf der nächsten Seite listet die wichtigsten Größen der Zuverlässigkeitstheorie auf.

Symbol	Bezeichnungen	englischer Begriff
λ, $\lambda(t)$ [a]	Ausfallrate	failure rate
$F(t)$	Ausfallwahrscheinlichkeit	probability of failure
$f(t)$	Ausfalldichte	failure intensity
$R(t)$	Zuverlässigkeit/ Überlebenswahrscheinlichkeit	reliability
$MTTF$	Mittlere Ausfallsfreie Zeit	mean time to failure

a In der Literatur ist auch $h(t)$ statt $\lambda(t)$ für die Ausfallrate gebräuchlich.

$V(t)$	Verfügbarkeit/ Punktverfügbarkeit	availability, dependability

Tabelle 2.5.: Grundgrößen der Zuverlässigkeit

Der mathematische Zusammenhang zwischen diesen Größen ist wie folgt:

Ausfallrate $\lambda(t)$ *[en: failure rate]*

Die *Ausfallrate* oder *momentane Ausfallrate* ist als Grenzwert der Ausfallwahrscheinlichkeitsdifferenz, dividiert durch die Überlebenswahrscheinlichkeit definiert:

$$\lambda(t) = \lim_{\Delta t \to 0} \frac{1}{\Delta t} \cdot \frac{F(t+\Delta t) - F(t)}{R(t)} = \frac{f(t)}{R(t)} \qquad \text{momentane Ausfallrate} \qquad (2.1)$$

Die *mittlere Ausfallrate* $\lambda(t_1,t_2)$ entspricht der gemittelten momentanen Ausfallrate über das gegebene Zeitintervall (t_1, t_2).

$$\bar{\lambda}(t_1,t_2) = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} \lambda(t)\, dt \qquad \text{mittlere Ausfallrate} \qquad (2.2)$$

Ausfallwahrscheinlichkeit $F(t)$ und Ausfalldichte $f(t)$

Die *Ausfalldichte* $f(t)$ erhält man durch Ableitung der *Ausfallwahrscheinlichkeit* $F(t)$ nach der Zeit.

$$F(t) = P(T \leq t) \qquad \text{Ausfallwahrscheinlichkeit} \qquad (2.3)$$

$$f(t) = \frac{dF(t)}{dt} \qquad \text{Ausfalldichte} \qquad (2.4)$$

Für die beiden ausfallsbezogenen Größen werden, entsprechend dem Anwendungsbereich, die dafür passenden Ausfallratenmodelle eingesetzt. Die Herleitung der Zusammenhänge für die Weibullverteilung ist in Abschnitt 2.2.2 auf Seite 20 beschrieben.

Überlebenswahrscheinlichkeit $R(t)$

Die umgangssprachlich meist als *Zuverlässigkeit* bezeichnete Größe ist folgendermaßen definiert:

Zuverlässigkeit ist eine *Charakteristik* einer betrachteten Einheit, ausgedrückt durch die *Wahrscheinlichkeit*, dass diese Einheit die *erwartete Funktion* unter *gegebenen Bedingungen* für ein *festgesetztes Zeitintervall* erfüllt.

Herleitung der Überlebenswahrscheinlichkeit $R(t)$

$$\lambda(t) = \frac{f(t)}{R(t)} = \frac{1}{R(t)} \cdot \frac{dR(t)}{dt}$$
$$= -\frac{d \ln R(t)}{dt} \qquad \text{Ausfallrate} \qquad (2.5)$$

$$R(t) = e^{-\int_0^t \lambda(x)dx} = e^{-\lambda t} \qquad \text{Zuverlässigkeit} \qquad (2.6)$$

Die *Überlebenswahrscheinlichkeit* $R(t)$ addiert mit der *Ausfallwahrscheinlichkeit* $F(t)$ ergibt immer hundert Prozent. Mathematisch ausgedrückt:

$$R(t) = 1 - F(t) \qquad \text{Zuverlässigkeit} \qquad (2.7)$$

Erwartungswert E(t)

Der Erwartungswert drückt die *mittlere Lebensdauer* als Summe der Lebensdauer aller einzeln betrachteten Systeme dividiert durch die Gesamtzahl dieser Systeme aus:

$$E(\tau) = \frac{t_1 + \cdots + t_n}{n}$$
$$= \int_0^t R(t)\, dt \qquad \text{Erwartungswert} \qquad (2.8)$$

Mit dieser Beziehung wird beispielsweise die Anzahl im Feld befindlicher Produkte mit der Überlebenswahrscheinlichkeit in Beziehung gesetzt.
Die *bedingte Lebenserwartung* oder auch *Restlebensdauer* kann wie folgt berechnet werden:

$$E_t(T) = \frac{1}{R(t)} \cdot \int_t^\infty R(\tau)\, d\tau \qquad \text{Restlebensdauer} \qquad (2.9)$$

Aus diesem Zusammenhang kann die im Mittel zu erwartende Restlebensdauer eines Systems zu jedem Zeitpunkt berechnet werde. Für $t = 0$ entspricht dies der im Mittel zu erwartenden Lebensdauer oder auch *Mittleren Ausfallsfreien Zeit*.

Mittlere Ausfallsfreie Zeit MTTF

Aus Abbildung 2.3 auf der nächsten Seite wird ersichtlich, dass die *mittlere ausfallsfreie Zeit* MTTF direkt im Zusammenhang mit weiteren Begriffen der *Wartung und Instandhaltung* zu sehen ist.

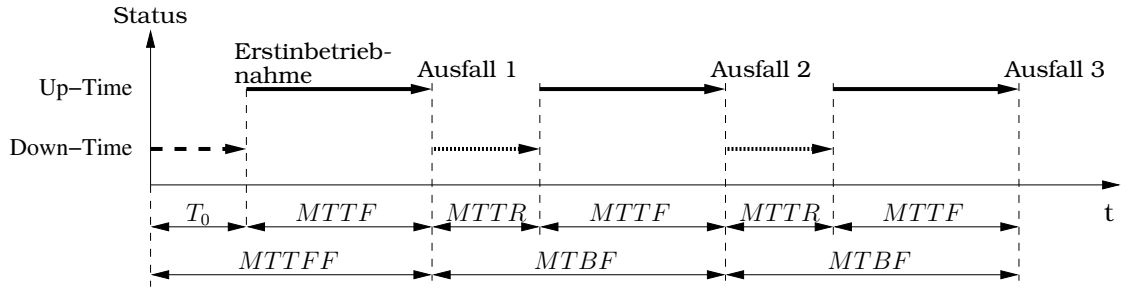


Abbildung 2.3.: Zusammenhang zwischen den verschiedenen Zeitdefinitionen von MTTFF, MTTF, MTBF, MTTR

Dabei berechnet sich die MTTFF (*Mittlere ausfallsfreie Arbeitszeit bis zum ersten Fehler*) als Summe der *garantiert ausfallsfreien Zeit* T_0 während der keinerlei Ausfälle zu verzeichnen sind und der MTTF. Damit sind die Zusammenhänge eines *nicht reparierbaren Systems* vollständig beschrieben. Weiters gilt $MTTFF = MTTF$ für $T_0 = 0$.

Bei *reparierbaren Systemen* folgt nach dem ersten Ausfall die Reparaturzeit MTTR. Diese dient zur vollständigen Wiederherstellung der Funktionsfähigkeit des Systems. Danach beginnt wieder eine Zeitspanne MTTF in der das System arbeitet. Beim nächsten Ausfall beginnt dieser Zyklus wieder von vorne. Die Summe von Reparaturzeit und operativ wirksamer Zeit wird dabei mit MTBF (*Mittlere ausfallsfreie Arbeitszeit zwischen zwei Fehlern*) bezeichnet. In der Realität ist eine vollständige Reparatur meist nicht möglich. Somit ist in der Realität mit abnehmenden Zeitintervallen MTTF und MTBF nach jeder Reparatur zu rechnen.

Reparierbar heißt, dass nach dem Reparaturvorgang das System in einem Zustand wie neu ist. Das bedeutet, dass während des Vorgangs alle Teilsysteme oder Bauteile die einer Alterung unterworfen sind, also zeitabhängige Ausfallskennwerte besitzen, ausgetauscht werden. Somit ist klar, dass in der Praxis bei komplexen elektronischen Modulen meist nicht von diesem Fall ausgegangen werden kann und eine Reparatur normalerweise unvollständig im Sinne der Verfügbarkeit ist. Die Konsequenz daraus ist, dass elektronische Systeme in aller Regel als *nicht reparierbare Systeme* einzustufen sind.

Im Widerspruch zu dieser Definition findet man auch im Zusammenhang mit *nicht reparierbaren Systemen* die Angabe von $MTTR$ und $MTBF$. In diesen Fällen bezieht sich diese Zeitangabe auf die aufzuwendende Zeit für den *Austausch von ausgefallenen Komponenten*.

Diese Arbeit konzentriert sich auf die Umsetzung von Maßnahmen im Zusammenhang mit elektronischen Baugruppen, also *nicht reparierbaren Systemen*. Somit wird in weiterer Folge nur noch die *Mittlere Ausfallsfreie Zeit MTTF* betrachtet. Diese definiert sich über den Erwartungswert bzw. das Integral der

Überlebenswahrscheinlichkeit über die gesamte Lebensspanne:

$$MTTF = E[\tau] = \int_0^\infty R(t)\,dt$$
$$= \int_0^\infty e^{-\lambda t}\,dt = \frac{1}{\lambda} \tag{2.10}$$

Setzt man dieses Ergebnis in die Formel für die Überlebenswahrscheinlichkeit $R(t)$ ein, erhält man:

$$R(t) = e^{-\lambda t} = e^{-\frac{t}{MTTF}} \tag{2.11}$$

Zum Zeitpunkt $t = MTTF$ ergibt dies folgendes Ergebnis:

$$R(t) = e^{-1} = 0{,}37 \tag{2.12}$$

Dieses Ergebnis ist in der Praxis folgendermaßen interpretierbar [EPS05]:

- Bei einer großen Anzahl von Systemen überstehen nur 37% einen Betriebszeitraum länger als die mittlere ausfallfreie Zeit $MTTF$.
- Die Wahrscheinlichkeit, dass ein einzelnes System länger als $MTTF$ arbeitet, beträgt 37%.
- Ein System fällt mit Konfidenzniveau von 37% genau zum Zeitpunkt $MTTF$ aus.

Im Sprachgebrauch ist auf die exakte Unterscheidung zwischen MTTF und MTBF zu achten, da diese sehr oft verwechselt werden. Weiters unterscheidet sich die *Mittlere Ausfallfreie Zeit MTTF* von der in der Sicherheitstechnik relevanten *Mittleren ausfallsfreien Zeit bis zu einem gefährlichen Ausfall* $MTTF_D$ (siehe Abschnitt 2.3.2 auf Seite 35).

Verfügbarkeit $V(t)$

Mit Kenntnis von MTTF und MTTR lässt sich die *Verfügbarkeit* oder auch *Punktverfügbarkeit* berechnen:

$$V(t) = \frac{MTTF}{MTTF + MTTR} \qquad \text{Verfügbarkeit} \tag{2.13}$$

Aus diesem Zusammenhang ist erkennbar, dass die Verfügbarkeit nicht zwingend etwas über die Ausfallshäufigkeit aussagt. Ist ein System leicht austauschbar oder reparierbar, ist die Gesamtverfügbarkeit gleich zu bewerten wie bei einem sehr langzeitstabilen, wenig ausfallenden System, welches einen hohen Zeitaufwand beim Austausch fordert.

ANMERKUNG: Die Ausfallrate und auch die Verfügbarkeit beziehen sich auf die Einsatzzeit eines Systems. Lagerzeiten bedingen zwar auch eine gewisse Alterung, allerdings in wesentlich abgeschwächter Form gegenüber dem Betrieb innerhalb der Arbeitsumgebung. Da diese Zeiten im Allgemeinen nicht bekannt sind, die Verfügbarkeitsbetrachtungen jedoch nur einseitig zu Ungunsten des Produzenten verschlechtern, dürfen diese unberücksichtigt bleiben.

Mathematischer Zusammenhang zwischen Zuverlässigkeitskenngrößen

Eine einfache Umrechnung zwischen den Zuverlässigkeitsgrößen ermöglicht Tabelle 2.6.

	Ausfallswahrscheinlichkeit	**Überlebenswahrscheinlichkeit**	**Ausfalldichte**	**Ausfallrate**
	$F(t)$	$R(t)$	$f(t)$	$\lambda(t)$
$F(t)$		$1 - R(t)$	$\int_0^t f(\tau)\,d\tau$	$1 - e^{\left(-\int_0^t \lambda(\tau)\,d\tau\right)}$
$R(t)$	$1 - F(t)$		$\int_t^\infty f(\tau)\,d\tau$	$e^{\left(-\int_0^t \lambda(\tau)\,d\tau\right)}$
$f(t)$	$\frac{d\,F(t)}{dt}$	$-\frac{d\,R(t)}{dt}$		$\lambda(t) \cdot e^{\left(-\int_0^t \lambda(\tau)\,d\tau\right)}$
$\lambda(t)$	$\frac{1}{1-F(t)} \cdot \frac{d\,F(t)}{dt}$	$-\frac{1}{R(t)} \cdot \frac{d\,R(t)}{dt}$	$\frac{f(t)}{\int_t^\infty f(\tau)\,d\tau}$	

Tabelle 2.6.: Mathematischer Zusammenhang zwischen ausgewählten Zuverlässigkeitskenngrößen [Pau03, Kap. 2.1]

2.2.2. Ausfallratenmodelle

Gerne auch als *Bauteilalterung* bezeichnet, beschreibt dieser Term eine Reduktion der Ursprungsfunktionalität aufgrund unterschiedlicher Stress-Faktoren (siehe Stressmodell in Abschnitt 4.2.5 auf Seite 68). Diese führen über die Zeit zu Funktionsstörungen, Veränderungen von Bauteilkennwerten und schließlich zum Ausfall.

Ausfall wegen	**Ursachen**
elektrischer und/oder thermischer Überlastung	Kurzschluss, Dauer(über)last, erhöhte Umgebungstemperatur
thermomechanischem Stress	Temperaturwechsel
Kurzschluss	Überspannung, Dendritenwachstum bei Elektromigration

mechanischer Überlastung	Bei elektromechanische Bauteile wie Relais, aber auch Lötstellen sowie bei Steckanschlüssen durch Schalt- bzw. Steckvorgänge

Tabelle 2.7.: Ausfälle von Bauteilen mit Ursachen

Statistisch betrachtet fallen mit Abstand am häufigsten ICs aus. Danach folgen Kondensatoren, Widerstände, Transistoren, Quarze, Dioden usw.

Mathematisch treten diese Ausfälle nach bestimmten Wahrscheinlichkeitsverteilungen auf. Diese lassen sich unterschiedlichen Verteilungsfunktionen zuordnen. Übliche Vertreter sind die *Normalverteilung*, *Binomialverteilung*, *Poissonverteilung*, *Student-t Verteilung* und weitere. Im spezifischen Bereich der Zuverlässigkeitsanalyse von elektronischen Systemen wird die *Weibullverteilung* angewendet. Auf diese wird in Folge etwas näher eingegangen.

Weibull-Verteilung

Die *Weibullverteilung*, wie in Abbildung 2.4 dargestellt, beschreibt die Ausfallrate über die Zeit. Die typische *Badewannenkurve* erhält man durch Anwendung von Gleichung 2.15 auf Seite 24 und Vorgabe von unterschiedlichen Werten für den Formparameter β für die drei unterschiedlichen Abschnitte im Lebenszyklus einer Baugruppe.

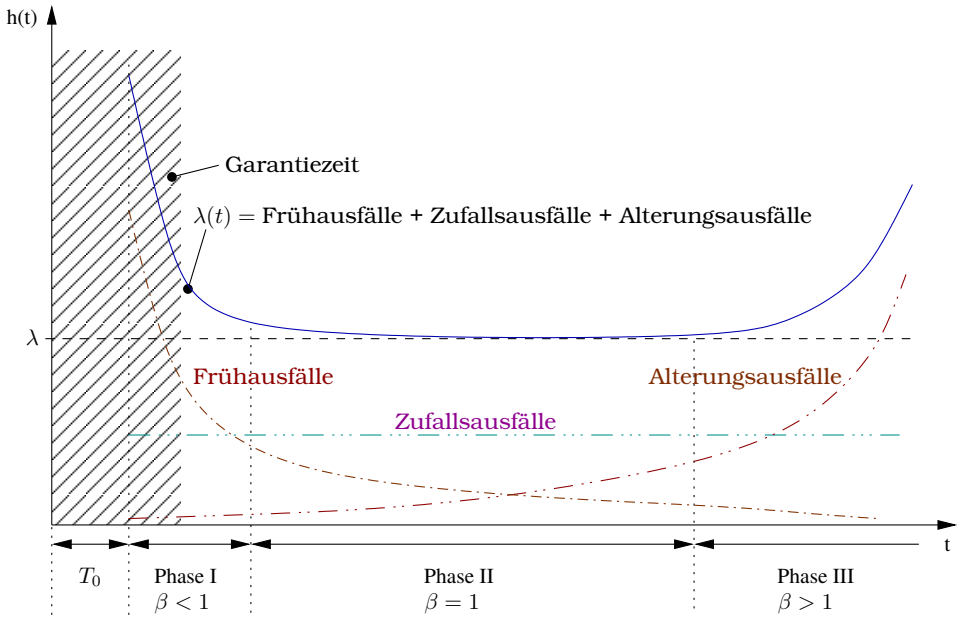


Abbildung 2.4.: Die Weibullverteilung als Summe von Früh-, Zufalls- und Alterungsausfällen

Die drei Parameter bilden das mathematische Charakteristikum der drei Lebensphasen eines mit Verschleiß behafteten Systems:

I $\beta < 1$ **Frühausfälle** ***[en: early failure period]***
. . . aufgrund von Material- und Bauteilschwächen, Produktions- und Qualitätsproblemen.

II $\beta = 1$ **Ausfälle mit (beinahe) konstanter Ausfallrate** ***[en: useful life period]***
Zufällige Ausfälle mit nahezu linearem Verlauf (bei elektronischen Baugruppen).

III $\beta > 1$ **Alterungsausfälle** ***[en: wear-out]***
. . . aufgrund von Verschleiß, Alterung und Ermüdung von Bauteilen

In der Produktion wird durch *gezielte Vorbelastung* (*Run In*) und die daraus resultierende *beschleunigte Alterung* versucht, den größten Teil der fehlerhaften Produkte bereits am Ort der Produktionsstätte auszuscheiden. Dadurch erreicht man, abhängig vom investierten Aufwand, dass ausgelieferte Produkte näher an der Grenze zur Phase mit konstanter Ausfallrate liegen.

Die *Nutzungsdauer* eines Systems erstreckt sich vom *Auslieferungszeitpunkt* bis zur *planmäßigen Außerbetriebnahme* oder dem *unplanmäßigen Ausfall*.

Die Bemessung der *Garantiezeit* hängt von Überlegungen zur Wirtschaftlichkeit und der tatsächlichen Qualität des Produkts ab. Wirtschaftlich sinnvoll ist es, diese Grenze knapp an das Ende der Frühausfallsphase zu legen. Damit werden dem Kunden Defekte in diesem nichtlinearen Bereich ersetzt. Wie später noch gezeigt wird, ist diese Grenze maßgeblich für die sinnvolle Festlegung einer mindestens zu erreichenden Ausfallrate bzw. der charakteristischen MTTF eines neu zu entwickelnden Produkts.

Der geschilderte Zusammenhang stellt sich in der Theorie sehr einfach dar. In der Praxis ist es hingegen keineswegs trivial festzustellen, an welchem Punkt auf der Verteilungskurve man sich mit einem Produkt tatsächlich befindet. Dies ist aber Grundvoraussetzung für eine optimale *Planung der Vorbelastungszeit*, der *Garantiezeit* und auch der *Lagerhaltung von Ersatzteilen*. Tabelle 2.8 auf der nächsten Seite zeigt die Auswirkungen unterschiedlicher Fehlannahmen in diesem Bereich.

Fehlannahme	Auswirkung
Run In Phase zu kurz	Imageschäden durch vermehrte Frühausfälle
	Kunden machen Garantieansprüche geltend
Run In zu lange	Produkte verbleiben länger in Produktionsstätte → erhöhter Platzbedarf in internen Lagern
	Kosten steigen durch erhöhten Energie- und Platzverbrauch beim Run In

	kein weiterer Nutzen → Baugruppen in linearem Bereich
	Thermische "Vorschädigung" der Produkte und somit Verkürzung der Nutzungsdauer
Bemessung der Garantiezeit	
. . . zu kurz	Imageschaden wegen überhöhtem Fehleranteil und als ungenügend empfundenem Kundenservice
. . . zu lang	Wirtschaftlicher Schaden da Kostenersatz auch im linearen Bereich erstattet wird.
	Lagerhaltung bei Bauteilabkündigungen muss erhöht werden
	Produktabkündigungen werden erschwert

Tabelle 2.8.: Auswirkungen von Fehlannahmen bei Festlegung wirtschaftlich relevanter, zeitlicher Kenndaten.

Die Anwendbarkeit der Weibullverteilung wurde durch verschiedene, langjährig durchgeführte, empirische Auswertungen bestätigt. Diese, durch Betriebe wie Siemens oder Organisationen im Nahbereich von Militär und Raumfahrt durchgeführten Auswertungen, führten zu unterschiedlichen Kennwert-Datenbanken die in Abschnitt 3.1.1 auf Seite 51 näher betrachtet werden. Aus diesen Untersuchungen ergab sich, dass die Linearität für elektronische Bauelemente angenommen werden darf, da diese, statistisch betrachtet, in dieser Phase keinem alterungsbedingten Verschleiß unterliegen. Dies gilt natürlich nur innerhalb der vorgegebenen Betriebsgrenzen.

Die Weibullverteilung ist grundsätzlich auf alle mit Verschleiß behafteten Vorgänge anwendbar. In Abbildung 2.5 auf der nächsten Seite ist über der Kennlinie für eine elektronische Baugruppe der mögliche Verlauf für ein mechanisches Bauteil eingetragen. Dabei kennzeichnet die nichtlinear ansteigende Phase II die mechanische Abnutzung und Ermüdungserscheinungen des Materials. Die Auswirkung einer erhöhten thermischen und/oder elektrischen Belastung von elektronischen Baugruppen wird in der dritten Kurve dargestellt. Dabei fällt auf, dass sich generell die Ausfallrate über die Zeit deutlich erhöht und die Nutzungsdauer durch die Verlängerung der Phasen I und III verringert.

Mathematischer Hintergrund der Weibull-Verteilung

Ausgehend von der *dreiparametrigen Weibullverteilung* berechnet sich die Dichtefunktion $f(t)$ wie folgt:

$$f(t) = \frac{\beta}{T - T_0} \left(\frac{t - T_0}{T - T_0} \right)^{\beta - 1} \cdot e^{-\left(\frac{t - T_0}{T - T_0} \right)^{\beta}} \tag{2.14}$$

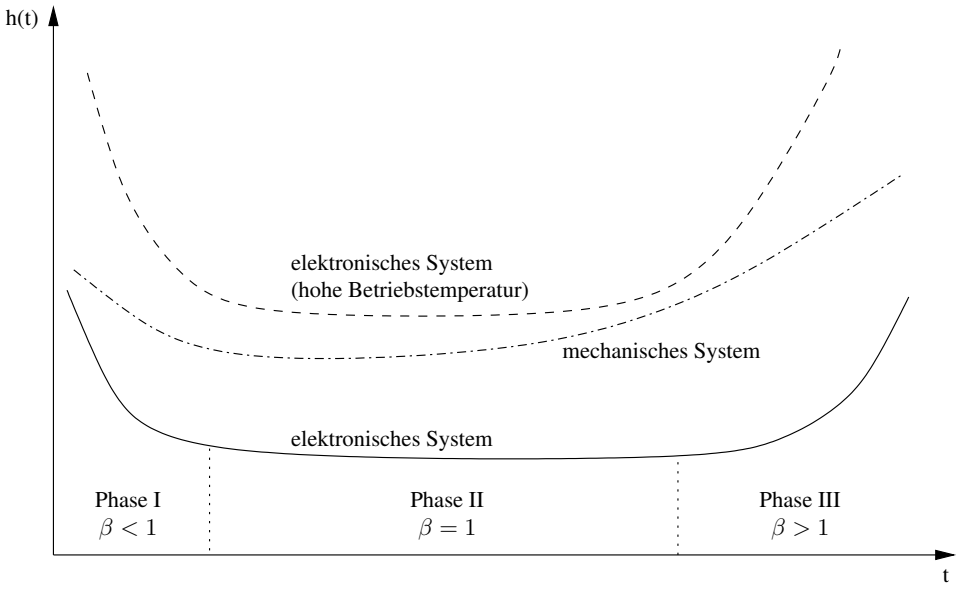


Abbildung 2.5.: Gegenüberstellung der Ausfallraten eines elektronischen Systems mit durchschnittlicher und mit überdurchschnittlicher Belastung im Vergleich zu einem mechanischen Bauteil.

Dabei entspricht T der *charakteristischen Lebensdauer* bzw. der *mittleren ausfallsfreien Zeit* $MTTF$ und β dem Formparameter der Weibullverteilung.
Setzt man $T_0 = 0$ dann spricht man von der *zweiparametrigen Weibullverteilung*:

$$f(t) = \frac{\beta}{T}\left(\frac{t}{T}\right)^{\beta-1} \cdot e^{-\left(\frac{t}{T}\right)^{\beta}} \qquad \text{Ausfalldichte} \qquad (2.15)$$

Da elektronische Bauteile keine garantiert ausfallfreie Zeit $T_0 \neq 0$ besitzen, ist die Annahme korrekt.
Die Summenhäufigkeit und somit Ausfallwahrscheinlichkeit berechnet sich aus dem Integral über die Verteilungsfunktion:

$$F(t) = \int_0^t f(\tau)\, d\tau = 1 - e^{-\left(\frac{t}{T}\right)^{\beta}} \qquad \text{Ausfallwahrscheinlichkeit} \qquad (2.16)$$

In Abbildung 2.6 auf der nächsten Seite sind die *zweiparametrige Weibullverteilungsdichte* und die daraus abgeleitete *Ausfallwahrscheinlichkeit* dargestellt.

Unter Annahme einer Ausfallrate $\lambda = 0{,}2$ zeigt die Kurvenschar den Einfluss des Formparameters β. Auf der Zeitachse ist bei $t = 5$ eine vertikale Linie für die *mittlere ausfallsfreie Zeit* $MTTF = \lambda^{-1} = 5$ eingetragen. Entsprechend $F(t) = 1 - R(t)$ und den Erläuterungen zu Gleichung 2.12 auf Seite 19 entspricht der

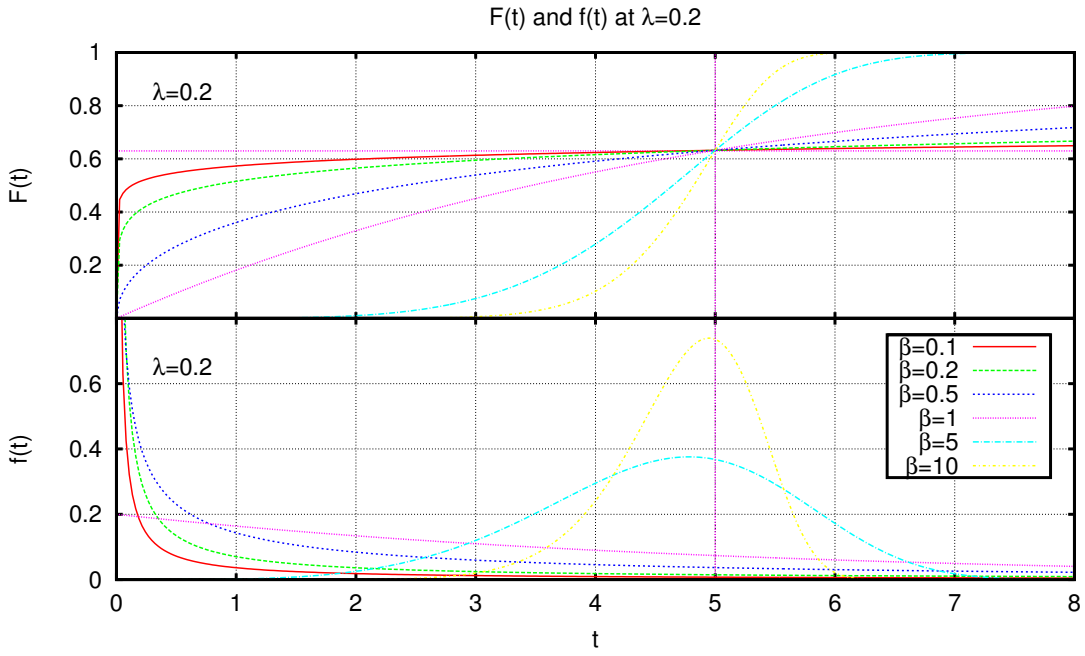


Abbildung 2.6.: Ausfallwahrscheinlichkeit $F(t)$ und Ausfalldichte $f(t)$ auf Basis der Weibullverteilung bei $\lambda = 0{,}2$ und verschiedenen Werten für den Formparameter β

Schnittpunkt der Kurvenschar einer Ausfallwahrscheinlichkeit von 63%.
Die Einheit für $MTTF$ ist je nach Anwendung in Stunden, Wochen, Jahren etc. einzusetzen.

Aus der Gleichung der Ausfallwahrscheinlichkeit lässt sich die Ausfallrate $\lambda(t)$ mit Hilfe von Tabelle 2.6 auf Seite 20 ableiten:

$$\begin{aligned}\lambda(t) &= \frac{1}{1-F(t)} \cdot \frac{d\,F(t)}{dt} = \frac{1}{1-F(t)} \cdot f(t) \\ &= \frac{1}{e^{-\left(\frac{t}{T}\right)^{\beta}}} \cdot \frac{\beta}{T}\left(\frac{t}{T}\right)^{\beta-1} \cdot e^{-\left(\frac{t}{T}\right)^{\beta}} \\ &= \frac{\beta}{T}\left(\frac{t}{T}\right)^{\beta-1} \qquad \text{Ausfallrate} \qquad (2.17)\end{aligned}$$

Die Steilheit der Ausfallrate ist durch den Faktor β gegeben. Während Phase II der Badewannenkurve wird für den Formparameter $\beta = 1$ angenommen. Somit entspricht in dieser Phase die *Weibullverteilung* einer *Exponentialverteilung*. Dies bedingt die für elektronische Bauteile typisch konstante, also zeitunabhängige Ausfallrate:

$$\begin{aligned}\lambda(t) &= \frac{\beta}{T}\left(\frac{t}{T}\right)^{\beta-1} && (\beta = 1)\\ &= \frac{1}{T}\left(\frac{t}{T}\right)^{1-1} = \frac{1}{T} = \lambda && \text{Konstante Ausfallrate}\end{aligned} \tag{2.18}$$

Setzt man nun das Ergebnis für $\lambda(t)$ in die Gleichung der Ausfallwahrscheinlichkeit auf Seite 24 ein, so bekommt man für die allgemeine Weibull-Verteilung:

$$F(t) = 1 - e^{-(\lambda t)^{\beta}} \tag{2.19}$$

Und für Phase II ($\beta = 1$):

$$F(t) = 1 - e^{-(\lambda t)} \tag{2.20}$$

Zu Beginn dieses Abschnitts ist in Abbildung 2.4 auf Seite 21 der schematische Zusammenhang der Weibullverteilung als Summe von Früh-, Zufalls- und Alterungsausfällen dargestellt. In Abbildung 2.7 auf der nächsten Seite wird auf Basis der hergeleiteten mathematischen Zusammenhänge unter Verwendung konkreter Werte dieses Schema bestätigt. Die konstante Ausfallrate für $\beta = 1$ berechnet sich dabei zu $\lambda = MTTF^{-1} = 0{,}1$.

Praktische Anwendung

Ausgehende von Gleichung 2.20 berechnet sich die Ausfallwahrscheinlichkeit von n Systemen im Feld zu einem beliebigen Zeitpunkt t nach:

$$\mu(t) = n \cdot F(t) = n \cdot \left(1 - e^{-(\lambda t)}\right) = n \cdot \left(1 - e^{-\frac{t}{MTTF}}\right) \tag{2.21}$$

Für $T \gg t$ kann dieser Zusammenhang weiter vereinfacht werden:

$$\mu(t) \approx \frac{n \cdot t}{T} = n\,\lambda\,t \tag{2.22}$$

Beispiel: Durch Umformung der Beziehung 2.21 lässt sich, bei gegebener Garantiezeit t_w und maximal erlaubtem prozentuellen Ausfallsverhältnis $\frac{\mu}{n}$, die daraus resultierende, maximale Ausfallrate des betrachteten Systems errechnen:

$$\begin{aligned}\mu(t) &= n \cdot \left(1 - e^{-(\lambda t_w)}\right)\\ \lambda(t) &= -\frac{1}{t_w} \cdot \ln\left(1 - \frac{\mu(t)}{n}\right)\end{aligned} \tag{2.23}$$

Der Kehrwert ergibt wieder die minimale mittlere ausfallfreie Zeit:

$$MTTF = \frac{1}{\lambda} = (-t_w)\left(\ln\left(1 - \frac{\mu(t)}{n}\right)\right)^{-1} \tag{2.24}$$

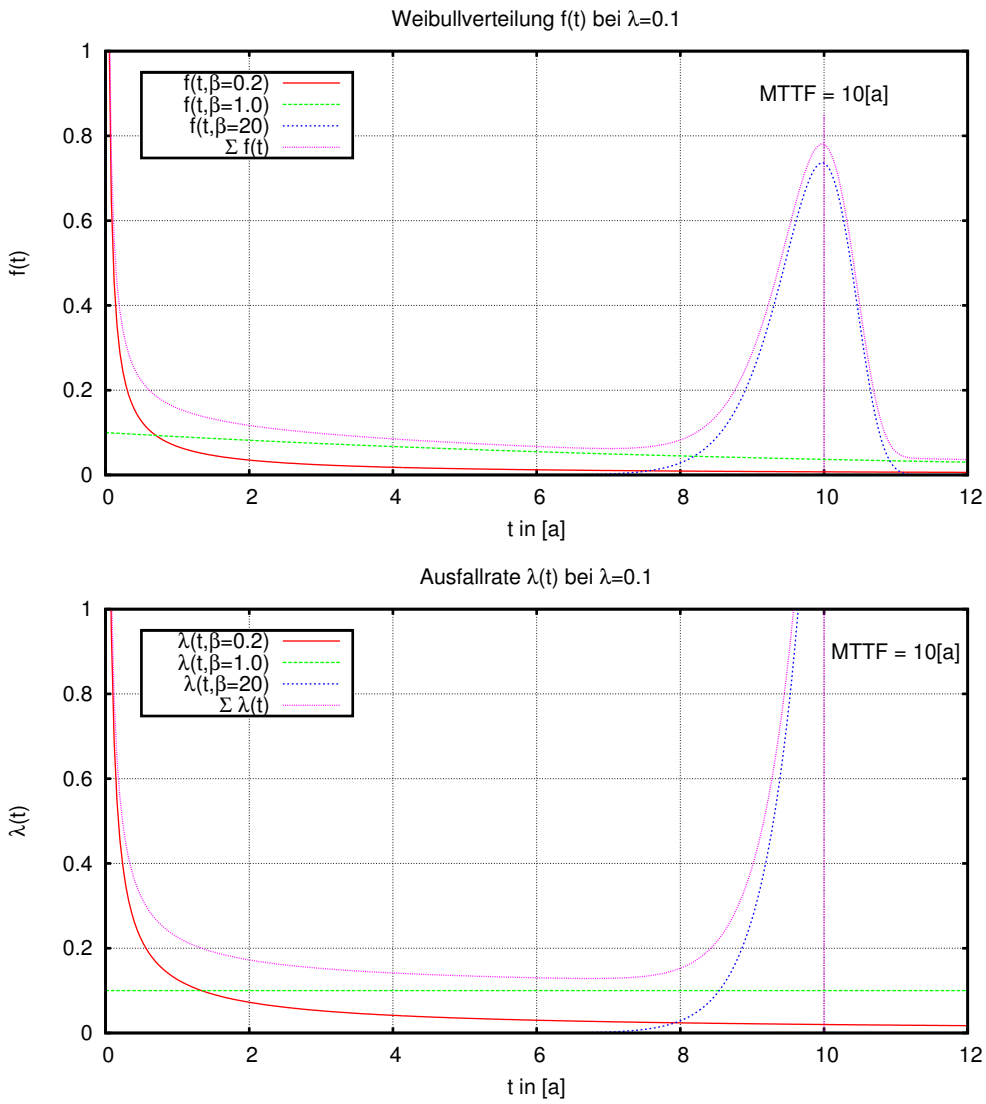


Abbildung 2.7.: Zusammengesetzte Wahrscheinlichkeitsdichte $f(t)$ und Ausfallrate $\lambda(t)$ auf Basis der zweiparametrigen Weibullverteilung für $MTTF = 10$ Jahre

Damit stehen mathematische Werkzeuge zur Verfügung um auf Basis eines gegebenen Qualitätsanspruchs, ausgedrückt durch die Garantiezeit und das prozentuelle Ausfallverhältnis, auf die zu erreichende Aufallsrate schließen zu können. Diese Kennzahl bildet eine wichtige Anforderung in der Entwicklung und Herstellung von komplexen Systemen und hat direkten Einfluss auf die Wirtschaftlichkeit eines Systems.

Die beiden Zusammenhänge sind in Abbildung 2.8 auf der nächsten Seite für unterschiedliche Garantiezeiten von ein bis zehn Jahren dargestellt.

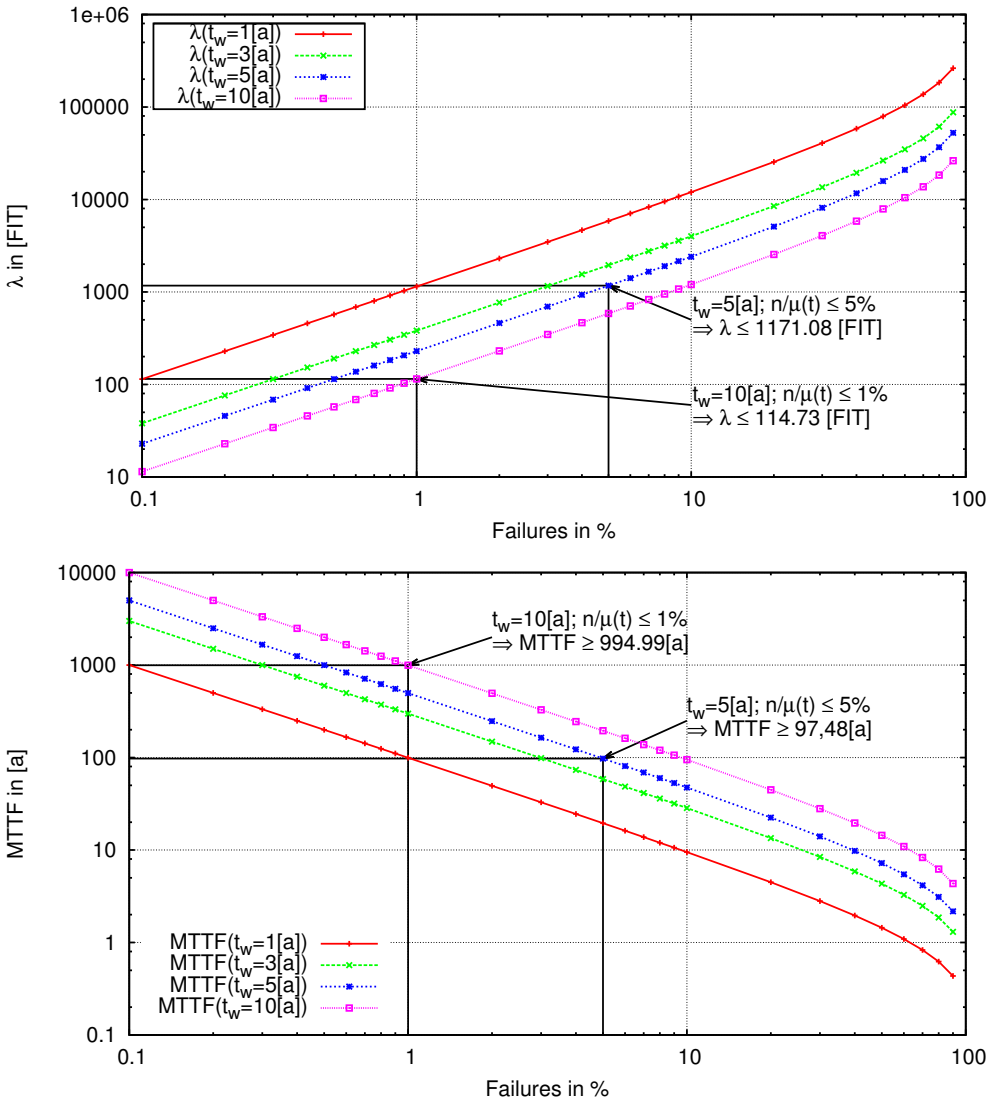


Abbildung 2.8.: Ausfallrate λ und deren Kehrwert $MTTF$ unter Annahme verschiedener Garantiezeiten (doppelt logarithmische Darstellung; 1 Jahr entspricht 8760 Einsatzstunden)

Mit Hilfe dieser Kurven lassen sich für den 24/7 Betrieb ($\rightarrow 8760\,\text{h/pro Jahr}$) die konkreten Grenzwerte direkt ablesen.

Zum Beispiel ergibt sich für die gegebene Garantiezeit von 5 Jahren und der Forderung, dass nach dieser Zeit maximal 5 % der Systeme ausgefallen sein dürfen, ein Vorgabewert für die Entwicklung von $\lambda \leq 1171{,}08\,\text{[FIT]}$ bzw. einen $MTTF \geq 97{,}47\,\text{[a]}$.

Erhöht man die Garantiezeit auf 10 Jahre und maximal 1% Ausfälle, muss die Entwicklung die bereits deutlich schwieriger zu erreichende Ausfallrate von $\lambda \leq$

114,73 [FIT] erfüllen. Umgerechnet bedeutet dies, dass nach 994,99 Jahren mehr als 37 % der Systeme ausfallsfrei ihre Aufgabe zu erfüllen hätten.

ANMERKUNG: *Abseits von Consumer electronic, also beispielsweise bei elektronischen Systemen im industriellen Einsatz, sind Garantiezeiten von fünf Jahren und mehr durchaus möglich bzw. von Endanwendern auch gefordert.*

2.3. Sicherheitstechnik

Sicherheit ist nach IEC61508 [IEC10, Teil 4] als die "*Freiheit von unvertretbaren Risiken*" definiert. Die *Sicherheitstechnik* dient demnach dem Zweck, Gefährdungen zu verringern um Schäden von Menschen und Umwelt fern zu halten. In der Entwicklung von sicherheitstechnischen Geräten wird die Zuverlässigkeitstheorie dazu verwendet, das Risiko eines gefährlichen Ausfalls zu bestimmen und entsprechende Systeme dahingehend zu optimieren.

Sicherheitstechnische Systeme sind aus Sicht dieser Arbeit deshalb interessant, da diese die höchsten Anforderungen an die Zuverlässigkeit stellen. Diese Anforderungen werden begleitet von strikten Vorgaben zu den Entwicklungsprozessen, sowie zu Maßnahmen der Validierung und Verifizierung von Kennwerten. Deshalb ist es unerlässlich, die Kennwerte und deren Ermittlung zu verstehen und in der Umsetzung mögliche Prozessanpassungen sowie die Entwicklung des Prediktionswerkzeugs, konform zu den Sicherheitsstandards einzuführen.

Nachfolgend werden die wichtigsten *Grundlagen und Kennwerte* der Sicherheitstechnik kurz vorgestellt. Die *Gegenüberstellung von Sicherheitstechnik und Standardtechnik* erfolgt in Abschnitt 2.3.2 auf Seite 35.

ANMERKUNG: Die Begriffe Sicherheit und Sicherheitstechnik sind im deutschen Sprachgebrauch zweideutig in Verwendung. Die hier im Fokus stehende *Funktionale Sicherheit [en: safety]* ist dabei nicht zu verwechseln mit der *IT-Sicherheit [en: security]*.

Sicherheitstechnische Standards

In Europa wurde die sicherheitstechnische Normung um 2005 neu definiert. Mit Einführung der generell anwendbaren Basisnorm IEC61508 [IEC10] wurde die Grundlage für eine Vielzahl abgeleiteter Normen geschaffen. Die damit abgedeckten Anwendungen gehen dabei von *einfachen Bearbeitungsmaschinen* über *Bahntechnik* bis zu *Atomkraftwerken*.

Die Normenbasis unterscheidet sich im Wesentlichen von den bisher gültigen sicherheitstechnischen Standards dadurch, dass der *statische, tabellarische Ansatz* gegen einen *probabilistischen Ansatz* ausgetauscht wurde. Konkret wird

dabei nun verlangt, dass *die Summe der Ausfallswahrscheinlichkeiten aller verwendeten Bauteile und Komponenten in einer Sicherheitskette kleiner als der geforderte, numerisch definierte Ausfallsgrenzwert* sein muss. Dies entspricht im Prinzip der Forderung nach Unterschreitung des *tolerierbaren Risikos*, auf welches im nächsten Unterkapitel näher eingegangen wird.

Neben den Kennwerten sind in den Standards *Prozesse* formuliert, welche unter anderem die Vorgehensweise für Entwicklung und Test vorgeben. Weiters gibt es eigene Normen zur Risikobeurteilung sowie gegebenenfalls zur Risikominderung von Sicherheitstechnischen Systemen.

Risiko

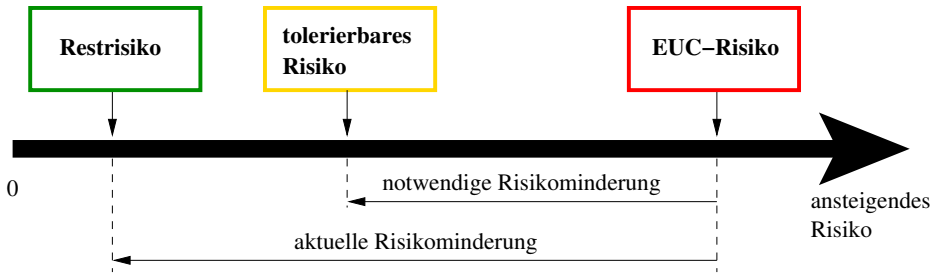


Abbildung 2.9.: Zusammenhang zwischen Risiko, Grenzrisiko und Sicherheitsmaßnahmen

Die Sicherheitstechnik ist stark verknüpft mit der Risikodefinition. Wie in Abbildung 2.9 dargestellt, besitzt jedes System ein, durch Bauart und Summe der verwendeten Bauteile vorgegebenes, Basisrisiko, das EUC-Risiko *[en: EUC: equipment under control]*. Gleichzeitig existiert ein definierter Risikogrenzwert des *tolerierbaren Risikos*, welcher durch Normen und Gesetze vorgegeben ist.

Liegt das Basisrisiko des Systems unter dieser Toleranzschwelle, gilt dieses als sicher. Liegt es darüber, müssen Maßnahmen getroffen werden, damit das Risiko um mindestens die *notwendige Risikominderung* verringert wird. Mögliche Maßnahmen sind dabei *Neukonstruktion*, Anwendung *sicherheitstechnischer Hilfsmittel* und *Benutzerinformation*. Diese Maßnahmen entsprechen den drei Schritten zur Risikominderung nach IEC 12100-1. Die Summe aller Maßnahmen ergibt die *aktuelle Risikominderung*.

Ein sicherheitsrelevantes System darf nur dann in entsprechenden Anwendungen eingesetzt werden, wenn dessen Basisrisiko bzw. das Restrisiko, nach Anwendung sicherheitstechnischer Maßnahmen, unterhalb des tolerierbaren Risikos liegt.

2.3.1. Kennwerte der Sicherheitstechnik

Im Rahmen einer *Baumusterzertifizierung* elektrischer, elektronischer und programmierbar elektronischer Geräte müssen diverse Kennwerte ermittelt oder festgelegt und den Abnahmebehörden sowie dem Anwender offengelegt werden. Die wichtigsten dieser Kenngrößen der Sicherheitstechnik sind in Tabelle 2.9 aufgelistet und werden im Anschluss genauer erklärt.

Abkürzung	Beschreibung	englischer Begriff
λ	Ausfallrate	failure rate
DC	Diagnosedeckungsgrad	diagnostic coverage
HFT	Hardware Fehlertoleranz	hardware fault tolerance
$MTTF_D$	Mittlere ausfallsfreie Zeit bis zu einem gefährlichen Ausfall	mean time to dangerous failure
PFD	Wahrscheinlichkeit eines Versagens auf Anforderung	probability of failure on demand
PFH	Versagenswahrscheinlichkeit pro Stunde (kontinuierlich); *Einheit* FIT *[en: failure in time]* $\rightarrow$ Ausfälle pro Zeiteinheit $1\,[FIT] = 10^{-9}\,[1/h] = 10^{-3}\,[ppm]$	probability of failure per hour
PFH_D	Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde	probability of dangerous failure per hour
SFF	Anteil sicherer Ausfälle bzw. Fehleraufteilungsrate	safe failure fraction
SIL	Sicherheits-Integritätslevel	safety integrity level

Tabelle 2.9.: Wichtige Kenngrößen der Sicherheitstechnik

Ausfallrate λ *[en: failure rate]*

In der Sicherheitstechnik wird die Ausfallrate gegenüber der Standardtechnik nochmals weiter präzisiert. Wie in Abbildung 2.10 auf der nächsten Seite dargestellt, setzt sich die Gesamtausfallrate aus *sicheren* und *gefährlichen* Anteilen (λ_S,λ_D) zusammen *[en: safe, dangerous]*:

$$\begin{aligned}\lambda &= \lambda_S + \lambda_D \\ &= \lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU} \qquad \text{Aufteilung der Ausfallrate}\end{aligned} \tag{2.25}$$

Sichere Ausfälle bedeuten dabei, dass durch diese Ausfallanteile keine zusätzlichen Gefährdungen entstehen. Dies ist beispielsweise bei nicht sicherheitstechnisch verwendeten Bauteilen, wie einer Status-LED abseits des kritischen Sicherheitspfads, der Fall.

Als *gefährliche Ausfälle* werden die Anteile bezeichnet, welche ohne weitere Maßnahmen eine potentielle Gefährdung auslösen.

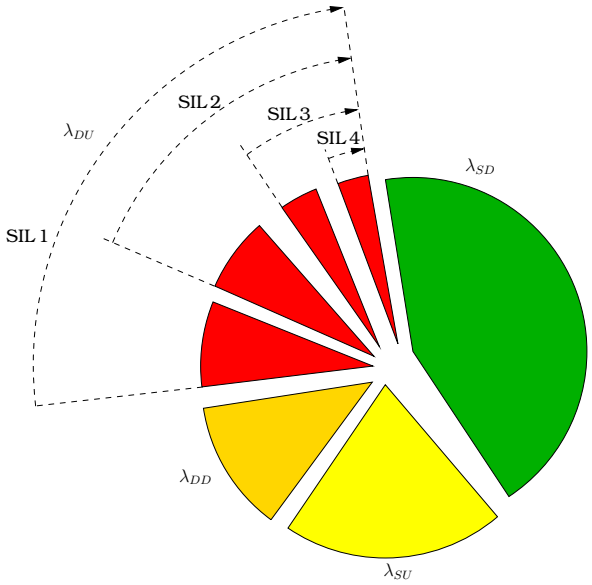


Abbildung 2.10.: Sicherheitstechnik: Aufteilung der Ausfallrate λ und Zuordnung der Safety Integrity Levels (SIL 1. . . 4)

Weiters werden die Ausfälle nach deren *Diagnostizierbarkeit* unterteilt. Der zweite Suffix der Ausfallsrate gibt dabei an, ob ein Ausfall der Kategorie *Entdeckt oder Unentdeckt* (*Detected* bzw. *Undetected*) zuzuordnen ist. So teilt sich λ_S in die in Gelb und Grün unterteilten Anteile von *sicheren entdeckten* und *sicheren unentdeckten* Ausfällen auf. Da beide Ausfallsanteile per Definition bereits sicher sind, kommt dieser Unterteilung nur eine untergeordnete Bedeutung zu.

Anders sieht es bei den gefährlichen Ausfällen aus. Potentiell *gefährliche aber entdeckte Ausfälle* (λ_{DD} in Orange) ermöglichen dem System eine entsprechende Reaktion. Somit ist diese Ausfallsart als sicher einzustufen. Die *Fehleraufdeckung*, als Maßnahme zur Erhöhung der entdeckten Ausfälle, kann nur durch konstruktive und softwaretechnische Maßnahmen während der Entwicklung verbessert werden.

Das Maß der *unentdeckt gefährlichen Ausfälle* λ_{DU} beschreibt schlussendliche das *Restrisiko*, dass ein System *in gefährlicher Art und Weise ausfällt*, was in der Grafik den roten Segmenten entspricht. Die Aufteilung dieser Segmente entspricht qualitativ den normativen Vorgaben für die Einstufung in die *Sicherheits-Integritätslevel SIL 1. . . 4*. Die niedrigsten Anforderungen werden dabei durch SIL 1 und die höchsten Anforderungen an die Restfehlerwahrscheinlichkeit durch SIL 4 ausgedrückt.

SFF, DC und HFT

Nach Ermittlung der genauen Aufteilung der Ausfallrate lässt sich der *Anteil sicherer Ausfälle SFF* und der *Diagnosedeckungsgrad DC* berechnen:

$$SFF = \frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_S + \sum \lambda_{DD} + \sum \lambda_{DU}} \tag{2.26}$$

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_D} \tag{2.27}$$

Dabei drückt die *Fehleraufteilungsrate SFF* das Verhältnis der *entdeckten Ausfälle* zu den *insgesamt möglichen Ausfällen* aus. Der *Diagnosedeckungsgrad* definiert den *Anteil der diagnostizierbaren, potentiell gefährlichen Ausfälle*.

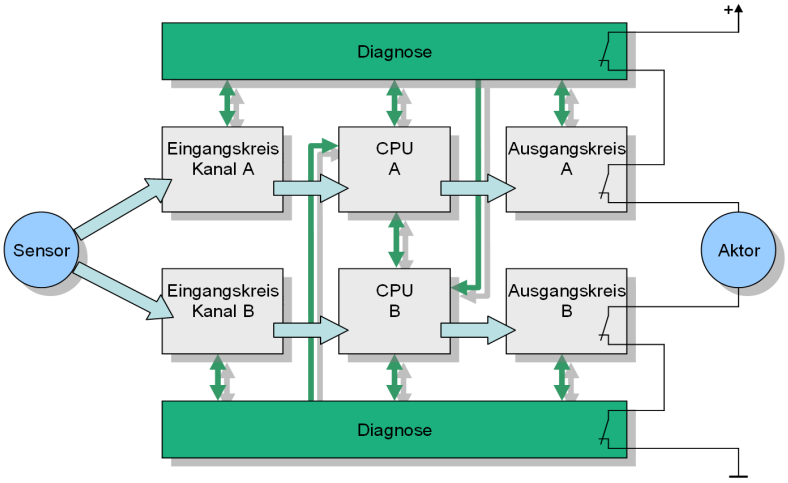


Abbildung 2.11.: Fehlersichere Hardware-Struktur mit HFT 1 (1oo2D); [siehe auch Bör06, S.287]

Die *Hardware-Fehlertoleranz HFT* drückt in der Sicherheitstechnik aus, wieviele *diagnostizierbaren Fehler und Ausfälle* innerhalb eines Systems auftreten dürfen, ohne die korrekte Ausführung der Sicherheitsfunktion zu beeinträchtigen. Eine HFT 1 definiert beispielsweise ein System, welches gegen *einen diagnostizierbaren Ausfall* resistent ist. Jeder weitere Fehler versetzt dieses System in einen potentiell gefährlichen Zustand, wo keine geordnete Fehlerreaktion mehr möglich ist.
ANMERKUNG: In der Sicherheitstechnik müssen Systeme so ausgelegt werden, dass eine *beliebige Anzahl von nicht diagnostizierbaren Fehlern und Ausfällen* innerhalb eines Systems dessen Funktionsfähigkeit nicht beeinträchtigen. Ob diese Fehler dabei parallel oder als Sequenz auftreten ist irrelevant.

Die Bezeichnung von hardwaretoleranten Systemen folgt üblicherweise dem Schema XooY *[en: X out of Y]*. Dies drückt die Fähigkeit einer entsprechenden

Architektur oder Struktur aus, noch korrekt zu arbeiten, wenn nur noch X von Y Kanälen intakt sind. Optional wird diese Bezeichnung durch den Suffix *D* für *Diagnose*, bei Systemen die zusätzliche Überwachungsmechanismen besitzen, erweitert. *1oo2D* beschreibt somit ein System, welches seine (sicherheitstechnische) Funktion bestimmungsgemäß ausführt, solange *einer von zwei* Kanälen korrekt arbeitet, was mittels Diagnose zusätzlich überwacht wird. Das Schema eines derartigen Systems ist zur Verdeutlichung in Abbildung 2.11 auf der vorherigen Seite dargestellt.

In der Praxis ist üblicherweise der zu erreichende *SIL-Level* durch das Risiko der Anwendung vorgegeben. Die *Hardwaretoleranz HFT* lässt sich durch Auswahl entsprechender Strukturen oder Geräte festlegen. Mit Hilfe von Tabelle 2.10 bestimmt man aus diesen beiden Angaben den mindestens zu erreichenden *Anteil der sicheren Ausfälle SFF*.

SFF	HFT 0	HFT 1	HFT 2
< 60 %	n.a.	SIL 1	SIL 2
60. . . < 90 %	SIL 1	SIL 2	SIL 3
90. . . < 99 %	SIL 2	SIL 3	SIL 3
≥ 99 %	SIL 3	SIL 3	SIL 3

Tabelle 2.10.: Zusammenhang zwischen *Fehleraufteilungsrate*, *Hardware Fehlertoleranz* und *Sicherheits Integritätslevel* [IEC10, Teil 2]

Umgekehrt angewendet kann die Entwicklung eines Sicherheitssystems durch günstige Wahl der HFT und der SFF wirtschaftlich positiv beeinflusst werden.

Beispiel: Es soll ein Sicherheitssystem für Anwendungen im Bereich *SIL 3* entwickelt werden. Legt man dem System eine Struktur mit *HFT 1* zugrunde, so muss mindestens eine *Fehleraufteilungsrate* von *90. . . < 99 %* erreicht werden. Alternativ ist das System auch mit einer höherwertigen *HFT 2-Struktur* realisierbar, was die Anforderung an die Fehleraufdeckung auf *SFF = 60. . . < 90 %* verringert.

PFD und PFH

Die Gleichungen zu PFD (*Probabilistic Failure on Demand*) und PFH (*Probabilistic Failure per Hour*) beschreiben den mathematischen Zusammenhang zwischen der gewählten Struktur für ein sicherheitstechnisches System und der Ausfallrate λ, unter Berücksichtigung der CCF (*Fehler gemeinsamer Ursache*) und spezifischer *Testintervalle zur Wiederherstellung* des betrachteten Systems.

So berechnet sich beispielsweise die *Wahrscheinlichkeit eines Versagens auf Anforderung PFD* für ein *1oo2D-System* wie folgt:

$$PFD_{1oo2D} = 2\,(1-\beta)\lambda_{DU}((1-\beta)\lambda_{DU} + (1-\beta_D)\lambda_{DD} + \lambda_{SD})t'_{CE}\,t'_{GE} + \\ + \beta_D\,\lambda_{DD}\,MTTR + \beta\,\lambda_{DU}(\frac{T_1}{2} + MTTR) \tag{2.28}$$

Die Bedeutung der einzelnen Größen (z.B. ist β in obiger Gleichung nicht zu verwechseln mit dem Formparameter der Weibullverteilung), sowie die weiteren Zusammenhänge sprengen den Rahmen dieser Arbeit und können bei Interesse im Standard IEC61508 [IEC10, Teil 6] nachgelesen werden.

Die Entscheidung ob *PFD oder PFH* einzusetzen ist, wird durch die Anwendung bestimmt. Bei Systemen mit *niedriger Anforderungsrate*, also dort wo eine Sicherheitsfunktion maximal einmal pro Jahr ausgeführt wird, setzt man *PFD* ein. Bei *hoher bzw. kontinuierlicher Anforderungsrate* wird die *PFH* verwendet.

Im Safety-Standard IEC61508 [IEC10, Teil 1] sind die *quantitativen Anforderungen an die Zuverlässigkeit von Sicherheitsbaugruppen* für die verschiedenen Sicherheits-Integritätsstufen definiert. Dabei gilt beispielsweise für SIL3 der Grenzwert für gefährliche Ausfälle pro Stunde: $10^{-8}[1/h] \leq PFH_D < 10^{-7}[1/h]$.

Dieser Wert gilt als Grenzwert für das gesamte System, also Messwerterfassung, Verarbeitung, Reaktion und Kommunikation. Dabei teilt sich die Ausfallrate so auf, dass 1% auf die Kommunikation und 10% auf die Verarbeitung entfallen dürfen. Somit ergibt sich also für die elektronische Sicherheitsbaugruppe ein Grenzwert von:

$$PFH_{D,\,SIL\,3,\,Baugruppe} < 10^{-8}\,[1/h] = 10\,[FIT] \text{ bzw.}$$
$$MTTF_{24/7} = 11\,415{,}53\,[a]$$

Der Vergleich dieser Ergebnisse mit den Resultaten der Ausfallraten- und MTTF-Berechnung auf Basis der Garantiezeit (Abschnitt 2.2.2 auf Seite 26) zeigt, dass die Anforderungen an sicherheitstechnische Baugruppen um ein Vielfaches höher sind, als an Standardbaugruppen. Diese höheren Anforderungen können entweder dadurch erreicht werden, dass die Entwicklung darauf ausgerichtet ist, eine entsprechend niedrige Basisausfallrate zu erreichen oder indem mittels Diagnose der Anteil gefährlicher Ausfälle entsprechend verringert wird, was aber meist die Basisausfallrate verschlechtert.

2.3.2. Standardtechnik vs. Sicherheitstechnik

Neben den bereits aufgeführten Beispielen gibt es weitere Unterschiede zwischen Baugruppen für den allgemeinen und sicherheitstechnischen Einsatz. In der nachfolgenden Tabelle sind einige qualitative Eigenschaften von Baugruppen in Automatisierungsanwendungen gegenübergestellt.

Non-Safety	Safety
Strukturelle Fehlertoleranz	
Üblicherweise steht nur eine CPU zur Verfügung, somit ist parallele Mehrfachausführung mit Quervergleichen ausgeschlossen. Programmierfehler oder (dynamische) Hardwarefehler sind u.U. sehr schwer nachverfolgbar.	Redundante oder gar diversitäre Ausführung des Laufzeitprogramms ermöglicht Diagnose von Abweichungen im Speicherabbild und von internen Verarbeitungsfehlern (CPU, Programmierfehler in System-SW, . . .)
Kommunikation	
Design von Kommunikationsschnittstellen und Protokollen erfolgt nach Effizienzkriterien	Kommunikation erfüllt Sicherheitsanforderungen → Die Wahrscheinlichkeit eines unentdeckten Fehlers muss für SIL 3 < 10^{-9} sein (Größenordnung: alle 100 000 Jahre ein unentdeckter Übertragungsfehler)
Ausfallreaktion	
Ausfälle in Hardware und Peripherie machen sich durch unvermittelte Systemabstürze und/oder untypisches Verhalten bemerkbar → schwer diagnostizierbar.	Ständige Prüfung auch nicht genutzter HW, wie beispielsweise momentan ungenutzter Speicherbereiche. Fehler in kritischen Teilen wie CPU, Speicher, Spannungsversorgung, Übertragungsstrecken usw. werden rasch aufgedeckt und können relativ leicht nachverfolgt werden.
Galvanische Trennung zur Ausfallseingrenzung	
Je nach Anwendung existiert galvanische Trennung nur zur Verarbeitungseinheit. Zur Nutzung von redundanten E/As müssen normalerweise mehrere Module herangezogen werden.	Galvanische Trennung zwischen Redundanzkanälen und zur Verarbeitungseinheit schützt das Gesamtsystem und ermöglicht überhaupt erst die Ein-/ Mehrfehlersicherheit.
Anwendungs-Programmierung der Systeme	
Verschiedenste Programmiersprachen anwendbar, auch hardwarenahe Sprachen wie Assembler, C, C++, . . .	Beschränkt auf wenige Programmiersprachen, typischerweise auf grafischer Basis wie z.B. FBD (IEC 61131)
Keine Absicherung von Compilern und lokalen Daten → Kein Schutz vor Verwechslung und Modifikation	Absicherung von Compilern und lokalen Programmdaten durch Mehrfachübertragungen, CRCs, . . .
Verfügbarkeit von Kennwerten	
Keine konkreten und geprüften Werte für Endanwender verfügbar.	Kennwerten müssen zur Zertifizierung vorliegen und entsprechend der Sicherheitseinstufung erfüllt werden.
Fehlertoleranz und Fehleraufdeckung	

bleibt im Allgemeinen unberücksichtigt	Abhängig von Architektur (1oo2, 1oo2D, 2oo3, etc.)
Qualitäts- und Prozessmaßnahmen	
Qualitätsvorgaben und deren organisatorisch verankerte Prüfung in Entwicklung und Dokumentation ist freiwillig und der jeweiligen Organisation freigestellt! → kein Verkaufsargument → bei Billigprodukten schwierig	Verschiedenste Maßnahmen: - Geprüfte Entwicklung, geprüfte Dokumentation (Entwicklungsdokumente, Benutzerdokumentation) - Betrachtungen zu Fehlern gemeinsamer Ursache - Änderungen müssen auf Auswirkungen überprüft, mit Prüfstelle abgesprochen, getestet, validiert und schriftlich hinterlegt werden - Verankerte Prozesse und Verfahren in Entwicklung, Produktion und Vertrieb

Tabelle 2.11.: Vergleich von Eigenschaften sicherheitstechnischer Produkte und Projekte mit Standard-Anwendungen

Betrachtet man die Kenngrößen der Sicherheitstechnik, so gilt es zu beachten, dass diese nicht mit den Standardgrößen verwechselt werden. Keinesfalls dürfen die Kennwerte von Standardsystemen für den sicherheitstechnischen Einsatz verwendet werden. Dies gilt besonders für MTTF und λ.

Da $MTTF_D$ nur die mittlere Zeit *bis zu einem gefährlichen Ausfall* berücksichtigt, ist diese immer *(viel) größer oder gleich* der mittleren Zeit bis zu einem Ausfall $MTTF$, welche *zusätzlich alle ungefährlichen Ausfälle* berücksichtigt. Die Ausfallrate entspricht dem Kehrwert der MTTF, somit gilt $\lambda_D \leq \lambda$ was in Abbildung 2.10 auf Seite 32 bzw. in Gleichung 2.25 auf Seite 31 offensichtlich wird.

Der relevante Wert für die Ausfallrate zur Berechnung von Garantiezeiten und Lagerhaltung ist nicht der sicherheitstechnische λ_D, sondern die Gesamtausfallrate λ als Summe der Ausfallraten von gefährlichen und ungefährlichen Ausfällen. Ein System welches auf gleicher schaltungstechnischer Basis für Standardaufgaben und für Sicherheitsaufgaben entwickelt wird, hat üblicherweise aufgrund des Zusatzaufwands an Bauteilen eine höhere Basisausfallrate. Dieser Zusatzaufwand stellt allerdings sicher, dass die überwiegende Mehrheit dieser Ausfälle keine gefährlichen Auswirkungen hat.

Abbildung 2.12 auf der nächsten Seite zeigt die direkte Gegenüberstellung von Standardrealisierung zu sicherheitstechnischer Realisierung einer diskreten digitalen Eingangsschaltung. Es ist sofort ersichtlich, dass allein durch die Anzahl der verwendeten Halbleiterbauelemente, die Basisausfallrate des Analog-

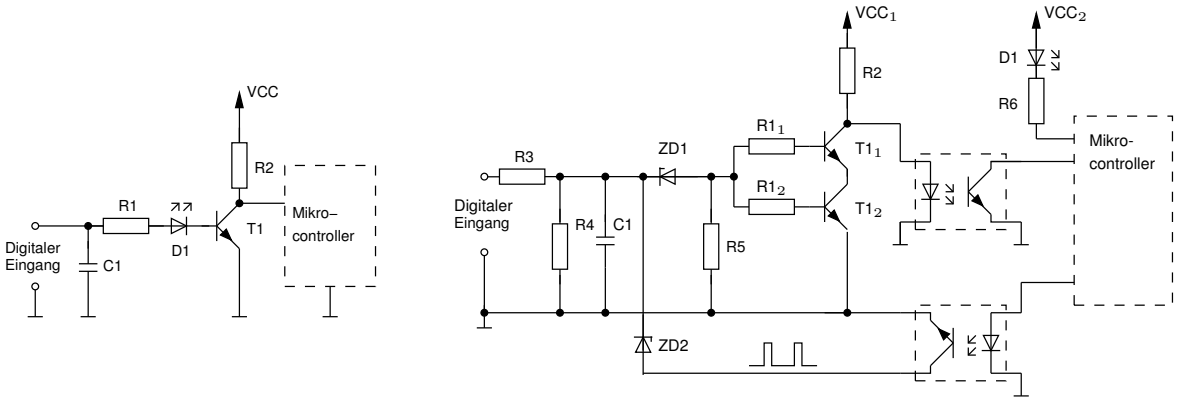


Abbildung 2.12.: Gegenüberstellung des Schemas eines Digitalen Eingangs in Standardausführung (links) und einer möglichen Sicherheitsvariante mit redundanten Eingangstransistoren und getakteter Diagnose (rechts)

teils der Sicherheitsschaltung in der Größenordnung mindestens dreimal so hoch sein wird wie die der Standardausführung.

Durch schaltungstechnische Maßnahmen zur Spannungs- und Strombegrenzung und dem Einsatz redundanter Schalttransistoren ist die sichere Variante der Standardschaltung gegenüber den Hauptausfallsursachen einzelner Bauteile deutlich überlegen. Die LED ist aus dem kritischen Pfad herausgenommen worden und wird nun direkt vom Mikrocontroller angesteuert, was den Wert von λ_{DU} verbessert. Durch die galvanische Trennung wird die logische Auswerteeinheit vom Eingangsteil entkoppelt. Schlussendlich garantiert die getaktete Diagnoseschaltung über ZD2, dass die Funktionsweise der Schaltung weitestmöglich diagnostiziert werden kann. Eine Prüfung mittels FMEA ergibt, dass lediglich ein Kurzschluss des Widerstands R3 als gefährlicher und unentdeckter Ausfall übrig bleibt.

Vergleicht man nun die Ausfallsraten dieser unentdeckt gefährlichen Ausfälle λ_{DU}, so erreicht die Standardschaltung einen Wert von mehr als 230 [FIT] und die Sicherheitsschaltung bleibt bei ca. 0,1 [FIT] (jeweils inklusive Berücksichtigung des Mikrocontrollers). Berechnet man die Gesamtausfallrate, dann verändert sich der Wert für die Standardschaltung nicht, das Ergebnis für die Sicherheitsschaltung erhöht sich auf $\lambda_{ges} = 350$ [FIT]. Das bedeutet, dass sich, aufgrund der zusätzlichen Sicherheitsmaßnahmen, die MTTF um ca. 50 % gegenüber der Standardschaltung verschlechtert.

Die Berechnung erfolgte nach Parts-Stress Methode auf Basis von Werten aus der SN 29500, bei 60 °C und unter Berücksichtigung der bauteiltypischen Ausfallsmodelle (Methode und Kennwerttabelle werden in nachfolgenden Kapiteln genauer vorgestellt).

Aufgrund der Ergebnisse ist klar ersichtlich, weshalb es unzulässig und sogar

gefährlich ist, Standardbaugruppen für Sicherheitstechnik einzusetzen.

TR 1 **Kennwerte der Sicherheits- und Standardtechnik berücksichtigen**
Für die Umsetzung des Werkzeugs zur Zuverlässigkeitsberechnung bedeuten die Erkenntnisse aus diesem Kapitel, dass sowohl Kenngrößen der Standard- als auch Sicherheitstechnik berechenbar sein müssen. Die genauere Betrachtung und *Aufteilung der Ausfallrate* und die daraus resultierenden Kennwerte zur *Fehleraufteilungsrate* sowie dem *Diagnosedeckungsgrad* müssen als Resultate vorliegen.

2.4. Ermittlung von Kenngrößen

Nachfolgend werden Varianten zur Ermittlung der Zuverlässigkeitskenngrößen vorgestellt und miteinander verglichen. Der Vergleich bezieht sich dabei auf die praktische Einsetzbarkeit in der Entwicklung von elektronischen Baugruppen. Das Ergebnis dieses Vergleichs dient zur Auswahl der geeigneten Methode in der Umsetzungsphase dieser Arbeit (Kapitel 8.2 auf Seite 142).

Ermittlungsverfahren von Zuverlässigkeitskenngrößen lassen sich in *Analysen während der Entwicklung* und *Analysen basierend auf statistischen Aufzeichnungen* zu Ausfällen während Produktion und Betrieb, wie beispielsweise den Reparaturrückläufer-Statistiken, aufteilen. Der Einfachheit halber werden diese beiden Ansätze in Folge kurz als *prediktive* und *empirische* Verfahren bezeichnet.

Eine Verfeinerung der Unterteilung von prediktiven Methoden nach Ermittlung der *Ausfallarten*, *Ausfallraten* und der *Systemzustandsanalyse* ist in Abbildung 2.13 auf der nächsten Seite dargestellt.

Das Ziel der prediktiven Ansätze ist es, schon in frühen Entwicklungsphasen, Kenngrößen möglichst genau zu ermitteln. Mittels statistischer Erfassung von Ausfallsraten und deren empirischer Auswertung können während Fertigung und Betrieb die Kennwerte aus der Entwicklung kontrolliert und verfeinert werden. Zusätzlich dient die Überwachung der Fehlerfälle nach Auslieferung der Systeme zur Warnung bei auffälligen Ausfallshäufungen. Im Rahmen dieser Arbeit werden die statistischen Werte zur *Verifikation der Umsetzung* und zur *Abschätzung des praktischen Nutzwerts* der Ergebnisse aus dem Prediktionswerkzeug hergenommen.

Auf weitere Fragestellungen und Probleme die im Laufe des *Lebenszyklus* eines Systems in Zusammenhang mit den Kennwerten beantwortet werden sollten, wird in Abschnitt A.2 auf Seite 172 kurz eingegangen.

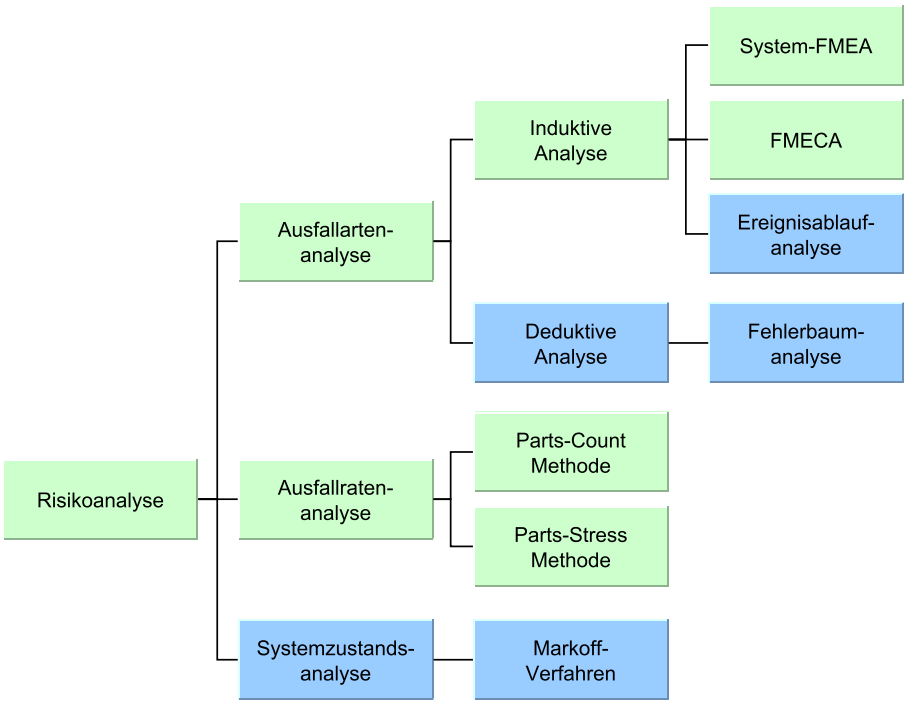


Abbildung 2.13.: Einteilung der Risiko- und Zuverlässigkeitsanalyse-Methoden [Pau03]. Grün hinterlegt sind die Methoden die in der Umsetzung des Analyse- und Berechnungswerkzeugs berücksichtigt werden.

2.4.1. Analytische Methoden während Entwicklungsphase

Ausgewählte *prediktive Methoden* werden nachfolgend kurz vorgestellt und in Kapitel 8.2 auf Seite 142 nach Eignung für die Umsetzung des Berechnungswerkzeugs bewertet.

Details zu den Verfahren, deren mathematischem Hintergrund und Anwendungsbeispiele finden sich in Birolini [Bir07], Dhillon [Dhi05, Kapitel 6], Pauli [Pau03] und Wilde [Wil06, Kapitel 5].

ANMERKUNG: Die nachfolgende Übersicht ist nicht vollständig. Neben den dargestellten Methoden werden weitere Verfahren wie *Petri-Netze*, *HAZOP-Analyse*, *Sneak-Circuit-Analyse* etc. in der Praxis angewendet. Die hier getroffene Auswahl beschränkt sich auf Methoden, welche in der einschlägigen Fachliteratur als anerkannter Standard gelten und für den Einsatz als Analysemethode in der Sicherheitstechnik zugelassen sind.

Fehlerzustandsart- und -auswirkungsanalyse FMEA[2] [IEC06a]

Bei der FMEA *[en: failure mode and effects analysis]* handelt es sich um eine *induktive Analysetechnik*. Bei dieser wird ausgehend vom höchsten Detailgrad, bei elektronischen Systemen ist dies die Bauteilebene, auf das Gesamtsystem geschlossen (*Bottom-Up Verfahren*). Durch Betrachtung jeder einzelnen Funktionseinheit und deren Ausfallsmechanismen wird ein vollständiges Bild des Ausfallverhaltens eines Systems erstellt.

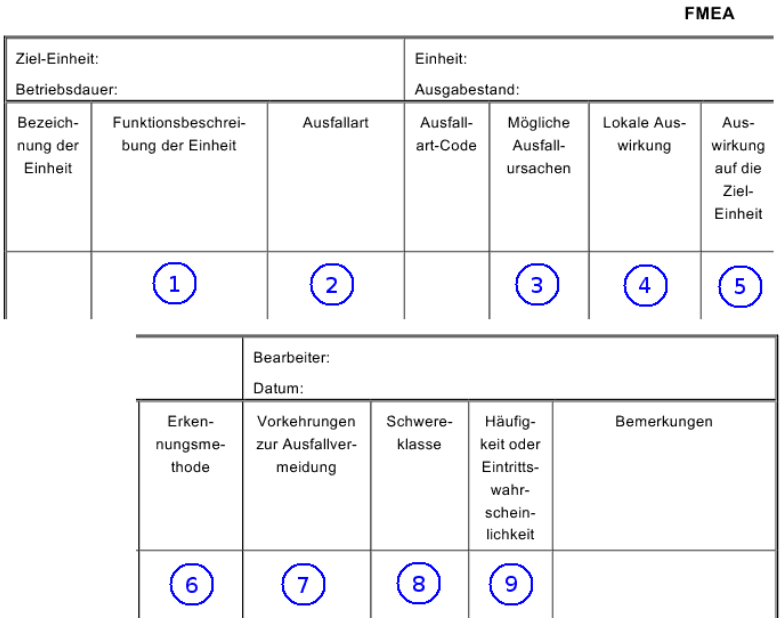


Abbildung 2.14.: Beispiel für das Format eines FMEA Arbeitsblattes [IEC06a, S. 36]

Abbildung 2.14 zeigt Ausschnitte eines Arbeitsblatts, wie es zur Durchführung einer FMEA herangezogen wird. Für jede potentiell gefährliche Situation wird eine Zeile angelegt, in welcher der Reihe nach folgende Fragen beantwortet werden:

1 - Funktionsbeschreibung Was ist die Funktion der betrachteten Einheit?

2 - Ausfallart Bei elektronischen Bauelementen werden üblicherweise die Fälle “Kurschluss”, “Leerlauf” und “Stuck-At” betrachtet. Der dritte Fall bezeichnet einen statischen, irreversiblen Zustand nach Zerstörung einer Funktionseinheit.

3 - Mögliche Ausfallursache Vollständige Aufzählung denkbarer Ursachen die zum beschriebenen Ausfall führen können.

2 Details zur deutschen Bezeichnung und Alternativen dazu im Abkürzungsverzeichnis

4 - Lokale Auswirkung Beschreibung der direkten Auswirkung auf das betrachtete Element und direkt vom Ausfall betroffene Nebenelemente.

5 - Auswirkung auf Zieleinheit Betrachtung des Ausfalls auf die Gesamteinheit.

6 - Erkennungsmethode Kann der Ausfall nach Auftreten diagnostiziert werden? Wie?

7 - Vorkehrungen zur Ausfallvermeidung Kann der Ausfall im Vorhinein, beispielsweise durch konstruktive Mittel oder Benutzerinformation vermieden werden? Können Symptome automatisch ausgewertet werden und kann in Folge dem Ausfall entgegengewirkt werden?

8 - Schweregrad/-klasse Einteilung in Schweregrad nach Auswirkung bzw. sicherheitstechnischer Relevanz;

9 - Häufigkeit oder Eintrittswahrscheinlichkeit Klassifizierung nach normiertem Schema oder Eintrag der Ausfallwahrscheinlichkeit laut beschriebenem Modell. Bei elektronischen Bauteilen können die Werte aus Bauteildatenbanken bezogen werden.

Mit einer FMEA lassen sich voneinander abhängige Ausfälle und auch Fehlersequenzen beschreiben. In Kombination mit anderen Methoden, wie beispielsweise dem *Parts Stress Verfahren*, lässt sich die Genauigkeit der Ausfallratenbestimmung deutlich erhöhen.

Zuverlässigkeits-Blockdiagrammanalyse RBD [IEC06c]

Das Verfahren des *Zuverlässigkeits-Blockdiagramms [en: reliability block diagram]* oder *Ereignisablauf- bzw. Ausfallratenanalyse* ist ein *kombinatorisches Modell* zur qualitativen und quantitativen Zuverlässigkeitsanalyse.

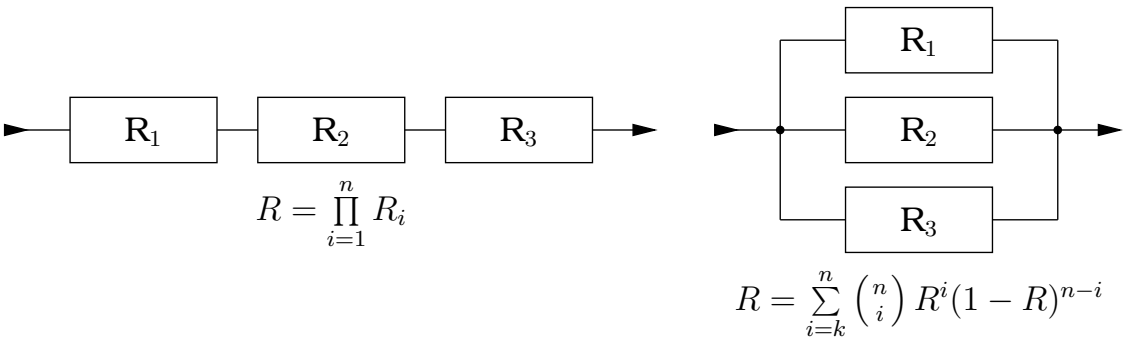


Abbildung 2.15.: Ereignisablaufanalyse - Darstellung und Berechnung von Serien- und Redundanzstruktur

Durch Serien- und Parallelschaltung von einfachen Blöcken (Komponenten, Bauelemente) wird der logische Zusammenhang der Zuverlässigkeit auf höchster Detailebene beschrieben. Die Blöcke können dabei nur zwei Zustände annehmen: *Betrieb oder Ausfall*.

Ein Nachteil dieser Methode ist, dass nicht alle Ausfallvarianten pro Bauelement mit einem Blockdiagramm beschreibbar sind, sondern vielmehr pro Ausfallvariante ein eigenes Blockdiagramm erstellt werden muss. Zur numerischen Analyse kann die Vielzahl möglicher Bäume vernachlässigt werden und, im Sinne einer Maximalwertaufgabe auf Basis der Hauptausfallursache jedes einzelnen Elements, der Worst-Case Fall modelliert und berechnet werden. Zuverlässigkeitsblockdiagramme sind zur Analyse von zeitabhängigen Ereignissen und somit auch Ausfallsequenzen ungeeignet.

Fehlzustandsbaumanalyse FTA [IEC06b]

Die *Fehlzustandsbaumanalyse* oder *Fehlerbaumanalyse [en: fault tree analysis]* ist ein *Top-Down Analyseverfahren*. Dabei erfolgt eine Verfeinerung von Grundannahmen, von einer höheren Systemebene (Hauptereignisse) auf eine niedrigere Systemebene (Unterereignisse). Dieser deduktive Ansatz wird wiederholt, bis eine weitere Aufteilung entweder nicht möglich oder nicht sinnvoll ist und somit die auslösenden Basisereignisse oder Komponenten identifiziert sind.

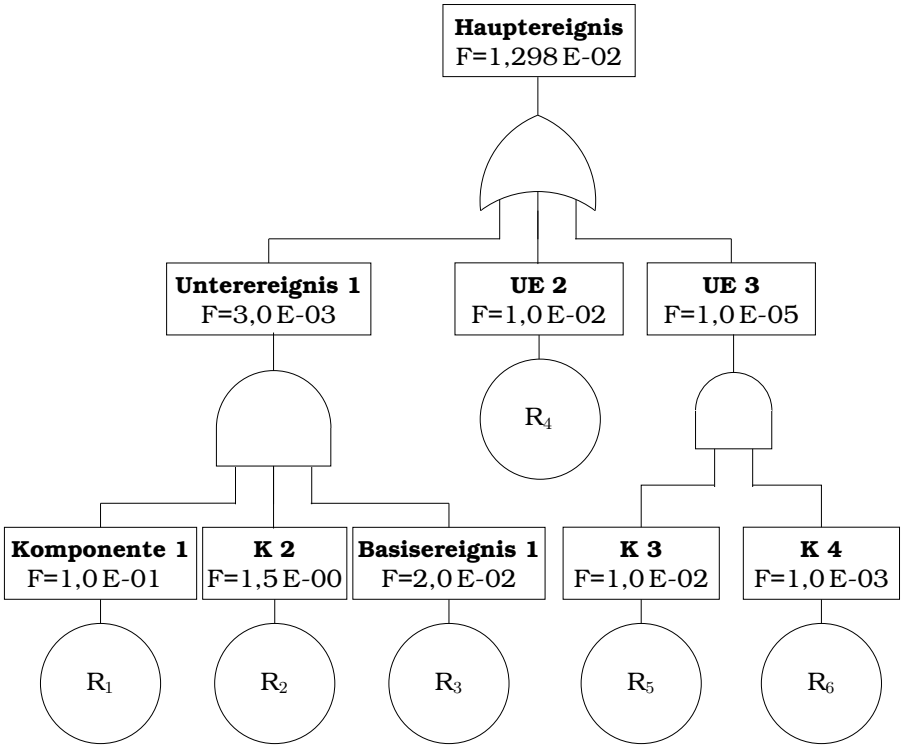


Abbildung 2.16.: Fehlzustandsbaumanalyse - Darstellung und Berechnung eines einfachen Beispiels laut [IEC06b]

Mit Hilfe logischer Verknüpfungen wird der Zusammenhang zwischen Unterereignissen und Hauptereignissen dargestellt. Wie in Abbildung 2.16 an einem einfachen Beispiel dargestellt, setzt sich die Ausfallwahrscheinlichkeit des

Hauptereignisses aus der logischen Kombination der Basisereignisse zusammen. Die Methode ist dabei nicht darauf beschränkt, Ausfallwahrscheinlichkeiten zu berechnen. Auf die gleiche Art ist eine *numerische Erfolgsanalyse* durchführbar, wobei dabei die Konzentration auf Erfolgsereignissen statt Ausfällen liegt. Neben der numerischen Anwendbarkeit ist auch eine rein *qualitative Analyse* möglich, wo beispielsweise eine Kategorisierung von Ereigniswahrscheinlichkeiten in “Hoch”, “Mittel” und “Niedrig” durchgeführt wird. Je nach Anwendung ist das Verfahren als *Ausfallraten-* (numerisch) oder *Ausfallartenanalyse* (qualitativ) einzustufen.

Markov-Verfahren [IEC06d]

Die Markov-Analyse ist eine sehr populäre quantitative Variante der Zuverlässigkeitsanalyse. Als *zustandsbasiertes stochastisches Verfahren* ist dieses nutzbar, statistisch unabhängige Ausfallsequenzen zu berücksichtigen und numerisch zu bewerten.

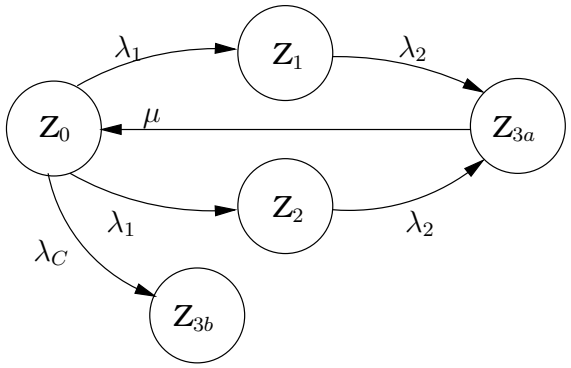


Abbildung 2.17.: Markov-Kette einer redundanten Struktur mit gemeinsamer Ausfallursache Z_{3b} und Reparaturmöglichkeit μ; [IEC06d]

In Abbildung 2.17 ist eine aktiv redundante Struktur, beispielsweise aus zwei gleichartigen Pumpen bestehend, dargestellt. In Zustand Z_0 arbeiten beide Pumpen in Teillast und haben eine Ausfallrate von λ_1. Fällt eine der Pumpen aus, übernimmt die jeweils andere deren Arbeitsanteil, was sich aber in einer höheren Beanspruchung und somit einer höheren Ausfallrate λ_2 niederschlägt. In Z_{3a} sind beide Pumpen ausgefallen und das System ist somit nicht mehr funktionsfähig. Um das System wieder in den funktionsfähigen Zustand zurückzuversetzen, wird in diesem Beispiel die Annahme getroffen, dass beide Pumpen gleichzeitig mit der Reparaturrate μ wieder Instand gesetzt werden. Der Zustand Z_{3b} wird durch einen *Ausfall gemeinsamer Ursache* λ_C erreicht. Dieser Ausfall wird in der Praxis beispielsweise durch einen Produktions- oder Serienfehler der Pumpen repräsentiert.

Die mathematische Behandlung der Markov-Ketten erfolgt durch Aufstellen eines Differentialgleichungssystems. Die numerische Auswertung kann beispiels-

weise via Monte Carlo Analyse durchgeführt werden.

Das Aufstellen des Markov-Diagramms ist bereits im hier vorliegenden, sehr einfachen Fall, nicht trivial. Die Komplexität und auch die Anzahl der Zustände steigt mit jeder zusätzlich betrachteten Komponente rapid an. Systeme mit dutzenden oder mehr Bauelementen sind nur durch Aufteilung in Teilsysteme erfassbar.

Part-Count Methode

Das einfachste Verfahren der numerischen Ausfallratenbestimmung eines Systems ist gleichzeitig deren *ungenaueste Variante*. Nachdem jedem Element dessen typische Ausfallrate zugeordnet wird, beispielsweise durch Einsatz einer Ausfallratendatenbank, summiert man alle Elemente ohne Rücksicht auf Struktur, Topologie oder Abhängigkeit untereinander auf. Das Ergebnis entspricht automatisch dem Wert einer Worst-Case Betrachtung unter Einbezug der tatsächlichen Ausfallkennwerte einzelner Bauelemente, jedoch ohne der Betrachtung von Umwelteinflüssen.

Part-Stress Methode

Die *Part-Stress* Methode erweitert die Parts-Count Methode um die Berücksichtigung von Umwelteinflüssen auf die Ausfallraten der einzelnen Komponenten.

Es handelt sich dabei um eine analytische Methode auf Basis mathematischer Bauteilmodelle. Dabei wird die Basisausfallrate λ_0 mit unterschiedlichen Korrekturfaktoren π multipliziert. Diese Faktoren sind für die verschiedenen Umwelteinflüsse entweder aus Tabellen und Datenblättern ablesbar oder mathematisch bestimmbar.

$$\lambda = \lambda_0 \cdot \pi_U \cdot \pi_I \cdot \pi_T \tag{2.29}$$

λ_0 ... Basisausfallrate unter Referenzbedingungen

π_U ... Faktor für Spannungsabhängigkeit

π_I ... Faktor für Stromabhängigkeit

π_T ... Faktor für Temperaturabhängigkeit

Ein Beispiel für einen mathematisch bestimmbaren Faktor ist die Temperaturabhängigkeit nach Arrhenius. Dieser Faktor wird beispielsweise für Kondensatoren oder Widerstände angewendet:

$$\begin{aligned} \lambda_T &= \lambda_0 \cdot e^{(\frac{1}{T_0} - \frac{1}{T}) \cdot \frac{E_a}{k}} \\ \Rightarrow \pi_T &= e^{(\frac{1}{T_0} - \frac{1}{T}) \cdot \frac{E_a}{k}} \end{aligned} \tag{2.30}$$

Weitere Korrekturfaktoren, z.B. für Schaltraten und Umgebungsbedingungen, sind verfügbar (siehe [IEC09]).

Neben der Möglichkeit die Abhängigkeit der Ausfallrate von den verschiedenen Umwelteinflüssen in beliebigen Kombination durch entsprechende Kurvenscharen auszudrücken, lässt sich durch geeignetes Einsetzen von Grenzwerten eine obere Schranke für die Ausfallrate angeben. Diese *Worst-Case* Betrachtung ist vor allem in sicherheitstechnischen Anwendung wichtig.

Sowohl die Part-Stress Methode als auch das Part-Count Verfahren lassen sich bei Vorliegen der mathematischen Zusammenhänge und der Bauteilkennwerte sehr einfach automatisch berechnen. Da keinerlei Berücksichtigung der Abhängigkeiten zwischen Bauteilen erfolgt, ist die tatsächliche numerische Differenz zum Realwert abhängig vom tatsächlichen Aufbau (z.B. Platzierung von Bauteilen, Leitungsführung) und der Komplexität des Gesamtsystems (einfache vs. aufwändige Schaltung).

2.4.2. Statistische Erfassung von Reparaturrückläufern

Die statistische Erfassung möglichst vollständiger Daten zu Ausfallsraten und deren Ursachen ist eine in der Praxis häufig angewendete *empirische Methode* zur Überprüfung von Zuverlässigkeitsaussagen.

Die Qualität dieser Auswertungen hängt maßgeblich von der Anzahl der Datensätze und dem Detailgrad der erfassten Daten ab. Bereits vor Beginn der Datensammlung sind Richtlinien festzulegen, welche zumindest eine klare Zieldefinition sowie Regeln zum Eintrag und zur Interpretation der Daten enthalten. Die Beantwortung von Fragenkatalogen, wie nachfolgend angedeutet, helfen bei der Festlegung dieser Definitionen:

Wann beginnt die Lebensdauer einer Baugruppe?
- Herstelldatum des ältesten Bauteils
- Fertigungszeitpunkt des Moduls
- Übergabezeitpunkt an End-Kunden (sofern bekannt)
- Ersteinsatz

Welche Zeiten zählen zur Einsatzdauer?
- reale Einsatzzeiten (unter Teil- bzw. Voll-Last)
- Lagerzeiten (beim Hersteller, Zwischenhändler, Endanwender)
- Lieferzeiten

Wie wird mit Systemänderungen umgegangen und was gilt als Änderung?
- Bauteile werden ersetzt, z.B. wegen Abkündigungen
- Systemrevision wegen Softwareänderung (Fehlerbehebung, neue Funktionen)
- Systemrevision wegen Hardwareänderung

Weitere Fragestellungen, eingeteilt über die gesamte Lebensdauer eines Systems, sind in Tabelle A.2 auf Seite 173 zu finden.

Wichtig ist zu erkennen, dass getroffene Definitionen weitreichende Auswirkungen sowohl auf die Ergebnisse der Auswertungen als auch auf die betrachteten Systeme an sich haben können. Beispielsweise lassen sich reale Werte für die Einsatzdauer nur dann erfassen, wenn entweder Kunden bei dieser Erfassung mitarbeiten oder das System mit einer Funktion zur automatischen Aufzeichnung der Daten ausgeliefert wird. Je nach Kundenstruktur ist aber dem Hersteller der Endanwender gar nicht bekannt und somit eine kooperative Methode nicht anwendbar. Die Zieldefinition der statistischen Erfassung ist deshalb notwendig, da es sowohl in der Erfassung als auch Auswertung der Daten zu unterscheiden gilt, ob der tatsächliche Wert der MTTF bestimmt werden soll, oder lediglich Daten zum Nachweis der Garantieerfüllung gesammelt werden. Bei Letzterem ist die Erfassung deutlich einfacher aber auch ungenauer und somit mit Risiko behaftet. Stellt ein Kunde von Lagerhaltung auf on-demand Lieferung um, verändern sich die erfassten Werte zum Schlechteren, ohne dass sich etwas an der eigentlichen Qualität der Systeme veränderte.

Werden die statistischen Daten zur tatsächlichen Qualitätsbestimmung und -sicherung verwendet, so sind auch hier weitere Überlegungen notwendig. Komplexe elektronische Baugruppen bestehen üblicherweise neben einer Vielzahl von unterschiedlichen Bauteilen auch aus Softwareteilen, welche entsprechend statistisch berücksichtigt werden müssen. Deshalb ist es bei der Auswertung von Reparaturrückläufern unerlässlich, in einer ersten Phase tatsächliche Hardwareausfälle durch Defekte von Ausfällen bedingt durch fehlerhafte Software, Konfigurationsproblemen und Bedienfehler zu trennen. Nichts desto trotz haben Fehler in Software großen Einfluss auf die Gesamtausfallstatistik. Das Restrisiko von unentdeckten Fehlern, beispielsweise in Firmware oder programmierbaren Bausteinen wie FPGAs, ist beeinflusst durch den Grad der Testabdeckung in der Entwicklungs- und Systemintegrationsphase. Im Gegensatz zu den meisten Hardwareproblemen ist der große Vorteil bei Ausfällen durch Software, dass diese üblicherweise durch Patches, ohne Austausch des Systems, behebbar sind und nachfolgend nicht mehr auftreten können. Der große Nachteil ist, dass immer sämtliche Systeme betroffen sind.

In der Praxis zeigt sich, dass die genannten Überlegungen im Vorhinein entweder nicht oder nur unvollständig gemacht oder diese nur unzureichend eingehalten werden. Resultierend daraus sind die daraus gewonnenen Datensätze nur bedingt verwendbar. Alternativ dazu können die Daten unter abgeschwächten Regeln betrachtet werden, was deren Aussagekraft jedoch negativ beeinflusst.

Offensichtliches Grundproblem jeder statistischen Methode die auf Rückläuferdaten basieren ist die Unzulänglichkeit als Alarmsystem. Bis eine repräsentative Anzahl von Rückläufern bei einer neu entwickelten Baugruppe, über eine Vielzahl von Kunden, statistisch relevante Aussagen zulassen, können viele Jahre vergehen. Wird erst dann festgestellt, dass zugesicherte Garantiezeiten in der

Praxis deutlich unterschritten werden, bleibt oft nur drastisches Redesign und (kostenloser) Austausch.

Selbst vergleichende Voraussagen sind kritisch zu beurteilen. Wird ein empirisch ermittelter Wert herangezogen um eine überarbeite Version eines Systems zu beurteilen, dann bleiben selbst bei Einhaltung sämtlicher statistischer Regeln immer noch erhebliche Unsicherheiten bezüglich Lücken im Datenbestand.

Zusammenfassend wird festgehalten, dass unter den Voraussetzungen ordentlicher Planung und Durchführung die Rückläuferstatistik, bei entsprechendem mathematischen Aufwand, sinnvoll sein kann. Dabei sind jedoch die große Zeitverzögerung bis zum Erhalt und die Problematik der Missinterpretation durch Unvollständigkeit der Daten zu berücksichtigen. Zur Qualitätsbestimmung wird diese Methode nicht empfohlen, als Kontrollmethode für zuvor prediktiv ermittelte Qualitätsdaten ist sie verwendbar.

2.4.3. Abweichungen zwischen prediktiven und empirischen Methoden

Üblicherweise ergeben sich zwischen berechneten und statistisch erhobenen Ausfallsdaten erhebliche Differenzen aufgrund unterschiedlichster Fehlerquellen:

Prediktive Methoden	Empirische Methoden
Berechnungsfehler	
Unpassende oder zu ungenaue Analysemethode	Qualität der statistischen Daten (Ungenauigkeiten in Erfassung und Auswertung)
Ungenauigkeit von Herstellerangaben von Bauelementen	Ungenügender Run-In (Frühausfallsphase noch nicht überwunden)
Erfahrung des Anwenders (bei manueller Berechnung)	Unbekannte reale Einsatzdauer
Vergessene Neuberechnung bei Revisionen	Unbekannte und nicht erfasste Umgebungsbedingungen bei Lagerung
Annahmen zu Umgebungsbedingungen (z. B. reale Einsatzhöhe, lokale Temperaturen in System, usw.)	Nicht erfasste Betriebsbedingungen

Tabelle 2.12.: Beispiele für potentielle Fehlerquellen prediktiver und empirischer Methoden bei der Kennwertbestimmung

Mathematisch wirken auftretende Ungenauigkeiten nach den Gesetzen der Fehlerfortpflanzung. Einige der angeführten Punkte lassen sich durch Kontrolle

und Ausbildung verbessern, bei anderen ist es schwierig, auch nur eine grobe Abschätzung des Fehlers anzugeben.

Bereits im vorigen Abschnitt wurde festgestellt, dass empirische Methoden als prediktives Mittel bestenfalls kritisch zu beurteilen sind. Im Geschäftsalltag hat dies zwei Seiten:

1. Für Ersatzteilplanung, Garantieberechnungen und wirtschaftliche Rückschlüsse sind die empirisch erhobenen Daten meist ausreichend. Tatsächlich werden nur jene Ausfälle finanziell schlagend, welche auch tatsächlich urgiert werden, unabhängig von der Qualität.
2. Besteht der Wunsch nach möglichst langfristiger Kundenbindung dann muss danach gestrebt werden, möglichst alle Ausfälle zu erheben. Neben dem zusätzlich entstehenden Aufwand, auf Kunden- und Herstellerseite, setzt sich der Hersteller, durch die erhöhte Aufmerksamkeit, erhöhtem Erklärungsbedarf bei auftretenden Qualitätsproblemen aus.

Bei Anwendung analytischer Methoden sind folgende Anmerkungen zu berücksichtigen:

- Die Voraussage von Zuverlässigkeitskennwerten unterliegt selbst bei korrekter, gewissenhafter Anwendung der Methoden einer erheblichen Differenz gegenüber den praktisch erzielten Werten.
- Werden identische Methoden bei gleichen Rahmenbedingungen angewendet, sind die daraus berechneten Zuverlässigkeitsdaten relativ zueinander sehr genau. Aussagen ob sich Designs gegenüber Referenzen verbessert oder verschlechtert haben, können damit getroffen werden.

3. Stand der Technik

Das vorliegende Kapitel betrachtet die Aufgabenstellung aus dem Blickwinkel der heute vorhandenen Mittel und Werkzeuge um diese gemäß Zielsetzung korrekt umzusetzen.

Abschnitt 3.1 stellt unterschiedliche Quellen für Bauteilkenndaten vor, welche zur analytischen Kenndatenermittlung von elektronischen Geräten herangezogen werden können.

Im Abschnitt 3.2 auf Seite 55 werden mehrere kommerziell verfügbare, Computer gestützte Werkzeuge zur analytischen Zuverlässigkeitsberechnung kurz vorgestellt und verglichen. Diese Marktübersicht und -analyse hat die Aufgabe, die Relevanz einer Eigenentwicklung zu untermauern.

Wie in Kapitel 2 auf Seite 9 handelt es sich bei den hier gewonnenen Erkenntnissen um Grundlagen bezüglich des Vorgehensmodells von Kruchten (1.2 auf Seite 3) und sind den Sichten *Prozess* und *Physik* zuzuordnen.

3.1. Kenndaten elektronischer Bauelemente

3.1.1. Herstellerangaben und Kennwert-Datenbanken

Zur Zuverlässigkeitsvorhersage können unterschiedliche Quellen herangezogen werden. Am genauesten und deshalb zu bevorzugen sind konkrete Herstellerangaben zu den exakt verwendeten Bauteiltypen. Probleme bei der praktischen Anwendung sind:

- Verfügbarkeit beim Hersteller
- Korrektheit der Herstellerangaben
- Aufwand zur Erfassung; Korrektur/Anpassung bei jeder Bauteiländerung
- Mögliche Fehler bei der Übertragung in Kenndatendatenbank

Als nächstbeste Quelle dienen Normen und normenähnliche Handbücher mit Listen von Basisdaten zu unterschiedlichen Bauteiltypen, sowie mathematischen Modellen zur Kennwertkorrektur, in Abhängigkeit von Umgebungsbedingungen. Diese Daten basieren üblicherweise auf langjährigen Untersuchungen

und Beobachtungen in Entwicklung und Fertigung. Tabelle 3.1 zeigt eine Auswahl von Kennwert-Datenbanken, welche in unterschiedlichen Anwendungsbereichen angewendet werden.

Bezeichnung	Hersteller / letztes bekanntes Update	Ursprung
SAE	*Society of Automotive Engineers, 1987*	Automotive
SN29500	*Siemens AG, 2011 (laufende Updates)* Die Siemens Norm 29500 basiert auf Überwachung und Verfolgung firmeninterner Entwicklungen von Bauteilen und deren Einsatz in Baugruppen. Als Berechnungsbasis wird die IEC 61709 verwendet (Referenzkonditionen und Stressmodelle).	Industrie
MIL-HDBK-217	*Department of Defense, 1995* US Military Standard, Sehr komplexer, weitreichender Standard und deshalb auch schwierig zu implementieren. Sehr pessimistische Daten und deshalb sind darauf basierende Ergebnisse als Worst Case einzustufen.	Militär
Bellcore / Telcordia SR-332	*Telcordia, früher Bell Communications Research, 2006* Der Special Report 332: Reliability Prediction Procedure for Electronic Equipment	Telekommunikation
RAC PRISM	*Reliability Analysis Center, 2000*	Militär / Kommerziell
British Telecom HRD4 and HRD5	*British Telecom* Handbook of Reliability Data for Components; used in Telecommunication Systems, Issue 4,5	Telekommunikation
RDF 2000	*French National Center for Telecommunication Studies (CNET, jetzt France Telecom R&D)* Union Technique de L'Electricité, Recueil de données des fiabilite	Telekommunikation

Tabelle 3.1.: Übersicht zu herstellerübergreifend verwendbaren Datenhandbüchern zur Kennwertbestimmung elektronischer Komponenten und Bauteile.

Weitere Datenquellen, deren Vergleich und der Vergleich weiterer Vorhersagensmodelle sind in [EPS05], in [IEE10] und [Wil08] zu finden.

Vorteil der herstellerübergreifend anwendbaren Kenndatenhandbücher ist die gute Vergleichbarkeit für unterschiedliche Baugruppen. Damit lässt sich beispielsweise bei zwei elektronischen Schaltungen mit identischer Zielsetzung ein Vergleich der Zuverlässigkeit, unabhängig von den Schaltungs-, Bauteil- und Lieferantenpräferenzen des jeweiligen Herstellers oder Entwicklers durchführen. Nachteil ist die reduzierte Genauigkeit des Gesamtergebnisses, da mit Ersatzdaten gearbeitet wird. Großes Problem ist die Uneinheitlichkeit der Basisdaten und Stressmodelle, worauf nachfolgend näher eingegangen wird.

3.1.2. Gegenüberstellung verschiedener Kennwert-Quellen

Um das Ziel zu erreichen, möglichst ausfallsichere Produkte zu bauen, ist die Auswahl der Kennwert-Quellen irrelevant, da es dabei darum geht, die mittlere ausfallsfreie Zeit zu maximieren. Heißt das Ziel jedoch, möglichst punktgenau eine Garantieaussage zu erreichen oder eine Sicherheitsbaugruppe zu bauen, welche möglichst ausfallsicher aber noch leistbar ist, dann sind die Bauteilkennwerte als Basis absolut essentiell.

Betrachtet man die unterschiedlichen Kennwert-Handbücher, dann stellt man fest, dass diese deutlich voneinander abweichen. Der simple Vergleich zwischen einzelnen Bauteilen, wie in Tabelle 3.2, offenbart Differenzen um Faktor zehn und deutlich mehr. Die Abweichung der Stressmodelle ist ebenso ein deutlicher Faktor. Abbildung 3.1 auf der nächsten Seite zeigt dies anhand des Vergleichs der Temperaturabhängigkeit eines ausgewählten Bauteils, unter Anwendung der verschiedenen Modelle.

	Siemens SN29500 (IEC 61709)	MIL HDBK 217	RAC Handbook	RDF Handbook	Bellcore
Kohlefilmwiderstand	0,3	0,12 .. 6,2	0,7	0,23	1,5
Diode	2	4,9 .. 622	49	7	9
IC 74LS00	1,68	105	11	11,9	15 .. 45
Reflowlötstelle	0,03	0,069	< 0,1	-	-

Tabelle 3.2.: Gegenüberstellung verschiedener Kennwertquellen anhand ausgewählter Bauteile; Anwendung entspricht “Ground Bening”, T=40 °C, permanent load (MIL HDBK 217); alle Werte in [FIT] [Wil06, Tabelle 4.2]

Erweitert man diese Erkenntnisse auf ganze Baugruppen, dann werden die Ergebnisse nicht besser. Laut Pauli [Pau03, Kap. 4.1] wurden nach Untersuchungen der George Washington Universität Kennwertvariationen für gleiche Geräte

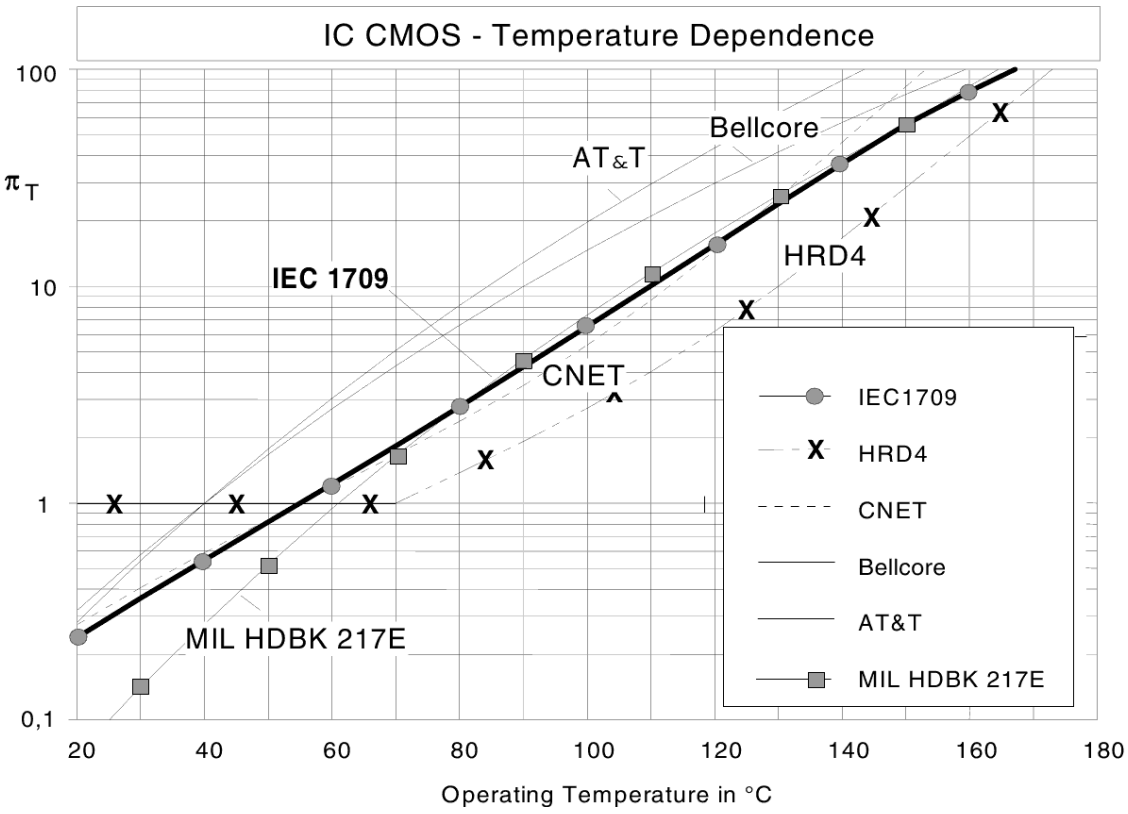


Abbildung 3.1.: Vergleich der Temperaturabhängigkeit verschiedener Kennwertquellen für einen CMOS-IC [EPS05, Bild 7.1]

im Bereich 1 : 2 : 4 (Bell : SAE : MIL) festgestellt, was einer vergleichsweise moderaten Abweichung entspricht. Die Untersuchungen der European Power Supply Manufacturers Association EPSMA [EPS05, Tabelle 7.1] kommen zu differierenden Ergebnissen für MTTF zwischen 281,4 Jahren (HRD5) und 11 895,0 Jahren (Telcordia SR332) bei Anwendung der Parts Stress Methode.

3.1.3. Fazit

Die Arbeit mit Kennwerthandbüchern erfordert im Allgemeinen genaues Wissen über deren Basisdaten und Stressmodelle und die gedachten Einsatzgebiete die bei der Erstellung dieser Daten verfolgt wurden. Werden die Daten nur für vergleichende Berechnungen verwendet und werden sämtliche Berechnungen auf Basis der selben Kennwertbasis durchgeführt, kann dies ignoriert werden.

Für die exakte Bestimmung von Baugruppenkennwerten sollte möglichst auf Datenblätter der Hersteller jedes einzelnen Bauelements zurückgegriffen werden und nur bei Nicht-Verfügbarkeit auf generische Kenndatenhandbücher.

In der vorliegenden Arbeit werden bestehende Daten aus unterschiedlichen Quellen, wie Reparaturrückläuferdaten, sowie mit unterschiedlichen Softwarehilfsmitteln berechnete Werte, mit einem selbst implementierten Verfahren verglichen. Die konkrete Auswahl spezifischer Kenndatenhandbücher und Verfahren ist dabei von untergeordneter Bedeutung, bei Bedarf sind diese austauschbar. Bei kommerziell erhältlichen Berechnungstools sind üblicherweise mehrere gängige Datenquellen hinterlegt und auswählbar.

Für die weitere Betrachtung und die Umsetzung wird eine Festlegung auf die Siemens Norm SN29500 für die Kenndaten und auf die Rechenvorschriften nach IEC 61709 (in SN29500 bereits angewendet) getroffen. Die Bauteilkenndaten der SN29500 sind gerade bei Industrieanwendungen im deutschsprachigen Gebiet verbreitet und vergleichsweise aktuell. Werden Spezialbauteile verwendet, welche nicht oder nur sehr unzulänglich einem Bauteil aus der SN29500 zugeordnet werden können, dann wird auf Herstellerangaben zurück gegriffen.

3.2. Elektronische Hilfsmittel

Dieser Abschnitt versucht, einen kurzen Überblick zu alternativen Software-Lösungen zu geben. Neben der hier propagierten Eigenkreation gibt es eine Reihe von mathematischen Unterstützungstools, kompletten Sicherheits-Suiten und Anwendungs-Hilfen.

Der nachfolgend gemachte Überblick stellt keinen Anspruch auf Vollständigkeit und Korrektheit. Es wird damit lediglich ein Ansatz für weitere Recherchen geboten. Insbesondere die Feststellungen zu Funktionsumfang, Handhabung und Preis wurden durch einfach Internet-Recherche und, sofern vorhanden, Studium der Bedienungshandbücher gemacht. Die Programme wurden nicht evaluiert, wozu auch der Kauf, die Installation und eine Auswertung auf Basis von entsprechenden Kriterien gehören würde.

Die meisten gefundenen Werkzeuge haben gemeinsam, dass sie ursprünglich einen Bedarf aus Safety-Anwendungen abdecken. Damit bieten diese Tools einen breiten und soliden theoretischen Unterbau, verbunden mit hoher Qualität der Berechnungen. Sie stellen mehrere Varianten der Berechnung zur Verfügung (siehe auch 2.3.1 auf Seite 31).

Neben klassischen, generisch einsetzbaren Mathematik-, Statistik- oder Tabellenkalkulationsprogrammen sind die kommerziellen Softwarewerkzeuge auch für die Berechnung von Kennwerten für Non-Safety anwendbar. Die Tools folgen relativ geradlinig vorgegebenen Berechnungsrichtlinien und benötigen, je nach Einsatzgebiet, recht viel Hintergrundwissen zur korrekten Handhabung. Die Lernschwelle ist somit als hoch einzustufen und die Funktionsvielfalt, die

in der Sicherheitsanwendung für die dort notwendigerweise vorhandenen Experten den Vorteil für situationsangepasste Auswertungsmöglichkeiten bietet, ist für die Standardanwendung eher hinderlich.

Die betrachteten und auch gesuchten Hersteller trennen sich mehrheitlich auf in wissenschaftliche Anbieter (Universitätsinstitute, wirtschaftlich orientierte Gesellschaften wie Fraunhofer), Anbieter die aus Eigenbedarf entsprechende Software entwickelten (z. B. Ölindustrie, Eisenbahnhersteller), Dienstleistungsanbietern aus Industrie (SGS, HBM Prenscia) und Prüfgesellschaften (TÜVs, DGUV).

Hersteller / Produktname	**Berechnungsarten [a] Kennwerte [b]**	**Anmerkungen [c] [d]**
BQR *fiXtress, CARE*	FB, FM, MA, ZB nach SN, MIL, SR, ...	Pro Lizenzkosten: €€€;
SGS und TÜV Saar *Exar*	FB, FM, MA, ZB nach IEC, SN, MIL, SR, ...	Pro Lizenzkosten: €€€
item Software *ITEM Toolkit*	FB, FM, MA, ZB nach SN, MIL, SR, ...	Pro Lizenzkosten: €€€
Prenscia (HBM) - Reliasoft *Xfmea, Weibull++, Lambda Predict, ...*	FB, FM, MA, ZB nach IEC, SN, MIL, SR, ...	Pro; Ansatz zur Vereinheitlichung der Bauteilbibliotheken (PartLibraries.org - non-free) Lizenzkosten: €€€
isograph *Reliability Workbench, Fault Tree Analysis*	FB, FM, MA, ZB nach IEC, SN, MIL, SR, ...	Pro Lizenzkosten: €€€
ReliabilityAnalytics - Seymour F. Morris *ReliabilityAnalytics-Toolkit*	Spezifische Berechnungsvorlagen für Verfügbarkeitsberechnung und Ausfallsanalyse von Systemen; keine Kennwertbibliotheken	Zusammenstellung diverser mathematischer Werkzeuge via Applets. Teilweise auch Excel-Templates. Lizenz: frei

a FA ... Fehlerbaumanalyse, FM ... FMEA, MA ... Markov-Analyse, ZB ... Zuverlässigkeits-Blockschaltbilder
b IEC ... IEC 61709, SN ... SN 29500, MIL ... MIL-HDBK-217F, SR ... SR-332
c Pro ... Professionelle Analyse Software mit verbundener Dienstleistung und Schulungen
d €€€ ... Mehrere tausend Euro pro Anwender

Diverse *R, Statistica, Mathematica, Matlab, Excel*	Berechnungsarten abhängig von Libraries und Templates bzw. selbst umzusetzen; keine Kennwertbibliotheken	Mathematische und Tabellenkalkulations-Werkzeuge; teilweise auch entsprechende Auswertungsbibliotheken erhältlich (Matlab, Statistica, R) oder Vorlagen online verfügbar (Excel); spezifische Tool-Kenntnisse notwendig; Lizenzkosten: unterschiedlich;

Tabelle 3.3.: Anbieter von Berechnungswerkzeugen, Funktionsübersicht

ANMERKUNG: Recht bekannte Werkzeuge aus dem deutschsprachigen Raum, wie ESSaRel (Fraunhofer IESE) und RATplus (Siemens) sind in der Onlinesuche als nicht mehr verfügbar aufgeschienen. Es scheint, als ob die Anzahl und Qualität der kommerziellen Produkte in Kombination mit guten mathematischen Werkzeugen wie Matlab und Ähnliche, diese spezialisierten Produkte obsolet gemacht hätten.

Was sind nun die Vorteile der Eigenentwicklung?

Der große Vorteil liegt in der *nahtlosen Integration in den Arbeitsablauf* der Hardware-Entwicklung. Durch einfache Handhabung und schlüssiger, übersichtlich gestalteter Ergebnisdarstellung soll eine intrinsisch motivierte Verbreitung gefördert und einer Sicht als Hindernis und Bremse im Entwicklungsalltag entgegengewirkt werden.

Eine mehrfache, im Extremfall sogar (teil-)manuelle Übertragung von Bauteiltabellen und Eingabe von Umgebungsbedingungen wird auf das absolute Minimum gesenkt, somit eine Fehlerquelle beinahe ausgeschlossen und die Bearbeitungszeit optimiert.

Die Kosten sind begrenzt und konstant, also ausschließlich von der Umsetzung und Pflege abhängig und nicht von der Anzahl der Anwender.

Nachteile

Gegenüber bereits eingeführten Werkzeugen muss die Korrektheit erst nachgewiesen werden. Durch Berechnung von Referenzbauteilen und -baugruppen lässt sich diese Ergebniskorrektheit jedoch relativ leicht nachweisen. Die Offenheit der Sourcecodes und die Anwendung von bekannten Verfahren lässt auch zu, dass eine Qualitätsprüfung durch Codereview mit begrenztem Aufwand möglich ist.

Ein Nachteil, der generell jeder Spezialisierung anhaftet, ist auch hier schlagend: Die Pflege der Lösung muss aktiv betrieben werden. Insbesondere Änderungen, Updates und Fehlerbehebungen, auch wenn diese beispielsweise aufgrund einer Normänderung gemacht werden müssen, sind auf eigene Kosten zu planen, umzusetzen und zu testen.

Die starke Einbindung in das bestehende HW-Entwicklungstool birgt dabei die Hauptgefahrenquelle. Bei Änderungen der verwendeten Programmierschnittstellen durch Dritte würde das ungeplante Änderungen nach sich zu ziehen. Eine Einführung eines neuen Schaltplan-Werkzeugs würde den kompletten Einbindungsteil obsolet machen.

4. Problemstellung

Vorteile und potentielle Fallstricke einer möglichst frühen Bestimmung von Zuverlässigkeitskennwerten innerhalb des Produktlebenszyklus, als Mittel zur qualitätsorientierten Entwicklung, wurden bereits in der theoretischen Aufarbeitung (Kapitel 2.4 auf Seite 39) beleuchtet. Das Fazit dabei war, dass die gezeigten Methoden gewinnbringend sein können, sofern deren Nachteile und Ungenauigkeiten dem Anwender bewusst sind.

Weshalb jedoch *automatisierte* Kennwertgenerierung? Zur Beantwortung dieser Frage dient die Falluntersuchung in Kapitel 4.2 auf Seite 62: Die Entwicklung einer Funktionsbaugruppe über mehrere Revisionen.

In Kapitel 4.3 auf Seite 73 werden Vorgaben und Anforderungen aus der konkreten Einsatzumgebung des untersuchten Wirtschaftsbetriebs aufgelistet.

4.1. Zuordnung zum Vorgehensmodell

Im *Regelkreis der Zuverlässigkeits- und Sicherheitsplanung* nach [Pau03] (Abbildung 4.1 auf der nächsten Seite) wird veranschaulicht, dass unterschiedliche Stellen, sowie eine Vielzahl an Methoden und Prozessen innerhalb eines Entwicklungsbetriebs zusammenarbeiten müssen, um hohe Produktzuverlässigkeit zu erreichen und zu garantieren.

Entsprechend dem, zu Beginn dieser Arbeit definierten Vorgehensmodell (siehe Kapitel 1.2 auf Seite 3), wird nachfolgend die Erhebung von Zuverlässigkeitskenndaten aus unterschiedlichen, praktischen Gesichtspunkten bewertet. Am Beispiel eines konkreten Entwicklungsprozesses, sowie spezifischer Projekte und Produkte wird in den folgenden Kapiteln der bestehende Regelkreis abgebildet und vorhandene Problemstellungen aufgezeigt. Abschließend wird versucht, aus diesen Erkenntnissen eine überarbeitete Version des Prozesses zu definieren.

Die eingenommenen Perspektiven und einige der daraus abzuleitende Fragen sind für die nächsten Unterkapitel nachfolgend kurz zusammengefasst.

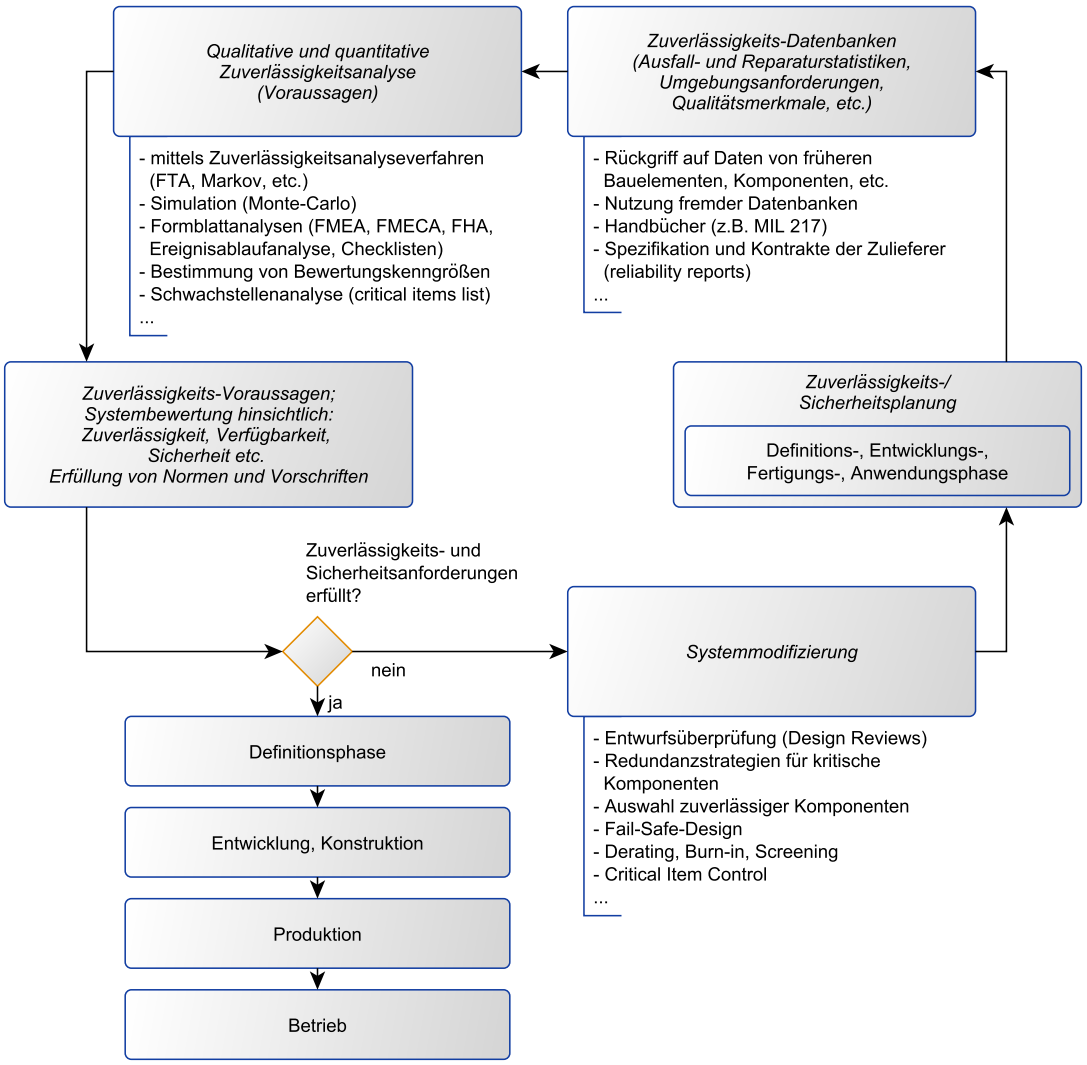


Abbildung 4.1.: Regelkreis der Zuverlässigkeits- und Sicherheitsplanung laut [Pau03]

Bestimmung der Wirtschaftlichkeit

Um entscheiden zu können, ob sich der Einsatz im wirtschaftlichen Umfeld lohnt, stellen sich für einen gewinnorientierten Betrieb folgende grundlegende Fragen:

- *Was sind die Vorteile und Nutzen einer prediktiven Kennwertermittlung in der Entwicklung und Produktion von elektronischen Baugruppen?*
- *Welche Kennwerte sind es wert, ermittelt zu werden? Wie können diese ermittelt werden? Welche Methoden bringen Kosten, Aufwand und Ergebnis in besten Einklang?*

- *Ist eine (teil-)automatische Kennwertermittlung notwendig? Weshalb nicht manuell?*
- *Überwiegen die Vorteile die Kosten und Aufwände? Wie hoch sind diese?*
- *Wurden und werden bereits Kennwerte erhoben? Sind diese als Referenzkennwerte für die Absolutbestimmung geeignet?*
- *Welche weiteren Gründe gibt es für und wider den generellen Einsatz?*

Erhebung und Überprüfung bestehender Methoden

Um die Fragen der Wirtschaftlickkeit beantworten zu können, ist es notwendig, den aktuellen Stand qualitätssichernder Maßnahmen und Prozesse zu erheben:

- *Wie sieht der momentane Qualitäts-Prozess aus?*
- *Wie ist das Zusammenspiel EW - Produktion - Qualitätscontrolling gestaltet?*
- *Wie werden konkrete Bauteil- und Baugruppenkennwerte erhoben?*
- *Gibt es einen definierten und somit einzuhaltenden Prozess, welcher konkrete Qualitätsziele benennt?*
- *Werden Qualitätsvorgaben systematisch überprüft und eingehalten?*

Prozess-Anpassungen

Daraus wiederum können Handlungsempfehlungen abgeleitet werden, unter Berücksichtigung folgender Fragen:

- *Was sind sinnvolle Schritte in Richtung Qualitätsprozessmanagement laut Stand der Technik?*
- *Welche konkreten Vorschläge ergeben sich aus den gewonnenen Erkenntnissen?*
- *Was sind die Vor- und Nachteile der ausgearbeiteten Vorschläge?*

Kapitelzuordnung

Im vorliegenden Kapitel 4, *Problemstellung*, wird die grundsätzliche Notwendigkeit, sowie zu erwartende Vor- und Nachteile bei Einführung eines prediktiven, automatisierten Zuverlässigkeitswerkzeugs diskutiert.

Die unterschiedlichen Methoden zur bisherigen *Erhebung von Verifikationsdaten* werden in Kapitel 5 auf Seite 77 gegenübergestellt. Aus diesen Erfahrungswerten ergeben sich wichtige Anforderungen für das Berechnungswerkzeug, sowie Referenzwerte zur Überprüfung.

Die *Wirtschaftlichkeitsbetrachtung* in Kapitel 6 auf Seite 91 befasst sich mit den oft diametralen Wünschen und Forderungen von Kunden die in einen nachhaltigen wirtschaftlichen Kontext gebracht werden müssen.

Die bestehenden *Prozesse und Methoden* werden in Kapitel 7 auf Seite 101 geprüft und direkt durch ein neues Vorgehensmodell, auf Basis eines in den Entwicklungsprozess integrierten Berechnungswerkzeugs, ersetzt.

Schlussendlich wird in Kapitel 8 auf Seite 137, *Umsetzung eines Werkzeugs zur Zuverlässigkeitsberechnung*, die Anforderungserhebung abgeschlossen, geeignete mathematische Methoden und Hilfswerkzeuge ausgewählt und exemplarische Berechnungen qualitativ mit den bestehenden Referenzen verglichen.

4.2. Untersuchung von Referenzbaugruppen

Für die Untersuchung wurden zwei Standard-Netzteile (genau: DC/DC Wandler) ausgewählt, wobei die zweite Variante als Nachfolger der ersten entwickelt wurde. Die Auswahl erfolgte, da mit diesen Baugruppen eine Einsatzspanne von knapp zehn Jahren abgedeckt wird. Es existieren für den betrachteten Zeitraum von 1998 bis inklusiv 2010 systematisch erfasste Qualitätsdaten. Der Einfachheit halber werden die Baugruppen nachfolgend mit NTv1 und NTv2 bezeichnet.

Die beiden Netzteile werden in späteren Abschnitten auch als Referenzbaugruppen für die Rückläuferbewertung und Prozessbeurteilung verwendet.

In diesem Abschnitt werden die ursprünglichen Anforderungen zur Zuverlässigkeit aus den elektronisch verfügbaren Projektunterlagen dargestellt und auf Erfüllbarkeit überprüft. Die folgenden Unterabschnitte folgen dem Entwicklungszeitstrahl und sind somit nicht strikt nach den beiden Baugruppen aufgeteilt. Diese Vorgehensweise wird gewählt um eine bessere Übersicht zur kontinuierlichen Weiterentwicklung der Anforderungen und Prüfungsanforderungen, hinsichtlich Zuverlässigkeit und Qualität, zu bieten.

Tabelle 4.1 gibt eine grobe Übersicht zu den Eckdaten der Entwicklung. Beide Baugruppen arbeiten ohne Verwendung von Software.

Eigenschaft	NTv1	NTv2
Verkaufsstart	1999, KW 2	2007, KW 34
untersucht bis	2009, KW 17 [a]	2010, KW 14
Anzahl ausgelieferter Baugruppen	27 259	14 446
Anzahl Bauelemente	190	363

a Ende Auslieferung durch Abkündigung nach Übergangsfrist

Elektrische Eigenschaften	
Eingangsspannungsbereich	+24V DC (18 . . . 34V DC)
Ausgangsspannungen	+5V, +15V, -15V

Tabelle 4.1.: Referenzbaugruppen - Übersicht

4.2.1. Spezifikation NTv1

Quelle

Das ursprüngliche Spezifikationsdokument stammt vom 27.1.1998. Darin sind die nachfolgenden Anforderungen hinterlegt.

Betriebstemperatur	0 . . . 60 °C bei 6 A 0 . . . 50 °C bei 8 A Temperaturbereich beim Einschalten: -20 . . . 0 °C
Lagertemperatur	-25 . . . +85 °C
Mechanischer Schock	Keine genauen Angaben, Verweis auf IEC 60068-2-27
Mechanische Vibration	Sinus Keine weiteren Angaben, Verweis auf IEC 60068-2-6
Zuverlässigkeit	MTBF $\geq$ 200 000 h bei typischer Umgebungstemperatur = 35 °C und 70 % Last

Tabelle 4.2.: Auszug zur Spezifikation der Netzteilbaugruppe NTv1

Bewertung und Anmerkungen

Bei den Anforderungen zur Betriebstemperatur fällt auf, dass das untere Limit mit 0 °C von den generell als Standard im Betriebseinsatz vorgegebenen -20 °C abweicht. Daraus möglicherweise resultierende Probleme wie Betauung und daraus folgende direkte Ausfälle durch Kurschluss oder schleichende Ausfälle durch Korrosion, sollten gegebenenfalls durch die Reparaturstatistiken aufgedeckt werden.

Die Angabe der Zuverlässigkeit erfolgt fälschlicherweise als MTBF-Wert (korrekt: MTTF), was bei korrekter Auslegung keinen Einfluss auf die Anforderungen hat.

Der veranschlagte Zuverlässigkeitsgrenzwert ist mit 200 000 h für eine Standardbaugruppe hoch angesetzt, aber erreichbar. Umgerechnet auf eine Jahreseinsatzzeit von 5 000 h ergibt sich eine mittlere erwartete Lebensdauer von 40

Jahren. Oder anders ausgedrückt: nach diesem Zeitraum, unter den geschilderten Betriebsbedingungen sollen noch mehr als 63,2 % der Baugruppen im Einsatz sein.

Aus dem MTTF-Wert berechnet sich λ mit 5 000 FIT. Berücksichtigt man, dass die Baugruppe aus etwa 190 Bauteilen besteht, kommt man auf einen durchschnittlichen Wert von etwas mehr als 26 FIT pro Bauteil (vergleiche Tabelle 4.7 auf Seite 72) und somit ist diese *Ausfallrate jedenfalls erreichbar*.

4.2.2. Lastenheft NTv2

Anforderungen [2] Die Tabelle gibt eine Übersicht zu den Betriebs- und Prüfungsanforderungen an die Baugruppe.

Betriebstemperatur	0 . . . 60 °C (in eingebautem Zustand, lüfterlos, ohne Derating); Prüfung nach IEC 60068-2-14
Lagertemperatur	-25 . . . +85 °C Prüfung: nach IEC 60068-2-2 und IEC 60068-2-1
Mechanischer Schock	Halbsinus 15 g, 11 ms Dauer 2 Schocks pro Achse in alle Richtungen Prüfung: nach IEC 60068-2-27
Mechanische Vibration	Sinus 10Hz . . . 57 Hz, 0,075 mm Auslenkung 58Hz . . . 150 Hz, 1,0 g Beschleunigung Sweep-Rate 1 Oktave/Minute (± 10 %) 10 Sweep-Zyklen pro Achse Prüfung: nach IEC 60068-2-6
Zuverlässigkeit	MTBF > 200 000 h bei mittlerer Umgebungstemperatur 40 °C (ohne künstliche Konvektion) und 80 % Last

Tabelle 4.3.: Auszug zu den Anforderungen aus dem Lastenheft zur Baugruppe NTv2

Bewertung

Die Anmerkungen zu NTv2 sind in großen Teilen identisch zu NTv1. Die Zuverlässigkeitsanforderungen sind in der Nachfolgebaugruppe etwas härter definiert: MTBF von 200 000 h und mehr sind zu erreichen bei Umgebungsbedingungen von 35 °C bei 70 % Last (NTv1) vs. 40 °C bei 80 % Last (NTv2). Für eine erste Bewertung wird dies hier vernachlässigt und somit bleiben die *Anforderungen erfüllbar* auch wenn die höhere Anzahl von Bauelementen (363) die Vorgabe auf etwas unter 14 FIT/Bauteil verringert.

2 *Quelle:* Lastenheft zur Baugruppe NTv2 vom 17.5.2000.

4.2.3. Revisions-Anforderungen NTv1 [3]

Anforderungen

> *Zuverlässigkeit (Wunsch):* Es soll eine Lebensdauer von 5 Jahren bei Dauer-Einsatz (24 h/Tag) mit Voll-Last bei 60 °C Umgebung erreicht werden.
> *Antwort der EW:* Wird bei den Realisierungsvorschlägen soweit als möglich berücksichtigt. Die Forderung wird sich voraussichtlich nur mit einer größeren Umentwicklung zur Wirkungsgradverbesserung erfüllen lassen.

Bewertung

Die einzige Quelle zur Anpassung der Zuverlässigkeit ist ein Gesprächsprotokoll. Es liegen keine genaueren Daten in Form eines Projektdokuments vor.

Unter der schlüssigen Annahme, dass mit *Lebensdauer* nicht die MTTF sondern die *Überlebensdauer* innerhalb der *Garantiezeit* von 5 Jahren gemeint ist, bedeutet die textuelle Anforderung eine drastische Verschärfung der Vorgaben. Selbst bei Annahme einer zulässigen Ausfallrate von 1 %, ergibt sich damit eine MTTF von beinahe 500 Jahren bzw. mehr als 4 Millionen Stunden, also *mehr als zwanzig mal so hoch wie die ursprüngliche Anforderung*. Da sich dadurch die durchschnittlich maximal erlaubte Ausfallsrate pro Bauteil auf ca. 1,3 FIT verringert, ist eine *Umsetzung lediglich unter den gerade getroffenen Annahmen möglich*.

Dass die Anforderung unter 60 °C Umgebungstemperatur definiert wurde, verschlechtert die Umsetzbarkeit nochmals (siehe Abschnitt 4.2.5 auf Seite 67).

4.2.4. Revisions-Anforderung NTv2

Anforderungen - Allgemeine Definition der Zuverlässigkeit - Revision 1

Quelle: Folgende Angaben wurden, auf das Wesentliche reduziert, aus der Baugruppenbeschreibung zur Revision des NTv2, erstellt am 2.4.2007, übernommen:

> Bei einer typischen Eingangsspannung von 24 V, einer typischen Last von 20 W und einer durchschnittlichen Umgebungstemperatur von 40 °C muß die rechnerische Überlebensdauer von 99 % der eingesetzten Netzteile mindestens 12 Jahre sein. Das NTv2 soll also eine MTTF von mindestens 10 500 000 h erreichen.

3 Revisionsanforderung vom 4.3.2002

Wichtiger Punkt bei dieser Betrachtung ist die Lebensdauer/Brauchbarkeitsdauer von Bauteilen mit verschleißbedingten Ausfällen (Elkos). Die zu erwartenden Ausfälle dieser Bauteile sollen die Zuverlässigkeit nicht verringern bzw. die zu erwartende Brauchbarkeitsdauer ebenfalls bei 12 Jahren liegen.

Anforderungen aus Baugruppenbeschreibung - Revision 2

Quelle: In der letztgültigen Baugruppenbeschreibung zur Revision des NTv2 vom 7.9.2007 findet sich die nachfolgende Definition.

Bei einer typischen Eingangsspannung von 24 V und einer typischen Last von 20 W und einer durchschnittlichen Umgebungstemperatur von 40 °C ist nach 12 Jahren die rechnerische Zuverlässigkeit 96 % der eingesetzten NTs (bewertet mit Umrechnungsfaktor gewonnen aus der Rücklieferdaten und dem rechnerischen MTTF des NTv1). Das NTv2 erreicht rechnerisch eine MTTF von mindestens 630 000 h unter den gegebenen Bedingungen, bei Berechnung nach SN29500.

Anforderungen - Umgebungsbedingungen

Die technischen Anforderungen werden bei beiden Revisionsversionen mit nachfolgender Tabelle definiert:

Betriebstemperatur	-20 . . . 60 °C in eingebautem Zustand ohne Betauung und ohne Derating Prüfung nach IEC 60068-2-14
Lagertemperatur	-40 . . . +85 °C Prüfung nach DIN/EN 60068-2-2 und DIN/EN 60068-2-1
Mechanischer Schock	Halbsinus 15 g, 11 ms Dauer 3 Schocks pro Achse in jeder der drei zueinander senkrechten Achsen (insgesamt 18 Schocks) Prüfung: nach IEC 60068-2-27
Mechanische Vibration	Sinusförmige Auslenkung 5 Hz . . . 9 Hz, 3,5 mm Amplitude 9 Hz . . . 500 Hz, 1,0 g Beschleunigung Sweep-Rate 1 Oktave/Minute 10 Sweep-Zyklen pro Achse in jeder der drei zueinander senkrechten Achsen Prüfung: nach IEC 60068-2-6
Zuverlässigkeit	MTBF > 200 000 h bei mittlerer Umgebungstemperatur 40 °C (ohne künstliche Konvektion) und 80 % Last

Tabelle 4.4.: Auszug zu den Anforderungen aus de Revisions-Pflichtenheften zur Baugruppe NTv2

Bewertung

Aus den gefundenen Anforderungen an das Produkt fällt die nicht durchgängige Beschreibung zur Zuverlässigkeit auf. Es werden jeweils deutlich unterschiedliche Werte in der tabellarischen Übersicht und im Text angeben. Positiv ist zu bemerken, dass die Anforderungen zu Mittlerer Ausfallrate und Garantiezeiten gezielter und genauer definiert werden, was auf einen grundsätzlich höheren Kenntnisstand und höheres Augenmerk schließen lässt.

Die schärfste Anforderung an die Ausfallsrate ist in der ersten Revisionsanforderung zu NTv2 (Unterkapitel 4.2.4 auf Seite 65) zu finden: *Mindestens 99% der Geräte sollen nach 12 Jahren noch funktionstüchtig sein.*

Aus Anwendung der Beziehung 2.24 auf Seite 26 [4] ergibt sich

$$\mathrm{MTTF} = \frac{-T_0}{\ln(\frac{N}{N_0})} = \frac{-12\,[\mathrm{a}]}{\ln(0{,}99)} = 1193{,}99\,[\mathrm{a}] = 10\,459\,350\,[\mathrm{h}] \tag{4.1}$$

Anmerkung: Das gewonnene Ergebnis entspricht Betriebsstunden und somit in der Praxis einem Einsatz im Dauerbetrieb, also 24h pro Tag, 365 Tage im Jahr (= 8760h).

Aus der MTTF lässt sich nun λ als Richtwert für die Entwicklung bestimmen:

$$\lambda = \frac{1}{MTTF} = \frac{1}{10\,459\,350\,[\mathrm{h}]} = 95{,}61\,[\mathrm{FIT}] \tag{4.2}$$

Umgelegt auf die durchschnittliche Ausfallrate pro Bauelement der Baugruppe, ergibt sich ein Wert von 0,26 FIT. Führt man sich die Kennwerte (SN29500) bei Umgebungstemperatur von typisch in Netzteilen verbauten Bauelementen, wie Kondensatoren (0,7 ... 10 FIT), Widerständen (0,1 ... 5 FIT) und Halbleiterdioden (1 ... 25 FIT) vor Augen, sieht man sofort, dass selbst unter der Referenztemperatur von 40 °C, *die angestrebten Werte nicht zu erreichen* sind.

4.2.5. Einfluss von Umgebungsfaktoren

In Kapitel 2.2.2 auf Seite 20 wurden bereits unterschiedliche Ausfallarten für Bauteile angeführt. Wie dort gezeigt, sind die Ursachen unterschiedliche Arten von Stress, wie Temperatureinflüsse, elektrische (Über)Belastung aber auch mechanischer Stress. Zur mathematischen Bestimmung dieser Belastungsarten werden sogenannte Stress-Modelle herangezogen. Diese Modelle gibt es in unterschiedlichen Varianten und bilden oft die Grundlage von Bauteilkennwert-Handbüchern. Nachfolgende Ausführungen beziehen sich auf die internationale Norm IEC 61709 [IEC09]. Das nachfolgend eingeführte Stress-Modell und die dazu gehörenden Beschreibungen stammen aus diesem Standard.

4 das dort definierte prozentuelle Ausfallsverhältnis $\frac{\mu(t)}{n}$ entspricht dem Term $1 - \ln(\frac{N}{N_0})$

Stress-Modell

Generisches Stress-Modell nach IEC 61709:

$$\lambda = \lambda_{ref} \cdot \pi_U \cdot \pi_I \cdot \pi_T \cdot \pi_E \cdot \pi_S \cdot \pi_{ES} \tag{4.3}$$

λ_{ref} ... Fehlerrate unter Referenzbedingungen
π_U ... Faktor der Spannungsabhängigkeit
π_I ... Faktor der Stromabhängigkeit
π_T ... Temperaturabhängigkeitsfaktor
π_E ... Umgebungsabhängigkeit
π_S ... Abhängigkeit zur Schaltrate
π_{ES} ... Elektrischer Stressfaktor

Im Standard werden neben der generischen Formel auch spezifische Stress-Modelle für die unterschiedlichen Bauteilkategorien angegeben. Diese Modelle folgen dem Schema, nicht anzuwendende Faktoren wegzulassen. So ist z.B. das angepasste Modell für ICs $\lambda = \lambda_{ref} \cdot \pi_T$, wobei für integrierte CMOS und bipolare Schaltkreise noch zusätzlich der Faktor der Spannungsabhängigkeit zu berücksichtigen ist.

Weiter beschreibt der Standard genau die Berechnung jedes einzelnen Faktors. Zur einfacheren Anwendbarkeit werden vorberechnete Tabellen zur Verfügung gestellt. Für einen der wichtigsten Faktoren, die Temperaturabhängigkeit, wird im nächsten Abschnitt dieser Zusammenhang und dessen Auswirkungen genauer betrachtet.

Temperatur

Ausfallkenndaten in Produktblättern werden sehr oft bei Raumtemperatur angegeben. Für Vergleiche zwischen unterschiedlichen Herstellern oder Revisionen ist dies ausreichend. Die tatsächlich zu erwartenden Einsatzzeiten weichen allerdings in der Regel deutlich von diesen Werten ab. Neben generell höher zu erwartenden Umgebungstemperaturen wie beispielsweise in einem Schaltschrank (40°C und höher), sind die Bauteiltemperaturen unter Belastung nochmals deutlich höher anzunehmen. Zonen um Bauelemente mit hoher Wärmeabgabe (sogenannte Hot-Spots) gilt es bereits in frühen Phasen der HW-Entwicklung ausfindig zu machen und beispielsweise durch Bauteilumverteilung am Print zu entschärfen, um eine möglichst gleichförmige Temperaturverteilung zu bekommen.

Mathematische Basis zur temperaturabhängigen Alterung liefert die *Arrhenius-Gleichung*. Diese beschreibt den Zusammenhang zwischen chemischer Reakti-

onsgeschwindigkeit und Temperatur:

$$k = A \cdot e^{\frac{-E_A}{R \cdot T}} \tag{4.4}$$

$A \ldots$ Frequenzfaktor
$E_A \ldots$ Aktivierungsenergie $J \cdot mol^{-1}$
$R \ldots$ Gaskonstante ($8{,}314\, J \cdot K^{-1} \cdot mol^{-1}$)
$T \ldots$ absolute Temperatur [K]

Durch Umformung erhält man den, im generischen Stress-Modell verwendeten Faktor π_T:

$$\pi_T = e^{\frac{Ea_1}{k_0}\left(\frac{1}{T_{ref}} - \frac{1}{T_{op}}\right)} \tag{4.5}$$

$k_0 \ldots 8{,}616 \cdot 10^{-5} eV/K$
$T_{ref}, T_{op} \ldots$ Referenz- bzw. Arbeitstemperatur

Diese mathematische Beziehung, bzw. eine in der Norm noch zusätzlich angeführte, erweiterte Form davon, bildet die Grundlage für die Berechnung der konkreten temperaturabhängigen Stressfaktoren. Diese müssen für jedes Bauteil und auch für unterschiedliche Ausführungen, aufgrund unterschiedlicher Materialzusammensetzung und Aufbau, bestimmt werden.

Als Faustformel gilt die sogenannte *RGT-Regel*, wonach eine chemische Reaktion bei um 10 K erhöhter Temperatur zwischen zwei- bis dreimal so schnell abläuft. Dies zeigt einerseits die hohe Temperaturabhängigkeit von Alterungsdegradierungen, kann aber auch in *beschleunigten Alterungstests* genutzt werden, um diese zu emulieren.

In unten stehender Tabelle 4.5 sind unterschiedliche Bauteile zur Untermauerung der Wichtigkeit von geplantem Temperaturmanagement für elektronische Baugruppen aufgeführt. Die Tabelle berücksichtigt nicht, dass die Referenztemperaturen für unterschiedliche Bauteile im Anwendungsfall deutlich voneinander abweichen.

Bauteil	40 °C	60 °C	85 °C	100 °C
IC [a]	0,55	1,2	3,4	6,5
Tranistor	0,55	1,2	2,8	6,5
Diode	0,51	1,2	2,7	5,5
LED (GaAs)	0,33	1,4	5,1	16
Widerstand (Metallfilm)	0,71	1,1	1,8	2,8

a gilt nicht für EPROM, FLASH-EPROM o.ä.; nicht für CMOS/bipolar

Elkolektrolyt-kondensator (Al, Festelektrolyt) [b]	1,0	1,2	1,4	1,5
Elko (Al, Flüssigelektrolyt) [b]	1,0	3,7	20	55

Tabelle 4.5.: Beispiele für den Temperatur-Korrekturfaktor π_T für elektronische Bauteile, bei unterschiedlichen Temperaturen laut [IEC09] [c]

Um eine entsprechend dem Standard korrekte Berechnung zu garantieren, müssen zuerst die Referenzbedingungen, die konkreten Umgebungs- und Arbeitsbedingungen pro Bauteil bestimmt werden. Diese Werte müssen anschließend zur Basis-Aufallsrate multipliziert werden.

Natürlich gilt dies nicht nur für den Korrekturfaktor der Temperatur, sondern auch für sämtliche anderen Korrekturfaktoren, welche in der Tabelle noch nicht berücksichtigt wurden. Konkret heißt das beispielsweise für einen Elektrolytkondensator, dass noch zusätzlich der Faktor π_U für die Spannungsabhängigkeit hinzumultipliziert werden muss.

Manuell ist dieses Verfahren offensichtlich sehr aufwändig und auch fehlerträchtig (Ablesefehler aus Tabellen, Fehler bei Annahme von Referenz- und Umgebungsbedingungen, ...). Im Gegensatz dazu kann dieses Verfahren, idealerweise unter Verwendung der exakten Formeln, mit vertretbarem Aufwand automatisiert werden. Danach stehen die Kennwerte für Teilberechnungen, Optimierungsaufgaben und Szenarienbetrachtungen, ohne weiteren Zusatzaufwand zur Verfügung.

Tatsächlich bieten auch einige der in Kapitel 3.2 auf Seite 55 vorgestellten Werkzeuge Berechnungsmethoden unter Anwendung von anpassbaren Umgebungs- und Stressvorgaben. Ein individuelles Werkzeug hat gegenüber diesen Werkzeugen den Vorteil, dass die Berechnungen noch genauer an die spezifischen Gegebenheiten angepasst werden können. Bei entsprechender Umsetzung können dabei kritische Baugruppenzonen (Hot-Spots) deutlich besser und einfacher berücksichtigt werden.

TR 2 Teilberechnungen unter alternativer Temperaturvorgabe
Das Berechnungswerkzeug soll die Möglichkeit bieten, neben Gesamtberechnungen auch Teilberechnungen von Baugruppen, mit abweichenden Basistemperaturen, durchführen zu können.

TR 3 Hot-Spot Berechnung
Das Berechnungswerkzeug soll die Beaufschlagung von Schaltplanmodulen, Bauelementgruppen und einzelnen Bauelementen mit erhöhten Basistemperaturen ermöglichen.

b Referenztemperatur angenommen: 40 °C
c sofern nicht anders angegeben, Umgebungstemperatur: 40 °C; Referenztemperatur: 55 °C

Einfluss auf konkrete Kennwerte

Die neuen Informationen werden nun auf das konkrete Baugruppenbeispiel angewendet. Dazu wird von einer der erfüllbaren Anforderungsversionen für NTv2 ausgegangen (siehe Unterkapitel 4.2.4 auf Seite 66):

Betriebstemperatur	-20 . . . 60 °C in eingebautem Zustand
Eingangsspannungsbereich	+24V DC (18 . . . 34V DC)
Zuverlässigkeit	MTBF > 200 000 h (≙ < 5 000 FIT) bei mittlerer Umgebungstemperatur 40 °C (ohne künstliche Konvektion) und 80 % Last

Die untere Temperaturschwelle wird für die Berechnung wiederum ignoriert. Die nachfolgende Tabelle gibt die Werte für 60 °C, 85 °C und 100 °C an. Dabei ist der niedrigste Wert wahrscheinlich nur bei einer aktiv gekühlten Umgebung realistisch. Messungen haben gezeigt, dass die Differenz zwischen Umgebungstemperatur bei Nennlast (= 24V Eingangsspannung) und Bauteiltemperatur am Stecker 20 °C beträgt. Bei Volllast (= 36V) beträgt die Differenz bereits 25 °C. Das bedeutet bei 60 °C Umgebungstemperatur bereits 85 °C Bauteiltemperatur. Bauteiltemperaturen von aktiven Elementen, wie beispielsweise dem Spannungswandler oder den Transistoren, sind nochmals entsprechend höher.

Bauteil	**Anz**	λ_{ref} [a]	$\Sigma\lambda\pi_{T40}$	$\Sigma\lambda\pi_{T60}$	$\Sigma\lambda\pi_{T85}$	$\Sigma\lambda\pi_{T100}$
Tantalkondensatoren	9	1,0	9,0	19,8	90,0	288,0
Keramikkond.	67	2,0	134,0	294,8	683,4	1 085,4
Al-Elkos	6	3,0	18,0	20,7	24,7	27,4
Widerstände (SMD)	177	0,1	17,7	19,5	35,4	49,6
SI-Dioden	41	1,0	41,0	49,2	135,3	225,5
Suppressordioden	4	7,0	28,0	67,2	182,0	308,0
LED	2	2,0	4,0	11,6	56,0	132,0
Transistoren (bipolar)	13	3,0	39,0	46,8	132,6	253,5
(MOS)FET	8	5,0	40,0	48,0	136,0	260,0
Transistoren (FET Kleinleistung)	3	20,0	60,0	21,6	60,0	114,0
Logic-IC	19	3,0	57,0	68,4	193,8	370,5
EEPROM	1	30,0	30,0	39,0	156,0	330,0

a Referenzausfallwert in FIT für ein Bauteil, unbelastet, bei Referenztemperatur (unterschiedlich je nach Bauteilart), Quelle: SN 29500

Induktivitäten	8	3,0	24,0	26,4	45,6	103,2
Übertrager	1	10,0	10,0	11,0	19,0	43,0
Stecker/Buchse [b]	2 (2 · 30)	0.15	9,0	9,0	9,0	9,0
Lötstellen	> 1 000	0,03	30,0	30,0	30,0	30,0
Platinen	2	120,0	240,0	240,0	240,0	240,0
Summe [c]	*363*	-	*790,7*	*1 023,0*	*2 228,8*	*3 869,0*

Tabelle 4.7.: Ausfallrate λ für NTv2 bei unterschiedlichen Temperaturen laut IEC 61709 [IEC09]

Die Ergebnisse zeigen, dass für alle Temperaturbereiche die Anforderung von 5 000 FIT eingehalten wird. Forderungen nach 4 Mio. oder sogar 10 Mio. Stunden MTTF (entspricht 250 bzw. 100 FIT), wie in späteren Revisionen aufgestellt, sind *schon bei 40 °C nicht mehr erfüllbar*.

In der Tabelle wird die einfachste Form der Berechnung durchgeführt, indem für alle Bauteile die selbe Umgebungstemperatur angenommen wird. Tatsächlich müsste man hier nochmals differenzieren, um auf exakte Werte zu kommen. Für den Nachweis der Anforderungseinhaltung reicht in diesem Fall die gewählte Vorgehensweise. Falls die Ergebnisse nicht den Erwartungen entsprechen, kann man Verbesserungen durch Erhöhung der Genauigkeit (z.B. Temperatur pro Bauteil bestimmen) bzw. zulässige Einschränkungen (Festlegung der Umgebungstemperatur) erzielen. Für die wirtschaftlich motivierte Garantieberechnung bzw. daraus abgeleitet auch Preisbestimmung ist eine möglichst genaue Berechnung immer vorteilhaft.

Die Berechnung ist mit der Berücksichtigung der Temperaturabhängigkeit noch nicht beendet. Als nächster Schritt müsste die Lastabhängigkeit in gleicher Form einfließen. Für Kondensatoren und Halbleiterbauelemente (Transistoren, Spannungswandler, Dioden) wäre im vorliegenden Fall der Spannungsfaktor π_U und für Stecker/Buchse der Stromfaktor π_I zu multiplizieren.

4.2.6. Fazit Umgebungsbedingungen

Das Beispiel einer einfachen elektronischen Baugruppe zeigt bereits an den Anforderungen, dass fundiertes Know-How für die korrekte Formulierung und spätere Umsetzung von Zuverlässigkeitsvorgaben notwendig ist.

In der Realisierung tendieren Entwickler dazu, Schönwetter-Werte als Basis einer Verfügbarkeitsbetrachtung zu verwenden. Dies hat mehrere Gründe. Zum

b der Referenzwert gilt pro beschalteten Kontakt; 48 Pin Stecker+Buchse, davon 30 beschaltet
c berechnet aus Anzahl multipliziert mit Lambdawert, über die Spalte aufsummiert

einen findet man in Datenblättern von Bauteilen meist nur die Referenzausfallwerte. Weiter ist die notwendige Theorie nicht oder zu wenig bekannt und oft ist unklar, welchen Nutzen diese Berechnungen haben. Wie in Kapitel 5.1 auf Seite 78 gezeigt, werden diese Fehlannahmen bzw. der unsorgfältige Umgang mit den Berechnungen oft durch missinterpretierbare Felddaten gestützt.

Dieser Abschnitt zeigt auf, dass die Berechnung von mathematisch korrekten Verfügbarkeitsdaten ein solides Wissen notwendig macht. Die Methode zur Berechnung ist aufwändig durch die Bestimmung der Referenzkennwerte, der Umgebungsfaktoren und die wiederholte Aufsummierung aller Bauteilkennwerte in den unterschiedlichen Arbeitsumgebungen. Das Schema ist immer das selbe und somit geschaffen für eine computergestützte Umsetzung.

4.3. Anforderungen der Einsatzumgebung

Nachfolgend werden Vorgaben, welche durch die konkrete Einsatzumgebung des auftraggebenden Wirtschaftsbetriebs bestehen, angeführt. Weiter werden Anforderungen formuliert, welche durch Beobachtung, Analyse der bestehenden Vorgehensweise und Interviews mit Entwicklern gesammelt wurden.

Vorgaben

Ausgangspunkt für eine Auswahl geeigneter Hilfsmittel ist das Anforderungsprofil des untersuchten Unternehmens:

- Integration in Mentor Graphics DxDesigner (Schaltplaneditor)
- möglichst geringer Zusatzaufwand für Entwickler
- möglichst niedrige Lernschwelle

Wie bereits am Ende von Kapitel 3.2 auf Seite 55 festgestellt, erfüllen verfügbare Softwarepakete von Drittherstellern aufgrund deren generischer Ausrichtung, diese Punkte nicht oder nicht ausreichend.

Welche Kennwerte sind zu Baugruppen anzugeben bzw. möchte der Hersteller angeben?

- MTTF(/MTBF) für Safety und Non-Safety Baugruppen
- Safety-Kennwerte: CCF, SFF (*Safe Failure Fraction*), λ, PFH/PFD

Eine Eigenimplementierung muss folgende Vorteile bieten:

- Möglichst exakte Kennwertbestimmung von Bauteilen, Baugruppen und Teilmodulen von Baugruppen unter Anwendung unterschiedlicher Kennwertbestimmungsmethoden, Kennwerttabellen und Umgebungsbedingungen.

- Angepasste Schnittstellen an die tatsächliche Arbeitsweise und den vorgegebenen Prozess.
- Zentrale Erfassung, Umsetzung und Nutzung von Know-How.
- Dokumentation für Anwender und Entwickler.
- Niedrige Lernschwelle und möglichst niedriger Zusatzaufwand für hohe Akzeptanz im Alltag.
- Offenheit für weitere Verbesserungen und Erweiterungen.

4.4. Zusammenfassung

Die Einführung eines automatisierten Werkzeugs zur Zuverlässigkeitsberechnung wird aufgrund der beobachteten Unsicherheiten in der Bestimmung von Zuverlässigkeitsdaten und der strategischen Ausrichtung (Sicherheitstechnik) im untersuchten Betrieb empfohlen.

Die Firma Mentor Graphics bietet keine Unterstützung hinsichtlich der geforderten Funktionalität. Ein Umstieg auf ein anderes Produkt ist aufgrund der tiefen Verankerung in Entwicklung und Produktion nicht möglich, weshalb die Fähigkeiten von Mitbewerbsprodukten nicht evaluiert wurden.

Nicht eingebettete Werkzeuge, die z.B. in der Raumfahrttechnik oder im Eisenbahnbau angewendet werden, wurden ausgeschieden. Spezialisierung, Komplexität und auch Preis dieser Produkte sind zu hoch für den betrachteten, begrenzten Anwendungsfall im untersuchten Betrieb. Dabei ist zu anzumerken, dass die Fähigkeiten dieser Produkte oft weit über die hier gestellten Ansprüche hinaus gehen.

Es gibt eine Reihe von eigenständigen Werkzeugen, welche auf die Berechnung von Zuverlässigkeitskennwerten spezialisiert sind. Diesen ist gemeinsam, dass auf Basis einer manuell zu erstellenden Stückliste, in Kombination mit integrierten Datenbanken zu den Bauteilen, entsprechende Kennwerte oder teilweise auch Kennwertserien berechnet werden. Die Eingabe von eigenen Bauteilen ist unterschiedlich komfortabel gestaltet und die Ausgabeformate sind ebenfalls dementsprechend. Die Produkte sind auch geeignet für den Einsatz in der Sicherheitstechnik. Sämtliche Berechnungsvarianten und Kennwerttabellen werden zur Verfügung gestellt. Negativ ist der oft sehr technisch/mathematisch gestaltete Zugang, die notwendige Mehrfacheingabe der Baugruppen-Bauelemente und die nicht vorhandene Einbettung in bestehende Werkzeuge und Prozesse.

Um den Prozess des kontinuierlichen Zuverlässigkeits-Managements zu etablieren und in das bestehende Qualitäts-Controlling einzubetten, ist es nicht ausreichend, eine punktuelle Maßnahme in Form der Programmierung eines

Hilfswerkzeugs umzusetzen. Die Einbettung in den bestehenden Entwicklungsprozess und die Kontrolle und Weiterverwendung der Erkenntnisse aus dem Prediktions-Tool sind mindestens genau so wichtig wie die Entwicklung desselben.

Auf Basis dieser Erkenntnis wird die **Aufgabenstellung erweitert**. So werden noch vor Umsetzung des Tools die Rahmenbedingungen für den nutzbringenden Einsatz geschaffen. Dazu werden die momentan etablierten Entwicklungs-, Produktions- und Qualitätsprozesse erhoben und mit dem Stand der Technik verglichen (siehe Kapitel 7 auf Seite 101). Auftretende Differenzen werden danach herausgearbeitet und als Vorschläge zur Prozess-Anpassung formuliert. Erst dann wird das eigentliche Tool, entsprechend den Vorgaben und der definierten Arbeits- und Prozessumgebung, umgesetzt.

5. Erhebung von Verifikationsdaten konkreter Baugruppen

Das vorliegende Kapitel befasst sich mit der Darstellung und Überprüfung von Kennwertbestimmungen, welche während der Verkaufsphase der beiden Baugruppen NTv1 und NTv2 vorgenommen wurden. Eignung und Einsatz der dabei verwendeten, manuellen und computergestützten Berechnungsmethoden und Werkzeuge wird bewertet und die Kennwertgenerierung so genau als möglich nachvollzogen.

Die Überprüfung dient folgenden Zielen:

1. Verifizierung bestehender Kennwerte und Auswahl bzw. Berechnung von Referenzkennwerten. Diese dienen später zur Prüfung der Korrektheit der Berechnungen im Prediktionswerkzeug.
2. Beurteilung ob Werte als Referenzen (absolut/relativ) dienen können.
3. Beurteilung der gesammelten Methoden und Kennwerte.

Dieses Kapitel ist entsprechend Kruchtens Vorgehensmodell 1.2 auf Seite 3 der *physikalischen Sicht* auf die Problemstellung zuzuordnen.

Unterkapitel 5.1 auf der nächsten Seite behandelt sämtliche gefundenen, systematischen Kennwerterhebungen und Überprüfungen der Methoden im Zeitraum von Anfang 1999 bis Juni 2012 für die genannten Baugruppen. Dies umfasst:

- *Rückläuferstatistiken* (→ 5.1.2 auf Seite 82)
- Zwei Prüfungen und Berechnungen des MTTFs 2007 und 2013 in den Abschnitten 5.1.3 auf Seite 83 und 5.1.4 auf Seite 85.

Die Untersuchungen basieren auf einer Referenzberechnung, welche im Zuge dieser Arbeit auf Basis der verfügbaren Kennwerte umgesetzt wird. Dabei ist die Vorgehensweise und konkrete Ermittlung der Kennwerte auf Rückläuferbasis genau dokumentiert.

Eine Gegenüberstellung der Ergebnisse und Empfehlungen für Verbesserungen schließen den Referenzdaten basierten Teil der Untersuchung ab (Abschnitt 5.2 auf Seite 87).

In Abschnitt 5.3 auf Seite 89 wird eine Sicherheitsbaugruppe (SBv1) den Referenzen hinzugefügt. Die unabhängige Prüfung der vorliegenden Kennwerte durch eine offizielle, zertifizierende TÜV-Stelle, qualifiziert diese direkt als Referenz.

5.1. Evaluierung bisheriger Untersuchungen

Sofern nicht anders angegeben, werden in den nachfolgenden Untersuchungen jeweils nur die Kennwerte der Baugruppen NTv1 bzw. NTv2 betrachtet. Genauere Angaben zu diesen Baugruppen finden sich in Kapitel 4.2 auf Seite 62.

Basis

Die Erhebung von Zuverlässigkeitskennwerten erfolgte bisher über zwei Methoden:

Automatische Ermittlung von MTTF-Werten auf Basis eines Datenbank-Systems mit selbst hinterlegten Berechnungsformeln. Berechnungsgrundlage sind dabei die Verkaufs- und Rückläufer- bzw. Reparaturstatistiken.
Anmerkung: Dieses System wurde Anfang 2010 durch eine moderne ERP-Umgebung abgelöst, welche eine *automatische Auswertung nicht unterstützt*.

Manuelle Berechnung einzelner Baugruppen. Als Grundlage dient jeweils der Schaltplan bzw. die Stückliste. Berechnungen erfolgten manuell, unter Einsatz von mathematischen Hilfsmitteln und einer Tabellenkalkulation, oder mittels des Berechnungstools *CARE Manager*.

5.1.1. Referenzberechnung auf Rückläuferbasis

Wichtigste Grundlage ist eine möglichst exakte und umfassende Erhebung der Daten. Damit ist die Voraussetzung gegeben, auch später noch auf alternative Berechnungsmodelle umzusteigen oder gefundene Fehler zu beheben.

Eigenschaft	**Wert / Erklärung**	
	NTv1	NTv2
Datenquelle	interne Rückläuferdatenbank	
Berechnungsgrundlage	nach Maximum-Likelihood-Methode	
Betrachteter Zeitraum	Q4/1998 . . . Q2/2010	Q3/2007 . . . Q2/2010
Auswertungsintervall	Quartal	Quartal
Produzierte Module	27 259	14 441

Rückgelieferte Module	476	71
davon verwendbar [a]	415	66
Nach Prüfung fehlerhaft [b]	242	30

Tabelle 5.1.: Annahmen zur Referenzberechnung auf Basis der Rückläuferdaten

Bei der Auswertung der Datenbank wurden Auffälligkeiten festgestellt, welche nachfolgend in *Grobe Mängel* und in *Verfälschende Faktoren* aufgeteilt werden.

Grobe Mängel:

Nicht zuordenbare und fehlerhafte Daten
: Datensätze mit negativen Einsatzzeiten oder wo das Produktionsjahr nicht zuordenbar ist. Betrifft ca. ein Achtel der Einträge aller Rücklieferungen bei NTv1.

Definitionen nicht verfügbar
: Erfassungsgrundlagen sind nicht nachvollziehbar. Damit sind auch Ergebnisse von berechneten Verfügbarkeitsdaten nicht überprüfbar. Die Rückläufer wurden intern geprüft und kategorisiert. Die Zuordnung dieser Kategorien ist nicht transparent mit den Verfügbarkeitsberechnungen verknüpft. Was wird nun als “Ausfall” im Sinne der Berechnung gewertet?

Kommentare nicht verfügbar
: Zumindest bei auffälligen Datensätzen sind Kommentare notwendig, damit eine (spätere) Prüfung möglich wird.

Keine lückenlose Weiterführung der Datenbank
: Lückenlose Erhebung inklusive Übernahme der alten Daten ist als Kontrollbasis notwendig. Neue Datenbank so rasch als möglich umsetzen.

Verfälschende Faktoren mit Einfluss auf die Berechnung:

Anzahl Rückläufer nicht vollständig
: Dies ist ein systematisches Problem bei Rückläufern. Die exakte Anzahl im Feld ausgefallener Baugruppen ist unbekannt. Nur tatsächlich zurückgesandte Baugruppen werden erfasst. Diese Anzahl ist zum Beispiel abhängig vom Preis. Rücksendungen werden auch lediglich innerhalb der Garantiezeit durchgeführt. Bei Baugruppen der

a Aufgrund von fehlerhaften bzw. nicht zuordenbaren Datenbankeinträgen reduzierte Anzahl.
b Alle rückgelieferten Module, welche nach interer Prüfung als defekt kategorisiert wurden. Also vor allem elektrische aber auch nicht bestimmbare und nicht reproduzierbare Ausfälle.

Preisklasse von NTv1 und NTv2 ist eine Erfassungsquote von $\leq 30\,\%$ realistisch.

Verfälschende Erfassung von Zeiten
Vermischung von Verkaufs- und Produktionsdatum sowie unklare Zeiträume zwischen tatsächlichem Ausfall und erfasstem Rückläufereingang.

Keine und mehrfache Seriennummern
Dadurch keine exakte Zuordnung der Ausfälle möglich. Serienausfälle bzw. Häufungen bleiben bei unsauberer Erfassung unentdeckt.

Berechnungsgrundlage
Wie wurden die Kennwerte ausgewertet? Pro Quartal, pro Monat, pro Jahr, pro Charge?

ANMERKUNG: Die Vorgehensweise, die Garantiezeit mit dem Produktionsdatum starten zu lassen, ist aus wirtschaftlichen Gesichtspunkten legitim. Für zielgerichtete Kennwertbestimmung, auf deren Basis kostensparende Maßnahmen durch Einsatz günstigerer Bauteile umgesetzt werden könnten, werden zusätzliche Daten benötigt, zumindest die tatsächliche Einsatzzeit.

Berechnungsmethoden nach Maximum-Likelihood Methode

Nachfolgend wird ein neues Berechnungsverfahren zur Anwendung auf Rückläuferdaten und Testreihen eingeführt (siehe [Pau03, S. 159]). Dem Modell liegt die Exponentialverteilung zugrunde. Ausgefallene Module werden nicht ersetzt, sondern als neue Auslieferungen behandelt.

Für die Rückläuferbewertung wird die Variante der *Schätzmethode bei gestutzter Stichprobe* angewendet. Das heißt, dass der Test mit n Baugruppen durchgeführt und nach Testzeitraum t_T abgebrochen wird.

$$T_f = \sum_{i=1}^{f} t_i + (n-f) * t_T \qquad \text{summierte Lebensdauer} \tag{5.1}$$

$$\lambda = \frac{f}{T_f} \qquad \text{Ausfallrate in } [\mathrm{h}^{-1}] \tag{5.2}$$

$$MTTF = \frac{1}{\lambda} \qquad \text{MTTF in [h]} \tag{5.3}$$

$\sum_{i=1}^{f} t_i$	summierte Zeiten bis zum Ausfall
t_T	betrachteter Zeitraum
n	Anzahl Baugruppen
f	Anzahl fehlerhafter Baugruppen

Nimmt man nun die Werte aus den Rückläuferaufzeichnungen und setzt diese entsprechend ein, kommt man zu folgender Auswertung:

	NTv1	NTv2
n	27 259	14 441
f	242	30
t_T *[h]*	91 992	26 280
$\sum_{i=1}^{f} t_i$ *[h]*	1 149 515 472	144 202 416
λ *[FIT]*	97,15	79,17
MTTF [h]	10 293 829,49	12 631 797,60
MTTF [a]	1 175,09	1 441,99

Tabelle 5.2.: Basisdaten und Berechnungsergebnisse nach Meyna/Pauli [Pau03, S. 159]

Bei diesen Ergebnissen ist zu berücksichtigen, dass das Berechnungsmodell davon ausgeht, dass sämtliche Module über den gesamten Zeitraum im Einsatz sind und nicht sukzessive produziert werden. Eine Methode für eine exakte Auswertung wäre, ein Auswerteintervall zu wählen (z.B. für jede Produktionswoche, Produktionscharge, Lieferzeitpunkt, . . .) und für jedes einzelne dieser Intervalle die Berechnung durchzuführen. Eine andere Variante ist die Reduktion der Einsatzzeit. Nachdem die Verkaufszahlen über die Zeit bekannt sind, kann man die maximal erreichbare Einsatzzeit entsprechend korrigieren.

Berücksichtigung beeinflussender Faktoren

Die unten stehenden Berechnungen werden lediglich für NTv2 durchgeführt. Einmal wird gegenüber der Referenzberechnung die *Einsatzzeit auf 25 % reduziert*. Dies basiert darauf, dass bei angenommen linearer Zunahme der Anzahl von Baugruppen im Feld, der maximal betrachtete Zeitraum halbiert werden darf. Weiter zeigen Rückmeldungen von Kunden, dass aufgrund tatsächlicher Arbeitszeit pro Tag, geplanter Stillstände, Wochenenden usw. nicht mehr als 50 % produktiver Einsatz erreicht wird. Danach wird die *Anzahl fehlerhafter Baugruppen verdreifacht*, was bereits zu Beginn des Abschnitts begründet wurde. Abschließend wird noch der *kombinierte Wert* berechnet.

	Referenz	25 % Einsatz	300 % Defekte	Kombination
λ *[FIT]*	79,17	316,08	238,19	947,52
MTTF [a]	1 441,99	361,16	479,25	120,48

Tabelle 5.3.: Rückläuferberechnung: Einfluss von Einsatzzeit und Anzahl unbekannter Ausfälle (NTv2)

Der Einfluss der veränderten Eingangsgrößen ist signifikant. Da die vorgenommenen Änderungen nicht artifizieller Art sind, sondern als Annäherung an die Realität betrachtet werden müssen, *verschlechtern* sich auch die *tatsächlich zu erwartenden Zuverlässigkeitsdaten*.

Als *interne Qualitätsannahme* und Basis für Verbesserungen ist aufgrund dieser Resultate ein *MTTF von 120 Jahren* bzw. eine *Ausfallrate von 950 FIT* anzunehmen.

Die *Garantiebewertung* darf hingegen ohne Gefahr besser angenommen werden. Bei bekannter Einsatzzeit und bekannten Umgebungseinflüssen sollte diese exakt berechnet werden. Falls nicht bekannt, ist die Annahme von *50 % Einsatzzeit* bei *dreifacher Rückläuferrate* immer noch auf der sicheren Seite, womit sich der *MTTF auf 240 Jahre* verdoppelt.

5.1.2. Auszüge aus Qualitätsberichten und Rückläuferstatistik

Bis ins Frühjahr 2010 wurden Qualitätsstatistiken automatisch generiert. Die Zusammenhänge, Annahmen und Berechnungsformeln die diesen Daten zugrunde lagen, konnte nicht mehr exakt eruiert werden. Die Ergebnisse werden trotz dieses Mangels betrachtet, insbesondere da diese bisher als Grundlage zu internen Qualitätsbetrachtungen herangezogen wurden.

Eigenschaft	NTv1	NTv2
Datenquelle	interne Rückläuferdatenbank	
Berechnungsgrundlage	unbekannt	
Betrachteter Zeitraum	wie bei Referenzberechnung	
Auswertungsintervall	unbekannt	
Produzierte Module *Rückgelieferte Module* *davon verwendbar* *Nach Prüfung fehlerhaft*	wie bei Referenzberechnung	

Einschränkungen und Mängel der Rückläuferdatenbank gelten im gleichen Maße, wie bereits in Abschnitt 5.1.1 auf Seite 78 aufgelistet.

PR 1 Wiederaufnahme der Kennwertermittlung
Für eine zuverlässigkeitsorientierte Entwicklung ist eine Bewertung der Rückläufer- und Reparaturstatistiken unerlässlich. Deshalb sollte die Kennwertermittlung auf Basis der neuen ERP-Umgebung mit hoher Priorität verfolgt werden. Die bestehende Datenbasis aus der alten Datenbank sollte übernommen und die fehlenden Daten seit 2010 entsprechend nachgepflegt werden.

In sogenannten “Reparaturanalysen” wurden regelmäßig statistische Auswertungen von Verkäufen und Rücklieferungen gemacht. Neben einer grundlegenden Klassifizierung von Fehlerkategorien liegt das Gewicht in diesen Dokumenten auf Reparaturberichten. Dabei werden in technischen Detailuntersuchungen, Fehlerursachen bzw. verursachende Bauteile betrachtet. Verfügbarkeitskennwerte werden dabei nicht berechnet.

5.1.3. Untersuchung mit CARE Manager

Im August 2007 wurde eine Untersuchung der Baugruppen NTv1/NTv2 zur Bestimmung der Zuverlässigkeitskenndaten durchgeführt. Die Untersuchung erfolgte mit dem Tool *CARE Manager V8.7* der israelischen Firma *BQR*. Die Ergebnisse wurden in einem Untersuchungsbericht zusammengefasst.

Eigenschaft	NTv1	NTv2
Datenquelle	Stücklisten, SN29500	
Berechnungsgrundlage	Exakte mathematische Methoden unbekannt, wahrscheinlich Parts-Count Verfahren; Berechnungen wurden unbelastet (25 °C) und unter Stress (nur Temperatur, bis 65 °C) berechnet.	

Die Berechnungsergebnisse des angewendeten computergestützten Werkzeugs:

Bauteiltemperatur 25 °C	NTv1	NTv2
λ *[FIT]*	1 262,99	1 688,90
MTTF [h]	791 766,00	592 101,00
MTTF [a]	90,38	67,59
Bauteiltemperatur 65 °C		
λ *[FIT]*	2 616,33	1 597,45 (!)
MTTF [h]	382 214,00	625 998,00 (!)
MTTF [a]	43,63	71,46 (!)

Tabelle 5.6.: Ergebnisse nach Anwendung des CARE-Managers auf NTv1/NTv2 (Basis SN29500)

Die Berechnungsergebnisse bei Referenztemperatur sind in erster Betrachtung nicht unrealistisch. Die Ergebnisse für NTv2 sind höher, was aufgrund der höheren Komplexität (mehr Bauteile) zu erwarten war. Bei den Werten für NTv1 unter Stress fällt auf, dass diese sich nur um den Faktor zwei ändern. Bei korrekter Erhöhung der Umgebungstemperatur um 45 °C durch das Werkzeug,

wäre aufgrund früherer Betrachtungen (siehe Tabelle 4.5 auf Seite 70) eine deutlichere Verschlechterung zu erwarten gewesen.

Die Berechnung von NTv2 weist unter Belastung bessere Werte als unbelastet. Die Untersuchung der Berechnungsdaten im Detail weist auf einen Bedienungsfehler hin. Die Ergebnisse bleiben in Folge unberücksichtigt.

Beobachtungen

Eine Internetrecherche zur Firma *BQR* und dem Tool *CARE Manager* brachte keinerlei Ergebnisse. Das Benutzerhandbuch beschreibt die Bauteil-Kennwertbasis, macht jedoch keine Angaben zu den Berechnungsmethoden. Aus Anmerkungen und Einschränkungen, die im Handbuch angedeutet werden, kann gefolgert werden, dass die Berechnung auf Basis des Parts-Count Verfahrens beruht. Aufgrund der Ausrichtung als prediktives Werkzeug, sind keine statistisch erhobenen Ausfalldaten bereitzustellen.

Zu den Untersuchungen mittels CARE-Manager muss gesagt werden, dass die Ergebnisse und Schlussfolgerungen stark zu hinterfragen sind. Neben der vermuteten Fehlbedingung des Werkzeugs, sind auch Übertragungsfehler von Ergebnissen bzw. Umrechnungsfehler zu finden.

Wie bereits in Abschnitt 4.2.5 auf Seite 68 untersucht, ist die angenommene Temperaturlast mit maximal 65 °C zumindest in stark belasteten Bereichen zu niedrig angenommen. Die im Bericht geschilderte Berechnung bei 25 °C laut Untersuchungsbericht, hat keinen praktischen Nutzen und wird laut Berechnungsrohdaten des Werkzeugs auch so nicht durchgeführt.

Der Untersuchungsbericht macht genaue Angaben zum Arbeitsaufwand der Kennwertermittlung. Der *Gesamtzeitaufwand* um die Bauteilbibliothek in das CARE-Tool einzupflegen, die Stücklisten im CARE-Tool anzulegen, die Berechnung mit und ohne Stressfaktoren durchzuführen und schlussendlich zusammenzufassen und zu bewerten, betrug ca. fünf Mannwochen.

Die Aufteilung auf die einzelnen Aufgaben war dabei wie folgt:

Bibliothek:	1,5 Wochen
Stressfaktoren einzeln berechnen bzw. messen:	2,5 Wochen
Stückliste in Tool einpflegen:	1 Woche
Zusammenfassung und Berechnung:	< 1 Tag

ANMERKUNG: Bei einer mündlichen Befragung wurde als Hinderungsgrund zur generellen Anwendung der kennwertbasierten Verfügbarkeitsberechnung mit dem bereits eingeführten Tool “CARE Manager V8.7” der Zusatzaufwand angegeben.

Positiv ist zu vermerken, dass der Untersuchungsbericht klar auf den Nutzen der systematischen Kennwertermittlung hinweist. Weiter ist offensichtlich auch

die Notwenigkeit für Berechnungen unter Stress bzw. erweiterten Umgebungstemperaturen bewusst. Der Bericht kommt auch zum Schluss, dass in der Vergangenheit gestellte Anforderungen (Details siehe 4.2 auf Seite 62) nicht umsetzbar sind.

Viele Ungenauigkeiten, Berechnungsfehler und fehlerhafte Schlussfolgerungen wären vermeidbar gewesen. Entweder wurde der Bericht unter hohem Zeitdruck und/oder auf zu wenig Wissen basierend durchgeführt. Einige Ergebnisse, speziell auch die Begründung für keine generelle Einführung des Tools, bieten wichtige Anhaltspunkte für die Funktionalität des eigenen Werkzeugs und auch Anregungen für die Verbesserung des Qualitätsprozesses.

Abgeleitete Anforderungen

PR 2 **Kennwert-Standards elektronisch verfügbar**
Standard-Kennwerte auf Basis der SN29500, IEC 61709 oder ähnlicher Standard-Werke müssen mittels Datenbank zur Verfügung stehen.

PR 3 **Hersteller-Kennwerte elektronisch verfügbar**
Hersteller-Kenndaten sollen ebenfalls in die gemeinsame Datenbank eingepflegt werden.

PR 4 **Elektronische Erfassung von Bauteil-Zuverlässigkeitsdaten**
Ein Datenbankeintrag zu einem Bauteil soll ausdrücklich auch sämtliche Kenndaten zur Zuverlässigkeitsberechnung beinhalten.

TR 4 **Bauteilerfassung: Zeitaufwand minimieren**
Zeitaufwand für Übernahme der Bauteile muss minimiert werden. *Größenordnung:* Minuten pro Baugruppe

5.1.4. Zweite systematische Untersuchung

Im Frühjahr 2013 wurden die maßgeblichen Zuverlässigkeitskenndaten MTTF und λ für ausgesuchte Baugruppen, darunter auch das Netzteil NTv2, sowie die Sicherheitsbaugruppe SBv1, auf Basis der SN29500 und unter Berücksichtigung von Temperatureinflüssen berechnet.

Der Untersuchungsbericht lag zum Zeitpunkt der Begutachtung im Rahmen dieser Arbeit nicht vor, somit konzentriert sich die nachfolgende Betrachtung ausschließlich auf die Interpretation der vollständig vorliegenden Berechnungsdaten.

Eigenschaft	NTv1	NTv2	SBv1
Datenquelle		Stücklisten, SN29500	

Berechnungsgrundlage

Laut Ergebnisdaten wurden drei Methoden angewendet:
1) Berechnungen/Einträge aus alter Datenbank
2) Schätzwert
3) SN29500
Die genau verwendete mathematische Methode ist unbekannt.
Berechnungen: unbelastet (25 °C) und unter Stress (nur Temperatur: bei 30 °C und 40 °C)

Die Inhalte des Untersuchungsberichts tabellarisch dargestellt:

		NTv2	SBv1
Berechnungen und Einträge aus alter Datenbank			
λ *[FIT]*		666,67	nicht erfasst
MTTF [h]		> 1 500 000,00	nicht erfasst
MTTF [a]		171,23	nicht erfasst
Während Untersuchung generierte Schätzwerte			
λ *[FIT]*		561,79	k.A.
MTTF [h]		1 780 000,00	k.A.
MTTF [a]		203,19	k.A.
Berechnung auf Basis der SN29500			
λ *[FIT]*	*bei 25 °C*	399,01	1 916,41
	bei 40 °C	707,41	3 789,02
MTTF [h]	*bei 25 °C*	2 506 200,00	521 810,00
	bei 40 °C	1 413 600,00	263 920,00
MTTF [a]	*bei 25 °C*	286,09	59,57
	bei 40 °C	161,37	30,13

Tabelle 5.9.: Ergebnisse der zweiten systematischen Verfügbarkeitsuntersuchung

Die Ergebnisse sind unauffällig, die Stress-Temperaturen zu niedrig gewählt. Die deutlich schlechteren Kennwerte der Sicherheitsbaugruppe erklären sich durch den erheblich aufwändigeren Aufbau mit deutlich mehr Bauteilen. Wie bereits in Abschnitt 2.3.2 auf Seite 35 erklärt, ist der hier berechnete, Bauteil spezifische Ausfallkennwert MTTF, nicht mit dem sicherheitsrelevanten $MTTF_D$ zu verwechseln.

Die vorliegende Auswertung ist aufwändig gemacht und versucht, sowohl alte als auch neue Kennwertberechnungen über sämtliche Baugruppen aufzulisten. Teilweise wurden zu den Komponenten auch Teilkennwerte (unterschiedliche

Prints) berechnet und Bauelemente mit hohem Einfluss auf das Ergebnis hervorgehoben.

5.2. Gegenüberstellung und Bewertung

Im diesem Abschnitt werden die unterschiedlichen Ergebnisse für die *Kennwerte für die unbelastete Baugruppe NTv2* aus den verschiedenen analytischen und empirischen Ermittlungsmethoden gegenübergestellt und abschließend auf ihre *Eignung als Referenzkennwerte bewertet*:

- Referenzberechnung mittels parts count Verfahren bei 40 °C und bei moderater Belastung von 60 °C (Tabelle 4.7 auf Seite 72).
- Zweite Referenzberechnung auf Basis der Rückläuferdaten unter worst case Annahme, also inklusive der beeinflussenden Faktoren zur Einsatzzeit- und Rückläuferkorrektur.
- CARE Manager 2007 (25 °C) [3]
- Aus Untersuchung 2013 (in Tabelle "Exam 2013" bezeichnet), die ermittelten Werte auf Basis der SN29500 bei 40 °C.

Aufgrund der ähnlich zu bewertenden Ermittlungsbasis wäre die Erwartung, dass die Ergebnisse der CARE-Untersuchung, das Ergebnis der Untersuchung von 2013 (Exam 2013) und die selbst berechnete Parts Count Referenz zu sehr ähnlichen Ergebnissen kommen.

		Parts Count Ref	Rückläufer	CARE 2007	Exam 2013
λ *[FIT]*	bei 40 °C	790,70	947,52	1 688,90	707,41
	bei 60 °C	1 023,00			
MTTF [a]	bei 40 °C	144,37	120,48	67,59	161,37
	bei 60 °C	111,59			

Tabelle 5.10.: Gegenüberstellung der praktisch ermittelten Ergebnisse aus unterschiedlichen Berechnungsquellen

Generell Die Ergebnisse der Parts Count Referenzberechnung und Exam 2013 weichen doch überraschend deutlich voneinander ab. Aufgrund der selben Berechnungsbasis und bei gleicher Temperatur, wäre eine bessere Übereinstimmung erwartet worden.
Die Rückläuferstatistik weicht auf den ersten Blick um knapp 20 %

3 Zum Vergleich werden die Kennwerte bei 25 °C herangezogen, die anderen Werte sind nicht vertrauenswürdig.

von der Referenzberechnung ab. Bedenkt man allerdings, dass dieses Ergebnis realen Umgebungsbedingungen, also Temperaturumgebungen auf Bauteilebene von 60 °C bis 85° C (gemessen) entspricht, dann reduziert sich diese Abweichung, wie ein Vergleich mit der Referenzberechnung bei 60 °C zeigt.
Die grobe Abweichung bei der Berechnung unter Verwendung des CARE Manager weist nochmals auf die bereits vermutete Fehlbedienung hin.

Rückläufer Die selbst durchgeführte Berechnung basiert auf Daten der Rückläuferdatenbank und entspricht nicht dem direkt berechneten Ergebnis, sondern der korrigierten Version (worst case). Das Ergebnis ist auch aufgrund aufgezeigter Ungenauigkeiten in Erfassung und Pflege der Datenquelle zu hinterfragen. Unter den gegebenen Annahmen sollte dieser Wert einem, im realen Anwendungsfall nicht zu überschreitenden, oberen Limit entsprechen.

CARE 2007 Bei Bewertung der Ergebnisse der CARE Untersuchung 2007 fällt auf, dass diese sogar unter Raumtemperatur-Annahmen schlecht ausfallen. Ohne detaillierten Einblick in die Berechnungsmethoden bzw. die verwendeten Bauteilkennwerte ist eine Diagnose schwierig. Die Kennwerte werden aufgrund der gesammelten Erkenntnisse als Referenz ausgeschlossen.

Exam 2013 Die ermittelten Kennwerte weichen um mehr als 10 % von der Referenz ab. Mögliche Gründe sind unterschiedliche Bewertungen bzw. (Nicht-)Berücksichtigung der Kennwerte für die Stecker/Buchsen, die Lötverbindungen und die Platinen. Ohne weitere Informationen zur Ermittlungsmethode, den genau erfassten Stücklisten bzw. den Details der berücksichtigten Stressbedingungen, ist eine Beurteilung und somit auch Verwendung in dieser Arbeit nicht seriös.

Aufgrund fehlender Daten und aufgedeckter Schwächen bei der Verwendung von Werkzeugen und in der Beurteilung der Ergebnisse, kann *kein Verfahren vorbehaltlos als Referenz empfohlen* werden. Deshalb wird für den Korrektheitsnachweis des eigenen Prediktivwerkzeugs die Sicherheitsbaugruppe SBv1 als Referenz verwendet.

Zur näheren Beschäftigung mit dem Thema der Kennwertbestimmung von Felddaten wird das Studium von Kimber [Kim09, Kapitel 6,7] und Pauli [Pau03, Kapitel 7,10] empfohlen. Die Bestimmung von Vertrauensbereiche unter Anwendung verschiedener Methoden kann wiederum in [Pau03] und Galyean [Gal09] nachgelesen werden.

5.3. Sicherheitsbaugruppe als Referenz

Die Entwicklung der Sicherheitsbaugruppe SBv1 erfolgte strikt normkonform nach V-Modell. Eine akkreditierte Prüfstelle (TÜV) überwachte projektbegleitend die angewendeten Methoden und deren korrekte und durchgängige Umsetzung. Die Berechnung der spezifischen Kennwerte, sowie die resultierenden Ergebnisse, sind Hauptbestandteil der sicherheitstechnischen Zulassung und wurden dementsprechend genau kontrolliert. Somit ist der Vertrauensgrad in die Kennwerte sehr hoch. Die Kennwertermittlung erfolgte manuell per *parts count* Verfahren bei 60 °C.

	SBv1
λ *[FIT]*	7 350,40
MTTF [a]	15,53

Tabelle 5.11.: Referenzkennwerte der Sicherheitsbaugruppe SBv1 als Basis für die Werkzeugvalidierung

Die Ausfallrate der Baugruppe ist im Vergleich zu den bisher untersuchten Netzteilbaugruppen sehr hoch. Dies hat zwei Gründe:

Funktionsvielfalt Es handelt sich um eine außergewöhnlich komplexe Baugruppe, welche verschiedene Funktionen in sich vereint. Neben 24 digitalen Ein- und Ausgängen erfüllt die Baugruppe die Aufgabe einer programmierbaren SPS-Steuerung. Die Anzahl der Funktionen bedingt an sich schon eine hohe Anzahl von notwendigen Elektronikbauteilen. Die Programmierbarkeit erfordert Bauelemente mit sehr hohen Ausfallswerten wie Microcontroller, RAM und EEPROMs.

Sicherheit Die Verwendung als Sicherheitsbaugruppe erfordert neben der generell redundanten Ausführung zusätzliche Überwachungsschaltkreise, welche in Summe nochmals die Anzahl der Bauelemente erhöht (siehe Abschnitt 2.3.2 auf Seite 35).

5.4. Fazit

Die Überprüfung der über Jahre gemachten Verfügbarkeitsberechnungen zeigt, dass neben dem kontinuierlichen Sammeln und Berechnen von Kennwerten auch das Wissen über die Verfügbarkeitstheorie, als Basis zur korrekten Interpretation der Kennwerte, entscheidend ist. Auch wenn über weite Strecken Daten gesammelt wurden, fehlt eine transparente Dokumentation und verleitet zu Spekulationen. Aufgrund der fehlenden Nachvollziehbarkeit, konnten die Werte

nicht als Referenz verwendet werden. Es gilt: Der Vertrauensgrad in die ermittelten Kennwerte bestimmt die spätere Verwendbarkeit.

Weiter wurde die fehlerhafte Anwendung von Berechnungsmethoden und des eingesetzten Tools festgestellt. Dies untermauert die These dieser Arbeit, dass die Ermittlung von Zuverlässigkeitskennzahlen als kontinuierlicher und automatisierter Vorgang, innerhalb eines qualitätsfokussierten Entwicklungsprozesses, deutlich gegenüber punktuellen, individuell durchgeführten Berechnungen zu bevorzugen ist.

6. Wirtschaftlichkeitsbetrachtung

Im folgenden Abschnitt wird die Problemstellung aus dem Blickwinkel der Wirtschaftlichkeit in einem Hard- und Software produzierenden Betrieb betrachtet. Qualitätssteigernde Maßnahmen sind tendenziell zeitaufwändig, teuer und nicht als primäre Produkteigenschaften für Kunden sichtbar. Nicht jeder potentielle Kunde ist bereit, für maximale Qualität zu bezahlen. Deshalb ist es gerade auch wirtschaftlich sehr wichtig, bei Qualitätsmerkmalen wie MTTF bzw. Garantiezeit, zielgerichtet und punktgenau die Produkte auf die Marktanforderungen auszurichten.

Auf dieser Basis wird die Motivation zur zuverlässigkeitsorientierten Produktentwicklung am Beispiel eines konkreten Herstellers untersucht. Zeit- und Kostentreiber werden aufgedeckt, mögliche und sinnvolle Ansatzpunkte zur gleichzeitigen Optimierung von Kosten, Zeit und Qualität werden angedacht. Schlussendlich werden auch begleitende Maßnahmen zur Argumentation gegenüber Kunden dargestellt.

Das untersuchte Unternehmen positioniert sich im Markt als Qualitätsanbieter von High-End Produkten zur Automatisierung von Maschinen und Anlagen. Das Portfolio umfasst unterschiedliche Leistungsgruppen von programmierbaren Zentralbaugruppen, analoge und digitale Ein- und Ausgangsbaugruppen in modularer Bauweise, Spezialbaugruppen und Anzeigeterminals.

Im Jahr 2009 wurde das Produktportfolio um ein modulares, voll integriertes *Sicherheitssystem* nach höchstem Industrie-Standard (Sicherheitskategorie SIL 3, PL e), erweitert. Das Sicherheitskonzept wurde dabei um eine homogen redundante Struktur in Hardware sowie eine diversitär arbeitende Software aufgebaut, um die hohe Anforderung hinsichtlich der Auftretenswahrscheinlichkeit eines gefährlich wirkenden Fehlers ($\mathrm{PFH} \leq 10^{-7} \frac{1}{\mathrm{h}}$ für die Gesamtanwendung bzw. $\mathrm{PFH} \leq 10^{-8} \frac{1}{\mathrm{h}}$ für den Steuerungsanteil) zu erreichen.

Bei der Entwicklung von Sicherheitsbaugruppen werden besondere Anforderungen an die Entwicklungsabteilungen und auch an die Produktion gestellt. Potentielle Ausfälle aufgrund von Software-Fehlern müssen genau gleich betrachtet und ausgeschlossen werden, wie Hardware-Ausfälle. So müssen weitreichende Maßnahmen zur Gewährleistung von Code-Qualität in der Software getroffen werden. Spezielle Test- und Diagnosemaßnahmen in der Hardware und schlußendlich auch in der Serienproduktion, schützen das Produkt über die gesamte Lebensdauer in höchstem Maß vor unentdeckten Fehlern und Ausfällen.

Qualität und Wirtschaftlichkeit

Allgemein wird bei näherer Betrachtung rasch offensichtlich, dass Maßnahmen zur Erhöhung der Verfügbarkeit üblicherweise einen (zeit-)aufwändigeren Entwicklungsprozess erfordern, nachhaltige Maßnahmen auf Produktebene in komplexeren Produkten resultieren und damit auch die Entwicklungs- und Herstellkosten steigen.

Bei [Bir07] findet man eine Übersicht zu Maßnahmen die zur Sicherstellung hoher Qualität anwendbar sind (Abbildung 6.1). Zusätzlich werden die Maßnahmen, die weiterhin die Wirtschaftlichkeit (bei Birolini *Cost-Effectiveness-Assurance*) gewährleisten, dargestellt.

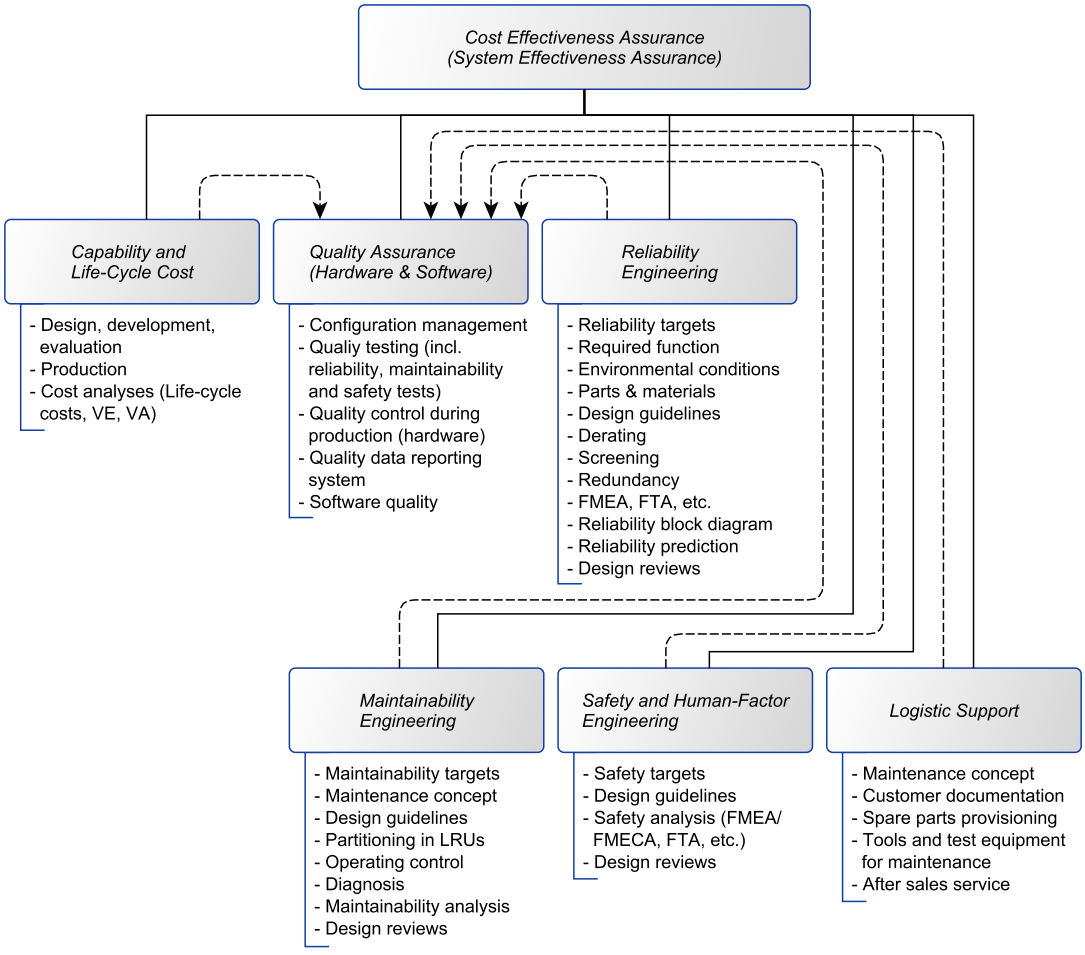


Abbildung 6.1.: Cost-Effectiveness-Assurance laut [Bir07]

6.1. Produkteigenschaften

Um ein genaues Bild der individuellen Festlegung des Qualitätsbegriffs im untersuchten Betrieb zu bekommen, werden in diesem Abschnitt bestehende Maßnahmen in Entwicklung und Produktion vorgestellt. Zuvor werden die wichtigsten Kennwerte und Produkteigenschaften, die diese Maßnahmen notwendig machen, aufgelistet.

Die Baugruppen zeichnen sich unter anderem durch folgende Eigenschaften aus:

- Betriebstemperaturbereich -30 °C . . . +60°C
- kompakte Bauweise, d.h. hohe Bauteildichte
- Modulvarianten mit erweitertem Temperaturbereich von -40 °C . . . +70 °C bei gleichzeitiger Betauungsfestigkeit
- Garantiezeiten von 5 Jahren und mehr (bis zu 15 Jahren)

Um diese Eigenschaften zu erreichen, werden verschiedenste Maßnahmen gesetzt, unter anderem:

- 48h Run-In jeder einzelnen Baugruppe
- Klimaprüfungen (DIN/EN 60068-2-14 mit erweitertem Temperaturbereich)
- Prüfung der Lagerungsfestigkeit bei Kälte und Hitze, mit Temperaturwechseln und bei hoher Feuchtigkeit (DIN/EN 60068-2-1, -2, -14, -30)
- EMV-Prüfungen mit erhöhten Pegeln
- Schock- und Vibrationsprüfungen (DIN/EN 60068-2-6 und -27)
- Messung von Bauteiltemperaturen kritischer Bauelemente zur Lokalisierung von Hot Spots
- HALT/HASS-Tests
- passives Kühlkonzept (Funktionsweise der Baugruppen somit nicht abhängig von mechanisch beweglichen Teilen)

Aus den Produkteigenschaften ist direkt ableitbar, dass der betrachtete Hersteller in hohem Maße mit den Problemen der Zuverlässigkeitstheorie konfrontiert ist. Erweiterte Temperaturbereiche bei gleichzeitig passiver Kühlung und der Einsatz in rauhen Umgebungen, wo zuverlässiger 24/7-Einsatz gefordert wird, stellen die Produktentwicklung vor hohe Herausforderungen.

Gleichzeitig zeigen die aufgeführten Maßnahmen, dass die Überprüfung und der Nachweis von Zuverlässigkeitseigenschaften erst recht spät im Entwicklungsprozess erfolgen. Tatsächlich werden erst im Prototypenstadium, also nach

Abschluss der eigentlichen Schaltungsentwicklung, wichtige Kenngrößen erfasst und führen somit immer wieder zu teuren und zeitraubenden Revisionen.

Daraus lässt sich die Motivation für *Maßnahmen die schon während der Produktentwicklung greifen*, direkt ableiten.

6.2. Zuverlässigkeitskennwerte - Strategischer Stellenwert

Das untersuchte Unternehmen hat sich einen Namen als Anbieter für hoch flexible, robuste und dauerhafte Steuerungslösungen gemacht. Das grundsätzliche Gerätedesign kommt der Anwendung in rauhen Umgebungen mit hohen Belastungen durch Vibration und großen Temperaturdifferenzen bei der gleichzeitigen Forderung nach Langzeitverfügbarkeit entgegen:

- Das rein passive Kühlkonzept schützt gegen Temperaturausfälle, verursacht von mechanischen Schäden aktiver Kühlkomponenten, wie beispielsweise Lüftern.
- Das Mechanik-Konzept bietet durch Verschraubung der aus Aluminium-Druckguss aufgebauten Baugruppengehäuse mit dem ebenfalls in Metall ausgeführten Baugruppenträger eine sehr hohe Resistenz gegen Vibration und Schock. Gleichzeitig ergeben sich daraus Vorteile in der Wärmeableitung.

Diese Eigenschaften passen sehr gut in Nischenmärkte wie der Automatisierung von Windenergieanlagen, Marineanwendungen oder in den Spezialmaschinenbau. In Breitenmärkten lässt sich, trotz unbestrittener Vorteile im Alltag, mit diesen Qualitätsmerkmalen deutlich weniger punkten. Weshalb ist das so?

6.2.1. Kundenwünsche und Lifecycle-Probleme

Kunden gehen in der betrachteten Automatisierungsbranche üblicherweise mit ihrem Steuerungslieferanten langfristige Partnerschaften ein. Lieferantenwechsel werden gut überlegt, da diese teuer sind, einen hohen Schulungs- und Entwicklungsaufwand bedeuten und das Risiko bergen, dass sich Produkteinführungen verzögern.

Kriterium	Erwartung
Preis	niedrig
Qualität	hoch
Robustheit	hoch
Bedienerfreundlichkeit	hoch

Wartungsfreundlichkeit	hoch
Funktionsvielfalt	hoch
Produktionsort	N/A[a]
Lebensdauerkosten	niedrig[b]

Tabelle 6.1.: Entscheidungskriterien und die entsprechende Erwartungshaltung bei der Auswahl eines Steuerungs-Lieferanten aus Sicht eines Maschinen- und Anlagenherstellers (Auswahl)

Wie nicht anders zu erwarten, stehen verschiedene Erwartungen zueinander im Widerspruch. In Auswahlverfahren wird gerne versucht, unterschiedliche Anbieter und deren individuellen Stärken gegeneinander auszuspielen. Geht ein Lieferant zu sehr auf Forderungen eines potentiellen Kunden ein, setzt er sich einem hohen wirtschaftlichen Risiko aus. Winken jedoch hohe Stückzahlen, so kann mit günstigeren Herstellkosten spekuliert werden, was wiederum das Risiko potentiell senkt. Man sieht, eine “richtige” Entscheidung ist nicht trivial.

Partnerschaften sind nach einer Zusage nicht statisch, sondern unterliegen einem stetigen Verhandlungsprozess. Lieferantenaudits, Qualitätsüberprüfungen, Auswertung von Rückläufer- und Reparaturstatistiken und jährliche Preisverhandlungen sind übliche Vorgänge. Dabei werden unterschiedlichste Wünsche und Forderungen an den Lieferanten herangetragen:

Wunsch/Forderung	Begründung(en) - Kundensicht	Problematik
Preisanpassung (jährlich)	Kostendruck im Wettbewerb; Bauteile werden immer günstiger	Standortkosten (z.B. durch Inflationsanpassung bei Gehältern)
Individuelle Funktionserweiterungen	Innovationsdruck, technologische Marktführung	oft unpassend für breite Kundenschicht, fehlende Umsetzungskapazitäten
Unterstützung bei Projekten	Time to market	(Wie) werden anfallende Kosten verrechnet?

Tabelle 6.2.: Beispiele für Wünsche und Forderungen gegenüber dem Gerätelieferanten

Gerade kleine und mittlere Unternehmen werden durch die hohe Abhängigkeit

a Entwicklungs- und Produktionsstandort spielt keine Rolle, es wird davon ausgegangen, dass die Gesetze, Bestimmungen und Normen am Einsatzort eingehalten werden.

b Lebensdauerkosten werden in Auswahlverfahren meist nicht speziell betrachtet, sind aber in den Erwartungen an Service und Reparatur inkludiert.

von einzelnen Kunden und geringe Personalreserven, mit solchen Erwartungen vor hohe Herausforderungen gestellt.

Es gibt auch Anfragen die sich spezifisch auf die Qualitätskennzahlen einzelner Produkte beziehen. So werden immer wieder “garantierte” MTTF-Werte oder auch “individuelle Absolutwertberechnungen der Lebensdauer” gefordert. Dass dies schon generell nur mit starken Einschränkungen der Genauigkeit und Einsetzbarkeit (z.B. auf Basis von Rückläuferstatistiken) oder mit erheblichem Aufwand (Lebensdauertests) möglich ist, wird von Kunden nur ungern akzeptiert. Wäre die Ermittlung der Kennwerte pro Baugruppe nur einmal durchzuführen, dann würde dies von Qualitätsanbietern durchaus in Erwägung gezogen. Dem steht aber der praktische Alltag in Entwicklung und Produktion entgegen:

- Time To Market als erfolgsentscheidender Faktor - keine Zeit für aufwändige Lebensdauertests.
- Im Vergleich zu Consumer-Produkten geringe Stückzahlen, wodurch aufwändige Tests schnell preislich relevant werden.
- Problem der Änderung von Baugruppen während des Lieferzeitraums, wodurch sich das Ausfallsverhalten dieser Baugruppen ändert:
  - Bauteile werden abgekündigt und werden durch Second Source Bauteile ersetzt.
  - Bauteile werden nach wichtigen Grundspezifikationen am freien Bauteilmarkt nach optimalem Preis ausgewählt, können sich also am jeweiligen Print pro Charge ändern.
  - Ausfallkennwerte, deren Qualität bzw. Nachvollziehbarkeit, sind bei Bauteil-Lieferanten unterschiedlich zu bewerten.
  - Bauteile, insbesondere integrierte Schaltkreise, werden durch den Hersteller im Zuge eines kontinuierlichen Cost-down und Verbesserungsprozesses intern verändert. Dies kann, beispielsweise bei Extremanforderungen an die Betriebstemperatur, negative Auswirkungen haben. Da eine aktive Information an den Integrator meist ausbleibt oder erst sehr spät erfolgt, ist das ein Qualitätsrisiko für Endprodukte.
- Optimierungen und Revisionen werden aufgrund von neuen Preisanforderungen oder auch Funktionsanpassungen und Fehlerbehebungen durchgeführt. Detaillierte Qualitätsbetrachtungen sind dabei meist nicht (mehr) im Fokus.

Aufgrund dieser Unwägbarkeiten, verbunden mit der unweigerlichen Erhöhung der Kosten und Verlängerung der Entwicklungszeit, wird in der Praxis meist auf die durchgängige Erhebung von Qualitäts- und Zuverlässigkeitskennzahlen verzichtet.

Bestehen bereits Methoden zur qualitätsorientierten Entwicklung und zumindest grundlegende, systematische Berechnungs- oder Nachweismethoden, dann lassen sich diese auch im Marketing und Vertrieb vorteilhaft bewerben. Weniger Ersatzteilhaltung, geringere Standzeiten und somit geringere Kosten und höherer Ertrag sind schlagende Argumente im Wettbewerb.

PR 5 Zuverlässigkeitskenndaten auf regelmäßiger Basis erfassen
Hoher Vertrauensgrad in die Korrektheit erhobener Daten muss für die Veröffentlichung gewährleistet werden. Entsprechende Tests und regelmäßige Vergleiche mit den praktisch erhobenen Daten sind zu definieren.

6.2.2. Hochwertige Produkte - Gutes Image

Zuverlässigkeit und Verfügbarkeit sind qualitative Grundanforderungen an Produkte. Diese werden durch Kunden überprüft und bei Nicht-Erfüllung urgiert, können aber nach Abschluss der Entwicklung eines Produkts kaum mehr verbessert werden. Versuche zur nachträglichen Erhöhung der Zuverlässigkeit, bedeuten immer einen Eingriff in das Produkt. Mögliche Maßnahmen sind dabei *Wartung, Austausch* oder *Redesign*. Es liegt somit im wirtschaftlichen Interesse, Verfügbarkeit so früh als möglich in einem Produkt als systemimmanente Eigenschaft zu verankern und auch zu prüfen.

In der einschlägigen Literatur findet man dazu den Begriff der *rule of ten* (siehe Abbildung 6.2). Die Grundaussage dieser Regel ist, dass korrigierende Maßnahmen, pro Phase in der deren Anwendung versäumt wurde, jeweils um den Faktor zehn teurer werden.

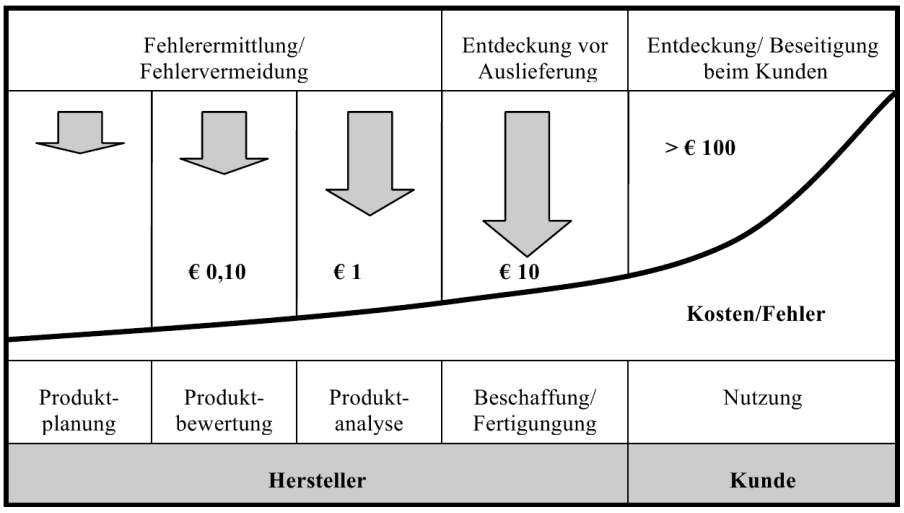


Abbildung 6.2.: “Rule of ten” ([TM03], Seite 41)

Auch aus diesem Blickwinkel ist ersichtlich, dass es das Ziel sein muss, die Zuverlässigkeit bereits in der Entwicklung zu berücksichtigen, ständig zu überwachen und Erfahrungen in den Entwicklungsprozess zurückfließen zu lassen. Zusätzlich muss auch in der Produktion gewährleistet werden, dass die gesetzten Maßnahmen über den gesamten Produktionszeitraum, die vorgegebenen Standards erfüllen oder sogar übertreffen.

Dabei besteht ausdrücklich nicht allein das Ziel, die Zuverlässigkeit zu maximieren. Viel mehr gilt es, sich auf das sensible Gleichgewicht zwischen Qualität und Preis zu fokussieren und gleichzeitig optimal mit herausragenden Funktionseigenschaften zu kombinieren. Abhängig vom Einsatzgebiet, dem Marktumfeld und den persönlichen Ansprüchen eines Herstellers und seiner Kunden, ergibt sich ein individueller Anspruch an die Produktqualität. Technische Normen, Standards und (inter-)nationale Vorschriften sind dabei verpflichtend zu erfüllende, äußere Einflussfaktoren. Marktposition (Qualitätsanbieter vs. Massenanbieter) und wirtschaftliche Strategie, sowie Zielmarkt hingegen frei gewählte, innere Einflussfaktoren.

6.3. Fazit

Die Fokussierung auf Zuverlässigkeit und höchste Qualität ist eine strategische Entscheidung. Die Forderung nach der stetigen Überwachung und Generierung von Kenndaten, lässt sich mit den folgenden Argumenten untermauern:

- Produkt-Qualität und Robustheit werden im Wettbewerb stetig wichtiger. Gerade in rauhen Umgebungen, wie beispielsweise Windkraftanlagen oder Offshore-Anwendungen, stellen auch kurze Ausfälle großen finanziellen Schaden dar und kurzfristige Vor-Ort-Reparatur ist in vielen Fällen nur mit erheblichem Aufwand, wenn überhaupt, möglich.

- Die Entwicklung der Sicherheitsbaugruppen zeigte, dass durch die konsequente Anwendung qualitätsorientierter Maßstäbe, bei paralleler Überwachung durch mathematische Methoden, bereits während der Hardware-Entwicklung überraschend neue Lösungsansätze gefunden wurden. Bereits etabliertes Wissen wurde durch die zusätzlich anzuwendenden Kontrollmechanismen hinterfragt und teilweise korrigiert.

- Reproduzierbare Qualität, rasche Feststellung von Problemen und die Forderung nach sukzessiver Verbesserung, erfordern eine ständige Überprüfung und Adaptierung des Qualitätsprozesses und entsprechende Werkzeuge, um den Aufwand gering und Verzögerungen im Time-To-Market niedrig zu halten.

- Gutes Zusammenspiel der Entwicklungsabteilungen mit der Produktion und den Stabsstellen für Qualität bilden einen Regelkreis, welcher im Idealfall zum jeweils raschest möglichen Zeitpunkt, Probleme aufzeigt und Verbesserungsvorschläge als Feedback zur jeweils zuständigen Stelle zurückliefert. Daraus ergibt sich eine steuerbare und stetig steigende Produktqualität, welche durch die ebenfalls stetig steigende Erfahrung der einzelnen Mitarbeiter positiv unterstützt wird.
- Dem Wunsch und der Forderung von Kunden nach (vergleichbaren) Kennwerten zur Zuverlässigkeit muss entsprochen werden.

Der zwingend aus den erhöhten Aufwänden, aufgrund zusätzlicher Maßnahmen in Entwicklung und Produktion, abzuleitende höhere Verkaufspreis, verringert die Wahrscheinlichkeit zum Einsatz in Massenmärkten sowie in Bereichen wo oberstes Ziel die Minimierung der *time to market* sind.

Im untersuchten Unternehmen passt die Entwicklung nach qualitätsorientierten Eigenschaften gut zur etablierten Kundenlandschaft, diese wird sogar gefordert. Damit kann mit erhöhter Robustheit, erweiterten Temperaturbereichen sowie verbesserter Widerstandsfähigkeit gegen spezifische Umweltbedingungen wie Schock, Vibration usw. als zentrale Marketingargumente geworben werden. Dies bringt für den Hersteller höhere Erträge, sofern nachweisbar höhere Verfügbarkeit vorliegt.

7. Prozesse und Methoden

Das vorliegende Kapitel befasst sich mit drei Schwerpunkten:

- *Erhebung und Beschreibung* der *bestehenden Prozesse* und Methoden beim untersuchten Entwicklungsbetrieb.
- Darstellung von *Vorschlägen zur Anpassung* dieser Prozesse als Voraussetzung einer nahtlosen Integration des Prediktions-Werkzeugs.
- Praxisorientierte Vorstellung der Umsetzung einer *Zuverlässigkeitsorientierten Schaltungsentwicklung*

Im ersten Teil wird jeweils zuerst der bestehende Prozess und dessen Eigenschaften kurz vorgestellt und gleich im Anschluss näher auf mögliche Anpassungen eingegangen. Entsprechend den Kapitel- und Unterkapitelüberschriften gibt es zu jedem Prozessteil das entsprechende Ablaufdiagramm:

- Baugruppen- bzw. *Produkt-Lebenszyklus*
  → Kap. 7.1 auf der nächsten Seite, Abb. 7.1 auf Seite 103
- *Produktrealisierung in der Hardware-Entwicklung*
  → Kap. 7.1.1 auf Seite 107, Abb. 7.2 auf Seite 108
- *Auswahl und Freigabe neuer Bauteile*
  → Kap. 7.1.2 auf Seite 109, Abb. 7.3 auf Seite 110
- *Erstellung des Schaltplans*
  → Kap. 7.1.3 auf Seite 115, Abb. 7.4 auf Seite 115
- *Manuelle und computerunterstützte Erstellung einer FMEA*
  → Kap. 7.1.4 auf Seite 117, Abb. 7.5 auf Seite 120 und 7.6 auf Seite 122

Die dabei verwendeten Ablaufdiagramme entsprechen inhaltlich den entsprechenden Teilen aus dem bestehenden Qualitätshandbuch, erweitert um die aus dieser Arbeit resultierenden Änderungs- und Erweiterungsvorschläge. Diese sind durch fette Umrahmung und grünen Hintergrund hervorgehoben.

Die in den Ablaufdiagrammen verwendete Notation hält sich an die BPMN-Notation (Business Process Model and Notation). Details können im entsprechenden Standard [OMG10] und unter der Projekthomepage (`http://www.bpmn.org/`) nachgelesen werden.

Nach Analyse und Adaption des bestehenden Entwicklungsprozesses bildet der Abschnitt *Zuverlässigkeitsorientierte Schaltungsentwicklung* (Kap. 7.2 auf Seite 129) die Verbindung der Theorie der Prozess-Anpassungsvorschläge mit konkreten Umsetzungsideen.

Den Abschluss dieses Kapitels bildet ein Fazit das auch die wirtschaftliche und somit praktische Umsetzbarkeit der Prozessadaptierungen betrachtet (Kap. 7.3 auf Seite 135).

7.1. Produkt-Lebenszyklus

Der Produkt-Lebenszyklus beschreibt die Summe aller Prozesse die ein intern in Auftrag gegebenes, entwickeltes, gefertigtes und schließlich abgekündigtes Produkt durchläuft. In Abbildung 7.1 auf der nächsten Seite ist dieser Produktlebenszyklus in zwei zu dieser Arbeit passende Prozesse aufgeteilt dargestellt:

1. *Produktrealisierung und -revision*: bereits etabliert, in einzelnen Punkten zu adaptieren
2. *Ermittlung von Zuverlässigkeitskennwerten*: noch nicht etabliert bzw. im Fall der Rückläufer- und Reparatur-Statistik stark zu adaptieren

Die farblich hervorgehobenen Teilprozesse werden außerhalb dieses Kapitels noch genauer untersucht:

- *Produktrealisierung in HW-Entwicklung* (→ 7.1.1 auf Seite 107)
- *FMEA erstellen* (→ 7.1.4 auf Seite 117)
- *Auswertung Rückläufer- und Reparaturstatistik* (→ 7.1.5 auf Seite 126)

Produktrealisierung

Der Prozess der übergeordneten Produktrealisierung entspricht einer klassischen Vorgehensweise nach dem Wasserfall-Modell. Nachdem der formale *Auftrag zur Produktentwicklung* erteilt ist, startet die *Entwicklung eines Neuprodukts*:

Planungsphase Erstellung aller relevanten Planungsdokumente für Software und Hardware. Unter anderem entstehen in dieser Phase das Lasten- und Pflichtenheft.

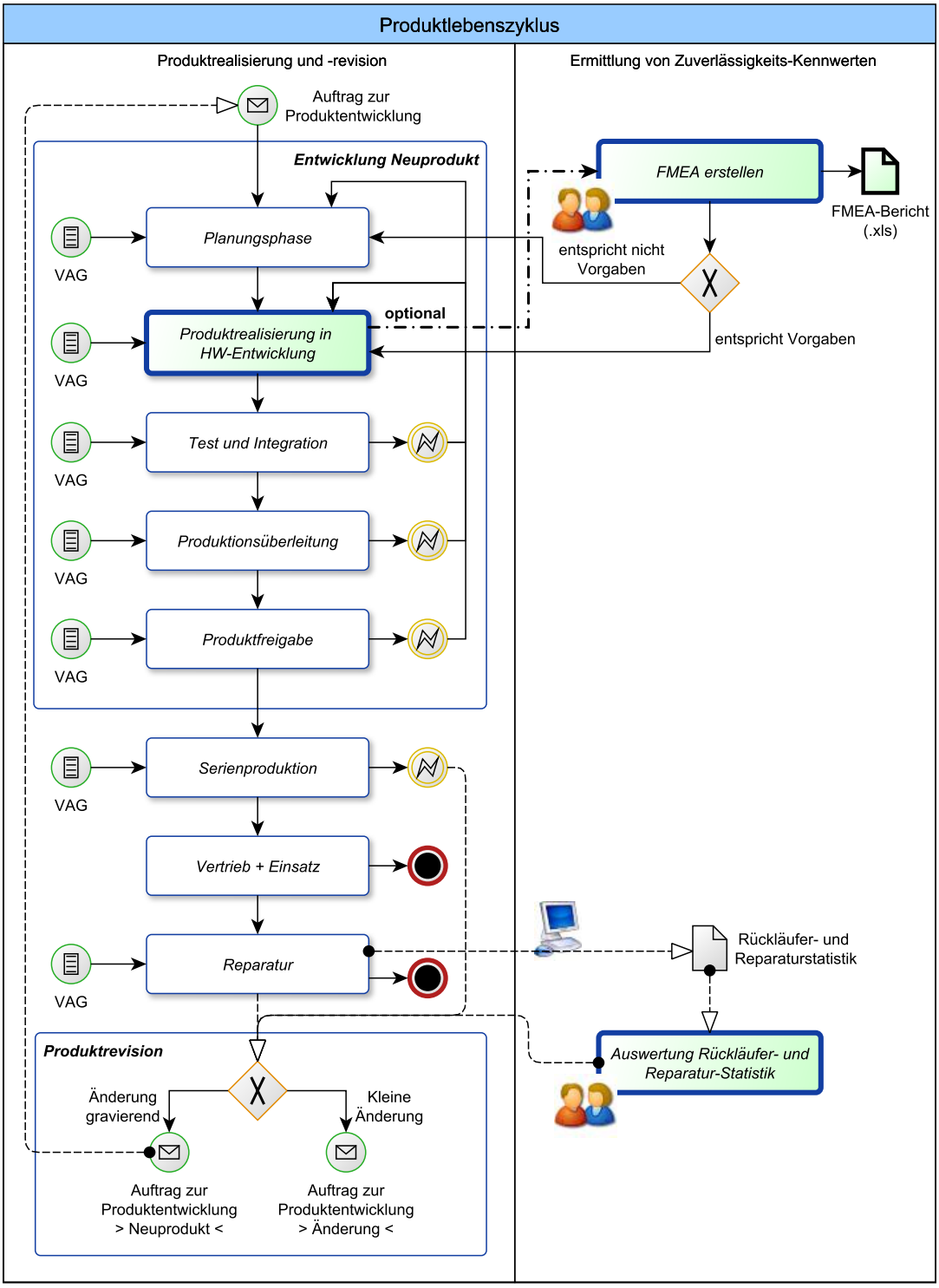


Abbildung 7.1.: Produktlebenszyklus

Produktrealisierung in HW-Entwicklung Aufbauend auf den Artefakten des vorhergehenden Prozessteils wird hierbei das Produkt bis zum Prototypenstadium umgesetzt. Bisher war optional die Erstellung einer FMEA möglich bzw. in sicherheitstechnischen Produkten durch entsprechende Vorschriften verpflichtend.

Test und Integration Die Produkteignung wird anhand passender Testmethoden verifiziert. Dabei kommen vor allem Black-Box-Tests zur Verifikation der Anforderungen aus Lasten- und Pflichtenheften und eigens definierte Integrations-Tests zum Nachweis der Eignung im Zusammenspiel mit anderen Komponenten zum Einsatz.

Produktionsüberleitung Verifikationsschritt der für die Serienproduktion notwendigen Prozesse, Arbeitsschritte und Bauteile. Entsprechen diese nicht den Vorgaben, beispielsweise ein Bauteil kann laut Auswahl nicht mit den eingeführten Lötverfahren befestigt werden, muss das Produkt im Realisierungs-Prozess neu überarbeitet werden, im Extremfall zurück in die Planungsphase. Hierbei wird auch die Wirtschaftlichkeit berücksichtigt.

Produktfreigabe Nach Abschluss aller Tests erfolgen die Einzelfreigaben in den verschiedenen Abteilungen. Die Freigaben für Software, Hardware, Prüfgeräte und Produktion müssen positiv absolviert werden um zu einer Produktfreigabe zu kommen. Mit diesem Schritt wird das Entwicklungsprojekt abgeschlossen. Die erarbeiteten Unterlagen aus den unterschiedlichen Entwicklungsbereichen werden archiviert und ein Abschlussbericht wird erstellt.

Serienproduktion In der Serienproduktion ist der interessante Aspekt die Detektierung, Erfassung und weitere Bearbeitung von defekten Produkten. Während jedem Produktionsschritt, also ausgehend von den Eingangsprüfungen aller Einzelteile, über das Print bestücken, die verschiedenen Lötvorgänge bis zur Endmontage mit abschließendem 48h-Run-In, werden die Zwischenprodukte immer wieder mit verschiedensten Methoden überprüft. Bei den dabei auftretenden Ausfällen unterscheidet man zwei Fehlerbilder:

- Zufällige und zwischen Produkten wechselnde Einzelausfälle von Komponenten und Gesamtprodukten.
- Systematische, also sich wiederholende Fehler bzw. Serienfehler.

Im ersten Fall wird, wenn möglich, der Fehler behoben und die Baugruppe, abhängig vom Umfang der Behebung, entweder vor oder bei dem Prüfschritt wo der Defekt detektiert wurde wieder in die Produktion eingegliedert. Bei Serienfehlern wird je nach Schweregrad durch das Qualitätswesen eine Eskalation gestartet, welche im nachfolgenden Prozess Maßnahmen zur Umgehung oder Behebung des Fehlers definiert. Eine dieser Maßnahmen kann sein, dass ein kom-

pletter Produktionsstopp erlassen wird und die Baugruppe mit einem Änderungsantrag an die Entwicklung auf den Produktrealisierungs-Prozess verwiesen wird.
ANMERKUNG: *Dieser Prozess ist etabliert und mit vollständiger Dokumentation hinterlegt. Im Rahmen dieser Arbeit erfolgte eine Überprüfung der Verfahrensdokumentation und verschiedener Fehlerprotokolle. Diese Überprüfung ergab, dass hier kein Handlungsbedarf besteht.*

Vertrieb und Einsatz Mit vorhandener Produktfreigabe wird ein Produkt in die offiziellen Produktlisten übernommen und darf vom Vertrieb an Kunden verkauft werden. Nachdem ein Kundenauftrag vorliegt, laut Bestellung produziert ist und ausgeliefert wird, verlässt das Produkt die Produktionsstätte. Aus qualitätstechnischer Sicht ist dies ein bemerkenswerter Zeitpunkt, da nun die Erhebung von statistischen Daten nicht mehr in der Hand des Produzenten liegt. Informationen über Zeitpunkt, Dauer, Umgebung des Einsatzes liegen nicht vor. Werden Produkte in dieser Phase defekt, werden sie entweder direkt verschrottet oder finden mittels Reparaturauftrag den Weg zur Produktionsstätte zurück. Wie in Abschnitt 2.4.2 auf Seite 46 gezeigt, führt die Summe dieser Informationsdefizite zu einer erheblichen Unsicherheit in der Bewertung von Rückläufern.

Reparatur Produkte die als "fehlerhaft" zurückgeliefert werden, untersucht man im ersten Schritt auf Fehlerreproduzierbarkeit. Liegt ein Defekt vor, wird der exakte Aufallsauslöser in Hardware und/oder Software gesucht und entsprechend auf mögliche Ausfallsursachen geschlossen. Entsprechend dieser Teilergebnisse dieses Prozesses erfolgt die Einteilung in die Rückläufer-Datenbank. Ist das Produkt defekt und eine Reparatur nicht sinnvoll oder durchführbar, wird dieses verschrottet. Andernfalls wird eine Reparatur durchgeführt, das Produkt wird dem selben qualitätssichernden Prozess mit Tests und Run-In wie bei der Herstellung unterzogen und bei positivem Abschluss an den Kunden mit entsprechendem Reparaturbericht retourniert.
Aus dem Prozess der Reparaturabwicklung und der statistischen Erfassung der Ausfälle und Defekte können die Folgeprozesse der *Produktrevision* und der *Produktabkündigung* angestoßen werden.

Die geschilderten Teilprozesse sind alle durch entsprechende interne Vorschriften definiert, in der Grafik mit "VAG" bezeichnet. Deren konkreter Inhalt ist auf dieser Beschreibungsebene ebenso wie die verschiedenen Ergebnisdokumente nicht relevant.

Im Ablaufdiagramm zum Produktlebenszyklus (Abb. 7.1 auf Seite 103) wurde die Rückkopplung aus der *Produktrealisierung in der Hardware-Entwicklung* in die *Planungsphase* bisher nicht betrachtet. Abhängig davon ob ein Produkt während oder nach der Entwicklungsphase den Qualitätsvorgaben entspricht, darf

der Prozess fortgesetzt werden. Entspricht es nicht diesen Vorgaben, so ist eine Anpassung der Planung vorzunehmen.

Dieser iterative Ansatz, welcher approximativ die Qualitätsvorgaben zur Zuverlässigkeit zu erreichen versucht, entspricht der zentralen Idee hinter den einzelnen Prozessverbesserungen. Im Kapitel *Zuverlässigkeitsorientierte Schaltungsentwicklung* (→ 7.2 auf Seite 129) wird die Umsetzungsmöglichkeit dieses Konzepts anhand eines Beispiels beschrieben.

Produktrevision

Produktrevisionen werden meist aus zwei Gründen durchgeführt:

1) Ausfallshäufung Tests im Zuge der Serienproduktion oder die Reparaturdatenbank weisen auf eine Häufung der Ausfälle bei einem Produkt hin.

2) Abkündigungen Bauteile wo keine Second-Sources verfügbar sind, werden vom Lieferanten abgekündigt und machen somit ein Neudesign oder eine Abkündigung des Produkts notwendig.

Aus Sicht des Zuverlässigkeitsprozesses ist nur der erste Punkt relevant, da bei Abkündigungen von Bauteilen der normale Entwicklungsprozess angestoßen wird. Gründe für die Ausfallshäufung können sein:

End of Life Das Produkt befindet sich am Ende des Lebenszyklus. Auf die Weibull-Verteilung übertragen, liegen die Ausfälle über der erwarteten Mittleren Lebensdauer und das Produkt tritt somit in die Phase der Altersausfälle ein.
ANMERKUNG: *Dies sollte in der Ausfallsdatenbank berücksichtigt werden.*

Qualitätsziel nicht erreicht Bauteil- oder Produktzuverlässigkeit ist niedriger als erwartet. Einflüsse auf Garantiezusicherung, Reparaturhäufigkeit und somit Lagerhaltung. Auswirkungen auf das subjektive Qualitätsempfinden und somit Image bzw. direkte wirtschaftliche Folgen durch mögliche Regressionsforderungen müssen abgeschätzt und darauf abgestimmte Gegenmaßnahmen ergriffen werden.

Chargenproblem Plötzliche Ausfallshäufungen in der Produktion weisen auf Qualitätsprobleme bei Bauteilchargen oder auch auf Fertigungsprobleme hin.

PR 6 Altersausfälle berücksichtigen
Ausfälle durch Erreichung des *End of Life* sollen aus der Ausfallsdatenbank herausgefiltert werden können, damit nicht sonstige Effekte und kritische Defekte kaschiert werden.

PR 7 Zuverlässigkeits-Kenndaten verfügbar machen
Bauteile und Produkte müssen während der Entwicklung flächendeckend mit Kenndaten ausgestattet werden und es müssen Grenzwerte definiert werden, welche als Alarm-Marker dienen können. Die durchgängige Berechnung und Bereitstellung der MTTF-Daten wird für Neuprodukte empfohlen. Bei kritischen Alt-Produkten wird eine Überprüfung der Kennwerte mittels Prediktions-Werkzeug empfohlen.

PR 8 Zuverlässigkeits-Grenzwerte definieren
Für Produkte und Produktteile müssen Grenzwerte für das akzeptable Maß an Ausfällen definiert werden. Diese Grenzwerte müssen von qualifizierten Personen festgelegt werden. Die Qualifikation definiert sich durch Wissen und Erfahrung in der Theorie der Zuverlässigkeitsberechnung und der Kenntnis der Produkte. Die Grenzwerte sind Erfahrungswerte und unterliegen somit einer zeitlichen Dynamik. Das heißt, dass mit steigender Erfahrung im Gebiet der Zuverlässigkeits-Bewertung auch die Grenzwertfestlegung für neue Baugruppen mit entsprechend höherem Vertrauensgrad durchgeführt werden kann.

Aus den geschilderten Gründen zur Produktrevision und in Folge der Ausfallshäufung ergeben sich Gegenmaßnahmen zur Verbesserung oder Behebung des negativen Trends. Wird eine produktbezogene Änderung beschlossen, so ist abhängig vom Umfang dieser Änderung entweder ein *Änderungs-Auftrag* oder ein *Auftrag zur Neuentwicklung* an die Produktentwicklung zu formulieren. Die Grenze dieser Entscheidung ist nicht exakt definierbar und wird von Fall zu Fall von Experten getroffen.

7.1.1. Produktrealisierung in der Hardware-Entwicklung

Nach Abschluss der Planungsphase folgt der Prozess der *Produktrealisierung in der Hardware-Entwicklung* (→ Abb. 7.2 auf der nächsten Seite). Dieser beschreibt die notwendigen Schritte zur Umsetzung eines Hardware-Produkts bzw. der hardwarebezogenen Teile eines kombinierten Produkts aus Software und Hardware. Dabei sind nicht nur die Planungstätigkeiten zur Sicherstellung der elektrischen/elektronischen Funktionalität vom Entwickler umzusetzen. Die Aufgaben umfassen ebenso die Sicherstellung der Produktionsfähigkeit des neu entwickelten Produkts. Das heißt, dass neu verwendete Bauteile und abweichende oder neue Produktionsverfahren auf Umsetzbarkeit geprüft werden und einer formalen Freigabe unterzogen werden müssen.

Der Prozess besteht im Wesentlichen aus folgenden Teilprozessen:

Auswahl und Freigabe neuer Bauteile Dieser Teilprozess wird im nächsten Abschnitt (7.1.2 auf Seite 109) detailliert analysiert.

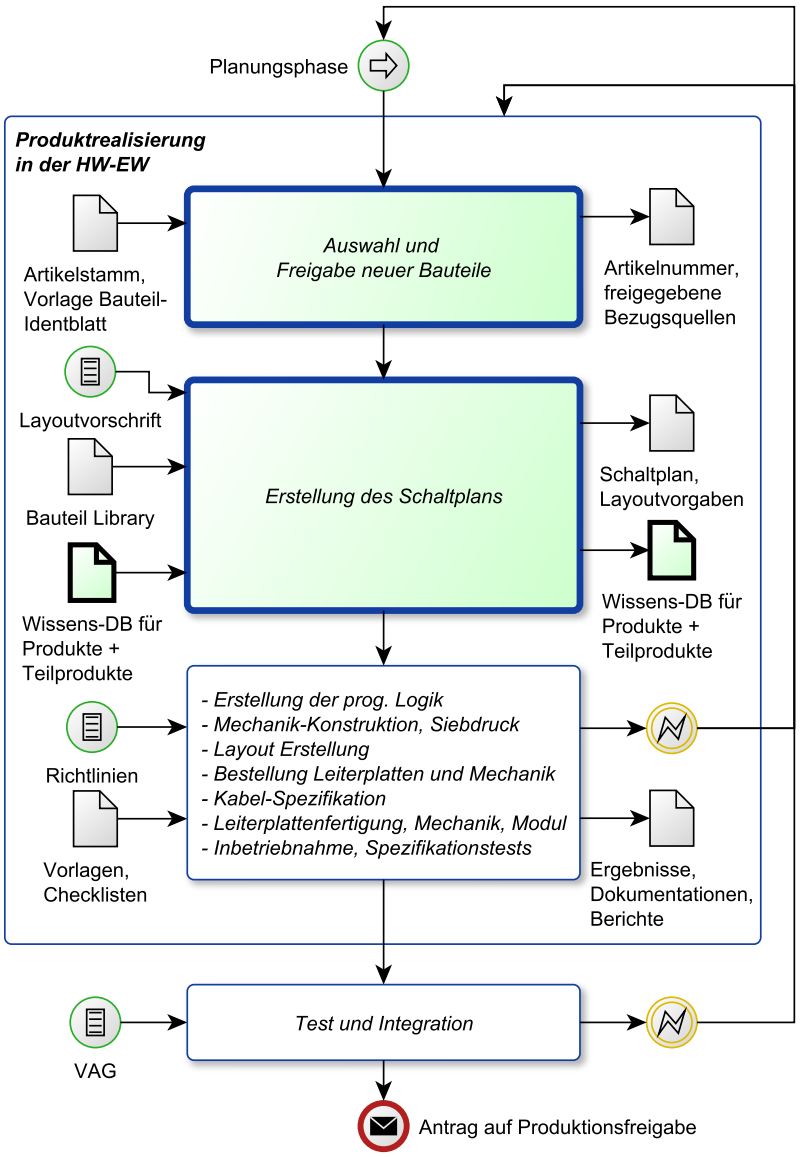


Abbildung 7.2.: Produktrealisierung in der Hardware-Entwicklung

Erstellung des Schaltplans wird im Detail in Kapitel 7.1.3 auf Seite 115 beschrieben.

Sammelblock Der letzte Teilprozess umfasst tatsächlich sieben einzelne Prozessschritte, welche im Zusammenhang mit dieser Arbeit nicht näher zu betrachten sind.

In Folge der *Produktrealisierung in der HW-EW* folgt die Überleitung aus der Hardware-Entwicklungsabteilung an die System-Engineering-Abteilung (Systemintegration und Test). Wie aus dem Ablaufdiagramm ersichtlich, führt ein

positiver Durchlauf dieses Schritts zu einem *Antrag zur Produktfreigabe*. Eine negative Untersuchung des Produkts führt zu einer Rückgabe an die Entwicklungsabteilung (Prozess *Produktrealisierung in der HW-EW*) mit dem Auftrag der Behebung der festgestellten Fehler, Unzulänglichkeiten und Abweichungen zu den Planungsdokumenten. Bei gravierenden Mängeln kann dies auch zu einer Neuaufnahme der *Planungsphase* führen.

7.1.2. Auswahl und Freigabe neuer Bauteile

Die *Auswahl und Freigabe neuer Bauteile* (→ Abb. 7.3 auf der nächsten Seite) ist ein optional durchlaufener Prozess. Als Unterprozess der *Produktrealisierung in der HW-EW* spielt dieser aus Sicht der zuverlässigkeitsorientierten Entwicklung von Hardware-Komponenten eine zentrale Rolle.

Werden Bauteile mit dem Wissen der Auswirkungen auf die Zuverlässigkeit ausgewählt, sind bei gleicher Funktionalität bessere Verfügbarkeitswerte erreichbar. Dabei ist nicht nur die simple Abfrage nach entsprechenden Kennwerten beim Hersteller gefragt. Die Datenblätter und Herstellerangaben müssen beispielsweise vom qualifizierten Experten für die extremen Anforderungen eines erweiterten Temperaturbereichs interpretiert und dahingehend überprüft werden. Gleichzeitig muss auch die Wirtschaftlichkeit zentrales Auswahlkriterium bleiben. Aus diesem Grund sind die Gedankengänge und Kriterien die zur Auswahl führen, für die Entwickler von Komponenten, die sich aus diesen Bauteilen zusammensetzen, als wertvolle Wissensbasis zu erhalten.

Die *Auswahl und Freigabe neuer Bauteile* erfolgt nach folgendem Schema:

Bestehenden Artikelstamm auf Verwendbarkeit prüfen
: Die bestehende Artikeldatenbank muss nach geeigneten Bauteilen zur Funktionserfüllung durchsucht werden. Dies ist vor allem aus Gründen der Wirtschaftlichkeit wichtig, da die Anlage neuer Bauteile sowohl erhöhten Aufwand in der Lagerhaltung als auch gebundenes Kapital bedeutet.

Antrag auf Einführung eines neuen Bauteils
: Der im Original nur aus einem Schritt bestehende Teilprozess wurde aufgrund der Bedeutung im Rahmen dieser Arbeit in drei Unterprozesse aufgeteilt:

  1. *Prüfung der Bauteileigenschaften*
     Bei jedem Antrag ist die Einsetzbarkeit für andere Produkte und die Zukunftssicherheit hinsichtlich EMV-Festigkeit, Temperaturbereich, Gehäuseform und Fertigungstechnologie zu prüfen und festzuhalten.

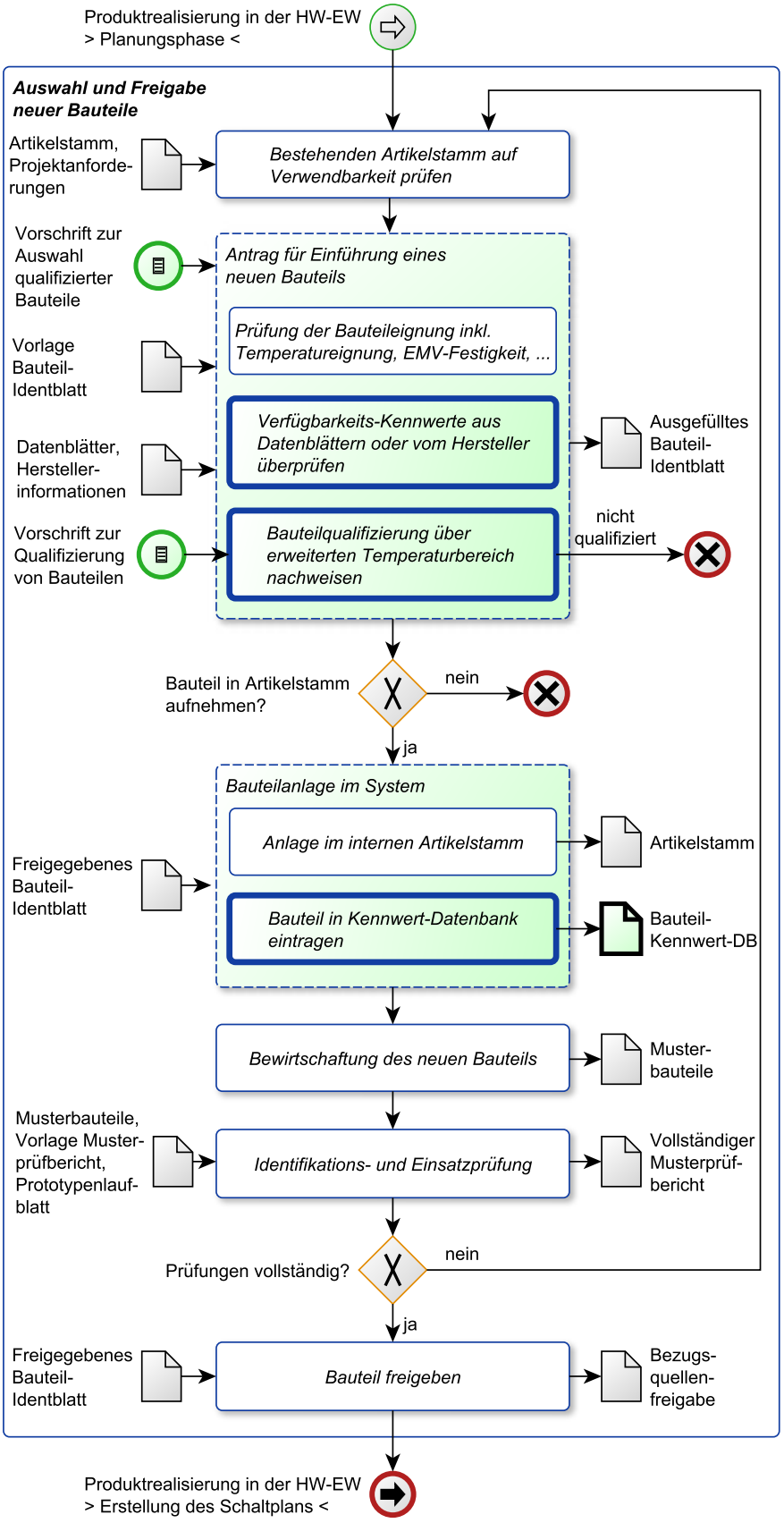


Abbildung 7.3.: Auswahl und Freigabe neuer Bauteile

2. *Verfügbarkeits-Kennwerte prüfen*
   In diesem Schritt werden die Bauteil-Kennwerte, wie in Tabelle 7.1 auf Seite 113 aufgeführt, erhoben und nach Eignung bewertet. Eine Beschreibung der Methodik und der Kriterien erfolgt im Anschluss an diese Prozessbeschreibung (siehe Prozess-Requirement auf Seite 114).
3. *Bauteilqualifizierung nachweisen*
   Auf Basis der *Vorschrift zur Qualifizierung von Bauteilen* (Beschreibung folgt) müssen Bauteile in definierten Prüfverfahren die praktische Eignung beweisen. Auf diese Weise werden Herstellerangaben überprüft, gegebenenfalls korrigiert und um fehlende Angaben erweitert.

Bauteil in Artikelstamm aufnehmen?
In diesem formalen Kontrollschritt wird auf Basis der vorhergehenden Prüfungen entschieden ob ein Bauteil in den Artikelstamm aufgenommen oder aufgrund negativer Ergebnisse ausgeschieden wird.

Bauteilanlage im System Durch die Erweiterung der Datenbasis um eine *Datenbank mit Bauteil-Kennwert* sind gegenüber dem bestehenden Prozess neu zwei Schritte zur Bauteilanlage im System notwendig:

1. *Anlage im internen Artikelstamm*
   Formelle Anlage des Bauteils im Artikelstamm durch das Qualitätswesen Bauteile.
2. *Bauteil in Kennwert-Datenbank eintragen*
   Formelle Anlage des Bauteils in der Bauteil-Kennwert-Datenbank.

Bewirtschaftung des neuen Bauteils
Muster-Beschaffungsvorgang durch den Einkauf.

Identifikations- und Einsatzprüfung
Vorbereitung zum Serieneinsatz anhand von Musterlieferung. Kontrolle der Beschreibung und Verpackung. In der Einsatzprüfung werden die funktionellen Anfoderungen und Spezifikationen des Bauteils laut Produktbeschreibung nachgewiesen. Gegebenenfalls wird neue Fertigungstechnik getestet.

Prüfungen vollständig?
In diesem formalen Kontrollschritt werden abschließend der Gesamtvorgang und alle Untersuchungen nochmals überprüft. Bei negativem Ergebnis wird das Bauteil an die Entwicklung mit der Forderung nach Nachbesserungen zurückgewiesen und der Prozess zur *Auswahl und Freigabe neuer Bauteile* startet von vorne.

Bauteil freigeben
Bei positivem Prüfungsergebnis erfolgt die offizielle Freigabe des Bauteils und darf damit bewirtschaftet, Eingang-geprüft, eingelagert und

verbaut werden.

Im Anschluss an die Bauteilfreigabe erfolgt der nächste Teilprozess der *Erstellung des Schaltplans*, wie im Abschnitt 7.1.3 auf Seite 115 beschrieben.

Als logischer Schluss und als Ergänzung zu den bereits beschriebenen Prozessanpassungen ergeben sich folgende Detail-Anforderungen:

PR 9 Definition und Einführung einer Bauteil-Kennwerte-Datenbank

Die etablierte elektronische Erfassung von Bauteil-Kennwerten soll wie folgt adaptiert werden:

- Die Erfassungszeit soll minimiert werden. Eine Eingabemaske mit automatischer Kontrolle auf Konformität wäre hilfreich.
- Die Kennwerte-Datenbank soll in die bestehende Infrastruktur zur Bauteilbeschaffung und Produktionsüberleitung (IFS-System) integriert werden.
- Der Import in die Schema- und Layout-Umgebung soll automatisch erfolgen.
- Ein Eintrag muss zur systematischen Verwendung bei Zuverlässigkeitsberechnungen zumindest die in Tabelle 7.1 aufgeführten Daten umfassen.
- Nicht vollständige Einträge müssen so rasch als möglich vervollständigt werden. Nicht vollständige und nicht konforme Einträge behindern jegliche automatische Verarbeitung der Daten. Zur Kontrolle ist ein Verantwortlicher zu benennen.
- Doppelte Datenerfassung und uneinheitliche Einträge sind zu verhindern.

Obige Aufzählung und die Tabelle konzentrieren sich auf die Ansprüche aus den gesammelten Anforderungen in dieser Arbeit. Darüber hinaus gehende Einträge sind noch zu spezifizieren bzw. von der bereits bestehenden Bauteil-Erfassung zu übernehmen.

Verpflichtende Einträge	
Bauteilkategorie	Einstufung in Bauteiltypen und Subtypen, wie z.B. integrierter Schaltkreis, Metallschichtwiderstand, Elektrolytkondensator usw.
Bauteil-Bezeichnung nach IEC-Norm	Bauteil-Symbol nach internationalem Standard (R, L, C, usw.)
Detail-Identifikation	Spezifische und eindeutige Bezeichnung, korrespondierend zu den Schaltplan-Bezeichnungen der Bauteile in *MentorGraphics*. Je detaillierter desto eindeutiger fällt die automatische Zuordnung durch das Prediktions-Werkzeug aus.

SN29500-Zuordnung	Dem Bauteil wird hierbei ein konkretes SN29500-Bauteil zugeordnet. Diese durchgängige Zuordnung ermöglicht eine normierte Beurteilung und Gegenüberstellung von Komponenten und Produkten. Dabei bleiben neue, teuere und spezielle Bauteile vollkommen unberücksichtigt und die Kennwertgenerierung erfolgt somit auf reinem Schaltungsniveau. Damit können auch ältere Produkte und Komponenten in unverfälschter Weise gegen neue Schaltungsdesigns verglichen werden.
Auswahlkriterien	Spezielle Eigenschaften die das Bauteil von anderen aus der selben Kategorie abheben (bei gleichem Preis) oder Forderungen durch den Einsatz in einer Komponente, welche die Auswahl einschränkten.
Zuverlässigkeits-Eigenschaften	Liste von Zuverlässigkeits-Kenndaten, zumindest λ bzw. MTTF, idealer Weise in Abhängigkeit der Temperatur, also zusätzlich als Formel eingetragen. Dieser Datensatz soll in einer Form vorliegen, wo er in geeigneter Weise vom Prediktions-Werkzeug abgerufen und in die Berechnung einbezogen werden kann.
Interne Bauteilqualifizierung	Verlinkter interner Qualifizierungsbericht, sofern vorhanden.
Datenblätter und Herstellerangaben	Aktuelle und vollständige Datensätze zu den Bauteilen.
Anmerkungen	Notizen, Besonderheiten, . . .
Optionale Einträge	
Produkt- und Komponenteneinsatz	Querverweise auf Komponenten und Produkten wo dieses Bauteil eingesetzt wird. Ob der Einsatz als First- oder als Second-Source vorgesehen ist, ist Zusatzinformation, wichtiger ist ob das Bauteil tatsächlich verbaut wird und in/ab welcher Produktcharge. Diese Information ist einerseits notwendig zur Abschätzung der Konsequenzen im Falle einer Abkündigung oder einer Dekommissionierung andererseits aber auch für eine genaue statistische Auswertung der Rückläuferstatistiken.
Second Source	Hier ist die Angabe eines funktional und qualitativ möglichst gleichwertigen Bauteils vorgesehen. Aus Sicht der Bauform und Wirtschaftlichkeit können hierbei im Einzelfall auch Abstriche gemacht werden.
Zuordnung im MIL-HDBK-217F	Gleicher Hintergund wie bei verpflichtendem Eintrag zur *SN29500-Zuordnung*, allerdings auf das MIL-Handbook bezogen.

Tabelle 7.1.: Verpflichtende und optionale Einträge in der Bauteil-Kennwert-Datenbank aus Sicht der Zuverlässigkeitsberechnung

PR 10 **Definition einer Vorschrift zur Auswahl qualifizierter Bauteile**

Es soll ein Leitfaden geschaffen werden, der den Hardware-Entwickler dabei unterstützt, ein Bauteil möglichst optimal nach funktionalen und zuverlässigkeitsspezifischen Eigenschaften auszusuchen. Diese Vorschrift muss genau definieren, welche Kriterien für spezifische Einsatzgebiete als Minimum zu erfüllen und welche Kennwerte für ein neu einzuführendes Bauteil zumindest anzugeben sind. Weiters wird beschrieben wie die Bauteil-Kennwerte und -Eigenschaften, wie in Tabelle 7.1 auf der vorherigen Seite aufgeführt, erhoben und nach Eignung bewertet werden müssen.
Quellen dieser Daten sind Datenblätter, Herstellerangaben oder einschlägige Fachliteratur. Berechnungen sollen auf Basis der SN29500 oder des MIL-HDBK-217F aufgebaut werden. Sollten auch diese nicht anwendbar sein, so müssen Ersatzwerte angenommen werden. Diese sind auf Basis von Worst-Case Annahmen und von Vergleichstabellen, beispielsweise aus Birolini [Bir07], abzuleiten und entsprechend zu dokumentieren.

PR 11 **Erstellung einer Vorschrift zur Qualifizierung von Bauteilen**

In dieser Vorschrift sind *wiederholbare* und genau *definierte Verfahren* zur Bauteilqualifizierung festzulegen.
Abhängig von der Bauteilart können dies unterschiedliche Prüfungen sein, welche auch über die Zeit anpassbar sein müssen, ohne an Aussagekraft, möglichst auch im rückblickenden Vergleich, einzubüßen. Beispielsweise können die heutigen Anforderungen hinsichtlich Betriebstemperaturbereich in einigen Jahren erweitert werden müssen.
Wichtig ist hierbei, dass ausreichend große Stückzahlen von Bauteilen unter Stress und unterschiedlichen Umgebungsbedingungen geprüft werden. Das Ergebnis soll den Herstellerangaben gegenübergestellt werden und bei groben Abweichungen entsprechende Stellungnahmen eingeholt werden.
Das *Ziel* dieser Untersuchungen ist nicht nur, die Herstellerangaben zu überprüfen, sondern einen optimalen Artikelstamm an Bauteilen aufzubauen die sowohl in wirtschaftlicher als auch qualitativer Hinsicht bestmögliche Kompromisse für die verschiedensten Anwendungsszenarien bieten. Im Idealfall kann der Entwickler mit den Angaben über *elektrischem Arbeitsbereich*, *Umgebungsbedingungen* und *Anforderungen an die Verfügbarkeit* die Datenbank abfragen und bekommt als Ergebnis eine Liste der geeigneten Bauteile.

Geeignete Verfahren und Methoden zur systematischen Bauteil-Verfügbarkeits-Qualifizierung finden sich unter anderem bei Birolini [Bir07, Kapitel 3 und 8] und Wilde [Wil08, Kapitel 6 ff.].

7.1.3. Erstellung des Schaltplans

Die *Erstellung des Schaltplans* (→ Abb. 7.4) bildet den wichtigsten Prozess für die Ausprägung der Eigenschaften eines Produkts. Aus Komponenten und Bauteilen werden komplexe Schaltungen zur spezifischen Funktionserfüllung zusammengestellt.

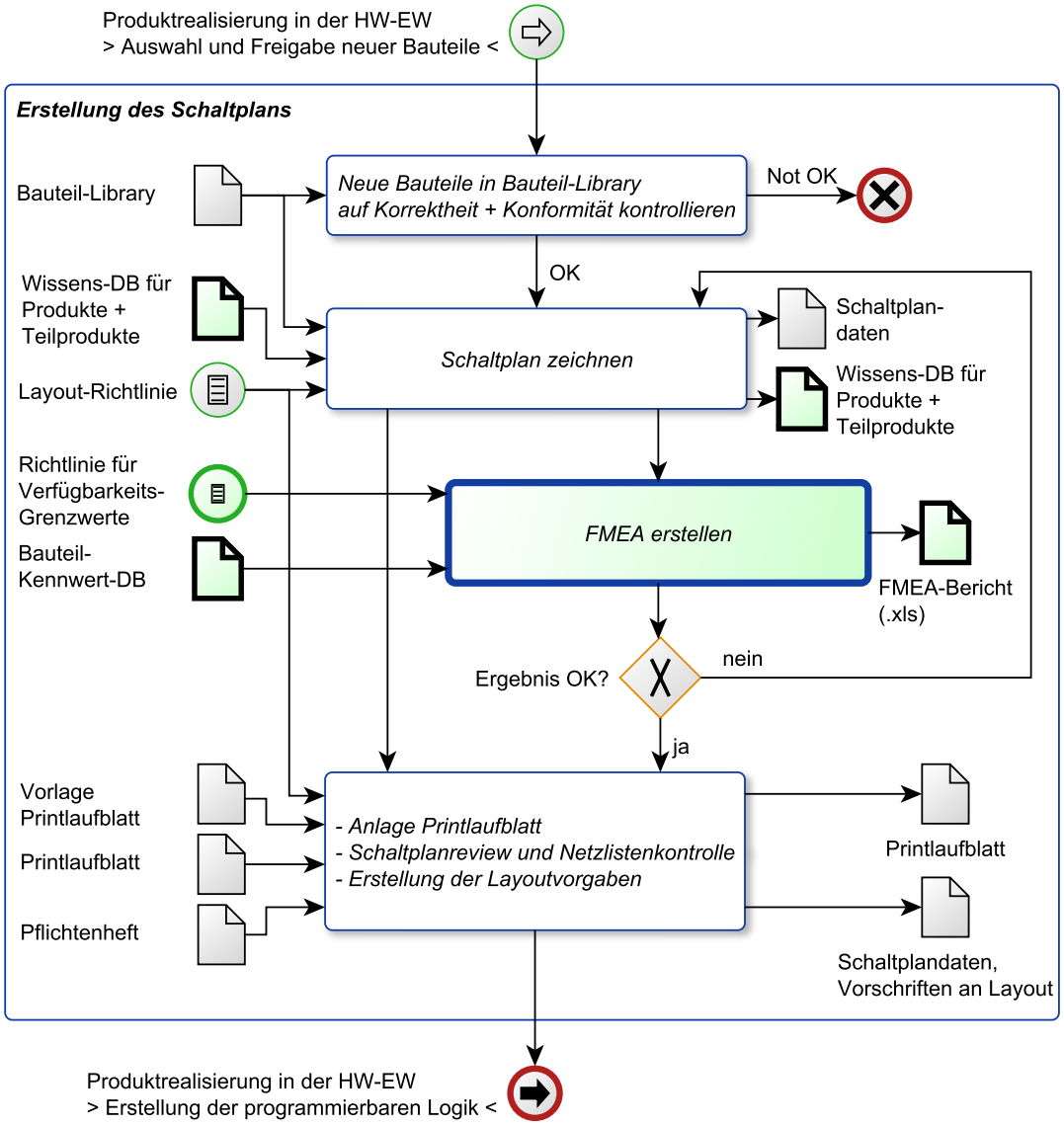


Abbildung 7.4.: Erstellung des Schaltplans

Dieser Schritt entscheidet maßgeblich, von welcher Qualität hinsichtlich Verfügbarkeit das Produkt sein wird. Diesbezügliche Schwachstellen sind nicht sofort sichtbar, resultieren aber in einer geringeren Lebenserwartung und hö-

heren Ausfallsrate. Aus diesen Gründen ist es unerlässlich, die verschiedenen Designs ständig zu kontrollieren, zu bewerten und die gemachten Erfahrungen allen Entwicklern zur Verfügung zu stellen.

Erfahrung und fachliche Qualifikation des Entwicklers spiegelt sich direkt in seinen Designs. Die gleiche Aufgabenstellung wird von unterschiedlichen Entwicklern auf unterschiedliche Art und Weise umgesetzt. Dabei wird jedes Mal die funktionale Aufgabenstellung erfüllt, die qualitativen Auswirkungen der verschiedenen Designs wird momentan nicht untersucht.

Im Sinne eines *Quick-Prototyping-Ansatzes* soll der Entwickler bereits *während der Schaltplanerstellung* dazu angehalten sein, ständig die Einhaltung qualitativer Maßstäbe zu kontrollieren. Um den daraus entstehenden Aufwand nicht explodieren zu lassen, ist ein wichtiger Teil dieser Arbeit, die *Einführung* eines in den Design-Prozess voll *integrierten Werkzeugs*, welches eine *computerunterstützte Erstellung von Qualitätsbewertungen* ermöglicht.

Die Definition des Prozesses umfasst folgende Schritte:

Neue Bauteile auf Korrektheit und Konformität prüfen Neue Bauteile werden auf Korrektheit und Konformität zu den Schaltplan-Richtlinien überprüft. Details wie das Symbol werden dabei nochmals mit dem Datenblatt verglichen. Dies ist Voraussetzung für die generelle Verwendung in Schaltplänen.

Schaltplan zeichnen Die Umsetzung des Schaltplans im dafür vorgesehenen Design-Programm auf Basis der Layout-Richtlinie. Neu ist die Anwendung einer *Wissens-Datenbank für Komponenten und Produkte*, welche unter den Prozess-Requirements genauer beschrieben wird.

FMEA erstellen Der Erstellung einer Bauteil-FMEA ist das gesamte folgende Kapitel 7.1.4 auf der nächsten Seite gewidmet.

Ergebnis OK? Eine negative Entscheidung in diesem Punkt führt zurück zu einem Redesign der Komponente oder des Produkts. Damit wird der iterative Charakter und die approximative Methodik zur Annäherung an die geforderten Grenzwerte im Prozess verankert. Ein mehrfaches Durchlaufen dieses Schritts ist durchaus erwünscht und gerade in der Anfangsphase nach Einführung der Methode nicht zu verhindern. Hier werden Erfahrungen gesammelt die wiederum in die Wissens-Datenbank einfließen.
Auch aus Sicht der Wirtschaftlichkeit sind Iterationen sinnvoll. Anstatt gleich mit bestmöglichen Bauelementen und komplexen, sich überwachenden Schaltkreisen einfache Probleme zu lösen, soll das Schaltplandesign das Notwendige und nicht das Machbare widerspiegeln.

Sammelblock In diesem Block wurden die einzelnen Prozess-Schritte *Anlage eines Printlaufblatts*, *Schaltplanreview und Netzlistenkontrolle* und *Erstellung der Layoutvorgaben* zusammengefasst. Grundsätzlich sind diese Teilprozesse im Zusammenhang mit dieser Arbeit nicht relevant, mit folgender Ausnahme:
ANMERKUNG: *Im zweiten Punkt wird eine Prüfung des Schaltplans und der Netzlisten durch eine qualifizierte zweite Person definiert. Dieser Punkt wäre im Zusammenhang einer generellen und verpflichtenden Einführung der Anlage einer FMEA auf Sinnhaftigkeit zu überprüfen und gegebenenfalls zu adaptieren.*

PR 12 Kennwert-Datenbank im Schaltplan- und Layout-Prozess verankern
Die momentan verwendete Datenbank soll mit der neuen Kennwert-Datenbank verknüpft oder von dieser ersetzt werden.
Ziel muss sein, dass die Kennwerte nur einmal und an einer Stelle eingegeben werden müssen. Dies ist sowohl aus Wirtschaftlichkeit als auch aus Gründen der Fehlervermeidung anzustreben.

PR 13 Wissens-Datenbank für Produkte und Komponenten anlegen
Neben allgemeinen Richtlinien zur Schaltplan-Erstellung soll dies eine zweite Wissens- und Erfahrungssammlung in der Hardwareentwicklung darstellen. Die Form, ob beschreibend, als Sammlung von Beispielen oder als Kombination, ist dabei zweitrangig.
ANMERKUNG: *Die Wissens-Datenbank gehört zur übergeordneten Idee zur zuverlässigkeitsorientierten Schaltungsentwicklung, welche in Kapitel 7.2 auf Seite 129 geschlossen beschrieben wird.*

PR 14 Evaluierung der FMEA- und Prediktions-Werkzeug-Einführung
Einmaliger Schritt! Nach einer ausreichend dimensionierten Probezeit, während dieser der angepasste Prozess der *Schaltplan-Erstellung* unter Verwendung des *Prediktions-Werkzeugs* in der Entwicklungsabteilung eingeführt wird, müssen die Erfahrungsberichte, Probleme und Verbesserungswünsche gesammelt und nach einer Bewertung begründet zurückgewiesen oder umgesetzt werden. Dieser Schritt ist zwingend notwendig, da erst der flächendeckende Einsatz ohne Vorbehalte die zu erwartenden, positiven Effekte voll wirksam macht.

7.1.4. Erstellung einer FMEA

Aus der FMEA in der hier verwendeten Form, als Werkzeug zur Analyse der Ausfallarten sowie der Ausfallraten eines Produkts, resultieren der Kennwert der zur erwartenden mittleren Ausfallszeit (MTTF) und die Aufschlüsselung der Gewichtung der einzelnen Bauteils-Ausfallsraten. Die MTTF soll auf Basis sinnvoller Annahmen optimiert werden, wobei die Aufschlüsselung dabei hilft, an den richtigen Bauteilen und damit Schaltungsteilen zu optimieren. Unter den

richtigen Bauteilen sind dabei die anteilsmäßig am stärksten an der Gesamt-Ausfallsrate beteiligten Bauelemente gemeint.

Die vorgestellte Bauteil-FMEA kann manuell oder mit Hilfe des *Prediktions-Werkzeugs* mit verschiedenen Zielsetzungen angewendet werden:

Gesamt-FMEA kombiniert mit Parts-Count Methode
: Worst-Case Untersuchung von Gesamt-Schaltplänen

Teil-FMEA in Kombination mit Parts-Count Methode
: Worst-Case Untersuchung von Produktteilen

FMEA zur Bestimmung sicherheitstechnischer Kennwerte
: Anwendung der Parts-Count Methode zur Teilbetrachtung von Produktteilen unter Berücksichtigung von Fehleraufteilungsmodell und Fehlervermeidung (Worst-Case Betrachtung)

FMEA in Kombination mit Parts-Stress Methode
: Alle bisher aufgezählten Varianten können bei entsprechender Datenbasis über Temperaturbereiche und somit auch auf Extremtemperaturen angewendet werden.

Details der aufgeführten Methoden sind im Theorie-Teil in Kapitel 2.4.1 auf Seite 40 nachzulesen.

In der bisherigen Entwicklungshistorie wurde eine FMEA nur für sicherheitstechnisch relevante Baugruppen erstellt. In der adaptierten Form des übergeordneten *Produktrealisierungs-Prozesses* soll diese FMEA als fixer Bestandteil der Entwicklung eines Neuprodukts eingeführt werden.

Zur besseren Erläuterung der Unterschiede zwischen dem herkömmlichen, manuell durchgeführten und auf Sicherheitstechnik ausgerichteten Prozess und dem neu einzuführenden, computerunterstützten und generell einsetzbaren Prozess, sind diese nachfolgend in zwei eigenen Unterkapiteln beschrieben.

Erstellung einer sicherheitstechnischen FMEA

Zur Zulassung eines sicherheitstechnisch konformen Produkts zur Basisnorm IEC61508 [IEC10] muss unter anderem der Nachweis erbracht werden, dass die Grenzwerte der in Kapitel 2.3.1 auf Seite 31 aufgeführten Sicherheits-Kennwerte eingehalten werden.

Die einfachste aber gleichzeitig ungenaueste Methode eines sicherheitstechnisch konformen Nachweises ist die *Ausfallsarten-Analyse mittels FMEA* mit anschließender *Bestimmung der Ausfallsraten im Parts-Count Verfahren*. Voraussetzung dafür ist ein vollständig vorliegender Schaltplan, welcher als Ausgangsbasis für den Prozess der *Manuellen Erstellung einer FMEA* (→ Abb. 7.5 auf Seite 120) dient.

Die Auswirkungen der angewendeten Methodenkombination können unter Abschnitt 2.4.1 auf Seite 40 nachgelesen werden.

Nachfolgend wird näher auf den bisher manuell durchgeführten Prozess eingegangen:

Manuelles Übertragen und Kontrollieren der Bauteil-IDs Bauteiltyp, Bezeichnung und Bauteilfunktion werden aus dem Schaltplan oder der Stückliste in die FMEA eingetragen.

Manuelles Übertragen der Bauteil-Kennwerte Für jedes Bauteil wird die Basisfehlerrate entsprechend der Bauteiltype aus der SN29500 extrahiert. Auf diesen Wert wird das allgemeine Fehlerratenmodell mit den gegebenen Umgebungswerten angewendet um die Fehlerrate bei Einsatzbedingungen zu erhalten. Alternativ können die Basisfehlerraten aus Datenblättern oder vom Hersteller bezogen werden.

Übertragen der Fehleraufteilungsraten Die Fehleraufteilungsraten werden entsprechend dem Bauteiltyp eingetragen.

Berechnung von Teilmodul- und kanalbezogener Kennwerte Auf Basis einer Gesamttabelle aller Bauteil-Fehlerraten werden für Teilberechnungen von Komponenten und Substrukturen die entsprechenden Bauteile und deren Kennwerte ausgewählt und auf eigene Berechnungsblätter übertragen.

Kontrolle durch zweite qualifizierte Person Dieser Kontrollschritt stellt die Korrektheit und Vollständigkeit vorangegangener Teilprozesse sicher. Die Anwendung kann in jedem Einzelschritt ausgelöst werden.

Übereinstimmung? Die Kontrolle muss eine Übereinstimmung ergeben, ansonsten muss der kontrollierte Schritt wiederholt werden.

Entsprechen Kennwerte den Vorgaben? Die Erreichung der sicherheitstechnischen Grenzwerte aus den zugrunde liegenden Normen ist Basis für die FMEA-Freigabe. Alternativ muss der Schaltplan überarbeitet werden und der gesamte FMEA-Vorgang beginnt von vorne.

FMEA-Freigabe Voraussetzung zur Freigabe der FMEA ist neben dem positiven Abschluss der vorangegangenen Teilprozesse auch die schriftliche Bestätigung der qualifizierten zweiten Person, die FMEA überprüft und für vollständig und korrekt befunden zu haben. Das Resultat ist der manuell erstellte FMEA-Bericht, welcher im Projektordner archiviert wird.

Es ist zu beachten, dass in jedem manuellen Schritt die optionale *Kontrolle durch eine zweite qualifizierte Person* vorgesehen ist. In der Praxis wird von dieser Möglichkeit häufig Gebrauch gemacht um Übertragungs- und Flüchtigkeitsfehlern aufgrund der Vielzahl von monotonen Wiederholungsschritten vorzubeugen.

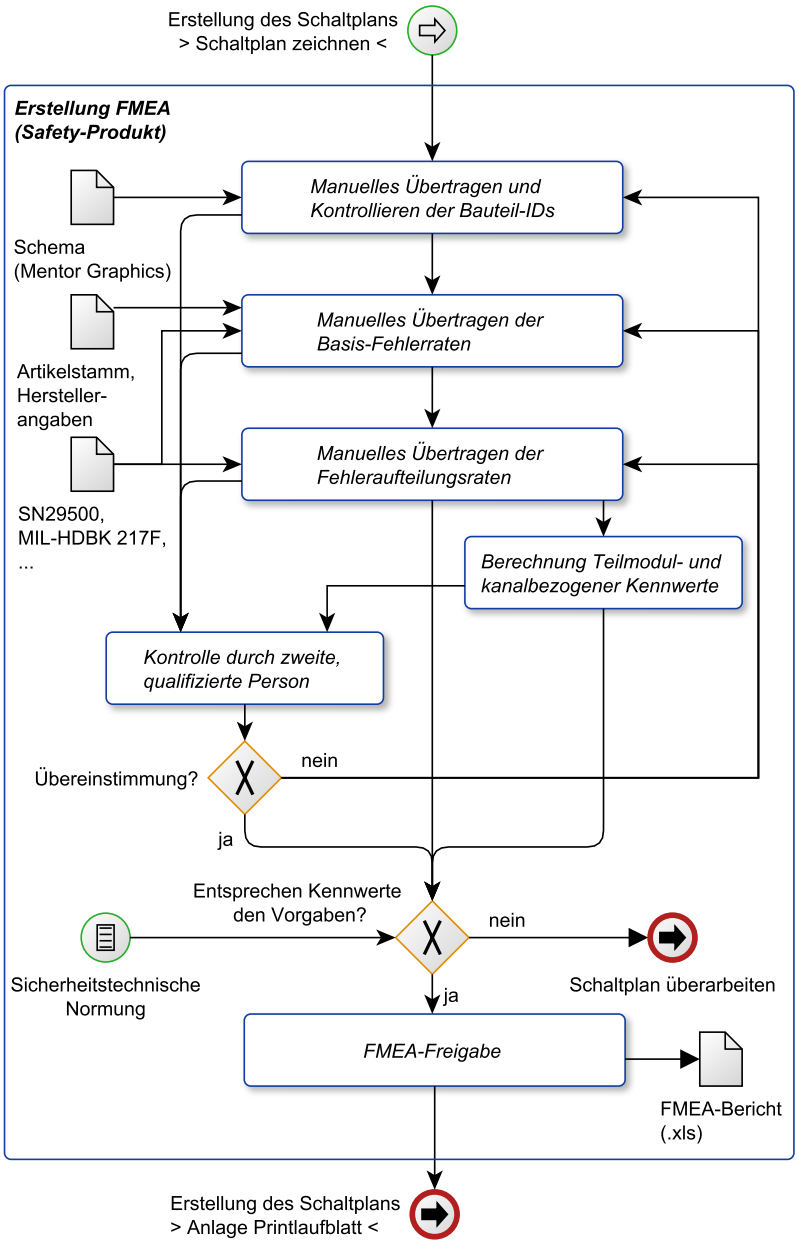


Abbildung 7.5.: Erstellung einer sicherheitstechnischen FMEA (manuelle Vorgehensweise)

Der vorliegende Prozess ist eingeführt und wurde bereits zur Umsetzung von sicherheitstechnischen Produkten angewendet und durch zertifizierende Stellen validiert. Deshalb sind Prozess-Anpassungen auf dieser Ebene nicht weiter sinnvoll und es wird auf entsprechende Vorschläge verzichtet.

Computerunterstützte Erstellung einer FMEA

Der erste Blick auf das Ablaufdiagramm des adaptierten Prozesses *Computerunterstützte Erstellung einer FMEA* (→ Abb. 7.6 auf der nächsten Seite) zeigt sofort, dass die Grundstruktur gegenüber der manuellen Variante beibehalten wurde. Diese Grundstruktur mit den Verifikationsschritten auf jeder Stufe und der abschließenden Validierung durch die Freigabe entspricht bereits dem, in der Sicherheitstechnik bevorzugten V-Modell.

Die Änderungen offenbaren sich innerhalb der einzelnen Prozessschritte:

Automatisches Übertragen der Bauteil-IDs
: Bauteiltyp, Bezeichnung, Bauteilfunktion, E-Nummer, Bauteilwert, Beschreibung, Packageinformationen, Verweis auf Datenblätter und Rückverweis auf Schemadatei werden automatisch exportiert. Diese Funktion lässt sich auf gesamte Schemas oder Teile anwenden.

Auswahl aus automatisch generierten Bauteil-Kennwert-Listen
: Die Bauteiltypen werden in die FMEA automatisch in Form von Auswahllisten eingetragen. Abhängig vom Detailgrad der Unterscheidung zwischen verschiedenen Bauteiltypen und der Spiegelung dieses Detailgrads in der Bauteil-Kennwerte-Datenbank, sind die Auswahllisten aufgrund der erhöhten Trefferwahrscheinlichkeit der textbasierten Vergleiche kürzer und bestehen im Idealfall nur aus einem Eintrag.

Automatisches Übertragen der Basis-Fehleraufteilungsraten
: Abhängig von der Auswahl des Bauteil-Typs, werden die Basisfehlerraten übernommen. Alternativ zu Einzelwerten können in der Kennwertdatenbank auch Formeln in Abhängigkeit der Temperatur hinterlegt sein.

Manuelles Überarbeiten der FMEA
: Das manuelle Übertragen von Spezialbauteilen und spezieller Fehleraufteilungsraten ist möglich und bleibt von weiteren automatischen Schritten unbeeinflusst.

Kontrolle durch zweite, qualifizierte Person
: Der Arbeitsaufwand in diesem Schritt sollte erheblich vermindert werden, da nur bei manuellen Änderungen der vorausgefüllten Werte eine Kontrolle notwendig ist. Da diese manuellen Eingriffe gekennzeichnet werden müssen, ist es für eine zweite Person einfach, sich auf diese

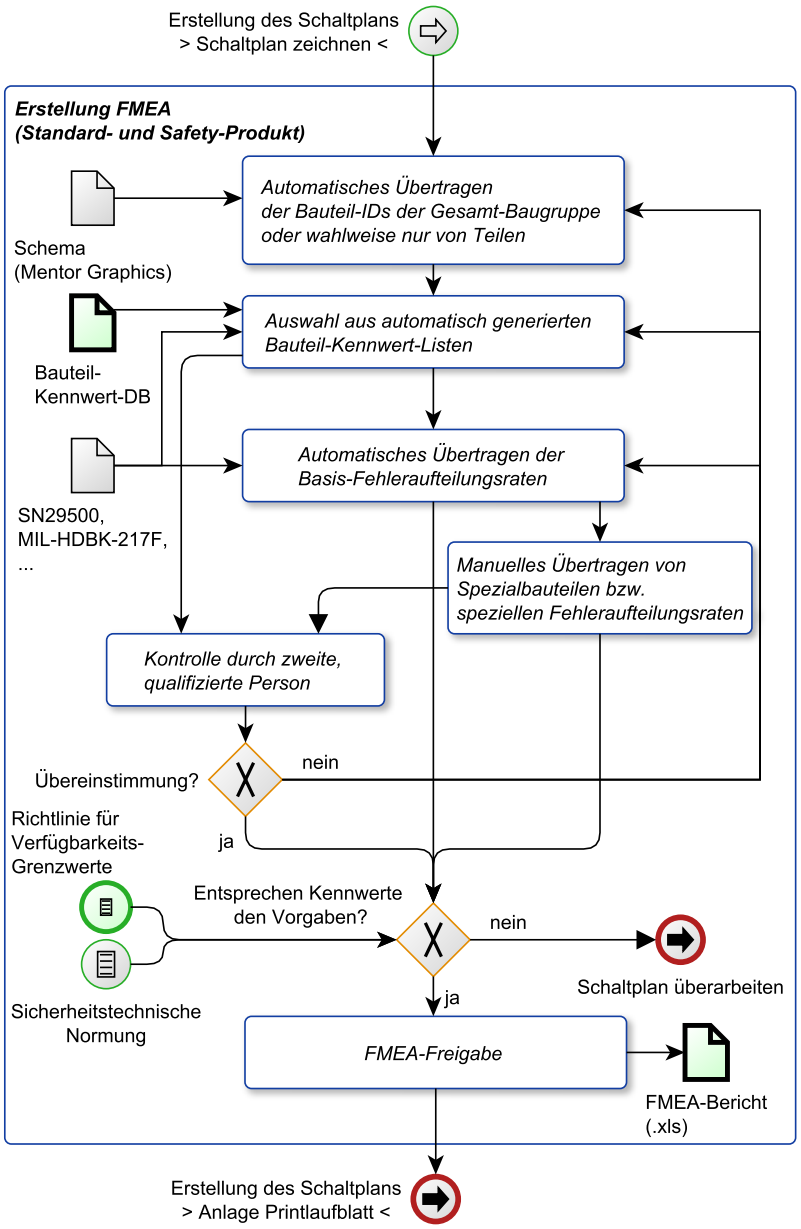


Abbildung 7.6.: Computerunterstützte Erstellung einer FMEA

Werte zu konzentrieren.
ANMERKUNG: *Der verbleibende Aufwand ist direkt verbunden mit der Qualität der Bauteil-Kennwerte-Datenbank.*

Übereinstimmung?
Die Kontrolle muss eine Übereinstimmung ergeben, ansonsten muss der kontrollierte Schritt wiederholt werden.
ANMERKUNG: *Methode bleibt unverändert.*

Entsprechen Kennwerte den Vorgaben?
Als Freigabevoraussetzung für Baugruppen außerhalb der Sicherheitstechnik wird die *Richtlinie für Verfügbarkeitsgrenzwerte* als Maßstab herangezogen. Die Erreichung der *sicherheitstechnischen Grenzwerte* aus den zugrunde liegenden *Normen* ist Basis für eine *sicherheitstechnische FMEA-Freigabe*. Fällt die Prüfung negativ aus, muss der Schaltplan überarbeitet werden und der gesamte FMEA-Vorgang beginnt von vorne.

FMEA-Freigabe
Die Freigabe erfolgt durch Kontrolle des positiven Abschlusses aller Teilprozesse und bei sicherheitstechnischen Abnahmen zusätzlich durch die schriftliche Bestätigung der zweiten Fachperson über die Kontrolle der FMEA im Detail. Das Ergebnis des Prozesses ist der freigegebene FMEA-Bericht.

Gegenüber dem manuellen Zugang sind aus Prozess-Sicht folgende Vorteile wirksam:

Wiederholbarkeit Das Prediktions-Tool wird entwickelt, um den Entwickler bei der monotonen und zeitraubenden Arbeit zur Erstellung einer Bauteil-FMEA bestmöglich zu unterstützen. Die vorliegende Erstversion ermöglicht auf Knopfdruck, gesamte Schaltplan-Designs oder wahlweise nur Teile eines Schaltplans in eine FMEA zu übernehmen. Auch Änderungen im Schaltplan bedeuten keine Wiederholung des zeitraubenden manuellen Verfahrens.
Dieser einfache Zugang macht es möglich, dass mit dem Werkzeug "gespielt" wird. Damit ist gemeint, dass die mehrfache Berechnung von Schaltungsvarianten oder Optimierungen auf Bauteilebene keinen Zusatzaufwand bedeuten und somit jederzeit durchgeführt werden können.

Reduktion des Zeitaufwands Durch die Einführung der geschilderten Methode wird eine generelle Reduktion des Zeitaufwands bei der Erstellung von FMEAs aus der Hardware-Entwicklungsabteilung erwartet. Neben diesem, vor genereller Einführung des neuen Prozesses noch nicht nachweisbaren Effekt, ist ein verminderter Grad der notwendigen Kontrolle bereits aus dem Prozessablauf sichtbar. Im Gegensatz zur ursprünglichen Vorgehensweise wird die Notwendigkeit zur *Kontrolle durch eine zweite qualifizierte Person* deutlich reduziert. Dabei wird einerseits die Überlegenheit des

Computers bei der Durchführung monotoner Arbeiten ausgenutzt und andererseits darauf vertraut, dass dieser, im Gegensatz zum Mensch, keine zufälligen Fehler produziert.
ANMERKUNG: *Der Nachweis der korrekten Funktion des Prediktions-Tools, welcher im Zuge der Funktionsprüfung in Kapitel 8.4 auf Seite 156 erbracht wird, ist sowohl für die Anwendung im Standard-Bereich als auch in der Sicherheitstechnik ausreichend. Der resultierende FMEA-Bericht beinhaltet alle Informationen die auch in einem manuellen Bericht zur Prüfung als für ausreichend befunden werden.*

Abnehmende Fehlerwahrscheinlichkeit Der erhöhte Automatisierungsgrad bei der Übertragung hunderter Werte aus verschiedenen Quellen führt bei geeigneter Verifikation des Werkzeugs zwangsläufig zu niedrigeren Fehlerquoten.
ANMERKUNG: *Diese Reduktion wird in der Praxis nicht unbedingt augenscheinlich werden. Da eine Bauteil-FMEA aus hunderten Zeilen und tausenden Werten bestehen kann, wird diese im Normalfall nur stichprobenartig geprüft. Werden dabei keine Fehler entdeckt und entspricht das Ergebnis in etwa der Erwartungshaltung, gilt die FMEA im Gesamten als korrekt. Daraus folgt direkt der nächste Vorteil:*

Erhöhung der Genauigkeit des Ergebnisses Geringere Fehlerquote bedingt die Erhöhung der Ergebnis-Genauigkeit.

Verbesserung der Qualität Bei Anwendung der qualitätsorientierten Methode mit dem Ziel der Optimierung hinsichtlich Zuverlässigkeit bei ausgewogener Wirtschaftlichkeit, erhöht sich die Qualität des einzelnen Produkts. Das Prediktions-Tool ermöglicht einen einfachen Zugang zu dieser Methode, ohne erheblichen Mehraufwand.

Um diese Verbesserungen zu erreichen, sind die folgenden Prozessanforderungen zu erfüllen:

PR 15 Richtlinie für Verfügbarkeitsgrenzwerte von Komponenten, Produkten und Produktgruppen definieren
Die Definition von sinnvollen Grenzwerten für Produktgruppen und Komponenten ist ein auf Erfahrung basierender Prozess (*best practice*). Aus den Anforderungen der Anwendungsgebiete, den internen Garantieanforderungen und wirtschaftlichen Betrachtungen müssen verschiedene Qualitätsstufen definiert werden. Sinnvoller Weise werden hier einige (wenige) Qualitätsstufen vorgegeben und mit konkreten Anwendungsgebieten gekoppelt. Beispielsweise spannen die Kategorien *Standardbaugruppe im Maschinenbau* und *Sicherheitstechnik in Offshore-Energieanlagen* den Bogen von verhältnismäßig niedrigen zu sehr hohen Anforderungen.

Bei Anwendungsgebieten wo zwischen Gesamt-Kennwerten und anwendungsspezifischen Kennwerten unterschieden wird, wie in der Sicherheitstechnik, wird empfohlen die Kennwerte sowohl für den einzelnen Kanal als auch für die Baugruppe im Gesamten festzulegen. Dadurch wird vermieden, dass Baugruppen entwickelt werden, welche zwar fokussiert auf den einzelnen Anwendungsfall (=Kanal) sehr hohen Ansprüchen genügen, aber durch ausufernde Komplexität eine sehr hohe Austauschfrequenz und somit subjektiv schlechte Qualität vermitteln.
ANMERKUNG: *Bei den Vorgaben und Anforderungsdefinitionen hinsichtlich Zuverlässigkeit wurden Defizite festgestellt (siehe Kapitel 4.2 auf Seite 62).*

PR 16 Schulung zur Zuverlässigkeitstheorie
Hardware-Entwickler sollten die grundlegenden Begriffe und Kennwerte kennen und unterscheiden können. Die Anwendung des Prediktionstools und die Interpretation interner Statistiken wie Produktionsausfall oder Reparaturrückläufer können nur korrekt erfolgen wenn die Theorie dahinter klar ist und auf intern festgelegte Grenzwerte vertraut werden kann. Gleiches gilt für Entwicklungs-Vorgaben wie geforderte MTTF-Werte oder zu erreichende Garantiezeiten.

PR 17 Design Reviews
Viele der vorgestellten Maßnahmen basieren auf Erfahrung. Ein lebendiger Erfahrungsaustausch ermöglicht erst den Aufbau einer *Wissensdatenbank für Produkte und Komponenten*. Design Reviews bieten die Möglichkeit der Weitergabe von Erfahrungen und des Mentoring neuer Mitarbeiter. Ziel dieser Reviews soll sein, dass jeder Entwickler die präferierten Grundschaltungen und Komponenten kennt. Dazu gehört auch, dass Entscheidungen auf Schaltungsebene nachvollziehbar und somit in eigenen Schaltungen wiederholbar sind.

PR 18 Richtlinie zur Erstellung einer FMEA
Basierend auf der vorliegenden Arbeit soll eine sinnvolle und praxisorientierte Vorgehensweise definiert werden. Das Hauptaugenmerk soll auf *Einfachheit* und *Ergebnisorientierung* gelegt werden. Die Einbindung der *Bauteil-Kennwert-Datenbank* und der *Wissensdatenbank für Komponenten und Produkte* muss berücksichtigt werden.

PR 19 Detaillierte Einträge in Bauteil-Kennwert-Datenbank
Je detaillierter die Kennwert-Datenbank vorliegt, desto genauer kann das Prediktions-Werkzeug die aus dem Schema extrahierten Typen zuordnen und die entsprechenden Fehlerraten in die FMEA übertragen. Der Aufwand zur Erstellung einer qualitativ hochstehenden Datenbank ist erheblich, jedoch muss der *einmalige Aufwand* für eine

Fachperson zum Eintragen eines Bauteils dem Aufwand gegenübergestellt werden, der auf der Basis einer ungenauen Datenbank entsteht. Dabei müsste bei *jeder* FMEA der Entwickler zuerst die Bauteile aus den Auswahllisten aussuchen und da dieser Schritt manuell erfolgt, das Ergebnis von einer zweiten Person überprüft werden.

7.1.5. Auswertung der Reparatur- und Rückläufer-Statistik

Die statistische Erfassung und Bewertung ausgefallener Produkte bildet die wichtigste analytische Meßmethode nach Abschluss einer Produkt-Entwicklung. Produktionsausfälle, Ausfälle während produktionsbegleitender Tests und im Run-In können dabei zu hundert Prozent erfasst und ausgewertet werden. Felddaten sind hingegen höchst unzuverlässig. Abhängig von der Art des Produkts, von der Art der Lieferbeziehung und der Austauschmentalität des Kunden, wird nur ein unbekannter Teil der tatsächlich ausgefallenen Produkte beim Hersteller erfasst. Bei diesen erfassbaren Rückläufern erschweren die unbekannte Einsatzdauer und unbekannte Umgebungsbedingungen während des Einsatz die exakte Zuordnung und Interpretation des Ausfalls.

Problematisch ist dies, da die Reparatur- und Rückläuferstatistik wichtige Basis für Anpassungsvorschläge von Zuverlässigkeitsgrenzen und Auslöser für Produktrevisionen ist. Die Qualitätsbeauftragten reagieren auf statistische Auffälligkeiten im Extremfall mit der Sperre von Bauteilen oder mit Auslieferspersperren von Produkten.

Die Früherkennung von möglichen Problemen hilft, Serienprobleme und daraus entstehende Direkt- und Folgekosten minimal zu halten. Dazu ist es notwendig, die Statistiken möglichst genau zu erfassen und detailliert auszuwerten. Die statistischen Basisdaten sind dabei umso aussagekräftiger je genauer die Untersuchung und daraus folgende Problemberichterstellung eines jeden Rückläufers erfolgt.

Die nachfolgenden Maßnahmen erhöhen die Aussagekraft der Rückläufer- und Reparaturstatistik:

PR 20 Reparatur-Rückläufer: Einfache Einsatzzeit-Erfassung
Reparatur-Eingangsdatum erfassen damit Zeitspanne zwischen Verlassen der Produktionsstätte und Reparatureingang möglichst exakt vorliegt. Das Verlassen der Produktionsstätte kann mittels Seriennummer basierten Ausgangstabellen erfasst werden.
ANMERKUNG: *Diese rudimentäre Maßnahme sollte rasch durch eine höherwertige Einsatzzeit-Erfassung, wie beispielsweise im nachfolgenden Absatz beschrieben, abgelöst werden.*

PR 21 Reparatur-Rückläufer: Genaue Einsatzzeit-Erfassung
Genaue statistische Erfassung der Einsatzzeit. Idealerweise mit Datum und Uhrzeit verknüpft, als Basis auch mittlere Zeit im Betriebszustand und Gesamtbetriebszeit ausreichend. Dazu ist eine Adaption der Hardware notwendig (siehe dazu die Requirements zur *Hochwertigen Auswertung* auf der nächsten Seite).
ANMERKUNG: *"Einfache Einsatzzeit-Erfassung"wird dadurch ersetzt.*

PR 22 Reparatur-Rückläufer: Austausch kritischer Komponenten/Bauteile
Die Rückläufer-Statistik eines Produkts soll sich immer auf den gleichen Produktstand in Software und Hardware beziehen. Damit wird es notwendig, nach dem (angeordneten) Austausch kritischer Bauelemente oder Komponenten, eigene Seriennummernkreise oder Produktcodes zu vergeben. Dies gilt ebenfalls bei Abkündigung oder Redesign von Komponenten und Bauelementen.

PR 23 Austausch kritischer Bauelemente: Hinweispflicht der Entwicklung
Für Produktion und Bauteilbeschaffung ist die Kennzeichnung von kritischen Bauelementen in Bezug auf bestimmte Produkte Grundvoraussetzung zur entsprechenden Beachtung bei wirtschaftlich oder technisch motiviertem Austausch für die Serienproduktion. Diese Information muss bei der Produktionsüberleitung von der Entwicklungsabteilung schriftlich an die Produktion/Bauteilbeschaffung weitergegeben werden.

PR 24 Reparatur-Rückläufer: Kundenspezifische Auswertung
Die Praxis zeigt, dass in Europa defekte Geräte eher retourniert werden als in Asien. Weiters wird teilweise kundenseitig eine Fehlersuche zur Eingrenzung auf einzelne Produkte durchgeführt, welche dann statt einem gesamten als defekt gekennzeichneten Baugruppenträger rückgeliefert werden. Die Rückliefermentalität hängt auch stark von der Wertigkeit des Produkts ab. Einfache und somit billigere Produkte wie digitale E/A-Karten werden eher direkt verschrottet als teure Produkte wie CPUs.
Diese und noch weitere Faktoren ändern die Gewichtung und verfälschen Auswertungen auf genereller Basis. Versuchsweise sollte eine kundenspezifische Auswertung der Rückläufer einer Gesamtauswertung auf Produktbasis gegenübergestellt werden um den tatsächlichen Einfluss nachvollziehbar zu machen.

PR 25 Reparatur-Rückläufer: Kunden zur Datenlieferung animieren
In Lieferverträgen und bei Kundenkontakten sollen diese zur Rücklieferung von defekten Geräten oder zumindest zur Rückmeldung von Defekten animiert werden.
ANMERKUNG: *Diese Maßnahme ist vor Einführung nochmals gesondert zu überprüfen. Es muss betrachtet werden, ob der Informationsgewinn*

die zu erwartenden Zusatzkosten und die erhöhte Aufmerksamkeit des Kunden auf Defekte aufwiegt.

PR 26 Hochwertige Auswertung - Temperatur-Erfassung

Die maximale Betriebstemperatur eines Produkts und spezifischer Bauelemente ist die kritischste Ursache der Lebensdauerverkürzung. Deshalb ist es sinnvoll die Betriebstemperatur und die korrespondierende Umgebungstemperatur feingranular aufzuzeichnen. *Minimum:* Einbau von Sensoren zur Erfassung der minimalen und maximalen Betriebstemperatur (Einzelpunkte, sowie Zähler zur Erfassung der Anzahl der Überschreitungen) in ausgewählten Baugruppen. Auswertung von integrierten Temperaturüberwachungseinrichtungen hochwertiger und hoch belasteter Bauelemente (CPUs, ASICs, Speicher, Leistungstransistoren, ...).
Idealfall: Genereller Einbau von Sensoren zur Erfassung der minimalen und maximalen Betriebstemperatur über den gesamten Einsatzzeitraum (z.B. Min und Max pro Tag).
ANMERKUNG: *Dabei ist zu vorzusehen, dass diese Werte auch mittels Fernzugriff abrufbar sind. Die Werte sollten vor Manipulation geschützt werden um unverfälschtes Datenmaterial bei der Abhandlung von Garantieansprüchen vorliegen zu haben.*

PR 27 Hochwertige Auswertung - Zusatz-Sensorik

Zeiterfassungen des Nutzerverhaltens geben Aufschluss über den genauen Erstinbetriebnahme-Zeitpunkt, über Betriebszeiten und die tatsächlich anfallenden Betriebsstunden über die Lebensdauer. Diese Daten müssen in einem remanenten Speicherbereich gesammelt werden, welcher auch nach einem Defekt mit hoher Wahrscheinlichkeit und möglichst mit einfachen Mitteln (vor Ort) auslesbar ist.
ANMERKUNG: *Weitere Informationen die in diesem Zusammenhang interessant wären, sind von der Qualitäts-Stabstelle gemeinsam mit der Hardware Entwicklungsabteilung zu definieren. Die Erfassung der Anzahl regulärer und durch Fehler forcierter Einschaltvorgänge wären ein weiteres Beispiel.*

PR 28 Gegenüberstellung Theorie - Praxis

Die Gegenüberstellung der im Zuge der Produkt-Entwicklung und Produktionseinführung generierten Voraussage-Werten mit den Praxiswerte aus der Reparatur-Rückläuferstatistik, ist Basis für weitere Qualitätslenkungsmaßnahmen. Abweichungen können erfasst und in zukünftigen Baugruppen oder bei der Bauteilauswahl berücksichtigt werden. Fehlannahmen fließen in die Wissensdatenbank ein und grobe Abweichungen von Herstellerangaben können Basis für Garantieforderungen sein. Weiters kann aus diesem Zusammenhang die Ersatzteilhaltung optimiert werden.

ANMERKUNG: *Diese Maßnahme setzt die Einführung hochwertiger Qualifizierungsmaßnahmen voraus. Diese können auf Bauteil-, Komponenten und Produktebene, wie am Ende von Kapitel 7.1.2 auf Seite 114 angedeutet, angewendet werden. Die Berechnungswerte auf Basis der Parts-Count-Methode werden als nicht hinreichend betrachtet, ein höherwertiges Berechnungsmodell sollte allerdings angestrebt werden. Lebensendtests und beschleunigte Alterungstests sind zusätzlich anzustreben.*

Im Zuge dieser Arbeit wurde auf Basis bestehender Rückläufer-Statistiken versucht, Qualitätskennwerte mathematisch exakt abzuleiten (siehe dazu Kapitel 5.1.2 auf Seite 82 ff.). Überraschender Weise ist diese mathematische Darstellung weit weniger eindeutig und theoretisch untermauert, wie dies zu erwarten wäre und lässt dadurch viel Spielraum für Interpretationen. Nichts desto trotz sollte die Einführung einer nachvollziehbaren und mathematisch fundierten Auswertung der Ausfälle im Feld eines der nachdringlichst verfolgten Ziele sein. Gerade die unvollständigen Datensätze ergeben bei vereinfachter Betrachtung verfälschte Aussagen. Das kann dazu führen, dass erhöhte Garantieleistungen zu erbringen sind, aber auch, dass die Produkte "overengineered" werden und somit im preislichen Konkurrenzkampf Probleme bekommen. Die Bewertungen an dieser Stelle haben somit einen hohen Einfluss auf die Wirtschaftlichkeitsbetrachtungen von Projekten und Produkten.

7.2. Zuverlässigkeitsorientierte Schaltungsentwicklung

In diesem Abschnitt soll auf Basis der erfolgten Bestandsaufnahme und Adaptierung der Prozesslandschaft die Methode der *zuverlässigkeitsorientierten Schaltungsentwicklung* genauer betrachtet werden.

Neu zu entwickelnde elektronische Produkte beinhalten üblicherweise verschiedenste Funktionsgruppen die nicht jedesmal neu designt werden müssen. Dies betrifft beispielsweise die Spannungsversorgung, Kommunikationsschnittstellen und ähnliche Teile, welche idealerweise als "best practice" Funktionskomponenten zum Import ins Design-Werkzeug zur Verfügung stehen. Baugruppenspezifische Funktionen werden hingegen neu entwickelt und sollten daher ein Maximum an Aufmerksamkeit des Entwicklers bekommen.

Diese Vorgehensweise hat zwei direkte Auswirkungen auf die Qualität der Baugruppen. Die Verwendung der "best practice" Komponenten garantiert dem Entwickler *maximale Zuverlässigkeit* bei *idealer Abstimmung auf das Einsatzgebiet* und *minimalem Zeitaufwand* zur Integration.

Dies macht eine *zeitliche und fachliche Konzentration* auf die *neuen und funktionsbestimmenden Teile* des Produktes möglich, was sich wiederum in einer erhöhten Qualität niederschlagen sollte.

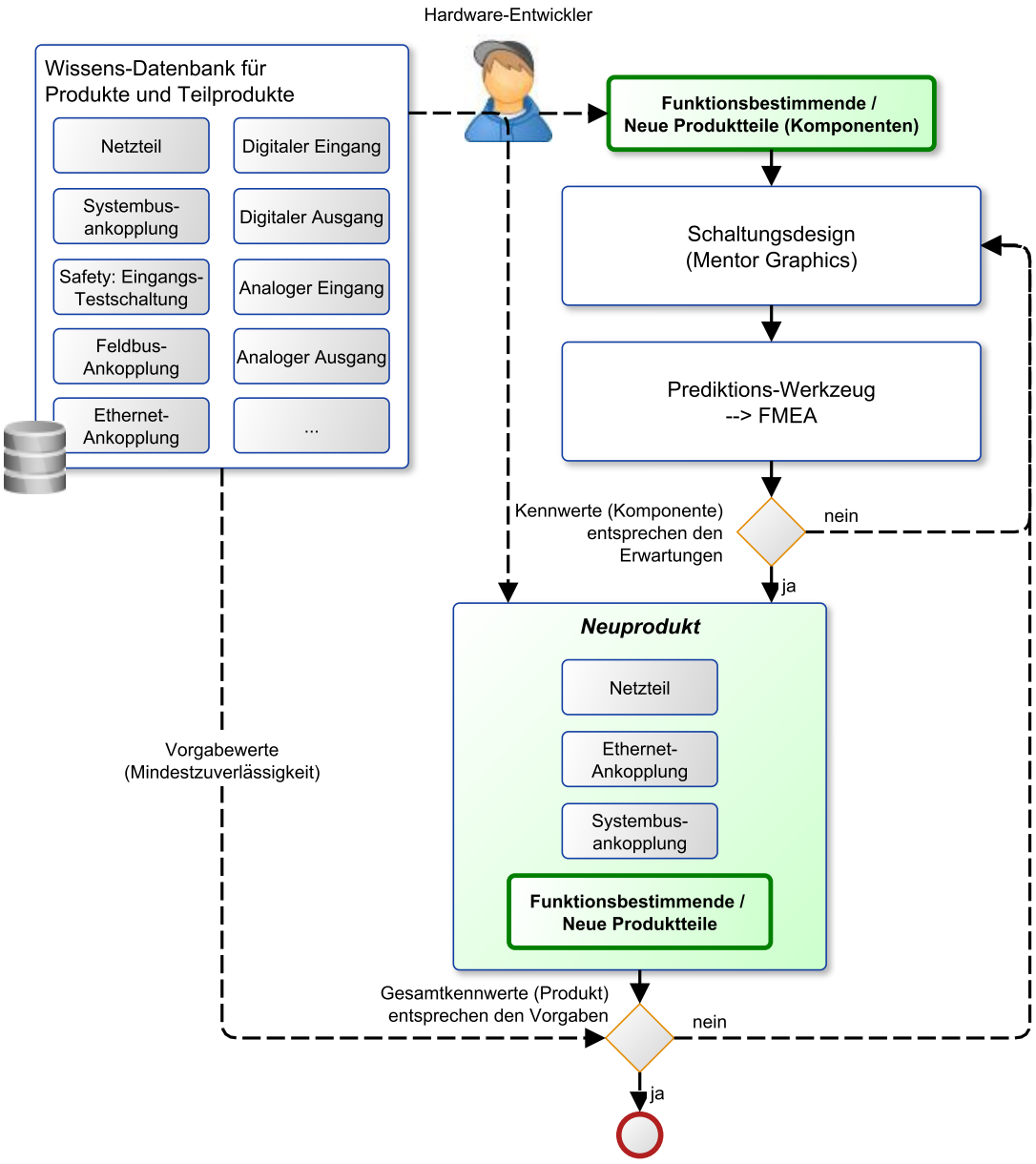


Abbildung 7.7.: Zuverlässigkeitsorientierte Schaltungsentwicklung

Wie in Abbildung 7.7 dargestellt, ist dabei die Grundidee sehr einfach. Der mit einem Auftrag zur Neuentwicklung oder Adaption eines Produkts betraute Hardware-Entwickler greift zum großen Teil auf bestehendes Wissen, eingeführte Methoden und Werkzeuge zurück.

Im Einzelnen sieht die Vorgangsweise für Produkte folgendermaßen aus:

Rohentwurf und Komponenten-Auswahl aus Wissens-Datenbank

Auf Basis eines in Funktionsblöcke aufgeteilten Schemaentwurfs und den Vorgaben hinsichtlich Einsatzgebiet und spezifischen Qualitätsanforderungen, werden passende Bestandskomponenten aus der Wissensdatenbank ausgesucht. Durch einfache Subtraktion der hinterlegten Ausfallsrate λ jeder einzelnen Bestandskomponente vom vorgegebenen Grenzwert der Gesamtausfallrate für das Neuprodukt, wird der minimal zu erreichende Grenzwert für die Neukomponente(n) festgelegt.

Schaltungsentwurf neuer Komponenten

Die Entwicklung der neuen Teile soll sich aus einem Top-Down Ansatz iterativ der optimalen Lösung hinsichtlich Funktion, Qualität und Preis annähern. Dazu ist das mehrfache Durchlaufen der Schleife *Schaltungsentwurf*, *Kennwertgenerierung* und *Kontrolle* vorgesehen:

Zuverlässigkeitskennwert-Bestimmung der Neukomponenten

Unter Anwendung des Prediktions-Werkzeugs soll in unterschiedlichen Stadien der Entwicklung die resultierende Ausfallsrate auf Basis der getroffenen Bauteilauswahl kontrolliert werden. Die Anwendung der *Parts-Count Methode* ist dabei nicht auf vollständige Schaltungsteile begrenzt. Die Auswertung kann auf nicht schaltungstechnisch verbundene Bauteile angewendet werden, womit eine einfache Kontrolle der Bauteilauswahl zum frühest möglichen Zeitraum wirksam wird.

***Safety:* Manuelle Anpassung der Fehleraufteilungsrate**

Anpassung der tatsächlichen Fehleraufteilung bei Abweichungen vom Standardmodell.

***Safety:* Manuelle Anpassung des Diagnose-Deckungsgrades**

Anpassung des entsprechenden Kennwerts (*DC*) im sicherheitstechnischen Teil der automatisch generierten FMEA.

Entwurf entspricht Vorgaben und Vorstellungen?

Wiederkehrende Kontrolle der Komponentenkennwerte durch Entwickler.

***Optional:* Optimierung und Varianten**

Die tabellarische Auflistung der Bauteile und deren Kennwerte, sowie die Möglichkeit zur Auswertung von Komponenten-Teilen, ermöglicht eien zielgerichtete Bestimmung maßgeblich am Gesamtergebnis beteiligter Teilkomponenten und Bauelemente. Damit wird sichergestellt, dass Optimierungsschritte hinsichtlich Zuverlässigkeit und Qualität nicht an falschen Bauelementen und Komponenten durchgeführt werden.

Die Optimierung kann auch durch Variation von Bauelementen oder Schaltungsteilen durchgeführt werden, was positive Auswirkungen auf Funktion oder Preis haben kann. Bei genügend Spielraum hinsichtlich zu erreichendem Qualitäts-Grenzwert, sind da-

durch resultierende Abschläge ausdrücklich erlaubt.

Berechnung der Gesamtzuverlässigkeit

Probe: Der Gesamtkennwert sollte bei korrekter Eingangsberechnung und Einhaltung der Grenzwerte nicht über dem Vorgabewert liegen. Grobe positive Abweichungen sollten dokumentiert werden und hinsichtlich Wirtschaftlichkeit überprüft werden. Nicht erreichte Vorgabeziele bedürfen einer gesonderten Genehmigung.

Die mit dem Präfix *Safety* gekennzeichneten Schritte sind für sicherheitsgerichtete Entwicklungen verpflichtend anzuwenden. Für Standard-Baugruppen kann darauf verzichtet werden.

Die beschriebene Methode basiert auf einem hohen Vertrauensgrad zu den Komponenten und deren Zuverlässigkeitskennwerten aus der entsprechenden Wissens-Datenbank. Daraus lassen sich folgende Anforderungen an die Einträge ableiten:

PR 29 Erhöhte Anforderungen an gemeinsame Komponenten definieren und umsetzen

Gemeinsame Funktionen müssen grundsätzlich höheren Qualitätskriterien genügen, als die individuell entwickelten Funktionen und Komponenten. Hinsichtlich der Verfügbarkeit bedeutet dies, dass gemeinsame Teile möglichst wenig Anteil an den Gesamtausfallsraten haben sollten. Dies gilt insbesondere für die verwendeten Bauteile. Deshalb ist es sinnvoll, in diese Funktionseinheiten entsprechend viel Zeit zur Optimierung zu investieren.

ANMERKUNG: *Eine gleichzeitige Optimierung der gegeneinander wirksamen Eigenschaften Qualität, Funktion und Preis ist nahezu unmöglich und meist wenig sinnvoll. Daher scheint eine Einteilung in Kategorien, wie im Unterabschnitt auf Seite 134 dargestellt, sinnvoll.*

PR 30 Reparatur-Rückläufer: Besondere Beobachtung gemeinsamer Komponenten

Gemeinsame Funktionseinheiten sind bei Rückläuferstatistiken gesondert zu betrachten. Die Anwendung aufwändiger und teurer Tests, die für Einzelbaugruppen nicht rentabel scheinen, sind auf gemeinsamen Funktionseinheiten genau abzuwägen. Hierbei ist immer zu berücksichtigen, dass jede Veränderung der Kennwerte sich auf die Ausfallsraten vieler Baugruppen auswirkt und sowohl Fehler als auch Verbesserungen entsprechend große Tragweite besitzen.

Der gesamte Prozess um die Schaltungsentwicklung ist darauf ausgerichtet, möglichst rasch die vorgegebenen Ziele hinsichtlich *spezifischer Funktionseigenschaften*, *Wirtschaftlichkeit* und aus dem Anwendungsgebiet definierter *Zuverlässigkeitseigenschaften* zu erreichen. In einem Pool von optimal abgestimmten Basiskomponenten sind im Laufe der Zeit immer mehr funktionale Einheiten in

verschiedenen Preisklassen und zu unterschiedlichen Qualitätsstufen abrufbar. Neu entwickelte Teile hingegen können und dürfen, entgegen genereller Qualitätsrichtlinien, schlechtere Eigenschaften aufweisen, sofern dies im Wissen um die Konsequenzen geschieht.

Spezielle Funktionen oder Anwendungen in Grenzbereichen werden oft nur dadurch ermöglicht, dass in anderen Bereichen Abschläge in Kauf genommen werden. Beispielsweise sind Produkte, welche auf Betriebs-Temperaturen von mehr als 60 °C ausgelegt werden, preislich nur dann sinnvoll zu entwickeln, wenn Abschläge in der Lebensdauer in Kauf genommen werden.

PR 31 Bauteilauswahl: Derating als Vorgabe

Aufgrund der standardmäßig sehr hohen, zulässigen Betriebstemperatur von 60 °C gilt es, Bauelemente mit höchstmöglicher Temperaturverträglichkeit bei akzeptablem Preis auszuwählen. Die Temperaturabhängigkeit muss zumindest als sehr wichtiges Maß bei der Einführung eines neuen Bauteils berücksichtigt werden. Bei gleichem Preis und vergleichbaren Eigenschaften ist immer das Bauteil mit besseren Temperatureigenschaften zu wählen.

PR 32 Kühlkonzept optimieren

Um die Komponenten und einzelnen Bauelemente nahe an der Umgebungstemperatur zu halten, sind weitere Maßnahmen bei kritischen Baugruppen zu treffen. Simulationen der Temperaturverteilung helfen schon im Stadium des Schaltungsentwurfs, Hotspots aufzudecken. Mit Hilfe des Prediktionswerkzeugs können auf Basis der temperaturabhängigen Ausfallskennwerte und der Übertragung der simulierten Temperaturzonen in den Schaltungsentwurf, die Auswirkungen auf die Lebensdauer des Produkts sehr einfach sichtbar gemacht werden. Das Ziel ist bei dieser Optimierung, die Hochtemperaturzonen strategisch so zu platzieren, dass

1. größere Zonen kleiner Temperaturerhöhung gegenüber kleinen Zonen großer Temperaturdifferenz zu bevorzugen sind.
2. kritische Bauelemente hinsichtlich temperaturbeschleunigter Alterung (z.B. Elkos), möglichst außerhalb dieser Zonen liegen.

PR 33 Alarmierung/Abschaltung bei Übertemperatur

Einführung einer schaltungstechnischen Maßnahme zur Sensibilisierung der Anwender und Verhinderung von lebensverkürzenden Vorschädigungen durch Übertemperaturen. Dabei wird die Maßnahme zur *Hochwertigen Temperatur-Erfassung* auf Seite 128 mit einer Warn- bzw. Ausschaltautomatik verbunden. Die Aktivierung der automatischen Abschaltung muss konfigurierbar sein, da diese nicht in jeder Applikation zulässig ist.

Wissens- und Kennwert-Datenbank für Komponenten und Produkte

Tabelle 7.2 soll die Idee der qualitäts- und kostenbezogenen Wissensdatenbank verdeutlichen. Für jede (wichtige) Funktionskomponente und/oder jedes Produkt sind Referenz-Designs als importierbare Schemas hinterlegt. Diese sind beispielsweise nach den dargestellten Kategorien, einmal nach wirtschaftlicher und einmal nach qualitätsorientierter Erfüllung, eingeordnet. Die Designs werden mit Beschreibung und Kennwert-Berechnung (FMEA) hinterlegt, um einen hohen Grad der Nachvollziehbarkeit zu garantieren und die Unterlagen auch als Vergleichsreferenzen heranziehen zu können.

Bezeichnung	***preisoptimiert***	***Standard***	***teuer***
qualitätsoptimiert	Billig & Gut	Gut	Teuer & Gut
Standard	Billig	Standard	Teuer
niedrige Qualität	Billig & Schlecht	Schlecht	Teuer & Schlecht
Schaltnetzteil	***preisoptimiert***	***Standard***	***teuer***
qualitätsoptimiert	`Schaltung_V4.1`	-	-
Standard	`Schaltung_V1.9`	-	`Schaltung_V1.3`
niedrigeQualität	-	-	`Schaltung_V0.6`

Tabelle 7.2.: Matrixeinteilung verschiedener Schaltungs-Designs von Komponenten und Teilprodukten mit beispielhaften Einteilungskategorien.

Diese Wissensdatenbank soll möglichst lebendig gestaltet werden. Wie in der Tabelle im unteren Bereich durch die Versionsnummern angedeutet, ist die Entwicklung von weniger gut nach gut auch ein evolutionärer Vorgang, der durch jede neue Schaltungsentwicklung wieder angestoßen wird. Beispielsweise soll es möglich sein, dass ein Entwickler die Aufnahme eines Designs als Referenz beantragt, worauf eine Kommission über die Aufnahme und die Kategorie bestimmt.

Aus wirtschaftlicher Sicht hat diese Design-Sammlung einen weiteren, sehr hohen Stellenwert. Bei einer sukzessiv größer und besser werdenden Datenbasis kann immer öfter, vor allem bei Standard-Komponenten, auf die Datenbank zurückgegriffen werden. Der Entwickler konzentriert dadurch sein Wissen und seine Energie auf die spezifische Funktionserfüllung des neu zu entwickelnden Produkts und darf darauf vertrauen, dass “Standard-Komponenten” aus wirtschaftlicher und qualitativer Sicht optimal sind.

Praktische Umsetzung

Die geschilderten Prozessanpassungen und Anforderungen an eine zuverlässigkeitszentrierte Entwicklung von Hardware-Komponenten sind mit erheblichem

Umsetzungsaufwand verbunden. Aus fachlicher Sicht sind sämtliche Einzelschritte sinnvoll, um ein optimales Ergebnis zu erzielen. Wirtschaftlich betrachtet, bedeutet die Vielzahl an Änderungen ein erhebliches Risiko.

Für die Umsetzung wird eine phasenweise Vorgehensweise vorgeschlagen:

Vorbereitung
: Training von Qualitätsspezialisten, Vorbereitung der formalen Voraussetzungen (Prozessdokumente, ...), Auswahl und Umsetzung der Kennwert- und Wissensdatenbank, Anpassungen und Tests des Werkzeugs.

Pilotphase
: Aufbauend auf ausgewählten Projekten, gemeinsam mit positiv motivierten Mitarbeitern wird transparent mit den Ergebnissen intern Marketing (lessons learned) für eine breite Anwendung betrieben.

Einführung
: Generelle Schulung zu den Prozessänderungen, zu den Grundlagen der Verfügbarkeitstheorie und zur konkreten Verwendung der Datenbanken und des Werkzeugs.

Wirksamkeitskontrolle
: Mit Retrospektiven und Reviews wird ein Regelkreis zu weiteren Anpassungen und Behebung von Problemen und Fehlerquellen geschaffen.

Im Mittelpunkt der Umsetzungstrategie soll stehen, dass am Ende die Entwicklungsmitarbeiter intrinsisch motiviert den angepassten Prozess und das Prediktionswerkzeug selbstverständlich einsetzen. Dies aus dem Bewusstsein, mit Hilfe der eingeführten Verbesserungen noch bessere Produkte realisieren zu können.

7.3. Zusammenfassung

Im vorliegenden Kapitel wurden die bestehenden Prozesse im *Lebenszyklus einer Produktes* analysiert und entsprechend einer *zuverlässigkeitsorientierten Schaltungsentwicklung* adaptiert.

Anpassungsvorschläge sind gemeinsam mit deren genauen Zielen im Detail vorgegeben worden. In eigenen Abschnitten sind die neu einzuführenden Konzepte der *zuverlässigkeitsorientierten Schaltungsentwicklung* und der *Wissens- und Kennwertdatenbank für Komponenten und Produkte* praxisnah beschrieben. Der Schwerpunkt wurde auf *praxisnahe Umsetzbarkeit* gelegt und nicht auf wissenschaftliche Vollständigkeit.

Die Anpassungen sind teils notwendige Voraussetzungen, teils fördernde Maßnahmen zur Sicherstellung der Unterstützung der am Prozess beteiligten Personen. Erst auf dieser Basis, im Gegensatz zu einem punktuellen Einsatz, wird das Prediktionswerkzeug die volle Wirkung entfalten können.

8. Umsetzung des Werkzeugs zur Zuverlässigkeitsberechnung

Ziel ist es, ein Prediktions-Werkzeug zu entwickeln, welches auf Basis der vorliegenden Theorie und eingebettet in die aktuelle Tool-Landschaft, den qualitätsorientierten Prozess unterstützt und möglichst sogar verbessert, ohne dabei als Hindernis im Entwicklungsalltag wahrgenommen zu werden.

Zur systematischen Umsetzung der zu programmierenden Teile, wird folgendermaßen vorgegangen:

1. *Sammlung und Bewertung der Anforderungen*
   Im Zuge dieser Arbeit, in Interviews mit Mitarbeitern und aufgrund gemachter Erfahrungen aus der Umsetzung der Sicherheitsbaugruppen liegen eine Reihe von Anforderungen, Funktionsbeschreibungen und Wünschen vor. In Unterkapitel 8.1 auf der nächsten Seite werden die für die erste Version des Programms relevanten Requirements ausgewählt.

2. *Studium des bestehenden Schaltplanerstellungstools*
   Die nahtlose Integration in das bestehende Schaltplanerstellungswerkzeug ist der Schlüssel zur Akzeptanz und einfachen Bedienbarkeit. Das Referenzhandbuch, die Schnittstellenbeschreibung, sowie Online-Ressourcen zum DxDesigner von Mentor Graphics dienen als Quelle zur Konzepterstellung.

3. *Auswahl einer geeigneten Berechnungsmethode*
   In Abschnitt 2.4.1 auf Seite 40 sind die standardisierten analytischen Ermittlungsverfahren vorgestellt. In Abschnitt 8.2 auf Seite 142 werden diese auf praktische Umsetzbarkeit in und für die vorliegende Anwendung überprüft. Kriterien sind dabei wiederum Bedienbarkeit, leichte Einbettung in den bestehenden Enwicklungsprozess, niedriger Schulungsaufwand und Überprüfbarkeit.

4. *Erstellung von Vorlagen*
   Das Prediktionswerkzeug verwendet unterschiedliche Eingangsdaten. Für die Berechnung am wichtigsten ist dabei die Kennwertdatenbank. In Ermangelung einer vorliegenden elektronischen Version, wird eine “Beispieldatenbank” (der Einfachheit halber als Excel-Tabelle ausgeführt) erstellt. Die Umsetzung erfolgt dabei nicht vollständig, sondern nur soweit, als für den Korrektheitsnachweis notwendig. Konkret werden die Basisdaten für

sämtliche Bauteile der Baugruppen NTv2 und SBv1 hinterlegt. Als Quelle dient die SN29500.
Neben den Kennwerttabellen sind auch mehrere Templates für Eingabe- und Ergebnisformulare umzusetzen.

5. *Umsetzung Interface-Skripts*
   Einbettung der Schnittstellen zur Verfügbarkeitsberechnung in das Schaltplanwerkzeug.

6. *Umsetzung der Berechnungsskripts*
   Das Berechnungsprogramm ist als eigenständiges Konsolenprojekt mit Schnittstellen zum Schaltplanwerkzeug realisiert.

7. *Prüfung auf Korrektheit*
   Zum Nachweis der korrekten Berechnung der Kennwerte wird mit der Referenzbaugruppe SBv1 und zusätzlich mit bestehenden Kennwerten von NTv2 verglichen (→ 8.4 auf Seite 156).

8. *Erstellung der Benutzerdokumentation*
   Zur einfacheren Einführung des Werkzeugs wird die Anwenderdokumentation nicht als Textdokument umgesetzt, sondern in Form kurzer Anwendungsfilme.

Am Ende dieses Kapitels sind neben der Beschreibung von nicht oder nicht vollständig umgesetzten Funktionen noch weitere Anregungen zur Erweiterung und Verbesserung des Werkzeugs angegeben (Abschn. 8.6 auf Seite 159).

ANMERKUNG: Im Zuge der Masterarbeit wurden nicht sämtliche Anforderungen, Wünsche und Berechnungsmethoden umgesetzt. Die konkrete Realisierung ist ein “Proof of Concept” und erfolgte mit *Fokus auf Korrektheit der Berechnungsergebnisse und Bedienbarkeit.*

8.1. Anwendungsszenarien, Anforderungen und Konfigurationsmanagement

8.1.1. Anwendungsszenario Standard

Der HW-Entwickler ist jederzeit in der Lage, direkt aus dem Schaltplan-Editor eine Berechnung anzustoßen. Er kann zwischen einer Gesamt- und einer Teilberechnung auswählen. Die Gesamtberechnung nimmt als Berechnungsgrundlage sämtliche Schaltungsteile des aktuell in Bearbeitung befindlichen Projekts, auch über mehrere Dateien bzw. “Blätter” verteilt. Die Teilberechnung erfordert eine Selektion der Schaltungsteile vor der Berechnungsauslösung. Im Anschluss erfolgt der Export sämtlicher ausgewählter Bauelementdaten des Gesamtschaltplans nach Excel zur weiteren Auswertung.

In Excel werden diverse Daten und Statistiken zum in Bearbeitung befindlichen Projekt und zum Extraktionsablauf aus dem Schaltplanprogramm zur Prüfung zur Verfügung gestellt.

Eine Stücklistenübersicht ermöglicht die Aktivierung/Deaktivierung von Bauelementen um wiederum Teilberechnungen zu ermöglichen bzw. optionale Baugruppenelemente (Funktions- und Bestückungsvarianten) berücksichtigen zu können. Fehler aus dem Schaltplanprogramm (z.B. nicht oder nicht vollständig hinterlegte Bauelementdaten) oder fehlende Kennwerte können manuell nachgetragen werden.

Das Ergebnis einer Standardberechnung sind die Werte für die *Ausfallrate* λ in FIT und die *mittlere ausfallfreie Arbeitszeit MTTF* in Jahren.

Sämtliche Daten und Einstellungen können ab dem Zeitpunkt der Extraktion gesichert werden. Die Bearbeitung/Berechnung kann aus einer Sicherungsdatei, auch nach zwischenzeitlicher Unterbrechung, weitergeführt werden.

Daten und Einstellungen die zur Berechnung benötigt werden, also auch konkrete Bauteilkennwerte, werden in der Berechnungsdatei abgespeichert. Auf Kosten erhöhten Platzbedarfs wird dadurch die Wiederholbarkeit alter Berechnungen garantiert, selbst wenn Schaltplan oder Bauteilkennwertdatenbank geändert werden.

8.1.2. Anwendungsszenario Safety

Sämtliche Angaben im “Anwendungsszenario Standard” gelten auch für die Sicherheitsvariante. Darüber hinaus sind zusätzliche Schritte durch den Anwender beim Berechnungsablauf in Excel durchzuführen.

Die Berechnungsergebnisse werden um die *mittlere Zeit bis zu einem gefährlichen Ausfall* $MTTF_D$ und die *Fehleraufteilung SFF* ergänzt. Das dazu notwendige FMEA-Formular wird automatisch erstellt und um die sicherheitstechnischen Felder erweitert. Die Fehleraufteilung muss pro Bauteil in die *Fehlerausfallarten* und in *sichere und unsichere Ausfälle* möglich sein. Nach Angabe des *Diagnosedeckungsgrades* ist die manuelle Eingabe abgeschlossen.

8.1.3. Anwendungsszenario Hotspot Berechnung

Aufgrund der hohen Bauteilkennwert-Änderungen unter Lastbedingungen, insbesondere Temperatur, soll es möglich sein, höher belastete Bauteile und Bauteilgruppen in der Berechnung entsprechend zu berücksichtigen.

8.1.4. Übersicht gesammelter Anforderungen

Im Anhang B.1 auf Seite 175 sind sämtliche im Rahmen dieser Masterarbeit gesammelten Anforderungen tabellarisch aufgelistet. Die Gliederung erfolgt nach praktischen Gesichtspunkten, aufgeteilt in Anforderungen an den Unternehmensprozess bzw. die Entwicklung (Tabelle B.1 auf Seite 176) und an das umzusetzende Prediktionswerkzeug (Tabelle B.2 auf Seite 177).

8.1.5. Zusätzliche Anforderungen

Um die Anforderungssuche abzuschließen, wurde mit unterschiedlichen Personen aus der HW-Entwicklungsabteilung, vor und während der Umsetzung des Werkzeugs, Gespräche geführt. Aus diesen Gesprächen wurden weitere Entwicklungsentscheidungen und Anforderungen abgeleitet:

TR 5 **Temperaturabhängigkeit der Bauteile berücksichtigen**
Das Ergebnis soll nicht nur einzelne, ausgewählte Temperaturen berücksichtigen, sondern möglichst den kompletten Temperatureinsatzbereich der Baugruppen berechnen und darstellen.

TR 6 **Möglichkeit zum manuellen Eingriff**
Die Ergebnisdateien müssen Möglichkeiten zu Kommentaren und Ergänzungen bieten. Dies ist zur Berücksichtigung besonderer Bauteile und Umgebungseinflüsse notwendig. Weiters sind Kommentare und Freitexte, zur Protokollierung im Sicherheitsbereich, notwendig.

TR 7 **Erweiterungen/Änderungen von Bauteilbeschreibungen übernehmen**
Erweiterungen der Bauteilbeschreibungen im Schema-Editor sollen auch nachträglich, ohne Eingriff in die Programmierung, in die Ergebnisdateien übernommen werden.

TR 8 **Anpassungsfähigkeit des Werkzeugs**
Generell soll das Werkzeug so umgesetzt werden, dass Veränderungen der Normenlandschaft, Kenndatenanpassungen, Änderung der Kenndaten-Datenbanken und auch Weiterentwicklungen des Schema-Tools mit minimalem Aufwand berücksichtigt werden können.

TR 9 **Einfache Handhabung bei Bedienung und Administration**
Fokus auf einfache Handhabung, sowohl in Anwendung als auch in Administration - Nutzungs-Hürde muss niedrig sein, Installation und Konfiguration trotz der geforderten Anpassungsfähigkeit möglichst einfach.

8.1.6. Arbeitsumgebung

Das Prediktions-Werkzeug wurde für zwei unterschiedliche Arbeitsumgebungen eingerichtet:

- Windows XP mit Office 2003
- Windows 7 mit Office 2010

Dies ergibt sich daraus, dass eine unternehmensweite Umstellung zwischen diesen beiden Arbeitsumgebungen während der Realisierungs- und Testphase vollzogen wurde.

ANMERKUNG: Inkompatibilitäten zwischen den beiden Office-Paketen machten dazu leider Eingriffe in den Source-Code notwendig. Es wurden zwei Sprachversionen (deutsch/englisch) angelegt. Auch hier waren Eingriffe in die Skript-Codes notwendig.

Gemeinsame Vorgaben	
Rechner-Hardware	Standard-PC (Notebook) mit Intel Core 2 Duo CPU T7300 (2GHz)
Schema-Design-Tool	Schemaeditor des Programmpakets *Mentor Graphics PADS V9.2*; ANMERKUNG: *In Folge wird auf den Schema-Editor unter dessen Produktbezeichnung "DxDesigner" verwiesen.*
Entwicklungsumgebungen	*1) Visual Studio 2010* Editor und Debugger mit angepasster JScript-Umgebung *2) MS-Office Visual Basic* Entwicklungsumgebung
Windows XP - Office 2003	
Tabellenkalkulation	MS-Excel, Versionen 2003, Deutsch
VBScript-Version /Scripting Host	V5.7
Windows 7 - Office 2010	
Tabellenkalkulation	MS-Excel, Versionen 2010, Deutsch
VBScript-Version /Scripting Host	V5.8

Tabelle 8.1.: Vorgaben zur Ausstattung eines Arbeitsplatzes für Entwicklung von Hardware-Komponenten und zur Programmierung des Werkzeugs (Software und Hardware)

Die nachfolgenden Beschreibungen beziehen sich alle auf die Konfigurationsvariante *Windows XP mit Office/Excel 2003* in der Spracheinstellung *Deutsch*.

Als Hauptinformationsquelle zur Implementierung des Prediktionswerkzeugs

diente hauptsächlich das *DxDesigner Referenz Handbuch*. Die Auswahl der Programmiersprache (VBScript) war durch den Schema-Editor vorgegeben. Änderungen am Interface sind nur mittels dieser Skriptsprache möglich. Die bereits etablierte und somit vom Entwicklungspersonal präferierte Microsoft Office Umgebung zur Ergebnisdarstellung, führte dann zur Entscheidung, die gesamte Berechnung ebenfalls mit VBScript umzusetzen.

8.2. Auswahl der geeigneten Methode zur Kennwertgenerierung

In der nachfolgenden Analyse der unterschiedlichen, bereits in Kapitel 2.4.1 auf Seite 40 vorgestellten, analytischen Kenngrößen-Bestimmungsverfahren wird deren bestmögliche Eignung zur computergestützten Kennwertberechnung bewertet.

Maßgebliches Kriterium ist die Berechnung von Sicherheitsbaugruppen auf Basis vorhandener Schaltplandaten. Da dies sowohl der Ausgangspunkt als auch eine in Zukunft wichtige und sehr kritische Anwendung bleibt, wird die Auswahl aus den dafür notwendigen Gesichtspunkten getroffen. Für Standardanwendungen sind sämtliche betrachteten Methoden ebenfalls geeignet.

Fehlerzustandsart- und -auswirkungsanalyse FMEA[1] [IEC06a]

Die FMEA ist *bedingt* für die automatische Auswertung von elektronischen Baugruppen *geeignet*. Durch die sequentielle Beurteilung jedes einzelnen Bauelements, automatische Zuordnung der Ausfallart und Ausfallwahrscheinlichkeit, wird der Methode entsprochen. Um die FMEA zu vervollständigen, ist der Eingriff eines Experten notwendig. Die Beschreibung möglicher Ausfallursachen, der Auswirkung auf die Zieleinheit, Diagnose- und Vermeidungsmöglichkeiten sind nicht automatisch eruierbar.

Mit einer FMEA lassen sich voneinander abhängige Ausfälle und auch Fehlersequenzen beschreiben. In Kombination mit anderen Methoden, wie beispielsweise dem Parts Stress Verfahren, lässt sich die Genauigkeit der Ausfallratenbestimmung deutlich erhöhen.

Zuverlässigkeits-Blockdiagrammanalyse RBD [IEC06c]

Die Ereignisablaufanalyse ist zur automatischen Auswertung elektronischer Schaltungen *wenig geeignet*, da die logische Verschaltung der Blöcke nicht den Serien- und Parallelverbindungen der elektronischen Schaltung folgt sondern

1 Details zur deutschen Bezeichnung und Alternativen dazu im Abkürzungsverzeichnis

viel mehr tatsächlich vorhandene Redundanzen auf Basis der betrachteten Ausfallart darstellt. Die mathematische Auswertung eines bestehenden Modells ist einfach computerunterstützt realisierbar.

Zuverlässigkeitsblockdiagramme sind zur Analyse von zeitabhängigen Ereignissen und somit auch Ausfallsequenzen ungeeignet.

Fehlzustandsbaumanalyse FTA [IEC06b]

Die Anwendbarkeit für das Prediktionstool wird als niedrig bewertet, da die Analyse von der Kenntnis der Ausfallshauptereignisse ausgeht. Dies steht in keinem automatisch erfassbaren Zusammenhang mit den Schaltplänen der Baugruppe. Voraussetzung dafür wäre eine semantische Analyse, beispielsweise via Schaltungssimulation.

Die Methode ist nicht ausschließlich darauf beschränkt, Ausfallwahrscheinlichkeiten zu berechnen. Auf die gleiche Art ist eine numerische Erfolgsanalyse durchführbar, wobei dabei die Konzentration auf Erfolgsereignissen statt Ausfällen liegt. Neben der numerischen Anwendbarkeit ist auch eine rein qualitative Analyse möglich, wo beispielsweise eine Kategorisierung von Ereigniswahrscheinlichkeiten in "Hoch", "Mittel" und "Niedrig" durchgeführt wird. Je nach Anwendung ist das Verfahren als Ausfallraten- (numerisch) oder Ausfallartenanalyse (qualitativ) einzustufen.

Markov-Verfahren [IEC06d]

Die vollautomatische Generierung einer Markov-Kette aus einer elektronischen Schaltung ist nicht einfach möglich. Das Verfahren dient dazu, Betriebszustände als Ergebnis von zeitlichen Sequenzen von vorgelagerten Zuständen und deren verbindenden Transitionen zu modellieren. Dieser Ansatz entspricht nicht der Zielsetzung des Prediktions-Werkzeugs und kann somit aus der weiteren Betrachtung ausscheiden.

Als zustandsbasiertes, stochastisches Verfahren ist dieses nutzbar, statistisch unabhängige Ausfallsequenzen zu berücksichtigen und numerisch zu bewerten. Die Komplexität und auch die Anzahl der Zustände steigt mit jeder zusätzlich betrachteten Komponente rapid an. Systeme mit dutzenden oder mehr Bauelementen sind nur durch Aufteilung in Teilsysteme erfassbar.

Parts-Count Methode

Die automatische Bestimmung eines Summenwerts eines Gesamtsystem, aber auch von Teilsystemen, ist sehr einfach möglich.

Parts-Stress Methode

Die automatische Generierung eines Parts-Stress Kennwerts aus einer elektronischen Schaltungsbeschreibung ist einfach möglich. Die Qualität der verknüpften Datenbank gibt dabei den Komfort in der Anwendung und die Genauigkeit des Ergebnisses vor. Entsprechende Implementierung ermöglicht den einfachen Austausch der verwendeten Datenbank. Dies ist für die Anwendung in verschiedenen Anwendungsbereichen und Ländern sinnvoll.

Auswahl der geeigneten Analysemethode

Die Kennwertbestimmung bei Umsetzung der Sicherheitsbaugruppe erfolgte mittels kombinierter Anwendung von Parts-Count Verfahren und FMEA. Aufgrund fehlender Erfahrungen mit anderen Methoden wird im Rahmen dieser Arbeit auf dieser Grundlage aufgebaut. Das Parts-Count Verfahren wird jedoch durch die ebenfalls einfach zu realisierende Parts-Stress Methode ersetzt.

Höherwertige Verfahren und andere Herangehensweisen können bei Bedarf auch nachträglich im Berechnungstool realisiert werden.

8.2.1. FMEA in Kombination mit Parts-Count Methode

Die ausgewählte Methodenkombination vernachlässigt grundsätzlich gegebene Schaltungsstrukturen und zeitliche Abhängigkeiten. Dadurch erreicht eine damit ermittelte Ausfallrate, bei gleicher Kennwertbasis, automatisch ein Maximum. Jegliche Berücksichtigung von Schaltungsinformationen wie Redundanzen oder Informationen bezüglich Funktion über die Zeit, sollte somit die Ausfallrate verbessern.

Aus sicherheitstechnischer Sicht ist die Anwendung dieser Worst-Case Methode für den Endanwender der Baugruppen (Kunde) ein Vorteil. Der damit errechnete, obere Grenzwert ist in Realität als besser einzustufen, was im Einsatz einen noch höheren Vertrauensgrad zu den Sicherheitsfunktionen bedeutet. Nachteil in Entwicklung und Produktion ist, dass die sicherheitstechnischen Kennwertgrenzen als Absolutwerte in den Standards vorgegeben und somit mit der “schlechteren” Methode schwieriger zu erreichen sind.

Praktische Durchführung einer FMEA

Die FMEA ist geeignet für die Anwendung auf Systeme, bestehend aus Hardware und Software, deren Wechselwirkungen und Prozesse. Die prinzipielle Vorgangsweise bei der Durchführung einer FMEA ist im Standard vorgegeben (Diagramm 8.1 auf der nächsten Seite).

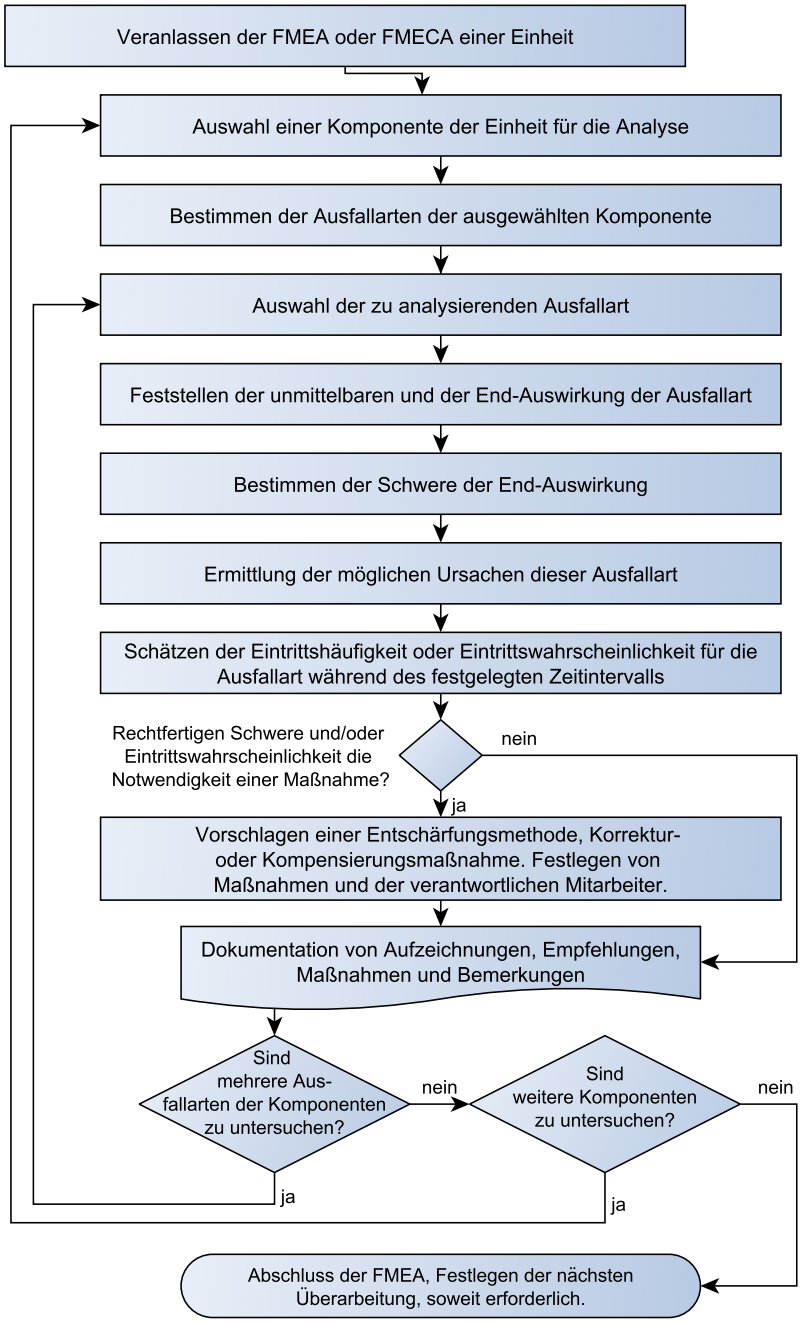


Abbildung 8.1.: Ablaufdiagramm zur FMEA-Analyse [IEC06a, Kapitel 5.2.10]

Grenzen und Unzulänglichkeiten der FMEA

Eine FMEA ist effizient, wenn sie zur Analyse von Elementen angewendet wird, die den Ausfall eines gesamten Systems oder einer Hauptfunktion des Systems verursachen. Bei komplexen Systemen mit Mehrfachfunktionen, an denen

unterschiedliche Systemkomponenten beteiligt sind, kann eine FMEA jedoch schwierig und aufwändig sein. Der Grund hierfür liegt in der Menge der zu berücksichtigenden detaillierten Informationen über das System. Diese Schwierigkeit kann noch dadurch verstärkt werden, dass es möglicherweise zeitliche Abhängigkeiten oder Funktionsvarianten, wie z.B. Betriebsarten gibt.

Nicht alle Beziehungen zwischen einzelnen oder Gruppen von Ausfallarten bzw. deren Ursachen können tatsächlich in einer FMEA dargestellt werden. Die wesentliche Voraussetzung dazu ist die Unabhängigkeit der analysierten Ausfallarten. Praktisch tritt dieses Problem bei Baugruppen mit Hardware-/Softwarewechselwirkungen auf.

8.2.2. Abschluss Spezifikationsphase

Die Anforderungsbestimmung und Methodenauswahl ist an diesem Punkt abgeschlossen und die Rahmenbedingungen für Programmierung und Betrieb des Prediktionswerkzeugs sind festgelegt. In den nun folgenden Abschnitten wird das Ergebnis der Tool-Umsetzung und die Ergebnisverifikation betrachtet.

8.3. Berechnungsablauf

Anhand der Beschreibung eines Berechnungsablaufs wird die prinzipielle Handhabung und Funktionsweise des Prediktionswerkzeugs beschrieben. Die Beschreibung wird durch Abbildung 8.2 auf der nächsten Seite unterstützt. In Anhang B.2 auf Seite 178 sind Screenshots zu Beispielaufrufen, Übergabeparametern und allen Eingabe- sowie Ergebnisdateien (siehe Anhang B auf Seite 175) abgedruckt und beschrieben.

Um eine bessere Vorstellung des praktischen Arbeitsablaufs zu bekommen, wurden im Rahmen der Anwenderdokumentation mehrere kurze Filme für die wichtigsten Anwendungsszenarien erstellt.

Das Berechnungswerkzeug besteht aus einem, aus der Kommandozeile zu startenden Hauptskript (`ExamineAvailability.vbs`). Das Skript wird mittels, in Anhang B genau beschriebenen, Übergabeparametern gesteuert. Um die Bedienung aus dem DxDesigner zu erleichtern, wurde im Designtool ein Menü hinzugefügt (`Menu.vbs`), welches bei Auswahl eines Menüpunktes das Hauptskript mit den entsprechenden Übergabeparametern aufruft.

Neben der korrekt eingerichteten Arbeitsumgebung, wie in Abschnitt 8.1.6 auf Seite 141 beschrieben, müssen für einen erfolgreichen Start des Hauptskripts folgende Voraussetzungen erfüllt sein:

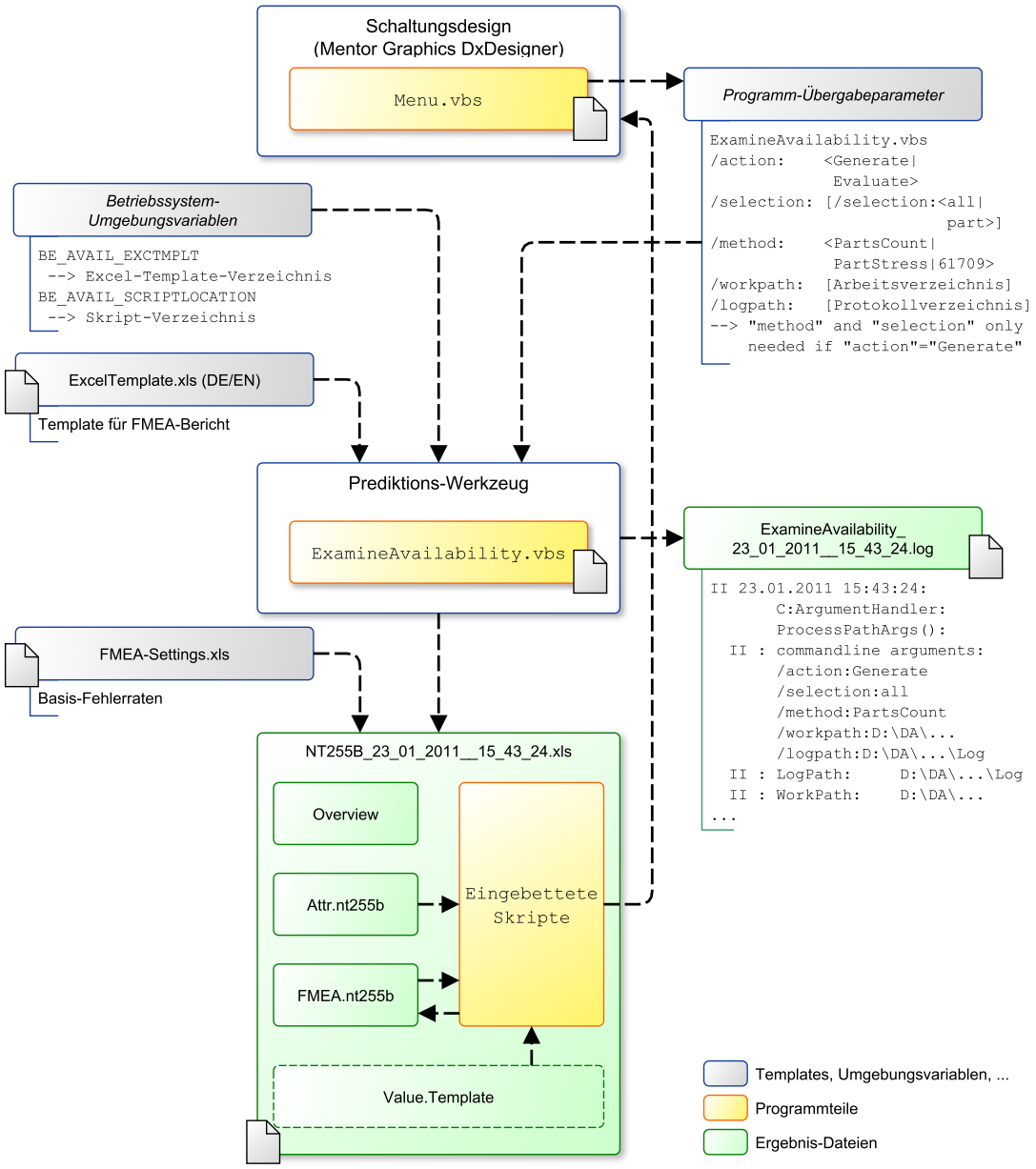


Abbildung 8.2.: Berechnungsablauf und Datenfluss im Prediktions-Werkzeug

- *Templates für FMEA-Bericht und Basis-Fehlerraten* für Programm zugänglich
- *Betriebssystem-Umgebungsvariablen* eingetragen
- *Übergabeparameter* vollständig und korrekt

Eine genaue Beschreibung dieser Punkte erfolgt in den Abschnitten B.3 auf Seite 185 und B.2.1 auf Seite 178.

Sind alle Voraussetzungen erfüllt, startet das Skript den *Extraktionsvorgang*. Dabei wird zuerst eine Kopie des `ExcelTemplate.xls` angelegt. Der Name der Kopie leitet sich dabei vom DxDesigner Projekt, sowie Datum und Uhrzeit des Berechnungslaufs ab. Die Vorlage beinhaltet Tabellenüberschriften, Formatvorlagen und eingebettete Skripte für die weitere Bearbeitung. Nach Anlegen der Kopie wird das Schaltplanschema Bauteil für Bauteil abgearbeitet und jeweils die notwendigen Informationen in den vorbereiteten FMEA-Bericht eingetragen. Zusätzlich werden auf der Übersichtsseite des Berichts (Tabellenblatt "Overview") statistische Informationen zum Schema und zum Programmablauf vermerkt. Diese dienen der Nachvollziehbarkeit zu einem späteren Zeitpunkt.

Jeder Programmdurchlauf generiert, auch bei Fehlerabbruch, zumindest eine Protokolldatei (siehe B.2.2 auf Seite 183). Wichtige Programmschritte werden beim Aufruf in dieser Protokolldatei vermerkt. Somit ist bei einem allfälligen Skriptabbruch sofort rückverfolgbar, an welcher Stelle der Fehler aufgetreten ist.

Sind die Bauteilinformationen erfolgreich vom DxDesigner übernommen worden, besteht die Möglichkeit, manuell einzelne Bauteile von der weiteren Berechnung auszuschließen.

8.3.1. Zuverlässigkeitsberechnung

Aus Sicht der Generierung der Bauteil-Stückliste werden die beiden folgenden Anwendungsfälle unterschieden:

1. Schaltplan wird in DxDesigner neu erstellt bzw. ein bereits existierender Schaltplan wird verändert. Komponenten-Daten werden in eine neue Auswertungstabelle exportiert.
2. Auswertungstabelle mit Verfügbarkeitskenndaten existiert (aus früherer Extrahierung) und dient als Basis für weitere Bearbeitungsschritte.

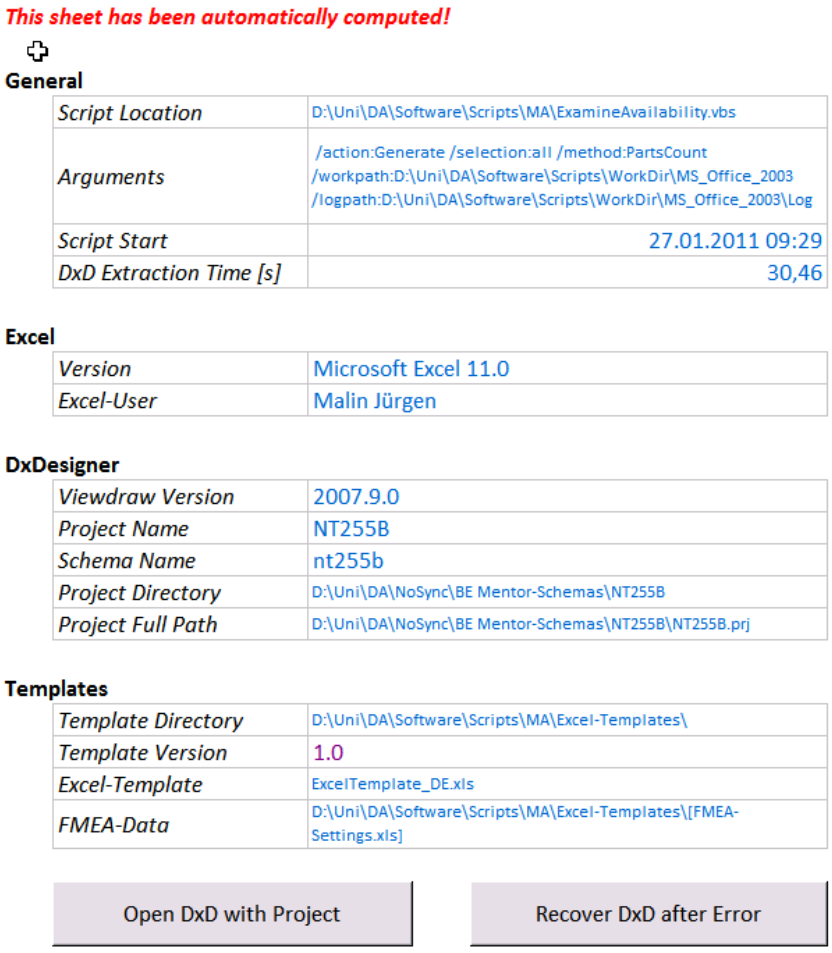
Schaltplan neu extrahieren

In diesem Fall ist der Schema-Editor der Ausgangspunkt der Anwendung. Ein Schaltplan wird neu erstellt oder geändert und danach, mittels entsprechender Menüauswahl, der Export der Komponentendaten gestartet.

Zur Auslösung der Bauteildaten-Extrahierung im DxDesigner gibt es zwei Möglichkeiten. Den *Export des gesamten Schaltplans*, ohne besondere Voraussetzungen oder den *Export eines Schaltplanteils*, wo eine Selektion von mindestens einem Bauteil erwartet wird.

Die Auswahl des entsprechenden Menüpunkts erstellt aus vordefinierten Templates eine leere Exceldatei und die Protokolldatei zur Verfolgung des Berechnungsablauf und gegebenenfalls zur Fehleraufarbeitung. Genauere Beschreibungen der Dateien sind in Anhang B.2.2 auf Seite 183 zu finden.

Die zwei generierten Dateien liegen nach erfolgreichem Durchlauf des Skripts im Arbeits- bzw. Protokollverzeichnis. Je nach Menüauswahl findet ein Gesamtexport aller Bauteilkenndaten der Baugruppe oder nur der selektierten Elemente in das Attribut-Registerblatt (siehe B.2.1 auf Seite 178) statt. Zusätzlich werden im Übersichts-Registerblatt Details zum Projekt, zum Skript und der Arbeitsumgebung erfasst (siehe Screenshots 8.3 und 8.4 auf der nächsten Seite). Dies dient der Protokollierung, der späteren Wiederholbarkeit und der Fehlersuche bei auftretenden Problemen.



This sheet has been automatically computed!

General

Script Location	D:\Uni\DA\Software\Scripts\MA\ExamineAvailability.vbs
Arguments	/action:Generate /selection:all /method:PartsCount /workpath:D:\Uni\DA\Software\Scripts\WorkDir\MS_Office_2003 /logpath:D:\Uni\DA\Software\Scripts\WorkDir\MS_Office_2003\Log
Script Start	27.01.2011 09:29
DxD Extraction Time [s]	30,46

Excel

Version	Microsoft Excel 11.0
Excel-User	Malin Jürgen

DxDesigner

Viewdraw Version	2007.9.0
Project Name	NT255B
Schema Name	nt255b
Project Directory	D:\Uni\DA\NoSync\BE Mentor-Schemas\NT255B
Project Full Path	D:\Uni\DA\NoSync\BE Mentor-Schemas\NT255B\NT255B.prj

Templates

Template Directory	D:\Uni\DA\Software\Scripts\MA\Excel-Templates\
Template Version	1.0
Excel-Template	ExcelTemplate_DE.xls
FMEA-Data	D:\Uni\DA\Software\Scripts\MA\Excel-Templates\[FMEA-Settings.xls]

Open DxD with Project | Recover DxD after Error

Abbildung 8.3.: Ergebnis einer Baugruppen-Extrahierung nach Excel, Registerblatt “Übersicht”: Informationen zum Berechnungslauf

Die abgebildeten Schaltflächen im unteren Bereich des Bildschirmfotos dienen zur Verbesserung der Bedienbarkeit. Bei Betätigung wird in beiden Fällen ver-

sucht, den Schaltplaneditor, mit dem gerade bearbeiteten Projekt, direkt aus Excel zu starten.

Component Statistics

Selected Components	All

Sheets	*Overall Count*		*Components*	*Test Points*	*ModuleCount*	*Pins*	*Annotations*	*Composites*	*Unknown*
	by GetMethod	*by Count*							
nt255b.1	77	77	39	10	49	27	1	0	0
nt255b.2	99	99	55	20	75	23	1	0	0
nt255b.3	123	123	38	39	77	45	1	0	0
nt255b.4	33	33	8	0	8	24	1	0	0

Abbildung 8.4.: Registerblatt “Übersicht”: Statistische Informationen zu den extrahierten Daten und Bauelementen

Die weiteren Schritte entsprechen dem nachfolgend beschriebenen Anwendungsfall mit bereits existierender Bauteilstückliste.

Bauteil-Stückliste existiert

In diesem Fall ist das generierte Excel-Dokument mit den exportierten Bauteil-Kenndaten die Arbeitsumgebung. Optional kann zuvor schon eine Berechnung der FMEA-Daten erfolgt sein. Das FMEA-Registerblatt ist in diesem Fall bereits mit Daten gefüllt (siehe Screenshot 8.6 auf Seite 153).

Screenshot 8.5 auf Seite 152 zeigt das Ergebnis einer vollständigen Übertragung eines Baugruppenschaltplans in die Berechnungsumgebung. Die Stückliste umfasst sämtliche, im Schaltplaneditor hinterlegten, Bauteilkennwerte. Besonders hervorzuheben sind folgende Spalten:

C steht für “calculate” und dient als Schalter zur (Nicht-)Berücksichtigung von Bauelementen für die weitere Berechnung.

dT Diese Spalte wird genutzt um Temperaturabweichungen gegenüber der Referenztemperatur, für Bauteile und Bauteilgruppen, als zusätzliche Eingangsgröße für die Berechnung zu hinterlegen. Damit sind auch Hot-Spots abbildbar. Dies erfolgt entweder bereits bei der Schaltplanerstellung (Werte werden bei Extrahierung eingetragen) oder während der Kennwertberechnung in der Tabellenkalkulation.

DxD-UID Der hier angezeigte Wert ist eine, vom DxDesigner vergebene, eindeutige Kennzeichnung des Bauelements, nach welcher dort gesucht werden kann. Im Registerblatt ist dieser Wert als Schaltfläche ausgeführt, welche bei Betätigung in den Schaltplaneditor wechselt und das entsprechende Bauelement selektiert.

Die Schaltfläche “Calculate New FMEA” im oberen Bereich des Registerblatts triggert die Ausführung einer FMEA-Erstellung auf Basis der vorhandenen bzw. veränderten Daten. Im einfachsten Fall wird nach einer Extraktion der Baugruppendaten lediglich auf der Übersichtsseite kontrolliert, ob die Übertragung erfolgreich verlief. Danach kann direkt die Erstellung der FMEA gestartet werden.

FMEA-Auswertung

In Screenshot 8.6 auf Seite 153 ist ein Teilausschnitt eines FMEA-Registerblatts zu sehen. Im Bereich über den Schaltflächen sind die Eingabefelder für die Umgebungs-, Maximaltemperatur (Labels “Environment Temperature”und “Maximum Temperature”) und die generelle Temperaturabweichung (ΔT). Sämtliche Werte sind für die Temperaturkurvenberechnung relevant.

Die Schaltfläche “Recalculate FMEA” triggert eine Neuberechnung der Verfügbarkeitskennwerte auf Basis der auf diesem Blatt verfügbaren Temperatureingaben und Bauteilkennwerte. Bei der Bauteilextrahierung erfolgt keine automatische Erstellung und Berechnung.

“Clear Sheet” löscht sämtliche manuellen Eingaben und setzt somit das Registerblatt in den Zustand nach der Erstellung zurück.

Direkt unter den Schaltflächen sind die Ergebnisse der Berechnung abzulesen. *SFF* und $MTTF_D$ für Sicherheitsbaugruppen, sowie *MTTF* und λ (“Sum”) für Standardbaugruppen.

Der untere Bereich des FMEA-Registerblatts ist den Bauteilkenndaten vorbehalten. Ausgehend von der Stückliste wird für jedes Bauteil, welches für die Berechnung zu berücksichtigen ist, eine Zeile angelegt. Wichtigstes Element ist dabei ein Drop-Down Feld für die exakte Typenauswahl des jeweiligen Bauelements. Das Berechnungswerkzeug versucht dabei, mittels String-Matching (Kombination von Bauteilkennzeichnung, “Type” und Bauteilbeschreibung) den passenden Ausfallkennwert aus der Kennwertdatenbank zuzuordnen. Schlägt die exakte Suche fehl, wird der SN29500 Basiswert aus Zuordnung zur Bauteilkennzeichnung (“RefDes”) eingetragen, also für C20 $\rightarrow$ C für IC3 $\rightarrow$ IC usw. Alternativwerte die der Bauteilkennzeichnung zugeordnet sind, sind danach über die Drop-Down Liste auswählbar.

Aus der Typenauswahl ergibt sich ein λ-Wert, welcher direkt nach Auswahl in die entsprechend Spalte eingetragen wird. Findet sich kein passender Wert in der Auswahlliste, kann dieser Wert direkt eingetragen werden.

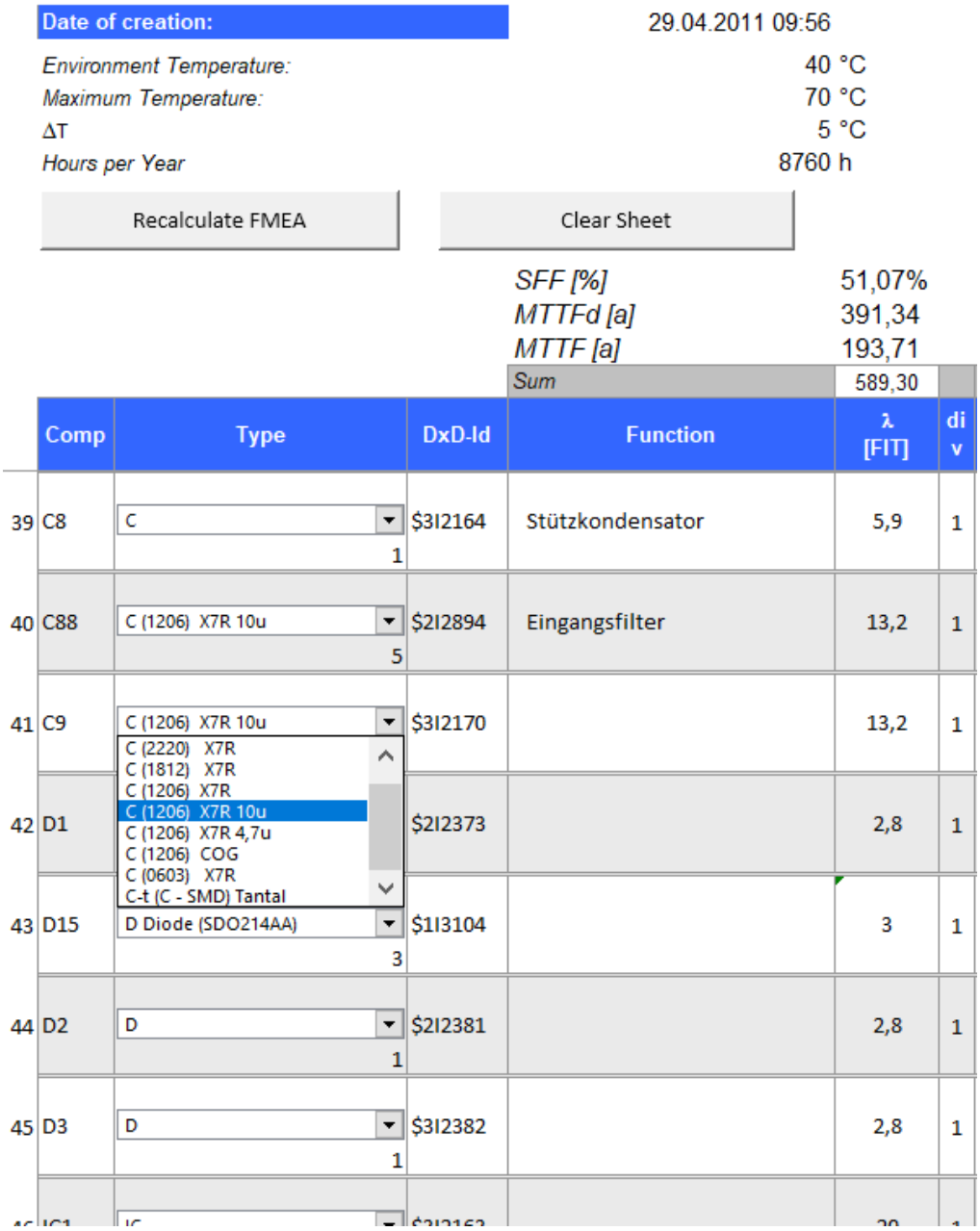
Date of creation	27.01.2011 09:29
Count of Components	140

Calculate New FMEA

C	RefDes	Typ	Value	E-Num	Type	dT	Description
☑	C7	KERAMIK	1U	E0781800			
☑	C8	KERAMIK	100N	E0853900			
☑	C88	KERAMIK	1N	E0892900			
☑	C9	KERAMIK	100N	E0853900			
☑	D1			E0413700	BAV70		SI-DIODE
☑	D15			E0413700	BAV70		SI-DIODE
☑	D2			E0558800	BZX84		ZENERDIODE
☑	D3			E0727000	LED	19	LEUCHTDIODE GELB
☑	IC1			E1104000	74AHCT1G125		LINE DRIVER
☑	IC10			E0895200	74FCT825		8-BIT BUS-INTERFACE REGISTER
☑	IC11			E0875900	74AC138		1 OF 8 DECODER
☑	IC12			E1422500	LM2903		DUAL DIFFERENTIAL COMPARATOR
☐	IC12			E1422500	LM2903		DUAL DIFFERENTIAL COMPARATOR
☐	IC12			E1422500	LM2903		DUAL DIFFERENTIAL COMPARATOR
☑	IC2			E0713000	74AC02	19	4-FACH NOR
☐	IC2			E0713000	74AC02		4-FACH NOR
☐	IC2			E0713000	74AC02		4-FACH NOR
☐	IC2			E0713000	74AC02		4-FACH NOR
☐	IC2			E0713000	74AC02		4-FACH NOR
☑	IC3			E0713000	74AC02	19	4-FACH NOR

Pkg-Type	Datasheet	DxD-Sheet	DxD-UID
1206		nt255b.1	$1I3116
603		nt255b.3	$3I2164
603		nt255b.2	$2I2894
603		nt255b.3	$3I2170
SOT23_1A2A3KK	Datasheet	nt255b.2	$2I2373
SOT23_1A2A3KK	Datasheet	nt255b.1	$1I3104
SOT23_1A2NC3K	Datasheet	nt255b.2	$2I2381
LED1		nt255b.3	$3I2382
SOT353	Datasheet	nt255b.3	$3I2163
QSOP24	Datasheet	nt255b.3	$3I2229
SO16R:SO16W1:SO16W2	Datasheet	nt255b.3	$3I2228
MSOP8	Datasheet	nt255b.2	$2I2920
MSOP8	Datasheet	nt255b.2	$2I2921
MSOP8	Datasheet	nt255b.2	$2I2919
SO14R:SO14W1:SO14W2	Datasheet	nt255b.3	$3I2239
SO14R:SO14W1:SO14W2	Datasheet	nt255b.3	$3I2231
SO14R:SO14W1:SO14W2	Datasheet	nt255b.3	$3I2232
SO14R:SO14W1:SO14W2	Datasheet	nt255b.3	$3I2233
SO14R:SO14W1:SO14W2	Datasheet	nt255b.3	$3I2230
SO14R:SO14W1:SO14W2	Datasheet	nt255b.3	$3I2238

Abbildung 8.5.: Bauteil-Stückliste nach erfolgreicher Baugruppen-Extrahierung aus DxDesigner



Date of creation:	29.04.2011 09:56
Environment Temperature:	40 °C
Maximum Temperature:	70 °C
ΔT	5 °C
Hours per Year	8760 h

Recalculate FMEA | Clear Sheet

SFF [%]	51,07%
MTTFd [a]	391,34
MTTF [a]	193,71
Sum	589,30

	Comp	Type	DxD-Id	Function	λ [FIT]	div
39	C8	C 1	$3I2164	Stützkondensator	5,9	1
40	C88	C (1206) X7R 10u 5	$2I2894	Eingangsfilter	13,2	1
41	C9	C (1206) X7R 10u	$3I2170		13,2	1
42	D1		$2I2373		2,8	1
43	D15	D Diode (SDO214AA) 3	$1I3104		3	1
44	D2	D 1	$2I2381		2,8	1
45	D3	D 1	$3I2382		2,8	1

C (2220) X7R
C (1812) X7R
C (1206) X7R
C (1206) X7R 10u
C (1206) X7R 4,7u
C (1206) COG
C (0603) X7R
C-t (C - SMD) Tantal

Abbildung 8.6.: FMEA-Registerblattausschnitt (Non-Safety Teil) als Ergebnis der Kennwertberechnung

Besonderheiten der Sicherheitsberechnung

Der sicherheitstechnisch relevante Teil des FMEA-Registerblatts ist in Screenshot 8.7 auf der nächsten Seite abgedruckt.

FMEA-Bewertung Jedes Bauteil kann als (nicht) sicherheitsrelevant eingestuft werden ("dc"... "don't care"). Sicherheitsrelevante Bauelemente sind manuell entsprechend ihrer Funktion nach der Gewichtung der Ausfallarten *Kurzschluss, Leerlauf* und *Drift* zu bewerten. Die Aufteilung in sicheren und unsicheren Ausfallanteil schließt die FMEA Eingabe ab.

Redundanz-Berücksichtigung Im Rahmen der Sicherheitsberechnung ist eine Pfad- bzw. Kanalbewertung entsprechend verschiedener Redundanz-Varianten (1oo1, 1oo2, 1oo2D, ...) optional durchführbar. Durch einfache Eingabe eines Divisors können somit Kennwerte bezüglich redundanter Funktionsblöcke bzw. Kanäle berechnet werden.

Date of creation:				29.04.2011 09:56						
Environment Temperature:				40 °C						
Maximum Temperature:				70 °C						
ΔT				5 °C						
Hours per Year				8760 h						
Recalculate FMEA			Clear Sheet							
				SFF [%]	51,07%					
				MTTFd [a]	391,34					
				MTTF [a]	193,71					
				Sum	589,30					

	Comp	Type	DxD-Id	Function	λ [FIT]	div	dc	Failure Type		Failure Effect
39	C8	C 1	$3I2164	Stützkondensator	5,9	1	☑	oc: sc: drift:	70% 10% 20%	
40	C88	C (1206) X7R 10u 5	$2I2894	Eingangsfilter	13,2	1	☐	oc: sc: drift:	70% 10% 20%	
41	C9	C (1206) X7R 10u 5	$3I2170		13,2	1	☐	oc: sc: drift:	70% 10% 20%	
42	D1	D-LED (2214) 7	$2I2373		2,8	1	☐	oc: sc: drift:	50% 30% 20%	
43	D15	D Diode (SDO214AA) 3	$1I3104		3	1	☐	oc: sc: drift:	50% 30% 20%	
44	D2	D 1	$2I2381		2,8	1	☐	oc: sc: drift:	50% 30% 20%	
45	D3	D 1	$3I2382		2,8	1	☐	oc: sc: drift:	50% 30% 20%	

		0,02	0,01		297,60	291,70	3,37	288,33	5,60	292,00
SFF	DFF	DCcompS [%]	DCcompD [%]	DM	λS [FIT]	λD [FIT]	λDD [FIT]	λDU [FIT]	λSD [FIT]	λSU [FIT]
100%	0%				4,13	0	0	0	0	4,13
100%	0%				0,59	0	0	0	0	0,59
100%	0%				1,18	0	0	0	0	1,18
50%	50%	90%	60%	gute Methode	4,62	4,62	2,772	1,848	4,158	0,462
50%	50%	99%	90%	sehr gute Methode	0,66	0,66	0,594	0,066	0,6534	0,0066
50%	50%	60%	0%	weniger gute Methode	1,32	1,32	0	1,32	0,792	0,528
50%	50%				4,62	4,62	0	4,62	0	4,62
50%	50%				0,66	0,66	0	0,66	0	0,66
50%	50%				1,32	1,32	0	1,32	0	1,32
50%	50%				0,7	0,7	0	0,7	0	0,7
50%	50%				0,42	0,42	0	0,42	0	0,42
50%	50%				0,28	0,28	0	0,28	0	0,28
50%	50%				0,75	0,75	0	0,75	0	0,75
50%	50%				0,45	0,45	0	0,45	0	0,45
50%	50%				0,3	0,3	0	0,3	0	0,3
50%	50%				0,7	0,7	0	0,7	0	0,7
50%	50%				0,42	0,42	0	0,42	0	0,42
50%	50%				0,28	0,28	0	0,28	0	0,28
50%	50%				0,7	0,7	0	0,7	0	0,7
50%	50%				0,42	0,42	0	0,42	0	0,42
50%	50%				0,28	0,28	0	0,28	0	0,28

Abbildung 8.7.: FMEA Berechnungsblatt - Gesamtansicht mit sicherheitstechnischen Eingaben

8.4. Korrektheitsprüfung

Wie in Kapitel 5 auf Seite 77 festgestellt, steht nach Bewertung verschiedener Möglichkeiten, lediglich die Sicherheitsbaugruppe SBv1 (→ 5.3 auf Seite 89) mit entsprechend hohem Vertrauensgrad in deren Kennwerte, als Referenz zur Verfügung.

Die Gegenüberstellung der manuell erstellten FMEA als Referenz und der Berechnung mittels Prediktiv-Werkzeug ergibt folgendes Ergebnis:

	Anzahl Bauelemente		
	Manuell	**Werkzeug**	**Differenz**
Busprint	584	583	-1
Frontprint	215	236	21
	Zuverlässigkeitskennwert [FIT]		
Busprint	7 350,40	7 307,52	42,88
Frontprint	2 311,19	2 313,59	-2,40

Tabelle 8.2.: Vergleich der manuell und mit Hilfe des Prediktionswerkzeugs ermittelten Ausfallrate

Die Differenz in der Anzahl der bewerteten Bauteile ergibt sich aus unterschiedlichen Gründen:

- Die automatische Auswertung berücksichtigt nicht, dass im Schaltplan verschiedene Bestückungsvarianten vorgesehen wurden. Deshalb sind in dieser deutlich mehr Bauteile berücksichtigt als in der manuellen Variante, wo nur die tatsächlich bestückten Elemente in die Berechnung einflossen.

- Die beiden Platinen der Baugruppe sind im Schaltplan nicht als Bauteile hinterlegt. Somit kann die automatische Kennwertbestimmung diese nicht berücksichtigen. Die Bauteile wurden in die Stückliste nach der Bauteilextrahierung manuell hinzugefügt und verändern somit das Kennwertergebnis nicht.

ANMERKUNG: Weitere “Bauteile”, welche nicht aus dem Schaltplan extrahiert werden können, in der manuellen Berechnung aber im Kennwert für die Platinen mit berücksichtigt wurden, sind Lötstellen, Testpunkte und Durchkontaktierungen. Zur genauen Bestimmung des Kennwerts müsste das Layout vorliegen und die genaue Anzahl berücksichtigt werden. Bei einer Baugruppe in der vorliegenden Komplexität erreicht man dabei Größenordnungen von 50 bis 100 FIT.

Der Vergleich der Ausfallrate ergibt eine Absolutdifferenz von ca. 40 FIT. Das Prediktionswerkzeug kommt zu einem niedrigeren Ergebnis als die manuell durchgeführte Berechnung.

Dieses Ergebnis beinhaltet bereits die Korrektur um die nicht berücksichtigten Bauelemente. Eine manuelle Prüfung der Stücklisten ergab, dass am Frontprint Unterschiede in der betrachteten Schaltung bestehen. Für den Kennwert ist dabei maßgeblich, dass andere Transistortypen verwendet wurden. Offensichtlich entsprechen die geprüften Schaltungsversionen nicht exakt dem selben Entwicklungsstand. Wo die Fehlerursache liegt, war nicht klar bestimmbar. Durch die manuelle Nachprüfung konnte jedoch festgestellt werden, dass die Unterschiede nicht nur in den extrahierten Tabellen, sondern auch in den Schaltplänen existieren. Die manuelle Korrektur dieses Unterschieds führt dann zu der erwarteten Differenz von Null, also identischen Werten der beiden Methoden.

Dies ist deshalb erwartungsgemäß, da die Berechnung mittels Prediktionswerkzeug methodisch und auch aus Sicht der Kennwertbasis identisch durchgeführt wurde. Somit ist dies eine gute Kontrolle, dass die semi-/automatischen Auswertungen keinen negativen Einfluss auf die Ergebnisse haben. Das Risiko systematischer Programmierfehler in der Berechnung wird durch die mehrfach erfolgreiche Anwendung, auch unter unterschiedlichen Temperaturannahmen, sowie durch Berechnung anderer Baugruppen, als niedrig eingestuft.

Aus der Kontrolle ergeben sich weitere Anforderungen für die zukünftige Umsetzung:

TR 10 Unterscheidung von Baugruppenvarianten im Designwerkzeug
Zur sauberen Berücksichtigung von Varianten wird eine entsprechende Kennzeichnung vorgeschlagen. Im DxDesigner kann dazu auf die Bauelement-Attribute zurückgegriffen werden bzw. es können neue Attribute definiert werden. Diese Kennzeichnung kann vom Extrahierungsprogramm durch einfache Erweiterung berücksichtigt werden.

TR 11 Verwaltung von Schaltplanversionen
Eine eindeutige Kennzeichnung und Speicherung von Versionen ist Grundlage für eine spätere Nachvollziehbarkeit eines Entwicklungsvorgangs und von Änderungen. Dies erfolgt idealerweise durch Verwendung eines geeigneten Versionierungs-Werkzeugs.

8.5. Benutzer-Dokumentation

Die Dokumentationen gliedern sich in die zwei Teile der *Umsetzungs- und Administrationsdokumentation* und in die *Anwendungsbeschreibung*. Das Ziel der Dokumentation war Vollständigkeit und Nachvollziehbarkeit.

Dokumentation der Programmierung und Administration

Die Programmteile sind im Source-Code beschrieben. Die Bedienung ist intuitiv und durch Informationstexte, sowie umfangreiche Fehlerausgaben geführt. Gemeinsam mit der Beschreibung des Berechnungsablaufs (Abschnitt 8.3 auf Seite 146) und der Ein- und Ausgabeartefakte (Abschnitt 8.3.1 auf Seite 148 und Anhang B auf Seite 175), sollte die Nachvollziehbarkeit gegeben, sowie eigene Erweiterungen möglich sein. Weiterführende Informationen zu den Vorlagen und Konfigurationsdaten sind in Anhang B auf Seite 175) nachzulesen.

Im Rahmen der Entwicklung entstand eine Reihe von Beispielprogrammen, welche einzelne Problemstellungen und Teilaufgaben kompakt lösen. Diese stehen zusätzlich zur Verfügung.

Anwender-Dokumentation

Zur Anwenderführung bei der Bedienung der Extrahierungs- und Berechnungsprogramme wurden Hilfstexte, die bei Bedarf direkt an der Konsole oder in entsprechenden Dialogen angezeigt werden, eingefügt.

Für jeden Berechnungsvorgang wird eine detaillierte Protokolldatei angelegt, welche im Bedarfsfall zur Fehlersuche dient.

Als Ergänzung, hauptsächlich zur initialen Schulung gedacht, sind die wichtigsten Benutzerszenarien mit Hilfe der interaktiven Schulungs-Software *Adobe Captivate* umgesetzt. Dabei werden folgende Themen behandelt (in Klammer der Dateiname des korrespondierenden Videos):

Vollständige Schaltungsextrahierung Export eines Gesamtschaltplans, Ergebnisdarstellung in Excel. [`01_FullCalcPartsCount`]

Teilextrahierung Varianten der Selektion von Teilschaltplänen und Extrahierung. [`02_SelectionCalcPartsCount`]

Definition von Temperaturabweichungen/Hotspots Spezifische Temperatur-Angaben für Bauteile und Bauteilgruppen vornehmen und extrahieren. [`03_SetTempProperty`]

Verbindung zwischen Excel-Ausgabe und Schaltplaneditor Direkter Aufruf des DxDesigners aus Stücklistenreiter in Excel und Übernahme editierter Temperaturwerte. [`04_SelectComponentsFromExcel`]

Artefakte und Übersichtsinformationen Anzeige von Speicherort und Inhalt der automatisch generierten Log-Datei. Hilfe zu den generierten Laufzeitinformationen im Übersichts-Reiter der Excel-Ausgabe und Schaltflächenbeschreibung. [`05_ProjectWorkdirAndLogAndOverview`]

Berechnung der Kennwerte/FMEA Einfache Kennwertberechnung und FMEA-Generierung. [`06_CalcFMEA`]

Erweiterte FMEA-Berechnungsfunktionen Beschreibung des FMEA Formblatts (Standard- und Sicherheitsteil). Demonstration der zerstörungsfreien Überarbeitungsfunktion (Schutz vor Löschen manueller Eingaben). [07_FMEAFunctions]

Die Demonstrationsfilme sind in einem Java-Script fähigen Browser oder alternativ in einem Video-Player abspielbar.

8.6. Weitere Funktionen und Anregungen

Während der Umsetzung wurden neue Ideen und Wünsche zur Prozessanpassung und zur Erweiterung des Berechnungswerkzeugs definiert.

TR 12 Modulare Extrahierungs- und FMEA-Methode
Eine automatisierte Variante der Extrahierung, wo eine Baugruppe anhand der Schaltungsstruktur zusammengehörige Bauelementgruppen selektiert und extrahiert. Z.B. können galvanisch getrennte Module automatisch selektiert werden. Weiter wäre die Kennzeichnung von Funktionsgruppen (z.B. Spannungsversorgung, Leistungsteil, Logikteil, E/A-Kanäle) wünschenswert. Diese Umsetzung würde eine detailliertere Betrachtung von Baugruppen auf Stücklisten- und FMEA-Basis ermöglichen. Zusätzlich wären auf den Einzelkanal bezogene Kennwertberechnungen möglich. DxDesigner stellt die dazu notwendige Netzplan-Struktur als API zur Verfügung.

TR 13 Vollständige Temperaturberechnung
In der vorliegenden Version ist die Temperaturberechnung erst einfachst möglich umgesetzt. Temperaturzonenberechnungen sind noch nicht realisiert.

TR 14 Berücksichtigung Impuls-/Digitalbetrieb
Bei analogen Halbleiter-Bauelementen, welche im Impulsbetrieb eingesetzt werden, verschlechtern sich die Zuverlässigkeitskenndaten (siehe SN29500-2 und -3).

TR 15 Berücksichtigung der RunIn Phase
Einbeziehung der RunIn Phase (accelerated aging), Berücksichtigung effektiver Einsatzzeiten (schon aktuell möglich) und die Kombination mit den bauteilspezifischen Werten für die Frühausfallsphase, entsprechend SN29500, ermöglicht eine genaue Ermittlung der resultierenden Garantiezeit.

TR 16 Markierung kritischer Bauelemente
Kennzeichnung der maßgeblichen Bauelemente am Kennwertergebnis. Schwellwerte sollen in Prozent oder absolut im FMEA-Berechnungsblatt angegeben werden können. Für Safety-Betrachtungen ist dabei der Anteil gefährlicher Ausfälle maßgeblich. Die Kennzeichnung soll sowohl in der Stückliste als auch im Schaltplaneditor erfolgen.

PR 34 Schaltplan-Richtlinien
Definition bzw. Erweiterung von Schaltplan-Richtlinien um genaue Definitionen zur auswertungskonformen Erstellung. Typbezeichner, Bauteileigenschaften, Namensgebungen, Attributverwendung, durchgängige Benennung von Schemas und Blättern und Versionsverwaltung, sind nur einige Beispiele für sinnvolle Vorschriften.

PR 35 Gesamtbaugruppen in einer Schema-Datei
Ebenfalls unter dem Thema Schaltplan-Richtlinien zu erfassen. Aktuell werden Schemas nicht pro Baugruppe, sondern pro Leiterplatte angelegt. Dies macht es ohne manuellen Eingriff unmöglich, eine komplette Baugruppe zu berechnen. Das Schema-Tool bietet die Möglichkeit, einzelne Leiterplatten unter einem Projekt zu bearbeiten ("Boards"), diese Funktion wird zumindest bei den untersuchten Baugruppen nicht genutzt.

Programmierung

Die Erfahrungen mit der Programmierumgebung sollen nicht unerwähnt bleiben. Die Entscheidung für VBScript erfolgte aus pragmatischen Gründen. Die API des Schaltplanwerkzeugs war einzig in dieser Variante verfügbar. Damit fiel die Wahl der Auswertungsumgebung auf Excel (gleiche Programmierumgebung).

Nachträglich betrachtet wäre bei der Verwendung einer höherwertigen Programmiersprache viel Zeitersparnis möglich gewesen. Das Fehlen von durchgängigen Debug-Methoden, vor allem bei der Programmierung der Schaltplan-Interfaces, musste durch viele Kommandozeilenausgaben kompensiert werden. Viele proprietäre Eigenheiten und Versions-Abhängigkeiten mussten mühsam in Online-Foren gefunden und dann Lösungen oder Umgehungen programmiert werden.

Innerhalb der Office-Umgebung ist die Sprachabhängigkeit der Programmiersprache das größte Problem. Eine Umsetzung in der deutschen Version ist nicht fehlerfrei in einer anderen Sprachversion ausführbar. Inkompatibilitäten der Office-Versionen bzw. keine Sicherstellung von Befehls- und Funktionskompatibilität gefährden die Zukunftssicherheit zusätzlich.

Bei einer neuerlichen Umsetzung würde die vorgegebene API mittels Wrapper in VBScript sauber realisiert. Damit wäre eine sinnvolle (Programmier-)Sprachunabhängigkeit umsetzbar.

9. Conclusio - Bewertung

Diese Masterarbeit verfolgte folgende Ziele bei der Umsetzung eines automatisierten Verfahrens zur Verfügbarkeits-Kennwertberechnung:

Automatisch Manuelle Arbeiten wo möglich automatisieren und damit die Fehlerquote beim Übertragen minimieren. Gleichzeitig Anreiz zur täglichen Anwendung erhöhen.

Zeitoptimiert und wirksam Den Zeitverlust durch die Kennwertgenerierung minimieren, im Idealfall sogar negieren.

Einfach Die Anwendung der Methode sollte ohne Detailkenntnisse der Verfügbarkeitstheorie und ohne langwierige Einschulungen einfach und natürlich in den momentanen Arbeitsablauf integrierbar sein.

Im Zuge der Beschäftigung mit dem Thema wurde zusätzlich klar, dass die Umsetzung einer computergestützen Berechnungsumgebung nur im Zuge einer *Überarbeitung und Anpassung der Entwicklungs-Prozesslandschaft* optimal wirksam wird.

Die Anwendung des *4+1 View Modells* von Philippe Kruchten ermöglichte eine systematische Vorgehensweise in der Gesamtbetrachtung der Problemstellung, auch wenn die original definierten Sichten angepasst werden mussten. Im laufenden technischen Alltag eher untergeordnet beachtete Perspektiven, wie der zugrunde liegende Prozess und die Wirtschaftlichkeit, erlangten dadurch einen erhöhten Stellenwert und steuerten wichtige Anforderungen für die Realisierung des Berechnungswerkzeugs und der Prozessanpassungen bei.

Ergebnisse und Bewertung des Prediktiv-Werkzeugs

Das wichtigste Resultat aus praktischer Sicht ist die Umsetzung des Verfügbarkeitskennwert-Berechnungsprogramms. Die nachfolgenden Punkte betrachten das Ergebnis kritisch und beleuchten sowohl erreichte, teilweise und nicht umgesetzte Eigenschaften.

Erhöhung des Automatisierungsgrades Die Einbindung in den Schaltplaneditor ist bereits optimiert und der Extrahierungsvorgang durchgängig automatisiert. Verbesserungen sind beim Befüllen des FMEA-Templates mit zur

Stückliste korrespondierenden Ausfallkennwerte möglich (siehe nächster Punkt).

Kennwertdatenbank nur teilweise umgesetzt Der sofortige Einsatz des umgesetzten Prediktionswerkzeugs im Entwicklungsalltag ist noch nicht möglich. Vor einer generellen Einführung muss zumindest eine vollständige Datenbank dem Werkzeug zugrunde gelegt werden.
Für den optimalen Gebrauch sollten die Bauteilkennzeichnungen und Typenbezeichner im Schaltplan vereinheitlicht werden. Dadurch könnte die Trefferquote zur automatischen Auswahl der Bauteile verbessert und die manuelle Nacharbeit verringert werden.
Erweiterungen durch zusätzliche Kennwertdatenbanken stellen kein Problem und keinen erheblichen Mehraufwand im Werkzeug dar.

Parts Count + FMEA Methode umgesetzt Aktuell ist die simpelste Berechnungsmethode umgesetzt worden. Auf Basis der Tabellenkalkulation ist die Komplettumsetzung des Parts-Stress Modells keine große Herausforderung. Es fehlen die temperaturabhängigen Werte in der Datenbank. Sollen andere Methoden angewendet werden, wird empfohlen die Berechnungsumgebung zu wechseln (z.B. Matlab, anderes Verfügbarkeits-Tool), da der Umbau des Werkzeugs erheblich wäre und kommerzielle Lösungen in guter Qualität verfügbar sind. Die niedrige Benutzerschwelle ginge durch diesen Schritt jedoch verloren.

Performance Der Extrahierungsvorgang und die Berechnungen dauern bei der komplexesten Anwendung im niedrigen Minutenbereich. Seitens Schaltplaneditor ist keine Optimierung möglich, da die offiziellen Schnittstellen verwendet werden.
In der Excel-Umgebung gibt es wahrscheinlich noch Optimierungspotential. Code-Review durch einen Spezialisten, Verwendung alternativer Programmiersprachen (nicht in VB-Skript) oder eine Alternative Umsetzung der Berechnung, ganz ohne Verwendung des Microsoft-Produkts, wären Ansatzpunkte.

Generische Umsetzung Das Tool ist auf Basis breit verfügbarer Programme und Werkzeuge umgesetzt worden. Die Abhängigkeit besteht im Schaltplan-Editor. Für weitere Anwender des Tools DxDesigner ist die realisierte Verfügbarkeitserweiterung ohne spezielle Kenntnisse oder Berechtigungen einsetzbar.

Benutzerfreundliche Bedienung Im Schaltplantool ist die Einbettung und Anwendung einfach und intuitiv. In Zusammenhang mit den Anwendungs-Kurzfilmen ist kein zusätzliches Training notwendig.
Die *Basis-Kennwertberechnung* in der Excel-Umgebung ist ebenfalls sehr einfach bedienbar.
Erweiterte Kennwertberechnungen mit anzupassenden Bauteilen, temperaturabhängige Berechnungen oder Safety-Kennwertbestimmungen sind

ohne manuellen Eingriff nicht möglich. Dazu ist entsprechendes Hintergrundwissen notwendig. Auch dabei erleichtert das Tool die Umsetzung durch das automatische Befüllen mit Standardwerten erheblich.

Berechnungszeit signifikant verringert Es konnte die notwendige Zeit zur Durchführung einer Parts-Count bzw. Parts-Stress basierten Verfügbarkeitsbewertung für eine elektronische Baugruppe, signifikant verringert werden. Eine Bauteil-Extrahierung mit Standardberechnung dauert somit wenige Minuten. Safety-Berechnungen können ebenfalls um Größenordnungen schneller durchgeführt werden (Vergleich für manuelle Durchführung: Tage bis Wochen). Lediglich die Aufteilung in die unterschiedlichen Fehlermodelle benötigt nach wie vor Zeit, wird allerdings durch die gute Unterstützung im Werkzeug ebenfalls beschleunigt.

Fehlerrisiko signifikant verringert Die Automatisierung von Wertübertragungen und sich wiederholenden Vorgängen, wie dem Zugriff auf die Kennwert-Datenbank oder das Generieren der Stückliste und FMEA-Tabelle, unterbindet Flüchtigkeits- und Ablesefehler. Gerade bei mehrfachen Änderungen, Verwendung neuer und alternativer Bauteile, Schaltungsänderungen, optionalen Funktionsgruppen, usw. war in der Vergangenheit das Risiko von Lösch- und Einfügefehlern hoch. Noch fataler war die manuelle Fehlersuche in riesigen Tabellen. Das Prediktivwerkzeug überzeugt in diesem Punkt bereits jetzt durch den hohen Vertrauensgrad und das niedrige Fehlerrisiko. Weitere Verbesserungen können hier durch Anwendung von Qualitätsmaßnahmen wie Code-Review und weitere Referenzberechnungen erzielt werden.

Der Nachweis wurde erbracht, dass Verfügbarkeitsberechnungen semi-automatisch ohne großen Zusatzaufwand durch den Entwicklungsingenieur selbst durchgeführt werden können. Dies ermöglicht unmittelbar den in Kapitel 7.2 auf Seite 129 definierten Prozess der *zuverlässigkeitsorientierten Schaltungsentwicklung*. Der HW-Entwickler muss kein Spezialist in Verfügbarkeitstheorie sein, kann aber bei Anwendung der skizzierten Methode einen effektiven und effizienten Schaltungsentwicklungsprozess mit dem Ergebnis von hochqualitativen und wirtschaftlichen Baugruppen umsetzen.

Status der Prozess-Anpassungen

Eine sehr aufwändige Aufgabe innerhalb der Master-Arbeit war die kritische Prüfung des Bestandsprozesses und die Ausarbeitung eines adaptierten, qualitätszentrierten Entwicklungsprozesses für Hardwarekomponenten (siehe Kapitel 7 auf Seite 101).

Die Kennwertermittlung kann nun, unter Anwendung des Prediktiv-Tools und der Prozessanpassungen, praktisch ohne weiteren Aufwand auf beliebige Bau-

gruppen angewendet und somit auch gezielt zur Schaltplanoptimierung und zur Eliminierung von Qualitäts-Schwachstellen herangezogen werden.

Die Vorschläge zur Prozessanpassung und der neue Prozessansatz wurden der Hardware-Entwicklungsabteilung vorgestellt. Die Rückmeldungen waren positiv und die Änderungsvorschläge wurden in weiten Teilen als schlüssig beurteilt. Tatsächliche Umstellungen und die Überprüfung der Auswirkungen sind während des praktischen Teils dieser Arbeit nicht erfolgt.

Make or Buy

Zum Abschluss der Bewertung wird noch kurz versucht, die interessante Frage abzuwägen, wie die Investition in Aufwand und Zeit zur Entwicklung eines eigenen Werkzeugs, im Vergleich zum Kauf eines kommerziellen Tools abschneidet.

Hinsichtlich Prozess und Know-How im laufenden Betrieb, sind die beiden Herangehensweisen als gleich aufwändig zu bewerten. Qualitätszentrierte Entwicklung, speziell im Sicherheitsbereich, benötigt solides Wissen und Training von mehreren Fachleuten.

Der Vorteil einer Kauflösung ist klar die Vielfalt an Methoden und Datenbanken die dem Anwender zur Verfügung gestellt wird. Es ist davon auszugehen, dass diese gut verifiziert sind und somit mit hohem Vertrauen verwendet werden können. Updates, Patches und Neuerungen werden kostenpflichtig zur Verfügung gestellt. Die Einzelberechnung, inklusiv Export der Stücklisten, ist als zeitaufwändiger zu beurteilen, das steigert die Hemmschwelle zur regelmäßigen Anwendung parallel zur Entwicklung. Weiterer Nachteil ist, zumindest bei den betrachteten Lösungen, das erhöhte Risiko von Fehlern durch die manuelle Übertragung von Stücklisten und Kenndaten.

Dem gegenüber stehen bei der Eigenentwicklung die Anpassbarkeit an Wünsche und Bedürfnisse und die tiefe Einbettung in den “normalen” Arbeitsalltag des HW-Entwicklers. Die Berechnungsgeschwindigkeit sollte sich die Waage halten und ob zusätzliche Methoden und Datenbanken benötigt werden, hängt vom Einsatz ab. Die Investition, um das Werkzeug erstmal in Produktivzustand zu bringen, ist begrenzt und einfach zum Vergleich dem Kaufpreis für ein kommerzielles Werkzeug gegenüberzustellen. Zu berücksichtigen ist, dass anstatt jährliche Lizenzkosten zu entrichten, zumindest ein Fachmann mit Programmierkenntnissen auf Dauer für Instandhaltung und Aktualisierung bereitzuhalten ist. Großes Plus der Eigenentwicklung ist die sehr intensive Beschäftigung mit dem Fachgebiet an sich und den Algorithmen speziell. Dieses Wissen ist auch neben der Weiterentwicklung des Werkzeugs eine große Hilfe im Entwicklungsalltag.

Fazit: Einen klaren Sieger gibt es nicht. Abhängig von strategischen Anforderungen und wirtschaftlichen Möglichkeiten, überwiegen die Vorteile der einen oder anderen Lösung. Ein Entscheidungskriterium kann auch die Größe des Entwicklungsbetriebs sein. Besteht bereits ein Team gut ausgebildeter Qualitätsmanager und sind sicherheitsrelevante Entwicklungen keine Besonderheit, dann kann ohne Bedenken ein kommerzielles Produkt eingesetzt werden. Steht der Betrieb erst am Beginn der qualitätszentrierten Entwicklung, dann überwiegt aus Sicht des Autors der Lerneffekt, den eine Eigenentwicklung mit sich bringt.

10. Ausblick

Prediktiv-Werkzeug

Die nicht im Rahmen dieser Arbeit umgesetzten Anforderungen an das computergestützte Werkzeug sind in Anhang B.1 auf Seite 175 zu finden. Anregungen für weitere Verbesserungen des Prediktivwerkzeugs und des Prozesses sind in Abschnitt 8.6 auf Seite 159 aufgelistet.

Prozess

Ein sehr interessanter Bereich wäre die Beobachtung der praktischen Einführung des Prozesses und die weitere Beschäftigung mit dessen Auswirkungen. Unabhängig davon, ob ein kommerzielles oder das hier umgesetzte Werkzeug verwendet wird, wäre eine Langzeitstudie zum Einfluss des vorgestellten, adaptierten Entwicklungsprozesses auf Ausfallraten, Qualität, Rückläuferanzahl, Preis und mögliche Zeitersparnisse in der Umsetzung von Baugruppen sehr interessant.

Korrektheit und Einsatz absoluter Kennwerte

Eine wichtige Erkenntnis im Rahmen dieser Arbeit war, dass Relativbewertungen zwischen Baugruppen, bei bekannten Ermittlungsmethoden, identischen Voraussetzungen und Kennwerten sehr hilfreich und verlässlich sind. Bei guter “Eichung” mittels verifizierter Methoden, wie z.B. Laufzeitendtests, sind diese auch für Absolutbewertungen einsetzbar. Ansonsten sind Absolutwerte für Ausfallsraten mit Vorsicht zu behandeln.

Die Beschäftigung mit der Absolutgenauigkeit von prediktiven Verfügbarkeitsmodellen scheint auch in der Forschung noch nicht abgeschlossen, obwohl es zum Thema bereits Literatur, Untersuchungen und sogar Standards gibt. Vor allem im Bereich automotiver Elektronikfertigung, Raumfahrt und Luftfahrt ist sehr viel Theorie aufgearbeitet und es stehen auch Datensammlungen über Jahrzehnte zur Verfügung. Doch die Abweichungen zwischen Vorgaben und Modellen der unterschiedlichen Anwendungen und Normen sind sehr hoch. Es bleibt also die Frage, weshalb bisher kein vereinheitlichtes Modell verwendet

wird? Eine weitere Frage ist, wie eine signifikante Genauigkeitserhöhung in kleinen und mittelständischen Fertigungsbetrieben erzielt werden kann, unter Berücksichtigung der verhältnismäßig kleinen Stückzahlen? Könnte in Folge dadurch die Wirtschaftlichkeit und Wettbewerbsfähigkeit maßgeblich verbessert werden oder ist der Effekt zu vernachlässigen?

Ansätze könnten praxisorientiert erfolgen, auf Basis von Rückläuferdaten mit erhöhter Genauigkeit, aber auch beispielsweise mit der genauen Beschäftigung von Ursprung, Idee und Ermittlung der unterschiedlichen Kennwertdatenbanken als Ausgangspunkt.

Anhang A.

Zuverlässigkeit und Sicherheit - Fortsetzung

A.1. Unfälle und Auswirkungen

Nachfolgende Tabelle gibt einen Überblick zu ausgesuchten Unfällen und Unfall-Statistiken der letzten 100 Jahre. Die Auswahl der aufgeführten Katastrophen erfolgte nicht nach deren medialer Größenordnung, sondern aufgrund des Einflusses, welchen die Erkenntnisse aus diesen Ereignissen direkt oder indirekt auf die Sicherheitstechnik hatten. Die angeführten Beispiele führten zu neuen und zusätzlichen Bestimmungen in deren Anwendungsgebieten, zu Gesetzen und Verordnungen, wie beispielsweise der Maschinenrichtlinie.

Die Angaben zu wirtschaftlichen Auswirkungen erfolgen dabei zum Zeitwert in der, sofern nicht anders angegeben, zur Zeit des Unfalls üblichen Orts- bzw. Konzernwährung.

Bereich	Unfälle	Zeitraum / Opfer / Schäden / Auswirkungen
Flugzeugindustrie	zahlreiche Abstürze und Zwischenfälle	seit 1946 erfasst < 1000 direkte und indirekte Opfer (Verletzte und Tote); finanzielle Schäden jeweils mehrere Mio. $, exklusiv Entschädigungen [a]
Raumfahrt	Challenger-Absturz	1986, Verlust von 7 Personen; 1,7 Mrd $ für Shuttle [b]; Erhöhung der Startkosten nach Unfall um mehr als 10% auf ca. 400 Mio $ [c]; 32 Monate kein Start

a Genaue Übersicht siehe: https://aviation-safety.net/statistics/

b Kosten für den Bau des Space Shuttle Endeavour als Ersatz für die Challenger (http://www.nasa.gov/centers/kennedy/about/information/shuttle_faq.html) entsprechen einem ungefähren Zeitwert von 3.5 Mrd. $ (2011).

c Die Kostenangaben zu den Space Shuttle Missionen stammen in Ermangelung offizieller Daten aus dem Raumfahrtblog von Bernd Leitenberger (http://www.bernd-leitenberger.de/blog/2009/09/07/ein-space-shuttle-start-kostet-790-millionen-dollar/).

	Columbia-Absturz	2003, Verlust von 7 Astronauten Verlust des Shuttles, bis 2005 keine Starts; Deutliche Erhöhung der Komplexität der Start- und Landevorbereitungen (Untersuchung der Schaumstoffteile am Boden, Keramikschutzschicht im Orbit) führten zur Startkostenerhöhung auf knapp 600 Mio. $; 2011 Abbruch des Space Shuttle Programms
Atomindustrie	Three Mile Island, US [d]	1979, keine direkten Todesopfer, Folgen der Strahlenbelastung bis heute unter Beobachtung [e]; Dekontamination von 1979 bis 1993, Kosten ca. 1 Mrd. US $ INES 5 [f]
	Tschernobyl, Russland	1986, mehrere Dutzend Todesopfer direkt (Aufräummannschaft - Liquidatoren), indirekte Opfer: offizielle Zahlen nicht bekannt, zahlreiche (spekulative) Artikel verfügbar; Absiedlung von mehr als 300 000 Menschen, Kontamination von mehr 200 000 km^2 Landfläche (eingeschränkt nutzbar, tw. dauerhaft nicht mehr verwendbar); Wirtschaftlicher Schaden viele Mrd. US $; Intransparenz führte (auch) zur Einführung der INES-Bewertung INES 7
	Fukushima, Japan	2011, direkte und indirekte Anzahl der Verletzten und Todesopfer unbekannt; Evakuierung von ca. 170 000 Einwohnern (großteils dauerhaft); Eindämmung und Entsorgung der zerstörten Reaktorblöcke dauert an; unterschiedliche Schätzungen gehen von Schadenshöhen um 150 Mrd. EUR aus; Weltweite Initiativen zum Atomausstieg (z.B. DE) INES 7

d Zusammenfassungen des NRC (https://www.nrc.gov/reading-rm/doc-collections/fact-sheets/3mile-isle.html) und der IAEA (https://www.iaea.org/sites/default/files/publications/magazines/bulletin/bull21-5/21502795459.pdf) beleuchten unterschiedliche Sichtweisen

e Joseph Mangano, 2004: Three Mile Island: Health Study Meltdown (http://journals.sagepub.com/doi/full/10.2968/060005010)

f INES-Einstufung: https://www.iaea.org/topics/emergency-preparedness-and-response-epr/international-nuclear-radiological-event-scale-ines

Chemische und petrochemische Industrie	Seveso, Italien	1976, keine direkten menschlichen Verluste, 200 Vergiftete, Folgewirkungen unter Beobachtung[g]; direkt Millionenstrafen, indirekte Entgiftungs- und Deponiekosten in unbekannter Höhe
	Bhopal, Indien	1984: Deutlich mehr als 1 000 direkte Todesopfer, ca. 500 000 Verletzte, Folgewirkungen nicht vollständig bekannt[h]; Mehr als 700 Mio. US $ Strafe (1989)
Medizintechnik	Therac 25[i]	1985 . . . 1987, medizinischer Linearbeschleuniger 3 Tote, 3 Schwerverletzte, Kosten unbekannt; Ursache: Fehlerhafte Software
Automobilindustrie	jährlich	Pannenstatistiken 80er/90er (DE vs. JPN); Rückrufaktionen aller Marken weltweit (mehrere 100 000 Autos pro Jahr); Direkt und indirekt damit verbundene Unfälle mit und ohne schwerwiegende Folgen für Leib und Leben (keine offiziellen Zahlen verfügbar). Kosten für Rückrufe allein: hunderte Millionen EUR pro Jahr
Arbeitsunfälle[j]	Österreich	Jährlich ca. 100 000 Arbeitsunfälle Berufstätiger, davon 111 tödlich (2017, Tendenz rückläufig)[k] Durchschnittskosten pro Arbeitsunfall betragen 5 000 EUR (Quelle: AUVA Wien, 2018)
	Deutschland	Jährlich ca. 800 000 geschädigte Personen in DE (Arbeitsunfähigkeit von mehr als 3 Tagen oder Tod als Folge); volkswirtschaftlicher Schaden in Milliardenhöhe

g P. A. Bertazzi, et al.: The Seveso studies on early and long-term effects of dioxin exposure: a review. https://www.ncbi.nlm.nih.gov/pubmed/9599710?dopt=Abstract

h Offizielle Zahlen nur spärlich vorhanden und tw. im Original nicht mehr auffindbar: https://web.archive.org/web/20120518020821/http://www.mp.gov.in/bgtrrdmp/relief.htm

i Originaluntersuchungsbericht: https://web.stanford.edu/class/cs240/old/sp2014/readings/therac-25.pdf, Kurzfassung: http://sunnyday.mit.edu/papers/therac.pdf

j Gesamteuropäische Statistiken sind via eurostat abrufbar: https://ec.europa.eu/eurostat/de/web/health/health-safety-work/data/database

k Quelle: AUVA, Auszug aus der Statistik 2017 https://www.auva.at/cdscontent/load?contentid=10008.633448&version=1526981135
Statistik Austria: http://www.statistik.at/web_de/statistiken/menschen_und_gesellschaft/gesundheit/unfaelle/arbeitsunfaelle/026374.html

Schweiz	Jährlich mehr als 250 000 neu registrierte Berufsunfälle mit mehr als 100 Toten, volkswirtschaftlicher Schaden > 1,5 Mrd. CHF pro Jahr[1]

Tabelle A.1.: Prominente Beispiele für Unfälle und deren Auswirkungen, sortiert nach Anwendungsgebieten

A.2. Lebensdauerbetrachtung

Der Hersteller eines Produktes möchte möglichst früh, möglichst genaue Informationen zu den Kenngrößen bezüglich Qualität und Zuverlässigkeit in Erfahrung bringen. In der nachfolgenden Tabelle sind, eingeteilt nach den Phasen der Weibullverteilung (siehe Abbildung 2.4 auf Seite 21), einige Probleme und Lösungsansätze im Zusammenhang mit diesem Thema aufgelistet.

I Frühausfälle	
Wann erfolgt Übergang in die Phase II?	Die genaue Bestimmung dieses Zeitpunkts ist ein *offenes Problem* der Zuverlässigkeitstheorie!
Wie kann Phase I beschleunigt werden?	*Run In* bzw. *Burn In* jedes auszuliefernden Produkts.
II Ausfälle mit (beinahe) konstanter Ausfallrate	
Wie kann die Nutzungsdauer dieser Phase maximiert werden?	Qualitätsorientierte Entwicklung, Auswahl entsprechender Bauteile, Derating, d.h. Bauteile arbeiten (deutlich) unter dem maximalen Arbeitspunkt
Wie kann die konstante Ausfallsrate minimiert werden?	Schaltungen so einfach als möglich halten, Derating
Wann ist Ende der Phase erreicht?	Abschätzung kann mittels *Ermittlung der kritischen Bauteile* (Stresstests wie HALT/HASS) erfolgen. *Lebensendtests* sind deutlich aufwändiger, aber auch genauer.
Reparatur- und Ausfallerfassung	
Wie bekomme ich möglichst genaue und vollständige Reparatur- und Rücklieferdaten?	Einbindung der Kunden, detaillierte Suche nach Fehlerursachen, genaue Erfassung von Betriebsdaten (Umgebungstemperatur und -feuchte, tatsächliche Betriebszeiten)
III Alterungsausfälle	

1 Quelle: Fünfjahresberichte der Unfallversicherung UVG https://www.unfallstatistik.ch/

Was sind die maßgeblichen Faktoren (Bauteile) für diese Ausfälle und wie können diese bestimmt werden?	Stresstests, statistische Erfassung der Systeme im Feld
Maßnahmen in Wartung und Reparatur, welche den Beginn und die Steilheit der Ausfallsrate positiv beeinflussen?	Reparaturpläne die in Kombination wirtschaftlicher Erwägungen mit Zeitabschätzungen der maximalen Lebensdauer eine Abwägung zwischen Reparatur und Ersatz treffen.

Tabelle A.2.: Problemstellungen und Lösungsansätze bzw. konkrete Maßnahmen im Zusammenhang mit der Bestimmung von Qualitäts- und Zuverlässigkeitskenngrößen auf Basis der Weibullverteilung

Anhang B.

Ergänzende Informationen zum Berechnungswerkzeug

B.1. Gesammelte Anforderungen

Die *Prozessanforderungen bzw. -verbesserungen (PR)*, deren Mehrzahl in Kapitel 7 auf Seite 101 genau beschrieben sind, und die Vorgaben an das Prediktions-Werkzeug (*Technischen Requirements TR*) sind in den nachfolgenden Tabellen entsprechend aufgeteilt.

B.1.1. Prozessanforderungen

PR Nr.	Titel	Abschnitt
1	Wiederaufnahme der Kennwertermittlung	5.1.2 auf Seite 82
2	Kennwert-Standards elektronisch verfügbar	5.1.3 auf Seite 85
3	Hersteller-Kennwerte elektronisch verfügbar	5.1.3 auf Seite 85
4	Elektronische Erfassung von Bauteil-Zuverlässigkeitsdaten	5.1.3 auf Seite 85
5	Altersausfälle berücksichtigen	7.1 auf Seite 106
6	Zuverlässigkeits-Kenndaten verfügbar machen	7.1 auf Seite 107
7	Zuverlässigkeits-Grenzwerte definieren	7.1 auf Seite 107
8	Definition und Einführung einer Bauteil-Kennwerte-Datenbank	7.1.2 auf Seite 112
9	Definition einer Vorschrift zur Auswahl qualifizierter Bauteile	7.1.2 auf Seite 114
10	Erstellung einer Vorschrift zur Qualifizierung von Bauteilen	7.1.2 auf Seite 114
11	Kennwert-Datenbank im Schaltplan- und Layout-Prozess verankern	7.1.3 auf Seite 117

12	Wissens-Datenbank für Produkte und Komponenten anlegen	7.1.3 auf Seite 117
13	Evaluierung der FMEA- und Prediktions-Werkzeug-Einführung	7.1.3 auf Seite 117
14	Richtlinie für Verfügbarkeitsgrenzwerte von Komponenten, Produkten und Produktgruppen definieren	7.1.4 auf Seite 124
15	Schulung zur Zuverlässigkeitstheorie	7.1.4 auf Seite 125
16	Design Reviews	7.1.4 auf Seite 125
17	Richtlinie zur Erstellung einer FMEA	7.1.4 auf Seite 125
18	Detaillierte Einträge in Bauteil-Kennwert-Datenbank	7.1.4 auf Seite 125
19	Reparatur-Rückläufer: Einfache Einsatzzeit-Erfassung	7.1.5 auf Seite 126
20	Reparatur-Rückläufer: Genaue Einsatzzeit-Erfassung	7.1.5 auf Seite 127
21	Reparatur-Rückläufer: Austausch kritischer Komponenten/Bauteile	7.1.5 auf Seite 127
22	Austausch kritischer Bauelemente: Hinweispflicht der Entwicklung	7.1.5 auf Seite 127
23	Reparatur-Rückläufer: Kundenspezifische Auswertung	7.1.5 auf Seite 127
24	Reparatur-Rückläufer: Kunden zur Datenlieferung animieren	7.1.5 auf Seite 127
25	Hochwertige Auswertung - Temperatur-Erfassung	7.1.5 auf Seite 128
26	Hochwertige Auswertung - Zusatz-Sensorik	7.1.5 auf Seite 128
27	Gegenüberstellung Theorie - Praxis	7.1.5 auf Seite 128
28	Erhöhte Anforderungen an gemeinsame Komponenten definieren und umsetzen	7.2 auf Seite 132
29	Reparatur-Rückläufer: Besondere Beobachtung gemeinsamer Komponenten	7.2 auf Seite 132
30	Bauteilauswahl: Derating als Vorgabe	7.2 auf Seite 133
31	Kühlkonzept optimieren	7.2 auf Seite 133
32	Alarmierung/Abschaltung bei Übertemperatur	7.2 auf Seite 133
33	Schaltplan-Richtlinien	8.6 auf Seite 160
34	Gesamtbaugruppen in einer Schema-Datei	8.6 auf Seite 160

Tabelle B.1.: Übersicht aller gesammelten Prozessanforderungen

B.1.2. Umgesetzte Anforderungen

Die Listen in diesem und im nächsten Abschnitt verweisen auf *zusätzliche Anforderungen* die sich im Laufe der Ausarbeitung ergeben haben.

Anforderungen die sich durch die Beschreibung der Benutzerszenarien (Abschnitt 8.1 auf Seite 138), der Auswahl der Berechnungsmethoden (siehe 8.2 auf Seite 142) und als Resultat des Berechnungsablaufs (Abschnitt 8.3 auf Seite 146) ergeben, sind nicht nochmals aufgeführt.

TR Nr.	Titel	Abschnitt
1	Kennwerte der Sicherheits- und Standardtechnik berücksichtigen	2.3.2 auf Seite 39
2	Teilberechnungen unter alternativer Temperaturvorgabe	4.2.5 auf Seite 70
3	Hot-Spot Berechnung	4.2.5 auf Seite 70
4	Bauteilerfassung: Zeitaufwand minimieren	5.1.3 auf Seite 85

Tabelle B.2.: Übersicht der realisierten Anforderungen an das Prediktionswerkzeug

B.1.3. Zukünftige Verbesserungen

Nachfolgend die gesammelten Wünsche und Anforderungen die nicht im Rahmen der *proof of concept* Umsetzung des Berechnungswerkzeugs realisiert wurden.

TR Nr.	Titel	Abschnitt
5	Temperaturabhängigkeit der Bauteile berücksichtigen	8.1.5 auf Seite 140
6	Möglichkeit zum manuellen Eingriff	8.1.5 auf Seite 140
7	Erweiterungen/Änderungen von Bauteilbeschreibungen übernehmen	8.1.5 auf Seite 140
8	Anpassungsfähigkeit des Werkzeugs	8.1.5 auf Seite 140
9	Einfache Handhabung bei Bedienung und Administration	8.1.5 auf Seite 140
10	Unterscheidung von Baugruppenvarianten im Designwerkzeug	8.4 auf Seite 157
11	Verwaltung von Schaltplanversionen	8.4 auf Seite 157
12	Modulare Extrahierungs- und FMEA-Methode	8.6 auf Seite 159
13	Vollständige Temperaturberechnung	8.6 auf Seite 159

14	Berücksichtigung Impuls-/Digitalbetrieb	8.6 auf Seite 159
15	Berücksichtigung der RunIn Phase	8.6 auf Seite 159
16	Markierung kritischer Bauelemente	8.6 auf Seite 160

Tabelle B.3.: Prediktionswerkzeug: Übersicht zukünftiger Verbesserungen

B.2. Eingangsdaten und Ergebnisdateien

Neben der Beschreibung des Werkzeugs und verschiedener Benutzerszenarien in Kapitel 8.3 auf Seite 146, sind nachfolgend weitere wichtige Teile des Prediktions-Werkzeugs kurz beschrieben.

B.2.1. Templates

Vorlage für Bauteilkennwert-Datenbank

Die Vorlage (Abb. B.1 auf Seite 180) folgt einem simplen, manuell einfach wartbaren Schema als Excel-Tabelle. Der Vorteil ist dabei, neben der Durchgängigkeit der verwendeten Office-Anwendungen, vor allem die Lesbarkeit. Gerade während der Umsetzung konnten somit Fehler leicht gefunden bzw. ausgeschlossen werden.

Der Aufbau ist wie folgt:

Präambel Nach der Überschrift folgen drei Zeilen mit den Angaben zu relevanten Spaltenbezügen. Zuerst der Bezug zu den Bauteilkennwerten (`FR_PartCols`), dann das Suchkriterium (`FR_DescCols`, entspricht hier der Kurzbenennung). Abschließend die Angabe der Ausfallrate unter Einsatzbedingungen (`FR_LambdaCols`).
Die grau hinterlegte Überschriftszeile dient der Lesbarkeit und der Beschreibung der Spalten.

Bauteil-Kennwertgruppen Pro Bauteiltyp gibt es jeweils eine Kennwertgruppe, welche immer aus zwei Hilfszeilen mit Zeilenbezügen und den eigentlichen Bauteilkennwertzeilen besteht. Der erste Hilfseintrag steht für die Zeilennummer wo die Gruppe beginnt (`FR_[X]_Rows`), der zweite für die Anzahl der Einträge (`FR_[X]_RowCount`). `[X]` steht dabei jeweils für den Bauteiltyp. Die einzelnen Einträge entsprechen den tatsächlich verwendeten Bauteiltypen und die Kurzbenennung sollte mit der Beschreibung im Schaltplan-Editor übereinstimmen. Der erste Eintrag pro Bauteiltyp entspricht immer dem Standard-Eintrag, welcher bei fehlgeschlagener Suche nach der Kurzbenennung im FMEA-Tabellenblatt angezeigt wird.

ANMERKUNG: *Bei einer Erweiterung ist zu beachten, dass sämtliche Angaben lediglich zur besseren Kontrolle in der Tabelle dargestellt werden. Die Zeilen- und Spaltenangaben sollten nicht manuell verändert werden. Diese werden automatisch berechnet und sind als "Namen" in Excel hinterlegt. Sämtliche Skripte greifen darüber auf die Inhalte zu.*
Weitere Bauteile können einfach durch Copy/Paste oder durch Einfügen einer Zeile in eine Gruppe hinzugefügt werden. Lediglich bei Einfügen eines komplett neuen Bauteiltyps muss dieser auch im Skript hinterlegt werden.

ANMERKUNG: *Für die beispielhafte Realisierung war das Format vorteilhaft, für eine weitergehende und umfangreichere Verwendung sollten die Kennwertdaten in einer echten Datenbank erfasst werden.*

Stücklistenvorlage

Abbildung B.2 auf Seite 181 zeigt die Vorlage zur Stücklistengenerierung. Die Vorlage ist direkt im Tabellenblatt selbst beschrieben. Hier werden deshalb nur weiterführende Informationen gegeben:

Generell Die Vorlage folgt dem Schema, dass in der ersten Spalte der Variablenname, dann der Wert bzw. Wertebereich und in der letzten Spalte die Beschreibung zu finden ist.

Zeile "CompAttr" Diese Zeile dokumentiert die Zuordnung der Bechreibungsvariablen zu den entsprechenden Spalten. Das heißt, dass das Skript zur Generierung jeder Ergebniszeile über die, in dieser Zeile angegebenen Namen, auf die Werte zugreift.

FMEA-Datenvorlage

Dem gleichen Schema folgt die Vorlage zur FMEA (Abb. B.3 auf Seite 182). Wiederum sind viele Einträge lediglich zur besseren Lesbarkeit angegeben und wie bereits zuvor geschildert, greifen die Programmteile über Variablen (in Excel "Namen" genannt) auf die Informationen zu.

Sämtliche Ergebniszellen und -variablen sind in der Variablenliste durch den Präfix `FMEA_` gekennzeichnet.

ANMERKUNG: *Sowohl bei der Stücklistenvorlage als auch bei der FMEA-Vorlage erfolgt die Generierung so, dass nach Anlage des Registerblatts und der Kopfzeilen, jeweils die Vorlagenzeilen aus dem Template kopiert und dann per Skript mit Werten befüllt werden. Damit sind Formatänderungen leicht machbar, indem im Template die gewünschten Anpassungen vorgenommen werden.*

Fehlerraten der verwendeten Bauteile nach SN29500 :

FR_PartCols 6
FR_DescCols 2
FR_LambdaCols 9

Kurzbenennung	Bauteiltyp	Bauform	Beschreibung	short circuit	open circuit	drift	Fehlerrate bei Einsatzbedingungen λ = λ(ref) * π(T) * π(U) * π(I) * π(Q)	Ba be t
FR_R_Rows 13								
FR_R_RowCount 5								
R	R	1206	R (1206) Resistor (61709)	20%	60%	20%	0,36	
R (0603)	R	603	metal film resistor	20%	60%	20%	0,36	
R (1206)	R	1206	metal film resistor	20%	60%	20%	0,36	
RN (1206)	RN	1206	Widerstandsnetzwerk 4 R	0%	40%	60%	0,72	
RM (1206)	RM	1206	minimelf metal film resistor	0%	40%	60%	0,36	
FR_L_Rows 21								
FR_L_RowCount 2								
L	L		L - Drossel	40%	40%	20%	10	
L (SMD 3,81 x 3,81)	L		Speicherdrossel 1,8 uH für Schaltregeler	40%	40%	20%	10	
FR_C_Rows 26								
FR_C_RowCount 9								
C	C	1206	C (1206) Kondensator (61709)	70%	10%	20%	5,9	
C (2220) X7R	C	2220	Keramikkondensator X7R	70%	10%	20%	5,9	
C (1812) X7R	C	1812	Keramikkondensator X7R	70%	10%	20%	1,76	

n	Basisfehlerrate bei Referenz-temperatur λ(ref)	Σπ	π(T)	π(U)	Berechnungen nach SN29500
06					
36	0,2	1,8			R(0603) maximale Umgebungstemp. 60°C (80 innen) λ = λ(ref) * π(T) nach SN29500: 0,36 = 0,2 * 1,8
36	0,2	1,8			R(1206) maximale Umgebungstemp. 60°C (80 innen) λ = λ(ref) * π(T) nach SN29500: 0,36 = 0,2 * 1,8
72	0,4	1,8			RN maximale Umgebungstemp. 60°C (80 innen) λ = λ(ref) * π(T) nach SN29500: 0,72 = 0,4 * 1,8
36	0,2	1,8			RN maximale Umgebungstemp. 60°C (80 innen) λ = λ(ref) * π(T) nach SN29500: 0,36 = 0,2 * 1,8
10					
10	10	1			λ(ref)
5,9					
5,9	2	2,95			X7R schlechteste Falle U=36V und Umax=100V maximale Umgebungstemp. 60°C (80 innen) λ = λ(ref) * π(U) * π(T) * π(Q) nach SN29500: 5,896 = 2 * 0,67 * 4,4 * 1
76	2	0,88			X7R Umax=1000V (normal wenige Volt) maximale Umgebungstemp. 60°C (80 innen) λ = λ(ref) * π(U) * π(T) * π(Q) nach SN29500: 1,76 = 2 * 0,2 * 4,4 * 1

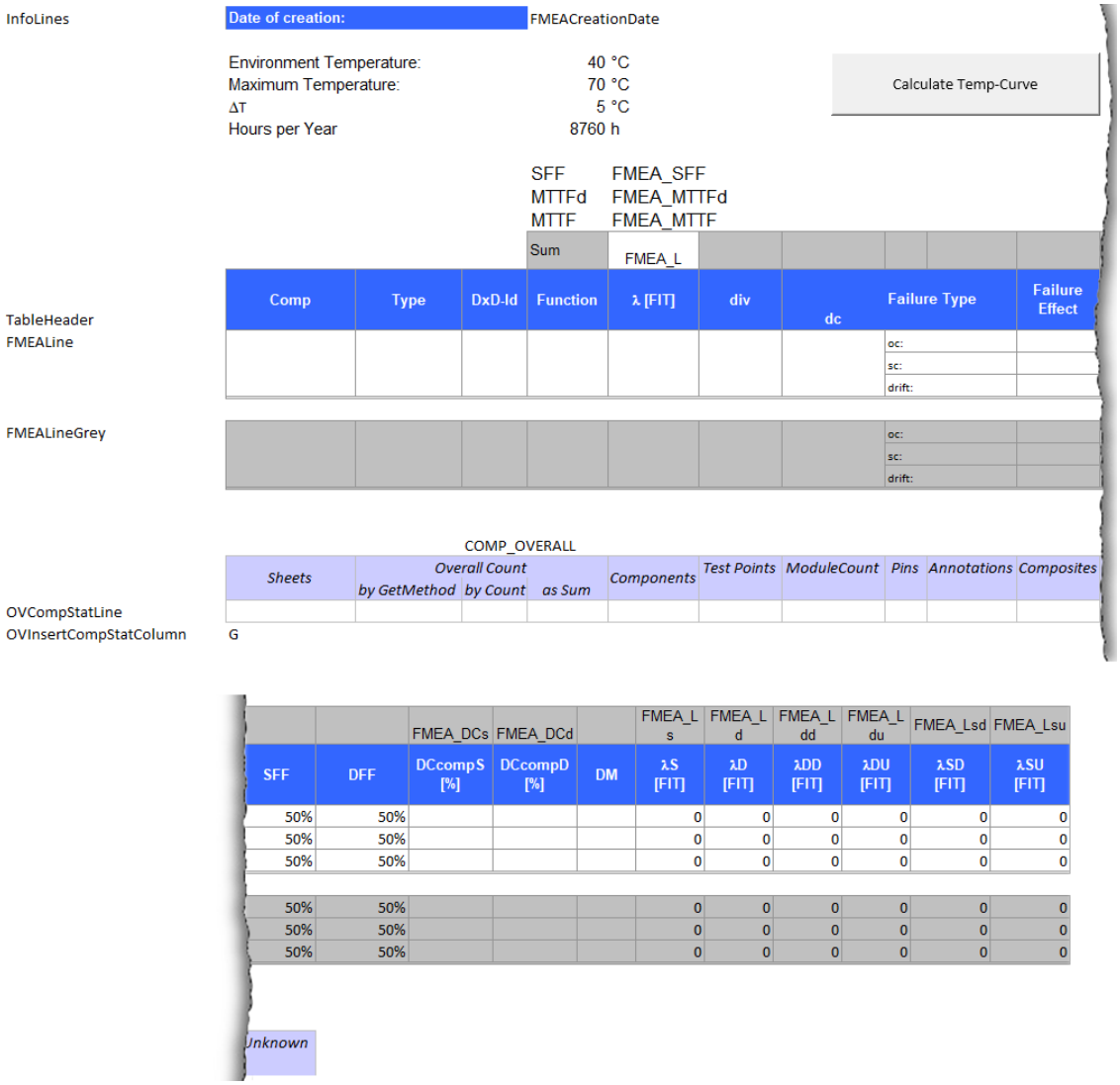
Abbildung B.1.: Bauteilkennwert-Datenbank

AttrInfoRange	B2:G2		*Zellenbereich mit Informationen (der gesamte Bereich wird zuerst kopiert - in letzter Zeile, letzter Spalte wird immer automatisch das letzte Änderungsdatum eingetragen)*
AttrStartTableHeader	B9		*linke obere Ecke des Headers*
AttrStartTableRow		10	*1. Zeile des Tabelleninhalts*
AttrNum		12	*Anzahl der Attribute*
AttrStringCell	D13		*verweist auf Beginn der String-Vorlage*
AttrSortCell	C10		*nach welcher Zeile sortiert wird*

	Date of creation:	AttrCreationDate

	C	RefDes	Typ	Value	E-Num	Type	dT	Description	Pkg-Type	Datasheet	DxD-Sheet	DxD-UID
AttrTableHeader		DxDComp.RefDes	TYP	VALUE	E-NUMMER	TYPE	DTEMP	BESCHREIBUNG	PKG_TYPE	DATENBLATT	DxD.ActSheetName	DxDComp.Id
CompAttr												
AttrLine												
AttrLineGrey												
FMEAStartInfoHeader		B2						*linke obere Ecke des Infobereichs*				
FMEAStartTableHeader		B16						*linke obere Ecke des Headers*				
FMEAStartTableRow			17					*1. Zeile des Tabelleninhalts*				
FMEAInfoRange		D10:G11						*Zellenbereich mit Informationen (der gesamte Bereich wird zuerst kopiert - in letzter Zeile, letzter Spalte wird immer automatisch das letzte Änderungsdatum eingetragen)*				
FMEATableHeaderRange		D12:W12						*Zellenbereich des Headers (wird genau so kopiert*				
FMEALineNumLines			3									

Abbildung B.2.: Template zur Stücklistengenerierung



InfoLines

Date of creation:	FMEACreationDate

Environment Temperature:	40 °C
Maximum Temperature:	70 °C
ΔT	5 °C
Hours per Year	8760 h

Calculate Temp-Curve

SFF FMEA_SFF
MTTFd FMEA_MTTFd
MTTF FMEA_MTTF

TableHeader
FMEALine
FMEALineGrey

			Sum	FMEA_L					
Comp	Type	DxD-Id	Function	λ [FIT]	div	dc	Failure Type		Failure Effect
							oc:		
							sc:		
							drift:		
							oc:		
							sc:		
							drift:		

COMP_OVERALL

Sheets	Overall Count			Components	Test Points	ModuleCount	Pins	Annotations	Composites
	by GetMethod	by Count	as Sum						

OVCompStatLine
OVInsertCompStatColumn G

		FMEA_DCs	FMEA_DCd		FMEA_L s	FMEA_L d	FMEA_L dd	FMEA_L du	FMEA_Lsd	FMEA_Lsu
SFF	DFF	DCcompS [%]	DCcompD [%]	DM	λS [FIT]	λD [FIT]	λDD [FIT]	λDU [FIT]	λSD [FIT]	λSU [FIT]
50%	50%				0	0	0	0	0	0
50%	50%				0	0	0	0	0	0
50%	50%				0	0	0	0	0	0
50%	50%				0	0	0	0	0	0
50%	50%				0	0	0	0	0	0
50%	50%				0	0	0	0	0	0

Unknown

Abbildung B.3.: FMEA Berechnungsvorlage

B.2.2. Format der Ergebnisdateien

Wie in Abschnitt 8.3 auf Seite 146 beschrieben, generiert jeder Extrahierungslauf, neben der Ergebnisdatei im Excel-Format, auch eine Protokolldatei. Die Namensgebung für die zwei generierten Dateien ist wie folgt:

1) `[Schema-Name]_[Timestamp].xlsm`
2) `ExamineAvailability_[Timestamp].log`

Der Zeitstempel der beiden Dateien ist für einen Berechnungslauf identisch und auch innerhalb der Protokolldatei zu finden. Die Ergebnisdatei des Berechnungsablaufs wird in Kapitel 8.3.1 auf Seite 148 im Detail beschrieben. Aufbau und Inhalt der Protokolldatei werden nachfolgend erläutert.

Protokoll-Datei

Das nachfolgende Listing stellt die Ausgabe einer erfolgreich durchgeführten Berechnung dar.

```
1  II 27.01.2011 09:05:26: C:ArgumentHandler: ProcessPathArgs():
     II : commandline arguments:  /action:Generate /selection:all
         /method:PartsCount /workpath:D:\DA\Software\Scripts\WorkDir\
         MS_Office_2003 /logpath:D:\DA\Software\Scripts\WorkDir\MS_Office_2003\
         Log
     II : LogPath:                D:\DA\Software\Scripts\WorkDir\MS_Office_2003\
         Log
     II : WorkPath:               D:\DA\Software\Scripts\WorkDir\MS_Office_2003

6  II 27.01.2011 09:05:26: C:ArgumentHandler: ProcessWorkerArgs():

   II 27.01.2011 09:05:26: C:DxdApp: Initialize():

   --> Script Infos
11 ----------------
     Script Name:                 ExamineAvailability.vbs
     Script Path:                 D:\DA\Software\Scripts\MA\
   <-- Script Infos

16 II 27.01.2011 09:05:28: C:EnVarHandler: Initialize():
     II : Script Location:        D:\DA\Software\Scripts\MA\
     II : UserTemplatePath:       D:\DA\Software\Scripts\MA\Excel-Templates\
     II : Full Template Path:     D:\DA\Software\Scripts\MA\Excel-Templates\
         ExcelTemplate_DE.xls

21 II 27.01.2011 09:05:28: C:MyExcelEnv Initialize():
     II : TemplatePath:           D:\DA\Software\Scripts\MA\Excel-Templates\
     II : WorkPath:               D:\DA\Software\Scripts\WorkDir\MS_Office_2003\
     II : DataTemplate:           D:\DA\Software\Scripts\MA\Excel-Templates\
         FMEA-Settings.xls
     II : DataTemplate call:      D:\DA\Software\Scripts\MA\Excel-Templates\[
         FMEA-Settings.xls]
26   II : GenPartsCount(): calling Sub GenPartsCount all
```

```
II 27.01.2011 09:05:28: C:DxdApp: getPrjInfo():
DxD-Info
  II : ViewDraw Version:        2007.9.0
  II : Project Name:            NT255B
  II : Project Path:            D:\DA\NoSync\BE Mentor-Schemas\NT255B
NT255B- Project Info
  II : Number of Boards:               1
  II :  Board-Names:
  II :                          nt255b
  II : Active Board:            nt255b
  II : Number of Schematics:    1
  II :  Schematic-Names:
  II :                          nt255b
  II : Active Schematic:        nt255b
  II : Number of Sheets:               4
  II :  Sheet-Names:
  II :                          1
  II :                          2
  II :                          3
  II :                          4
  II : Active Sheet:    1

II 27.01.2011 09:05:28: C:MyExcelEnv prepNewPrj():
  II : Full Work Path:          D:\DA\Software\Scripts\WorkDir\MS_Office_2003\
      NT255B_27_01_2011__09_05_28.xls

II 27.01.2011 09:05:30: C:OVSheet Create():
  II : Template version:               1.0

II 27.01.2011 09:05:45: C:MyExcelEnv prepareFMEA():

--> Session Infos
-----------------
  Script Start:                 27.01.2011 09:05:26
  Script End:                   27.01.2011 09:05:45
  DxD Extraction time:          19,4707
<-- Session Infos
```

Die Generierung der Log-Datei erfolgt schrittweise und wird jeweils durch die aktuell aufgerufene Klasse selbst befüllt. Die erste Zeile einer intern ausgeführten Funktion hat immer die selbe Form:

```
[XX] [timestamp] C:[classname]: [function]
```

Dabei steht `[XX]` für die Kritikalitätsbewertung der ausgeführten Funktion und somit für die möglichen Auswirkungen auf den weiteren Ablauf:

II ... Information Ausführungsinformationen, zur Kontrolle des korrekten Ablaufs und der erwarteten Einstellungen (Projekt, Pfade, ...).

WW ... Warning Kann in Folge falsche Ergebnisse liefern und/oder in eine fehlerhaften Ausführung münden.

EE ... Error Verhindert weitere und/oder korrekte Ausführung.

`[classname]` steht für die gerade ausgeführte Klasse (in Beispielzeile 56 also `MyExcelEnv`) und `[function]` für die ausgeführte Funktion `prepareFMEA()`.

Informationen die innerhalb einer Funktion protokolliert werden, besitzen das selbe Prefix-Schema und sind um zwei Leerzeichen eingerückt.

Der Inhalt der Datei gliedert sich in die folgenden Teile:

Initialisierung Der Initialisierungsteil spiegelt den Kommandozeilenaufruf, welcher direkt via Prompt oder indirekt aus einem Programmteil übergeben wird (Zeilen 1 bis 5). Daraus werden die notwendigen Pfade und Ausführungsinformationen extrahiert. In den Zeilen 6-9 werden Vorbereitungsroutinen gestartet und initialisiert. Dabei werden Verfügbarkeit und Ausführungsrechte für Schaltplaneditor und die Tabellenkalkulation kontrolliert. Bei korrektem Ablauf wird zum Abschluss noch Name und Ausführungsort des zentralen Berechnungsskript ausgegeben (im Beispiel Zeilen 10-15).

Ausführung Zwischen Zeile 16 und 56 sind die verschiedenden Schritte eines Berechnungsvorgangs sichtbar. Vorbereitung mit Suche der Templates (16-24), Extrahierungsaufruf (26), Extrahierung im Schaltplaneditor mit Ausgabe von Projektinformationen (27-48) und abschließend die Zusammenstellung der Excel-Ergebnisdatei aus den Templates und extrahierten Informationen (50-56).

Zusammenfassung Das Ende eines erfolgreich durchgeführten Berechnungslaufs ist gekennzeichnet durch die zusammengefassten Laufzeitinformationen in den Zeilen 58-63.

B.3. Betriebssystem-Umgebung und Übergabeparameter

Die Arbeitsumgebungen für Anwendung und Programmierung sind in Kapitel 8.1.6 auf Seite 141 ff. beschrieben. Vorbereitungen der Systemumgebung und konkreter Aufruf der zentralen Skripte, inklusive Beschreibung der Übergabeparameter, sind nachfolgend zu finden.

Betriebssystem-Vorbereitungen

Bevor die VBScript Programme ausgeführt werden können, müssen folgende Vorbereitungen getroffen werden:

1. Setzen von Umgebungsvariablen/Pfaden:
   - Das *Excel-Template-Verzeichnis* für die Vorlagen von Kennwertdatenbank, Stücklisten- und FMEA-Format, muss mittels Umgebungsvariable `BE_AVAIL_EXCTMPLT` zur Verfügung gestellt werden.

- Das *Skript-Verzeichnis*, wo sich sämtliche VBScript Programmdateien befinden, wird in die Umgebungsvariable `BE_AVAIL_SCRIPTLOCATION` eintragen.

2. Im Script `menu.vbs`, welches das zusätzliche Berechnungsmenü im Schaltplaneditor einfügt, müssen die Variablen `Workpath` (für den Speicherort der Ergebnisdateien) und `Logpath` (für die Protokolldateien) eingetragen werden.

3. Sollten die Skripte aus dem Schema-Editor nicht starten, muss der Skriptpfad nochmals manuell im DxDesigner zu den ausführbaren Verzeichnissen hinzugefügt werden. Dazu startet man den Editor und trägt diese via Menü `Dashboard`, Untermenü `WDIR` im sich öffnenden Dialog entsprechend ein.

Programm-Übergabeparameter

Die Beschreibung der Übergabeparameter sind für die Anpassung und Erweiterung, aber auch für den Start der bestehenden Programme aus anderen Skripten oder von der Kommandozeile aus zu berücksichtigen.

Ein Beispielaufruf für die Generierung einer Berechnung vom Kommandozeilenprompt sieht wie folgt aus:

```
ExamineAvailability /action:Generate /selection:all /method:PartsCount
    /workpath:F:\MA\Scripts\WorkDir /logpath:F:\MA\Scripts\WorkDir\Log
```

Hier wird eine Gesamtberechnung nach Parts Count Methode, unter Angabe von speziellen Arbeits- und Protokollpfaden, durchgeführt.

Für bessere Kontrolle der Ausführungsschicht, sollte dieser Programmaufruf mittels `cscript` erfolgen. Damit wird sichergestellt, dass die *Windows Script Host* Umgebung verwendet wird. Mit der option `//nologo` werden störende Ausgaben des Skripting Hosts unterdrückt:

```
cscript //nologo ExamineAvailability.vbs /action:Generate /selection:all
    /method:PartsCount
```

Sämtliche Optionen des Start-Skripts sind nachfolgend aufgeführt:

```
ExamineAvailability
  /action:<Generate|Evaluate>
  /selection:<all|part>
  /method:<PartsCount|PartStress|61709>
  [/workpath:]
  [/logpath:]
```

ExamineAvailability Skript-Name des Hauptprogrammes.

/action Es kann zwischen `Generate` für die Extrahierung, Berechnung und Generierung der Ausgabedatei und `Evaluate` für eine Dummy-Ausführung zur Prüfung der Einstellungen ausgewählt werden. Dabei werden die Umgebungsvariablen, die Existenz der Skripte und auch die Pfadangaben geprüft. Es wird nicht versucht, Excel auszuführen oder die Templates tatsächlich zu laden. Bei erfolgreicher Ausführung wird eine Erfolgsmeldung ausgegeben und eine Protokolldatei zur Kontrolle angelegt. Bei Problemen wird entweder eine Fehlermeldung des Programmes oder ein Laufzeitfehler des Scripting Hosts ausgegeben. Die Protokolldatei sollte dann helfen, den Fehler einzugrenzen.

/selection Die beiden Optionen stehen für die Gesamtberechnung (`all`), unabhängig von bestehenden Selektionen, oder Teilberechnung (`part`) von ausgewählten Schaltungsteilen.

/method Angabe von `PartsCount` entspricht der Berechnung nach Parts Count Methode. Die Parameter `PartStress` und `61709` führen in der Beispielumsetzung, mit entsprechendem Hinweis, die selbe Berechnung durch. Diese wurden für eine entsprechende Erweiterung bereits vorgesehen.

Optional */workpath* Die optionale Angabe eines Pfads zur Ausgabe der Ergebnisse kann zum manuellen override oder generell anstatt der Angabe der entsprechenden Umgebungsvariable verwendet werden.

Optional */logpath* ... Funktion wie `/workpath`

Glossar

Die nachfolgenden Definitionen wurden, wo möglich, aus gültigen Normen und Standardwerken direkt übernommen. Wichtigste Quelle ist dabei der frei zugängliche Standard IEC60050-192 [IEC15]. Dieser bietet die Übersetzung von einschlägigen Begriffen in eine Vielzahl von Sprachen, sowie deren Definition in englischer Sprache. Um durch eigenhändige Übersetzung keine Fehler zu produzieren, wurden die Definitionen zwar gekürzt, aber in Originalsprache übernommen.

Ausfälle gemeinsamer Ursache *[en: common cause failures]* failures of multiple items, which would otherwise be considered independent of one another, resulting from a single cause
Note: The potential for common cause failures reduces the effectiveness of system redundancy.

Ausfall *[en: failure]* the termination of the ability of an item to perform a required function
A failure results in a fault (Fehler / Fehlzustand).
Note: "Failure" is an event, as distinguished from "fault", which is a state.

Ausfallrate λ *[en: (instantaneous) failure rate]* the limit, if it exists, of the quotient of the conditional probability that the instant of a failure of a non-repaired item falls within a given time interval $(t, t + \Delta t)$ and the duration of this time interval, Δt, when Δt tends to zero, given that the item has not failed up to the beginning of the time interval.
Note: An estimated value of the instantaneous failure rate can be obtained by dividing the ratio of the number of items which have failed during a given time interval to the number of non-failed items at the beginning of the time interval, by the duration of the time interval.
Note: Other terms for the instantaneous failure rate are "*hazard function*" and "*hazard rate*".

Dienstgüte *[en: quality of service]* Der Überbegriff der *Dienstgüte* bildet den Ausgangspunkt verschiedener Definitionen der Zuverlässigkeitstheorie.
[en: quality of service] the collective effect of service performance which determines the degree of satisfaction of a user of the service
Note: The quality of service is characterized by the combined aspects of service support performance, service operability performance, serveability performance, service integrity and other factors specific to each service.

Note: ISO defines “quality” as the ability of a product or service to satisfy user’s needs.

Fehlaussage *[en: error]* discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition
Note: An error within a system may be caused by failure of one or more of its components, or by the activation of a systematic fault.

Fehler / Fehlzustand *[en: error]* the state of an item characterized by inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources
Note: A fault is often the result of a failure of the item itself, but may exist without prior failure.

Fehlverhalten / Menschliches Versagen *[en: human error]* discrepancy between the human action taken or omitted, and that intended or required, e.g. performing an incorrect action; omitting a required action, miscalculation; misreading a value;
Note: In the deprecated version of the standard (-191) the term “mistake” was used.

Funktionale Sicherheit *[en: (functional) safety]* Die Funktionale Sicherheit ist der Teil der Gesamtsicherheit, bezogen auf die Maschine und das Maschinensteuerungssystem, die von der korrekten Funktion des sicherheitsbezogenen elektrischen oder elektronischen Steuerungssystems, sicherheitsbezogenen Systemen anderer Technologie und externen Einrichtungen zur Risikominderung abhängt.
Quelle: [IEC10]

Funktionsfähigkeit *[en: reliability]* ability to perform as required, without failure, for a given time interval, under given conditions
Note: Given conditions include aspects that affect reliability, such as: mode of operation, stress levels, environmental conditions, and maintenance.
DE: auch als Zuverlässigkeit bezeichnet (redundante Definition mit “dependability”)

Produkt *[en: product]* Der Begriff *Produkt* wird in Folge für ein aus Software, Hardware und Mechanikteilen aufgebautes Modul der Firma Bachmann electronic verwendet. Diese Bezeichnung wird aufgrund der Durchgängigkeit und der Zuordenbarkeit zu den Originaldokumenten des Entwicklungsprozesses beibehalten.
Das *Produkt*, wie hier beschrieben, entspricht in der Verfügbarkeitstheorie einem *System*, welches wiederum aus verschiedenen *Komponenten* zusammengesetzt ist, welche aus *Bauteilen* bestehen.

Qualität *[en: quality]* Der Grad, in dem ein Satz inhärenter Merkmale Anforderungen erfüllt.
Quelle: ISO 9000:2000

System *[en: system]* set of interrelated items that collectively fulfil a requirement *Note:* A system is considered to have a defined real or abstract boundary.
Note: External resources (from outside the system boundary) may be required for the system to operate.
Note: A system structure may be hierarchical, e.g. system, subsystem, component, etc.
Note: Conditions of use and maintenance should be expressed or implied within the requirement.

Überlebenswahrscheinlichkeit $R(t_1 t_2)$ *[en: reliability]* probability that an item can perform a required function under given conditions for a given time interval (t_1, t_2)
Note: Given conditions include aspects that affect reliability, such as: mode of operation, stress levels, environmental conditions, and maintenance.

Verfügbarkeit *[en: availability]* ability to be in a state to perform as required
Note: Availability depends upon the combined characteristics of the reliability (IEV 192-01-24), recoverability (IEV 192-01-25), and maintainability (IEV 192-01-27) of the item, and the maintenance support performance (IEV 192-01-29).

Zuverlässigkeit *[en: dependability]* ability to perform as and when required
Note: Dependability includes availability (IEV 192-01-23), reliability (IEV 192-01-24), recoverability (IEV 192-01-25), maintainability (IEV 192-01-27), and maintenance support performance (IEV 192-01-29), and, in some cases, other characteristics such as durability (IEV 192-01-21), safety and security.
Note: Dependability is used as a collective term for the time-related quality characteristics of an item.

Abkürzungsverzeichnis

Eine gute Quelle für Definition und Übersetzung von sicherheitstechnischen Begriffen ist die Siemens Schrift “Safety Integrated - Terms and Standards - Terminologie in der Maschinensicherheit“, auf welche, in der Version von 2007, bei den nachfolgenden Beschreibungen zurückgegriffen wurde.

CCF ..... *Fehler gemeinsamer Ursache* - Sicherheitstechnik
en: Common Cause Failure

CMMI ..... *Capability Maturity Model Integration*
Von der Carnegie Mellon University erfundenes und vermarktetes Referenzmodell zur systematischen Bewertung und Verbesserung bewährter Praktiken innerhalb eines Unternehmens.

DC ..... *Diagnosedeckungsgrad*
Sicherheitstechnik: DC = $\sum \lambda_{DD}/\lambda_D$ mit

- λ_{DD} Ausfallrate der detektierten gefährlichen Ausfälle
- λ_D Ausfallrate aller gefahrbringenden Ausfälle

en: Diagnostic Coverage

E/E/PES .... *Elektrisch/elektronisch/programmierbare elektronische Systeme*
en: electrical and/or electronic and/or programmable electronic technologies of safety related systems

EUC ..... *Equipment under Control*
Einrichtung, Maschine, Apparat oder Anlage, verwendet zur Fertigung, Stoffumformung, zum Transport, zu medizinischen oder anderen Tätigkeiten

FIT ..... *Failures in time*
Einheit der Ausfallrate in $[\frac{10^{-9}}{h}] \rightarrow$ PPM

FMEA ..... *Failure Modes and Effects Analysis*
Qualitative Methode zur Analyse von Fehlerauswirkungen. Einzelne (Bauteil-)Ausfälle werden auf deren Auswirkungen untersucht (Bottom-Up-Analyse-Verfahren). $\rightarrow$ FMECA
ALTERNATIV VERWENDETE BEZEICHNUNGEN: *Fehlermöglichkeits- und Einflussanalyse*; *Fehlerzustandsart- und -auswirkungsanalyse* ([IEC06a]); *Ausfallarten- und Auswirkungsanalyse*

FMECA ..... *Failure Modes, Effects and Criticality Analysis*
Qualitativ und quantitative Methode zur Analyse von Fehlerauswirkungen. Die Methode basiert auf der →FMEA, ist jedoch um die numerische Bewertung der Eintrittswahrscheinlichkeit und deren Schweregrad von bestimmten Ausfallszenarien erweitert.

FTA..... *Fault Tree Analysis*
Fehlerbaumanalyse - Deduktives Top–Down Fehleranalyseverfahren wo mit Hilfe von boolschen Verknüpfungen Fehlerbäume erstellt und damit Ursachen für Systemversagen ermittelt werden.

HALT/HASS *Highly Accelerated Life-Time/Highly Accelerated Stress Screening*
Beschleunigte Grenzlastprüfung / Prüfung bei stark erhöhter Belastung: Qualitative Testverfahren um elektronische und elektromechanische Baugruppen einer beschleunigten Alterung (bei HALT) bzw. unter Grenzbedingungen (HASS) auf Zuverlässigkeit zu prüfen. Die Beschleunigung wird dabei durch Verschärfung der Umweltbedingungen (z.B. Temperatur/Feuchte, zyklischer Wechsel innerhalb der Grenzbetriebswerte) aber auch mittels künstlicher, mechanischer (Vibration) und elektrischer (Hochlast, Impulsbetrieb) Belastungen erreicht.

MTBF ..... *Mittlere ausfallsfreie Arbeitszeit zwischen zwei Fehlern*
Gilt nur für reparierbare Systeme, siehe Abschnitt 2.2.1
en: Mean Time Between Failures

MTTF..... *Mittlere ausfallsfreie Arbeitszeit bis zu einem Fehler*
Gilt für nicht reparierbare Systeme. Bei konstanter Ausfallrate ist der Mittelwert der ausfallfreien Arbeitszeit MTTF = $1/\lambda$. Statistisch sind nach Ablauf der MTTF 63,2 % der Komponenten ausgefallen.
siehe Abschnitt 2.2.1, [Pau03] Seite 52
en: Mean Time To Failure

MTTF$_D$ ..... *Mittlere Zeit bis zu einem gefährlichen Ausfall*
Sicherheitstechnik - siehe Abschnitt 2.3.2
en: Mean Time To Dangerous Failure

MTTFF ..... *Mittlere ausfallsfreie Arbeitszeit bis zum ersten Fehler*
siehe Abschnitt 2.2.1
en: Mean Time To First Failure

MTTR ..... *Mean Time To Restoration / Mean Time To Repair (old)*
siehe Abschnitt 2.2.1
en: Mean Time To Repair

PFD ..... *Probabilistic Failure on Demand*
Sicherheitstechnik - Ausfallswahrscheinlichkeit bei Anforderung oder Auslösung einer (Sicherheits-)Funktion

PFH ..... *Probabilistic Failure per Hour*
Sicherheitstechnik - Ausfallswahrscheinlichkeit pro Stunde bei kontinuierlicher Anforderung einer (Sicherheits-)Funktion; *Einheit:* $[h^{-1}]$

PL ..... *Performance Level*
Sicherheitskategorie (PL_a ... PL_e, ISO 13849)
Beschreibt die Fähigkeit, eine Sicherheitsfunktion unter vorhersehbaren Bedingungen auszuführen. Wird verwendet zur Einstufung der Kritikalität einer Anwendung und in Folge zur Festlegung von Systemanforderungen wie Redundanz und maximale Ausfallrate.

PPM ..... *part per million*
Einheit der Ausfallrate in $[\frac{10^{-6}}{h}] \rightarrow$ FIT

RAMS ..... *Reliability, Availability, Maintainability, Safety*
steht für: Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit und ist ein Prozess oder eine Methode, die in der Bahntechnik bereits während der Planungs- und Entwicklungsphase Fehler im fertigen System verhindern und aufdecken soll (siehe EN 50129).
Bereich Risk Assessment Management Systeme

SELV/PELV . *Separated or Safety Extra Low Voltage / Protected Extra Low Voltage*
Funktionskleinspannung mit sicherer Trennung (SELV) / Schutzkleinspannung (PELV)
Bestimmung zum sicheren Umgang mit (offenen) elektrischen Schaltkreisen unter Kleinspannung, durch zusätzliche Begrenzung der Spannung und schaltungstechnische Vorschriften.

SFF ..... *Safe Failure Fraction*
Sicherheitstechnik - Anteil sicherer Ausfälle, siehe auch 2.3.1
SFF = $(\sum \lambda_S + \sum \lambda_{DD})/(\sum \lambda_S + \sum \lambda_D)$

SIL ..... *Safety Integrity Level*
Sicherheitskategorie (SIL 1 ... SIL 4; EN 62061, IEC 61508)
Zuordnung eines Sicherheitssystems (im Gegensatz zum $\rightarrow$PL, welcher die Zuordnung einer Sicherheitsanwendung bzw. -funktion beschreibt)

SPS ..... *Speicherprogrammierbare Steuerung*
en: Programmable Logic Controller (PLC)

Literatur

[Bir07] Alessandro Birolini. *Reliability Engineering*. 5. Aufl. Springer, 2007.

[Bör06] Josef Börcsök. *Funktionale Sicherheit - Grundzüge sicherheitstechnischer Systeme*. Hüthig, 2006.

[Bör09] Josef Börcsök. *Lexikon Sicherheitstechnik*. Hüthig, 2009.

[Dhi05] B.S. Dhillon. *Reliability, Quality, and Safety for Engineers*. CRC Press, 2005.

[EPS05] EPSMA. *Reliability - Guidelines to Understanding Reliability Prediction*. European Power Supply Manufacturers Association (EPSMA). Juni 2005.

[Fey86] Richard P. Feynman. *Report of the PRESIDENTIAL COMMISSION on the Space Shuttle Challenger Accident; Appendix F: Personal Observations on Reliability of Shuttle*. Bd. 2. NASA, 1986. URL: http://history.nasa.gov/rogersrep/v2appf.htm.

[Gal09] Dr. Homayoon Dezfuli; Dana Kelly; Dr. Curtis Smith; Kurt Vedros; William Galyean. *NASA-SP-2009-569: Bayesian inference for NASA probabilistic Risk and Reliability*. NASA, 2009.

[IEC06a] IEC60812. *Analysetechniken für die Funktionsfähigkeit von Systemen - Verfahren für die Fehlzustandsart- und -auswirkungsanalyse (FMEA)*. IEC60812. IEC, 2006.

[IEC06b] IEC61025. *Fehlzustandsbaumanalyse*. IEC, 2006.

[IEC06c] IEC61078. *Techniken für die Analyse der Zuverlässigkeit - Zuverlässigkeitsblockdiagramm und Boole'sche Verfahren*. IEC, 2006.

[IEC06d] IEC61165. *Anwendung des Markoff-Verfahrens*. IEC, 2006.

[IEC09] IEC61709. *Electronic components - Reliability - Reference conditions for failure rates and stress models for conversion*. Committee draft for vote (CDV). IEC, Nov. 2009.

[IEC10] IEC61508. *1-7 Ed. 2.0: Functional safety of electrical/electronic/programmable electronic safety-related systems*. IEC, Jan. 2010.

[IEC15] IEC60050-192. *International electrotechnical vocabulary - Part 192: Dependability*. IEC, Feb. 2015. URL: http://www.electropedia.org/iev/iev.nsf/index?openform&part=192.

[IEE10] IEEE-Standard. *IEEE Std 1413-2010 - Standard Framework for Reliability Prediction of Hardware*. (Revision of IEEE Std 1413-1998). 2010. DOI: 10.1109/IEEESTD.2010.5446443.

[Kim09] Eric Bauer; Xuemei Zhang; Douglas A. Kimber. *Practical System Reliability*. IEEE Press, Published by John Wiley & Sons, 2009.

[Kru95] Philippe Kruchten. „Architectural blueprints–the '4+1' view model of software architecture". In: *IEEE Software* (1995).

[Mic00] Deputy Associate Administrator Michael A. Greenfield. *Risk Management Tools*. Langley Research Center: Office of Safety und Mission Assurance, NASA, Mai 2000.

[OMG10] OMG. *Business Process Model and Notation (BPMN)*. Bd. Version 2.0. OMG, 2010. URL: http://www.omg.org/spec/BPMN/2.0.

[Pau03] Arno Meyna; Bernhard Pauli. *Taschenbuch der Zuverlässigkeits- und Sicherheitstechnik*. Hanser, 2003.

[TM03] Thorsten Tietjen und Dieter H. Müller. *FMEA Praxis*. Verlag Hanser München, 2003.

[Wil06] Jürgen Wilde. *Skriptum zur Vorlesung Zuverlässigkeit und Sicherheit*. Albert-Ludwigs-Universität Freiburg, 2006.

[Wil08] Jürgen Wilde. *Skriptum zur Vorlesung Testverfahren und Qualifikation*. Albert-Ludwigs-Universität Freiburg, 2008.