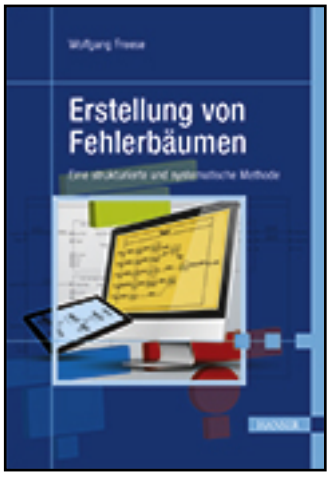
HANSER



Leseprobe

Wolfgang Freese

Erstellung von Fehlerbäumen

Eine strukturierte und systematische Methode

ISBN (Buch): 978-3-446-44578-9

Weitere Informationen oder Bestellungen unter

http://www.hanser-fachbuch.de/978-3-446-44578-9

sowie im Buchhandel.

Vorwort

Kennen Sie das? Es ist Freitag, später Nachmittag. In sprichwörtlich letzter Minute hat ein Kollege in der Spezifikation einen potenziellen Funktionsausfall gefunden, der bisher im technischen Sicherheitskonzept nicht berücksichtigt worden ist. Nun sollen Sie mittels Fehlerbaumanalyse nach möglichen Ursachen suchen und geeignete Sicherheitsmaßnahmen definieren. Das Problem: Die Randbedingungen sind alles andere als optimal. Von den Kollegen, die Sie benötigen, sind zwei auf einer Fortbildung, drei erkrankt, einer auf Dienstreise, und der Rest hat entweder Vaterschaftsurlaub oder ist schon auf dem Weg ins Stadion. Das Verständnis der Kollegen und Kolleginnen ist eh größtenteils eher gering. „Du immer mit Deinen Fehlerbäumen. Früher hat eine FMEA auch gereicht."

Ihre Motivation könnte geringer kaum sein, aber es bleiben nur zwei Tage, dann müssen Ergebnisse vorliegen. Also machen Sie sich wie üblich selber dran, besorgen sich den Schaltplan (per email vom Kollegen aus Indien – der arbeitet jetzt noch?), definieren als Top Level Event die Sicherheitslücke und legen los. Als es schließlich darum geht, die Resultate zu diskutieren, wird auch das zum Spießrutenlauf. Jedem rennt die Zeit davon; Sie mögen bitte per email mitteilen, welche Änderungen notwendig seien. Endgültig frustriert empfehlen Sie wie gewünscht ein paar Designänderungen, beschweren sich noch über die schlechte Zusammenarbeit (interessiert aber niemanden) und setzen ihren Chef in Kopie in der Hoffnung, dass es in Zukunft besser werden wird (wird es nicht). Immerhin haben Sie es mal wieder geschafft, den Karren aus dem Dreck zu ziehen. Ohne Sie hätte die Lieferung der Prototypen in einer Woche verschoben werden müssen. Der Kunde hätte getobt, der Chef hätte getobt, die Kollegen hätten getobt. So aber konnte der Zeitplan eingehalten werden, alle sind zufrieden.

Drei Wochen später fallen fünf Prototypen während der Wintertests in Skandinavien aus. Der Kunde tobt, der Chef tobt, die Kollegen toben. Ursache ist nicht die Sicherheitslücke gewesen. Die von ihnen vorgeschlagenen Maßnahmen haben gegriffen. Ursache war ein Designfehler an ganz anderer Stelle – ist nur leider im Rahmen der Fehlerbaumanalysen nicht aufgefallen. Aber wer denkt auch schon an den Einfluss der Umgebungstemperatur auf den Oszillator?

Das hier geschilderte Szenario ist frei erfunden und möglicherweise auch übertrieben. Aber das ein oder andere Detail des Geschehens wird manch Leser vielleicht aus eigener Erfahrung kennen. Hin und wieder ist man im täglichen Arbeiten weit weg vom Idealfall.

Gerade bei der Arbeit mit Fehlerbäumen ist es von besonderer Bedeutung, große Sorgfalt walten zu lassen. Ansonsten läuft man schnell Gefahr, fehlerhafte Fehlerbäume zu erstellen, die am Ende nur Zeit gekostet haben ohne die eigentlichen Show Stopper gefunden und geeignete Sicherheitsmaßnahmen definiert zu haben.

Zeitdruck, fehlende Kollegen, schlechte Vorbereitung, mangelhafte Spezifikationen … – das sind nur einige der möglichen Ursachen für qualitativ minderwertige Fehlerbaumanalysen. Das mit Abstand größte Risiko besteht allerdings vermutlich darin, dass sehr häufig niemand mehr die Zeit findet, über die Fehler und Risiken nachzudenken und die eigene Arbeitsweise zu hinterfragen und dann zu verbessern. Dies gilt auch, wenn es darum geht, einen Fehlerbaum zu erstellen. Eine strukturierte und systematische Vorgehensweise scheint es nicht zu geben.

Auf dem Markt findet sich jede Menge Literatur zur Auswertung von Fehlerbäumen. Das wundert nicht, denn die Methode ist bereits einige Jahrzehnte etabliert, die Mathematik bekannt. Auch ist die Zahl professioneller Software in den letzten Jahren kontinuierlich gestiegen und wird vermutlich weiter steigen. Sucht man allerdings nach einem Artikel, einer wissenschaftlichen Arbeit oder einem Buch zum Thema der Erstellung eines Fehlerbaums, so wird man überrascht sein, wie wenig es hierzu gibt. Einen Fehlerbaum zu analysieren impliziert, dass der Fehlerbaum schon existiert. Wie aber einen solchen erstellen?

Das vorliegende Buch macht einen ersten Schritt, um diese Lücke zu schließen. Der Autor hat zunächst als Functional Safety Manager und mittlerweile Engineering Group Manager Europe über einen Zeitraum von mehreren Jahren die hier vorgestellte Methode entwickelt, nachdem er selber immer wieder an Fehlerbäumen von mangelhafter Qualität verzweifelt ist – die eigenen mit eingeschlossen. Viele Fehlversuche, Diskussionen mit Kollegen, Reviews, Gespräche auf Konferenzen und nicht zuletzt der Gedankenaustausch im Internet haben dazu beigetragen, dieses Thema voranzutreiben. Es ist der ausdrückliche Wunsch des Autors, mit diesem Buch seine Methode zur Diskussion zu stellen, anstatt sie nur für sich zu verwenden, um sie basierend auf Rückmeldungen gemeinsam weiter verbessern und jedem zu Verfügung stellen zu können. Der enorme Vorteil liegt ja vor allem gerade darin, dass sie unabhängig von der Art des betrachteten Systems einsetzbar ist. Aus diesem Grunde adressiert das Buch nicht nur Functional Safety Manager der Automobilindustrie, sondern jeden, der mittels Fehlerbaumanalyse versuchen möchte, Ursachen in einem System zu identifizieren, die zu einem Funktionsausfall führen können.

Lindlar, den 31. März 2015

Dr. Wolfgang Freese

Inhalt


Definition, Begriffserklärung, Beispiel


Anmerkungen, Hinweise


Bitte beachten

Einleitung

Fehlerbaumanalysen sind eine seit den 1950er Jahren etablierte Methode zur Analyse von Systemen hinsichtlich der Fragestellung „Wie konnte das passieren?“ oder „Mit welcher Wahrscheinlichkeit kann das bei unserem System passieren?“ Motivation für die Entwicklung dieser Methode war die Suche nach den Ursachen eines bereits geschehenen Unglücks. Erst später wurde die Fehlerbaumanalyse auch präventiv eingesetzt, um für ein gegebenes System abschätzen zu können, mit welcher Wahrscheinlichkeit ein angenommener Fehlerfall passieren kann. Hierdurch ist es möglich geworden, Systeme iterativ sicherer zu machen bis ein akzeptables Restrisiko erreicht wurde.

Oftmals wird nicht erkannt, dass die Struktur eines Fehlerbaums mindestens genauso viel Einfluss auf das Ergebnis der Analyse hat, wie die eigentliche Auswertung selbst. Das zusätzliche Risiko, das sich für die Sicherheit eines Systems ergibt, wenn der Fehlerbaum z. B. unvollständig ist, kann leicht unterschätzt werden. Ein Blick auf den Markt zeigt jedoch relativ schnell, dass es nur sehr wenig Literatur dazu gibt, wie ein Fehlerbaum aufgebaut werden sollte. Dies ist umso erstaunlicher, da die Fehlerbaumanalyse schon seit mehreren Jahrzehnten in den unterschiedlichsten Branchen zum Einsatz kommt. Auf Konferenzen, Workshops und in diversen Internetforen stellt man fest, dass scheinbar jeder einzelne eine für sich optimale Methode entwickelt hat. Viele davon sind sich ähnlich und offenbar erfolgreich, die Ergebnisse sprechen für sich. Auf der anderen Seite muss man aber auch immer wieder feststellen, dass sich gerade die Neulinge unter den Fehlerbaumanalysten z. T. sehr schwer damit tun, einen sinnvollen Fehlerbaum zu erstellen – sinnvoll im Sinne von: Dieser Fehlerbaum hilft effizient ein System sicherer zu machen. Diese Lücke auf dem Buchmarkt wenigstens ein bisschen zu schließen, ist das Ziel der vorliegenden Arbeit.

Ein Buch zum Thema Fehlerbaumanalyse zu schreiben, ist insofern eine Herausforderung, als dass es sehr viele unterschiedliche Aspekte dieser Methodik gibt, über die geschrieben werden könnte. Es war jedoch von Anfang an das Ziel, sich ausschließlich auf die Erstellung von Fehlerbäumen zu beschränken. Daher wird der Leser z. B. vergeblich nach mathematischen Grundlagen oder der Erklärung

von Grundbegriffen suchen. Auch die quantitative Auswertung von Fehlerbäumen wird nicht diskutiert. Es gibt mittlerweile zahlreiche Software Tools am Markt, mit denen sich diese Aufgabe weitestgehend automatisiert erledigen lässt.

Vom Leser wird erwartet, dass er die Methode der Fehlerbaumanalyse grundsätzlich kennt und weiß, wann sie eingesetzt wird. Möglicherweise hat er schon einige oder gar viele Fehlerbäume erstellt und analysiert. Dieses Buch soll ihm dabei helfen, dass Fehlerbäume zukünftig besser strukturiert sind und darüber hinaus Bereiche und Aspekte umfassen, die bisher vielleicht noch gar nicht in Betracht gezogen wurden.

Um den Leser nicht gleich zu Anfang durch zu viele theoretische Betrachtungen zu verlieren, wurde Wert darauf gelegt, so schnell wie möglich zum Thema zu kommen und die systematische Erstellung von Fehlerbäumen im Detail zu erklären. Daher werden in Teil 1 des Buches lediglich einige grundlegende Betrachtungen an den Anfang gestellt, bevor im eigentlichen Hauptteil (Teil 2) mittels der Beispielfunktion die Herleitung von Top Level Events sowie der Aufbau der Fehlerbäume auf den unterschiedlichen Ebenen (System, Software, Hardware) vorgestellt werden. Dass ein Fehlerbaum nicht nur für technische Systeme, sondern auch für Prozesse, Methoden oder Tools anwendbar ist, wird am Beispiel des Review Meetings als Verifikationsmaßnahme erläutert.

Darüber hinaus werden im letzten Teil des Buches allgemeinere Aspekte von Fehlerbäumen betrachtet: Eigenschaften der qualitativen Fehlerbaumanalyse, das Hinzufügen von Sicherheitsmaßnahmen, die Berücksichtigung von externen Komponenten und Modulen sowie die Herleitung und Anwendung von Qualitätskriterien. Es ist hinzuzufügen, dass bewusst darauf verzichtet wurde, Sicherheitsmaßnahmen an jeder denkbaren Stelle im Text und in den Diagrammen hinzuzufügen. Diesem Thema ist ein eigenes Kapitel gewidmet. Durch den Verzicht sind die dargestellten Fehlerbäume deutlich übersichtlicher und verständlicher, ohne dass die jeweilige Kernaussage verzerrt oder gar verloren gegangen ist.

Die in diesem Buch abgedruckten Fehlerbäume sind bewusst einfacher gehalten, als es in der Praxis häufig der Fall ist. Fehlerbäume können sehr schnell sehr umfangreich werden und der eigentliche Aspekt im jeweiligen Abschnitt wäre zu stark in den Hintergrund getreten.

Einige Begriffe haben sich in der Branche durchweg in der jeweiligen englischen Übersetzung etabliert, wie z. B. Review Meeting. Der Autor hat beschlossen, auf die Verwendung einer nicht üblichen Übersetzung in die deutsche Sprache zu verzichten, da er darin weder einen literarischen Gewinn noch eine Verbesserung der Lesbarkeit und Verständlichkeit des Textes erkennen kann.

Es sei noch angemerkt, dass dieses Buch nicht zum Ziel hat, technische Systeme mithilfe einer Modellsprache wie SysML [1] oder UML [2] vollständig zu beschreiben. Daher wurde auf die konsequente Verwendung dieser oder anderer Standards

verzichtet, zumal die Erfahrung des Autors gezeigt hat, dass derartige Sprachen viel zu wenig verbreitet sind, als dass erwartet werden könnte, dass jeder potenzielle Leser dieses Buches einen Gewinn daraus ziehen könnte. Das primäre Anliegen war, den Kerngedanken zu vermitteln und aus diesem Grunde ist die Alltagssprache bewusst gegenüber einer Modellsprache bevorzugt worden.

Teil 1

Vorbereitende Überlegungen

Wie im Vorwort angekündigt, werden im ersten Teil des Buches einige grundlegende Themen erörtert, die für das Verständnis des Hauptteils wichtig sind.

So sollen zunächst die Begriffe *Funktion* und *System* definiert werden, da diese häufig nicht klar voneinander getrennt verwendet werden. Für die Struktur der Spezifikationen sowie die Definition von Anforderungen und somit letzten Endes für die Qualität der Fehlerbäume ist dies allerdings von großer Bedeutung.

Anschließend wird eine Beispielfunktion, die in den späteren Kapiteln immer wieder verwendet werden wird, um die jeweiligen Aspekte anschaulicher zu machen, im Detail vorgestellt.

Die im Hauptteil vorgestellte Methode zur systematischen Erstellung von Fehlerbäumen setzt die Top-Ereignisse als gegeben voraus. Wie diese aus der Spezifikation des Systems und der Definition der Funktion hergeleitet werden können, wird ebenfalls im Detail beschrieben.

1 Funktionen und Systeme

Fehleranalysen werden durchgeführt, um nach Ursachen dafür zu suchen, dass benötigte Funktionen nicht mehr wie erforderlich bereitstehen. Typische Beispiele aus dem Automotive-Bereich sind etwa die folgenden:

- Der Motor des Scheibenwischers wird nicht mehr aktiviert, wenn der Fahrer den Scheibenwischer anfordert.
- Das Seitenfenster wird hochgefahren, ohne dass der Knopf des Fensterhebers betätigt worden ist.
- Der Blinker beginnt erst nach einer Verzögerung zu blinken.
- Die Frontscheinwerfer gehen plötzlich aus.
- Das Fahrzeug beschleunigt während der Fahrt ohne Aufforderung durch den Fahrer.
- Das Lenkradschloss verriegelt während der Fahrt.

Sowohl die Funktionsdefinition als auch die Spezifikation des Systems sind nicht nur die Grundlage für die Entwicklung und Produktion des Systems, sondern insbesondere auch für die Fehleranalyse. Egal, ob der Ausgangspunkt ein angenommener Funktionsausfall, ein negatives Testergebnis oder eine Kundenreklamation ist, stets wird man sich anhand von Systemarchitektur, Softwaredesign, Schaltplan etc. auf die Suche nach den möglichen Ursachen machen. Fehlerhafte Dokumente sind daher im doppelten Sinn gefährlich. Eine besondere Bedeutung kommt der Struktur von Anforderungen zu, insbesondere der Bedeutung der Begriffe *Funktion* und *System*. Eine Fehleranalyse beruht grundsätzlich auf einem Funktionsfehler (sollte es zumindest). Aus rein funktionaler Sicht ist ein Systemfehler unkritisch, solange die geforderte Funktionalität gewährleistet ist. Dies kann zwar zu latenten Fehlern im Sinne der ISO 26262 führen, aber die Relevanz wird üblicherweise mittels einer FMEA untersucht.

Die Analyse von Funktionsfehlern beginnt dementsprechend bei der Definition der Funktion und wird auf das System und somit die Spezifikation des Systems (bzw. der Systeme) ausgedehnt. Wenn nun aber die Dokumente schon schlecht strukturiert sind, dann werden die Analysen und insbesondere die Fehlerbäume nur in den seltensten Fällen brauchbare Ergebnisse liefern.

Index