FTA im Projektumfeld

8

8.1 Einleitung

Nicht nur die Analyse selbst kann komplex werden, auch die Rahmenbedingungen sind es häufig, wie in Abb. 8.1 plakativ und ohne Anspruch auf Vollständigkeit illustriert. Wie bereits in Abschn. 7.4 betont, ist eine Fehlerbaumanalyse kein Einzelkunstwerk, sondern Mittel zum Zweck. Analyst und andere Beteiligte benötigen hierfür eine solide Grundlage für die Zusammenarbeit. In der Regel kann der Analyst diese Grundlage nicht im Rahmen einer „*One-Man-Show*“ schaffen, sondern sie benötigt auch den zielgerichteten Beitrag z. B. von Fachverantwortlichen, Projektleitung, Auftraggebern, Lieferanten. Hol- und Bringschuld für Informationen, Analyseergebnisse, Prüfung und Freigabe sollten definiert sein.

Dies erfordert inhaltliche und organisatorische Zielsetzung (Abschn. 8.2), Planung mit wiederholtem Soll-Ist-Abgleich (Abschn. 8.3) und geeigneter Ergebnisprüfung (Abschn. 8.4). Wenn mehrere Organisationen beteiligt sind, z. B. bei verteilter Entwicklung, ergeben sich zusätzliche Anforderungen, aber auch Möglichkeiten, die FTA zielführend einzusetzen (Abschn. 8.5).

8.2 Rechtzeitige Definition der Rahmenbedingungen

Die in diesem Abschnitt behandelten Punkte sollten die FTA-Verantwortlichen, d. h. Ersteller *und* Adressaten der Analyse *möglichst vor Analysebeginn* klären, um aufwändige Anpassungen im späteren Verlauf zu vermeiden.

© Springer-Verlag Berlin Heidelberg 2015

F. Edler, M. Soden, R. Hankammer, *Fehlerbaumanalyse in Theorie und Praxis*,
DOI 10.1007/978-3-662-48166-0_8

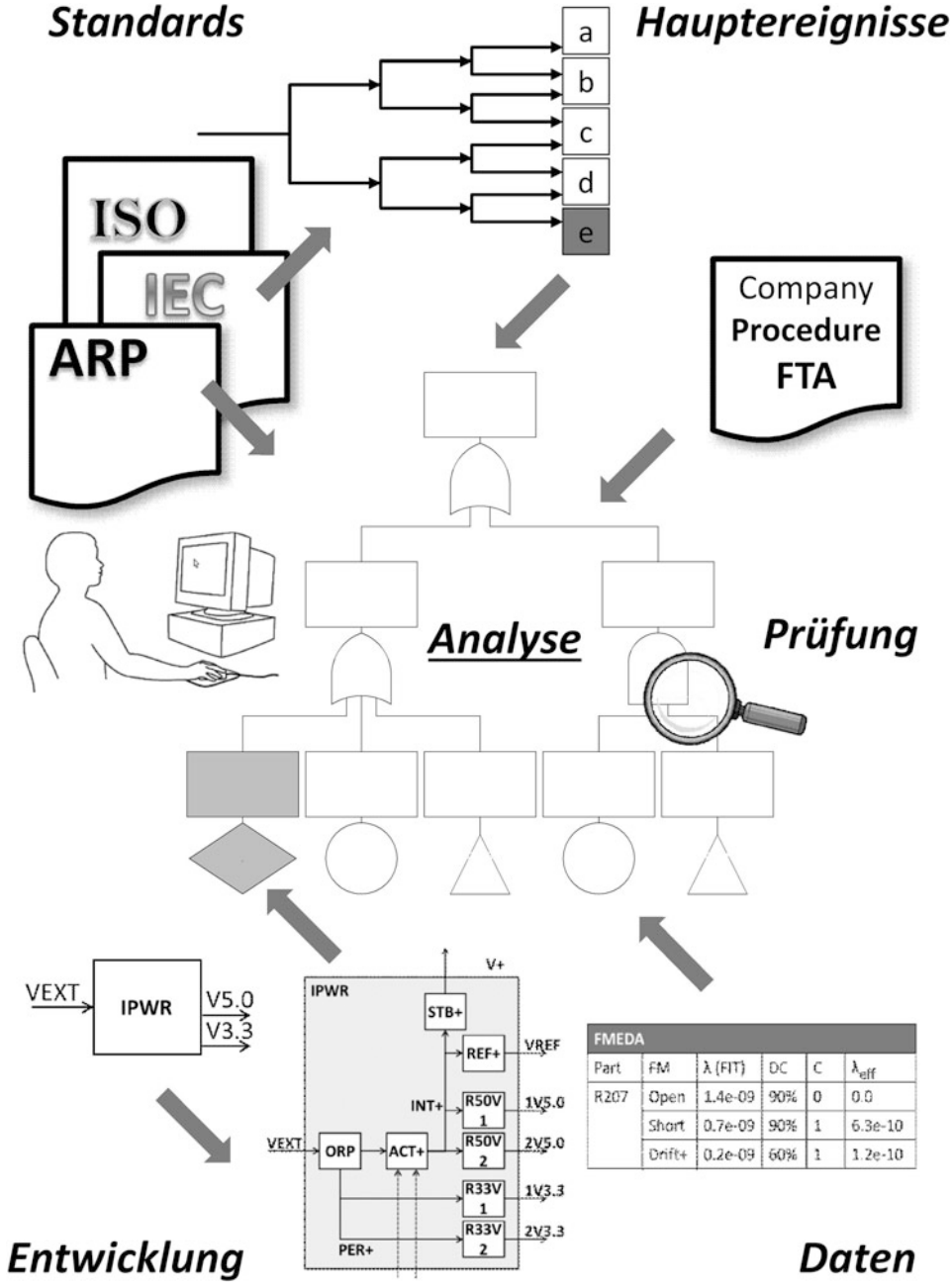

Abb. 8.1 Illustration der Einbindung von FTAs in einen Gesamtkontext

8.2.1 Einsatzgebiet der Analyse

Der Zweck des Unterfangens muss für den Analysten und andere Beteiligte klar erkennbar sein. Es macht einen großen Unterschied, ob eine FTA beispielsweise als Nachweisdokument im Rahmen eines Zulassungsprozesses benötigt wird oder ob sie rein unternehmensinternen Zielen dient.

Im ersten Fall werden Analyse und Analysebericht oft Freigabeinstanzen zur Begutachtung vorgelegt. Die Freigabeverfahren finden meist spät im Entwicklungslebenszyklus statt, so dass analytische Mängel (oder gar übersehene Mängel im Untersuchungsgenstand selbst) nur mit großem Aufwand zu beheben sind.

Im zweiten Fall, wenn etwa die analytisch begründete Auswahl einer konkreten Architektur- oder Designvariante im Fokus der FTA steht, hat die Analyse bei Abschluss ihren Zweck getan. Eventuell unterliegt sie in der Folge auch keiner besonderen Archivierungspflicht.

Es versteht sich daher, dass die Anforderungen an Plausibilität und Nachvollziehbarkeit der FTA im ersten Fall wesentlich strenger ausfallen müssen als im zweiten Fall. Das erfordert entsprechende planerische und qualitätssichernde Maßnahmen. Nicht nur der Analyst, sondern auch die anderen Beteiligten (Auftraggeber, Reviewer, Gutachter etc.) leisten dazu ihren Beitrag. Insbesondere setzt dies voraus, dass alle diese Beteiligten gleiche (oder zumindest sehr ähnliche) Vorstellungen von Ziel und Zweck der FTA haben.

Schon ein grobes Abstecken des organisatorischen Rahmens der Analyse ist eine große Hilfe – anstelle von unscharfen Formulierungen wie z. B. „der Zulieferer hat eine Fehlerbaumanalyse zu erstellen“, wie sie sich manchmal in Anforderungsdokumenten finden lassen. Beispiele dafür, wie die Rahmenbedingungen einer FTA grob umrissen werden können:

- An die Zulassungsbehörde ist als sicherheitstechnischer Nachweis eine quantitative FTA abzugeben
- Die FTA soll bisherige und neue Systemarchitektur hinsichtlich der Fehlertoleranz vergleichen
- Für die Schadensanalyse wird eine (streng vertrauliche!) FTA zur Abschätzung der wahrscheinlichsten Ursachen durchgeführt.

8.2.2 Klärung von Erwartungshaltungen

Unabhängig davon, für wen die Analyse erstellt wird und an wen sie weitergegeben werden soll, sollten folgende Punkte rechtzeitig geklärt werden:

- Welche Vorgaben gibt es für die methodische Vorgehensweise (z. B. durch einschlägige Normen, interne Verfahrensanweisungen etc.)?
- Welche formalen Aspekte sind bei der Dokumentation zu beachten (z. B. im Analysebericht)?
- Wie ist der Terminrahmen für fachliche Abstimmung, Reviews und Abschluss der Analyse gesteckt?
- Welche Nachweise für die Tauglichkeit verwendeter Daten und Werkzeuge müssen erbracht werden?

Oft wird unterschätzt, wie viel Aufwand erforderlich sein kann, um zu gemeinsamem Verständnis der Analyseinhalte und zu einem abgestimmten Vorgehen zu gelangen. Insbesondere wenn die Methode FTA erstmalig in einer Organisation angewendet wird oder wenn eine grundlegende Neuentwicklung analysiert werden soll, ist der Klärungsbedarf höher. Wird demgegenüber eine FTA für die Abwandlung eines bereits untersuchten Systems in bekanntem Projektkontext benötigt, ist von Beginn an meist vieles klarer.

Ohne Anspruch auf Vollständigkeit zeigt die Erfahrung, dass folgende Fragen helfen können, den Aufwand zur Abstimmung von Erwartungshaltungen abzuschätzen:

- Wie gut ist der Erfahrungshintergrund zur Methode in den beteiligten Organisationen?
- Wie hoch ist der Innovationsgrad des Untersuchungsgegenstandes?
- Wie gut ist die Kenntnis der Branchengepflogenheiten?
- Wie viele Erfahrungswerte können bei der methodischen und inhaltlichen Abstimmung zwischen den einzelnen Beteiligten und Organisationen genutzt werden?

Es lohnt sich, dieses Umfeld in frühen Phasen eines FTA-Projekts zu sondieren, um unliebsamen Überraschungen und vermeidbarer Nacharbeit vorzubeugen.

8.2.3 Betrachtungsumfang der Analyse

Für die Verantwortlichen einer Analyse ist es wichtig, sich rechtzeitig einen Überblick zu verschaffen, welche Anforderungen an die Analyse aus dem Systemkontext heraus entstehen. Betrachtungsumfang und damit der Aufwand für FTA wird maßgeblich bestimmt durch Merkmale des Untersuchungsgegenstands (analysiertes System) und der zu analysierenden Hauptereignisse. Zum Einfluss der notwendigen bzw. angestrebten Detaillierungstiefe s. Abschn. 8.2.4.

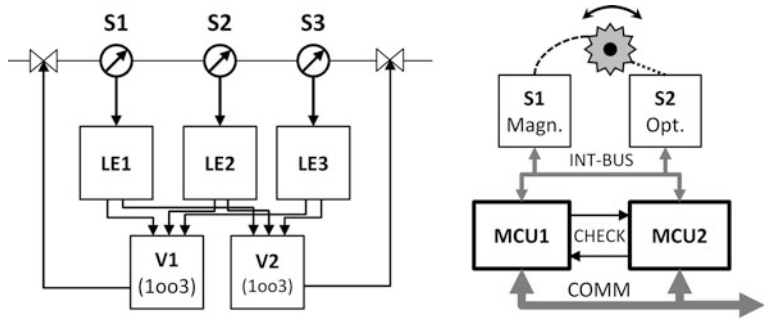

Abb. 8.2 Zwei Systemarchitekturen im Komplexitätsvergleich

8.2.3.1 Merkmale des Untersuchungsgegenstands

Zum einen sind es Merkmale des untersuchten Systems selbst, zum anderen aber auch Anforderungen an den inhaltlichen Betrachtungsumfang der Systemanalyse, die eine große Rolle spielen, wie folgende Frageliste zeigt (ohne Anspruch auf Vollständigkeit):

- Systemumfang: gibt es viele oder wenige durch die Analyse zu erfassende Systemelemente und/oder funktionale Schnittstellen?
- Technische Komplexität: gibt es viele oder wenige gleichartige Elemente und Funktionen?
- Einbeziehung bzw. Ausgrenzung bestimmter Themenfelder: ist z. B. nur eine HW-Analyse notwendig oder müssen auch externe Störungen, potentielle SW-Fehler usw. betrachtet werden?
- Ggf. Variantenübersicht: wie groß ist die Anzahl und Ähnlichkeit bzw. Unterschiedlichkeit von zu untersuchenden Varianten?

Man kann durch Klärung dieser Fragen eine erste Abschätzung für den Mindestaufwand bekommen, der selbst bei größtmöglicher Granularität der Analyse erforderlich ist.

Beispiel

Abbildung 8.2 zeigt zwei Systemarchitekturen, wie sie in realen Anwendungen angetroffen werden können. Links ist eine dreikanalige Drucküberwachung mit zwei Mehrheitsentscheidern (V), die bei mindestens zwei gemeldeten Überdruckwarnungen der drei Logikeinheiten (LE) die Notablassventile öffnen sollen. Diese Architektur basiert durchgehend auf *homogen redundanten* Elementen. Rechts ist eine zweikanalige Mess- und Auswerteeinheit mit kreuzweiser Überwachung und Plausibilisierung, die nur dann als gültig codierte Messwerte auf einen Kommunikationsbus ausgeben soll, wenn sowohl die Sensoren, als auch die Controller zu näherungsweise gleichen Ergebnissen gelangen. Diese Architektur ist *diversitär redundant*. Obwohl die dreikanalige Systemarchitektur mehr Funktionsblöcke

und Schnittstellen enthält als die zweikanalige, ist der Aufwand für eine FTA im letzteren Fall voraussichtlich höher. Dies folgt aus der Diversität (d. h. vorgefertigte Teilbäume sind nur eingeschränkt nutzbar) und vor allem, weil ein deutlich komplexeres Schnittstellenverhalten untersucht werden muss (Signalaustausch der Controller).

8.2.3.2 Merkmale und Anzahl der zu untersuchenden Hauptereignisse

Weil es so wichtig ist, möchten wir auch an dieser Stelle nicht versäumen, zu betonen, wie wichtig Schlüssigkeit und Prägnanz bei der Definition von Hauptereignissen ist. Unklar formulierte Hauptereignisse bergen das Risiko des bekannten Syndroms „*garbage in, garbage out*“, d. h. eine Analyse schlechter Qualität aufgrund eines schlecht definierten Einstiegspunkts, s. a. Abschn. 3.2.1.

Stellen sich vor oder bei Analysebeginn grundlegende Fragen zur Interpretation bereits formulierter Hauptereignisse, empfiehlt es sich dringend, diese zu beantworten. Das Beseitigen sprachlicher Mängel (vgl. Abschn. 6.2) ist hier besonders wichtig. Gegen verkürzte Formulierungen, die ja Platz in den Textboxen für das Hauptereignis finden müssen, spricht nichts, solange es dazu eine ausführlichere Erklärung gibt (s. a. [2], S. 31–32). Es lohnt sich, hier Aufwand zu investieren, auch um nachgelagerte Ressourcenvergeudung zu vermeiden.

Die Hauptereignisse sollte man auch im Rahmen des Systemkontextes betrachten, um einen besseren Überblick des Betrachtungsumfangs zu gewinnen. Nachfolgend finden sich dafür Anhaltspunkte:

- Ein- oder ausgegrenzter Betrachtungsumfang durch Formulierung der Hauptereignisse (so grenzt z. B. die enger gefasste Formulierung „Überhitzung der Leistungselektronik“ den Analyseumfang stärker ein als „Überhitzung im System“)
- Ähnlichkeit oder Unterschiedlichkeit der Wirkketten, die zu den verschiedenen Hauptereignisse führen (d. h. lassen sich viele oder wenige ähnlich strukturierte Teilbäume bilden, eventuell auf Basis von Schablonen, s. Abschn. 6.2.2).

Tipp

Sind mehrere Hauptereignisse für ein System zu untersuchen, finden sich häufig gleiche oder sehr ähnliche Wirkketten. Der Analyseaufwand steigt folglich meist nicht linear mit der Anzahl der Hauptereignisse – vorausgesetzt man benutzt eine gemeinsame Datenbasis in der FTA-Software (und nicht verschiedene, wie im Negativbeispiel aus Abschn. 7.3.2).

8.2.4 Detaillierungsgrad festlegen

Für die Planung des Analyseablaufs sollte geklärt werden, welche Detaillierung durch die zu erstellende FTA angestrebt wird. Dabei kann es durchaus vorkommen, dass der notwendige Detaillierungsgrad zu Beginn einer Analyse noch nicht erreichbar ist, z. B. weil die erforderlichen Informationen in einem Entwicklungsprojekt erst später verfügbar werden. Man sollte sich aber auch klar machen, dass *nicht alles, was möglich ist, auch notwendig sein muss*.

8.2.4.1 Möglicher Detaillierungsgrad

Der mögliche Detaillierungsgrad einer (entwicklungsbegleitenden) Analyse wird hauptsächlich bestimmt von folgenden Faktoren:

- Die zunehmende Reife der Systemauslegung bestimmt die Verfügbarkeit zunehmend detaillierter Informationen und Daten. Typische Meilensteine sind dabei Konzept, Designentwurf, Design Freeze und Definition von Anforderungen an den Betrieb wie Inspektions- und Wartungsverfahren.
- Abgrenzung von Zuständigkeiten. Beispielsweise ist ein OEM verantwortlich für Integration von Steuergeräten in einen Funktionsverbund, ein Zulieferer demgegenüber für die detaillierte HW- und SW-Entwicklung.

Man kann daraus ablesen, dass es für die Planung einer FTA einerseits einen zeitlichen Aspekt gibt, andererseits einen organisatorischen. Beim ersten Punkt stellt sich die Frage, wann eine FTA sinnvollerweise gestartet wird. Dazu gibt es kein Patentrezept, weil jeder Projektkontext ein anderer sein kann.

Beispiele

Bei einer innovativen Neuentwicklung ist dies eventuell in der Konzeptphase empfehlenswert, z. B. um möglichst frühzeitig eine Aussage über die Tauglichkeit einer Grobarchitektur zu erhalten und die FTA dann im Entwicklungsfortschritt nachzuziehen. Bei der Anpassung einer Plattform-Entwicklung auf eine individuelle Anwendung reicht es demgegenüber meist aus, die FTA nach dem Design Freeze zu beginnen, weil es bereits Basisnachweise der Tauglichkeit hinsichtlich Sicherheit und/oder Zuverlässigkeit gibt. In letzterem Fall sollte geklärt werden, inwieweit es wiederverwendbare Analyseergebnisse gibt…

Beim zweiten, organisatorischen Punkt ist es wichtig, die jeweilige Hol- und Bringschuld bei den beteiligten Organisationen zu definieren. Wird beispielsweise eine quantitative FTA für einen Funktionsverbund gefordert, dessen Teilsysteme von verschiedenen Herstellern zugeliefert werden, ist eine Schnittstellenabstimmung für Grob- und Detailanalysen erforderlich. Wir vertiefen dies in Abschn. 8.5.1.

http://www.springer.com/978-3-662-48165-3

Fehlerbaumanalyse in Theorie und Praxis
Grundlagen und Anwendung der Methode

Edler, F.; Soden, M.; Hankammer, R.

2015, XVIII, 290 S. 105 Abb., 9 Abb. in Farbe.,
Hardcover
ISBN: 978-3-662-48165-3