

Aufgabe 7-1: Fehlerbaumanalyse/„Fault Tree Analysis“

Lernziel: Erlernen der Fehlerbaumanalyse.

Oft will man zur Verbesserung der Sicherheit die möglichen Ursachen unerwünschter Ereignisse verstehen. Dazu eignet sich die Fehlerbaumanalyse (*Fault Tree Analysis*), eine Top-Down-Methode: Man gibt ein Ereignis vor, das nicht eintreten soll – das so genannte Top-Ereignis – und beschreibt in Form einer Baumstruktur, welche untergeordneten Ereignisse eintreten müssten, damit das jeweilige übergeordnete Ereignis eintritt. Man stellt dabei ein so genanntes Fehlerbaummodell auf.

(Definition nach <http://www.software-kompetenz.de/?18331>)

Arbeiten Sie sich in das Verfahren der Fehlerbaumanalyse und in deren Syntax ein. Beginnen Sie mit Fehlerbaumanalyse_ESchwindt.pdf (im KVV, Ordner „Material“) und recherchieren Sie evtl. fehlende Information selbst.

Beantworten Sie folgende Fragen:

- a)** Unter welchen Voraussetzungen bzw. in welchen Situationen sollte eine Fehlerbaumanalyse angewendet werden? In welchen Fällen ist sie wenig sinnvoll?
- b)** Welche Informationen liefert eine Fehlerbaumanalyse?
- c)** Welches sind die vier grundlegenden Elemente der Syntax eines Fehlerbaumes? Was ist deren jeweilige Bedeutung?
- d)** Welche weiteren syntaktischen Elemente gibt es? Was sind ihre Bedeutungen?
- e)** Was bedeuten *Minimal Cut Sets* (MCS) und *Single Point Failures* bei der Fehlerbaumanalyse?
- f)** Was ist unter einer qualitativen und was unter einer quantitativen Analyse eines Fehlerbaumes zu verstehen?
- g)** Was sind die größten Probleme bei der Fehlerbaumanalyse? Nennen Sie mindestens drei.
- h)** Betrachten Sie in einem beliebigen Fehlerbaum drei (nicht näher spezifizierte) Ereignisse (engl. *basic events*) die über eine UND-Verknüpfung (engl. *AND gate*) zu einem anderen Ereignis führen. Was muss für die Kopplung der Ereignisse gelten, damit die Ausfallwahrscheinlichkeit des Top-Ereignisses im Fehlerbaum bestimmt werden kann?

Aufgabe 7-2: Anwendung Fehlerbaumanalyse

Wenden Sie nun Ihre Kenntnisse aus der vorherigen Aufgabe an. Lesen Sie dazu zunächst die folgende Szenario-Beschreibung:

Die Redaktion einer Nachrichtensendung im Fernsehen stellt eine Liste ihrer Topthemen der 20-Uhr-Ausgabe eine Stunde vor Ausstrahlung über ihren Internetauftritt zur Verfügung. Zur Verwaltung der Inhalte im Web verwendet sie hierbei ein elektronisches Redaktionssystem. In dieses trägt der Verantwortliche für die Topthemen (hier im weiteren Redakteur A genannt) die Themen der 20-Uhr-Ausgabe im Laufe des Nachmittags ein. Er erhält diese auf Anfrage in Form von handschriftlichen Notizen nach der Redaktionssitzung. Die Redaktionssitzung endet dabei immer spätestens um 17:30 Uhr.

Nach dem Eintragen der Topthemen in die Erfassungsmaske des Redaktionssystems sind diese allerdings nicht sofort im Web verfügbar, da vorher eine Freigabe durch den Chefredakteur oder den Sendungsleiter erfolgen muss. Zu diesem Zweck versendet das Redaktionssystem nach dem Einstellen der Topthemen automatisch an beide Personen eine Email, die auffordert, die Topthemen über eine Funktion im Redaktionssystem zu überprüfen und freizugeben. Erst wenn eine der beiden Personen die Freigabe vorgenommen hat, erscheint die Liste der Topthemen im Web.

Sowohl Chefredakteur als auch Sendungsleiter sind auf eine Benachrichtigung durch eine Mail angewiesen, da sie beide sehr beschäftigt sind und außerdem nicht feststeht, wann Redakteur A mit seiner Arbeit fertig ist.

Leider ist der Sendungsleiter im Laufe des Nachmittags selten an seinem Rechner und liest die Benachrichtigungsemail somit oft nicht rechtzeitig. Dies weiß auch Redakteur A und benachrichtigt den Sendungsleiter deshalb immer auch via Anruf auf seinem Mobiltelefon.

Obwohl der Mechanismus der Topthemeneinstellung genau festgelegt ist, kommt es gelegentlich vor, dass die Themen vor der Ausstrahlung der Sendung nicht im Web zur Verfügung stehen.

Nehmen Sie an, dass nur folgende primäre Ereignisse dazu führen können:

1. Redakteur A erhält die Liste der Topthemen nicht
2. Die Erfassungsmaske für die Topthemen im Redaktionssystem fällt aus
3. Der Chefredakteur kommt im Laufe des Nachmittags nicht zum Lesen seiner Email.
4. Der Sendungsleiter kommt im Laufe des Nachmittags nicht zum Lesen seiner Email.
5. Der Mailserver fällt aus.
6. Redakteur A ist krank.
7. Im Sendestudio ist gerade kein Handyempfang möglich (Netz nicht verfügbar).

Bearbeiten Sie folgende Teilaufgaben:

- a)** Erstellen Sie einen Fehlerbaum für das Top-Ereignis: **Topthemen stehen vor Ausstrahlung der Sendung nicht online zur Verfügung**. Diesem Top-Ereignis soll u.a. folgendes Zwischenereignis untergeordnet sein: **Topthemen sind eingestellt, aber nicht freigegeben**.

Es soll ein vollständiger Fehlerbaum entstehen, in dem alle oben angegebenen Primärerignisse mindestens einmal vorkommen. Insgesamt soll ihr Fehlerbaum nicht mehr als 5 Zwischenereignisse besitzen. Sie können Ihre Primärerignisse mit den oben angegebenen Zahlen bezeichnen.

- b)** Bestimmen Sie alle *Minimal Cut Sets* Ihres Fehlerbaums. Sie dürfen wiederum die obige Nummerierung verwenden.
- c)** Gegen welche Primärerignisse lohnt es sich also Maßnahmen zu ergreifen? Machen Sie konkrete Vorschläge!