Freie Universität Berlin, Institut für Informatik, Arbeitsgruppe Software Engineering
Prof. Dr. L. Prechelt, S. Salinger, J. Schenk, Ute Neise, Alexander Pepper, Sebastian Ziller

Übungsblatt 6 WS 2009/2010 zum 2.3.2010

Aufgabe 6-1: (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*).

Fehlerbaumanalyse ist 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 wie eintreten müssten, damit das jeweilige übergeordnete Ereignis eintritt. Man stellt dabei ein so genanntes Fehlerbaummodell auf (Definition nach www.software-kompetenz.de).

Arbeiten Sie sich in das Verfahren der Fehlerbaumanalyse und in deren Syntax sein. Beginnen Sie mit http://wwwcs.upb.de/cs/ag-schaefer/Lehre/Lehrveranstaltungen/Seminare/AEIzS/Abgaben/Folien/3_FTA_ESchwindt.pdf (diesen Foliensatz finden Sie auch im hinteren Abschnitt des Skriptes) und recherchieren Sie evtl. fehlende Information selbst.

Beantworten Sie folgende Fragen:

1. Unter welchen Voraussetzungen bzw. in welchen Situationen sollte eine Fehlerbaumanalyse angewendet werden?
2. Welche Informationen liefert eine Fehlerbaumanalyse?
3. Welches sind die vier grundlegenden Elemente (und deren Bedeutung) der Syntax eines Fehlerbaumes?
4. Welche weiteren syntaktischen Elemente gibt es? Was sind ihre Bedeutungen?
5. Was bedeuten *Minimal Cut Sets* (MCS) und *Single Point Failures* bei der Fehlerbaumanalyse?
6. Was ist unter einer qualitativen und was unter einer quantitativen Analyse eines Fehlerbaumes zu verstehen?
7. Was sind die größten Probleme bei der Fehlerbaumanalyse?
8. 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. Welche Bedingung der Ereignisse untereinander muss beachtet werden, damit die Ausfallwahrscheinlichkeit des Top-Ereignisses im Fehlerbaum bestimmt werden kann?

Wenden Sie nun in der nachfolgenden Aufgabe Ihre neuen Kenntnisse an.

Aufgabe 6-2: (Anwendung Fehlerbaumanalyse)

Lernziel: Anwenden der Fehlerbaumanalyse

Sicherlich möchten Sie keine Minute der Vorlesung "Anwendungssysteme" verpassen. Deshalb betrachten Sie das Top-Ereignis, dass Sie verspätet in der um 10Uhr beginnenden Vorlesung eintreffen.

Entwickeln Sie für dieses Ereignis einen Fehlerbaum. Achten Sie darauf, dass Sie das Ereignis erst grob zerlegen und nicht gleich mit Basisereignissen beginnen. So wird beispielsweise eines der Ereignisse auf dem ersten Level "Verschlafen" sein. Dieses ist aber kein Basisereignis.

Ziel der Analyse ist es, Maßnahmen erkennen zu können, mit denen Sie das Eintreten des Top-Ereignisses in zumindest vielen Fällen vermeiden können oder seinen Schaden (d.h. die Verspätung) verringern.

Stoppen Sie deshalb bei der Analyse das Erweitern des Baumes dort, wo eine der folgenden Situationen eintritt

a.) Es ist offensichtlich, welcher Eingriff dieses Ereignis vermeiden hilft oder

b.) es ist offensichtlich, dass Sie dieses Ereignis ohnehin nicht beeinflussen können.

Im Rahmen dieser Aufgabe müssen Sie nicht Wahrscheinlichkeiten festlegen bzw. ermitteln.

Bestimmen Sie aber alle *MCS* und *Single Point Failures* (MCS erster Ordnung) ihres Baumes.