Anwendbarkeit von modellgestützten Safety-Analysen

Torge Hinrichs
HAW Hamburg

Agenda

- Was sind Safety – Requirements?
- Motivation / Problemstellung
- Zielsetzung
- Überblick über Verfahren / Techniken
- Konferenzen / Workshops
- Ausblick

Was sind Safety – Requirements?

- “specification that contains all the requirements of the safety instrumented functions that have to be performed by the safety instrumented systems”
  (IEC 61511)

Warum Safety – Analysen?

- Safety-Analysen helfen…
  - Zu prüfen, ob Requirements eingehalten werden
  - Fehlerquellen und kritische Bereiche zu identifizieren

Motivation

- In sicherheitskritischen Systemen muss Funktionalität belegt / bewiesen werden
  - Besonders Risiken für Anwender / Dritte
- Im Bereich Luft- & Raumfahrt und Bahn gesetzlich vorgeschrieben sonst keine Zertifizierung

Motivation(2)

- Funktionale Sicherheit (ISO 26262)
  - „ Absence of unreasonable risk due to *hazard*s caused by malfunctioning behaviour of Electrical/Electronic systems.“

- Systematische Tests
- Reviews
- …

Auftritswahrscheinlichkeit verringern

- Redundanz
- HW Selbsttest
- Diagnosen
- …

Konsequenzen unvermeidbarer Fehler verringern

[15]

Problemstellung

- Analysen zeitaufwendig
  - meist Tool gestützt, aber dennoch manuell durchgeführt
- Hoher Ressourcenaufwand
  - Viele / Große zu prüfende Systeme

Zielsetzung

- Senken des Aufwands der Analysetechniken

- Grundseminar:
  - Ausarbeitung eines Konzepts
  - Welche Verfahren werden genutzt?
  - Wie Aufwendig sind diese?
  - Welcher Nutzen kann daraus gezogen werden?
  - Was fehlt oder ist nur Umständlich zu realisieren?

Überblick über Verfahren / Techniken

- Fault Tree Analysis (FTA)
- Event tree analysis (ETA)
- Failure modes and effects analysis (FMEA)
- Failure modes, effects and criticality analysis (FMECA)
- HAZard and OPerability studies (HAZOP)

[9]

Fault Tree Analysis (FTA)

- Grafischer Analyseansatz
- Ungewollte Zustände stehen im Fokus
- Ziel: **alle** sequenziellen und parallelen Fehlerereignisse finden, die den Zustand verursachen
- Beispiele für Ereignisse:
  - Hard-, Software Fehler, menschliches Versagen oder andere sachdienliche Fehler
- Ereignisse werden nur mit UND / ODER verknüpft

[2] Kapitel 1

Fault Tree Analysis

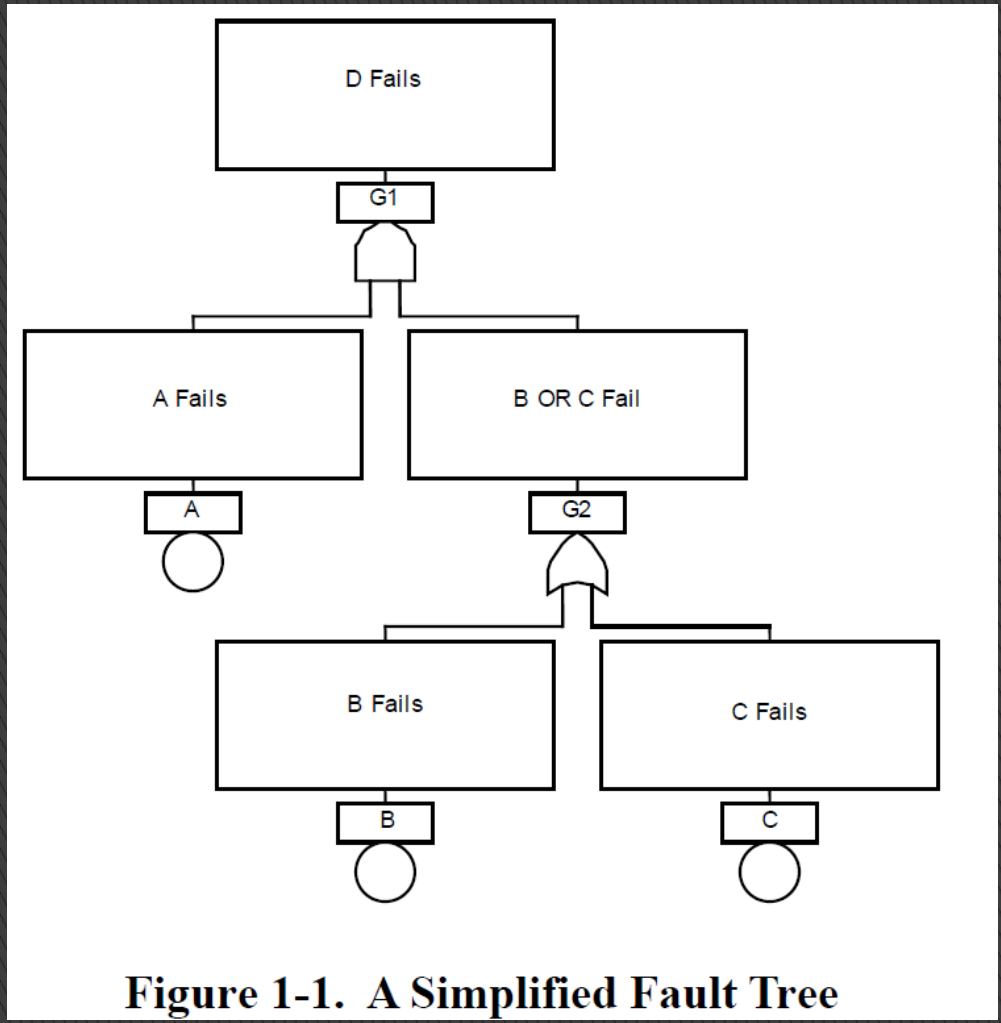


Figure 1-1. A Simplified Fault Tree

[2], S16f

Auswertung FTA

- Aus Fault Tree mit Ausfallwahrscheilichkeiten kann „minimal failure set“ bestimmt werden
- Einzelne Komponenten können ermittelt werden, die das System zum Versagen bringen
  - Beispiel: Fehler in einem Ventil kann zum Ausfall aller Ventile führen.

[2] Kapitel 1
[4]
[5]

Failure Modes and Effects Analysis

- Initiiert ein Fehlverhalten in einer Komponente
  - Fehlerhafte Daten
  - Verzögerte Antwort
  - Keine Antwort
- Analysiert die Reaktion auf Fehlverhalten in beteiligten Komponenten

[6]
[7]

Beispiel: Failure Modes and Effects Analysis

Data Label	Data Item	Data Fault Type	Description	Effect
999	MODE WD 1	Absent Data or Timing of Data Wrong	No Data (Flight Control Failure) or Obsolete Data (Flight Control Failure should be declared)	ACTIVE ALTITUDE TYPE ^{X,Y}, ALTITUDE ARM/ALTITUDE ABORT: VERTICAL ARM MODE (Altitude Arm, Vertical Approach); ACTIVE ALTITUDE TYPE, MANY OTHER ELEMENTS: VERTICAL CAPTURE MODE/Vertical Degradation removed 5 sec after Flight Control Failure
999	MODE WD 1	Incorrect Data	Wrong Data (or Flight Control Failure incorrectly declared)	ACTIVE ALTITUDE TYPE ^{X,Y}, ALTITUDE ARM/ALTITUDE ABORT: VERTICAL ARM MODE (Altitude Arm, Vertical Approach); ACTIVE ALTITUDE

[6]

Auswertung FMEA

- Liefert eine Liste von möglichen Risiken und Fehlerquellen in einem System
- Ermöglicht die Analyse ob und wo bestimmte Fehler aufgefangen werden
- Bildet Grundlage für weitere Analysen

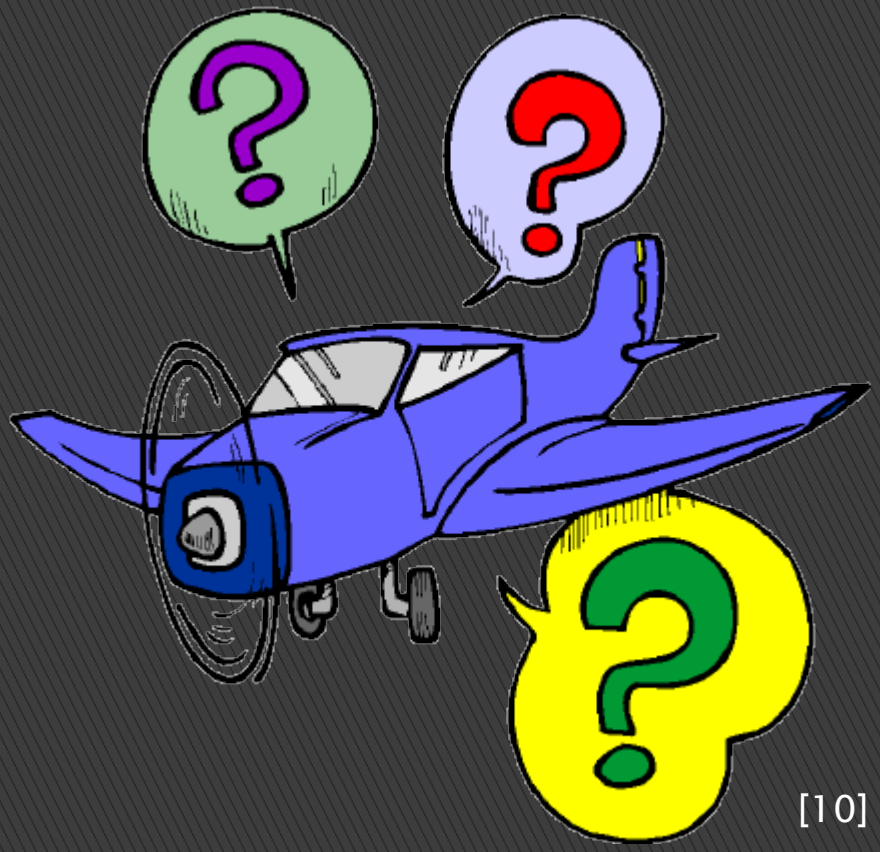
Konferenzen / Workshops

- International Conference on Evaluation and Assessment in Software Engineering [11]
- SAFECON [12]
- SafeComp [13]
- ARTEMIS / CRYSTAL [14]

Ausblick

- Grundprojekt:
  - Umsetzen des Konzepts
  - Erstellen einer Demo
  - Anwenden der verschiedenen Verfahren & Techniken auf das Modell
  - Verifizieren der Ergebnisse durch dynamische Tests
    - Beispiele: Mutationtest, Regressiontest, …

Noch fragen?



[10]

Quellenangaben

- [1] http://www.gfse.de Stand: 1.11.2014
- [2] Dr. Michael Stamatelatos at al, „NASA Fault Tree Handbook with Aerospace Applications“, 2002
- [3] Robyn R. Lutz, Hui-Yin Shaw,“ Applying Adaptive Safety Analysis Techniques“, 1999
- [4] Philipp Helle, „Automatic SysML-based Safety Analysis“, 2012
- [5] Adrien Mouaffo, Davide Taibi, Kavyashree Jamboti, „Controlled Experiments Comparing Fault-Tree-based Safety Analysis Techniques”, 2014
- [6] Robyn R. Lutz, “Safety Analysis of Requirements for a Product Family”, 1998
- [7] P. Struss, A. Fraracci, „FMEA of a Braking System”, 2011
- [8] Irene Bicchierai, Giacomo Bucci, Carlo Nocentini, Enrico Vicario, “Integrating Metrics in an Ontological Framework Supporting SW-FMEA”, 2012
- [9] Storey, 1996
- [10] http://www.seniorenfragen.de/ Flugzeug_pflegende_angehorige_pflege_zu_hause_hausliche_Pflege.gif Stand 11.11.2014
- [11] http://ease2014.org/ Stand 11.11.2014
- [12] https://aviation.osu.edu/safecon-2014 Stand 11.11.2014
- [13] http://www.safecomp2014.unifi.it/ Stand 11.11.2014
- [14] http://www.crystal-artemis.eu/ Stand 12.11.2014
- [15] Dr.-Ing. Thomas Scharnhorst , SIT – Safety in Transportsystemen, 2013
- [16] Nancy G. Leveson, Engineering a Safer World, 2011

Gesellschaft für Systems Engineering e.V.

[Q] gfse.de/images/stories/GfSE.png

- Seit 22. Juli 2014 eine ständige Arbeitsgruppe konstituiert
  - Project Lifecycle Management for Modell Based Systems Engineering (PLM4MBSE)

- Ziel der Arbeitsgruppe:
  - Identifikation von potentiellen Standardisierungsarbeiten in Kollaboration mit Organisationen wie OMG, OASIS und ProSTEP iViP [1]