Modellgestützte Safety- und Reliability-Analysen auf funktionaler Ebene für Hardware

Master Informatik HAW Hamburg

Grundseminar WS 2014

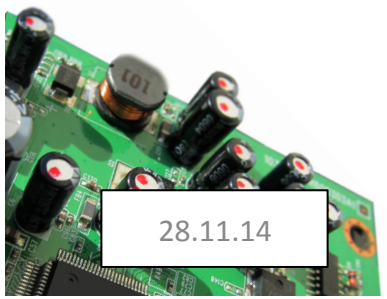
Arne Maximilian Richter

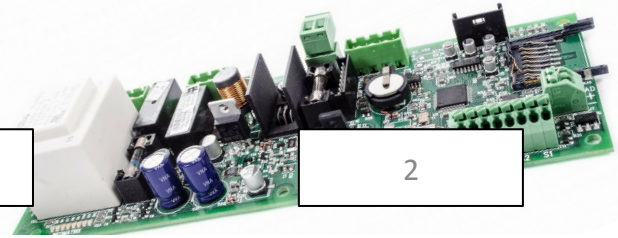
Vortrag am 28.11.2014

Gliederung

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

- Vorstellung des Themenbereiches
- Vorstellung der Verfahren
- Subjektive Betrachtung der praktischen Anwendung
- Ausblick in die aktuelle Forschung
- Ziele der Arbeit

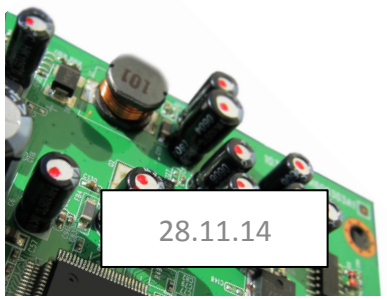


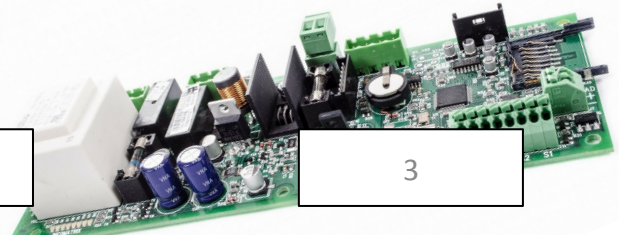


Technische Systeme

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

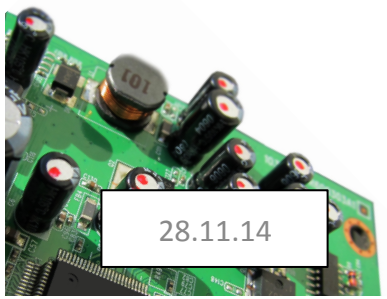
- Technische Systeme teilen Funktionen auf mehrere Komponenten auf.
- Das Zusammenspiel der Komponenten wirkt sich auf die Safety und die Reliability des Gesamtsystems aus.
- Analysen werden verwendet, um das Zusammenspiel zu durchleuchten.

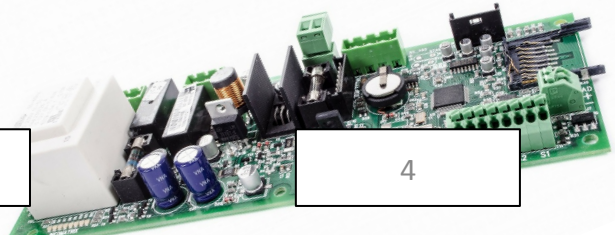




Beispiel: Beatmungsgerät

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

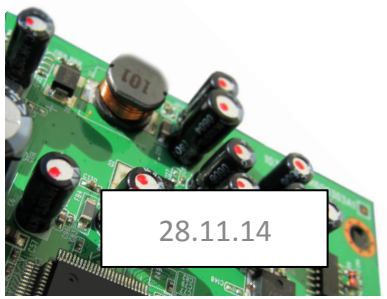


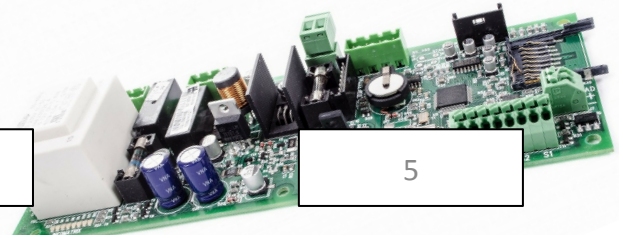


Grundlagen der Analysen

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

- Anforderungen (vom Kunden, durch Normen, etc.)
- Das System (ein entsprechendes Modell)
  - Aufbau/Struktur
  - Verhalten
- Analysetechniken

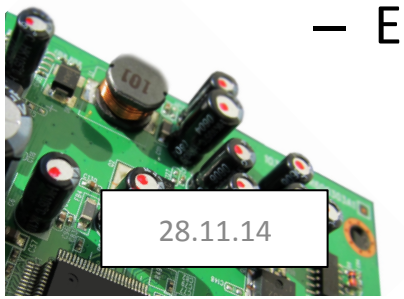


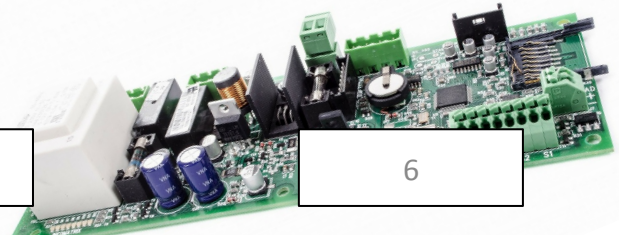


Systemmodellierung

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

- Textuelle Beschreibungen
  - Fließtext
  - XML
- Mathematische Formeln
- Diagramme, Grafiken, etc.
  - Eigene (Firmen-/Branchen-/Personenspezifisch)
  - UML
  - SysML
- Interessante Aspekte für die Arbeit:
  - Angepasste SysML für die Repräsentation der Verbindungen.
  - Eine XML für die Beschreibung der Zusammenhänge.



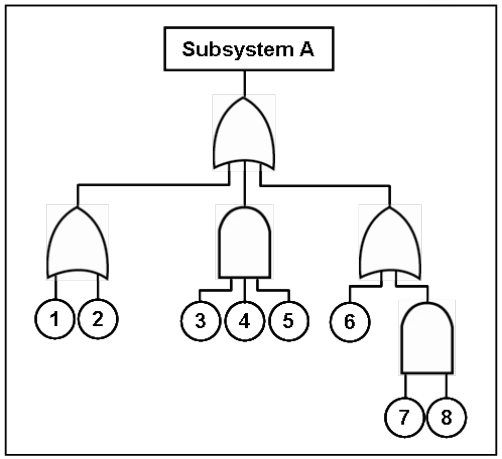


Fault tree analysis (FTA)

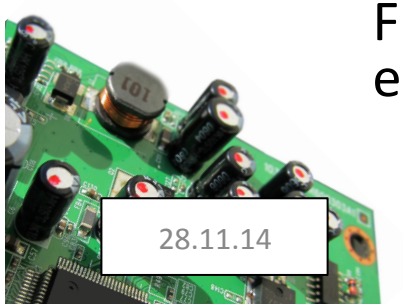
Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

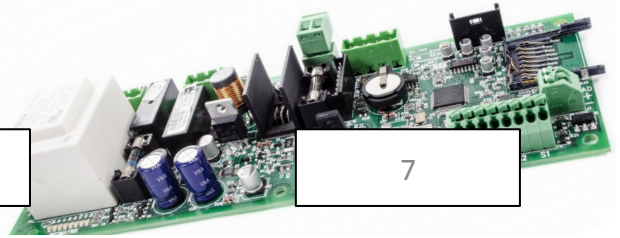
- Betrachtet die Ursachen möglicher Fehler einer Komponente oder Funktion.
- Ursachen werden als Baum dargestellt.

- Kann zu einer Formel umgebaut werden:
  Fehler in Subsystem A =
  $((1 \vee 2) \vee (3 \wedge 4 \wedge 5) \vee (6 \vee (7 \wedge 8)))$
- Interessante Aspekte für die Arbeit:
  - Was muss erfüllt sein, damit eine Funktion/Komponente seine Funktion erfüllen kann.



Quelle:
www.en.wikipedia.org
Autor: Wyatts



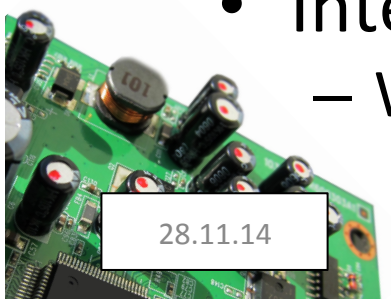


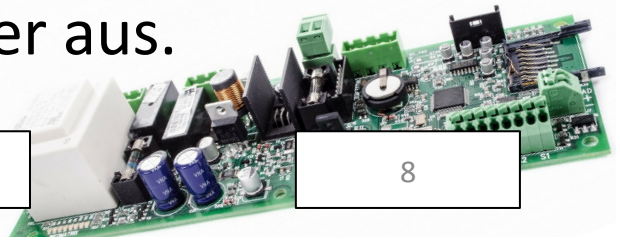
Failure modes and effects analysis (FMEA)

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

- Betrachtet einen Fehler in einer Komponente oder Funktion.
- Analysiert wird die Auswirkungen der Fehler auf angrenzende Komponenten und Funktionen.

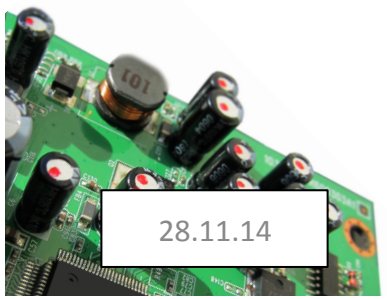
- Wird meistens tabellarisch festgehalten.
- Aktuell in der Forschung:
  - FMVEA – Failure Mode, Vulnerabilities and Effect Analysis [Bondavalli2014]
- Interessante Aspekte für die Arbeit:
  - Wie breiten und wirken sich Fehler aus.

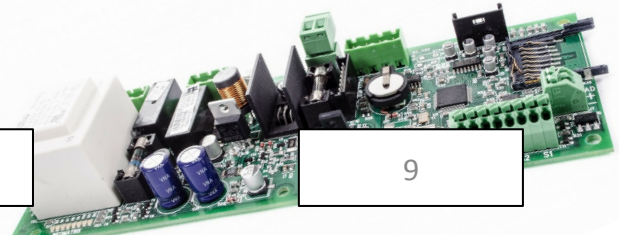




Beispiel: Beatmungsgerät

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

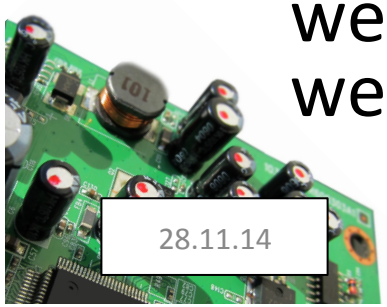


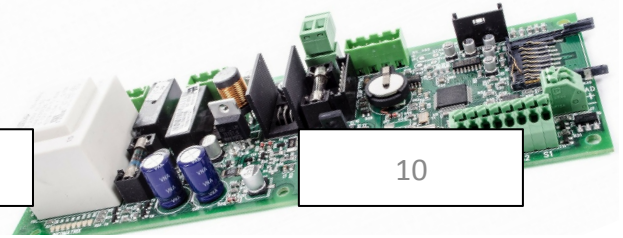


Probleme in der Praxis

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

- Analyse- und Modellierungstools sind nicht kombiniert.
- Analysen sind sehr aufwendig (kosten Zeit und wirken sich somit auf das Budget aus).
- Die Analysen benötigen ein gewisses Know-How.
- Zulassungswichtige Analysen werden folglich erst am Projektende durchgeführt.
- Wenn kein offensichtlicher Bedarf besteht werden die Analysen entsprechend weggelassen.

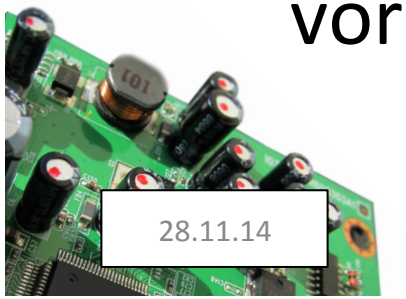


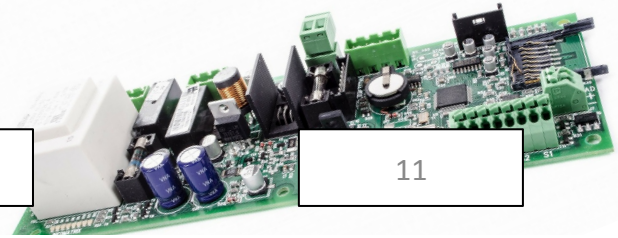


Kombination aus Analyse und Modell (1)

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

- Die Kombination von Modellen und Analysen ist aktuell Forschungsschwerpunkt.
- [Helle2012] stellt eine Kombination von SysML und Safety-Requirements vor.
- [Lauer2011] stellt eine automatisierte Fehlerbaumanalyse auf Basis der UML vor.

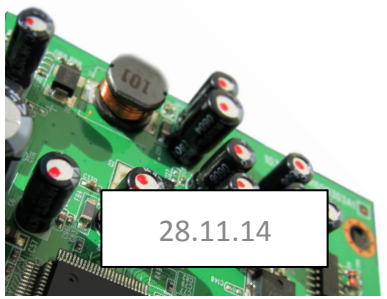


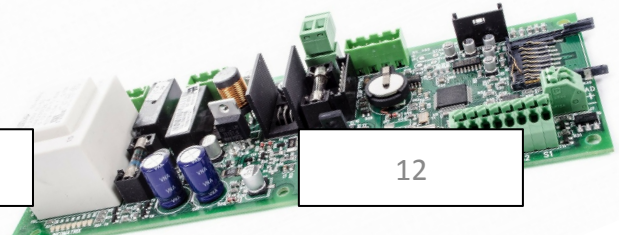


Kombination aus Analyse und Modell (2)

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

- Das EU-Projekt CRYSTAL beschäftigt sich mit der Zusammenführung von Analysen und Modellierungen.
- Es wurde eine GfSE Gruppe für die Kombination von SysML und Safety-Analysen gegründet.

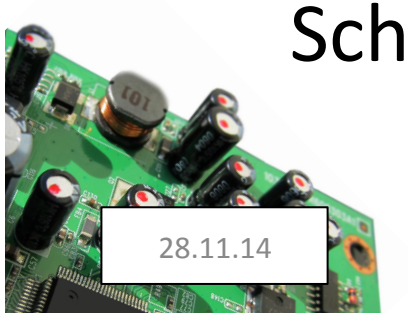


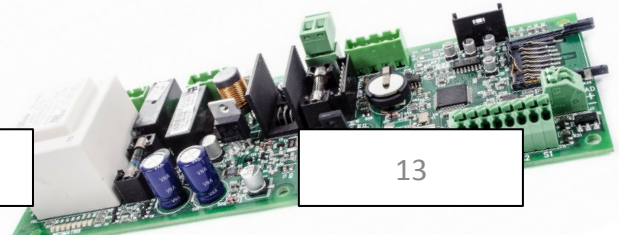


Persönliche Ziele

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

- Eine Kombination aus Analyse- und Modellierungstechnik.
- Die Analyse soll Fälle wie die Analysen im Beispiel und in [Mariani2007] abdecken.
- Sie soll von der Anwendung vergleichbar mit einer Schaltungssimulation in der Schaltungsentwicklung sein.

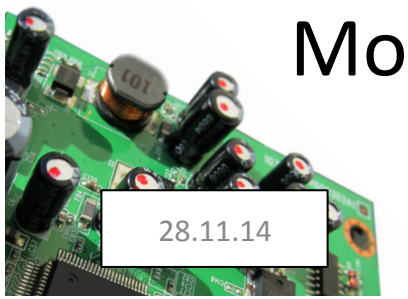


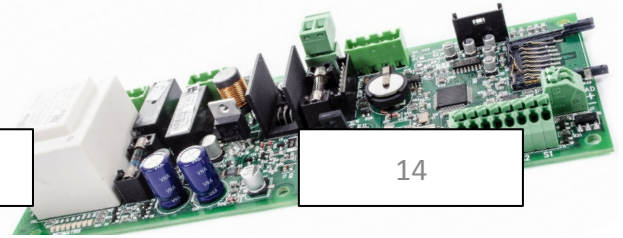


Nächste Schritte

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

- Suchen und erstellen von Anwendungsbeispielen für die Analyse.
- Identifikation und Eingrenzung von Zusammenhängen und Merkmalen, die abgedeckt werden sollen und müssen.
- Definition und Auswahl der Modellierungssprachen.
- Testen der Kombination aus Analyse und Modellierung.

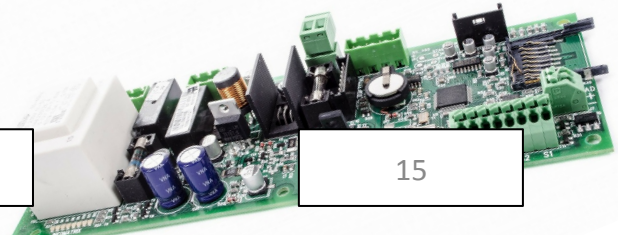




Konferenzen, Workshops & Gruppen

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

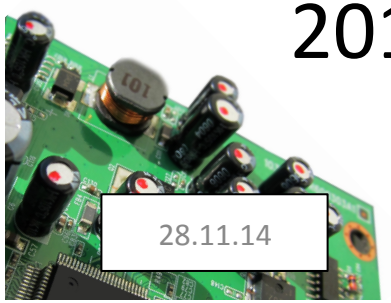
- VDE (Verband der Elektrotechnik, Elektronik und Informationstechnik)
- GfSE (Gesellschaft für System Engineering)
- ARTEMIS (Advanced Research & Technology for Embedded Intelligence and Systems)
  - CRYSTAL
  - VARIES
- SafeComp (International Conference on Computer Safety, Reliability & Security)

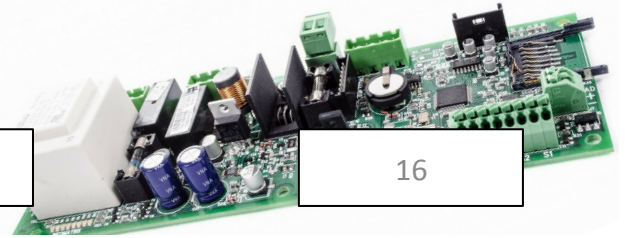


Literatur (1)

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

- Storey, Neil: **Safety-Critical Computer Systems**. Addison Wesley Longman. 1996.
- Leveson, Nancy G.: **Engineering a Safer World**. Massachusetts Institute of Technologie. 2011.
- Friedenthal, S., Moore, A., Steiner, R.: **A Practical Guide to SysML**. Elsevier Inc.. 2012.

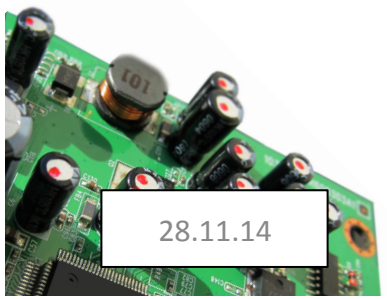


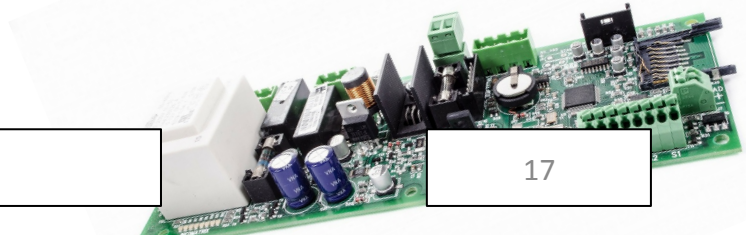


Literatur (2)

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

- Dougless, Bruce Powel: **Real-Time UML Workshop for Embedded Systems**. Newnes. 2014.
- Bondavalli, A., Ceccarelli, A., Ortmeier, F.: **Computer Safety, Reliability, and Security**. Springer. 2014

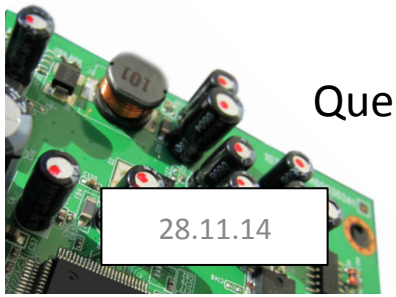




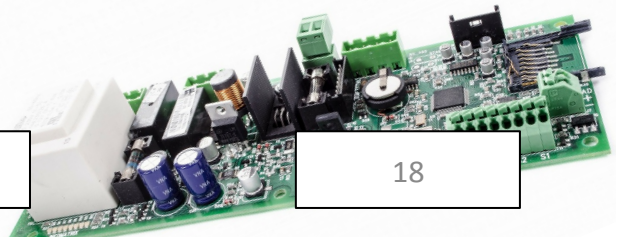
Literatur (3)

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

- Lauer, C., German, R., Pollmer, J.: **Fault Tree Synthesis from UML Models for Reliability Analysis at Early Design Stages**. ACM SIGSOFT Software Engineering Notes. 2011.
- Helle, Philipp: **Automatic SysML-based safety analysis**. 5th International Workshop on Model Based Architecting and Construction of Embedded Systems. 2012.
- Mariani, R., Fuhrmann, P.: **Comparing dail-safe microcontroller architectures in light of IEC 61508**. 22nd IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems. 2007.



Quelle der Hintergrundbilder: http://pixabay.com/




Danke für die Aufmerksamkeit!