Schienenfahrzeuge sicher steuern – Ein methodischer Ansatz für Sicherheitsbetrachtungen

Dipl. Wirtsch.-Ing. Stefan Schrank

Alstom LHB GmbH
Plattform Regio CITADIS™
Salzgitter

Dr.-Ing. Michael Meyer zu Hörste

Deutsches Zentrum für Luft- und Raumfahrt
Institut für Verkehrsführung und Fahrzeugsteuerung, Braunschweig

Gliederung

- Motivation
- Modulares Fahrzeug: Systemspezifische Anforderungen und Einsatzgebiete
- Sicherheitsbetrachtungen
- Definitionen, Annahmen und Schlussfolgerungen
- Ansatz: Methodisches Vorgehen
- Probleme / offene Punkte

Motivation

- neues modulares Fahrzeug
- verschiedene Zulassungsbehörden
- Software mit Sicherheitsverant-wortung
- Unterteilung der Software in

SIL = 0 oder SIL > 0

als Grundlage für eine Diskussion zwischen Hersteller, Gutachter und zulassender Behörde

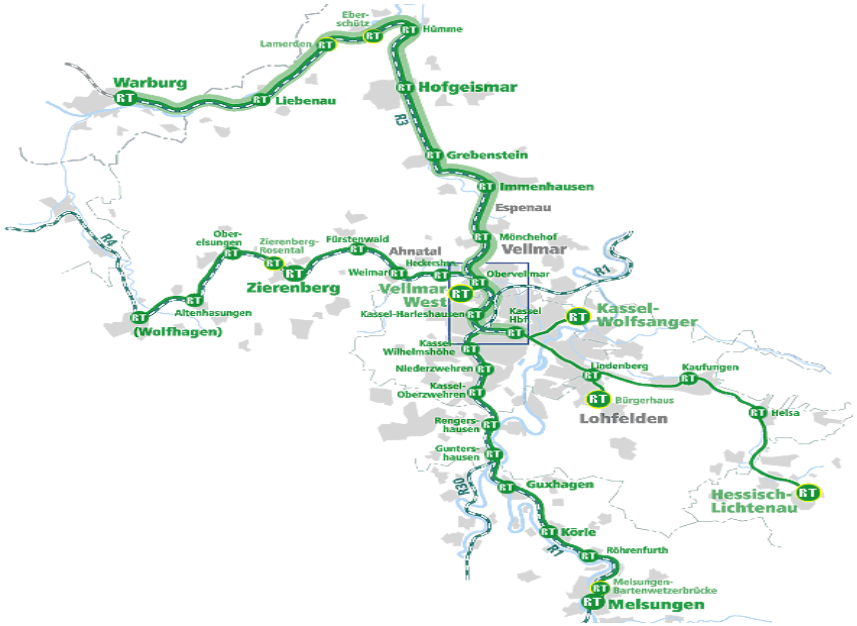
Die Zulassung eines variablen und modularen Fahrzeugs verlangt eine transparente und modulare Sicherheitsbetrachtung

SIL: Sicherheitsintegritätsstufe (Safety Integrity Level)

Systemspezifische Anforderungen

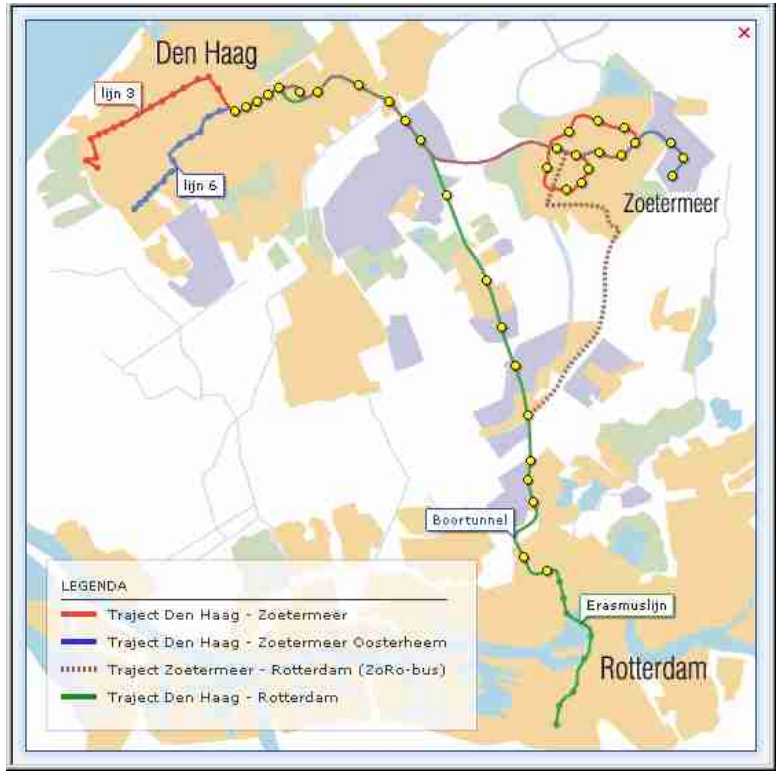
Auf der Eisenbahn		In der Stadt
16-22t	Zulässige Achslast	10-11t
~ 125 m	Kleinster Kurvenradius	~ 25 m
Fahren mit Zugsicherung	Betriebsart	Fahren auf Sicht
bis 3 m	Zulässige Fahrzeugbreite	2,65 m
380-550-760 mm	Übliche Bahnsteighöhen	0-250 mm
15kV~, 25kV~, 1500 V –, Diesel	Energieversorgung	750 V –
~ 1,3 m/s²	Max. Bremsverzögerung	~ 3,0 m/s²
passiv Hohe Festigkeit + geringes Bremsvermögen	Sicherheitsphilosophie	aktiv Hohes Bremsvermögen + geringe Festigkeit

Einsatzgebiete



RegioTram Kassel

RandstadRail Den Haag



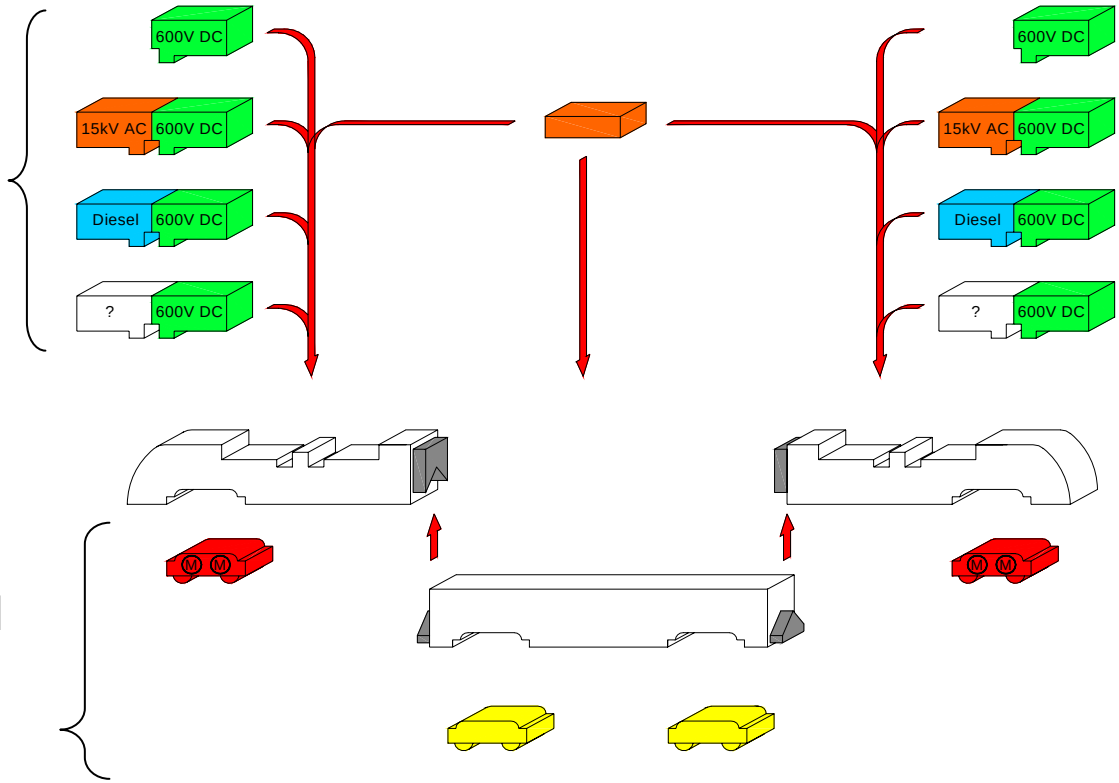
Modulares Fahrzeug

Mögliche Energie-Module

Endwagen-Modul

Mittelwagen-Modul

Drehgestelle



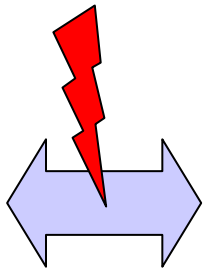
Sicherheitsbetrachtungen bisher

- Expertenwissen, daher nur bedingt reproduzierbar
- nur Kernfunktionen des Fahrzeugs herausgegriffen
- kein dokumentierter methodischer Ansatz

Sicherheitsbetrachtungen heute

Forderungen TÜV / EBA

- „mehr“
- systematischer Ansatz
- Wiederholbarkeit
- Transparenz
- Annäherung an die CENELEC-Normen



Forderungen Hersteller

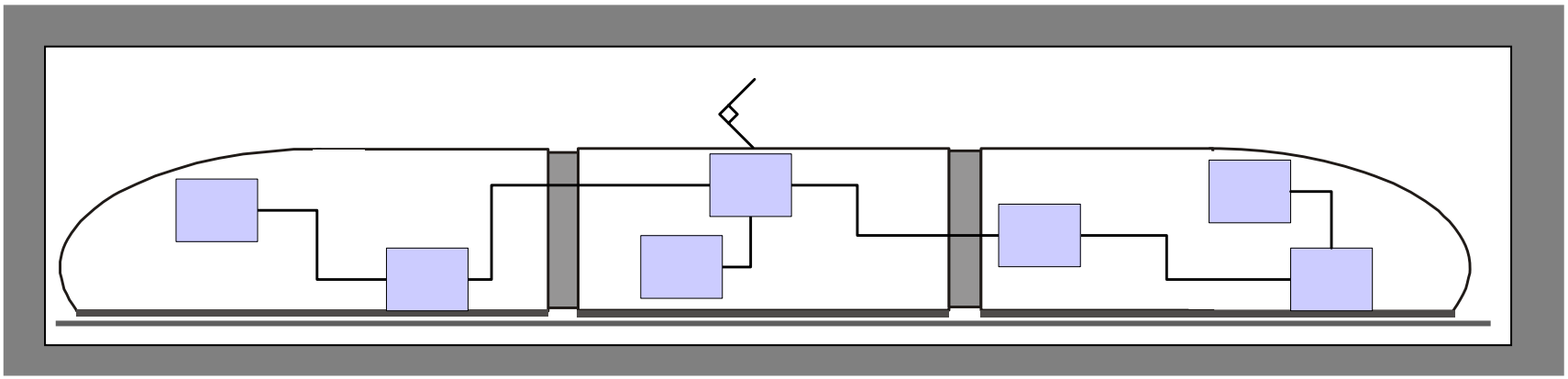
- weg vom Expertenwissen
- methodisches Vorgehen
- Wiederholbarkeit
- Transparenz
- nur leichte Annäherung an die Normen
- keinen Standard setzen
- pragmatisch

Unterteilung des Gesamtsystems

Gesamtssystem wird eine Vielzahl von Systemen unterteilt, wie z.B.:

- Türen inkl. Steuerung
- Innenraumbeleuchtung
- Sicherheitsfahrschaltung (SiFa)
- Antrieb / Bremse inkl. Regelung
- Leittechnik

Betrachtung der elektronischen Komponenten



Definitionen, Annahmen und Schlussfolgerungen

Außenwelt

- Umgebung des Fahrzeugs
- andere Verkehrsteilnehmer
- Triebfahrzeugführer
- Fahrgäste

Sicherheitsrelevanz

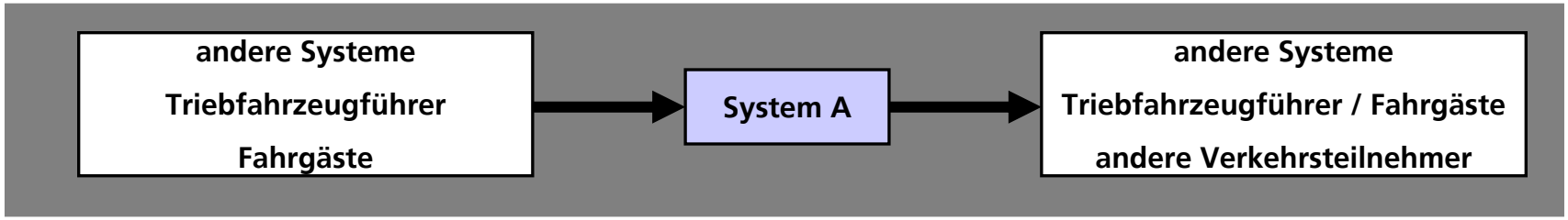
- „Ein System ist genau dann sicherheitsrelevant, wenn es durch eine Fehlfunktion Menschen gefährden kann, d.h. wenn ein Fehler in diesem System für Menschen im Fahrzeug oder in der Umgebung Schaden zur Folge haben kann.“

Definitionen, Annahmen und Schlussfolgerungen

direkter / indirekter Schaden

Es gibt für ein System zwei Möglichkeiten, Schaden anzurichten:

- *direkt:* durch Fehler, die direkt nach außen wirken
  Bsp.: Eine Tür klemmt einen Fahrgast ein.
- *indirekt:* durch Fehler, die zu einem Fehlverhalten in einem angrenzenden System führen
  Bsp.: Ein angrenzendes System befiehlt, die Tür zu öffnen.



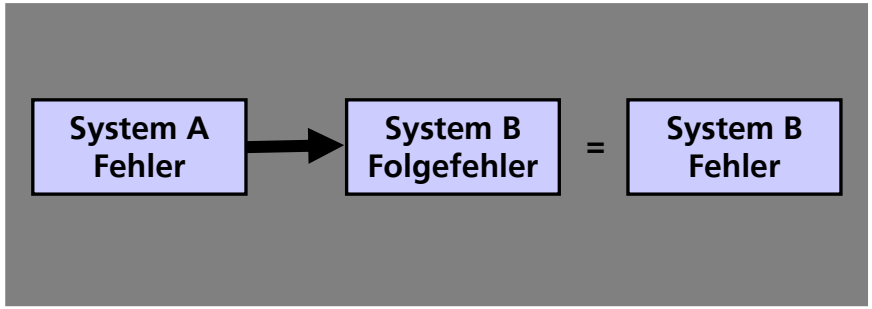
Folgerung:

Ein System ist genau dann sicherheitsrelevant, wenn es direkt oder indirekt Schaden anrichten kann.

Fehlerquellen

Annahme

Jeder Fehler, der durch ein falsches eingehendes Signal in ein System hineingetragen werden kann, kann auch in diesem System selbst entstehen.



Folgerung

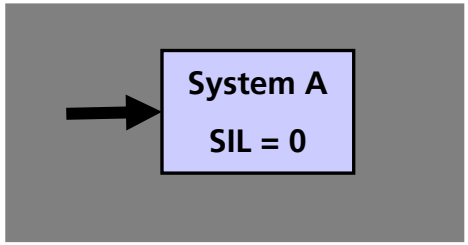
Die Sicherheitsrelevanz eines Systems hängt einzig und allein von seinen Verbindungen zur Außenwelt und zu anderen Systemen ab.

Systeme ohne Außenwirkung

Folgerung

Ein System ohne Verbindung nach außen kann keinen Schaden anrichten.

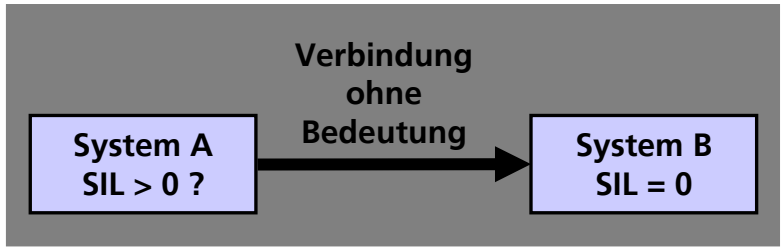
Ein System ohne Verbindung nach außen ist nicht sicherheitsrelevant.



Verbindungen ohne Bedeutung

Annahme

Ein nicht-sicherheitsrelevantes System kann keinen Schaden anrichten.



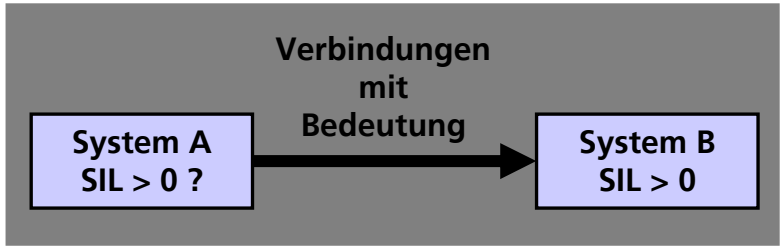
Folgerung

Ausgehende Verbindungen in ein nicht-sicherheitsrelevantes System können nicht dazu führen, dass das sendende System sicherheitsrelevant wird.

Verbindungen mit Bedeutung

Folgerung

Ein System kann nur dann indirekten Schaden anrichten, wenn es Signale an ein sicherheitsrelevantes System weitergibt.



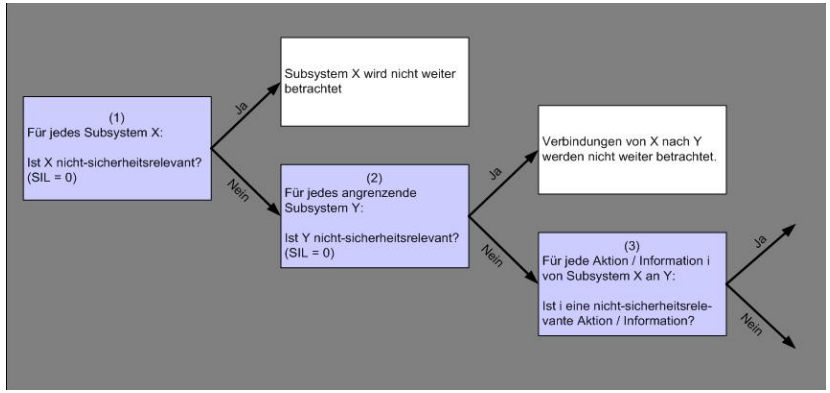
Sicherheitsrelevanz kann von außen nach innen übertragen werden.

Methodisches Vorgehen

- Fehler ergeben sich aus der Negation von Funktionen.
- Analyse der Systeme von außen nach innen.
- Es werden nur Einzelfehler betrachtete. Ausnahme: Systeme die ausschließlich als Rückfallebenen gebaut wurden, wie z.B. die Sifa oder die Sicherheitsschleife, werden in die Situation versetzt, für die sie entworfen wurden, z.B. unaufmerksamer Triebfahrzeugführer

Für jedes System:

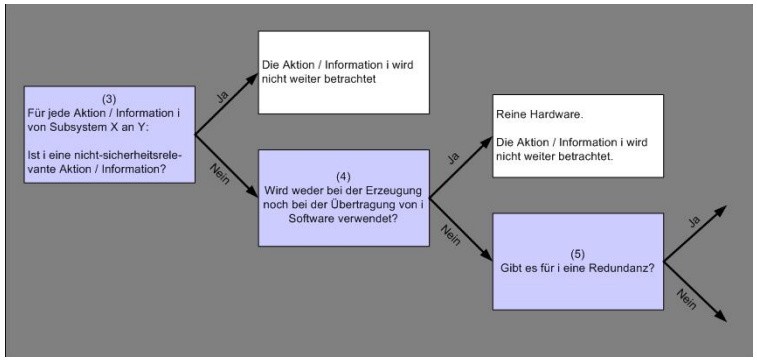
- Analyse der Funktionen
- Analyse der ausgehenden Verbindungen:
  - zur Außenwelt
  - zu angrenzenden Systemen

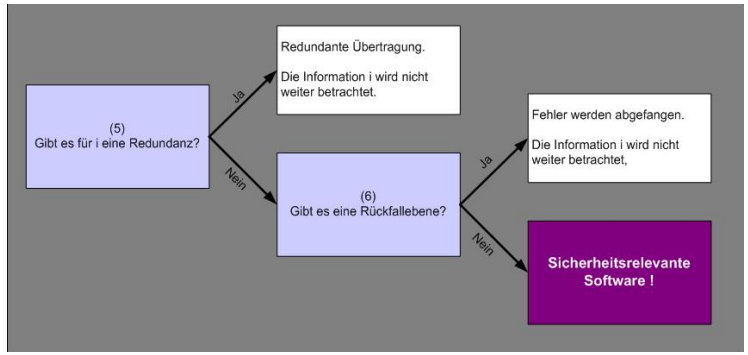


Methodisches Vorgehen

- Analyse der möglichen Fehler und ihrer Auswirkungen
  - für Verbindungen zur Außenwelt
  - für Verbindungen zu angrenzenden sicherheitsrelevanten Systemen
  - unter Beachtung von Rückfallebenen
- Bestimmung der Sicherheitsrelevanz
- Analyse der eingehenden Verbindungen
- Analyse der Anfälligkeit für falsche eingehende Signale

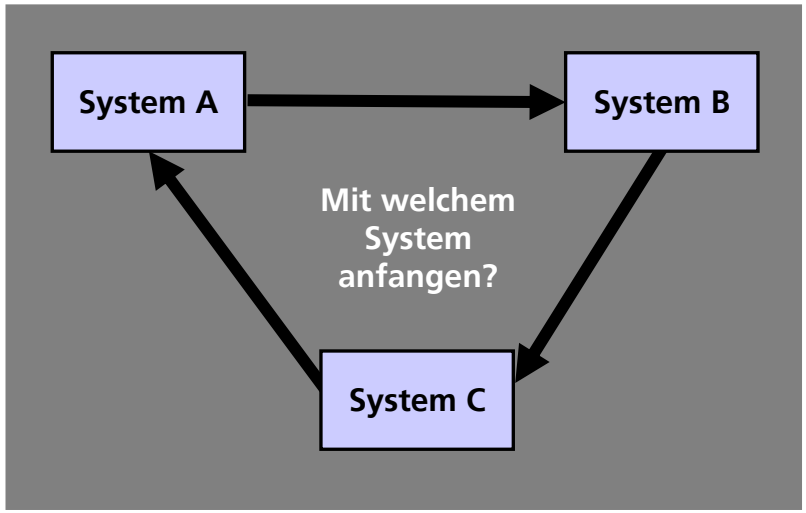
als Vorarbeit für die Systeme, die weiter im Innern liegen.





Weiteres Vorgehen / offene Punkte

- Stark verflochtene Systeme
- Design-Varianten
- Common Cause Failures
- Betrachtung von Mehrfachfehler
- Vollständigkeitskontrolle
- geeignete Systemgrenzen bzw. funktionale Abgrenzung



Vielen Dank für Ihre Aufmerksamkeit!