



Rail

Funktionale Systemdefinition anhand der EN 0015380-4

Ulrich Weber, TÜV Süd Rail GmbH
Sonja-Lara Kurz, TU Braunschweig

10./11. Oktober 2007
10. Workshop BieleSchweig in Braunschweig

TÜV SÜD Rail GmbH

TÜV®

Inhalt



Rail

- Motivation
- Ausgangslage
 - Was sagen die Normen?
 - Anforderungen an Systemdefinition
 - Projekt „KBTech Sicherungssystem“
- Systemdefinition
 - prEN 0015380-4
 - Klassifizierung mittels ERA Prozess
- Ausblick

TÜV SÜD Rail GmbH

TÜV®

10. Workshop BieleSchweig 10./11.10.2007

2



- gemäß CENELEC wird eine Systemdefinition für RAMS-Nachweise von Eisenbahnsystemen benötigt
- TÜV SÜD Rail GmbH führt Consulting - Projekt für koreanischen Hersteller KBTech durch:
Risikoanalyse zwecks Erstellung eines Hazard Logs
(Zugsicherungssystem für Metros oder Stadtbahnen („Light Rail“) angelehnt an ETCS Level2)
- auf Vorschlag von TÜV Süd Rail GmbH wird in diesem Projekt BP-Risk als Risikobewertungsmethode verwendet mit Zustimmung des Korean Railroad Resarch Institute (KRRI)



- **System:** „Eine Menge von Teilsystemen, die entsprechend einem Entwurf zusammenwirken“
- Es liegt in der Verantwortung der Eisenbahnverwaltung
 - das System zu definieren
(unabhängig von der technischen Realisierung !!!)
 - die für das System relevanten Gefährdungen zu identifizieren

Erste Aktivität der Risikoanalyse ist die Systemdefinition.

Abhängigkeit Gefährdungen zu Systemdefinition:

„Die Gefährdungen hängen von der Systemdefinition und insbesondere von den Systemgrenzen ab. Dieses erlaubt eine hierarchische Strukturierung der Gefährdungen in Bezug auf die Systeme und Teilsysteme. Das bedeutet auch, dass Gefährdungsidentifikation und Ursachenanalyse während der Systementwicklung auf verschiedenen Detaillierungsebenen wiederholt durchgeführt werden müssen.“

Phase 2: Systemdefinition und Anwendungsbedingungen

Zielsetzungen

- a) Festlegung des Betriebsaufgaben-Profiles des Systems
- b) Festlegung der Systemgrenzen
- c) Erstellen der Anwendungsbedingungen, die die Systemmerkmale beeinflussen
- d) Festlegung des Umfangs der Systemgefahrenanalyse (Hazard Analysis)

...

- **Function:** „specific purpose or objective to be accomplished, that can be specified or described without reference to the physical means of achieving it“ (IEC 61226:2005)
- **Requirement:** „necessary condition or ability to constrain the solutions of a task or an aim“
- „A function is not a requirement“

Ausgangslage

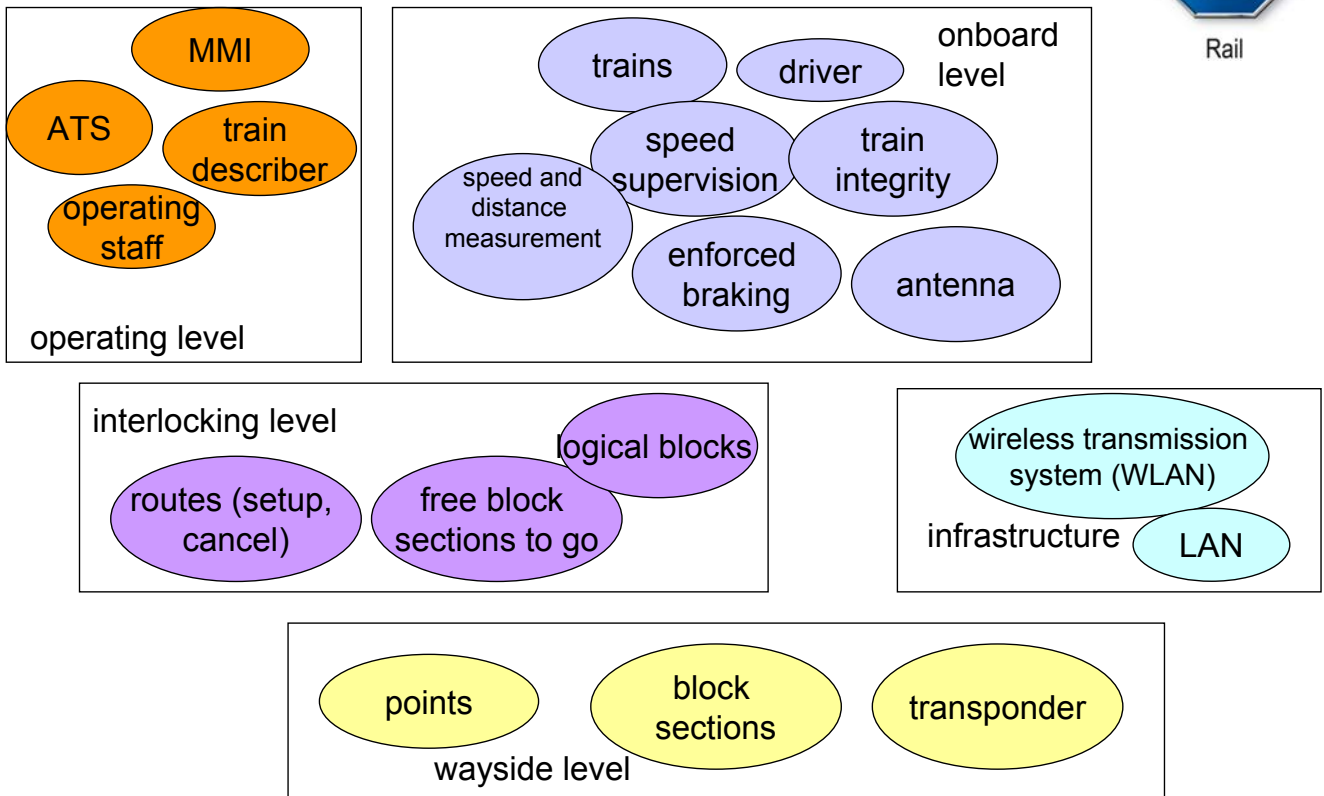
- bisher so gut wie keine Systemdefinitionen vorhanden
- die zukünftige Systemarchitektur ist (noch) nicht festgelegt aber evtl. aus vergleichbaren Projekten bekannt
- Systemanforderungen nicht oder nur teilweise spezifiziert (evtl. erste Entwürfe vorhanden)
- meistens ist eine allgemeine Systembeschreibung mit einigen Bildern vorhanden

- klare und präzise Formulierung der Funktionalität,
- Unabhängigkeit von der technischen Realisierung
- Identifizierbarkeit der Funktionen
- Strukturierung
 - sinnvolle d.h. realitätsnahe Strukturierung (Gruppierung)
 - hierarchische Strukturierung zur einfachen Identifikation von Gefährdungen

Wünschenswert:

- Unabhängigkeit zwischen Systemdefinition und Gefährdungen
- Standardisierung (soweit möglich)

- geplante Anwendung: **Metro und Light Rail**
- Ziel: Gesicherter Betrieb von Metro- oder Stadtbahnzügen („**KBTech System**“)
 - Fahrzeugseitig: Zugüberwachungsfunktionen (ATS)
 - Streckenseitig:
 - Stellwerksfunktionen,
 - Weichensteuerung,
 - Funktionen zur Zuglaufverfolgung,
 - automatische Fahrstraßeneinstellung,



Erfahrungen zu Systemdefinitionen

- nur wenige Begutachtungsprojekte vom TÜV Süd Rail GmbH, in denen Systemdefinitionen vorkommen (insbesondere in Deutschland)
- zur Begutachtung von Stellwerken, Zugbeeinflussungen etc. wird auf Anforderungsspezifikationen aufgesetzt und nur die Gefährdungsbeherrschung betrachtet
- weitere Projektbeispiele mit einer Systemdefinition:
 - ERTMS/ETCS (FRS ?)
 - Taiwan Highspeed Railway (Shinkansen) (?)

Bahnanwendungen – Kennzeichnungssystematik für Schienenfahrzeuge – Teil 4: **Funktionsgruppen** (Entwurf)

- Grundlage: DIN 25002 Teil 5 (Entwurf) und MODTrain Struktur von Siemens TS (= AEIF Struktur)
- Funktionen sind gruppiert in Levels, unabhängig von ihrer technischen Realisierung!
- Definition weiterer Funktionen ist ausdrücklich vorgesehen
- Entwurf (derzeit Bearbeitung in working group CEN/CENELEC/TC256/TC9X), noch nicht allgemein erhältlich

- Functional Breakdown Structure (FBS) – hierarchische Strukturierung, die Funktionen mit dem gleichen Fokus oder Service zusammenfasst
- Strukturierung der Funktionen in mehrere Levels (5 Level und übergreifende („traverse“) Funktionen
 - „traverse functions“ – vorgesehen für die gleichzeitige Verwendung in verschiedenen Levels
- Kennzeichnungsgruppen mittels „Code-Buchstaben“
- keine Klassifizierung als Sicherheitsfunktionen, da zunächst **alle** Funktionen gelistet werden sollen

B	Carry and protect passenger, train, crew and load
C	Provide appropriate conditions to passenger, train crew and payload
D	Provide access and loading
E	Connect vehicles and/or consists
F	Provide energy
G	Accelerate, maintain speed, brake and stop
H	Provide train communication, monitoring and control
J	Support and guide the train on the track
L	Integrate the vehicle into the complete system railway

Systemdefinition - Idee



- Vollständige Systemdefinition eines Schienenfahrzeugs anhand der EN 15380-4 (Ebenen 2 und 3)
- durch vollständige Schnittstellenbeschreibung zusätzliche Funktionen für das Eisenbahnsystem

Level				Function (level 1 to 5)	Example / explanation
1	2	3	*		
B	B			Arrange interior space	Interior design
B	B	B		Provide floor and flooring	Non slip floor covering
B	B	C		Provide roof and roofing	
B	B	D		Provide partitioning	Walls, screens, doors
B	C			Carry and enclose the load	(people and equipment)
B	D			Protect in case of crash	
B	E			Protect against fire	

Systemdefinition – Beispiel

Funktionsgruppe aus
EN 0015380-4 →

Zusätzliche Funktion
an Schnittstelle →

Code	Function	Interface
KEB	Provide interface with ATC	ATC
LEB	Supervise movement limits	ATP

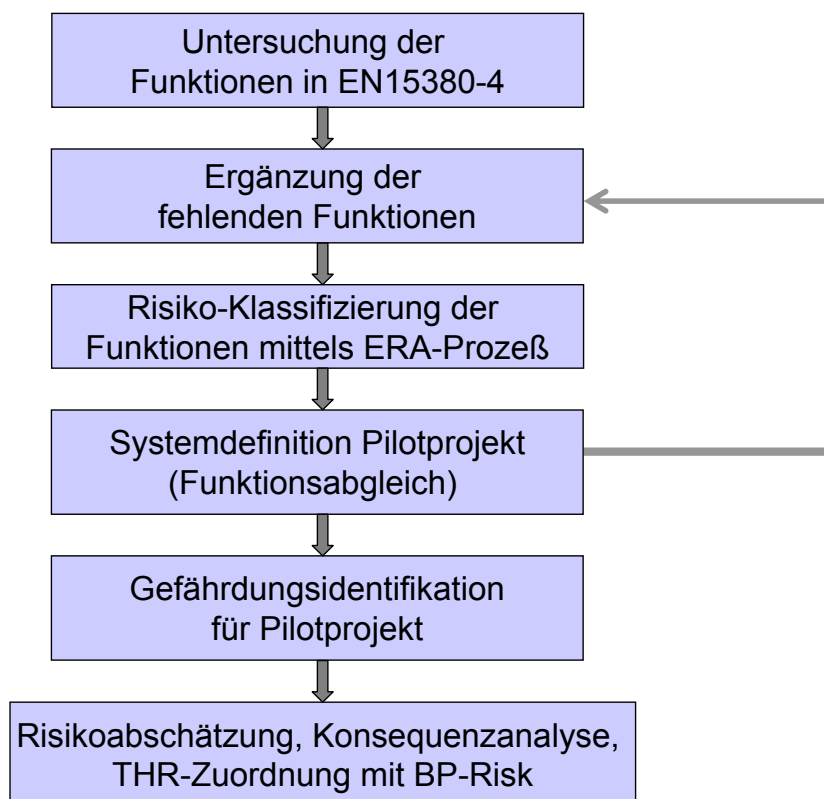
Beispiele für zusätzlich definierte Funktionen:

LGB – Control switches

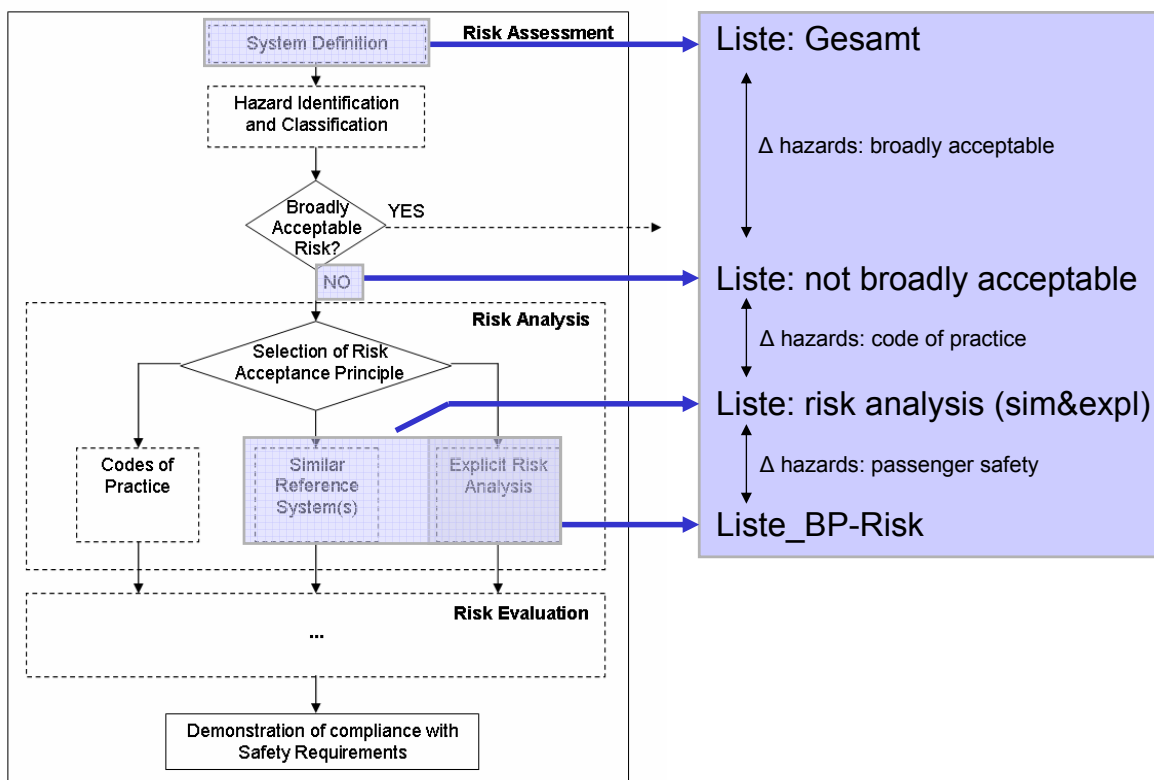
LGD – Supervise Level crossing

LGE – Ensure train spacing

Prinzipielle Vorgehensweise



ERA Prozess



- Methodik zur Kennzeichnung von Funktionen ist praktikabel auch für Ergänzungen oder zusätzliche Funktionen
- Funktionen sind jedoch ungenau spezifiziert bzw. unzureichend erläutert (Interpretierbarkeit)
- Funktionsstruktur aus prEN 15380-4 ist nur schwer auf Sicherungssysteme übertragbar - Ergänzungen sind notwendig
- Systemdefinition im Sinne dieses Vortrages erfüllt die Anforderungen der EN5012x, allerdings bezieht sich die EN50126 auf die Phase „Systemdefinition“, die weitere Aktivitäten umfasst

- Anwendbarkeit für Systemdefinition und anschließender Gefährdungsidentifikation anhand eines Pilotprojektes von TÜV Süd Rail GmbH erproben
- evtl. notwendige Verbesserungen/Ergänzungen zu der prEN0015380 der CENELEC working group vorschlagen
- Systemdefinition liegt in der Verantwortung der Eisenbahnverwaltung, d.h. genannte Probleme sind lösbar, allerdings sind unterschiedliche Systemausprägungen möglich
- offen ist die Behandlung von Funktionen, für deren Versagen die Risikoabschätzung nicht mit BP-Risk möglich ist

Vielen Dank für Ihre Aufmerksamkeit!

Fragen?