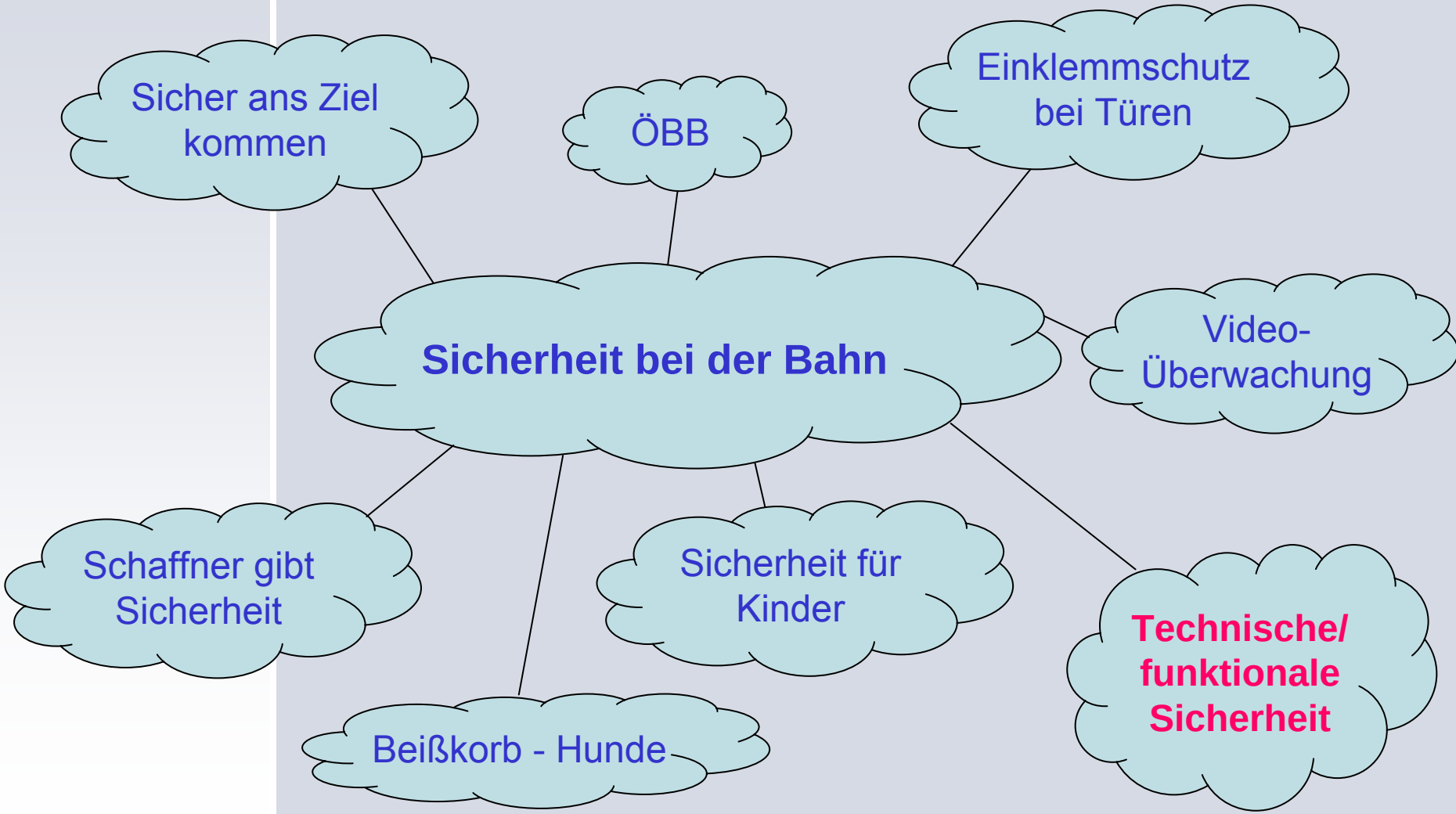
Quantitative Bewertung einer Sicherheitsfunktion

Tagung Moderne Schienenfahrzeuge
Graz 2007
16. April 2007

Dr. Daniel PROSTREDNIK
Dr. Hermann GEYER
Dipl.-Ing. Herbert SCHAMBÖCK
Dr. Rainer WEINMANN

ELIN EBG Traction
Cumberlandstraße 32-34
A-1140 Wien

Sicherheit bei der Bahn



ELIN EBG Traction

Sicherheitsanalyse bei Fahrzeugprojekten

Sicherheitsüberlegungen in der Bahntechnik

Bewertung technisch erreichbarer Sicherheit

Vermeidung von Risiken / Risikobewertung

Risikomatrix 

Schwere der Auswirkung eines Ereignisses und Eintrittswahrscheinlichkeit führt zur SIL-Einstufung

Risikoanalyse auf Betreiberseite /
Gefährdungsanalyse auf Herstellerseite

Sicherheitsanalyse bei Fahrzeugprojekten

Gefährdungsanalyse auf Fahrzeugebene führt zu sicherheitsrelvanten Teilsystemen, die dann in einer FMECA untersucht werden.

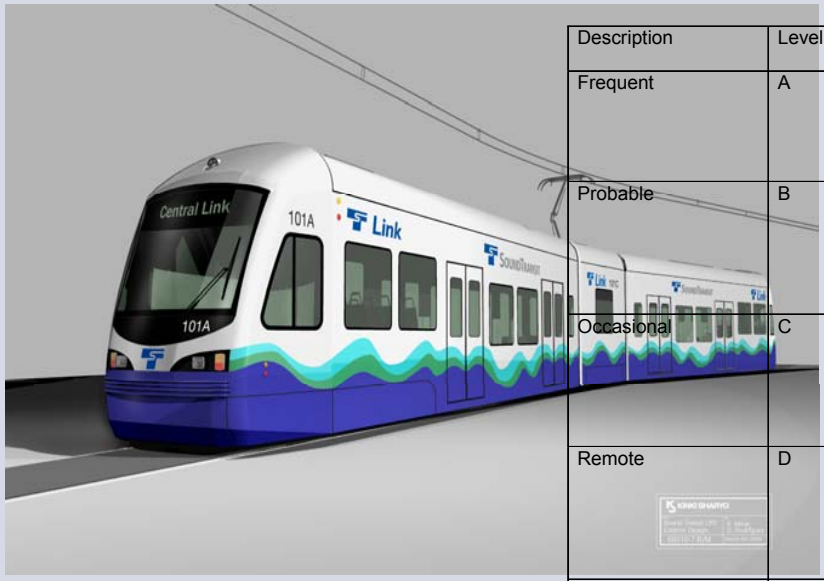
FMECA auf unterschiedlichen Ebenen (lokal/Bauteil, System, Fahrzeug, Betrieb, Sicherheit im Bahnsystem)

FMECA mit Quantifizierung für sicherheitsrelevante Subsysteme (z.B. Tür, Bremse) oder Fahrzeugfunktionen (z.B. Traktionssperre, Geschwindigkeitserfassung)

Fehlererkennung durch Überwachung / Funktionstests / Wartung

ELIN EBG Traction

Light Rail Vehicles Phoenix, Seattle / Gefährdungsanalyse



Description	Level	Specific Individual Item	Fleet or Inventory
Frequent	A	Likely to occur often in the life of an item, with a probability of occurrence greater than 10^{-1} in that life.	Continuously experienced.
Probable	B	Will occur several times in the life of an item, with a probability of occurrence less than 10^{-1} but greater than 10^{-2} in that life.	Will occur frequently.
Occasional	C	Likely to occur some time in the life of an item, with a probability of occurrence less than 10^{-2} but greater than 10^{-3} in that life.	Will occur several times.
Remote	D	Unlikely but possible to occur in the life of an item, with a probability of occurrence less than 10^{-3} but greater than 10^{-6} in that life.	Unlikely, but can reasonably be expected to occur.
Improbable	E	So unlikely, it can be assumed occurrence may not be experienced, with a probability of occurrence less than 10^{-6} in that life.	Unlikely to occur, but possible.

Description	Category	Environmental, Safety, and Health Result Criteria
Catastrophic	I	Could result in death, permanent total disability, loss exceeding $1M, or irreversible severe environmental damage that violates law or regulation.
Critical	II	Could result in permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel, loss exceeding $200K but less than $1M, or reversible environmental damage causing a violation of law or regulation.
Marginal	III	Could result in injury or occupational illness resulting in one or more lost work day(s), loss exceeding $10K but less than $200K, or mitigatible environmental damage without violation of law or regulation where restoration activities can be accomplished.
Negligible	IV	Could result in injury or illness not resulting in a lost work day, loss exceeding $2K but less than $10K, or minimal environmental damage not violating law or regulation.

ELIN EBG Traction

E-Talent Rh. 4023/4024 / fit-Werte für Gefährdungsanalyse

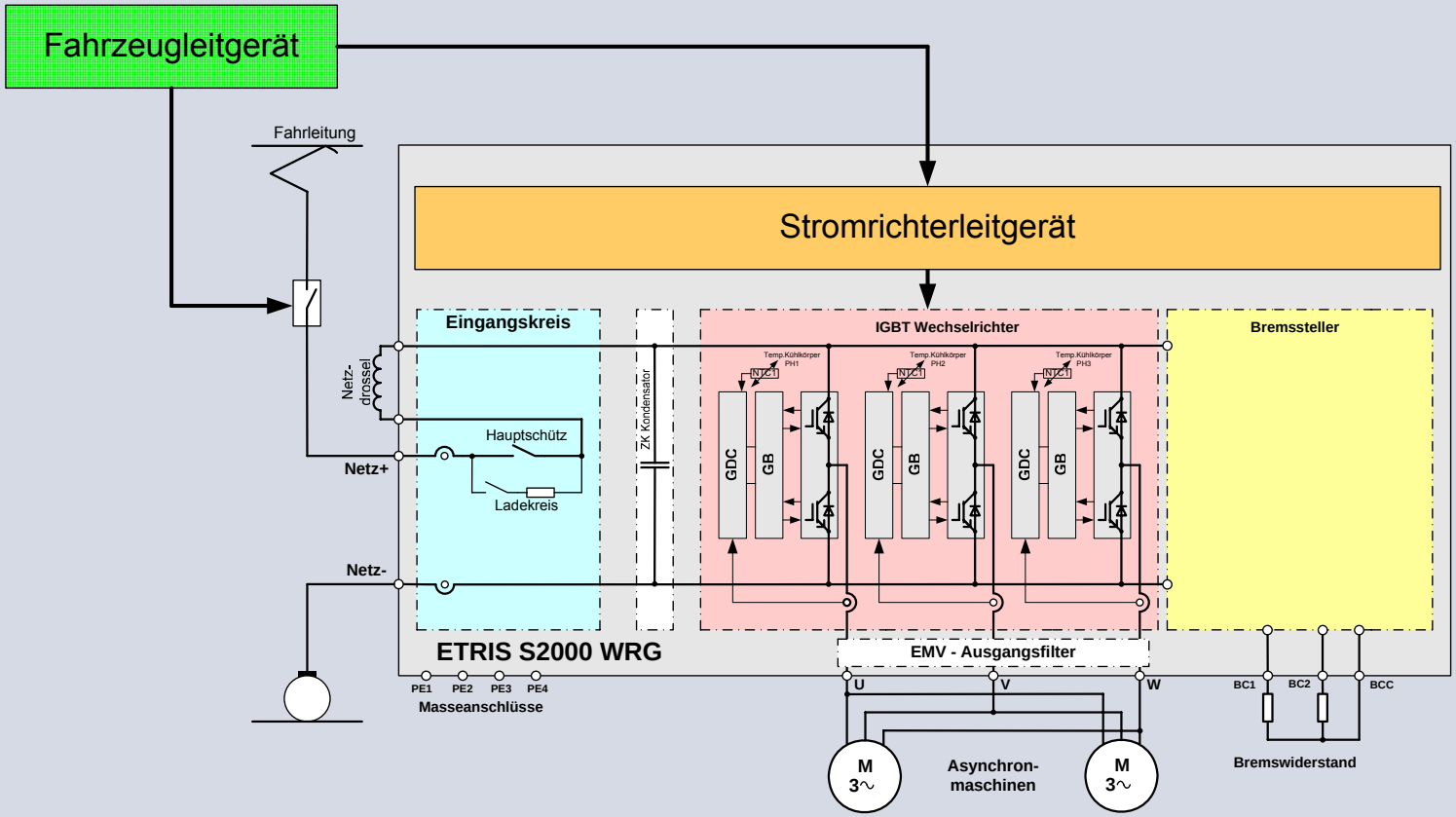
fit-Werte mit Zuordnung zur Ausfallshäufigkeit in der Risikoanalyse;

führt zu nachvollziehbarer und konsistenter Klassifizierung

Kategorie	Definition	Häufigkeit bei einem Fahrzeug über die Lebensdauer (30 Jahre)	fit-Bereich (Fehler / 10^9 Stunden)
häufig (F)	Wird häufig auftreten. Die Gefahr ist ständig gegenwärtig	>30 Fehler	210.000
wahrscheinlich (E)	Wird mehrmals auftreten. Es ist zu erwarten, dass die Gefahr oft eintritt	10-30 Fehler	69.000-210.000
gelegentlich (D)	Kann mehrmals auftreten. Es ist zu erwarten, dass die Gefahr mehrmals eintritt	3-10 Fehler	21.000-69.000
selten (C)	Kann manchmal während des Lebenszyklusses eintreten. Es ist sinnvoll, mit dem Eintreten der Gefahr zu rechnen.	1-3 Fehler	6.900-21.000
unwahrscheinlich (B)	Das Auftreten ist unwahrscheinlich, aber möglich. Es darf angenommen werden, dass diese Gefahr nur in Ausnahmefällen eintritt	0,01-1 Fehler	69-6.900
unvorstellbar (A)	Das Auftreten ist extrem unwahrscheinlich. Es darf angenommen werden, dass diese Gefahr nicht eintritt.	< 0,01 Fehler	< 69

Realisierungsansatz

Antriebsstrang - Prinzip:

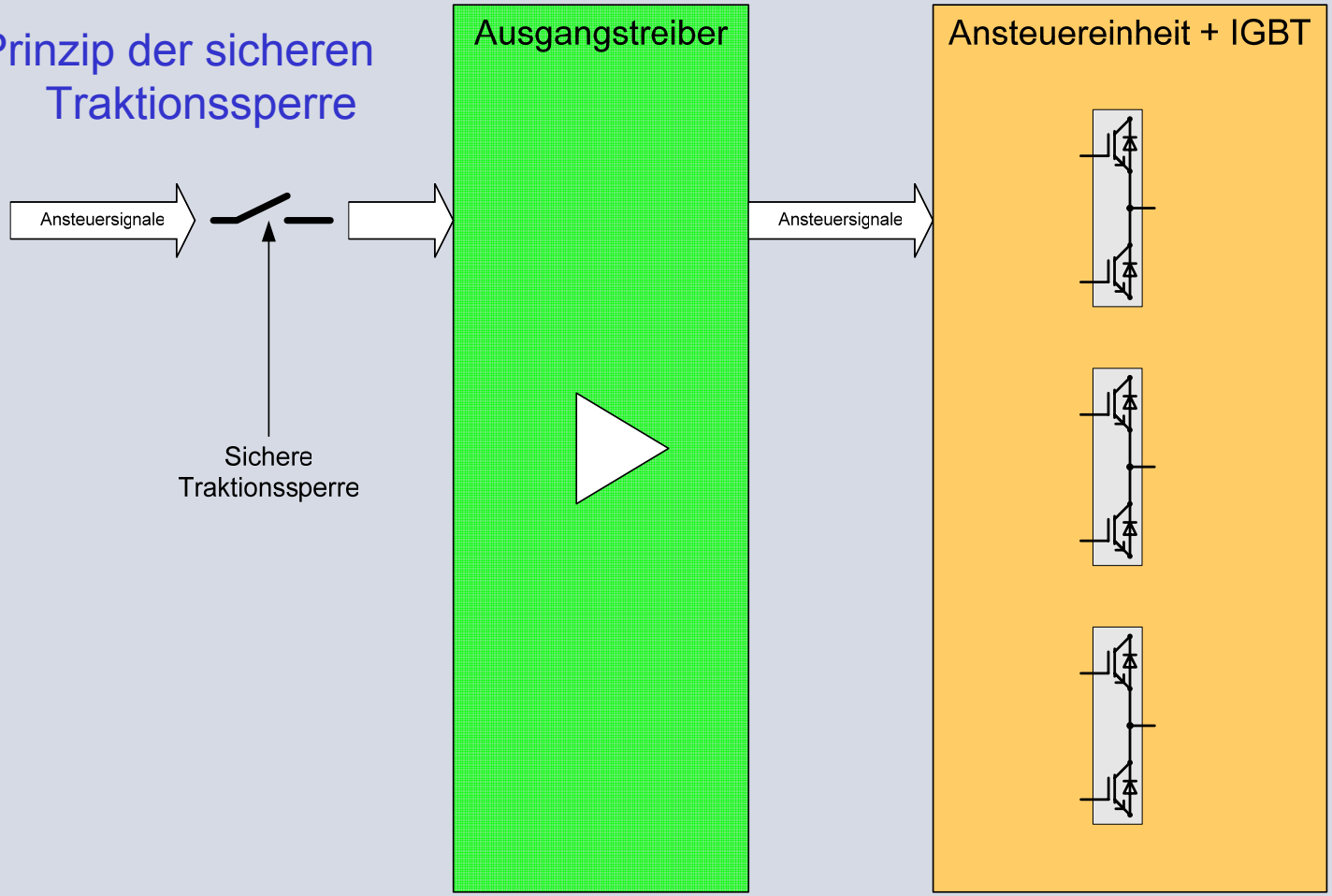


Hauptschalter - generell
- nach einer Bewegung v> Grenzwert

Realisierungsansatz

Bildung eines Drehmomentes durch den Umrichter muss sicher verhindert werden (Risikoanalyse -> SIL3)

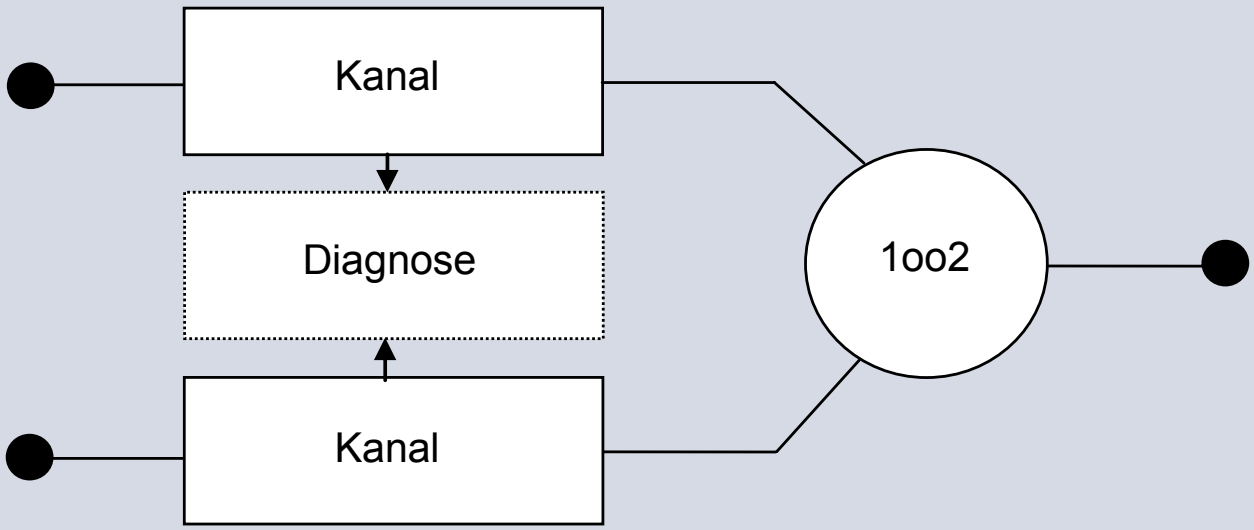
Prinzip der sicheren Traktionssperre



Entwicklung einer SIL Fahrzeugsteuerung

- Es müssen Maßnahmen zur Beherrschung der systematischen Fehler (entsprechen geforderter SIL Stufe) eingehalten werden
  - V Modell
- Es muss nachgewiesen werden, dass die Ausfallswahrscheinlichkeit der Sicherheitsfunktion (verursacht durch Zufallsfehler) kleiner ist als die für jeweilige SIL Stufe definierte Ausfallswahrscheinlichkeit.

SIL3 Anforderung = minimal zweikanalige Architektur



Funktion der Ausfallswahrscheinlichkeit eines Sicherheitsprozesses (nach IEC 61508)

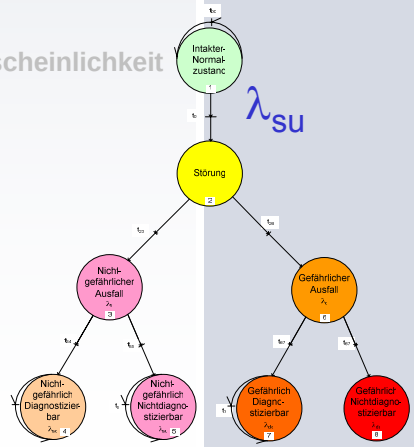
$$PFD\,(PFH) = f(\lambda_{dd}, \lambda_{du}, \lambda_{sd}, \lambda_{su}, \beta, \beta_D, T_1, MTTR)$$

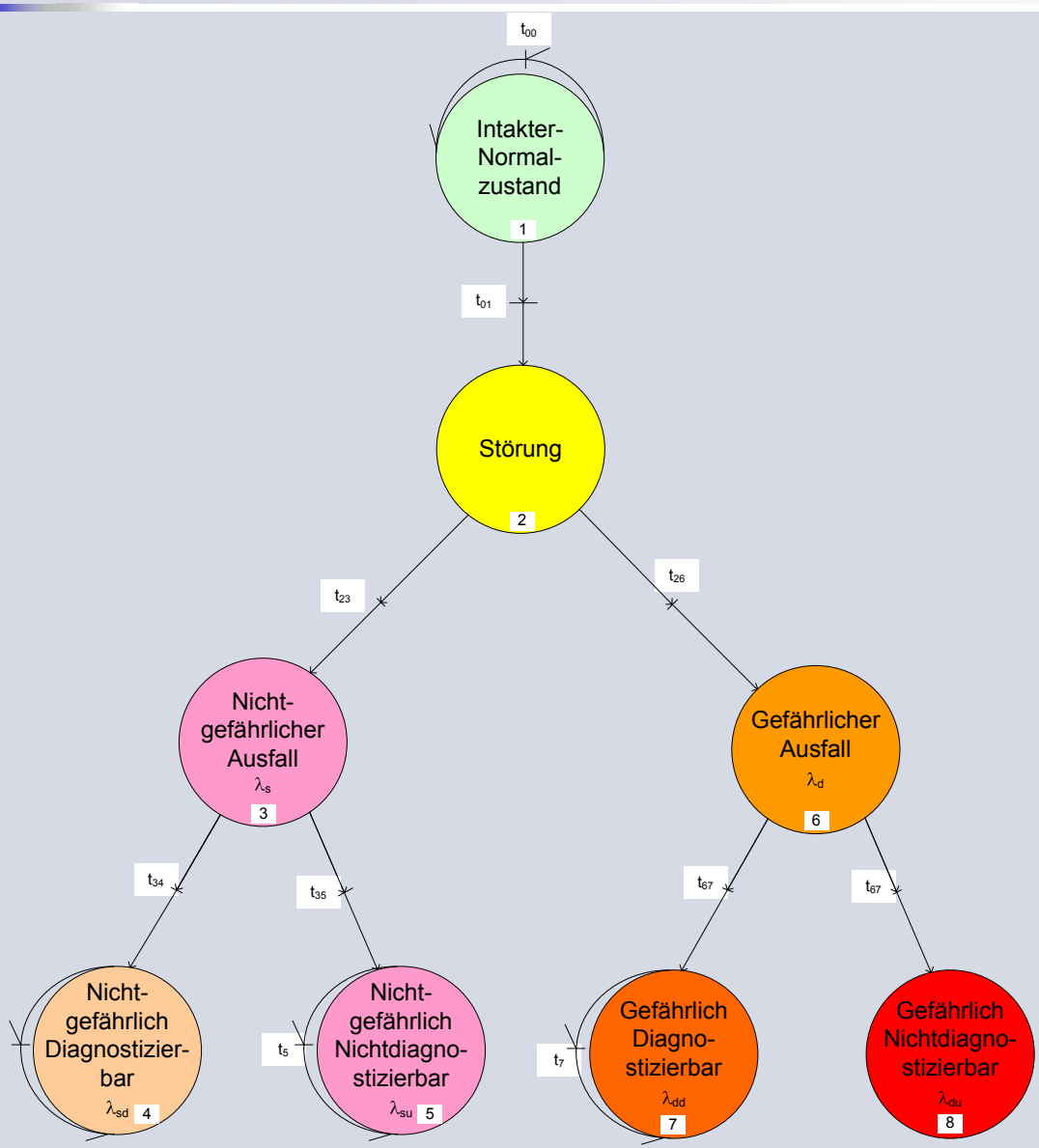
λ_{dd} Erkennbare (im Betrieb), sicherheitskritische Ausfälle (Fehler die durch Diagnose abgedeckt sind)

λ_{du} Nicht erkennbare (im Betrieb), sicherheitskritische Ausfälle (Fehler die durch Diagnose nicht abgedeckt sind)

λ_{sd} Erkennbare, nicht sicherheitskritische Ausfälle (Fehler die durch Diagnose abgedeckt sind)

λ_{su} Nicht erkennbare, nicht sicherheitskritische Ausfälle (Fehler die durch Diagnose nicht abgedeckt sind)





Funktion der Ausfallswahrscheinlichkeit eines Sicherheitsprozesses (nach IEC 61508)

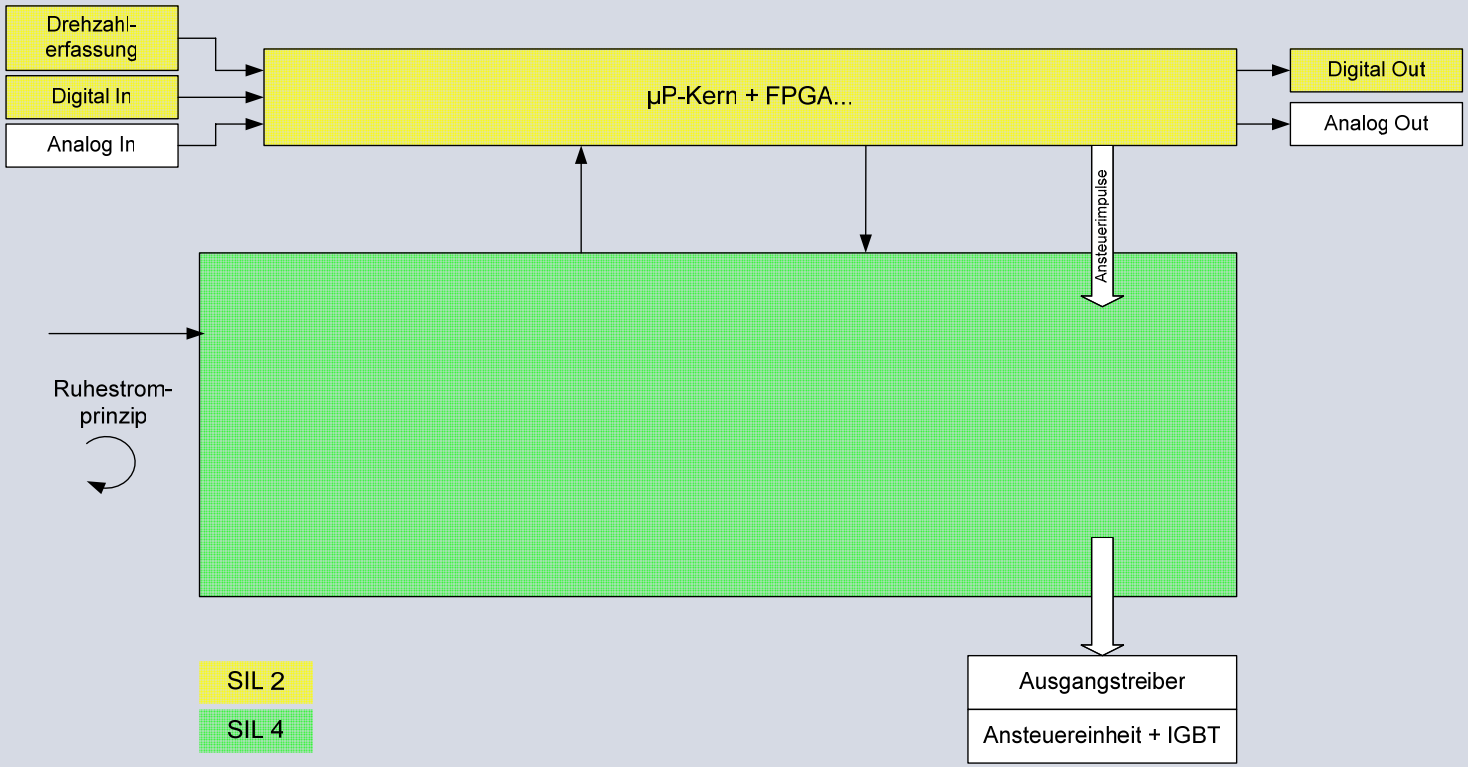
$$PFD\,(PFH) = f(\beta, \beta_D, \lambda_{dd}, \lambda_{du}, \lambda_{sd}, \lambda_{su}, T_1, MTTR)$$

β	Anteil unerkannter Ausfälle infolge gemeinsamer Ursache (β wird oft als $2x\beta_D$ angenommen)
β_D	Der Anteil der Ausfälle infolge gemeinsamer Ursache, die durch den Diagnosetest erkannt werden
T1	Intervall der Wiederholungsprüfung in [h]
MTTR	mittlere Zeit zur Wiederherstellung (sinngemäß jene Zeit, die im defekten Zustand gefahren werden muss) in [h]

FMEA - ein zentrales Werkzeug zur quantitativen Sicherheitsbewertung

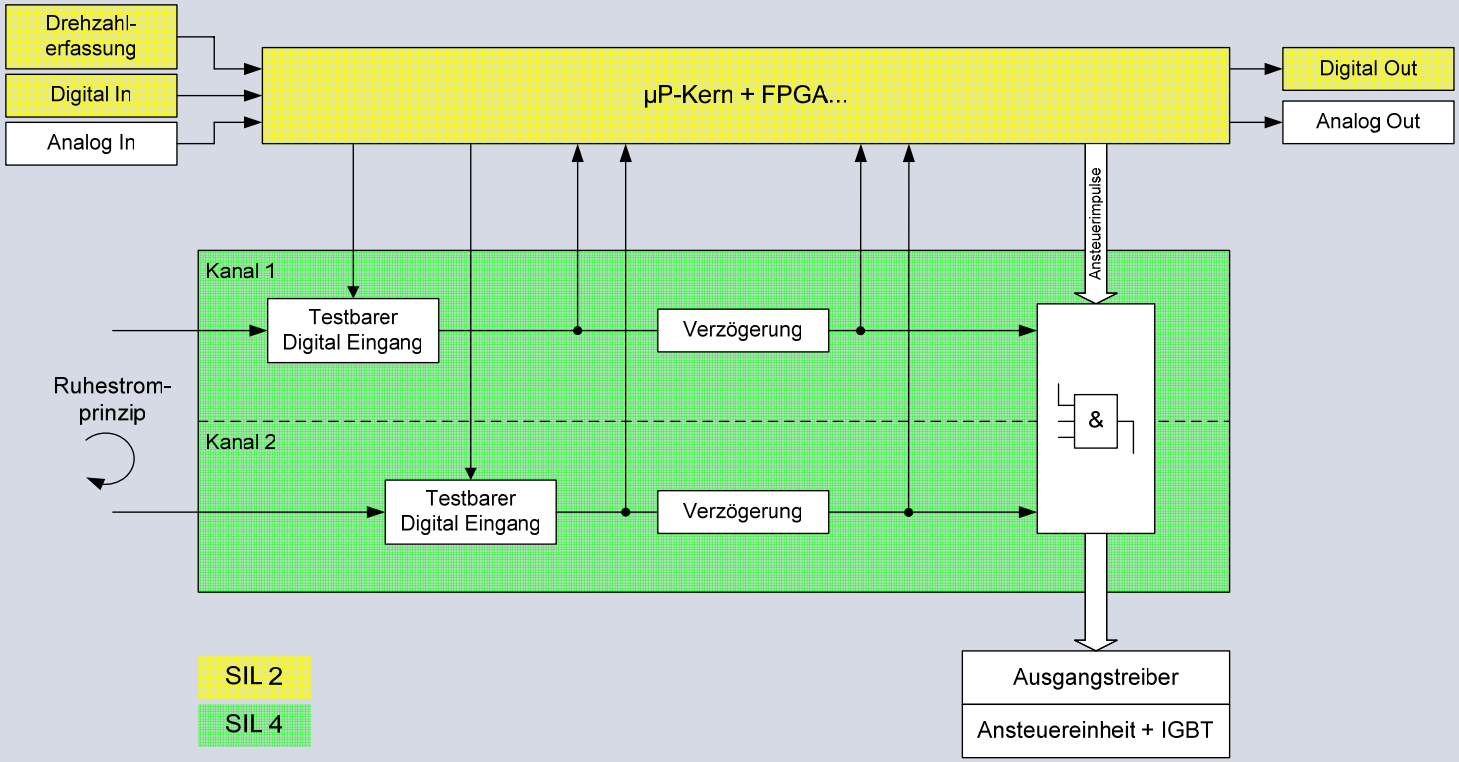
- Aufgabe - alle möglichen Fehler aufzulisten.
- Zu jeder Art des Fehlers ist die entsprechende Ursache zu finden, so wie die mögliche Auswirkung festzuhalten.
- „Fehlerbeherrschung“ führt die Maßnahme gegen den möglichen Fehler an.
- Die FMEA dient auch dazu, mögliche, nicht beherrschbare Fehler aufzulisten.
- Die „Fehlererkennung“ beschreibt wie ein Fehler im System erkannt werden kann (event. Anforderung an die Ergänzung der Architektur).
- Die Ausfallrate und Ausfallart haben eine Schlüsselfunktion

System **FMEA**



- Betrachtung der Gesamtfunktionalität
- Eine Quantifizierung kaum Möglich

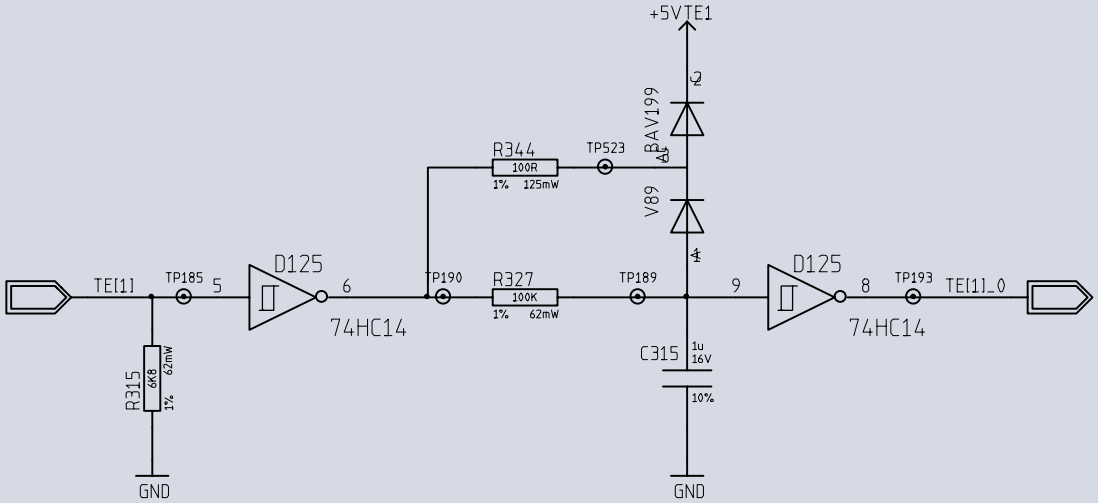
Block - **FMEA**



- Fehlermechanismen sind gut analysierbar Auswirkung und Beherrschung so wie die Quantifizierung der einzelnen Ausfallarten ist - auch wenn nur mit einer niedrigeren Genauigkeit - ausführbar.

Bauteil - **FMEA**

- Basisart der FMEA
- Zuverlässigste quantitative Sicherheitsbewertung.
- Ausfallswahrscheinlichkeit und die Ausfallart der Bauteile spielen eine besondere Rolle.



ELIN EBG Traction

Bauteil - **FMEA**

	Nr.	Bezeichnung	Fehler/Ausfall Sicherheitsfunktion	Fehlerursache	Fehlerauswirkung	Fehlerbeherrschung	Fehlererkennung	Maßnahme wenn notwendig (Selbstest /HW_SW)	Bemerkung
	B	**Fehler bei Betrachtung eines Kanals**							
	7A	**Einseitige Verzögerung**	Fehlerbedingt ist am Ausgangs des Blocks TE1_0 bzw. TE2_0 High-Level	Ausfall der Elektronik	Sichere Traktionssperre eines Kanals kann nicht ausgelöst werden	durch den zweiten Kanal	durch Überwachung und Vergleich der Signale TE1 (2) und DI-DO1 (2)	Durchführung des Vergleichs	Block 100% testbar
	7A1			Ausfall Keramikkondensator C315		durch den zweiten Kanal			
	7A2			Ausfall Widerstand R315		durch den zweiten Kanal			
	7A3			Ausfall Widerstand R327		durch den zweiten Kanal			
	7A4			Ausfall Diode UNI V89		durch den zweiten Kanal			
	7A5			Ausfall Diode UNI V199		durch den zweiten Kanal			
	7A6	**Einseitige Verzögerung**		Ausfall Digitale MOS-IC D215		durch den zweiten Kanal			
	7A7			Ausfall Lötstelle (6x)		durch den zweiten Kanal			
	7B	Block 31, 32 (Eingänge TE1; TE2, Ausgänge TE1_0; TE2_0	Fehlerbedingt ist am Ausgangs des Blocks TE1_0 bzw. TE2_0 Low-Level	Ausfall der Elektronik	Sichere Traktionssperre eines Kanals wird ständig ausgelöst (sicherer Zustand)	nicht notwendig	durch Überwachung und ergleich der Signale TE1 (2) und DI-DO1 (2)	Durchführung des Vergleichs	
	B1B1			Ausfall Keramikkondensator C315		durch den zweiten Kanal			
	B1B2			Ausfall Widerstand R344		durch den zweiten Kanal			
	B1B3			Ausfall Diode UNI V199		durch den zweiten Kanal			
	B1B4			Ausfall Digitale MOS-IC D215		durch den zweiten Kanal			
	B1B5			Ausfall Lötstelle (6x)		durch den zweiten Kanal			

Ausfallswahrscheinlichkeit

$$\lambda = \lambda_{ref} \,.\, a \,.\, b \,.\, c \,.\, d \,.\, ...$$

λ_{ref}	Ausfallrate bei Referenzbedingungen
a	Faktor für Spannungsabhängigkeit
b	Faktor für Stromabhängigkeit
c	Faktor für Temperaturabhängigkeit
d	Faktor für Abhängigkeit von Verschmutzung durch Staub
…..	Weitere Faktoren (chemische Einflüsse, Strahlung usw.)

Berechnung der MTBF Werte
- nach MIL-HDBK-217F
- nach SN 29500 (Berechnungsprogramms EXAR)

IEC TR 62380 und MIL-HDBK-338B führen auch die Basiswerte bzw. Korrekturparameter und Ausfallmodelle für die Berechnung der Ausfallraten an.

Ausfallsarten

Der Wert λ (Ausfallrate) trägt keine Information über die Art eines Ausfalls, bzw. über die Aufteilung (oder der Wahrscheinlichkeit der Aufteilung) der Ausfallarten.

Beispiel: Ein Widerstand kann (nach EN 50129) auf fünf Arten ausfallen:

- Unterbrechung
- Kurzschluss
- Vergrößerung des Widerstandes
- Verkleinerung des Widerstandes
- Kurzschluss zum Gehäuse

Von der konkreten Schaltung hängt es ab, ob eine bestimmte Ausfallart einen gefährlichen oder einen ungefährlichen Ausfall verursacht und ob ein solcher Ausfall mit eigenen Diagnosemitteln erkannt werden kann.

$\lambda = 1$ fit

Normativ geregelt:
EN 50129; MIL HDBK 338B; IEC TR 62380

Beurteilung durch Safety engineer

Ergebnis der Bauteil FMEA:
Vier Summen der Ausfallswahrscheinlichkeiten (λ_{du}, λ_{dd}, λ_{su}, λ_{sd}) für einen untersuchten Block/Kanal.

Klasse A und Klasse B von Subsystemen

Ein Subsystem wird der Klasse A zugerechnet wenn:

- Fehlermodelle von allen betrachteten Bauteilen bekannt sind und
- Das Fehlerverhalten des Subsystems bestimmbar ist und
- Ausreichend Daten über die tatsächliche Fehlerrate aus dem Feld vorliegen

Ein Subsystem wird der Klasse B zugerechnet wenn:

- Fehlermodelle von mindestens einem betrachteten Bauteil nicht bekannt ist und
- Das Fehlerverhalten des Subsystems nicht bestimmbar ist und
- Ausreichend Daten über die tatsächliche Fehlerrate aus dem Feld nicht vorliegen

Bei komplexeren elektronischen Systemen haben wir es praktisch ausschließlich mit der Klasse B zu tun.

Anteil ungefährlicher Ausfälle

SFF (Safe Failure Fraction) wird nach folgender Formel berechnet:

$$SFF = \frac{\sum \lambda_{su} + \lambda_{sd} + \lambda_{dd}}{\sum \lambda_{total}} \qquad DC = \frac{\sum \lambda_{dd}}{\sum \lambda_{dd} + \lambda_{du}}$$

Klasse A				Klasse B			
Anteil ungefährlicher Ausfälle	Hardware Fehlertoleranz			Anteil ungefährlicher Ausfälle	Hardware Fehlertoleranz		
SFF	N=0 (1oo1D, 2002D)	N=1 (1oo2D, 2oo3D)	N=2 (1oo3D)	SFF	N=0 (1oo1D, 2002D)	N=1 (1oo2D, 2oo3D)	N=2 (1oo3D)
< 60%	SIL1	SIL2	SIL3	< 60%	Nicht erlaubt	SIL1	SIL2
60% bis 90%	SIL2	SIL3	SIL4	60% bis 90%	SIL1	SIL2	SIL3
90% bis 99%	SIL3	SIL4	SIL4	90% bis 99%	SIL2	SIL3	SIL4
>= 99%	SIL4	SIL4	SIL4	>= 99%	SIL3	SIL4	SIL4

Fehlertoleranz N bedeutet N+1 Fehler können einen Verlust der Sicherheitsfunktion bedeuten

Ausfälle infolge gemeinsamer Ursache

Ein Ausfall der gleichzeitig in zwei (oder mehreren) getrennten Kanälen als Folge einer Ursache eintritt, führt zum Systemausfall und ist als besonders gefährlich zu betrachten.

Typische Beispiele:

- EMV Störungen
- Übertemperatur
- Spannungsversorgung

Bewertung mittels eines Fragenkataloges der IEC 61508-6

Berechnung der Ausfallswahrscheinlichkeit einer Sicherheitsfunktion

Bestimmung der PFD/PFH anhand der IEC 61508-6 - rechnerisch:

Architektur 1oo2D

$$PFH = 2((1-\beta)\lambda_{du}((1-\beta)\lambda_{du}) + (1-\beta_d)\lambda_{dd} + \lambda_{sd})t_{CE} + \beta_d\lambda_{dd} + \beta\lambda_{du}$$

$$t_{CE} = \frac{\lambda_{du}(\frac{T_1}{2} + MTTR) + (\lambda_{dd} + \lambda_{sd})MTTR}{\lambda_{du} + \lambda_{dd} + \lambda_{sd}}$$

Berechnung der Ausfallswahrscheinlichkeit einer Sicherheitsfunktion

Berechnungen der PFD/PFH Werte in der ELIN EBG Traction mit dem bereits vorgestellten Tool:

Common cause Parameter						
[%]	β =	2	Berechnung Beta			
Intervall der Wiederholprüfung						
[h]	T_1 =	24				
Mittlere Zeit zur Wiederherstellung						
[h]	MTTR =	8				
1oo2 ist ausgewählt						
		1oo1	**1oo2**	**1oo2D**	**2oo2**	**2oo3**
Mittlere Äquivalenzunklarzeit						
[h]	t_{CE} =	9,0	9,0	8,5	9,0	9,0
Mittlere Äquivalenzunklarzeit für eine Gruppe mit Ausgangsvergleicher oder Mehrheitsentscheider						
[h]	t_{GE} =	--	8,7	0,7	8,7	8,7
Wahrscheinlichkeit eines Ausfalls bei Anforderung						
	PFD =	7,91286E-04	1,1E-05	9,44731E-06	1,58320E-03	1,29696E-05
Ausfallswahrscheinlichkeit pro Stunde						
	PFH =	7,58000E-06	1,08726E-06	9,72748E-07	1,51600E-05	1,35858E-06

Antriebsleitgerät ELTAS ECON / Features

Ansteuerung für bis zu 10 Halbbrücken eines Antriebsstromrichters

Bussysteme (MVB, CAN, LON, RS485)

Digitale / analoge I/O in SIL2

Traktionssperre in SIL3 (4)

Programmierung nach IEC 61131

Diagnose-Software am PC

ELIN EBG Traction

Antriebsleitgerät ELTAS ECON / Anwendungen

Wiener Niederflur-
Straßenbahn ULF

Straßenbahn Sevilla / Spanien

Light Rail Vehicle Phoenix / Arizona

Light Rail Vehicle Seattle / Washington

Metro Brüssel

power that moves

Danke für Ihre Aufmerksamkeit!

Sicherheitsanalyse bei Fahrzeugprojekten

Risikomatrix nach EN50126

*Häufigkeit eines Gefahrenfalls	Risikostufen nach EN50126			
häufig	unerwünscht	intolerabel	intolerabel	intolerabel
wahrscheinlich	tolerabel	unerwünscht	intolerabel	intolerabel
gelegentlich	tolerabel	unerwünscht	unerwünscht	intolerabel
selten	vernachlässigbar	tolerabel	unerwünscht	unerwünscht
unwahrscheinlich	vernachlässigbar	vernachlässigbar	tolerabel	tolerabel
unvorstellbar	vernachlässigbar	vernachlässigbar	vernachlässigbar	vernachlässigbar
	unbedeutend	marginal	kritisch	katastrophal
	Gefahrenstufen			

*Die quantitative Bewertung der Häufigkeit von Gefahrenfällen hängt von der jeweiligen Anwendung ab

intolerabel	Muss ausgeschlossen werden
unerwünscht	Darf nur akzeptiert werden, wenn eine Risikoverminderung praktisch nicht durchführbar ist und eine Zustimmung des Bahnunternehmers vorliegt
tolerabel	Akzeptierbar bei geeigneter Überwachung und mit der Zustimmung des Bahnunternehmens
vernachlässigbar	Akzeptierbar, ohne weitere Zustimmung des Bahnunternehmens