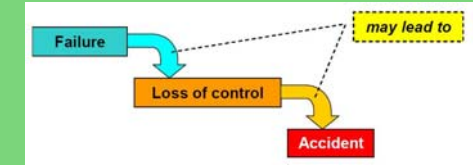
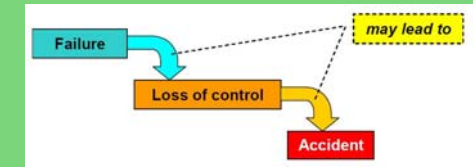


Das Controllability-Verfahren der Automobilwirtschaft und seine Übertragbarkeit in das Eisenbahnwesen



Gliederung

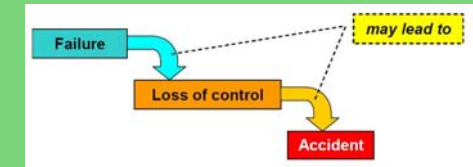
- Das Controllability-Verfahren
 - Herkunft
 - Vorgehen
 - Qualitatives und quantitatives Risikomodell
- Übertragbarkeit des Controllability-Verfahrens in das Eisenbahnwesen



Controllability - Motivation

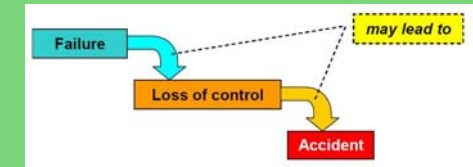
Aus Guidelines for the Safety Analysis of Vehicle Based Programmable Systems

- *Assessing the risk associated with a moving vehicle hazard is difficult because the vehicle is not static, and therefore the road (traffic) environment within which the vehicle operates varies continuously.*
- *severity... depends on the situation at the time*
- *Worst case scenarios not much help*



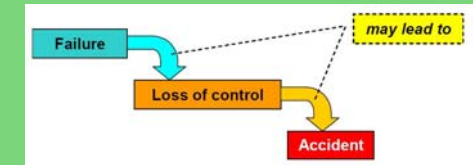
Herkunft

- Entwickelt im Rahmen des EU-Projektes DRIVE Safely
- Übernommen und weiterentwickelt durch MISRA
 - MISRA: Motor Industry Software Reliability Association
 - Konsortium verschiedener Organisationen z.B. Uk Department of Trade and Industry
Ford, Society of Motor Manufacturers and Traders, University of Leeds
 - Aufgabe: Entwicklung von „Guidelines for Vehicle Based Software“
- Veröffentlicht im MISRA Technical Report : Hazard Classification for Moving Vehicle Hazards
Controllability (May 2004) [1]



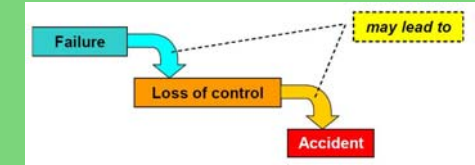
Controllability-Verfahren: Grundlagen

- Anzuwenden auf Gefährdungen des fahrenden Fahrzeugs
- Anwendung auf Gefährdungen des stehenden Fahrzeugs war nicht erfolgreich (keine Begründung gegeben); Berücksichtigung von Gefährdungen des stehenden Fahrzeugs in einem Risikographen [2]



Idee (I)

- Ein Versagen führt nicht notwendigerweise zu einem Unfall
- Fahrer oder Operator (von fahrzeugexternen Systemen) reagieren auf das Versagen und haben so die Möglichkeit, einen Unfall zu vermeiden
- Controllability beschreibt die Fähigkeit des Fahrers, von Fahrzeuginsassen oder des Operators, die Sicherheit der Fahrsituation nach Auftreten eines Versagens aufrecht zu erhalten.
- Weitere Reduktionsfaktoren werden nicht betrachtet.



Idee (II)

Parameter

- Level of System inter-dependency
- Loss of authority or control due to the hazard
- Provision of backup or mitigation
- Reaction time

Beurteilung auf einer Ordinalskale:

A (worst case) bis E (best case)

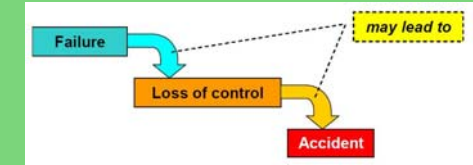
abschließende Klassenbildung durch

qualitative Mittelwertbildung



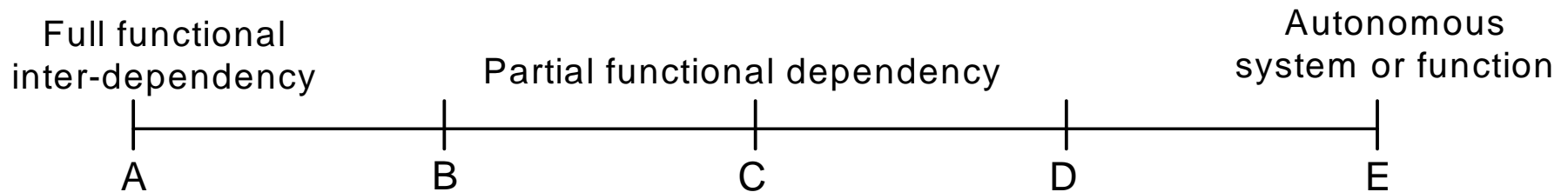
Controllability category	Definition
Uncontrollable	This relates to failures whose effects are not controllable by the road user, or vehicle occupants, and which are most likely to lead to extremely severe outcomes. The outcome cannot be influenced by a human response.
Difficult to control	This relates to failures whose effects are not normally controllable by the road user, or vehicle occupants but could, under favourable circumstances, be influenced by a human response. They are likely to lead to severe outcomes.
Debilitating	This relates to failures which significantly reduce the safety margin, but where a sensible human response can be expected. The outcomes are at worst severe.
Distracting	This relates to failures which produce operational limitations, but a normal human response will limit the outcome to no worse than minor.
Nuisance only	This relates to failures where safety is not normally considered to be affected, and where customer satisfaction is the main consideration.

höchsten Controllability-Klasse definiert
Safety Integrity Level für das System

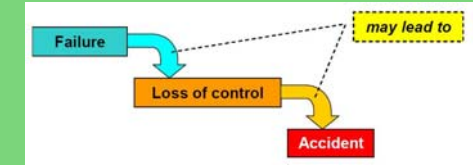


Level of System inter-dependency

- Wie sehr ist das Funktionieren anderer Systeme vom korrekten Funktionieren des betrachteten Systems abhängig?
- Betrachtet wird die funktionale Abhängigkeit

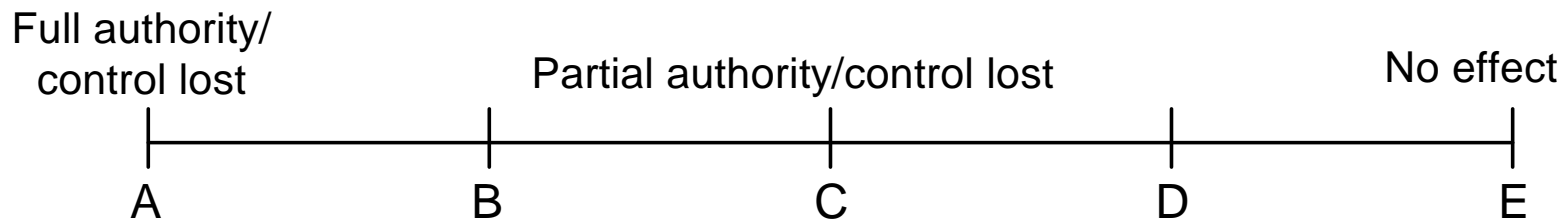


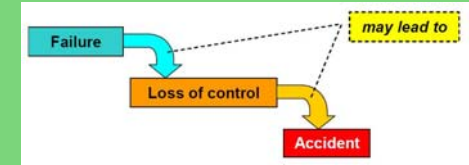
Controllability-Verfahren: Parameter



Loss of authority or control due to the hazards

- Wie stark ist die Beherrschung bzw. Kontrolle des Systems durch die Gefährdung eingeschränkt?





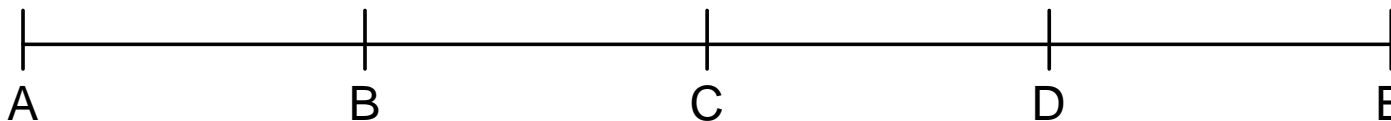
Provision of backup or mitigation

- Gibt es andere Funktionen (in anderen Systemen) mit deren Hilfe die Verkehrssicherheit aufrecht erhalten bzw. wieder hergestellt werden kann?

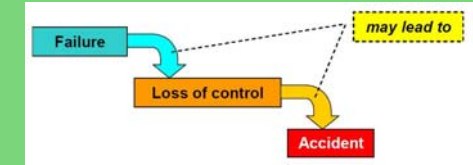
No other functions available

Other functions available, but with reduced functionality or safe state

Full redundancy or diversity, or functions not affected



Controllability-Verfahren: Parameter



Reaction time

- Mit welcher Geschwindigkeit muss eine Reaktion auf die Gefährdung erfolgen, um die Verkehrssicherheit mit Hilfe von Back-up- Funktionen wieder herzustellen?

Much faster than
humanly possible

A

B

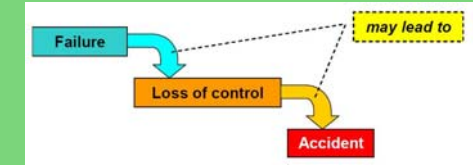
Similar to human

C

D

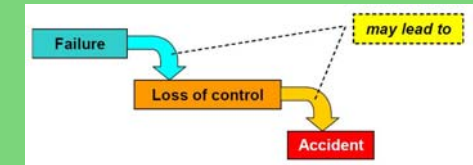
Similar to normal
traffic situation

E



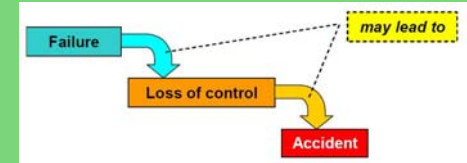
Controllability-Kategorien

	Controllability category	Definition	
A →	Uncontrollable	This relates to failures whose effects are not controllable by the road user, or vehicle occupants, and which are most likely to lead to extremely severe outcomes. The outcome cannot be influenced by a human response.	→ SIL 4
B →	Difficult to control	This relates to failures whose effects are not normally controllable by the road user, or vehicle occupants but could, under favourable circumstances, be influenced by a mature human response. They are likely to lead to very severe outcomes.	→ SIL 3
C →	Debilitating	This relates to failures whose effects are usually controllable by a sensible human response and, whilst there is a reduction in the safety margin, can usually be expected to lead to outcomes which are at worst severe.	→ SIL 2
D →	Distracting	This relates to failures which produce operational limitations, but a normal human response will limit the outcome to no worse than minor.	→ SIL 1
E →	Nuisance only	This relates to failures where safety is not normally considered to be affected, and where customer satisfaction is the main consideration.	



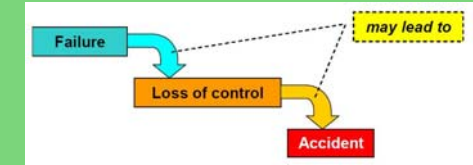
Diskussion der Grundlagen

- Es werden keine Definitionen gegeben.
- Es ist zu prüfen, ob das Verfahren in der Designphase zu sinnvollen Ergebnissen führt.
- Alle vier Parameter gehen gleichwertig in die Ergebnisermittlung ein.
- Es ist nicht angegeben, ob und ggf. wie die Wirkung weiterer Reduktionsfaktoren zu berücksichtigen ist.
- Es wird in den Kategorien ein Zusammenhang zwischen Controllability und Schadensausmaß hergestellt.

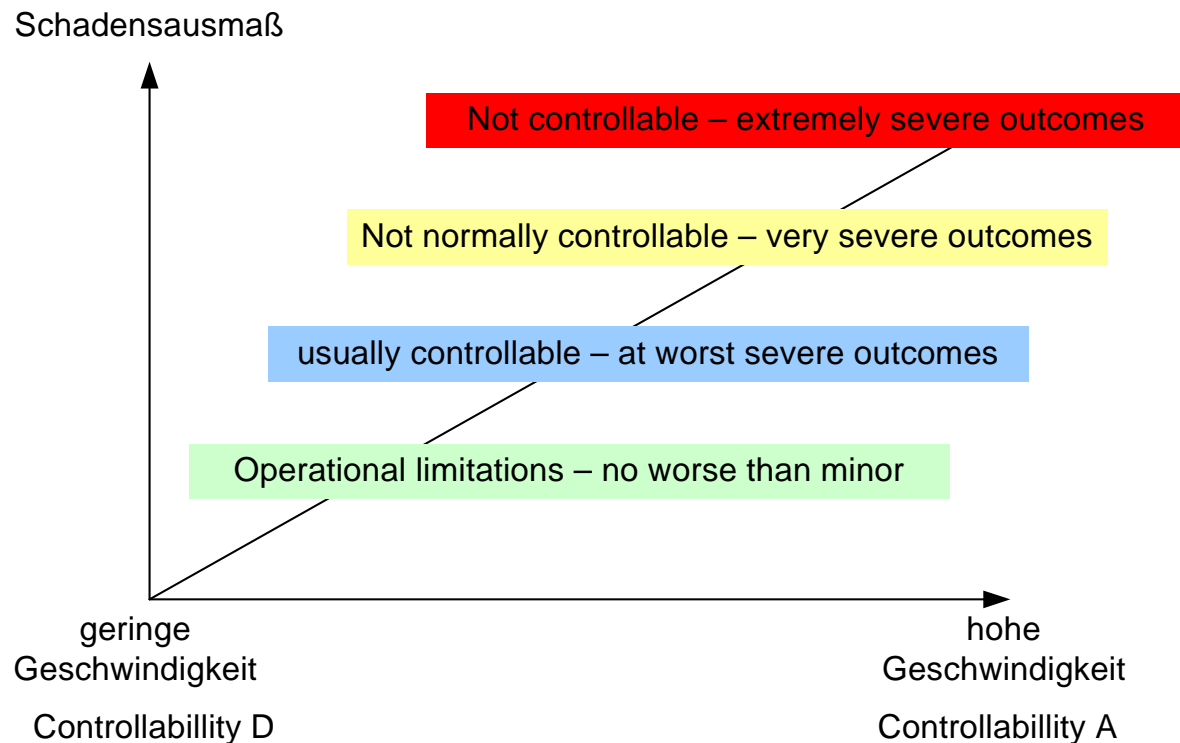


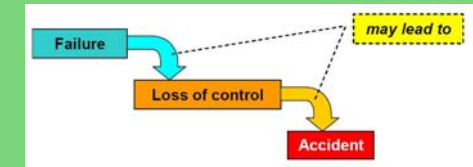
Diskussion der Grundlagen – Details (I)

- Die Controllability-Kategorien verknüpfen die Controllability mit dem Schadensausmaß. z.B. Kategorie: *Difficult to Control – very severe outcomes*; *Debilitating – at worst severe*
- Der Zusammenhang ist nachvollziehbar, wenn
 - die Geschwindigkeit als maßgebend für das Schadensausmaß angenommen wird, d.h. dass bessere Kontrollierbarkeit bedeutet, dass die Geschwindigkeit besser reduziert wird und damit das Schadensausmaß sinkt
 - davon ausgegangen wird, dass alle Unfälle bei gleicher (hoher) Geschwindigkeit auftreten
 - die Controllability der einzige bzgl. der Unfallabwehr zu berücksichtigende Faktor ist
- Gilt der Zusammenhang, ist dies die Begründung, warum die Anwendung auf Gefährdungen des stehenden Fahrzeugs nicht erfolgreich war.



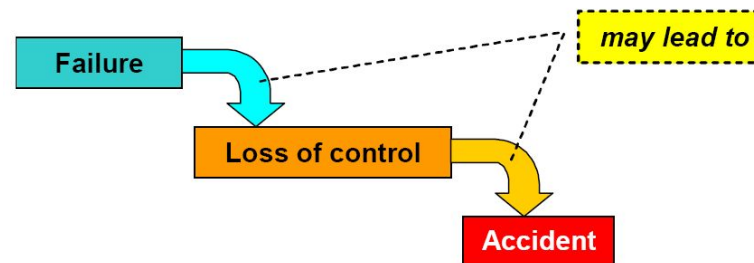
Diskussion der Grundlagen – Details (II)

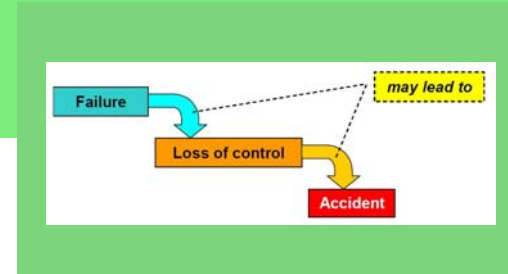




Qualitatives Risikomodell

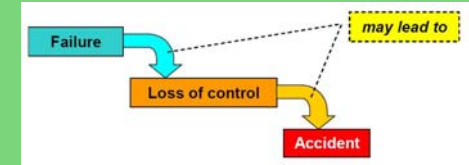
- Der Zusammenhang von Failure, Loss of control und Accident wird gegeben.
- Es werden keine weiteren Aussagen zu den den Parametern (Zusammenwirken, Einheiten) getroffen.
- Es werden keine Aussagen zu den Randbedingungen getroffen.





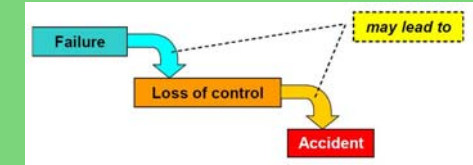
Quantitatives Risikomodell: SIL nach IEC 61508

SAFETY INTEGRITY LEVEL	LOW DEMAND MODE OF OPERATION (Probability of failure to perform its design function on demand)	CONTINUOUS/HIGH DEMAND MODE OF OPERATION (Prob of a dangerous failure per hour)
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$



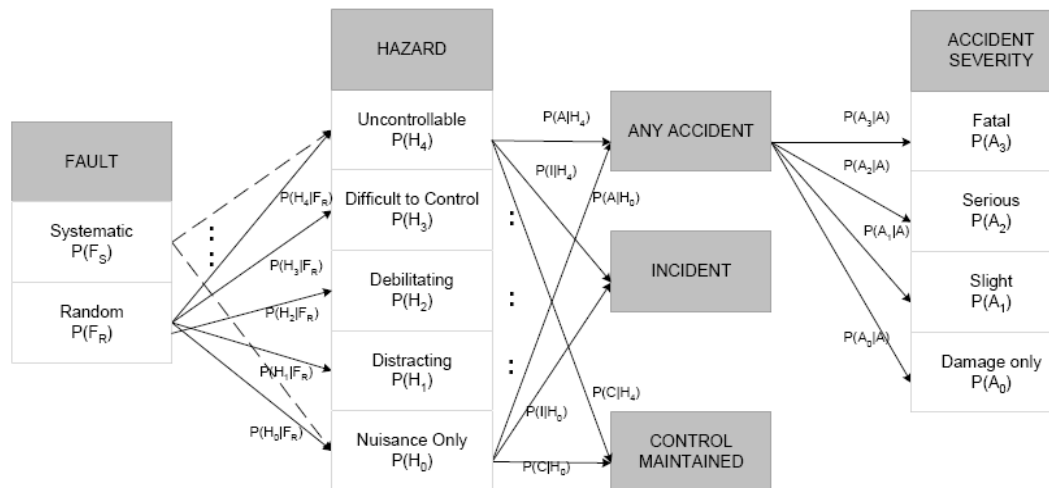
Alternative Betrachtung: Arbeit nach Evans [3]

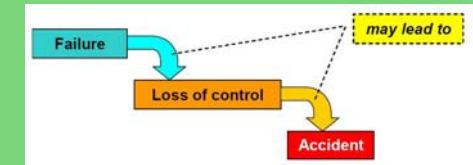
- Basierend auf Ergebnisse von DRIVE Safely: Ableitung von Safety Targets für Random Failure of Programmable Vehicle Based Systems
- Evans gibt qualitatives Risikomodell, welches die Controllability berücksichtigt
- Evans leitet Zahlenwerte her.



Alternatives qualitatives Risikomodell

- Evans gibt ein Risikomodell als Grundlage zur Risikoberechnung, dem die Einbindung des Controllability-Faktors zu entnehmen ist.

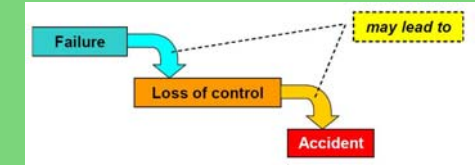




Modell nach Evans (I)

Vorgehen zur Ableitung von Sicherheitszielen für Random Failure für die Controllability-Kategorie Uncontrollable:

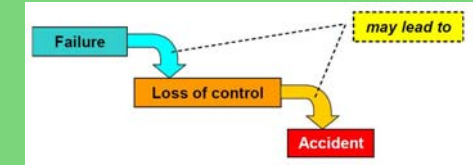
- Ableitung eines tolerierbaren Risikos nach MEM und HSE: 10^{-5} und 10^{-6} Tote je Person und Jahr
- Nur gültig unter der Annahme, dass im Fall eines Unfalls maximal ein Todesopfer zu beklagen ist
- Zuweisung des Risikoanteils für die Uncontrollable-Kategorie anhand Unfallschaden-Verteilung für Todesfälle (0,09 %)



Modell nach Evans (II)

- *For moving vehicle hazards, the distribution of outcomes given a hazardous event, is considered to be constant [jesty06]*
- *A statistical analysis of a sample of the data shows that the severity distribution is largely independent of driving condition...the overall distribution of outcomes is fixed and that the significant factor becomes the probability of an accident, independent of the level of uncontrollability of a hazard [3]*

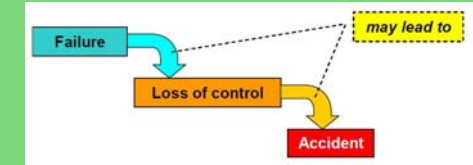
Unfälle mit	Angabe in Prozent nach [Evans00]
Todesfällen	0,09
Schwerverletzten	0,92
Leichtverletzten	5,23
Sachschaden	93,76



Modell nach Evans (III)

Vorgehen zur Ableitung von Sicherheitszielen für Random Failure für die Controllability-Kategorie Uncontrollable :

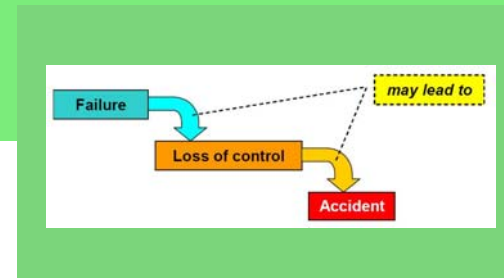
- Ableitung eines tolerierbaren Risikos nach MEM und HSE: 10^{-5} und 10^{-6} Tote je Person und Jahr
- Nur gültig unter der Annahme, dass im Fall eines Unfalls maximal ein Todesopfer zu beklagen ist
- Zuweisung des Risikoanteils für die Uncontrollable-Kategorie anhand Unfallschaden-Verteilung für Todesfälle (0,09 %)
- Aufteilung des Wertes auf 10 Systeme, die überhaupt nur Gefährdungen der obersten Klasse zur Folge haben können
- Zulässige Gefährdungsrate für Uncontrollable –Gefährdungen: 10^{-7} Gefährdungen pro Stunde
- „*results for the remaining controlability categories may be calculated in the same way*“



Modell nach Evans (IV)

Diskussion:

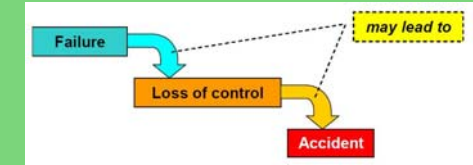
- Werte für andere Klassen können nicht entsprechend kalkuliert werden, da u.a. es nur zwei weitere Schadensgruppen, aber drei weitere Controllability-Kategorien gibt
- stattdessen: Berechnung erfolgt unter Berücksichtigung des 0,09 prozentigen Anteils für tödlichen Personenschaden; variiert wird der Einfluss des Controllability-Faktors



Modell nach Evans (VI)

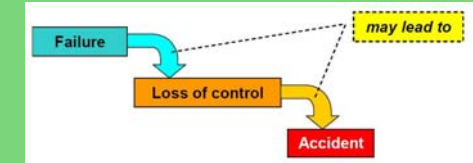
- *A hazard classified as uncontrollable will result in either an incident or an accident with a probability of 1.*
- *A hazard classified as nuisance only will not result in an incident or accident.*
- *There is likely to be a logarithmic relationship linking the likelihood of an accident for the remaining three categories of controllability. [3]*

Kontrollierbarkeitskategorie		Angenommene Wahrscheinlichkeit für einen Unfall nach Auftreten einer Gefährdung	
Uncontrollable	A	1	Jede Gefährdung führt zum Unfall
Difficult to control	B	0,1	Eine von 10 Gefährdungen führt zum Unfall.
Debilitating	C	0,01	Eine von 100 Gefährdungen führt zum Unfall.
Distracting	D	0,001	Eine von 1000 Gefährdungen führt zum Unfall.
Nuisance only	E	0	Keine Gefährdung führt zum Unfall.



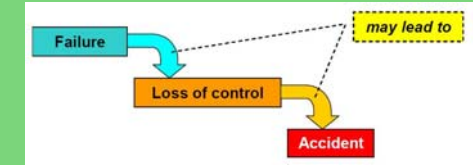
Modell nach Evans (VII)

Kategorie	Unfall-/Vorfall-wahrscheinlichkeit	zul Gefährdungsrate
Uncontrollable	1	10^{-7}
Difficult to Control	0,1	10^{-6}
Debilyting	0,01	10^{-5}
Distracting	0,001	10^{-4}
Nuisance only	0	



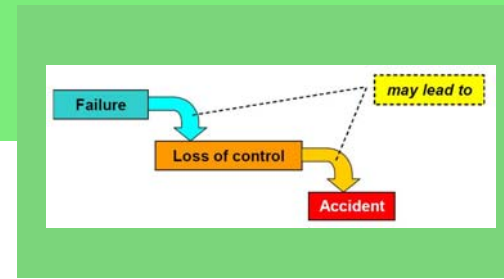
Modell Controllability-Faktor (I)

- Laut MISRA ist Risiko Produkt aus Schaden S , Auftretensfrequenz F und Controllability C : $R=S*F*C$
- Führt zu sinnvollen Ergebnissen, wenn die Gefährdungsrate h berücksichtigt wird: $R=S*F*C *h$
- Annahme: Berechnung der zulässigen Gefährdungsrate $h_{zul}=R_{tol}/(S*F*C)$



Modell Controllability-Faktot (II)

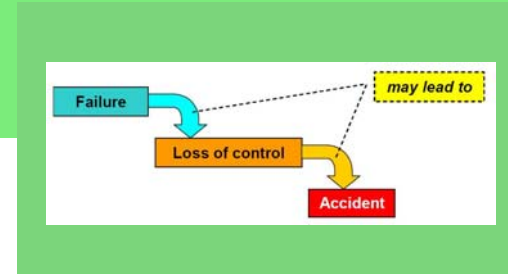
- Für den Schaden kann der worst case angenommen werden: Bei jedem Unfall ist mit einem Toten zu rechnen.
- Alternativ kann anhand des Schadensprofils ein durchschnittlicher Schaden berechnet werden:
 - $1 \text{ äquivalenter Tote} = \text{Tote} + \text{Schwerverletzte}/10 + \text{Leichtverletzte}/100$
 - Daraus ergibt sich: $1 * 1,52 + 0,1 * 14,73 + 0,01 * 83,75 = 0,04$ äquivalente Tote



Modell Controllability-Faktot (III)

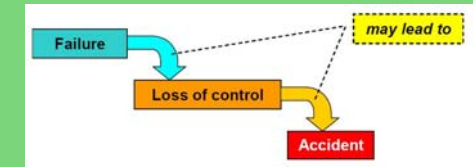
- „...Travelling in a vehicle along a road is, by its very nature, a hazardous undertaking, and thus the ‘frequency and exposure time’ parameter is effectively a constant” [4]: Der Wert für F wird zu eins gesetzt.
- Controllability C:

Kontrollierbarkeitskategorie		Angenommene Wahrscheinlichkeit für einen Unfall nach Auftreten einer Gefährdung	
Uncontrollable	A	1	Jede Gefährdung führt zum Unfall
Difficult to control	B	0,1	Eine von 10 Gefährdungen führt zum Unfall.
Debilitating	C	0,01	Eine von 100 Gefährdungen führt zum Unfall.
Distracting	D	0,001	Eine von 1000 Gefährdungen führt zum Unfall.
Nuisance only	E	0	Keine Gefährdung führt zum Unfall.



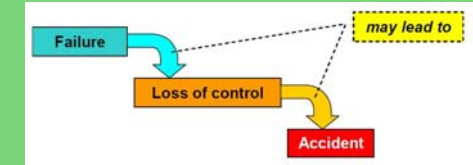
Modell Controllability-Faktot (V)

Kategorie	Unfall-/Vorfall-wahrscheinlichkeit	zul Gefährdungsrate (pro Stunde)	
		worst case	Durchschnitt
Uncontrollable	1	10^{-9}	$2,5 * 10^{-8}$
Difficult to Control	0,1	10^{-8}	$2,5 * 10^{-7}$
Debilyting	0,01	10^{-7}	$2,5 * 10^{-6}$
Distracting	0,001	10^{-6}	$2,5 * 10^{-5}$
Nuisance only	0		



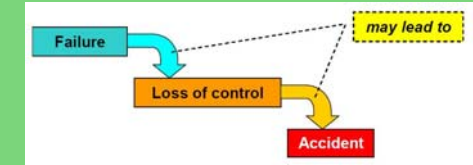
Das Controllability-Verfahren im Eisenbahnwesen

- Vorgehen bei der Risikoanalyse z.B. in EN 50126, EN 50129 festgelegt
- Konsequenzenanalyse, Risikoabschätzung schwierig, da
 - Reduktionsfaktoren schwierig und niemals vollständig zu ermitteln sind
 - Schadensschätzungen von zu vielen Randbedingungen anhängig sind
 - zuverlässige Zahlenwerte fehlen
- Controllability-Verfahren erlaubt den Verzicht auf eine detaillierte Konsequenzenanalyse; Reduktionsfaktoren gehen implizit bei der Verfahrenskonstruktion ein oder werden allein durch Controllability-Beschreibung ersetzt



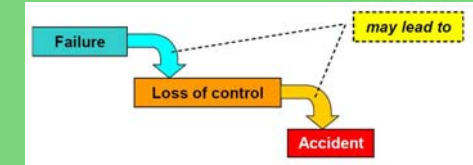
Vorgehen

- Ist die Grundidee übertragbar?
- Sind die Parameter übertragbar?
- Ist das Risikomodell übertragbar?
- Welche Unterschied sind bei der Ableitung der quantitativen Werte zu beachten?



Grundidee

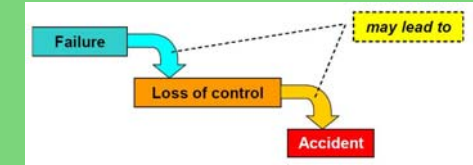
- Ein Versagen führt nicht notwendigerweise zu einem Unfall
→ ok.
- Fahrer oder Operator reagieren auf das Versagen und haben so die Möglichkeit, einen Unfall zu vermeiden
→ an Stelle von Operator: Fahrdienstleiter
- Controllability beschreibt die Fähigkeit des Fahrers, von Fahrzeuginsassen oder des Operators, die Sicherheit der Fahrsituation nach Auftreten eines Versagens aufrecht zu erhalten.
→ Einfluss haben Fahrer und Fahrdienstleiter, u.U. Betriebspersonal, nicht Fahrgäste



Parameter (I)

Level of System inter-dependency

- Zusammenhang gilt auch im Eisenbahnwesen
- Abhängigkeiten innerhalb von Systemen werden durch Perrow [4] beschrieben: *Complexity* und *Coupling*
- Abbildung beider Einflussgrößen in Parametern scheint sinnvoll; ist zu prüfen



Parameter (II)

Loss of authority or control due to the hazard

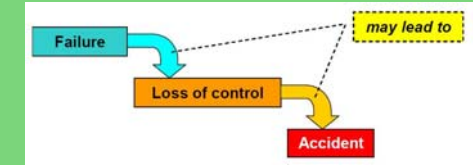
- sollte berücksichtigt werden
- aber: Autofahrer hat mehr Freiheitsgrade als Triebfahrzeugführer

Provision of backup or mitigation

- Zusammenhang gilt auch im Eisenbahnwesen
- u.U. ungewünschte Einschränkungen, da funktionale Abhängigkeiten im Design-Prozess noch geändert werden können

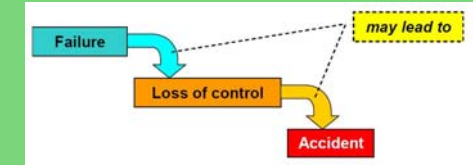
Reaction time

- Parameter kann übernommen werden



Parameter (III)

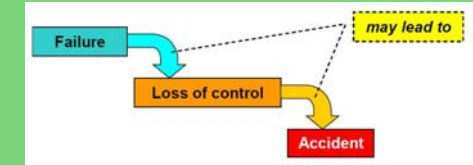
- Es sollte ein (formelmäßiger?) Zusammenhang zwischen den Parametern aufgestellt werden. In diesem Zusammenhang ist die Wichtung der Parameter zu diskutieren.
- Es ist zu entscheiden, wie vorzugehen ist, wenn die Beurteilung für einen oder mehrere Parameter nicht möglich ist.
- Es ist zu analysieren, ob weitere Parameter (Reduktionsfaktoren) zur Beurteilung der Unfallwahrscheinlichkeit herangezogen werden sollten – explizit oder implizit



Reduktionsfaktoren

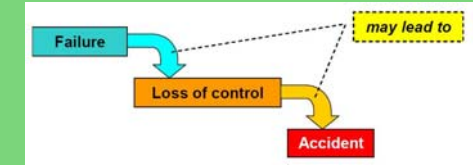
Typische Reduktionsfaktoren im Eisenbahnwesen:

- Einfluss der Infrastruktur
 - Eisenbahnfahrzeuge haben definierten Fahrweg, nur an wenigen Punkten bestehen Kreuzungsmöglichkeiten
 - Eisenbahnfahrzeuge können nicht ausweichen
- Einfluss des Betriebsprogramms:
 - Zügen folgen mit zeitlichem Mindestabstand
 - In Abhängigkeit der betrachteten Strecke sind Aussagen zum Betriebsprogramm möglich
 - Kurzfristige, wesentliche Änderungen der Auslastung sind nicht zu erwarten
- Einfluss von Sicherheitssystemen: wird im Controllability-Verfahren erfasst
- Einfluss des Menschen: wird im Controllability-Verfahren erfasst



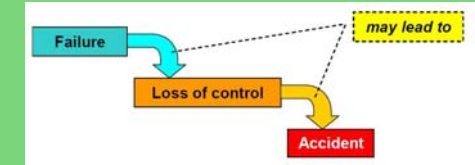
Qualitatives und quantitatives Risikomodell

- Es ist ein Risikomodell aufzustellen, welches als Basis zur Ableitung der tolerierbaren Gefährdungsraten dienen kann.
- Aussagen beispielsweise zu
 - betrachtetem Risiko
 - betrachteten Personen
 - Annahmen zum Schadensausmaß

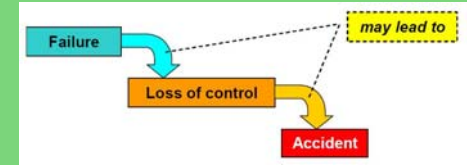


Ziel

- Es muss das Ziel sein, in Anlehnung an das Controllability-Verfahren oder das Verfahren der Functional Hazard Analysis der Luftfahrt ein rein qualitatives Verfahren zur Risikoabschätzung zu entwickeln, welches durch Beschreibung der Ereignisumstände zum Ergebnis kommt und welches ohne detaillierte Zahlenschätzungen (z.B. zum Schadensausmaß) auskommt.
- Da derartige Verfahren sowohl in der Luftfahrt wie auch in der Automobilwirtschaft zum Einsatz kommen, scheint grundsätzlich die Möglichkeit zur Konstruktion eines solchen Verfahrens gegeben zu sein.
- Die Übertragbarkeit des Controllability-Verfahrens ggf. unter Berücksichtigung einzelner weiterer Parameter scheint gegeben.
- Die Konstruktion und Kalibrierung eines solchen Verfahrens ist forschungs- und zeitaufwändig.
- In der Anwendung können hingegen Zeit und Ressourcen gespart werden.



Vielen Dank für die Aufmerksamkeit!



Referenzen

- [1] MISRA Technical Report : Hazard Classification for Moving Vehicle Hazards Controllability, May 2004
- [2] MISRA: Development Guidelines for vehicle based programmable Systems, Draft, 2005
- [3] Richard Evans and Jonathan Moffett: Derivation of Safety Targets for the Random Failure of Programmable Vehicle Based Systems, SAFECOMP 2000, LNCS 1943, pp. 240-249, 2000. Springer-Verlag Berlin Heidelberg 2000
- [4] Peter H Jesty, Keith M Hopley, Richard Evans and Ian Kendall: Safety Analysis of Vehicle-Based Systems. Proceedings of the 8th Safety-critical Systems Symposium, 2000.