

Benutzerhandbuch

# BP-Risk-Analyse

ENTWURF

Version	Ausgabedatum	Autor	geprüft	freigegeben
0.8	24.01.2011	SLB, MSR		

**Inhalt**

	Seite
1 Änderungsübersicht .....	5
2 Einführung .....	6
3 Voraussetzungen zur BP-Risk-Analyse .....	7
3.1 Systemdefinition .....	7
3.2 Gefährdungsidentifikation .....	8
4 Grundsätzliche Konstruktion von BP-Risk .....	10
5 Durchführung der BP-Risk-Analyse .....	11
5.1 BP-Risk Tabellen .....	13
5.2 Gefahrenabwehr $G$ .....	14
5.3 Schadensausmass $S$ .....	18
5.4 Zulässige Versagenshäufigkeit $F$ .....	21
6 Beispiel Bahnübergang .....	22
7 Anhang .....	29
7.1 Funktionsliste Eisenbahnfahrzeug .....	29
7.2 Fragen zu BP-Risk .....	36

**Tabellen**

	Seite
Tabelle 1: Aufbauprinzip der BP-Risk-Tabellen .....	14
Tabelle 2: Skala für Parameter $B$ .....	15
Tabelle 3: Skala für Parameter $M$ .....	16
Tabelle 4: Skala für Parameter $T$ .....	19
Tabelle 5: Skala für Parameter $V$ .....	20
Tabelle 6: Skala für Parameter $A$ .....	20
Tabelle 7: Skala zur Bestimmung der zulässigen Versagenshäufigkeit $F$ .....	21
Tabelle 8: Zusammenfassung funktionale FMEA .....	25
Tabelle 9: Funktion LH aus Funktionsliste .....	26
Tabelle 10: Umrechnungsfaktor .....	28

**Abbildungen**

	Seite
Abbildung 1: Prinzip der Systemdefinition für BP-Risk .....	7
Abbildung 2: Gefährdungsmodell .....	8
Abbildung 3: Konstruktion von BP-Risk .....	10
Abbildung 4: Ablauf der BP-Risk-Analyse .....	12

Abbildung 5: Schnittstelle Zug – BÜ.....	22
Abbildung 6: Fehlerbaum BÜ .....	27

## Abkürzungen

BP-Risk	Best-Practice Risk
BÜ	Bahnübergang
BÜSA	Bahnübergangssicherungsanlage
CENELEC	European Committee for Electrotechnical Standardization
DB AG	Deutsche Bahn AG
DIN	Deutsches Institut für Normung
EBA	Eisenbahnbundesamt
EUB	Eisenbahn-Unfalluntersuchungsstelle des Bundes
EN	Europäische Norm
Fdl	Fahrdienstleiter
FMEA	Failure Mode and Effects Analysis
HGV	Hochgeschwindigkeitsverkehr
prEN	Entwurf für Europäische Norm
Sifa	Sicherheitsfahrerschaltung
SGV	Schienengüterverkehr
SPFV	Schienenpersonenfernverkehr
SPNV	Schienenpersonennahverkehr
Tf	Triebfahrzeugführer
THR	Tolerable Hazard Rate (tolerierbare Gefährdungsrate)

## BP-Risk-Parameter

A	Anzahl betroffener Personen
B	Betriebsdichte
G	Gefahrenabwehr
i	Index für Funktionsversagen (Gefährdung)
M	Menschliche Gefahrenabwehr
S	Schadensausmass
T	maximale Last
V	massgebliche Geschwindigkeit

## Quellenverzeichnis

- [1] Bepperling, Sonja-Lara: „Validierung eines semi-quantitativen Ansatzes zur Risikobeurteilung in der Eisenbahntechnik“. Schriftenreihe des Instituts für Verkehrsplanung und Transportsysteme (IVT) der ETH Zürich, Band 144. Zürich 2009
- [2] CENELEC (Hrsg.): EN 50126 Bahnanwendungen – Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS); 1999.
- [3] CENELEC (Hrsg.): EN 50128 Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Software für Eisenbahnsteuerungs- und Überwachungssysteme; 2001.
- [4] CENELEC (Hrsg.): EN 50129 Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Sicherheitsrelevante elektronische Systeme für Signaltechnik; 2003.
- [5] CENELEC (Hrsg.): EN 60812 Analysetechniken für die Funktionsfähigkeit von Systemen – Verfahren für die Fehlzustandsart- und –auswirkungsanalyse (FMEA); 2006.
- [6] DIN (Hrsg.): DIN VDE 0831-101 Elektrische Bahn-Signalanlagen – Teil 101: Semi-quantitative Verfahren zur Risikoanalyse technischer Funktionen in der Eisenbahnsignaltechnik; 2010.
- [7] DIN (Hrsg.): E DIN EN 15380-4 (Entwurf) Bahnanwendungen – Kennzeichnungssystematik für Schienenfahrzeuge – Teil 4: Funktionsgruppen; 2009
- [8] EBA (Hrsg.): Allgemeinverfügung zum Melden von gefährlichen Ereignissen im Eisenbahnbetrieb vom 10.11.2009
- [9] Hinzen, Albrecht: Der Einfluß des menschlichen Fehlers auf die Sicherheit der Eisenbahn. Veröffentlichungen des verkehrswissenschaftlichen Institutes der Rheinisch-Westfälischen Technischen Hochschule Aachen, Heft 48. Aachen (Dissertation); 1993.
- [10] Verordnung (EG) Nr. 352/2009 der Kommission vom 24. April 2009 über die Festlegung einer gemeinsamen Sicherheitsmethode für die Evaluierung und Bewertung von Risiken gemäß Artikel 6 Absatz 3 Buchstabe a der Richtlinie 2004/49/EG des Europäischen Parlaments und des Rates; 2009.

## 1 Änderungsübersicht

Version	Ausgabedatum	Autor	geprüft	freigegeben	Änderungen
0.0		Schranil			
0.1	27.01.2010	SLB			Überarbeitung; Beispiel hinzugefügt (Kapitel 6)
0.2	03.02.2010	SLB			Korrekturen, Ergänzungen
0.3	10.02.2010	SLB			Formatänderungen, Ergänzung der L- Funktionen
0.4	19.02.2010	SLB			alte L-Funktionen eingefügt
0.5	28.04.2010	SLB			Ergänzungen aus Vornorm-Anforderungen
0.6	29.04.2010	SLB			Korrekturen
0.7	21.01.2011	MSR			Korrekturen; Quellenverzeichnis hinzugefügt
0.8	24.01.2011	SLB			Schlusskorrekturen

## 2 Einführung

BP-Risk (Best-Practice Risk) stellt ein semi-quantitatives Verfahren zur Risikobeurteilung in der Eisenbahnleit- und -sicherungstechnik dar. Seine Herleitung erfolgte im Rahmen der Dissertation „Validierung eines semi-quantitativen Ansatzes zur Risikobeurteilung in der Eisenbahntechnik“ [1] durch Dr. Sonja-Lara Bepperling. Dieses Benutzerhandbuch fasst die wichtigsten Schritte zur Risikobeurteilung mit Hilfe des Verfahrens „BP-Risk“ zusammen. Es richtet sich damit primär an einen bereits mit Risikobeurteilungen vertrauten Anwender im Bahntechnikbereich und soll die methodisch-theoretischen Hintergründe lediglich ansatzweise darlegen. Zur Vertiefung der wissenschaftlichen Begründungen sowie der getroffenen Annahmen und Randbedingungen sei hier lediglich auf die genannte Dissertationsschrift verwiesen.

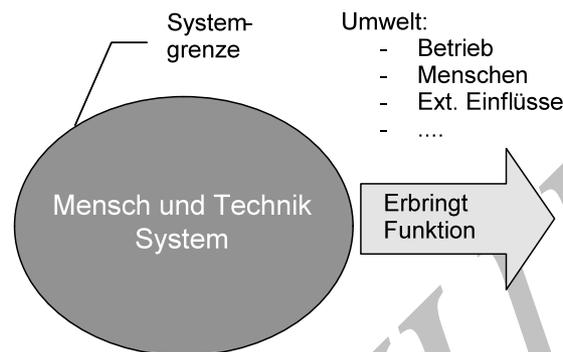
Der Begriff ‚best practice‘ stammt aus der angloamerikanischen Betriebswirtschaft und wird meist mit ‚Standardverfahren‘ oder ‚Erfolgsrezept‘ übersetzt. Best-Practice Risk wurde anhand von Anforderungen konstruiert, die bisher das ‚best practice‘ zum Thema Risikobeurteilung repräsentieren. BP-Risk eröffnet somit die Möglichkeit, positive Eigenschaften von verbreiteten Ansätzen der Risikobeurteilung zu kombinieren. Dieser Ansatz soll eine effiziente und anwenderfreundliche Durchführung der Ableitung von zulässigen Häufigkeiten für Versagen der Funktionen eines Mensch-Maschine-Systems ermöglichen.

Nach einer kurzen Einführung in die grundsätzliche Vorgehensweise im Rahmen einer Risikobeurteilung wird die Durchführung der BP-Risk-Analyse in diesem Handbuch vorgestellt. Gesetzliche und normative Grundlagen sind sowohl die Verordnung (EG) Nr. 352/2009 [10] als auch die CENELEC-Normen EN 50126 [2], EN 50128 [3] und EN 50129 [4] sowie die deutsche Vornorm DIN VDE 0831-101 [6] zu semi-quantitativen Risikoanalysemethoden.

### 3 Voraussetzungen zur BP-Risk-Analyse

#### 3.1 Systemdefinition

Das System, welches im Rahmen einer Risikobeurteilung mit Hilfe von BP-Risk analysiert werden soll, erbringt seine Funktion i. d. R. durch das Zusammenwirken von Mensch und Technik (Abbildung 1):



**Abbildung 1: Prinzip der Systemdefinition für BP-Risk**

Im konkreten Fall ist das System, welches mit BP-Risk betrachtet wird, ein Zug mit der Betrachtungseinheit „eine Stunde Zugfahrt“. Zur Identifizierung von gültigen Funktionen für dieses System steht im Anhang dieses Handbuches (siehe Kapitel 7.1) eine Funktionsliste aus der Schienenfahrzeugtechnik ([7], erweitert durch Infrastrukturfunktionen) zur Verfügung, die auf einer für das Risikomodell von BP-Risk abgestimmten Systemebene definiert ist. Generell ist darauf zu achten, dass die Funktionen in der korrekten Ebene definiert werden. Sollte eine tiefere Ebene (höhere Detaillierung, z. B. bei Komponentenbetrachtung) erforderlich sein, bietet sich beispielsweise eine Fehlerbaumanalyse an, die der BP-Risk Analyse anzuschliessen wäre.

Ist eine Funktion nicht in der Funktionsliste vorhanden, muss sie in der Analyse definiert werden, wobei zu beachten ist, dass die gleiche Systemebene gewählt wird wie für die in der Funktionsliste enthaltenen Funktionen.

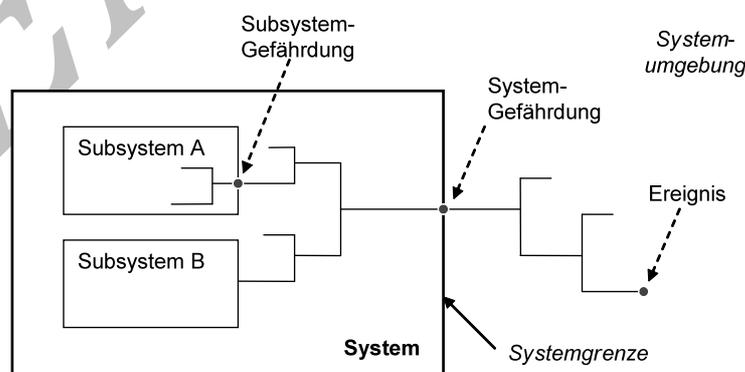
### 3.2 Gefährdungsidentifikation

Im Zusammenhang mit der Systemsicherheit ist eine Gefährdung ein ungesicherter Zustand des Systems, der zu einem Unfall führen kann. Im Allgemeinen beinhaltet die Gefährdungsidentifikation eine systematische Analyse des Systems und umfasst zwei Phasen – eine empirische und eine kreative Phase.

Die empirische Phase umfasst die Nutzung von Erfahrungen, z. B. aus Beinahe-Unfällen oder Unfallstatistiken. Die kreative Phase beinhaltet Vorhersagen, z. B. in Form von strukturierten „Was-wäre-wenn-Studien“ oder Checklisten.

Die empirische und die kreative Phase der Gefährdungsidentifikation ergänzen einander, so dass angenommen werden kann, dass alle signifikanten Gefährdungen identifiziert werden. Im Rahmen der kreativen Phase kann eine vereinfachte funktionale FMEA (Failure Mode and Effects Analysis) nach EN 60812 [5] durchgeführt werden. Eine generische Gefährdungsidentifikation auf Basis der erstellten Funktionsliste (siehe Systemdefinition) ist grundsätzlich möglich. Dazu kann für eine grobe Abschätzung aus der Liste der Systemfunktionen durch Negation eine Liste der Systemgefährdungen abgeleitet werden. Dieses Ergebnis sollte jedoch durch eine FMEA abgesichert werden.

Die Identifikation der betrieblichen Gefährdungen erfolgt im Bezug auf die Systemgrenze und bildet den Ausgangspunkt für die Folgen- und Schadensanalyse mit Hilfe von BP-Risk. Das hier zu Grunde liegende Gefährdungsmodell ist in Abbildung 2 dargestellt:



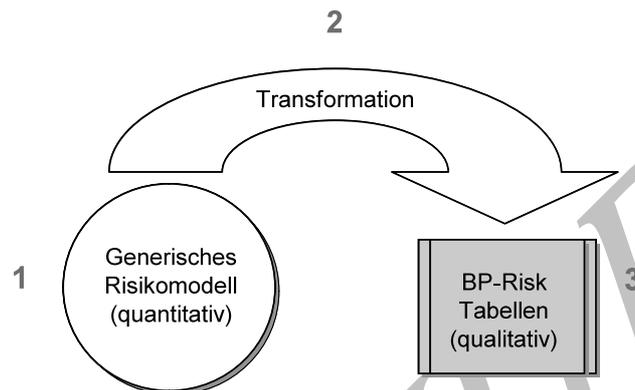
**Abbildung 2: Gefährdungsmodell**

Gefährdungen werden stets an der Systemgrenze definiert. Abbildung 2 macht deutlich, dass eine Subsystem-Gefährdung an der Systemgrenze von Subsystem A eine Gefährdung sein kann, wenn man nur das Subsystem A separat betrachten würde. Geht die Betrachtung jedoch vom gesamten System aus, so ist die Subsystem-Gefährdung von Subsystem A lediglich eine Ursache für die System-Gefährdung an der Systemgrenze des gesamten Systems.

ENTWURF

#### 4 Grundsätzliche Konstruktion von BP-Risk

Die grundsätzliche Konstruktion von BP-Risk wird an dieser Stelle als Hintergrundinformation dargelegt und kann in der oben genannten Dissertation [1] detaillierter nachgelesen werden. An dieser Stelle werden nur kurz die wichtigsten Schritte der Konstruktion von BP-Risk genannt:



**Abbildung 3: Konstruktion von BP-Risk**

##### 1) Generisches Risikomodell

Beim grundlegenden BP-Risk Ansatz ist ein probabilistisches Modell definiert, das die relevanten Parameter und Annahmen enthält (generisches Risikomodell). Dieses Modell ist gut geeignet für Systeme mit geringer Komplexität bzw. für hohe Systemebenen. Für diese Systeme können das Schadensausmass und die Eintrittswahrscheinlichkeit sowie die Wahrscheinlichkeit der Fehleroffenbarung für ein bestimmtes Funktionsversagen direkt analysiert werden.

##### 2) Transformation

Das probabilistische Modell wird mittels einer mathematischen Transformation, welche die wesentlichen Eigenschaften des Modells (Monotonie, Vergleichbarkeit, Einfachheit) aufweist, auf ein qualitatives Modell abgebildet. Dabei werden die quantitativen Parameter diskretisiert und auf Parameterbereiche abgebildet.

##### 3) BP-Risk Tabellen

Die Parameterbereiche werden hinsichtlich der Minimierung von Diskretisierungsfehlern und der sinnvollen verbalen Beschreibung optimiert.

## 5 Durchführung der BP-Risk-Analyse

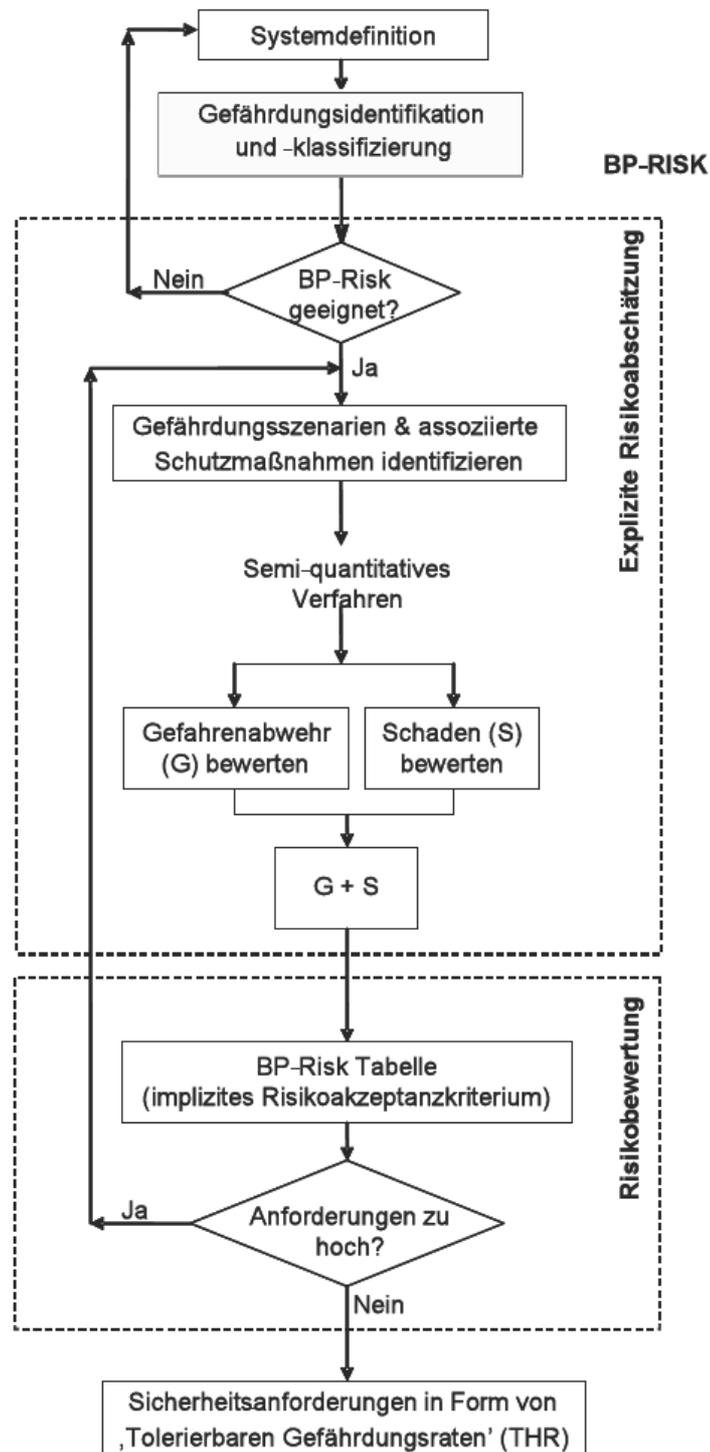
Die Systemdefinition und Gefährdungsidentifikation werden von BP-Risk methodisch nicht explizit unterstützt, sind aber zwingende Voraussetzungen. BP-Risk stellt Vorgaben auf, unter welchen Randbedingungen die Systemdefinition und die Gefährdungsidentifikation zu erstellen sind, so dass BP-Risk anwendbar ist. Folgende Bedingungen müssen für eine Anwendung von BP-Risk erfüllt sein:

- System besitzt geringe Komplexität oder wird auf hohem Systemlevel betrachtet
- Systemdefinition erfolgt auf Ebene der Funktionsliste von BP-Risk
- Betrachtungseinheit ist ein Zug (kollektives Risiko); *Betrachtungseinheit Streckenelement kann im Rahmen von BP-Risk umgerechnet werden.*

Bei Nichterfüllung der oben genannten Bedingungen müsste entweder die Systemdefinition der Analyse oder die Konstruktion der Methode angepasst werden. Falls diese Anpassungen nicht möglich sind, muss eine andere Methode für die Risikobeurteilung verwendet werden.

Im Rahmen der BP-Risk Analyse erfolgt für jede Systemgefährdung eine Abschätzung des typischen Schadensausmasses sowie der möglichen Gefahrenabwehr. Es ist hierbei von entscheidender Bedeutung, dass für die Bewertung keine ‚worst-case‘-Situationen, sondern durchschnittliche oder typischerweise auftretende Gegebenheiten, angenommen werden. Ein Abweichen würde eine falsche Einstufung der zulässigen Versagenshäufigkeit bewirken und zu unangemessen hohen Sicherheitsanforderungen führen.

Insgesamt ergibt sich folgender Prozess für die Risikobeurteilung (explizite Risikoabschätzung und Risikobewertung nach CSM-Verordnung) mit BP-Risk (Abbildung 4).



**Abbildung 4: Ablauf der BP-Risk-Analyse**

Wenn BP-Risk für die Anwendung geeignet ist, dann müssen die Gefährdungsszenarien gefunden und dargestellt werden. Dazu gehört eine

Beschreibung der schon vorhandenen Schutzmassnahmen (also der vorhandenen Barrieren). Dies kann methodisch mit der Darstellung als Ereignisbaum erfolgen.

Danach wird aus der Vielzahl von Szenarien ein „massgebliches Szenario“ ausgewählt, auf dessen Basis die Bewertung mit Hilfe der BP-Risk Tabellen stattfindet. Zur Ermittlung des „massgeblichen Szenarios“ können z.B. die Gefährdungen nach dem sich aus ihnen ergebenden Risiko eingeschätzt werden. Die Auswahl des massgeblichen Szenarios muss entweder durch eine solche Analyse oder eine begründete Entscheidung eines Expertenkreises (sog. Sachverständigenurteil) erfolgen. Alternativ können alle relevanten Szenarien ausgewertet werden. Es ist allerdings ausreichend, in der Risikobeurteilung das massgebliche Szenario zu bewerten.

Alle Gefährdungsszenarien müssen in einem Gefährdungsprotokoll dokumentiert werden, um die Vollständigkeit der Gefährdungsermittlung sicherzustellen. Im Gefährdungsprotokoll müssen die erkannten Gefährdungen, die damit zusammenhängenden Massnahmen und die Ursachen der Gefährdungen dokumentiert und Angaben zu der für das Gefährdungsmanagement verantwortlichen Organisation gemacht werden. Ausserdem müssen die bei der Gefährdungsermittlung ggf. identifizierten Sicherheitsmassnahmen erfasst werden.

### **5.1 BP-Risk Tabellen**

Das Ziel von BP-Risk in Bezug auf die konkrete Anwendbarkeit besteht darin, dass der Anwender lediglich Tabellen korrekt anwenden muss, weil er darauf vertrauen kann, dass die Konstruktion des Verfahrens richtig ist. Die eigentliche Anwendung von BP-Risk ist somit unkompliziert möglich. Allerdings muss dabei beachtet werden, dass eine Methode niemals das (Mit-) Denken des Anwenders ersetzen kann. Falls Bedingungen unklar sind und der Anwender keine passende Parametereinstufung finden kann, müssen Annahmen (Umstände und Randbedingungen) getroffen und dann als sicherheitsrelevante Anwendungsaufgaben definiert werden. Ausnahmen sind allgemein anerkannte Tatsachen (Bestimmung durch einen Expertenkreis) oder durch Vorschriften bereits abgedeckte Sachverhalte.

Im Folgenden wird näher auf die einzelnen Parameter eingegangen, wobei die jeweiligen Skalen erläutert werden. Die Tabellen sind grundsätzlich nach folgendem Prinzip aufgebaut (Tabelle 1):

Abkürzung	Mathematische Transformation				Transformation	Qualitative Beschr.	Beispiel
für Anwender	nicht sichtbar				sichtbar		
Erläuterung	Quantitativer Wert	Logarithmus zur Basis Wurzel 10	Absoluter Rundungsfehler $R_f = X - \log x$	Ganzzahliger (gerundeter) Wert	Transformierter Wert (Verschiebung des Skalennullpunkts)	Qualitative Beschreibung	Beispiele

**Tabelle 1: Aufbauprinzip der BP-Risk-Tabellen**

Der für den Anwender nicht sichtbare Bereich (mathematische Transformation) wird in diesem Handbuch nicht näher erläutert. Ebenso wird an dieser Stelle nicht auf die Kalibrierung der BP-Risk Methode eingegangen, sondern lediglich auf die genannte Dissertationsschrift verwiesen.

## 5.2 Gefahrenabwehr G

Mit Hilfe des Parameters Gefahrenabwehr wird eine vereinfachte Folgenanalyse durchgeführt. Somit werden die möglichen Konsequenzen bewertet, die sich aus einer Gefährdung ergeben können. Da nicht alle Gefährdungen unmittelbar zu Unfällen führen, werden vor allem die verschiedenen Schutzmassnahmen identifiziert und beurteilt. Die Subparameter für die Gefahrenabwehr berücksichtigen deshalb Massnahmen zur Verhinderung von Unfällen und zur Reduzierung des resultierenden Schadens. Diese Ereignisse oder Gegebenheiten müssen jedoch explizit ausserhalb des definierten Systems liegen.

Die Gefahrenabwehr setzt sich aus den betrieblichen Randbedingungen  $B$  und der menschlichen Gefahrenabwehr  $M$  zusammen:

$$G_i = B_i + M_i \quad (\text{Formel 1})$$

$B_i$  betriebliche Randbedingungen. Dieser Wert sagt aus, wie wahrscheinlich es unter gegebenen betrieblichen Randbedingungen ist, dass sich im folgenden Abschnitt ein Zug befindet.

$M_i$  Möglichkeit der menschlichen Gefahrenabwehr. Es werden menschliche Handlungen berücksichtigt, die nicht dem System zugerechnet werden können bzw. nicht planmässig erfolgen.

### Betriebsdichte $B$

In Abhängigkeit des mittleren Belegungsgrades des deutschen Bahnnetzes lassen sich folgende betrieblichen Randbedingungen formulieren (siehe Tabelle 2):

$B$	Betriebsdichte	Beispiele
1	gering	unter Netzdurchschnitt, z. B. auf Güterverkehrsstrecken
2	normal	Netzdurchschnitt, z. B. auf Regionalverkehrsstrecken
3	erhöht	über Netzdurchschnitt, z. B. auf Fern- oder HGV-Strecken

Tabelle 2: Skala für Parameter  $B$

### Menschliche Gefahrenabwehr $M$

Grundsätzlich sollten bei Risikobeurteilungen der Mensch als Bediener oder Benutzer in die Analyse einbezogen werden. Allerdings ist sehr genau zu prüfen, ob der Mensch Teil des betrachteten Systems ist (dies ist i. d. R. der Fall).

Bei der Betrachtung des Parameters  $M$  soll nun bewertet werden, inwiefern der Mensch die Gefahr erkennen und den Schaden noch abwenden kann. An dieser Stelle soll nur der Eingriff des Menschen betrachtet werden, der durch seine Handlung eine Gefahr abwehren kann. So ist es z. B. denkbar, dass ein Triebfahrzeugführer (Tf), dem eine zu hohe Geschwindigkeit für eine abzweigende Weiche signalisiert wird, aufgrund seiner Streckenkenntnis die gefährliche Situation erkennt und die Geschwindigkeit noch rechtzeitig drosseln kann. Ausserdem könnte es sein, dass ihm ein Abschnitt fälschlicherweise als frei signalisiert wird, der Tf jedoch die Gefahr (möglicherweise einen im Abschnitt stehenden Zug) erkennt und seinen Zug noch rechtzeitig anhalten kann. Ein weiterer Fall wäre, dass einem

Fahrdienstleiter (Fdl) oder Tf im betrieblichen Ablauf eine Unstimmigkeit oder Besonderheit zufällig auffällt, dieser dann zum Beispiel über Zugfunk einen Nothaltauftrag erteilt und damit die drohende Betriebsgefahr abwendet.

Die hier in Frage kommenden menschlichen Handlungen finden in der Regel unter ungünstigen Umständen statt und werden bei kurzer Reaktionszeit unter Stress durchgeführt. Daher wird im Rahmen von BP-Risk nur eine menschliche Handlung bewertet. Bei mehreren Auswahlmöglichkeiten sollte die erfolgsversprechendste berücksichtigt werden.

<i>M</i>	Menschliche Gefahrenabwehr	Beschreibung
1	häufig möglich	fertigkeits-basierende Handlung unter ungünstigen Umständen
3	selten möglich	regel-basierende Handlungen unter ungünstigen Umständen
5	fast nie möglich	zufälliges Eingreifen des Menschen

**Tabelle 3: Skala für Parameter *M***

Bei der Einteilung der menschlichen Handlungen gelten folgende Kategorien:

„**Fertigkeits-basierendes** Verhalten ist gegeben, wenn der Mensch die ihm gestellte Aufgabe eindeutig verstanden hat und sie aufgrund seiner Ausbildung mit automatisch ablaufenden, sensomotorischen Reaktionen ausführen kann“ ([9], S. 62). Für den Bahnbetrieb sind dies beispielsweise:

- Fernmündliche Meldung
- Fahrwegsicherung
- Feststellen der korrekten Weichenlage
- Tf fährt auf Sicht
- Zuordnung von Signalen zu Gleisen und Bedeutung durch Tf
- Streckenkenntnis des Tf über Besonderheiten
- anstandslose Bedienung der Sifa nur im Wachzustand
- Bemerkten und Beachten des Halt zeigenden Signals
- Fdl bietet Zug an und wiederholt Annahme
- Nachbar-Fdl nimmt Zug an und bestätigt Richtigkeit

„**Regel-basierendes** Verhalten ist dann gegeben, wenn der Mensch die ihm gestellte Aufgabe aufgrund festgelegter Symptome einer gelernten Sammlung von Verhaltensregeln der Form ‚Wenn - Dann‘ zuordnen und mit der so gefundenen Regel ausführen kann“ ([9], S.62), beispielsweise:

- Zugschlussfeststellung
- Signalhaltfeststellung
- Fdl diktiert Befehl und bestätigt Richtigkeit
- Tf schreibt Befehl und wiederholt Wortlaut
- Fdl bietet falsch fahrenden Zug an und wiederholt Annahme
- Nachbar-Fdl nimmt falsch fahrenden Zug an, bestätigt Richtigkeit der Wiederholung

„**Wissens-basierendes** Verhalten ist dann gegeben, wenn der Mensch die ihm gestellte Aufgabe aus Mangel an Erfahrung nur lösen kann, indem er seinen Wissensschatz über die Funktionsweise des Systems nutzt, um komplexe oder gar mehrdeutige Informationen auszuwerten, eine Entscheidung aufgrund allgemeiner Ziele zu treffen und dann zu handeln.“ ([9], S. 62)

Der Anwender hat bei der Bewertung vom Parameter  $M$  zu entscheiden, um welche Kategorie menschlichen Verhaltens es sich handelt. Dabei ist zu beachten, dass die Bewertung von BP-Risk ein Gefährdungsszenario betrachtet, d. h. die Gefährdung liegt bereits vor. Es ist zu diskutieren, ob bei Vorhandensein einer gefährlichen Situation überhaupt noch ein fertigkeiten-basierendes Verhalten des Menschen möglich ist. In der Regel sind Gefährdungen und dementsprechende menschliche Hilfsaktionen sehr selten und kaum trainiert – es liegen somit keine routinemässigen Handlungen vor. Es mag jedoch Ausnahmen geben, bei denen noch fertigkeiten-basierende Handlungen selbst unter ungünstigen Umständen möglich sind, z. B. das Erkennen, ob eine Weiche falsch steht.

In Ausnahmefällen können für die Bewertung des  $M$ -Parameters auch andere technische Systeme zum Tragen kommen, dabei ist dann aber immer zu prüfen:

- Liegt Unabhängigkeit zum betrachteten System vor?
- Spielen ggf. wieder menschliche Handlungen eine Rolle?
- Wird die Gefahrenabwehr quasi automatisch unterstützt?

Die Bewertung zusätzlicher technischer Barrieren sollte sich an anerkannten, einfach zu beurteilenden Masstäben für das Sicherheitsniveau der technischen Funktion, die die Barriere darstellt, orientieren (z.B. SIL- oder THR-Einstufung).

### 5.3 Schadensausmass S

Im Rahmen von Risikobeurteilungen wird oft der Personenschaden als Risikokenngrösse verwendet. Es wird dabei angenommen: wenn das Transportgefäss (Fahrzeug) gesichert ist, ist die Sicherheit insgesamt gegeben. Demnach wird auch bei BP-Risk davon ausgegangen, dass die anderen Rechtsgüter (wie Personen, Umwelt, Sachwerte, Image des Bahnbetreibers, etc.) hinreichend geschützt sind, wenn der zu betrachtende Zug hinreichend geschützt ist.

Für BP-Risk bildet die Formel der kinetischen Energie die Grundlage der Schadensbewertung. Bei der Einschätzung des Schadens für den zu betrachtenden Zug soll beurteilt werden, welches Ausmass der Personenschaden einnehmen könnte, falls die Gefahrenabwehr misslingt.

$$S_i = T_i + V_i + A_i \quad (\text{Formel 2})$$

- $T_i$  Masse, ausgedrückt durch die durchschnittlich maximale Last für die jeweilige Zuggattung.
- $V_i$  massgebliche Geschwindigkeit des zu betrachtenden Zuges, kategorisiert durch die erlaubte Geschwindigkeit auf bestimmten Strecken bzw. bei bestimmten Betriebsmodi.
- $A_i$  Anzahl betroffener Personen, in Abhängigkeit der jeweiligen Unfallkategorie.

#### Maximale Last $T$

Die maximale Last wird für die jeweilige Zuggattung angegeben. Für den Parameter  $T$  resultiert nunmehr (Tabelle 4):

<b>T</b>	<b>Zuggattung</b>	<b>Beispiele</b>
1	SPNV	Regionalbahn, S-Bahn-Züge
2	SPFV + HGV	Triebzüge, bespannte Personenverkehrszüge, Nachtzüge, Autoreisezüge
3	SGV	Güterzüge (auch Schnellgüterzüge)

**Tabelle 4: Skala für Parameter T**

Die hohe Gewichtung der Zuggattung Güterzüge wirft die Frage auf, ob die Anforderungen für den Güterverkehr im Vergleich zum Personenverkehr nicht zu hoch bewertet werden. Allerdings bietet BP-Risk durch die Parameter Geschwindigkeit und Betriebsdichte die Möglichkeit, diese Gewichtung auszugleichen. Im Güterverkehr ist mit geringeren Geschwindigkeiten und mit einer geringeren Betriebsdichte zu rechnen als im Personenverkehr, so dass die Anforderungen mindestens zwei Stufen geringer sind, was ungefähr einer Zehnerpotenz entspricht. Bei Mischverkehr ist zu prüfen, ob der Personenverkehr oder der Güterverkehr massgebend sind.

### **Massgebliche Geschwindigkeit V**

Bei Unfällen des gleichen Typs können sehr starke Unterschiede bei den wirkenden Kräften auftreten. Diese sind in erster Linie von den gefahrenen Geschwindigkeiten abhängig. Zu beachten ist, dass nicht die Differenzgeschwindigkeit von z. B zwei zusammenstossenden Zügen, sondern im Rahmen von BP-Risk nur die massgebliche Geschwindigkeit des zu betrachtenden Zuges berücksichtigt wird. Dabei ist weiterhin wichtig, dass die durchschnittlich auftretende Situation bewertet wird. ‚Worst-case‘-Annahmen würden hierbei zu falschen Ergebnissen führen.

Der Parameter V gibt die für den zu betrachtenden Zug massgebliche durchschnittliche Geschwindigkeit an (Tabelle 5). Diese ist auf Grundlage bestimmter Strecken- und Betriebsmodi kategorisiert.

V	Massgebliche Geschwindigkeit	Beispiele
1	gering	Rangieren, Fahrt auf Befehl, Güterverkehrsstrecke
2	mittel	Nebenstrecke
3	hoch	Nebenstrecke oder Regionalverkehrsstrecke
4	sehr hoch	Fernverkehrsstrecke oder HGV-Strecke

**Tabelle 5: Skala für Parameter V**

### Anzahl betroffener Personen A

Bei der Bewertung der Anzahl betroffener Personen ist für den Anwender die Frage zu beantworten, welche typische Folge das betrachtete Gefährdungsszenario hat. Für den Parameter A wird die mittlere Anzahl der betroffenen Personen in Abhängigkeit des Unfalltyps angegeben. Die Kategorisierung der Unfalltypen erfolgt gemäss der „Allgemeinverfügung zum Melden von gefährlichen Ereignissen im Eisenbahnbetrieb“ [8] der EUB (Tabelle 6):

A	Anzahl Betroffener	Beispiele (Unfalltyp)
1	einzelne Person	Aufprall oder im Güterverkehr
2	wenige Personen	Zusammenprall
3	einige Personen	Entgleisung
4	viele Personen	
5	sehr viele Personen	Zusammenstoss

**Tabelle 6: Skala für Parameter A**

Dabei ist zu beachten, dass die zu betrachtenden Personen Reisende und Mitarbeiter sind. Es werden keine Dritten (z. B. Unbefugte oder Strassenverkehrsteilnehmer am Bahnübergang) berücksichtigt, da sie ausserhalb der Systemdefinition von BP-Risk liegen.

## 5.4 Zulässige Versagenshäufigkeit $F$

Nach der vereinfachten Folgen- und Konsequenzenanalyse kann nun die BP-Risk-Tabelle für die zulässige Versagenshäufigkeit angewendet werden (Tabelle 7):

<b>G + S</b>	<b>THR = <math>(\sqrt{10})^F</math></b>	<b>Beschreibung</b>
9	$3 \cdot 10^{-5} /h$	Einmal in 3 Jahren
10	$10^{-5} /h$	Einmal in 10 Jahren
11	$3 \cdot 10^{-6} /h$	Einmal in 30 Jahren
12	$10^{-6} /h$	Einmal in 100 Jahren
13	$3 \cdot 10^{-7} /h$	Einmal in 300 Jahren
14	$10^{-7} /h$	Einmal in 1'000 Jahren
15	$3 \cdot 10^{-8} /h$	Einmal in 3'000 Jahren
16	$10^{-8} /h$	Einmal in 10'000 Jahren
17	$3 \cdot 10^{-9} /h$	Einmal in 30'000 Jahren
18	$10^{-9} /h$	Einmal in 100'000 Jahren
19	$3 \cdot 10^{-10} /h$	Einmal in 300'000 Jahren
20	$10^{-10} /h$	Einmal in 1'000'000 Jahren

**Tabelle 7: Skala zur Bestimmung der zulässigen Versagenshäufigkeit  $F$**

Anhand der Summe der Parameter  $G$  und  $S$  erhält der Anwender aus Tabelle 7 oder obiger Gleichung die zulässige Versagenshäufigkeit einer Systemfunktion. Die THR (tolerierbare Ausfallrate) kann ebenso mit Hilfe folgender Gleichung berechnet werden:

$$THR = \sqrt{10}^{-(G+S)} \quad (\text{Formel 3})$$

Die THR bezieht sich auf eine Betriebsstunde, da als Risikoakzeptanz das Kriterium RAC-TS der Tabelle 7 zu Grunde gelegt ist. Weitere Details zur Kalibrierung von BP-Risk befinden sich in der genannten Dissertationsschrift.

Die zulässige Versagenshäufigkeit einer Systemfunktion als Ergebnis von BP-Risk steht nun für Auswertungen und Betrachtungen ausserhalb des BP-Risk-Prozesses zur Verfügung, wie z. B. einer Fehlerbaumanalyse, um die tolerierbare Versagenshäufigkeit weiter herunter zu brechen.

## 6 Beispiel Bahnübergang

### System abgrenzen

Das System ist abgegrenzt durch die vorgegebene Funktionsliste im Anhang (Kapitel 7). Abbildung 5 zeigt die Systemgrenzen und die zugehörige Schnittstelle. Es wird davon ausgegangen, dass die Bahnübergangssicherungsanlage (BÜSA) vom Fahrzeug aktiviert wird (d. h. das Fahrzeug wird von der BÜSA detektiert), so dass in diesem Fall das Stellwerk keine Rolle spielt.

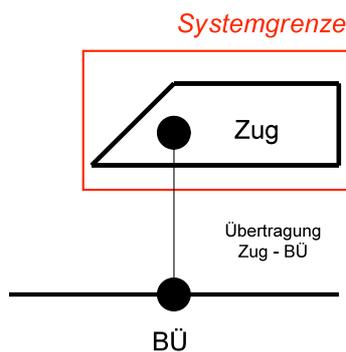


Abbildung 5: Schnittstelle Zug – BÜ

### Systemfunktionen beschreiben

Die zu betrachtende Systemfunktion laut Funktionsliste (Funktion LH) heisst: „BÜ sichern“. Diese befindet sich an der Schnittstelle zwischen Zug und BÜ. Es wird im Rahmen dieses Beispiels von einer zuggesteuerten Anlage ausgegangen. Die Sicherung für den Strassenverkehr (in Form von Lichtzeichen- oder Blinklichtanlagen mit oder ohne Halbschranken) werden vom Zug über Einschaltkontakte im Gleis aktiviert und über Ausschaltkontakte oder eine Induktionsschleifen ausgeschaltet. Bei der Überwachung wird i. d. R. zwischen dem Überwachen der eingetretenen Sicherung (Hauptsignal und Überwachungssignal) und dem Überwachen der Verfügbarkeit der Anlage (Fernüberwacht und Überwachungssignal mit optischer Einschaltung) unterschieden. Dadurch ergeben sich verschiedene Informationsinhalte an den Schnittstellen BÜSA – Stellwerk oder Überwachungssignal (BÜSA) – Tf. Für das vorliegende Beispiel wird zur Vereinfachung nur die Überwachungsart Überwachungssignal (ÜS) betrachtet.

Bei der Überwachungsart ÜS signalisieren sogenannte Überwachungssignale dem Triebfahrzeugführer, dass die BÜSA eingeschaltet wurde und ordnungsgemäss arbeitet. Die Überwachungssignale sind im Bremswegabstand vor dem BÜ aufgestellt, so dass der Zug bei Versagen der Einschaltung vor dem BÜ anhalten kann. Falls das ÜS anzeigt, dass die Sicherungsanlage nicht eingeschaltet wurde, muss der BÜ manuell gesichert werden. Das Schienenfahrzeug muss vor der Strasse anhalten und anschliessend muss der BÜ

behelfsmässig oder örtlich gesichert werden. Das Befahren des BÜs ist dann nur mit grösster Vorsicht und unter Abgabe akustischer Achtungssignale zulässig.

Die Ausschaltung erfolgt durch verschiedene lineare Systeme, z. B. Achszählkreise oder Schaltpunkte. Die BÜSA wird ausgeschaltet, sobald der Zug den betreffenden Abschnitt geräumt hat (BÜ ‚frei‘ gefahren).

### **Versagensmodi festlegen**

Da der Betrachtungsgegenstand ein Schienenfahrzeug ist, sind nur diejenigen Gefährdungen relevant, die auf den Zug wirken. Das bedeutet, es werden nur diejenigen Funktionsversagen betrachtet, die für einen Zug gefährlich werden und zu einem Unfall führen können, z. B. die Kollision eines Zuges am BÜ mit einem Hindernis (Strassenfahrzeug, Fussgänger oder liegendegebliebenes Hindernis). Unfälle, die den BÜ allein betreffen, wie z. B. die Kollision eines Verkehrsteilnehmers mit einer Schranke, werden nicht betrachtet.

Für die grobe Abschätzung lautet die Gefährdung aus der Negation der Funktion: ‚BÜ nicht gesichert‘. Bei einer ergänzenden Durchführung einer funktionalen FMEA werden die verschiedenen Ausfallmodi der Funktion betrachtet. Die EN 60812 [5] beschreibt die allgemeinen Versagensmodi wie folgt:

- Funktion wird nicht ausgeführt (totaler Ausfall),
- Funktion wird nicht zur vorgeschriebenen Zeit ausgeführt,
- Funktion wird nicht zur vorgeschriebenen Zeit beendet,
- Funktion wird vorzeitig ausgeführt.

Angewendet auf die Beispielfunktion, lauten die Versagensmodi:

- a) BÜ-Sicherung wird nicht ausgeführt (totaler Ausfall),
- b) BÜ-Sicherung wird nicht zur vorgeschriebenen Zeit ausgeführt,
- c) BÜ-Sicherung wird nicht zur vorgeschriebenen Zeit beendet,
- d) BÜ-Sicherung wird vorzeitig ausgeführt.

## **FMEA - Analyse durchführen**

Bei der Betrachtung der Versagensmodi ist es wichtig, diese in einen betrieblichen Kontext zu setzen. Was bedeutet also ein totaler Ausfall der BÜ-Sicherung betrieblich? Dazu muss bekannt sein, wie die BÜ-Sicherung funktioniert.

### **Fall a)**

Ein mögliches Szenario für den ersten Fall wäre zum Beispiel, dass sowohl die strassenseitige Sicherung (Lichtzeichen) als auch die schienenseitige Sicherung (Überwachungssignal) versagt. Dabei ist es wichtig zu unterscheiden, ob ein Ausfallmodus wirklich gefährlich ist (also zu einem Unfall führen könnte) oder nur betriebshemmend wirkt. Dazu müssen die betrieblichen Auswirkungen des Funktionsausfalls betrachtet werden.

Beim Bahnübergang gibt es beispielsweise folgenden Auswirkungen:

- BÜ steht unerkannt ungesichert offen (gefährlich).
- BÜ ist nach Fehler dauerhaft geschlossen (betriebshemmend).

In beiden Fällen ist die Sicherungsanlage ‚ausgefallen‘. Der zweite Ausfallmodus ist vorerst nur betriebshemmend, da der BÜ durch die geschlossenen Schranken gesichert ist. Jedoch kann solch eine Situation gefährlich werden, wenn die wartenden Strassenverkehrsteilnehmer bei langem Nichterscheinen eines Zuges die BÜ-Sicherung umgehen. In einem solchen Fall sind die menschlichen Handlungen entscheidend, ob es zu einer Gefährdung kommt oder nicht.

Laut DB AG Statistiken sind 98 % der Unfälle an Bahnübergängen auf das Fehlverhalten der Strassenverkehrsteilnehmer zurückzuführen. Leichtsinn, Unaufmerksamkeit oder Unkenntnis sind die häufigsten Ursachen.

### **Fall b)**

Wird die BÜ-Sicherung nicht zur vorgeschriebenen Zeit ausgeführt, kann dies auch bezeichnet werden als ‚Sicherung zur Unzeit‘, z. B. das Schliessen der Schranken zur Unzeit. Zu erwähnen ist hierbei, dass der BÜ als gesichert gilt, wenn die Rotlichter das erste Mal aufleuchten.

Beim Schliessen der Schranken zur Unzeit kann ein Verkehrsteilnehmer ohne Vorwarnung gegen die Schranken fahren. Dieses wäre ein Unfalltyp, der nicht den Zug betrifft und insofern nicht weiter betrachtet wird.

### **Fall c)**

Wird die BÜ-Sicherung nicht zur vorgeschriebenen Zeit beendet, würde dies im vorliegenden Beispiel besagen, dass die Ausschaltung vorzeitig erfolgt. Dies bedeutet betrieblich, dass der Zug sich noch im Kreuzungsbereich mit der Strasse befindet und die Schranken bereits geöffnet werden. Dieses Szenario wäre nur dann gefährlich, wenn der Zug das

Überwachungssignal schon passiert hat, aber noch nicht am BÜ angekommen ist. Allerdings ist hierbei zu beachten, dass es bereits Unfälle gab, wo Verkehrsteilnehmer in den fahrenden Zug gefahren sind.

Ein anderer Fall für die nicht rechtzeitige Beendigung der Sicherung wäre z. B., dass die roten Lichtzeichen eingeschaltet bleiben bzw. die Schranken sich nicht öffnen, obwohl der Zug den BÜ geräumt hat. Diese Situation könnte die Strassenverkehrsteilnehmer dazu verleiten, die Warneinrichtungen zu ignorieren.

**Fall d)**

Wird die BÜ-Sicherung vorzeitig ausgeführt, würde das für den Beispielfall einer zu frühen Sicherung entsprechen. Eine zu frühe Einschaltung ist betrieblich allerdings nicht gefährlich, sondern nur betriebshemmend. Die Strassenverkehrsteilnehmer müssten jedoch länger am BÜ warten, was wiederum zu Ungeduld führen kann.

	Ausfallart	Beispiel	Folge	Gefährdung
a	BÜ-Sicherung wird nicht ausgeführt (totaler Ausfall).	Überwachungssignal zeigt BÜ ist gesichert obwohl BÜ nicht gesichert ist. Lichtzeichen bleibt dunkel, obwohl es rot zeigen sollte; Schranken werden nicht geschlossen, obwohl Zug sich nähert.	Schienenfahrzeug überfährt ungesicherten BÜ.	ja
b	BÜ-Sicherung wird nicht zur vorgeschriebenen Zeit ausgeführt.	Schließen der Schranken zur Unzeit; Einschaltung der Lichtsignale zur Unzeit.	1) Straßenverkehrsteilnehmer fährt gegen Schranke; 2) Schienenfahrzeug befährt ungesicherten BÜ; 3) Schienenfahrzeug trifft zu früh nach eingetretener Sicherung am BÜ ein.	1) nicht für das Schienenfahrzeug 2) ja 3) ja
c	BÜ-Sicherung wird nicht zur vorgeschriebenen Zeit beendet.	1) BÜSA wird vorzeitig ausgeschaltet; 2) Lichtzeichen bleiben rot oder Schranken werden nicht geöffnet.	1) Zug überfährt ungesicherten BÜ; 2) Straßenverkehrsteilnehmer wartet, obwohl kein Zug kommt.	1) ja, wenn Zug ÜS passiert, aber BÜ noch nicht erreicht hat (auch abhängig von menschl. Handlungen) 2) möglich (abhängig von menschl. Handlungen)
d	BÜ-Sicherung wird vorzeitig ausgeführt.	BÜ wird vorzeitig eingeschaltet.	Straßenverkehrsteilnehmer wartet, obwohl kein Zug kommt.	möglich (abhängig von menschl. Handlungen)

**Tabelle 8: Zusammenfassung funktionale FMEA**

Das Ergebnis der FMEA ist eine Liste von betrieblichen Gefährdungen der Systemfunktionen, eine Zusammenfassung für das oben genannte Beispiel gibt Tabelle 8.

### BP-Risk Analyse

Für die Berechnung der Versagenshäufigkeit für ein Streckenelement wird im Folgenden ein Bahnübergang (BÜ) bewertet. Die zugehörige Funktion aus der Funktionsliste befindet sich an der Schnittstelle zur Funktion KGC und lautet: „BÜ sichern“ (siehe Tabelle 9).

**Tabelle 9: Funktion LH aus Funktionsliste**

Ebene			Funktion	Erläuterung
1	2	3		
K	G	C	Signale steuern und überwachen	Funktionsgruppe aus E DIN EN 15380-4 [7]
L	B	H	BÜ sichern	Zusätzliche Streckenfunktion

Aus Sicht des Fahrzeugs bedeutet diese Funktion den Schutz des Bahnverkehrs vor kreuzenden Kraftfahrzeugen (Strassenverkehrsteilnehmern). Die daraus abgeleitete vereinfachte Gefährdung lautet: ‚BÜ nicht gesichert‘. Damit ist gemeint, dass die BÜSA sowohl für den Bahnbetrieb als auch für den Strassenverkehr unerkannt versagt. Nach FMEA sind detaillierte Ausfallmodi, wie die vorzeitige Ein- und Ausschaltung im Falle einer zugüberwachten BÜ-Anlage möglich. Das System einer zugüberwachten Anlage (Überwachung ÜS) wird auch im folgenden Beispiel betrachtet.

Technisch gesicherte Bahnübergänge kommen in allen Betriebsarten und bei Geschwindigkeiten bis 160 km/h vor. Zur Bewertung mit BP-Risk wird eine Nahverkehrsstrecke angenommen, für die nach Tabelle 2 eine normale Betriebsdichte angesetzt wird ( $B = 2$ ).

Zur menschlichen Gefahrenabwehr können sowohl der Triebfahrzeugführer (Tf) als auch die Strassenverkehrsteilnehmer beitragen. Da in den meisten Fällen nicht davon ausgegangen werden kann, dass der Tf bei Versagen der BÜ-Sicherung die Geschwindigkeit erheblich reduzieren kann, wird in diesem Fall die menschliche Gefahrenabwehr durch den Tf als fast nie möglich eingestuft. Eine menschliche Gefahrenabwehr ist jedoch möglich durch eine Notreaktion des Strassenverkehrsteilnehmers möglich, allerdings stark abhängig von örtlichen Gegebenheiten (Bebauung, Wetter, Tageszeit, Verkehrsdichte, usw.), so dass von einer stärkeren Risikoreduktion nicht ausgegangen wird. Die Gefahrenabwehr wird anhand von Tabelle 3 als möglich eingestuft ( $M = 3$ ), da bei zwei menschlichen Handlungen die Erfolgversprechendste bewertet werden soll.

Zusammenfassend ergeben die Werte der Subparameter *B* und *M* den Parameterwert für die Gefahrenabwehr  $G = 2 + 3 = 5$ .

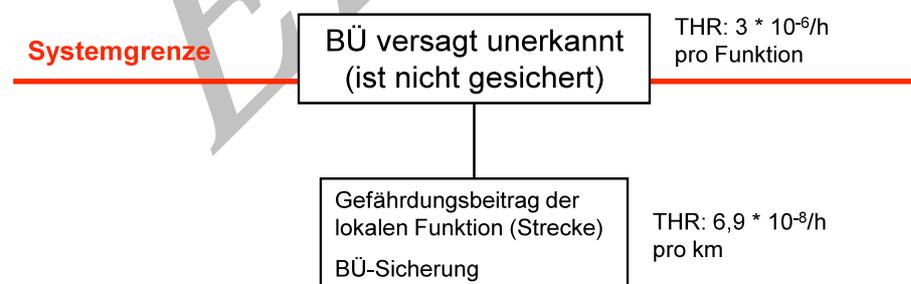
Wie vorhergehend beschrieben wird für das zu betrachtende Gefährdungsszenario eine Nahverkehrsstrecke angenommen. Laut Tabelle 4 wird der Wert für die Zuggattung im spurgeführten Nahverkehr (SPNV) mit  $T = 1$  bewertet. Für Nahverkehrsstrecken wird nach Tabelle 5 die massgebliche Geschwindigkeit als hoch eingestuft. Der Parameter *V* erhält den Wert 3.

Bei Unfällen an Bahnübergängen kommen in der Regel die beteiligten Strassenverkehrsteilnehmer sowie ggf. der Tf ernsthaft zu Schaden. Unfälle mit vielen Opfern bilden die Ausnahme. Der Wert für Parameter *A* wird anhand von Tabelle 6 zu  $A = 2$  bestimmt, da die typische Unfallfolge am BÜ ein ‚Zusammenprall‘ ist.

Aus den Subparametern *T*, *V* und *A* ergibt sich für das Schadenspotenzial *S* zusammenfassend folgender Wert  $S = 1 + 3 + 2 = 6$ . Anhand der Summe aus den Parametern *G* und *S* ( $G + S = 11$ ) wird mit Hilfe der Tabelle 7 die zulässige Versagenshäufigkeit bestimmt zu  $3 \cdot 10^{-6}/h$  pro Funktion, also einem tolerierbaren gefährlichen Versagen in 30 Jahren.

**Fehlerbaumanalyse**

Der für den Fall BÜ konkretisierte Fehlerbaum ist in Abbildung 6 dargestellt. Damit kann die Versagenshäufigkeit von BP-Risk weiter aufgeteilt werden. Da wie oben erwähnt die ÜS-Anlagen keine Verbindung zum Stellwerk haben, entfällt der Gefährdungsbeitrag der zentralen Funktion. Auch der Beitrag aus der Kommunikation entfällt hier, da keine Übertragung zwischen Fahrzeug und der Ein- und Ausschaltung stattfindet. Die Radsensoren detektieren das vorbeifahrende Fahrzeug – es werden jedoch keine Informationen im eigentlichen Sinne übertragen.



**Abbildung 6: Fehlerbaum BÜ**

Die THR der lokalen Funktion beträgt somit  $3 \cdot 10^{-6}/h$ . Das Fahrzeug hat keinen Anteil an dieser Funktion, so dass die THR für den Bezug auf die Strecke mit Hilfe des Umrechnungsfaktors  $u$  aus Tabelle 10 umgerechnet wird. Dabei wird für den Nahverkehr eine SPNV 120 angenommen. Somit beträgt die THR für die Strecke  $3 \cdot 10^{-6}/h \cdot 0,023 \approx 6.9 \cdot 10^{-8}/h$  pro Streckenkilometer.

**Tabelle 10: Umrechnungsfaktor**

Standard	$V_R$ in km/h	Auslastung in Zug/h	$u$ in Zug/km
HGV	135	5.00	0.037
SPFV230	108	3.86	0.036
SPFV160	93	3.05	0.033
SPNV120	90	2.06	0.023
SPNV80	60	1.33	0.022
SGV	18	0.42	0.023

Um die THR pro Streckenelement zu erhalten, ist eine weitere Umrechnung nötig, welche die Anzahl der Streckenelemente pro Kilometer berücksichtigt. Laut DB-Jahresbericht befinden sich insgesamt 20'317 Bahnübergänge im Netz der DB AG, was eine Betriebslänge von 34'128 km hat. Da Bahnübergänge im Fern- und Hochgeschwindigkeitsverkehr nicht vorkommen, wird die Anzahl der Bahnübergänge auf die Strecken des SPFV 160, SPNV und SGV aufgeteilt. Die prozentuale Einteilung der Betriebskilometer erfolgt nach den Vorgaben der Netz 21 Strategie der DB AG. Nach Expertenschätzung wird für die Strecken des SPFV 160 und SPNV 120 angenommen, dass sich ca. alle 3 km ein BÜ befindet. Für die Strecken des SPNV 80 und SGV wird angenommen, dass sich ca. alle 1 km ein BÜ befindet. Der Kehrwert (km pro BÜ) kann als die Anzahl der Kilometer verstanden werden, die sich durchschnittlich zwischen zwei Bahnübergängen auf der Strecke befinden. Mit diesem Wert wird die neue THR bestimmt. Sie beträgt für eine SPNV 120-Strecke:

$$6.9 \cdot 10^{-8}/h \text{ pro km} \cdot 3.0 \text{ km pro BÜ} = 2.07 \cdot 10^{-7}/h \text{ pro BÜ.}$$

Es ist wichtig zu erwähnen, dass diese Anforderung für ein System gilt, das aus Mensch und Technik besteht. Wenn man den untersuchten Bahnübergang jedoch weitestgehend durch Technik sichert, liegt das vorliegende Ergebnis in derselben Grössenordnung wie die Sicherheitsanforderung für Bahnübergänge, die beispielhaft anhand der Risikoformel ermittelt wurde.

## 7 Anhang

### 7.1 Funktionsliste Eisenbahnfahrzeug nach [7]

CODE	Funktion	Beispiele/ Erläuterungen	Kommentar
B B	Räume aufteilen, gestalten, verkleiden	Trenn- oder Schirmwände, Innentüren, Verkleidungen	
B C	Transportgut tragen/ aufnehmen/ umschliessen	Fahrzeugkasten, Einhausung, um Reaktionskräfte aufzunehmen	
B D	Aufprall schützen	Aufkletterschutz, Energieabsorptionselemente im Falle eines Crashes, strukturelle Wagenkastenfestigkeit	
B E	Vor Feuer schützen	Brandschutzkonzept	Brandmelde- und -löschanlage
C B	Sichere & komfortable Aufenthalts- & Sitzlandschaften bereitstellen	Sitze, Liegen, Vorkehrungen für sicheres Stehen	
C C	Blick-/Beobachtungsmöglichkeit nach Aussen sicherstellen	Fenster, ggf. auch Kameras	
C D	Innenbeleuchtung bereitstellen	Innenbeleuchtung	
C E	Fahrzeugklimatisierung bereitstellen	Heizung, Lüftung, Klimatisierung	
C F	Bereitstellen von "public address", Passagierinformation, Intercom & Entertainment	Kommunikation, Beschriftung, Fahrplaninfo, Audio- und Videounterhaltung	auch sicherheitsrelevante Warnhinweise der Crew an die Passagiere durch Lautsprecherdurchsagen
C G	Passagier- / Ladungsüberwachung ermöglichen	CCTV (Closed Circuit Tele Vision) system	interne Videoüberwachung der Passagier- und Laderäume
C H	Sanitärfunktionen bereitstellen	Toiletten, Waschräume	
C J	Gastronomische Funktionen bereitstellen	Restaurant, Bistro, Galley	
C K	Sonstige Servicefunktionen bereitstellen	Fahrkartenautomaten	Fahrgastzähleinrichtung
C L	Neigung aus Komfortgründen zur Limitierung der Querbeschleunigung im Wagenkasten	Bogenschnelles Fahren (Neigetechnik)	
C L B	Neigungsvorgang überwachen	Steuerung Neigetechnik; Positions- und Geschwindigkeitsüberwachung	
C L C	Fahrzeugkasten neigen	Neigeantrieb	aktive Neigetechnik mit Antrieb
C L E	ausreichendes Lichtraumprofil für Neigung sicherstellen	Streckenprofilüberwachung	Lichtraumprofil im Zusammenhang mit der Neigetechnik; durch die Neigung des Wagenkastens kann das Lichtraumprofil

CODE				Funktion	Beispiele/ Erläuterungen	Kommentar
						verletzt werden.
D	B			Zugang von aussen ermöglichen	Türen, Notausstiege, Tritte, Treppen, Haltegriffe, Geländer, Laderampen, Rollstuhlhilfe, Laufstege, rutschfeste Beläge	Funktionen, verbunden mit dem Management der Aussentüren
D	B	B		Aussentüren lösen	Türöffnung durch Fahrgäste ermöglichen	
D	B	E		Türsystem bei Hindernis managen	Positions- und Zustandserkennung	
D	B	F		Aussentüren verriegeln		
D	B	H		Selektives Öffnen von Aussentüren ermöglichen	z.B. um bestimmte Fahrzeuge des Zugs unzugänglich zu halten	
D	B	N		Öffnen der Aussentüren im Notfall ermöglichen	Hebel mit Ausschnitt für Türantrieb und -kontrolle	Erkennung des Öffnungs- und Ableitungssignals zur Zugkontrolle zur Einleitung der Notbremsung / zur Vermeidung des Starts
D	C			Zugang über Innentüren ermöglichen	Türen zwischen den Fahrzeugen, die den Fahrgästen die Bewegung im Zug ermöglichen	
D	D			Fracht laden und entladen ermöglichen	Luken, Laderaumtüren, Befüllereinrichtungen, Entleereinrichtung, Schwerkraftentladung	Laden und Entladen von Gütern über Türen oder Schüttguteinrichtungen
E	B			Flexible Konfiguration ermöglichen	Freies Zusammenstellen von Zugteilen im Betrieb	
E	B	B		Kuppeln steuern		
E	B	C		Entkuppeln steuern		
E	B	D		Kräfte über Kupplung übertragen	Zug- und Stosskräfte	
E	B	E		Signalleitungen, Energie- und Hilfsenergieleitungen verbinden	Zugsteuerleitungen, Bussysteme, Druckleitungen	Elektrisches und pneumatisches Kuppeln und Entkuppeln

CODE				Funktion	Beispiele/ Erläuterungen	Kommentar
E	B	F		Zugtrennung erkennen und darauf reagieren	Rückmeldung zum Kuppelstatus (gekuppelt, entkuppelt)	
E	C			Passagier- und Nutzlasttransfer zwischen den Wagen ermöglichen	Fahrzeugübergang, Mittelpufferkupplung	
F	B			Traktionsenergie bereitstellen	Stromzuführung inkl. Rückstromführung	Oberleitung, aber auch mittels Generator
F	C			Elektrische Energie für Hilfsbetriebe bereitstellen	Bordnetzumrichter, Bordnetzgenerator, Hilfsdiesel, Hauptluftpresser, Hilfsluftpresser	Bordnetzumrichter wird aus dem Zwischenkreis oder der Oberleitung gespeist
F	D			Strömungsenergie für Traktion bereitstellen	Transformer, Stromrichter, Dieselmotor, Hydraulik	
F	E			Strömungsenergie für Hilfsbetriebe bereitstellen		
F	F			Mechanische Energie für Traktion bereitstellen		
F	G			Mechanische Energie für Hilfsbetriebe bereitstellen		
F	H			Chemische Energie für Traktion bereitstellen		
G	B			Vortriebskraft und Bremskraft erzeugen	Traktionsstromrichter, Getriebe und Fahrmotor	
G	B	C		Bereitstellung der geforderten Traktion	verarbeitet Traktionsanforderung durch den Tf oder andere Steuerungseinrichtungen (z.B. ATO) innerhalb der Traktionsteuerung weiter	
G	B	C	D	Traktionssperre		
G	C			Bremsen	generelle Bremsfunktionalität, inklusive pneumatische Bremse	
G	C	B		Bremsüberwachung		
G	C	C		Bereitstellen der geforderten Bremsleistung	Bremsanforderungen innerhalb des Fahrzeugs, durch den Tf aber auch z.B. durch die Zugsicherungseinrichtung; auch das Managen des Brake Blendings zwischen den verschiedenen Bremsarten (elektrisches oder mechanisches Bremsen)	kann unterteilt werden in direkte und indirekte Bremsanforderungen durch den Tf
G	C	D		Priorisierung der Bremsanforderung, Auswahl		

CODE	Funktion	Beispiele/ Erläuterungen	Kommentar
	des Bremsmodus		
G C E	Feststellen des Bremsbedarfs		
G C F	Bremsregelung abhängig von Zugkonfiguration, Bremsmodus und Bremsanforderung		
G C G	Anforderung und Auflösen der Bremskraft		
G C H	Bereitstellen des Gleitschutzes		die WSP-Funktion hebt ggf. den Bremszugriff auf, greift massiv in das Bremssystem ein
G D	Kraftschlussbeiwert Rad/Schiene verbessern	Gleitschutz, Sandung, Putzklötze	
H B	Zugpersonal informieren	alle Funktionen, um das Zugpersonal über den Zustand des Zuges und dessen Systeme zu informieren	
H C	Zugweite Kommunikation bereitstellen	betriebliche Kommunikation im Zug oder mit ortsfesten Einrichtungen	Kommunikation innerhalb des Zuges bzw. zwischen zusammengekuppelten Zügen
H C B	Zugtaufe	Zugtaufe zur Bestimmung der Zugkonfiguration (Anzahl, Reihenfolge, Richtung und Eigenschaften der einzelnen Wagen)	Daten für das Zugsteuergerät (ZSG); die vorhandenen Wagen und deren Reihenfolge sind notwendig zur Steuerung der Systeme
H C C	Zugbus steuern	Zugang, Datenpriorisierung, QoS	
H D	Zugbetriebsart steuern	Steuerung des Fahrzeuges in allen Betriebsphasen	
H E	Einwandfreie Steuerung ermöglichen	allgemeine Bedien- und Steuerungsfunktionen, hauptsächlich durch Tf	betreffen Funktionen innerhalb des Fahrzeuges
H E B	Führerstand steuern	Funktionen zur Cabsteuerung und zur Steuerung seiner Funktionalität	Schlüsselschalter zum Aufriegeln des Führerstandes (key switch)
H E C	Fahr- / Bremsanforderung steuern	Brems- und Beschleunigungsanforderung; Brake-Blending, bei welchem die Bremssteuerung die elektrische Bremse und die mechanische Bremse steuert	Übergeordnete Fahr- und Bremssteuerung des Fahrzeuges (durch den Tf, z.B. Fahr-Brems-Hebel)
H E D	Energieversorgung steuern	Zentrale Funktionen zur Steuerung von Batterie Hauptschalter, Hauptschalter, Pantograph	
H E E	Geeignete und sichere Bedingungen steuern	Zentrale Funktionen zur Steuerung von Komfort- und	Bedarfsgerechte Vorhaltung; Schaltwerk,

CODE				Funktion	Beispiele/ Erläuterungen	Kommentar
					Sicherheitsfunktionen	Pulswechselrichter inkl. Steuerungselektronik
H	E	F		Zugang, Be- und Entladen steuern	Türsteuerung	
H	E	G		Kuppeln steuern	Steuerung / Freigabe des Kuppelvorganges	Zentrale Funktionen zur Steuerung des Zugangs durch die Aussentüren
H	E	H		Zugparameter einstellen	Zentrale Funktionen zur Steuerung von Zugparametern wie Zeit, Strecke	
H	E	J		Integration in das Eisenbahnsystem steuern	Zentrale Funktionen zur Steuerung der externen Beleuchtung, Signale	
H	F			Zugselbsttests steuern		
H	G			Diagnose bereitstellen	Diagnose von Zug- und Komponentenzuständen	
H	H			Fehlersuche unterstützen		
H	J			Fahrer überwachen	Sicherheitsfahrerschaltung (Sifa)	
H	K			Gesicherte Datenaufzeichnung bereitstellen	Fahrtenschreiber	Fahrtenschreiber; ähnlich einer Black-Box in Flugzeugen; evtl. Aufzeichnung von ATP- und ATO-Daten
J	B			Führen des Zuges	Radsatzführung, -anlenkung, auch Spurwechselradsätze	
J	B	C		Entgleisungsinformation bereitstellen	Detektieren der Entgleisung eines Zuges mittels Überwachung der relevanten onboard Parameter mit einer Mindestzuverlässigkeit in jedem Betriebszustand	
J	B	D		Hindernisse im Gleis überwachen	Überwachen möglicher Hindernisse im Gleis während des Betriebseinsatzes eines Zuges	
J	B	N		Entgleisen verhindern		
J	C			Kräfte übertragen	Drehzapfen, Zug-/Druckstange, Wankstütze, Wankstabilisator, Querzentrierung, Fahrwerk- und Fahrzeugkastenbindung	
J	D			Beschleunigung in x-y-z-Richtung limitieren		
J	E			Fahrzeug innerhalb der Begrenzungslinie halten	Sicherstellen, dass das Fahrzeug mit der Fahrzeugbegrenzungslinie bei allen Betriebsbedingungen übereinstimmt	Beurteilung der Laufcharakteristiken, Laufqualität' des Fahrzeuges
J	E	B		Erkennen und Korrigieren von Neigebewegungen		

CODE				Funktion	Beispiele/ Erläuterungen	Kommentar
K	B			Gleisbelegung anderen (Fahrzeugen) anzeigen	Signallichtführung (Schlussignal), Makrofon	
K	B	D		Gleisbelegung durch Fzg.-Aussenbeleuchtung (Signalisierung) erkennbar machen	z.B. End- und Spitzensignal	
K	C			Fahrzeugidentifikation ermöglichen		
K	D			Betriebliche Kommunikation und Datenübertragung Zug-/Extern ermöglichen	alle Arten der Kommunikation	
K	D	B		Signaltechnische Beeinflussung des Fahrzeuges gewährleisten; Datenübertragung mit Streckensignalisierung sicherstellen	Steuerstromkreise, Bussysteme	Interface des Fahrzeugs zu den gleisseitigen Sicherungseinrichtungen (Balisen, Magnete) durch Fahrzeugantennen; die Verarbeitung der Daten erfolgt im ATP/ATC
K	D	C		Betriebliche Kommunikation vom Zug nach extern ermöglichen	Übertragung von Betriebs- und Diagnosedaten	Zugfunk zwischen Tf und Betriebs-zentrale oder anderem Personal; Kommunikation zwischen Zug und externen Einrichtungen
K	D	D		Datentransfer / Beeinflussbarkeit von extern zum Zug sicherstellen	Übertragung von Betriebs- und Diagnosedaten	evtl. löschen, da in KDC enthalten
K	E			Automatische Zugsicherung/-steuerung ermöglichen	Fahrerloses Fahren gewährleisten	Zugsicherung steuert auch zugintern die Fahr- und Bremsfunktionen, jedoch geschieht dies mittels Input von aussen (Balisen oder Gleisschleifen, geben Signal- oder Geschwindigkeitsbegriff für Streckenabschnitt vor
K	E	B		ATC-Schnittstelle bereitstellen	Über ATC in das Gesamtsystem integrieren	
K	F			Automatischen Zugbetrieb ermöglichen	Eingriff auf Fahr- und Bremssteuerung	
K	G			Korrekte Fahrwegwahl / Streckensignalansteuerung	Weichensteuerung Vorrangschaltung	KG Funktionsgruppe eher im Nahverkehr
K	G	B		Streckenführung wählen	Weichenstelleinrichtung	
K	G	C		Signale steuern und überwachen	Lichtsignalbeeinflussung	Streckensignale ansteuern

CODE				Funktion	Beispiele/ Erläuterungen	Kommentar
L	B			Streckenfunktionen steuern und sichern	Streckenfunktionen	(Transverse Funktion Z)
L	B	B		Gleisschaltmittel, Gleisfreimeldung	Gleisstromkreise, Achszähler	
L	B	C		streckenseitige Ortung	Balisen (Kilometersteine)	
L	B	D		streckenseitige Zugbeeinflussung	Balisen, Indusi-Magneten, Kabellinienleiter	
L	B	E		Betriebsfernmeldeanlagen bereitstellen	Beschallungs- und Wechselsprechanlagen, Melde- und Überwachungssysteme, betriebliche Gefahrenmeldeanlagen, Videotechnik, Zugfunk	
L	B	F		Bewegliche Fahrwegelemente sichern	Weichen, Gleissperren,	
L	B	G		BÜ sichern	Einschaltung, Ausschaltung, Überwachungssignal	
L	B	H		Korrektes Fahrsignal anzeigen	Stellbare Signale	auch Gleisabschluss (Prellbock, Hemmschuh)

## 7.2 FAQs

### - Für welchen Anwendungsfall sind die Parameter bemessen?

Die Parameter beziehen sich auf das System „ein Zug“. Ergebnis der Anwendung ist eine THR je Betriebsstunde, sodass man genauer von „einer Stunde Zugfahrt“ zu sprechen hat (s. Kapitel 3.1). Es ist aber möglich, den Anwendungsbereich, z.B. auf Systeme ausserhalb des Zuges zu erweitern. Einen Ansatz hierzu zeigt Kapitel 6.

### - Wie ist das Ergebnis von BP-Risk zu interpretieren?

Die THR, die der Summe der Parameter G und S entspricht, bezieht sich stets nur auf die untersuchte Funktion. Dies resultiert aus der Anforderung, dass eine Risikobeurteilung möglichst realisierungsunabhängig sein soll, um keine herstellereinspezifischen Resultate zu erhalten. Dies bedingt jedoch, dass die Analyse auf einer recht hohen Systemebene durchgeführt werden muss. Solche Funktionen werden meist nicht durch eine Baugruppe allein realisiert. Im Anschluss ist daher in der Regel eine Aufteilung der THR, z.B. mittels Fehlerbaumanalyse, nötig, um die zulässigen Ausfallraten der (Unter-)Baugruppen zu erhalten.

### - Führt die Anwendung von BP-Risk zu übermässigen Sicherheitsanforderungen?

Nein, Ziel des Verfahrens ist, typische Gefährdungsszenarien zu betrachten. Durch die Bemessung der Parameter ist gewährleistet, dass keine unverhältnismässigen Ergebnisse geliefert werden. Sollen ‚worst-case‘-Szenarien zu Grunde gelegt werden, benötigt man keine Risikobewertung!

### - Besteht die Gefahr, zu niedrige Sicherheitsanforderungen zu erhalten?

Nein. Sollte sich der Anwender an einer Stelle verschätzen und einen zu niedrigen Parameterwert wählen, ist durch die Konstruktion des Verfahrens gewährleistet, dass die Abweichung des Ergebnisses geringer als eine Zehnerpotenz ist.

- **Welche Voraussetzungen sind für die Anwendung von BP-Risk erforderlich?**

BP-Risk beinhaltet die Teile ‚explizite Risikoabschätzung‘ und ‚Risikoevaluierung‘ gemäss der Darstellung in der Anlage der CSM-Verordnung. Eine vollständige Risikobewertung besteht zusätzlich aus einer Systemdefinition sowie der Gefährdungsermittlung und -einstufung. Will man BP-Risk korrekt anwenden, sind diese beiden Schritte mit grosser Sorgfalt vorher durchzuführen. Für die Systemdefinition kann die Funktionsliste (Kapitel 7) hilfreich sein, die Gefährdungsermittlung kann bspw. in Form einer FMEA durchgeführt werden.

ENTWURF