

	DIN VDE 0831-101 (VDE 0831-101)	DIN
	Diese Norm ist zugleich eine VDE-Bestimmung im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Präsidium beschlossenen Genehmigungsverfahrens unter der oben angeführten Nummer in das VDE-Vorschriftenwerk aufgenommen und in der „etz Elektrotechnik + Automation“ bekannt gegeben worden.	VDE

ICS 93.100

Einsprüche bis 2010-07-31

Entwurf

**Elektrische Bahn-Signalanlagen –
Teil 101: Semi-quantitative Verfahren zur Risikoanalyse technischer Funktionen
in der Eisenbahnsignaltechnik**

Electric signalling systems for railways –
Part 101: Semi-quantitative processes for risk analysis of technical functions in railway
signalling

Dispositif de signalisation électrique pour le chemin de fer –
Partie 101: Procès semi-quantitatifs pour l’analyse des risques des fonctions techniques dans la
signalisation ferroviaire

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2010-05-25 wird der Öffentlichkeit zur Prüfung und
Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses
Entwurfes besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise als Datei per E-Mail an **dke@vde.com** in Form einer Tabelle. Die Vorlage dieser
Tabelle kann im Internet unter **www.dke.de/stellungnahme** abgerufen werden
- oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik
im DIN und VDE, Stresemannallee 15, 60596 Frankfurt am Main.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevante
Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 56 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE

Beginn der Gültigkeit

Diese Norm gilt ab ...

Inhalt

	Seite
Vorwort	5
Einleitung	7
1 Anwendungsbereich	8
2 Normative Verweisungen	8
3 Begriffe	8
4 Symbole und Abkürzungen	11
5 Risikoanalyse und Risikoakzeptanz	12
5.1 Gesetzliche und normative Festlegungen	12
5.2 Risikoakzeptanzkriterium Mindestens Gleiche Sicherheit (MGS)	13
5.3 Risikoakzeptanzkriterium für technische Systeme (RAC-TS)	13
5.4 Anwendung und Interpretation von semi-quantitativen Risikoanalysen	13
6 Prozess der semi-quantitativen Risikoanalyse technischer Funktionen	14
6.1 Einleitung	14
6.2 Allgemeine Anforderungen	15
6.3 Systemdefinition	16
6.4 Gefährdungsermittlung	17
6.5 Gefährdungseinstufung	17
6.6 Ermittlung von Szenarien und Sicherheitsmechanismen	17
6.7 Abschätzung der Schwere	18
6.8 Abschätzung der Häufigkeit	19
6.9 Vergleich mit Kriterien	22
6.10 Sicherheitsanforderungen	22
6.11 Klassifikation der Anforderungen	23
Anhang A (informativ) Darstellung von Risikographen als Risikomatrix und Bewertungstabellen	25
A.1 Einleitung	25
A.2 Beispiel IEC 61508	25
Anhang B (informativ) Systematische Ableitung von Funktionen aus betrieblichen Abläufen	27
B.1 Einleitung	27
B.2 Beispiel: Ableitung von Funktionen für Stellwerkstechnik	27
Anhang C (informativ) Semi-quantitatives Verfahren Risikograph	34
C.1 Einleitung	34
C.2 Allgemeine Vorstellung des Risikographen	35
C.3 Systemdefinition für Bahnsignalanlagen im Nahverkehr gemäß BOStrab	36
C.4 Kalibrierung des Risikographen für Nahverkehrsanwendungen	41

	Seite
C.4.1 Auswirkung des gefährlichen Vorfalls (C):.....	41
C.4.2 Häufigkeit und Zeit des Aufenthalts im Gefahrenbereich (F):.....	41
C.4.3 Möglichkeit, den gefährlichen Vorfall zu vermeiden (P):	42
C.4.4 Wahrscheinlichkeit des unerwünschten Ereignisses (W):	42
C.5 Anwendungshinweise zur Durchführung der Risikoanalyse.....	42
C.6 Darstellung des Risikographen als Risikomatrix.....	43
Anhang D (informativ) Semi-quantitatives Verfahren Risk Score Matrix (RSM).....	45
D.1 Problemstellung	45
D.2 Voraussetzungen	45
D.3 Systemdefinition.....	46
D.4 Gefährdungsidentifikation	48
D.5 Abschätzung der Unfallschwere	48
D.6 Abschätzung der Häufigkeit.....	49
D.6.1 Bewertung der menschlichen Gefahrenabwehr.....	50
D.6.2 Bewertung betrieblicher Barrieren	50
D.6.3 Bewertung weiterer Barrieren	51
D.6.4 Bewertung der Abhängigkeit von Barrieren	51
D.7 Sicherheitsanforderungen.....	51
D.8 Beispiele.....	53
D.8.1 Weiche stellen.....	53
D.8.2 Bahnübergangssicherung	53
D.8.3 Schutz gegen Gegenfahrten (Regionalstrecke).....	54
Anhang E (informativ) Weitgehend akzeptable Risiken.....	55
E.1 Einleitung	55
E.2 Wirtschaftliche Interpretation	55
E.3 Technische Interpretation	55
Literaturhinweise	56
Bilder	
Bild 1 – Interpretation von MGS für semi-quantitative Verfahren	14
Bild 2 – Grundlegendes Modell	17
Bild 3 – Ablauf Risikoanalyse unter Anwendung des Risikographen	34
Bild 4 – Risikograph nach DIN EN 61508-5	35
Bild 5 – Ablauf einer RSM-Bewertung.....	45
Tabellen	
Tabelle 1 – Abkürzungen	11
Tabelle 2 – Symbole.....	12
Tabelle 3 – Aspekte semi-quantitativer Risikoanalysen.....	15
Tabelle 4 – Beispiel für eine Risikomatrix	18
Tabelle 5 – Beispiel für eine direkte Zuordnung von Unfallklassen und Unfallhäufigkeiten	19

	Seite
Tabelle 6 – Generische Bewertungstabelle für eine Barriere.....	20
Tabelle 7 – Klassifizierung der Abhängigkeit von Barrieren.....	22
Tabelle 8 – Zusammenfassung der Anforderungen.....	24
Tabelle 9 – Parameterklassen nach IEC 61508-5	25
Tabelle 10 – Risikomatrix auf Basis Risikograph IEC 61508.....	26
Tabelle 11 – Funktionen der Stellwerkstechnik.....	27
Tabelle 12 – DIN EN 61508-5 Anhang D	36
Tabelle 13 – Basisfunktionen für die Durchführung des Fahrbetriebs	37
Tabelle 14 – Beispiel einer funktionalen Ableitung in Anlehnung an die Basisfunktionen für die Durchführung des Fahrbetriebs nach DIN EN 62290-1 und DIN EN 62267	38
Tabelle 15 – Darstellung des Risikographen als Risikomatrix	44
Tabelle 16 – Bewertung der Barrieren im Risikograph	44
Tabelle 17 – Beispielfunktionen für Leit- und Sicherungstechnik.....	46
Tabelle 18 – Unfall-Klassen.....	49
Tabelle 19 – Bewertung menschlicher Handlungen.....	50
Tabelle 20 – Bewertung von der Betriebsdichte abhängiger Barrieren	51
Tabelle 21 – Bewertungstabelle für Abhängigkeiten zwischen Barrieren	51
Tabelle 22 – Risk Score Matrix (RSM).....	52
Tabelle 23 – Alternative Darstellung als Risikotabelle	52
Tabelle 24 – Reduzierte Risk Score Matrix (RSM)	53

Vorwort

Für diesen Norm-Entwurf ist das nationale Arbeitsgremium UK 351.3 „Bahn-Signalanlagen“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE (www.dke.de) zuständig.

Dieses Dokument soll als Vornorm veröffentlicht werden.

Nationaler Anhang NA (informativ)

Zusammenhang mit Europäischen und Internationalen Normen

Für den Fall einer undatierten Verweisung im normativen Text (Verweisung auf eine Norm ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnittsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils neueste gültige Ausgabe der in Bezug genommenen Norm.

Für den Fall einer datierten Verweisung im normativen Text bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe der Norm.

Eine Information über den Zusammenhang der zitierten Normen mit den entsprechenden Deutschen Normen ist in Tabelle NA.1 wiedergegeben.

Tabelle NA.1

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
EN 50126:1999	–	DIN EN 50126 (VDE 0115-103):2000-03	VDE 0115-103
EN 50128:2001	–	DIN EN 50128 (VDE 0831-128):2001-11	VDE 0831-128
EN 50129:2003 CLC/TR 50506-1:2007	–	DIN EN 50129 (VDE 0831-129):2003-12 + DIN EN 50129 Beiblatt 1 (VDE 0831-129 Beiblatt 1):2008-06	VDE 0831-129 + VDE 0831-129 Beiblatt 1
EN 60812:2006	IEC 60812:2006	DIN EN 60812:2006-11	–
EN 61508 (Reihe)	IEC 61508 (Reihe)	DIN EN 61508 (VDE 0803) (Reihe)	VDE 0803 (Reihe)
EN 61508-1:2001	IEC 61508-1:1998 + Cor.:1999	DIN EN 61508-1 (VDE 0803-1):2002-11	VDE 0803-1
FprEN 62267:2008	IEC 9/1137/CDV:2008	E DIN EN 62267 (VDE 0831-267):2008-07	VDE 0831-267
EN 62290-1:2006	IEC 62290-1:2006	DIN EN 62290-1 (VDE 0831-290-1):2007-08	VDE 0831-290-1
–	IEC 62502:2009	–	–
–	–	DIN V VDE V 0831-100 (VDE V 0831-100):2009-08	VDE V 0831-100

Nationaler Anhang NB (informativ)

Literaturhinweise

DIN EN 50126 (VDE 0115-103):2000-03, *Bahnanwendungen – Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit (RAMS)*; Deutsche Fassung EN 50126:1999

DIN EN 50128 (VDE 0831-128):2001-11, *Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Software für Eisenbahnsteuerungs- und Überwachungssysteme*; Deutsche Fassung EN 50128:2001

DIN EN 50129 (VDE 0831-129):2003-12, *Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Sicherheitsrelevante elektronische Systeme für Signaltechnik*; Deutsche Fassung EN 50129:2003

DIN EN 50129 Beiblatt 1 (VDE 0831-129 Beiblatt 1):2008-06, *Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Anwendungsleitfaden für EN 50129 – Teil 1: Cross-acceptance*; Deutsche Fassung CLC/TR 50506-1:2007

DIN EN 60812:2006-11, *Analysetechniken für die Funktionsfähigkeit von Systemen – Verfahren für die Fehlzustands- und -auswirkungsanalyse (FMEA) (IEC 60812:2006)*; Deutsche Fassung EN 60812:2006

DIN EN 61508 (VDE 0803) (Reihe), *Funktionale Sicherheit elektrischer/elektronischer/programmierbarer elektronischer sicherheitsbezogener Systeme*

DIN EN 61508-1 (VDE 0803-1):2002-11, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 1: Allgemeine Anforderungen (IEC 61508-1:1998 + Cor.:1999)*; Deutsche Fassung EN 61508-1:2001

E DIN EN 62267 (VDE 0831-267):2008-07, *Bahnanwendungen – Automatischer städtischer schienengebundener Personennahverkehr (AUGT) – Sicherheitsanforderungen (IEC 9/1137/CDV:2008)*; Deutsche Fassung FprEN 62267:2008

DIN EN 62290-1 (VDE 0831-290-1):2007-08, *Bahnanwendungen – Betriebsleit- und Zugsicherungssysteme für den städtischen schienengebundenen Personennahverkehr – Teil 1: Systemgrundsätze und grundlegende Konzepte (IEC 62290-1:2006)*; Deutsche Fassung EN 62290-1:2006

DIN V VDE V 0831-100 (VDE V 0831-100):2009-08, *Elektrische Bahn-Signalanlagen – Teil 100: Risiko-orientierte Beurteilung von potenziellen Sicherheitsmängeln und risikoreduzierende Maßnahmen*

Einleitung

Seit die Forderung nach Risikoanalysen in der Eisenbahntechnik durch Inkraftsetzung der DIN EN 50126 Einzug gehalten hat, sind dazu zahlreiche Ansätze ausprobiert und mehr oder weniger gute Erfahrungen gewonnen worden. Wie in der Fachliteratur umfassend diskutiert, ist die in der DIN EN 50129 vorgeschlagene Vorgehensweise zur Risikoanalyse so flexibel, dass sie bisher auf alle aufgetretenen Anwendungsfälle in der Eisenbahnsignaltechnik erfolgreich angepasst werden konnte. Sie liefert lösungsunabhängige, diskriminierungsfreie Sicherheitsanforderungen und ihre Anwendungsmöglichkeiten sind keinesfalls nur auf Eisenbahnsignaltechnik beschränkt. Grundsätzlich konnte man dabei feststellen, dass der risikoorientierte Ansatz sich in der Eisenbahnsignaltechnik bewährt hat.

Dafür gibt es u. a. folgende Gründe:

- Durch diesen Ansatz wird der Beitrag der menschlichen Zuverlässigkeit und der technischen Verfügbarkeit in ein angemessenes Verhältnis zur technischen Sicherheit gerückt.
- Er erlaubt abgestufte Sicherheitsanforderungen.
- Er erlaubt die Optimierung der Kosten für die Sicherheitstechnik.
- Der technische Fortschritt wird durch diesen Ansatz gefördert, weil die Anforderungen unabhängig von der technischen Realisierung sind.

Auf der anderen Seite muss aber auch zugestanden werden, dass die bisher in Deutschland zugesicherten Risikoanalysen fast alle Unikate sind und sich bisher keine der dabei benutzten Vorgehensweisen als Standard durchsetzen konnte. Auch international gibt es große Unterschiede in den Vorgehensweisen zu Risikoanalysen: Während in angloamerikanisch geprägten Ländern sehr detaillierte, streckenbezogene Risikoanalysen durchgeführt werden, werden in Deutschland eher generische Risikoanalysen, z. B. beruhend auf Musterstrecken oder qualitativen Ansätzen bevorzugt.

Durch die Arbeiten der ERA, die zur VO (EG) 352/2009 (im Weiteren auch »EG CSM-Verordnung« genannt) geführt haben, sind mittlerweile aber Möglichkeiten geschaffen worden, Risikoanalysen zu vereinfachen bzw. die Effizienz von Risikoanalysen zu steigern, u. a. durch die Definition von Risikoakzeptanzkriterien wie RAC-TS sowie die Einführung des Begriffs „weitgehend akzeptabler Risiken“. Zur Umsetzung bieten sich insbesondere Risikoprioritätszahlen (RPZ) oder andere Varianten semi-quantitativer Verfahren an, die sich auch in ähnlichen Anwendungsbereichen bewährt haben, z. B. DIN V VDE V 0831-100.

Diese Vornorm enthält die Anforderungen, die semi-quantitative Methoden erfüllen müssen, damit bei Anwendung semi-quantitativer Methoden Sicherheitsanforderungen verlässlich abgeleitet werden können. In den Anhängen sind zusätzlich Beispiele für semi-quantitative Methoden aufgeführt, mit denen die Anforderungen dieser Norm erfüllt werden können. Allerdings ersetzen die Anhänge nicht Anwenderhandbücher, die zur verlässlichen Anwendung dieser Methoden notwendig sind.

1 Anwendungsbereich

Diese Vornorm ist anwendbar auf sicherheitsrelevante elektrische, elektronische und programmierbare elektronische Systeme (E/E/PES einschließlich Teilsysteme und Einrichtungen) für Eisenbahnsignalanwendungen.

Diese Vornorm stellt Anforderungen an die verlässliche Konstruktion und Anwendung semi-quantitativer Methoden zur Risikoanalyse in der Eisenbahnsignaltechnik auf. Sie gibt Anleitung, wie diese Methoden konstruiert und angewandt werden können, um Sicherheitsanforderungen für technische Systeme abzuleiten, indem

- grundlegende Prinzipien erklärt werden;
- die notwendigen Verfahrensschritte zur Durchführung der Risikoanalyse bereitgestellt werden;
- geeignete Benennungen, Voraussetzungen, Maßgrößen für die Beurteilung der maßgeblichen Parameter wie Schadensausmaß oder Wirksamkeit von Barrieren bereitgestellt werden;
- Beispiele für die notwendigen Arbeitsblätter oder andere Tabellenformen bereitgestellt werden.

Diese Vornorm ist anwendbar auf Funktionen innerhalb eines Gesamtsystems, für die Sicherheitsanforderungen in Form eines SIL und einer THR definiert werden können. Diese Vornorm gilt für generische Teilsysteme und Einrichtungen (beide anwendungsunabhängig oder für eine bestimmte Klasse von Anwendungen vorgesehen) und auch für anwendungsspezifische Systeme/Teilsysteme/Einrichtungen.

Diese Vornorm ist anwendbar auf die funktionale Sicherheit von Eisenbahnsignalsystemen. Sie befasst sich nicht mit der Arbeitssicherheit des Personals; dieses ist Gegenstand von anderen Normen.

Für den Anwendungsbereich dieser Vornorm bestehen keine regionalen oder internationalen Normen.

2 Normative Verweisungen

Die folgenden zitierten Dokumente sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

DIN EN 50126-1, *Bahnanwendungen – Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS)*, 2000

DIN EN 50128, *Bahnanwendungen – Software für Eisenbahnsteuerungs- und -überwachungssysteme*, 2001

DIN EN 50129, *Bahnanwendungen – Sicherheitsrelevante elektronische Systeme für Signaltechnik*, 2003

IEC 61508-1, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme, Teil 1: Allgemeine Anforderungen*, 2002

VO (EG) 352/2009, *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*

3 Begriffe

Für die Anwendung dieser Norm gelten die Definitionen und Abkürzungen aus den normativen Verweisungen. In diesem Abschnitt werden nur zusätzliche, dort nicht definierte Definitionen und Abkürzungen gesammelt, oder solche, deren Wiederholung das Verständnis der Vornorm fördern.

3.1

Barriere

ein Umstand (häufig ein System oder eine Prozedur), der die Häufigkeit oder den resultierenden Schaden des mutmaßlichen Unfalls verringert. Die Wirksamkeit von Barrieren hängt vom Grad ihrer Unabhängigkeit ab

ANMERKUNG Eine Barriere kann betrieblicher oder technischer Natur sein. Eine Barriere, die zur Risikoreduktion verwendet wird, hat in der Regel eine sicherheitsrelevante Anwendungsaufgabe (SAA) zur Folge.

3.2

Expertenkreis

ein Gremium, das sicherheitliche Einschätzungen durchführt, sofern die Grundlage für Entscheidungen nicht aus Analysen oder anderorts dokumentierten Angaben entnommen werden kann

3.3

Funktion

Art von Aktion oder Tätigkeit, durch die ein Produkt seinen beabsichtigten Zweck erfüllt

ANMERKUNG In der Regel wird eine Funktion durch eine Kombination von Hardware, Software und menschlichem Handeln erbracht.

[DIN EN 50129]

3.4

Funktionsliste

Zusammenstellung der Funktionen, auf die die Methode zur Risikobewertung angewendet wird

3.5

Gefährdungsszenario

ein Pfad, ausgehend von einer Gefährdung über die Barrieren bis zum Schadensereignis, wird als Gefährdungsszenario bezeichnet. Eine Gefährdung kann verschiedene Auswirkungen (Pfade) haben und somit verschiedene Gefährdungsszenarien aufweisen.

3.6

katastrophale Folgen

Todesfälle und/oder zahlreiche schwere Verletzungen und/oder schwerwiegende Umweltschäden infolge eines Unfalls

[VO (EG) 352/2009]

3.7

Kritizität

Fehlerbedeutung

Kombination der Schwere einer Auswirkung und der Häufigkeit ihres Auftretens oder anderer Eigenschaften eines Fehlers als Maß der Notwendigkeit, sich damit zu befassen und sie zu verringern

ANMERKUNG Kritizität ist ein qualitatives oder semi-quantitatives Maß für Risiko.

[DIN EN 60812]

3.8

maßgebliches Gefährdungsszenario

das Gefährdungsszenario, das im Rahmen der Bewertung mit einer semi-quantitativen Methode als Basis für die Bewertung ausgewählt wird

3.9

mindestens Gleiche Sicherheit (MGS) im Vergleich mit einem Referenzsystem

wenn ein Referenzsystem die in 3.10 genannten Anforderungen erfüllt, gilt für das System, das der Bewertung unterzogen wird, Folgendes: Die Risiken, die mit den vom Referenzsystem abgedeckten Gefährdungen verbunden sind, werden als vertretbar angesehen.

[nach VO (EG) 352/2009]

3.10

Referenzsystem

ein System, das sich in der Praxis bewährt hat, ein akzeptables Sicherheitsniveau gewährleistet und es ermöglicht, im Wege eines Vergleichs die Vertretbarkeit der von einem zu bewertenden System ausgehenden Risiken zu evaluieren

[VO (EG) 352/2009]

3.11

Risiko

die Kombination der Wahrscheinlichkeit des Eintretens von (durch Gefährdungen verursachten) Unfällen und Zwischenfällen, die zu einem Schaden führen, und des Ausmaßes dieses Schadens

[VO (EG) 352/2009]

3.12

Risikoakzeptanzkriterien

die Bezugskriterien, anhand deren die Vertretbarkeit eines spezifischen Risikos bewertet wird; diese Kriterien werden herangezogen, um zu bestimmen, ob das Risiko so gering ist, dass keine Sofortmaßnahmen zu seiner weiteren Eindämmung erforderlich sind

[VO (EG) 352/2009]

3.13

Risikoanalyse

die systematische Auswertung aller verfügbaren Informationen zur Identifizierung von Gefährdungen und Abschätzung von Risiken

[VO (EG) 352/2009]

3.14

Risikoprioritätszahl

Risikoprioritätszahlen stellen eine Methode der semi-quantitativen Bestimmung der Kritizität dar. Sie werden aufgrund der Verknüpfung tabellierter Werte für die Parameter wie Häufigkeit, Möglichkeit zur Gefahrenabwehr oder Schadensausmaß ermittelt

[nach DIN EN 60812]

3.15

Schutzobjekt

das Schutzobjekt bezeichnet bei Risikoanalysen das Objekt, zu dessen Schutz Sicherheitsanforderungen abgeleitet werden sollen

ANMERKUNG Typischerweise stellen Menschen (Reisende, Mitarbeiter, Anwohner) im Eisenbahnwesen wichtige Schutzobjekte dar. Zu den Schutzobjekten können aber auch Sachwerte oder die Umwelt zählen.

3.16

semi-quantitative Methode

semi-quantitativ bedeutet, eine Menge in einer bestimmten Gruppen- oder Intervall-Einteilung zu messen. Semi-quantitative Methoden benutzen ordinal skalierte numerische Werte zur Einschätzung von Parametern, die über eine Zuordnung (Graph, Formel oder Tabelle) zu einem Gesamtergebnis verknüpft werden

ANMERKUNG Weit verbreitete semi-quantitative Methoden der Risikoanalyse sind z. B. Risikomatrix, Risikograph oder Risikoprioritätszahlen.

3.17

Sicherheitsanforderungen

die (qualitativen oder quantitativen) Sicherheitsmerkmale eines Systems und dessen Betriebs (einschließlich Betriebsvorschriften), die zur Erfüllung gesetzlicher oder unternehmensspezifischer Sicherheitsziele erforderlich sind

[VO (EG) 352/2009]

3.18

sicherheitsrelevante Anwendungs-Auflagen

Auflagen, die aus Annahmen oder Randbedingungen einer Risikoanalyse eines technischen Systems resultieren, und die im Betrieb eingehalten werden müssen, damit das durch das technische System verursachte Risiko akzeptabel ist

ANMERKUNG Im Prinzip entspricht das Konzept der sicherheitsrelevanten Anwendungs-Auflagen dem Konzept der sicherheitsrelevanten Anwendungs-Vorschrift. Der Unterschied besteht darin, dass Letztere aus Annahmen und Randbedingungen der Sicherheitsnachweise resultiert.

3.19

technisches System

das Bauteil oder die Baugruppe, einschließlich Planung, Realisierung und Begleitdokumentation; die Entwicklung eines technischen Systems beginnt mit der Festlegung der Anforderungen an das System und endet mit seiner Zulassung; auch wenn dabei die relevanten Schnittstellen zum menschlichen Verhalten berücksichtigt werden, sind das Personal und dessen Handlungen nicht Bestandteil eines technischen Systems; der Wartungsprozess wird in den Wartungshandbüchern beschrieben, ist aber selbst nicht Bestandteil des technischen Systems

[VO (EG) 352/2009]

3.20

weitgehend akzeptables Risiko

(en: broadly acceptable risk)

aus Gefährdungen resultierende Risiken können beispielsweise dann als weitgehend akzeptabel eingestuft werden, wenn das Risiko so gering ist, dass die Einführung zusätzlicher Sicherheitsmaßnahmen nicht angemessen wäre. Das Sachverständigenurteil berücksichtigt, dass der Gesamtumfang aller weitgehend akzeptablen Risiken einen bestimmten Anteil am Gesamtrisiko nicht übersteigen darf

ANMERKUNG Die fachlich zutreffende Übersetzung von „broadly acceptable risk“ ist „allgemein akzeptables Risiko“.

[nach VO (EG) 352/2009]

4 Symbole und Abkürzungen

Die folgenden Abkürzungen werden in dieser Norm verwendet, siehe Tabelle 1.

Tabelle 1 – Abkürzungen

Abkürzung	
AKA	Ankündigungsanlage
ALARP	As low as reasonably practicable
ASEP	Accident Sequence Evaluation Program
BOS _{Strab}	Straßenbahn-Bau- und Betriebsordnung
BÜ	Bahnübergang
BÜSA	Bahnübergangs-Sicherungsanlage
CCF	Common Cause Failure
CSM	Common Safety Method
DTO	Driverless Train Operation
E/E/PES	Elektrische/Elektronische/Programmierbare Elektronische Systeme
ERA	European Railway Agency
ESTW	Elektronisches Stellwerk
FWSI	Fatalities and Weighted Serious Injuries
GOA	Grade of Automation

Tabelle 1 (fortgesetzt)

HEART	Human Error Assessment and Reduction Technique
HR	Hazard Rate
MGS	Mindestens gleiche Sicherheit
NTO	Non Automated Train Operation
RAC-TS	Risikoakzeptanzkriterium für Technische Systeme
RPZ	Risikoprioritätszahl
SAA	Sicherheitsrelevante Anwendungsaufgabe
SIL	Safety Integrity Level
SMS	Sicherheitsmanagement-System
STO	Semi Automated Train Operation
THR	Tolerable Hazard Rate
TOS	Train Operation on Sight
UTO	Unattended Train Operation
ZN	Zugnummer

Die folgenden Symbole aus Tabelle 2 werden in dieser Norm verwendet:

Tabelle 2 – Symbole

Symbol	
A1, A2, ...	Nummerierung der Anforderungen an semi-quantitative Verfahren
b	Bandbreite einer Klasse bei semi-quantitativen Verfahren
B_i	Barriere i
β_i	Bewertung der i-ten Barriere
φ_i	Abhängigkeit der i-ten Barriere von den Vorgängern

5 Risikoanalyse und Risikoakzeptanz

5.1 Gesetzliche und normative Festlegungen

Ziel einer Risikoanalyse ist die systematische Auswertung aller verfügbaren Informationen zur Identifizierung von Gefährdungen und Abschätzung von Risiken, um Sicherheitsanforderungen abzuleiten. Dabei sind bezüglich des Prozesses sowie insbesondere der Risikoakzeptanz gesetzliche und normative Randbedingungen zu beachten.

Zukünftig wird hierbei die EG CSM-Verordnung eine wichtige Rolle spielen, da ihre Prinzipien ab Juli 2010 für alle technischen Systeme sowie ab Juli 2012 allgemein bei signifikanten Änderungen im Eisenbahnwesen gelten. Sie muss jedoch nicht für die in der EG CSM Verordnung ausgenommenen Bahnsysteme angewendet werden (vgl. Art. 2 (3) der EG CSM Verordnung).

Der in der Verordnung definierte Prozess geht davon aus, dass im Zentrum der Sicherheitsbetrachtungen die Beherrschung von Gefährdungen steht, d. h. auf Grundlage einer Systemdefinition werden Gefährdungen identifiziert, zu deren Beherrschung Sicherheitsanforderungen abgeleitet und nachgewiesen werden.

Auf eine Risikoanalyse für eine Funktion darf verzichtet werden, wenn

- keine Gefährdung bei einem Funktionsversagen erkennbar ist, d. h. es sich nicht um eine sicherheitsbezogene Funktion handelt; oder

- es sich um eine Funktion von sicherheitstechnisch untergeordneter Bedeutung handelt, z. B. wenn es sich um ein weitgehend akzeptables Risiko handelt; oder
- von vornherein die höchste Sicherheitsanforderungsstufe festgelegt wird (vgl. 5.3).

Die Vertretbarkeit des Risikos des zu bewertenden Systems wird unter Zugrundelegung eines oder mehrerer der folgenden Grundsätze der Risikoakzeptanz evaluiert:

- a) Anwendung der anerkannten Regeln der Technik;
- b) Vergleich mit ähnlichen Systemen (Referenzsystem);
- c) explizite Risikoabschätzung.

Bezogen auf eine Funktion ist die Anwendung eines der vorgenannten Grundsätze ausreichend. Im Rahmen dieser Vornorm ist nur der Fall der expliziten Risikoabschätzung relevant. Der Vergleich mit einem Referenzsystem könnte jedoch auch bei expliziter Risikoanalyse zur Kalibrierung einer Methode zur expliziten Risikoabschätzung verwendet werden und wird daher auf Grund seiner fundamentalen Bedeutung und der Vollständigkeit halber betrachtet

5.2 Risikoakzeptanzkriterium Mindestens Gleiche Sicherheit (MGS)

Ein Referenzsystem R bezeichnet nach EG CSM-Verordnung ein System, das sich im Betrieb im Hinblick auf ein akzeptables Sicherheitsniveau bewährt hat, und das als Vergleichssystem herangezogen werden kann, wenn ein System, das einer Bewertung unterzogen wird, auf die Vertretbarkeit seiner Risiken geprüft wird.

Wenn nun für ein neues oder verändertes System S Sicherheitsanforderungen definiert werden sollen, so kann dies unter bestimmten Voraussetzungen unter Bezugnahme auf die Sicherheitsanforderungen eines Referenzsystems geschehen. Daher kann das Risikoakzeptanzkriterium MGS auch zur Kalibrierung von Methoden zur Risikobewertung angewendet werden.

5.3 Risikoakzeptanzkriterium für technische Systeme (RAC-TS)

Für technische Systeme enthält die EG CSM-Verordnung in 2.5.4 ein explizites Risikoakzeptanzkriterium:

„Wenn sich aus Ausfällen technischer Systeme Gefährdungen ergeben, die nicht von den anerkannten Regeln der Technik oder der Verwendung eines Referenzsystems abgedeckt werden, gilt für die Planung des technischen Systems folgendes Risikoakzeptanzkriterium:

Bei technischen Systemen, bei denen im Falle eines funktionellen Ausfalls von unmittelbaren katastrophalen Folgen auszugehen ist, muss das damit verbundene Risiko nicht weiter eingedämmt werden, wenn die Ausfallrate pro Betriebsstunde kleiner oder gleich 10^{-9} ist.“

RAC-TS muss als hinreichendes, allerdings nicht notwendiges Kriterium verstanden werden: wenn ein technisches System RAC-TS erfüllt, findet das Prinzip der gegenseitigen Anerkennung nach der EG CSM-Verordnung Anwendung. Es ist allerdings freigestellt, begründet abweichende Sicherheitsanforderungen zu stellen, z. B. auf Grund von gesetzlichen Vorschriften wie TSI oder weil das Sicherheitsniveau auch mit geringeren Sicherheitsanforderungen aufrecht erhalten werden kann.

5.4 Anwendung und Interpretation von semi-quantitativen Risikoanalysen

Unter Fachleuten ist unstrittig, dass bei vielen Annahmen und Ergebnissen von quantitativen Risikoanalysen sowie Sicherheitsbetrachtungen zum Nachweis auf Grund der Unsicherheiten in Daten und Schätzwerten bestenfalls die Größenordnung korrekt ist.

Dieser Argumentation ist auch die ERA gefolgt, in dem sie im CSM Guide in 2.5.6.1 [G1] (h) ausführt: „wo quantitative Kriterien benutzt werden: entweder ist die zulässige Genauigkeit des Gesamtergebnis innerhalb einer Größenordnung oder alle für die Quantifizierung benutzten Parameter sind konservativ.“

Diese Erkenntnis machen sich auch semi-quantitative Verfahren zur Risikoanalyse wie Risikomatrix, Risikograph oder Risikoprioritätszahlen zu Nutze, die üblicherweise mit Klasseneinteilungen der Bandbreite b von

ca. 3 bis 10 arbeiten, d. h. hier wird eine mittlere Ungenauigkeit um einen Faktor $3=1,7$ bis $10=3,2$ akzeptiert. Ähnliche statistische Unsicherheiten bestehen beim Vergleich von zugelassenen Systemen auf Grundlage empirischer Daten (vgl. DIN V VDE V 0831-100).

ANMERKUNG Würde man derartige Toleranzbereiche z. B. für die Anwendung von MGS nicht akzeptieren, so müsste man einen wirtschaftlich unvernünftigen Automatismus der kontinuierlichen Erhöhung von Sicherheitsanforderungen in Kauf nehmen. Diesem Sachverhalt trägt auch die EG CSM-Verordnung in anderer Form Rechnung durch die Definition eines weitgehend akzeptablen (broadly acceptable) Risikos: „Aus Gefährdungen resultierende Risiken können beispielsweise dann als weitgehend akzeptabel eingestuft werden, wenn das Risiko so gering ist, dass die Einführung zusätzlicher Sicherheitsmaßnahmen nicht angemessen wäre.“ Dies gilt insbesondere auch für weitgehende akzeptierbare Risikoerhöhungen in den o. a. Toleranzbereichen.

In Bild 1 wird die Interpretation für semi-quantitative Verfahren gezeigt, bei denen die Parameterwerte in Klassen mit gewissen Bandbreiten eingeteilt werden. Hier bedeutet MGS, dass die Bewertungsergebnisse in die gleiche Klasse fallen.

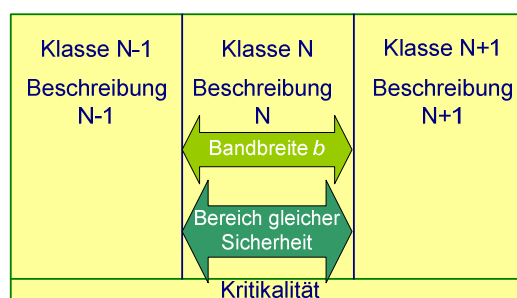


Bild 1 – Interpretation von MGS für semi-quantitative Verfahren

6 Prozess der semi-quantitativen Risikoanalyse technischer Funktionen

6.1 Einleitung

Eine Risikoanalyse mit semi-quantitativen Methoden folgt grundsätzlich dem allgemeinen Risikoanalyseprozess der EG CSM-Verordnung, allerdings werden viele Schritte standardisiert, um eine Vereinfachung bzw. Effizienzsteigerung zu erhalten. Bei Einhaltung der Anforderungen dieser Vornorm erfüllt eine semi-quantitative Methode die Vorgaben EG CSM-Verordnung zur Risikobewertung.

In dieser Vornorm wird vorausgesetzt, dass sich semi-quantitative Methoden als eine Kombination einer Risikomatrix sowie Tabellen zur Bewertung von Barrieren im Sinne von Risikoreduktionsfaktoren darstellen lassen. Für Methoden wie die Risikomatrix oder Risikoprioritätszahlen ist dies unmittelbar gegeben, für Risikographen wird dies in Annex A erläutert. Alle derzeit veröffentlichten semi-quantitativen Methoden gehören entweder zu einer der Methodenklassen oder stellen eine Kombination daraus dar.

Tabelle 3 stellt die wesentlichen Aspekte bzw. Merkmale semi-quantitativer Risikoanalysen beispielhaft zusammen.

ANMERKUNG Die Benennung der Prozess-Schritte entspricht der EG CSM-Verordnung.

Tabelle 3 – Aspekte semi-quantitativer Risikoanalysen

Nr.	EG CSM Prozess-Schritt	Kapitel	Aspekte bei semi-quantitativen Risikoanalysen
1	Systemdefinition	6.3	Häufig in Form von (zumindest exemplarischen) Funktionslisten.
2	Gefährdungsermittlung	6.4	Häufig Vorgabe von Gefährdungslisten
3	Gefährdungseinstufung	6.5	Häufig direkt anhand des Schadensausmaßes, oder mittels einer Risikomatrix
4	Grundsatz der Risikoakzeptanz	5	In der Regel durch das Verfahren fest vorgegeben.
5	Ermittlung von Szenarien und Sicherheitsmechanismen	6.6	In der Regel Beschränkung pro Funktion oder Gefährdung auf ein maßgebliches Szenario.
6	Abschätzung der Schwere	6.7	In der Regel qualitativ durch Zuordnung des Szenarios zu Folgen-Klassen
7	Abschätzung der Häufigkeit	6.8	In der Regel semi-quantitativ durch Bewertung der Wirksamkeit von Barrieren als Risikoreduktionsfaktoren mittels Zuordnung zu Klassen
8	Vergleich mit Kriterien	6.9	In der Regel in die Methode integriert, häufig Kriterien wie MGS oder RAC-TS.
9	Sicherheitsanforderungen	6.10	In der Regel Ausweisung als HR für Gefährdungen oder SIL für Funktionen (je nach Betrachtungsebene)

In dieser Vornorm werden die relevanten Anforderungen für semi-quantitative Risikoanalysen dargelegt, bei deren Einhaltung die Erfüllung der EG CSM-Verordnung zur Risikobewertung sichergestellt ist. Zur besseren Nachverfolgung der Anforderungen werden diese fortlaufend mit A1, A2 ... durchnummeriert. Diese Anforderungen untergliedern sich in Anforderungen an die Konstruktion der Methode sowie deren Anwendung. Tabelle 8 klassifiziert die Anforderungen.

6.2 Allgemeine Anforderungen

Aus den Anmerkungen in Tabelle 3 wird direkt deutlich, dass die Vereinfachungen, die bei semi-quantitativen Risikoanalysen zu einer Effizienzsteigerung führen, gleichzeitig das Risiko der Missinterpretation bzw. Fehlanwendung erhöhen. Daher muss bei der Konstruktion solcher Methoden sowie bei der Dokumentation der damit erzielten Ergebnisse eine hohe Sorgfalt angewendet werden:

A1) Die Methode muss folgende Punkte eindeutig definieren

- a) das Schutzobjekt (z. B. Fahrgast) und die Bezugseinheiten (z. B. Schadensfälle pro Fahrgaststunde), auf die sich die Methode und ihre Parameter beziehen (erforderlich, weil die Methoden Risikoakzeptanzkriterien und Parameter für Barrieren definieren, deren Anwendung ohne saubere Definition nicht eindeutig ist);
- b) den Anwendungsbereich und den technischen Kontext, auf den sich die Methode und ihre Parameter beziehen (z. B. muss definiert sein, ob sich die Methode und damit das Risikoakzeptanzkriterium auf die Funktion einer einzelnen Komponente einer technischen Einrichtung, auf die Funktion einer vollständigen Applikation einer technischen Einrichtung oder auf die Gesamtheit aller z. B. innerhalb eines Landes installierten Einrichtungen des gleichen technischen Typs bezieht.);
- c) ggf. weitere Parameter und Rahmenbedingungen, die für die eindeutige Anwendbarkeit der Methode erforderlich sind.

- A2) Die Konstruktion von semi-quantitativen Methoden muss im Grundsatz konservativ sein, d. h. im Zweifel müssen bei der Konstruktion entsprechender Klassen Abschätzungen zur sicheren Seite verwendet werden. Dies bedeutet aber nicht, dass alle Abschätzungen oder Beschreibungen worst-case sein müssen, aber in der Regel sollte für das Ergebnis der Methode ein deutliches Abweichen vom Mittelwert zur sicheren Seite hin erkennbar sein (z. B. 90. Perzentil, falls statistische Daten vorliegen)
- A3) Die Bandbreite b bei Klasseneinteilungen sollte in der Regel nicht größer als 10 sein (da in der Regel Sicherheitsanforderungsklassen wie SIL diese Granularität aufweisen)
- A4) Für jede semi-quantitative Methode muss ein Anwender-Handbuch erstellt werden, das Erläuterungen und Beispielanwendungen enthält.
- A5) Bei jeder Anwendung der Methode muss die Wahl der verwendeten Klassen so ausführlich begründet werden, dass sie leicht nachvollziehbar ist.

Die nachfolgenden Unterkapitel beziehen sich auf die einzelnen Prozessschritte aus Tabelle 3 und legen detaillierte Anforderungen und Randbedingungen bei der Nutzung semi-quantitativer Methoden zur Risikoanalyse technischer Funktionen fest.

6.3 Systemdefinition

Nach EG CSM-Verordnung müssen die folgenden Aspekte berücksichtigt werden:

- a) Definition der Zielsetzung des Systems, z. B. der vorgesehene Zweck;
- b) Definition der Funktionen und Bestandteile des Systems, sofern relevant (einschließlich z. B. menschlicher, technischer und betrieblicher Bestandteile);
- c) Definition von Systemgrenzen, einschließlich der Schnittstellen mit anderen Systemen ;
- d) Definition der physischen (d. h. der Systeme, mit denen Schnittstellen vorhanden sind) und funktionalen (d. h. funktionale Ein- und Ausgabe) Schnittstellen;
- e) Definition der Systemumgebung (z. B. Energie- und Wärmefluss, Erschütterungen, Schwingungen, elektromagnetische Störung, Betrieb);
- f) Definition der bestehenden Sicherheitsmaßnahmen;
- g) Definition der Annahmen, die die Grenzen für die Risikobewertung bestimmen.

Viele dieser Anforderungen können durch eine standardisierte Funktionsliste erfüllt werden, die implizit die oben aufgeführten Aspekte definiert.

ANMERKUNG Z. B. definiert eine Funktion „Auslösen der Zwangsbremse im Fahrzeug“ a, b, c, d und e der oben aufgeführten Aspekte. Durch ergänzende Erläuterungen, z. B. bei verdeckt (ohne Führerraumsignalisierung) arbeitender Zugbeeinflussung sowie ausgebildeten und überwachten Eisenbahnfahrzeugführern können dann auch f und g erfüllt werden.

Allerdings werden solche standardisierten Funktionslisten in der Regel nicht vollständig sein, weshalb in der Analyse eines spezifischen Systems eine Gefährdungsermittlung durchzuführen ist. Bei semi-quantitativen Verfahren lassen sich leicht widersprüchliche bzw. falsche Ergebnisse erzielen, wenn solche Methoden auf unterschiedliche Ebenen eines Systems (mit unterschiedlichem Detaillierungsgrad etc) angewendet werden. Daraus ergibt sich die folgende Anforderung:

- A6) Es muss für eine semi-quantitative Methode unter Berücksichtigung der oben genannten Punkte a-g definiert werden, auf welcher Ebene und unter welchen Rahmenbedingungen sie anwendbar ist. Dies kann z. B. durch eine exemplarische Funktionsliste für die zu betrachtenden technischen Funktionen erreicht werden. Die Funktionen der Funktionsliste müssen jeweils einer einheitlichen Systemebene angehören. 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.

Beispiele für solche Funktionslisten finden sich in den Anhängen B, C und D.

6.4 Gefährdungsermittlung

Nach EG CSM-Verordnung sollen sämtliche nach vernünftigem Ermessen vorhersehbaren Gefährdungen für das gesamte zu bewertende System und gegebenenfalls für dessen relevante Funktionen sowie dessen Schnittstellen systematisch ermittelt werden, unter Rückgriff auf die umfassende Fachkenntnis eines qualifizierten Teams.

Im Prinzip kann die Gefährdungsermittlung bei jeder Anwendung neu erfolgen, z. B. mit bekannten Methoden wie FMEA oder HAZOP. Dies hat den Vorteil, dass z. B. im betrachteten Anwendungskontext neu auftretende oder veränderte Gefährdungen leichter erkannt werden. Um die Effizienz zu steigern, sollte empfohlen werden:

- A7) Die Methode muss die Gefährdungsermittlung nach einem bewährten Verfahren enthalten. Es sollte eine Standard-Zuordnung geben, welche Gefährdungen für welche Funktionen betrachtet werden sollten. Bei Verwendung einer Standard-Zuordnung muss zusätzlich untersucht werden, ob im Anwendungskontext ggf. neue oder veränderte Gefährdungen entstehen können.

6.5 Gefährdungseinstufung

Hierbei geht es insbesondere um die effiziente Erkennung von weitgehend akzeptablen Risiken, für deren Beherrschung keine Sicherheitsanforderungen an Funktionen technischer Systeme gestellt werden müssen. Einige semi-quantitative Methoden erlauben es, solche Entscheidungen z. B. anhand der maßgeblichen Unfallschwere zu treffen. Da dieser Schritt nach EG CSM-Verordnung optional ist, sollte empfohlen werden:

- A8) Die semi-quantitative Methode sollte eine einfache Identifikation von weitgehend akzeptablen Risiken erlauben.

6.6 Ermittlung von Szenarien und Sicherheitsmechanismen

Eine Gefährdung (im Sinne eines Funktions-Versagens) muss nicht notwendigerweise einen Unfall verursachen, denn in der Regel gibt es Barrieren im Gesamtsystem, die den Unfall noch verhindern können. Bei den Barrieren kann man unterscheiden zwischen verlässlich bewertbaren Barrieren und solchen, die nur schwer plan- oder bewertbar sind, und deshalb in Risikoanalysen nicht ausgenutzt werden können, siehe Bild 2.

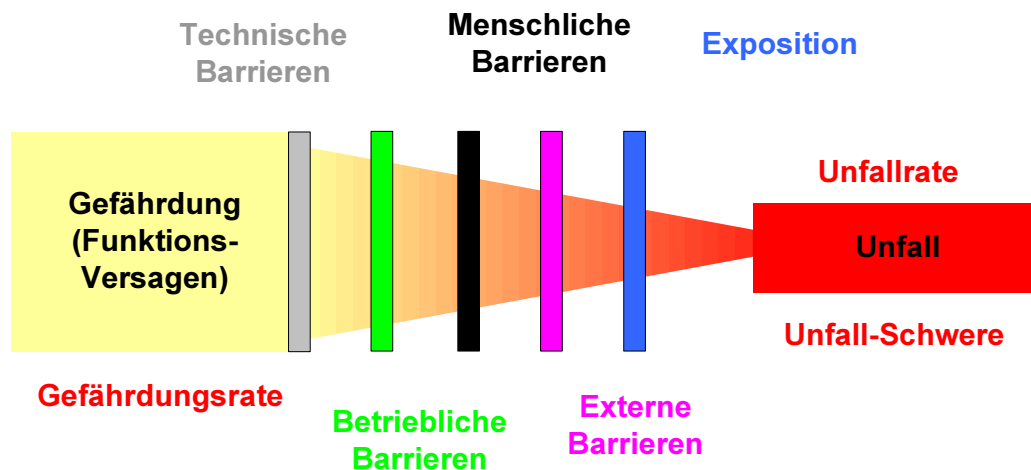


Bild 2 – Grundlegendes Modell

Ein Pfad, ausgehend von der Gefährdung, über die Barrieren zum Schadensereignis (Unfall), wird als Gefährdungsszenario einer Gefährdung bezeichnet.

Nach EG CSM-Verordnung müssen die für die explizite Risikoabschätzung eingesetzten Methoden das System, das der Bewertung unterzogen wird, und seine Parameter (einschließlich aller Betriebsmodi) korrekt wiedergeben.