Preprint IVWT 2009, Dresden

Risikoorientierte Beurteilung von potenziellen Sicherheitsmängeln

J. Braband, E. de Stefano, J. Stutzbach

Siemens AG, Industry Sector, Mobility Division

Ackerstr. 22, 38106 Braunschweig, Deutschland

Kurzfassung:

Im August 2009 ist die Vornorm DIN V VDE V 0831-100 erschienen, die sich mit der Risikobeurteilung potenzieller Sicherheitsmängel (PSM) befasst. In diesem Beitrag wird ein spezifisches Verfahren vorgestellt, das die Anforderungen dieser Norm erfüllt und damit die Entscheidungsfindung bei PSM nachvollziehbar und transparent macht. Das so genannte PSM-RPZ-Verfahren hat sich in unterschiedlichen Varianten seit mehreren Jahren in der Praxis bewährt. Es ist nach ingenieurwissenschaftlichen Prinzipien konstruiert und führt bei korrekter Anwendung nachweislich zu verlässlichen Entscheidungen. Es leistet einen wesentlichen Beitrag sowohl zur Steigerung der Wirtschaftlichkeit des Eisenbahnbetriebs als auch zur Erhöhung der Qualität, insbesondere im Bereich Complaint Management.

Schlagworte:

Funktionale Sicherheit, Risikoprioritätszahl, Risikobeurteilung, potenzieller Sicherheitsmangel.

1 Einleitung

Bei potenziellen Sicherheitsmängeln besteht der Verdacht einer Abweichung vom spezifizierten Normalverhalten. Es liegt also eine potenziell gefährliche betriebliche Situation vor. Kurzfristig muss bewertet werden, wie hoch das Risiko des (Wieder-)Eintritts des PSM ist und welche (Sofort-)Maßnahmen gegebenenfalls ergriffen werden müssen, um mindestens gleiche Sicherheit bis zur Behebung des PSM zu gewährleisten.

Bei klassischen Risikoanalysen geht es vornehmlich darum, das Risiko einer Vielzahl von Gefährdungen zu bewerten, die in der Regel noch nicht eingetreten sind. Dies bedeutet, ein (zumeist) hypothetischer Fall wird pro-aktiv bewertet. Bei PSM stellt sich das Problem anders dar: Wird ein PSM bei einem Eisenbahnsystem bekannt, befinden sich alle Beteiligten (z. B. Hersteller, Betreiber, Gutachter, Sicherheitsbehörde) bei den modernen, hochverfügbaren und hoch zentralisierten technischen Systemen in einer doppelten Zwickmühle: Wenn aufgrund des PSM z. B. ein technisches System abgeschaltet wird, ist die Betriebsführung in der Rückfallebene unsicherer als der technisch gesicherte Normalbetrieb. Wenn aufgrund des PSM risikoreduzierende Maßnahmen (RM) getroffen werden müssen, wird es in der Regel verschiedene mögliche Maßnahmen geben, die hinsichtlich ihrer Wirksamkeit und ihrer wirtschaftlichen Angemessenheit kurzfristig bewertet werden müssen.

Unterstützung bietet in diesem Fall eine risikobasierte Vorgehensweise. Sie kann:

- eine objektivierbare Entscheidungshilfe bieten, in welchem Ausmaß und welcher Dringlichkeit Maßnahmen durchzuführen sind, um technisch oder betrieblich die Sicherheit des Betriebs weiterhin zu gewährleisten,
- eine objektive Entscheidungshilfe bieten, wie lange ein PSM (bei möglicherweise eingeleiteten Maßnahmen) gegebenenfalls geduldet werden kann, sowie
- die Ableitung vergleichbarer Maßnahmen für ähnlich kritische PSM ermöglichen.

Dabei müssen die aufgrund einer solchen Vorgehensweise getroffenen Entscheidungen sowohl verlässlich sein als auch zeitnah zum Auftreten des PSM getroffen werden können. Daher bieten sich insbesondere Risikoprioritätszahlen (RPZ) oder andere Varianten semi-quantitativer Verfahren an.

Um verbindliche Vorgaben sowohl für den Prozess der Bearbeitung von PSM als auch für Bewertungsmethoden zu machen, wurde die DIN V VDE V 0831-100 [1] erarbeitet.

2 Normative Grundlagen

Die DIN V VDE V 0831-100 ist nach Kenntnis der Autoren die einzige Norm in der Eisenbahntechnik, die sich mit der Behandlung von PSM befasst. Ihr Anwendungsbereich ist die funktionale Sicherheit von Eisenbahnautomatisierungssystemen und deckt sich mit dem der DIN EN 50129 [2] und DIN EN 50128 [3]. Sie ist als nationale Vornorm erstellt worden, da eine internationale Normung derzeit nicht als aussichtsreich eingeschätzt wird – zumindest nicht in einem überschaubaren Zeitraum.

Die Herausgabe der Vornorm bedeutet Rechtssicherheit für Anwender (insbesondere Gutachter), die Entscheidungen im Zusammenhang mit PSM treffen müssen. Bei Einhaltung einer Norm gilt nämlich die (allerdings widerlegbare) Vermutung, dass die Beurteilung des Produktsicherheitsmangels dem Stand der Technik entspricht. Hinsichtlich der rechtlichen Bedeutung sind Normen und Vornormen gleichgestellt.

Die Vornorm gliedert sich im Wesentlichen wie folgt:

1. Risikakzeptanzkriterium „Mindestens Gleiche Sicherheit“ (MGS)
2. Prozess zur PSM-Bewertung
3. Anwendungsbeispiele (informativ)

2.1 Risikoakzeptanz

Die Diskussion des Risikakzeptanzkriterium „Mindestens Gleiche Sicherheit“ (MGS) ist bereits in der Fachliteratur detailliert erfolgt [4] und soll hier nur kurz zusammengefasst werden.

Unter Fachleuten ist unstrittig, dass bei Ergebnissen von quantitativen Risikoanalysen und deren Nachweisen aufgrund der Unsicherheiten in Daten und Schätzwerten bestenfalls die Größenordnung korrekt ist. Dieser Auffassung folgt auch die Vornorm, indem sie vorschlägt, semi-quantitative Verfahren zu verwenden, bei denen die Parameterwerte in Klassen mit gewissen Bandbreiten eingeteilt werden. Hier bedeutet MGS, dass bei der Bewertung eines Systems gegenüber einem Referenzsystem die Bewertungsergebnisse in die gleiche Klasse fallen (siehe Abbildung 1).

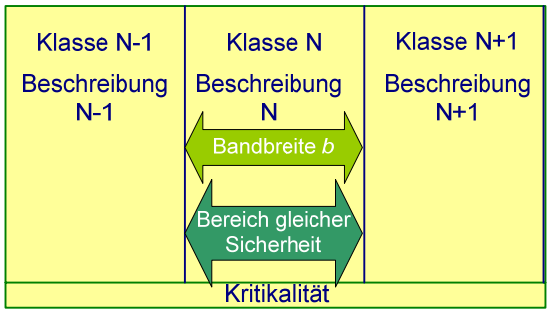

Abbildung 1: Interpretation von MGS für semi-quantitative Verfahren

2.2 Bewertungsprozess

Die Prozessdarstellung in Abbildung 2 ist weitgehend selbsterklärend. Für die Details des Prozesses sei auf die Vornorm verwiesen [1]. Hier sei nur auf einige wichtige Anforderungen hingewiesen: Zu Beginn der PSM-Bewertung und auch während jedes Prozessschrittes muss geprüft werden, ob der PSM die folgenden Bedingungen erfüllt:

1. Der PSM kann bei einem in Betrieb befindlichen System auftreten.
2. Der PSM betrifft eine Sicherheitsfunktion.
3. Der PSM wirkt sich risikoerhöhend (im Vergleich zur expliziten Sicherheitsanforderung) aus.

Bei PSM muss grundsätzlich (von klar abgegrenzten Ausnahmen abgesehen) jeder erkannte Sicherheitsmangel behoben werden. Es geht also darum festzulegen, in welchem Zeitraum der Fehler behoben werden muss und ob gleichzeitig Maßnahmen zu ergreifen sind. Der PSM-Prozess ist damit Teil der Sicherheitsmanagement-Systems (SMS).

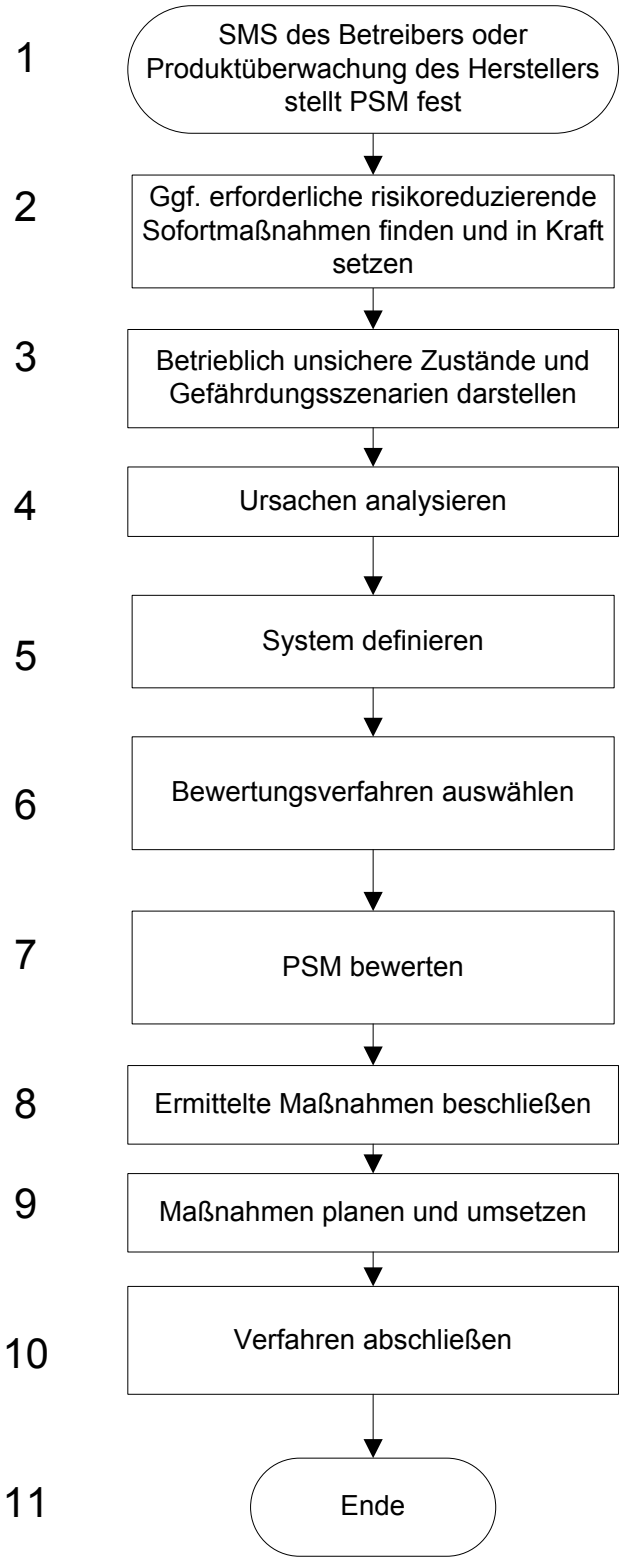

Abbildung 2: Prozess der PSM-Bewertung

2.3 Grundmodell der PSM-Bewertung

Dem Prozess liegt folgendes Modell zugrunde: Ein PSM kann unter bestimmten technischen und betrieblichen Randbedingungen in Erscheinung treten. Dies ist dann der Fall, wenn durch den PSM ein betrieblicher Zustand eintritt, der vom normalen betrieblichen Zustand gefährlich abweicht. Beispiel: Dem Eisenbahnfahrzeugführer wird eine höhere Geschwindigkeit signalisiert als zulässig ist.

Unter ungünstigen Randbedingungen kann es aufgrund des PSM zu einem Schaden kommen. Bildlich vorstellen kann man sich diese Randbedingungen als Barrieren zwischen dem vom PSM betroffenen System und dem Schadensereignis (siehe Abbildung 3). Als Barrieren wirken in erster Linie technische und betriebliche Randbedingungen. Sie beeinflussen primär, wie häufig der PSM betrieblich in Erscheinung tritt. Letzte Barriere sind oft die Bediener (z. B. Fahrdienstleiter oder Eisenbahnfahrzeugführer) und Außenstehende (z. B. Straßenverkehrsteilnehmer oder Reisende). Beide können eventuell das drohende Schadensereignis (betrieblich unsicherer Zustand) erkennen und den bevorstehenden Unfall abwenden (menschliche Gefahrenabwehr).

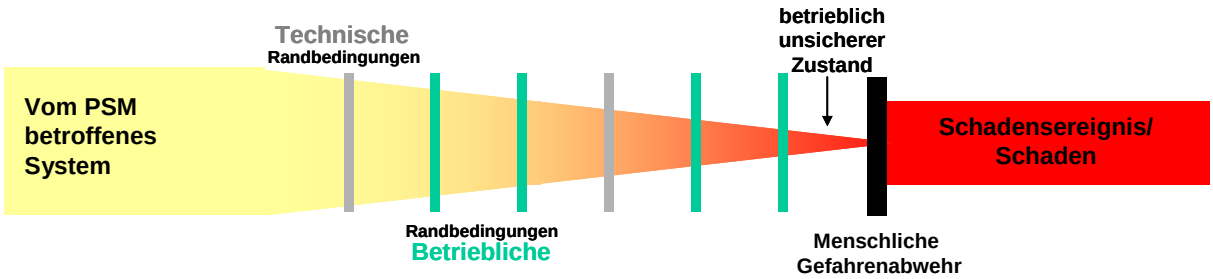

Abbildung 3: Grundmodell der PSM-Bewertung

Ein durch einen PSM verursachter betrieblich unsicherer Zustand liegt vor, wenn nur noch durch menschliche Gefahrenabwehr ein Schaden abgewendet werden kann. Ein Pfad über die Randbedingungen, den betrieblich unsicheren Zustand und die gescheiterte menschliche Gefahrenabwehr hin zum Schadensereignis, wird als Gefährdungsszenario eines PSM bezeichnet. Ein PSM kann verschiedene Auswirkungen haben und somit verschiedene Gefährdungsszenarien aufweisen.

In Verbindung mit einem Gefährdungsszenario steht eine Funktion, die durch eine Kombination von Hardware, Software und menschlichem Handeln erbracht wird. Diese Funktion soll das Eintreten des betrieblich unsicheren Zustands verhindern, ist jedoch durch den PSM beeinträchtigt, d. h. fehlerbehaftet.

Viele PSM beeinflussen nur die Häufigkeit, mit der ein Gefährdungsszenario eintritt, nicht aber das Schadensausmaß oder die Möglichkeiten zur Gefahrenabwehr. In diesem Fall kann man anhand der Sicherheitsanforderungen der Funktion (SIL) und der Häufigkeit des Gefährdungsszenarios direkt eine Abschätzung herleiten, ob RM notwendig sind und wie lange der PSM toleriert werden kann.

Ergibt die Analyse, dass RM notwendig sind, so müssen weitere Parameter bewertet werden – je nachdem, auf welchen Parameter die jeweils vorgeschlagene RM wirken soll. In diesem Fall wird die Bewertung solange iteriert, bis genügend wirksame RM

definiert sind und der PSM unter diesen veränderten Randbedingungen bis zu seiner Behebung toleriert werden kann.

2.4 Bewertung von PSM mit RPZ

Grundsätzlich werden bei semi-quantitativen Verfahren die zur Risikobewertung herangezogenen Parameter nicht quantifiziert, sondern mit Rangzahlen klassifiziert (siehe Abbildung 1). Dabei werden üblicherweise die gleichen oder ähnliche Parameter wie bei Risikoanalysen betrachtet, d. h. Schadensausmaß und Schadenshäufigkeit. Bei Bedarf werden diese Parameter durch Beurteilung weiterer Subparameter ermittelt, z. B. Möglichkeit zur Gefahrenabwehr.

In der Vornorm werden die Verfahren verwendet, die auf der FMECA der DIN EN 60812 [5] basieren. Für jeden verwendeten Parameter müssen eine Bewertungstabelle sowie eine Verknüpfungsvorschrift für die Parameterwerte zur Ermittlung der Kritikalität aufgestellt werden. Die Kritikalität, hier ausgedrückt durch die RPZ, ist ein semi-quantitatives Maß für das Risiko. Das Risikoakzeptanzkriterium MGS wird hier interpretiert als „Höchstens Gleiche Kritikalität“ bzw. „Höchstens Gleiche RPZ“.

Um zu verlässlichen Einschätzungen zu kommen, müssen RPZ-Verfahren die folgenden Eigenschaften besitzen:

1. Rationale Skalierung: Die Skalierung der Bewertungstabellen muss zumindest approximativ rational sein, d. h., die Bandbreite der Klassen b sollten annähernd gleich sein.
2. Monotonie: Wenn das Risiko für Szenario i kleiner als für Szenario j ist, so muss die RPZ für Szenario i kleiner oder gleich der RPZ für Szenario j sein.
3. Genauigkeit: Wenn die RPZ für Szenario i gleich der RPZ für Szenario j ist, so müssen das Risiko für Szenario i und das Risiko für Szenario j annähernd gleich sein.
4. Sensitivität: Kleine Änderungen in den Parameterwerten bewirken nur kleine Änderungen in der RPZ.

Bei der RPZ-Bewertung muss entweder fallweise ein Referenzsystem oder eine explizite Sicherheitsanforderung definiert werden (beides hier als Referenzsystem R bezeichnet). Dann wird für das System S die RPZ bestimmt. Für das Referenzsystem R wird die RPZ für die oben ermittelten Gefährdungsszenarien ermittelt (unter Berücksichtigung des geplanten Behebungszeitraums). Bei Bedarf müssen zusätzliche Maßnahmen definiert werden, um das Risikoakzeptanzkriterium MGS zu erreichen.

Anstatt die RPZ für beide Systeme explizit zu bestimmen, kann bei Vorliegen von expliziten Sicherheitsanforderungen auch direkt der zulässige Behebungszeitraum aus den Parameterwerten ermittelt werden.

3 Das Verfahren PSM-RPZ

Mit dem Verfahren PSM-RPZ wird eine semi-quantitative Kritikalitätsbewertung durchgeführt. Nach Anwendung des Verfahrens soll das System mit dem potenziellen Sicherheitsmangel S keine höhere Kritikalität aufweisen als durch die expliziten Sicherheitsanforderungen erlaubt. Dies bedeutet, dass nach Anwendung von PSM-RPZ das Risikoakzeptanzkriterium MGS erfüllt ist.

Ziel ist die Ermittlung eines angemessenen Behebungszeitraums des PSM anhand seiner Kritikalität in Bezug auf die expliziten Sicherheitsanforderungen.

3.1 Voraussetzungen

Das Verfahren PSM-RPZ wird nur angewendet, wenn die Ursache ein Fehler einer sicherheitsrelevanten Funktion ist, für die eine explizite Sicherheitsanforderung in Form eines SIL vorliegt oder ermittelt wurde. Aus dem übergeordneten Prozess sind die betrieblich unsicheren Zustände sowie die Gefährdungsszenarien bekannt. Das grundlegende Modell für die Anwendung dieses Verfahrens ist in Abbildung 3 dargestellt.

3.2 Bewertungsprozess

Die wesentlichen Prozessschritte sind in Abbildung 4 dargestellt und werden in den folgenden Abschnitten beschrieben.

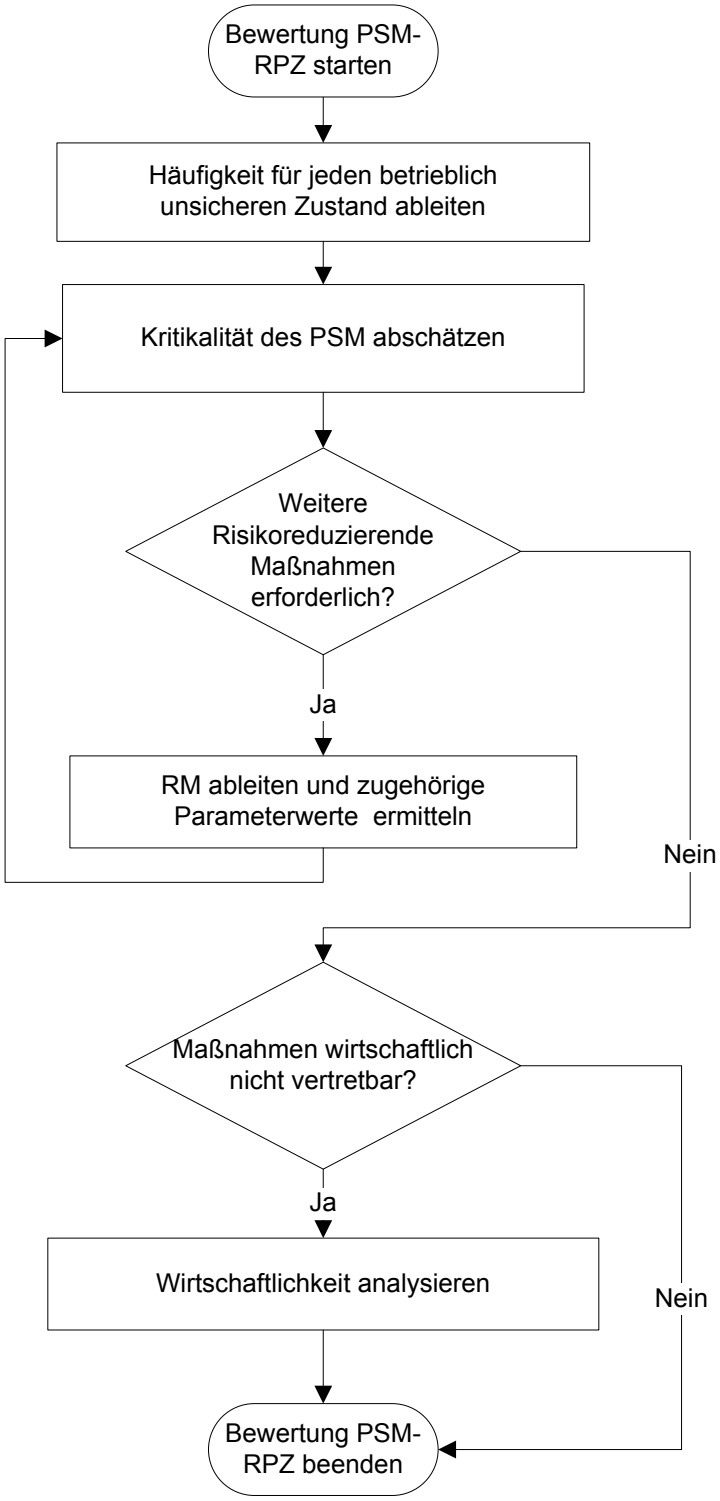

Abbildung 4: Ablauf der PSM-RPZ-Bewertung

3.3 Bewertung der Häufigkeit

Der Parameter Häufigkeit (H)

- wird für jede vom PSM betroffene Funktion und somit für jedes Gefährdungsszenario ermittelt,
- bezieht sich jeweils auf eine Gruppe von Hardware- und Software-Elementen, die die jeweilige Funktion realisiert, und
- gibt jeweils für die vom PSM betroffene Funktion an, wie lange es bezogen auf den einzelnen Betrachtungsgegenstand im Mittel dauert, bis der betrieblich unsichere Zustand das nächste Mal auftritt.

Beispiel: Von einem PSM betroffen sei die Funktion „Weichensteuerung“. Beteiligt an dieser Funktion seien für eine Weiche bestimmte Hardware- und Software-Elemente. Betrachtungsgegenstand ist die einzelne Weiche und nicht die Summe aller vom PSM betroffenen Weichen. Eine unter dem Zug umlaufende Weiche tritt aufgrund der von einem PSM betroffenen Funktion „Weichensteuerung“ pro Weiche alle x Jahre auf.

Detaillierte Informationen sind bei Beginn der Risikobewertung eines PSM meistens nicht vorhanden. Der Parameter H und somit auch die Endergebnisse werden sich bei Bekanntwerden neuer Randbedingungen ändern. Da die Berücksichtigung von Randbedingungen als Reduktionsfaktoren bei der Ermittlung der Häufigkeit eingehen, bedeuten fehlende Informationen einen größeren Parameter H und somit eine konservative Einschätzung der Kritikalität.

Die Beschreibung der betrieblich unsicheren Zustände bildet die Grundlage für die Einschätzung der Häufigkeit. In den nächsten Schritten werden die Randbedingungen aufgeführt, die den PSM in Gestalt dieser betrieblich unsicheren Zustände „erscheinen“ lassen. Diese Bedingungen sollen prägnant in ein oder zwei Sätzen dargestellt werden.

An dieser Stelle sollen also weder der Mangel selbst in seiner Ausprägung noch seine Ursachen oder das mögliche Schadensereignis beschrieben werden.

Ein PSM kann entweder betrieblich in Erscheinung treten (mit oder ohne Schadenfolge) oder durch theoretische Analysen bzw. Labortests entdeckt werden. In jedem dieser Fälle können und sollen die möglichen Auswirkungen des PSM in Form der betrieblich unsicheren Zustände formuliert werden.

Bei jedem Gefährdungsszenario werden für den betrieblich unsicheren Zustand alle Umstände (Randbedingungen) aufgelistet, die vorhanden sein oder hinzukommen müssen, damit dieser Zustand auftritt. Diese Randbedingungen können sowohl Zustände als auch Ereignisse sein.

Das Geflecht an Randbedingungen kann sehr komplex sein. An dieser Stelle sollen einige Zustände und Ereignisse beispielhaft genannt werden, die mögliche Randbedingungen sein könnten.

Zustände:

- Belegung von Abschnitten
- Signalbilder
- Weichenlage

Ereignisse:

- Störungen, Ausfälle von Hardware oder systematisch ungewünschtes Verhalten von Software
- Anforderungsgemäßes Verhalten von Hardware oder Software
- Ankunft eines Zuges (z. B. an einen Bahnübergang oder an einem Zählpunkt)
- Fahrstraßenfestlegung
- Fahrstraßenauflösung
- Weichenumlauf
- Handlungen des Personals
- Handlungen von Dritten

Oft gibt es zwischen den Randbedingungen zeitliche Abhängigkeiten, die Einfluss haben auf die Auftretenswahrscheinlichkeit eines Ereignisses oder Zustandes. Für die spätere Berechnung ist die Beschreibung dieser Abhängigkeiten sehr wichtig.

Es ist darauf zu achten, dass eine eventuell mögliche menschliche Gefahrenabwehr nicht als Randbedingung bei der Bewertung des Parameters H berücksichtigt werden darf. Aus diesem Grund ist es besonders wichtig, den betrieblich unsicheren Zustand klar zu beschreiben. Nur so kann dieser als klare Trennung zwischen den technischen/betrieblichen Randbedingungen und der menschlichen Gefahrenabwehr dienen.

Die Randbedingungen sollten in Form von Ereignissen und Zuständen aufgelistet werden. Aus der Liste der Randbedingungen muss eine Randbedingung bestimmt werden, für die eine Häufigkeitseinschätzung in der Form: „Ein Mal in x Tagen, Monaten oder Jahren“ getroffen werden kann.

Beispiele:

- Zuverlässigkeitsprognose einer Baugruppe, die im Durchschnitt ein Mal in 20 Jahren ausfällt
- Beeinflussung eines Zählpunktes durch einen Zug, die im Durchschnitt ein Mal in fünf Minuten auftritt

Für die Berechnung der Wiederholungshäufigkeit des betrieblich unsicheren Zustandes wird diese Häufigkeitseinschätzung als Ausgangspunkt verwendet.

Alle weiteren Randbedingungen gehen in Form von Reduktionsfaktoren in die Berechnung der Häufigkeit ein. Beispielsweise kann es als Randbedingung notwendig sein, dass sich eine Weiche zu einem bestimmten Zeitpunkt in einer bestimmten Lage befindet. Schätzt man ein, dass dies etwa in jedem zehnten Fall so ist, ergibt sich der Faktor 1/10.

Sofern quantitative Parameterwerte nicht aus Berechnungen oder anderorts dokumentierten Angaben entnommen werden können, ist eine Schätzklausur mit drei bis fünf Personen durchzuführen. Die an der Schätzklausur Beteiligten müssen sich einvernehmlich auf einen Wert einigen.

Die Parameterwerte je betrieblich unsicherem Zustand (und somit je betroffener Funktion) werden berechnet, indem man die zur Funktion gehörige Häufigkeit (1/Zeiteinheit) mit den ebenfalls zur Funktion gehörigen Wahrscheinlichkeiten (einheitenlos) multipliziert. Die ermittelten Häufigkeiten (1 Mal in x Tagen, Monaten oder

Jahren) liefern die Eingangswerte für die Tabelle 1: Skala für Parameter H**Fehler! Verweisquelle konnte nicht gefunden werden.**, aus der sich die entsprechenden Parameterwerte H für die Häufigkeit der betrieblich unsicheren Zustände ablesen lassen.

Wenn nur die Symptome eines PSM beobachtet worden oder bekannt sind, ist es nur sehr begrenzt oder gar nicht möglich, die notwendigen Randbedingungen darzustellen, die zum betrieblich unsicheren Zustand führen. Eine Bewertung des Parameters H ist über die Einzelbewertung der Randbedingungen somit nicht möglich.

Der einzig mögliche Weg zur Ermittlung des Parameterwertes H führt über die Auswertung der Betriebserfahrung: „Bestehenszeit des PSM ohne aufgetretenem betrieblich unsicheren Zustand“.

Beispiel: Von einem PSM betroffen sei die Funktion „Weichensteuerung“. Beteiligt an dieser Funktion seien für eine Weiche bestimmte Hardware- und Software-Elemente. Betrachtungsgegenstand ist die einzelne Weiche und nicht die Summe aller von dem PSM betroffenen Weichen.

Der PSM sei in diesem Beispiel beobachtet worden durch den betrieblich unsicheren Zustand „Weiche läuft zur Unzeit um“. Die genauen Einzelheiten des Mangels sollen jedoch nicht bekannt sein. Somit lassen sich die notwendigen Randbedingungen nicht darstellen, die zum Umlaufen der Weiche zur Unzeit führen.

Zur Ermittlung des Zeitraums mit PSM ohne aufgetretenen betrieblich unsicheren Zustand wären folgende Aspekte zu berücksichtigen:

- Wie lange ist die Funktion mit PSM in Betrieb?
- Wie lange ist die bestehende Kombination von Hardware- und Software-Elementen (bezogen auf die betroffene Funktion) im Einsatz?
- Haben sich in dieser Zeit betriebliche oder technische Randbedingungen geändert, die ein Auftreten eines betrieblich unsicheren Zustands erst ermöglichen oder wahrscheinlicher machen? Wenn ja, dann wäre der Zeitraum von der geänderten Situation bis zur erstmaligen Beobachtung relevant.
- Wie viele Weichen waren in dem relevanten Zeitraum vom PSM betroffen?

Wenn die Anzahl nicht über den gesamten Zeitraum konstant war, ist ein Durchschnittswert zu ermitteln. Als Ergebnis würde man folgende Argumentation verwenden:

Bei einer Anzahl von X Weichen im relevanten Zeitraum von Y (in Jahren) ist der PSM ein Mal in Erscheinung getreten. Auf eine Weiche bezogen ist mit einer Häufigkeit von ein Mal alle X*Y Jahre damit zu rechnen, dass der PSM betrieblich unsicher in Erscheinung tritt.

3.4 Skalierung des Parameters H

Die Häufigkeitstabelle wurde ähnlich wie bei semi-quantitativen Verfahren zur Risikoanalyse [6] approximativ mit dem Faktor $\sqrt{10} \cong 3{,}2$ skaliert. Diese Genauigkeit ist für praktische Anwendungen ausreichend. Zudem lässt sich in der Regel auch mit quantitativen Betrachtungen keine höhere Genauigkeit erreichen und man sollte diese auch nicht suggerieren.

Beschreibung für H	H
Täglich	17
Halbwöchentlich	16
Wöchentlich	15
Monatlich	14
Vierteljährlich	13
Jährlich	12
Einmal je 3 Jahre	11
Einmal je 10 Jahre	10
Einmal je 30 Jahre	9
Einmal je 100 Jahre	8
Einmal je 300 Jahre	7
Einmal je 1.000 Jahre	6
Einmal je 3.000 Jahre	5
Einmal je 10.000 Jahre	4
Einmal je 30.000 Jahre	3
Einmal je 100.000 Jahre	2
Einmal je 300.000 Jahre	1
Einmal je 1.000.000 Jahre	0

Tabelle 1: Skala für Parameter H

3.5 Bestimmung des Behebungszeitraums für den PSM

Ein PSM kann unterschiedliche Gefährdungsszenarien mit unterschiedlichen betrieblich unsicheren Zuständen aufweisen. In Verbindung mit einem Gefährdungsszenario steht eine Funktion, die durch eine Kombination von Hardware, Software und menschlichem Handeln erbracht wird. Diese Funktion soll das Eintreten des zum Gefährdungsszenario gehörenden betrieblich unsicheren Zustands verhindern.

Jede vom Mangel betroffene Funktion wird mit dem ermittelten Parameter H und (falls risikoreduzierende Maßnahmen notwendig sind) mit dem weiteren Parameter ΔRM in Bezug zur Sicherheitsintegritätsanforderung (SIL) dieser Funktion gesetzt (siehe Tabelle 2). Das Ergebnis ist ein zulässiger Behebungszeitraum für die vom PSM betroffene Funktion. Dabei wurde aus pragmatischen Gründen die Obergrenze auf 60 Monate gesetzt, obwohl rechnerisch noch größere Werte erlaubt wären (in den grau unterlegten Zellen).

Wenn keine risikoreduzierenden Maßnahmen geplant sind oder ergriffen werden, geht der Parameter ΔRM nicht in die Ermittlung ein.

<table>
<tr><th>H-ΔRM</th><th>SIL-1-Funktion</th><th>SIL-2-Funktion</th><th>SIL-3-Funktion</th><th>SIL-4-Funktion</th></tr>
<tr><td>0</td><td rowspan="8">60 Monate</td><td rowspan="5">60 Monate</td><td rowspan="3">60 Monate</td><td rowspan="2">60 Monate</td></tr>
<tr><td>1</td></tr>
<tr><td>2</td><td>36 Monate</td></tr>
<tr><td>3</td><td>12 Monate</td></tr>
<tr><td>4</td><td>36 Monate</td><td>4 Monate</td></tr>
<tr><td>5</td><td>12 Monate</td><td>1 Monat</td></tr>
<tr><td>6</td><td>36 Monate</td><td>4 Monate</td><td rowspan="6"></td></tr>
<tr><td>7</td><td>12 Monate</td><td>1 Monat</td></tr>
<tr><td>8</td><td>36 Monate</td><td>4 Monate</td><td rowspan="4">Risikoreduzierede Maßnahmen sind notwendig</td></tr>
<tr><td>9</td><td>12 Monate</td><td>1 Monat</td></tr>
<tr><td>10</td><td>4 Monate</td><td rowspan="3"></td></tr>
<tr><td>11</td><td>1 Monat</td></tr>
<tr><td>>11</td><td colspan="3"></td></tr>
</table>

Tabelle 2: Matrix zur Ermittlung des Behebungszeitraums

Wenn die Sicherheitsintegritätsanforderung SIL der vom PSM betroffenen Funktion nicht aus Risiko- oder Gefährdungsanalysen bekannt ist, kann sie durch entsprechende Analysen ermittelt werden. Ist dies nicht möglich oder liegen entsprechende Ergebnisse nicht vor, so muss SIL 4 angenommen werden.

Wenn der zulässige Behebungszeitraum zu kurz ist, müssen RM definiert und bewertet werden.

3.6 Bewertung von risikoreduzierenden Maßnahmen (RM)

Die Ableitung von risikoreduzierenden Maßnahmen kann erforderlich geworden sein, weil

- mit Tabelle 2 dieses Ergebnis ermittelt wurde,
- innerhalb des mit Tabelle 2 ermittelten Zeitraums die Behebung des PSM nicht realisierbar ist und man durch den Einfluss von RM eine Verlängerung des zulässigen Behebungszeitraums erwirken möchte.

Natürlich können auch RM ergriffen werden, obwohl sie aufgrund der Analysen nicht unbedingt erforderlich gewesen wären. Dies ist z. B. dann sinnvoll, wenn sich mit geringem zusätzlichen Aufwand das Risiko deutlich reduzieren lässt.

Die Wirksamkeit der betrieblichen Maßnahmen kann über ihre Risikoreduktion bewertet werden. Durch diese Risikoreduktion kann der zulässige Zeitraum für das Beheben einer mangelbehafteten Funktion verlängert werden.

Risikoreduzierende betriebliche Maßnahmen können ihre Wirkung in jedem der folgenden drei Bereiche haben:

- RM mit Wirkung im Bereich Häufigkeit: Die geplanten Maßnahmen fügen für ein oder mehrere Gefährdungsszenarien entweder eine weitere Barriere (Randbedingung) hinzu oder verändern die Wirksamkeit einer bestehenden Barriere. Dadurch reduziert sich die Häufigkeit eines oder mehrerer betrieblich unsicherer Zustände.
- RM mit Wirkung im Bereich Schadensausmaß: Die geplanten Maßnahmen reduzieren die Schwere des Schadens eines oder mehrerer Gefährdungsszenarien (z. B. Geschwindigkeitseinschränkungen).
- RM mit Wirkung im Bereich Gefahrenabwehr: Die geplanten Maßnahmen schaffen eine Möglichkeit zur menschlichen Gefahrenabwehr (z. B. Betriebspersonal wird zur Überwachung bestimmter Abläufe zusätzlich bereitgestellt) oder sie verbessern eine bestehende Möglichkeit (z. B. Anweisungen an das Betriebspersonal, in bestimmten Situationen auf bestimmte Art und Weise zu reagieren).

Die Bewertung der RM mit Wirkung im Bereich Häufigkeit ist offensichtlich. Für die anderen Wirkungsbereiche ist die damit ereichte Risikoreduktion zu bewerten. Die Bewertung kann individuell geschehen (unter der Berücksichtigung, dass eine Stufe in Tabelle 2 approximativ dem Faktor $\sqrt{10} \cong 3{,}2$ entspricht) oder durch zusätzliche Tabellen für den jeweiligen Wirkungsbereich. Dies wird beispielhaft für RM mit Wirkung im Bereich der menschlichen Gefahrenabwehr dargestellt, da dies einer der häufigsten Anwendungsfälle ist.

3.7 Bewertung von RM im Bereich menschlicher Gefahrenabwehr

Der Parameter Gefahrenabwehr (G) kann nur dann bewertet werden, wenn RM abgeleitet wurden, die im Bereich der menschlichen Gefahrenabwehr wirken. Für die betroffene Funktion müssen daher der Parameterwert H_M ohne Berücksichtigung der RM und der Parameterwert G_{RM} unter Berücksichtigung der RM ermittelt werden.

Wenn der PSM betrieblich in Erscheinung tritt, d. h. der zugehörige betrieblich unsichere Zustand aufgrund der Anwesenheit der „erforderlichen“ Randbedingungen auftreten konnte, ist es eventuell noch möglich, dass es nicht zum Schadensereignis kommt. An dieser Stelle soll nur der Eingriff des Menschen bewertet werden, der durch seine Handlung einen Schaden abwenden kann. Es ist möglich, dass einem Eisenbahnfahrzeugführer ein Abschnitt fälschlicherweise als frei signalisiert wird, er jedoch die Gefahr (möglicherweise ein im Abschnitt stehender Zug) erkennt und seinen Zug noch rechtzeitig anhalten kann.

Der Bewertung des Parameters G soll nur eine mögliche menschliche Handlung zugrunde gelegt werden. Es soll nur die Handlung bewertet werden, die am wirksamsten ist. Wichtig ist dabei auch, dass diese mögliche menschliche Handlung nur an dieser Stelle und nicht bei der Bewertung des Parameters Häufigkeit berücksichtigt werden darf.

Unter zwei Voraussetzungen lässt sich die Gefahr abwehren, die vom betrieblich gefährlichen Zustand ausgeht. Erstens muss die Gefahr vom Menschen erkannt werden. Zweitens muss die Wirksamkeit der Abwehr unabhängig von den Randbedingungen sein, die zum Auftreten des betrieblich unsicheren Zustands führten. Ein Eisenbahnfahrzeugführer darf beispielsweise nicht als Gefahrenabwehr berücksichtigt werden, wenn er die Gefahr nur mit Hilfe einer Anzeige wahrnehmen kann, die zuvor ausgefallen ist und mit zum Auftreten des betrieblich unsicheren Zustands geführt hat.

Die Art und somit die Wirksamkeit der Handlungen soll wie folgt bestimmt werden:

- Regelbasiertes Handeln unter günstigen bzw. ungünstigen Bedingungen:
  Es gibt eindeutige Anweisungen, wie zu handeln ist. Die Regeln wurden geübt, gehören aber nicht zum täglichen Handlungsrepertoire. Da bei der Gefahrenabwehr immer eine betriebliche Ausnahmesituation vorliegt, ist der Mensch auch immer einer Stresssituation ausgesetzt. Unter ungünstigen Bedingungen soll an dieser Stelle eine Situation verstanden werden, in der nicht genug Zeit vorhanden ist darüber nachzudenken, welche Handlung am effektivsten wäre.
- Wissensbasiertes Handeln unter günstigen bzw. ungünstigen Bedingungen:
  Für die Situation existieren keine Regeln. Der Mensch ist bei der Bewältigung der Situation auf sich allein gestellt. Da bei der Gefahrenabwehr immer eine betriebliche Ausnahmesituation vorliegt, ist der Mensch auch immer einer Stresssituation ausgesetzt. Unter ungünstigen Bedingungen soll an dieser Stelle eine Situation verstanden werden, in der zwar eine effektive Handlung zur Gefahrenabwehr möglich ist, aber die Zeit sehr knapp ist, um die richtige Entscheidung zu treffen.

Handlungen, die man als fertigkeitsbasiert bezeichnen würde, da sie regelmäßig ausgeführt werden und sozusagen in „Fleisch und Blut“ übergegangen sind, kommen als Handlungen zur Gefahrenabwehr nicht in Frage, da es sich bei einem betrieblich unsicheren Zustand immer um eine betriebliche Ausnahmesituation handelt.

In Tabelle 3 wurde die qualitative Bewertung analog zu dem Vorgehen bei Risikoanalysen [6] in ein semi-quantitatives Schema umgesetzt.

Beschreibung für G	G
Nicht möglich	4
Wissensbasiertes Handeln unter ungünstigen Bedingungen	3
Wissensbasiertes Handeln unter günstigen Bedingungen	2
Regelbasiertes Handeln unter ungünstigen Bedingungen	1
Regelbasiertes Handeln unter günstigen Bedingungen	0

Tabelle 3: Skala für den Parameter Gefahrenabwehr

3.8 Einfluss der RM auf den Behebungszeitraum

Im Regelfall wird sich die Wirkung von RM auf einen Bereich beschränken. Je nach Wirkungsbereich der RM wurden die Parameter unter dem Einfluss der RM ermittelt. Es ergeben sich je Funktion, für die RM abgeleitet wurden, die Parameterwerte H_{RM}, G_{RM} und S_{RM}. Diese ermittelten Werte werden in Beziehung zu den Werten gesetzt, die ohne RM ermittelt wurden: H, G und S.

Anhand der folgenden Formel leitet sich der Eingangswert ΔRM für Tabelle 2 ab:

$$\Delta RM = (H\text{-}H_{RM}) + (G - G_{RM}) + (S - S_{RM})$$

3.9 Wirtschaftlichkeitsanalyse

Der Grundsatz bei PSM-RPZ besteht darin, dass alle Sicherheitsmängel behoben werden müssen. Dafür gibt es gute Gründe. Bei komplexen Systemen könnten z. B. nicht behobene Fehler zusammen mit anderen Fehlern zu neuen Ursachenkombinationen und damit zu neuen gefährlichen Szenarien führen.

Es gibt erfahrungsgemäß Fälle, die zwar mit PSM-RPZ behandelt werden können, bei denen die formale Behandlung der PSM aber an Grenzen stößt:

1. Fehler, deren Ursache innerhalb der Fehlerbehebungszeit nicht gefunden werden
2. Fehler, deren Behebungskosten in einem groben Missverhältnis zum Restrisiko stehen

Insbesondere wenn die aus dem PSM resultierende Risikoerhöhung sehr gering ist, könnte eine Außerbetriebnahme oder ein Austauschen der betroffenen Komponenten (z. B. im Fall 1) oder eine Fehlerbehebung dem „vernünftigen Ermessen“ widersprechen, das z. B. auch in der EU-Sicherheitsdirektive gefordert wird. Unter Umständen wird die Wettbewerbsfähigkeit der Eisenbahn beeinträchtigt.

Bei Fehlerauswertungen im Rahmen von Zuverlässigkeitsbetrachtungen wird für komplexe Systeme ein hoher Anteil von Fehlern klassifiziert als „No-Failure-Found“ (NFF). Zwar kann man unterstellen, dass bei Sicherheitsbetrachtungen ein erheblich höherer Aufwand bei der Fehlersuche betrieben wird. Doch auch hier kann nicht ausgeschlossen werden, dass in Einzelfällen Fehlerursachen nicht gefunden werden können. Der letztere Fall betrifft insbesondere transiente oder singuläre Phänomene, die auch nach eingehender Untersuchung weder im Feld noch im Labor nachgestellt werden können. Wenn die Kritikalität des PSM gering ist (Fehlerbehebungszeit mindestens 60 Monate nach Tabelle 2) und nach dem Ermessen der Fachleute ein solcher Fall vorliegt, kann eine detaillierte Betrachtung angestoßen werden.

Die Wirtschaftlichkeitsanalyse sollte dem Stand der Technik entsprechen. Notwendige Risikobetrachtungen im Rahmen einer solchen Analyse werden in der Regel nicht mit dem in oben beschriebenen semi-quantitativen Verfahren durchgeführt, sondern mit quantitativen Methoden. Im Rahmen einer solchen Risikoanalyse sollten u. a. auch die Risiken betrachtet werden, die sich durch Änderungen an alten oder obsoleten Techniken für das Gesamtsystem ergeben können.

Wenn die Kosten in einem groben Missverhältnis zum Risiko stehen, darf von den in Tabelle 2 vorgegebenen Behebungszeiträumen abgewichen werden und der Mangel braucht gegebenenfalls nicht behoben werden.

Wenn die Ursache des Mangels nicht gefunden werden kann, sollte zusätzlich ein Fehleranalysebericht erstellt werden, der dem Stand der Technik entspricht. Im Fehleranalysebericht wird explizit dargestellt, welche Schritte zur Fehlerursachenermittlung durchgeführt und mit welchem konkreten Ergebnis diese abgeschlossen wurden. Der Fehleranalysebericht sollte durch ein Gutachten (fachlich und methodisch) bestätigt werden. In diesem Fall kann auf die Fehlerbehebung verzichtet werden.

Wenn es sich bei dem betroffenen System um ein Teilsystem geringer Komplexität (Typ A nach IEC 61508 [7]) handelt, kann nach Erstellung einer Auswirkungsanalyse (für die Nichtbehebung des Fehlers) auf die Fehlerbehebung verzichtet werden.

Die Wirtschaftlichkeitsanalyse sollte durch ein Gutachten bestätigt werden, das insbesondere die Verhältnismäßigkeit der Maßnahmen bewertet.

3.10 Allgemein akzeptable Risiken

Damit Eisenbahnbetreiber zur Analyse und Beherrschung von nicht signifikanten Risiken keinen unangemessen hohen Aufwand betreiben müssen, hat die European Railway Agency (ERA) in der Verordnung zu einer Common Safety Method (CSM) [8] den Begriff der allgemein akzeptablen Risiken eingeführt. Grundsätzlich können demnach Risiken aus Gefährdungen als allgemein akzeptabel eingestuft werden, wenn das Risiko so gering ist, dass die Einführung zusätzlicher Sicherheitsmaßnahmen nicht angemessen wäre. Dieser Begriff kann auch im Rahmen der PSM-Bewertung zur Wirtschaftlichkeitsanalyse verwendet werden.

In einer wirtschaftlichen Interpretation müsste ein Grenzwert festgelegt werden, für den man sich nicht vorstellen kann, zusätzliche Sicherheitsmaßnahmen durchzuführen. Ähnlich wie bei ALARP-Betrachtungen müsste der Nutzen von Sicherheitsmaßnahmen festgelegt werden (z. B. „Willingness to Pay“ oder „Value of Prevented Fatality“). Solche Festlegungen sollen zukünftig von der ERA getroffen werden. Allerdings scheint derzeit eine technische Interpretation des Begriffs effektiver.

Der Begriff kann in direkten Zusammenhang mit dem Risikoakzeptanzkriterium MGS gebracht werden: Wenn das Risiko bzw. die Risikoerhöhung so gering ist, dass sich mit hoher Wahrscheinlichkeit keine Änderung bezüglich der Risikoakzeptanz nach MGS ergibt, kann das Risiko als allgemein akzeptabel eingeschätzt werden.

Man kann also davon ausgehen, dass ein Risiko allgemein akzeptabel ist, wenn es im Vergleich zu einem tolerierten Risiko nur einen kleinen Bruchteil davon ausmacht. Diese Interpretation ist in Einklang mit anderen Vorschlägen aus der Fachwelt – z. B. dem ALARP-Kriterium: Eine Gefährdung darf als allgemein akzeptabel angesehen werden, wenn das mit ihr verbundene Risiko mindestens zwei Größenordnungen geringer ist als das maximal tolerierbare Risiko.

Als allgemein akzeptables Risiko wird danach ein Wert von 1×10^{-11} gefährlicher Ereignisse je Element und Betriebsstunde in einem technischen System angesehen. Begründung:

- Der Wert ist zwei Größenordnungen kleiner als tolerierte Risiken pro Element in heutiger Technik. Beispiel: Schnittstelle für eine Weiche (ohne Weiche selbst) liegt heute bei etwa $10^{-9}\,h^{-1}$.
- Es müssen also für ein Element 100 Fehler auftreten, um in die Größenordnung der stochastisch akzeptierten Fehler zu kommen.
- Der in ERA CSM festgelegte Risikoakzeptanz-Wert liegt bei $1 \times 10^{-9}\,h^{-1}$ pro Funktion.

4 Zusammenfassung und Ausblick

Das in diesem Beitrag vorgestellte Verfahren PSM-RPZ stellt die Entscheidungsfindung bei PSM auf eine transparente und nachvollziehbare Grundlage. Durch die konsequente Anwendung kann sichergestellt werden, dass in vergleichbaren Fällen ähnliche Maßnahmen getroffen werden. Dadurch wird erreicht, dass in kritischen Fällen wirksame RM eingeführt werden und eine rasche Fehlerbehebung erfolgt, während in weniger kritischen Fällen möglicherweise sogar ganz auf RM verzichtet werden kann oder die Fehlerbehebung bei planmäßig stattfindenden Wartungsarbeiten oder Release-Wechseln erfolgen kann. Damit leistet PSM-RPZ einen wesentlichen

Beitrag sowohl zum Erhalt des hohen Sicherheitsniveaus als auch zur Verbesserung der Wirtschaftlichkeit des Systems Eisenbahn.

PSM-RPZ gehört zu einer Familie von nach ingenieurwissenschaftlichen Prinzipien konstruierten Verfahren zur Risikobeurteilung, deren Konstruktion 2007 von der Deutschen Gesellschaft für Qualität (DGQ) mit dem Walter-Masing-Preis für innovatives Qualitätsmanagement ausgezeichnet wurde. Das Verfahren stellt damit den neuesten Stand der Wissenschaft und Forschung dar. Da es bereits praxisbewährt ist und die Vorgaben der DIN V VDE V 0831-100 erfüllt, kann es als anerkannte Regel der Technik bezeichnet werden.

Danksagung:

Die Autoren möchten sich insbesondere bei den Kollegen aus dem DKE UK 351.3 bedanken, die an der Erstellung der DIN V VDE V 0831-100 beteiligt waren, und bei dem Obmann des Gremiums, Harald Peters, für seine tatkräftige Unterstützung.

Literatur

[1] DIN V VDE V 0831-100: Risikoorientierte Beurteilung von potenziellen Sicherheitsmängeln und risikoreduzierenden Maßnahmen, 2009

[2] DIN EN 50129 Bahnanwendungen - Sicherheitsrelevante elektronische Systeme für Signaltechnik

[3] DIN EN 50128 Bahnanwendungen – Software für Eisenbahnsteuerungs- und überwachungssysteme

[4] Braband, J., Nachweis mindestens gleicher Sicherheit gegenüber Referenzsystemen, Signal+Draht, Heft 12, 2008, 39-43

[5] DIN EN 60812: Analysetechniken für die Funktionsfähigkeit von Systemen –Verfahren für die Fehlzustandsart- und -auswirkungsanalyse (FMEA)

[6] Braband, J.: Risikoanalysen in der Eisenbahn-Automatisierung, Eurailpress, 2005

[7] IEC 61508: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme

[8] EU Kommission: 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