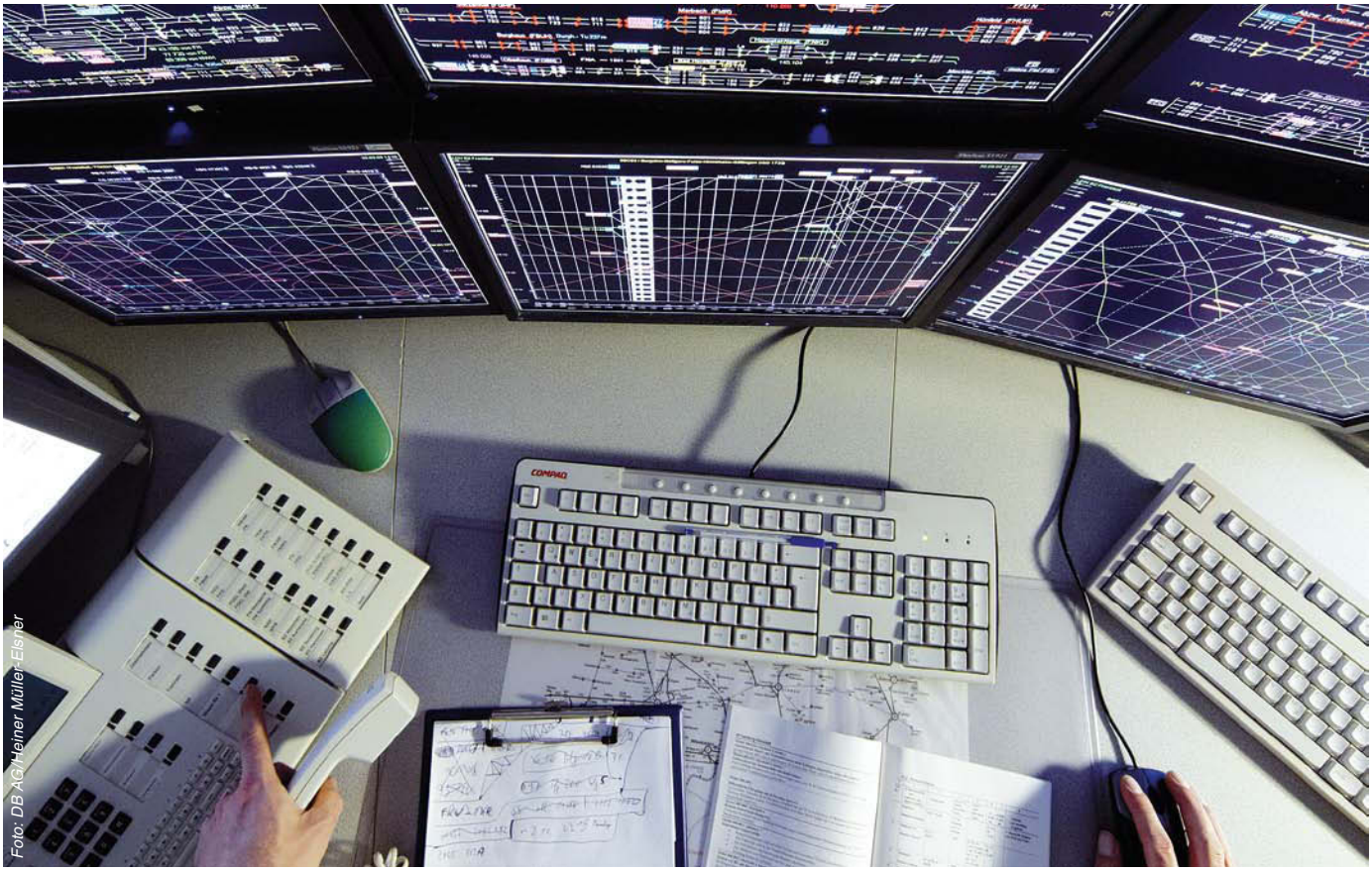
Foto: DB AG/Heiner Müller-Elsner

**Common Safety Methods – Teil 2**

# Grundbegriffe für Sicherheits- und Risikobetrachtungen

**Dr.-Ing. Gunnar Bosse,** Institut für Eisenbahnwesen und Verkehrssicherung der Technischen Universität Braunschweig

In dem in Deine Bahn 12/2013, Seite 18ff veröffentlichten ersten Teil dieses Beitrags wurde zunächst der Begriff „Risiko“ definiert. In diesem zweiten Teil wird intensiver auf den Begriff „Gefährdung“ eingegangen und beschrieben, welche Bedeutung er für die Risiko- und Sicherheitsanalyseprozesse besitzt. Anschließend werden die Unterschiede zu den Begriffen „Unfall“ und „Fehler/Ausfall“ herausgearbeitet. Im Hinblick auf eine systematische Identifikation der Gefährdungen wird der Zusammenhang zwischen „Gefährdung“ und „Funktion“ hergestellt. Die Bezüge des sich daraus bei Risiko- und Sicherheitsbetrachtungen ergebenden Verfahrens zur CSM-Verordnung und des damit verbundenen Vorgehens werden dargestellt.

https://doi.org/10.24355/dbbs.084-202005050941-0

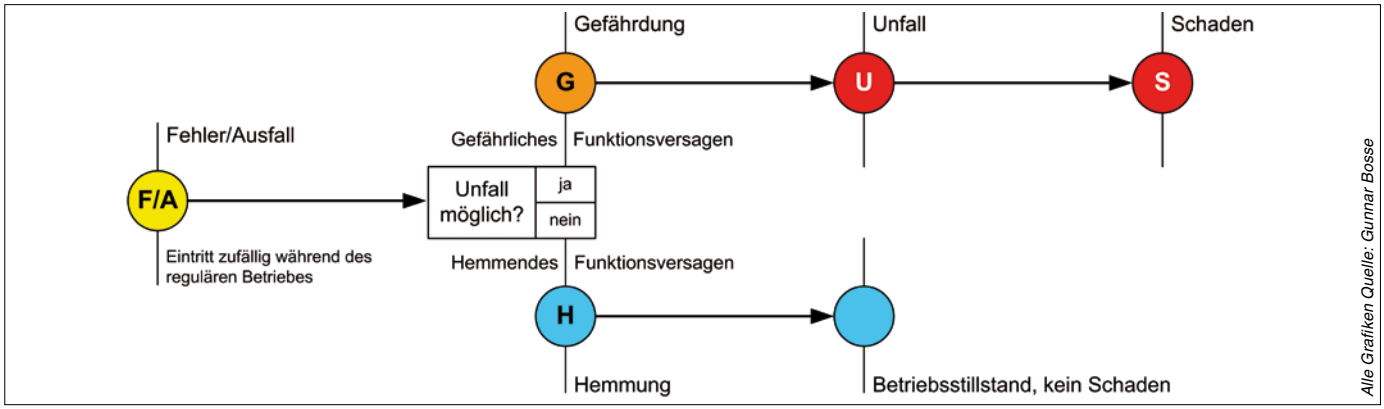


*Abbildung 1: Unterscheidung des Funktionsversagens in Gefährdungen und Hemmungen*

## Gefährdung

Gefährdungen sind betriebliche Situationen, aus denen sich ein Unfall ergeben kann. Gemeint sind aber nicht die Betriebssituationen, die sich im normalen, planmäßigen Betrieb eines Verkehrssystems ergeben, sondern das Eintreten oder Vorhandensein von unplanmäßigen, nicht ordnungsgemäßen Zuständen während des Betriebes. Der bis dahin reguläre Betrieb kann in diesen Fällen in einen gefährlichen Zustand übergehen.

Gefährdungen können entstehen, wenn beim Betrieb eines technischen Systems Ausfälle oder Fehler auftreten bzw. im Betrieb von Menschen Fehlhandlungen begangen werden. Dies führt zum Versagen der beabsichtigen betrieblichen Funktionen. Treten durch diese Versagen Betriebszustände ein, aus den sich Unfälle ergeben können, werden diese als Gefährdungen bezeichnet. Treten dagegen Betriebszustände ein, die als sicher gelten, wird von Hemmungen gesprochen. Der Betrieb kommt dabei so zum Stillstand, dass kein Unfall eintreten kann (Abbildung 1).

Nicht nur in der europäischen Verordnung 352/2009 „über die Festlegung einer gemeinsamen Sicherheitsmethode für die Evaluierung und Bewertung von Risiken“, der CSM-Verordnung[1)] bilden die Gefährdungen den zentralen Dreh- und Angelpunkt bei Sicherheitsbetrachtungen, sondern auch in der noch älteren CENELEC-Norm EN 50129[2)]. (CELENEK ist das europäische Komitee für elektrotechnische Normung). Der Grund für diese herausgehobene Bedeutung der Gefährdungen liegt in ihrer Funktion als „Schnittstelle“ zwischen den sich im Rahmen der Sicherheitsarbeit von Betreibern und Herstellern eines Systems ergebenden Verantwortungsbereichen.

Während der Betreiber eines Systems Anforderungen festlegen muss, wie sicher ein von ihm eingesetztes System im Betrieb funktionieren muss, ist der Hersteller aufgefordert, an dieser Schnittstelle nachzuweisen, dass das von ihm entwickelte, hergestellte und gelieferte System diesen Sicherheitsanforderungen genügt.

Da nur der Betreiber des Systems dessen betriebliche Einsatzbedingungen und die weiteren Randbedingungen kennt, kann auch er nur die Übergangswahrscheinlichkeit zwischen einer Gefährdung und einem Unfall ermitteln sowie das bei einem Unfall zu erwartende Schadensausmaß abschätzen. Den dritten Faktor der Risikoformel, die Gefährdungswahrscheinlichkeit, kann er selbst nicht ermitteln, da diese nur aus den Fehler- und Ausfallraten des Systems und in Abhängigkeit von der Systemarchitektur errechnet werden können. Folglich kann der Betreiber ausgehend von einem einzuhaltenden zulässigen Risikowert nur einen Vorgabewert für die Gefährdungsrate bestimmen, der den Hersteller als Anforderung übergibt.

Der Hersteller eines Systems kann hingegen in unzureichender Kenntnis der betrieblichen Bedingungen weder eine Übergangswahrscheinlichkeit noch ein Schadensausmaß ermitteln. Als „Kenner“ des von ihm entwickelten und hergestellten Systems obliegt ihm aber der Nachweis, dass in dem System hinreichend wenig Fehler oder Ausfälle auftreten, um den Vorgabewert für die Gefährdungswahrscheinlichkeit einzuhalten.

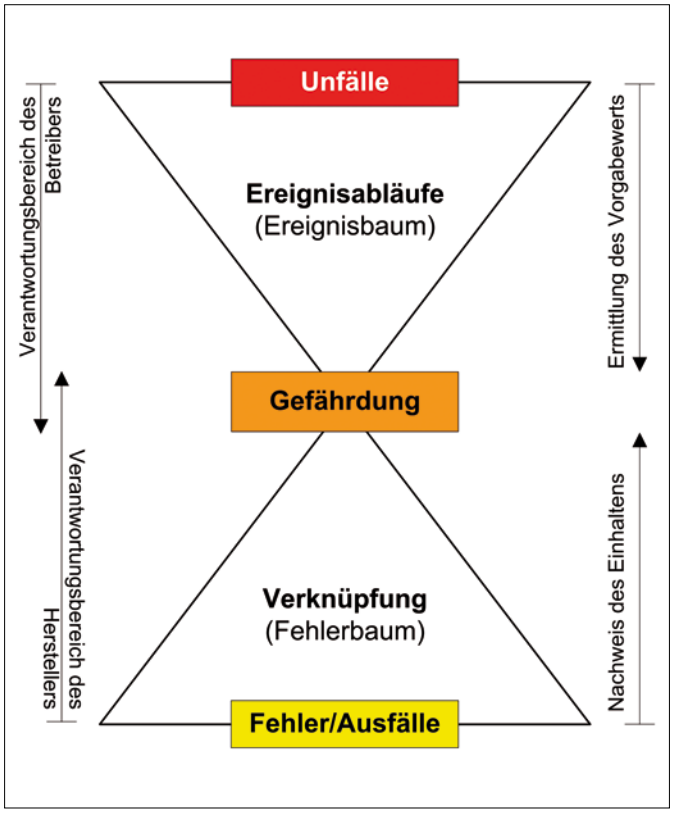


*Abbildung 2: Die Gefährdung als Schnittstelle zwischen Betreiber- und Herstellerverantwortung*


https://doi.org/10.24355/dbbs.084-202005050941-0

| Gefährdung | Unfall | |
|---|---|---|
| hier als gefährlicher Zustand, gefährliche falsche Information | schadenverursachender Vorgang | Schaden |
| Nicht ordnungsgemäß anliegende Weichenzunge | Entgleisung | Fahrwegschäden, Fahrzeugschäden |
| Während der Fahrt geöffnete Waggontür | Sturz einer Person aus dem Fahrzeug | Personenschaden |
| Betrieb eines angerissenen Radsatzes | Bruch des Radsatzes = Entgleisung | Fahrwegschäden, Fahrzeugschäden |
| Information „Gleisabschnitt frei", obwohl belegt | Kollision zweier Fahrzeuge | Fahrzeugschäden, Personenschäden, Fahrwegschäden |

*Abbildung 3: Überprüfung der Abgrenzung zwischen Gefährdungen und Unfällen anhand des schadenverursachenden Vorgangs (Beispiele)*

Die Gefährdung ist somit die „natürliche" Schnittstelle zwischen dem Verantwortungsbereich eines Betreibers und dem eines Herstellers. An ihr werden die Sicherheitsanforderungen vom Betreiber übergeben und ihre Einhaltung vom Hersteller nachgewiesen. Besonders anschaulich kommt dieser Zusammenhang in der so genannten CENELEC-Sanduhr zum Ausdruck (Abbildung 2).

## Abgrenzung

Damit die in der Risikoformel enthaltenen Wahrscheinlichkeiten korrekt ermittelt und berücksichtigt werden können, müssen die Gefährdungen gegenüber den sie auslösenden Fehlern und Ausfällen sowie gegenüber den ihnen möglicherweise folgenden Unfällen abgegrenzt werden. Es sollte daher vermieden werden, dass in den Gefährdungslisten Fehler und Ausfälle oder Unfälle als Gefährdungen definiert werden. Nachfolgend wird erläutert, wie solche Fehler vermieden werden können.

### Abgrenzung Gefährdung – Unfall

Mitunter werden Unfallfolgen als Gefährdungen definiert, weil sie sich anschaulicher beschreiben lassen. Dies ist jedoch problematisch, weil es im Allgemeinen noch eine von den betrieblichen Umständen abhängige Übergangswahrscheinlichkeit gibt, mit der eine Gefährdung in einen Unfall übergeht. Diese würde nicht oder nur unzureichend berücksichtigt werden kann.

Deshalb sollten Gefährdungen möglichst NICHT wie folgt definiert werden:

- „Entgleisung an nicht ordnungsgemäß anliegender Weichenzunge",
- „Sturz einer Person aus geöffneter Waggontür",
- „Bruch eines Radsatzes",
- „Kollision infolge falscher Freimeldung".

So formuliert handelt sich in allen Fällen um Unfallbeschreibungen. Derartige Gefährdungsdefinitionen lassen sich aber recht einfach vermeiden, indem überprüft wird, ob mit der Definition nicht bereits ein Sachverhalt beschrieben wird, der unmittelbar einen Schaden bewirkt. Der Beginn eines Schädigungsvorgangs markiert den Unfallbeginn. Deshalb sollte ein schadenverursachender Vorgang nicht als Gefährdung definiert werden. Nachfolgend wird diese Abgrenzung anhand der vier vorstehenden Beispiele erörtert.

- Eine Entgleisung verursacht unmittelbar Schäden an dem Fahrweg und meist auch am Fahrzeug. Sie ist stets als ein Unfallereignis anzusehen und darf deshalb nicht als Gefährdung definiert werden. Eine nicht ordnungsgemäß anliegende Weichenzunge verursacht hingegen noch keinen unmittelbaren Schaden, sondern sie ist die Ursache für die schadenverursachende Entgleisung. Sie kann deshalb als Gefährdung definiert werden.

- Der Sturz einer Person aus einem fahrenden Eisenbahnfahrzeug führt unmittelbar zur Verletzung derselben. Er ist ein Unfallereignis. Eine während der Fahrt geöffnete Tür ist dagegen noch kein Unfall, denn dieser Zustand schädigt die Person nicht.

- Der Bruch eines Radsatzes ist gleichbedeutend mit einer Entgleisung, weil mit dem Eintritt des Bruchs keine oder keine ordnungsgemäße Spurführung mehr gegeben ist. Ein gebrochener Radsatz gilt somit bereits als entgleist, selbst wenn er noch mehrere Kilometer auf den Schienen weiterrollen würde. Die Fahrt des betroffenen Zuges wird folglich nicht erst durch den Bruch gefährdet, sondern sie ist es bereits durch den Betrieb des angerissenen Radsatzes. Der Anriss selbst verursacht noch keine weiteren Schäden, doch mit dem Eintreten des Bruchs tritt nicht nur eine Entgleisung ein, sondern es werden auch erste Schäden am Fahrzeug und in der Regel auch am Fahrweg hervorgerufen. Deshalb ist der Betrieb des angerissenen Radreifens und nicht der Bruch als Gefährdung zu definieren.

- Mit der Kollision zweier Fahrzeuge beginnt der Schädigungsvorgang. Eine Kollision kann daher nicht als eine Gefährdung definiert werden. Eine falsche Information über den Belegungszustand einer Gleisabschnitts verursacht hingegen noch zu keinem Schaden und kann daher als Gefährdung definiert werden.

Die vier Beispiele zeigen, wie Gefährdungen mittels der Betrachtung des (ersten) schadenverursachenden Vorgangs recht anschaulich gegenüber den ihnen möglicherweise folgenden Unfallereignissen abgegrenzt werden können.

Während zwischen dem Schädigungsvorgang und dem Schaden eine Zwangsläufigkeit besteht, liegt zwischen der Gefährdung und dem Unfall eine Übergangswahrscheinlichkeit. Eine solche Abgrenzung kann gut in tabellarischer Form erfolgen (Abbildung 3).

https://doi.org/10.24355/dbbs.084-202005050941-0

### Abgrenzung Gefährdung – Fehler/Ausfall

Während eine Gefährdung mittels der Betrachtung des Schädigungsbeginns gut gegenüber einem Unfall abgrenzt werden kann, gestaltet sich ihre Abgrenzung zu Fehlern und Ausfällen auf den ersten Blick etwas schwieriger. Warum handelt es sich beispielsweise bei der Gefährdung „der Stellweg einer Weiche wird unvollständig zurückgelegt" nicht um einen Fehler oder einen Ausfall? Um solche und ähnliche Fragestellungen beantworten zu können, soll zunächst geklärt werden, wodurch Fehler und Ausfälle charakterisiert sind.

Umgangssprachlich verbindet man mit dem Begriff „Fehler" Handlungen von Menschen, die zu einem nicht beabsichtigten Ergebnis führen. „Jemand hat einen Fehler begangen" oder der Begriff „Fehlhandlung" drücken dies aus. Sowohl die Benennung als auch die Beschreibung eines Fehlers bzw. die Einstufung einer Handlung als Fehlhandlung beruhen auf Soll-Ist-Vergleichen. Denn nur wenn bekannt ist, was hätte getan werden sollen, kann beurteilt werden, ob abweichend davon ein Fehler begangen worden ist. Fehler werden also an konkreten Handlungen konkret zu benennender Menschen oder Menschengruppen festgemacht.

Ähnlich verhält es sich mit dem Begriff „Ausfall". Damit werden in der Regel konkrete technische Einrichtungen oder Systeme verbunden: „Eine Ampel ist ausgefallen", „Durch den Ausfall eines Triebwerks ..." und „Der Ausfall eines Weichenantriebs ..." seien nur drei Beispiele für eine derartige Verknüpfung. Aber auch die Feststellung, jemand habe einen „Black out" gehabt, zielt in diese Richtung.

In der DIN 40041 wird unter einem Fehler die „Nichterfüllung einer Forderung" verstanden und mit den Begriffen „Planungs-, Realisierungs-, Entwurfs-, Fertigungsfehler" erläutert. Die Verwendung dieser Begriffe deutet auch hier darauf hin, dass der Begriff „Fehler" im Zusammenhang mit konkreten Systemen zu verstehen ist, deren Strukturen und Komponenten bekannt sind.

Der Begriff „Ausfall" wird in der DIN 40041 als die „Beendigung der Funktionsfähigkeit einer materiellen Einheit im Rahmen der zugelassenen Beanspruchung" verstanden. „Materielle Einheit" weist auch in diesem Fall auf ein konkretes System oder eine konkrete Systemkomponente hin.

Fazit: Fehler und Ausfälle werden sowohl umgangssprachlich als auch in der Norm mit konkreten Systemen und Systemkomponenten, die sowohl technischer als auch menschlicher Natur sein können, verbunden. Sie können daher gegenüber Gefährdungen abgegrenzt werden, indem geprüft wird, ob sie konkret benennbaren Systemen oder Systemkomponenten zugeordnet werden können. Die Gefährdungen beschreiben dagegen die aus diesen Fehlern und Ausfällen resultierenden betrieblichen Verhältnisse, die zu einem Unfall führen können. Auch diese Abgrenzung kann in tabellarischer Form systematisch durchgeführt werden (Abbildung 4).

Das heutige Eisenbahnsystem ist allerdings so ausgelegt, dass ein einzelner Fehler oder Ausfall selten zu einer Gefährdung führen kann, sondern weitere Fehler oder Ausfälle hinzukommen müssen, um eine gefährliche betriebliche Situation entstehen zu lassen. Das Vermeiden solcher Situationen und das Einhalten der zulässigen Gefährdungswahrscheinlichkeiten werden durch die entsprechende Gestaltung der Systemarchitekturen, also durch die Anordnung und Verknüpfung der Systemkomponenten erreicht. Doch auch wenn ein einzelner Fehler nicht zu einer Gefährdung führen kann, so sollte im Rahmen von Risiko- und Sicherheitsbetrachtungen stets beachtet werden, dass diesen Fehlern ein Gefährdungspotenzial innewohnt. Sie sollten daher zusammen mit den Fehlern der weiteren Komponenten der entsprechenden Gefährdung zugeordnet werden.

## Gefährdungsbeschreibungen

Gefährdungen können auf verschiedene Arten beschrieben werden. Die Verordnungen machen diesbezüglich keine Vorgaben. In den Abbildungen 3 und 4 wurden sie beispielsweise mittels nicht ordnungsgemäßer Zustände und falscher Informationszustände beschrieben. Es ist aber auch möglich, sie durch das Versagen von Betriebsvorgängen und -prozessen zu beschreiben. Beide Beschreibungsweisen stehen dabei in einem unmittelbaren Zusammenhang, weil Betriebsvorgänge und -prozesse stets der Beibehaltung oder Änderung von Betriebszuständen dienen. Dies schließt auch die Ermittlung und Verarbeitung von Informationen mit ein.

### Als gefährliche Zustände definierte Gefährdungen

Gefährdungen können auf der Basis von nicht ordnungsgemäßen Zuständen oder von Informationen definiert werden, die von den tatsächlich vorhandenen Zuständen abweichen werden. Dazu wieder vier Beispiele:

- Eine nicht ordnungsgemäß anliegende Weichenzunge ist ein Zustand, der mit einer bestimmten Wahrscheinlichkeit zu einer Entgleisung führen kann. Der Betrieb ist folglich gefährdet. Es liegt eine Gefährdung vor, die sich als Zustand formiert als „Nicht ordnungsgemäß anliegende Weichenzunge" definieren lässt.
- Eine während der Fahrt geöffnete Waggontür ist ebenfalls ein gefährlicher Zustand, weil eine Person aus dem Zug stürzen kann. Die Gefährdung lautet entsprechend „Während der Fahrt geöffnete Waggontür".
- Ein angerissener Radsatz, dessen Zustand nicht erkannt wird und der in Betrieb geht, kann während einer Fahrt brechen und entgleisen. Die Gefährdung kann als „angerissener Radsatz in Betrieb" formuliert werden.
- Befindet sich in einem Gleisabschnitt ein Schienenfahrzeug und der Belegungszustand dieses Abschnitts wird – durch welche Form der Gleisfreimeldung auch immer – als „frei" erfasst, kann es aufgrund dieser falschen Zustandsinformation zu einem Unfall kommen. Die Gefährdung ließe sich als „Gleisabschnitt frei gemeldet, obwohl belegt" formulieren.

Als Zustände formulierte Gefährdungen sind konkret genug, um auf ihrer Basis die ihnen möglicherweise folgenden Ereignis- und Unfallabläufe auf einer sehr hohen, abstrakten Ebene zumindest qualitativ beschreiben und sie gegenüber Unfällen abgrenzen zu können.

### An Betriebsprozessen orientierte Definitionen

Gefährdungsdefinitionen in Form gefährlicher Zustände fallen allerdings häufig sehr abstrakt aus und können für sich allein


https://doi.org/10.24355/dbbs.084-202005050941-0

| Fehler/Ausfall | | Gefährdung | Unfall |
|---|---|---|---|
| Konkretes System, Komponente, Person | Fehler, Ausfall, Fehlhandlung | hier als gefährlicher Zustand, gefährliche falsche Information | schadenverursachender Vorgang |
| Inspektionspersonal | prüft das Verschleißmaß nicht | nicht ordnungsgemäß anliegende Weichenzunge | Entgleisung |
| Steuereinheit des Türantriebs | löst selbsttätig das Öffnen der Tür aus | während der Fahrt geöffnete Waggontür | Sturz einer Person aus dem Fahrzeug |
| Diagnosegerät | erfasst den Anriss eines Radsatzes nicht | Betrieb eines angerissenen Radsatzes | Bruch des Radsatzes = Entgleisung |
| Fahrdienstleiter (mech. Stw) | verwechselt bei Inaugenscheinnahme zwei Gleise | Information „Gleisabschnitt frei", obwohl belegt | Kollision zweier Fahrzeuge |

*(Beispiele)*

*Abbildung 4: Überprüfung der Abgrenzung zwischen Gefährdungen und Fehlern und Ausfällen anhand der Betrachtung konkreter Systeme und Komponenten*

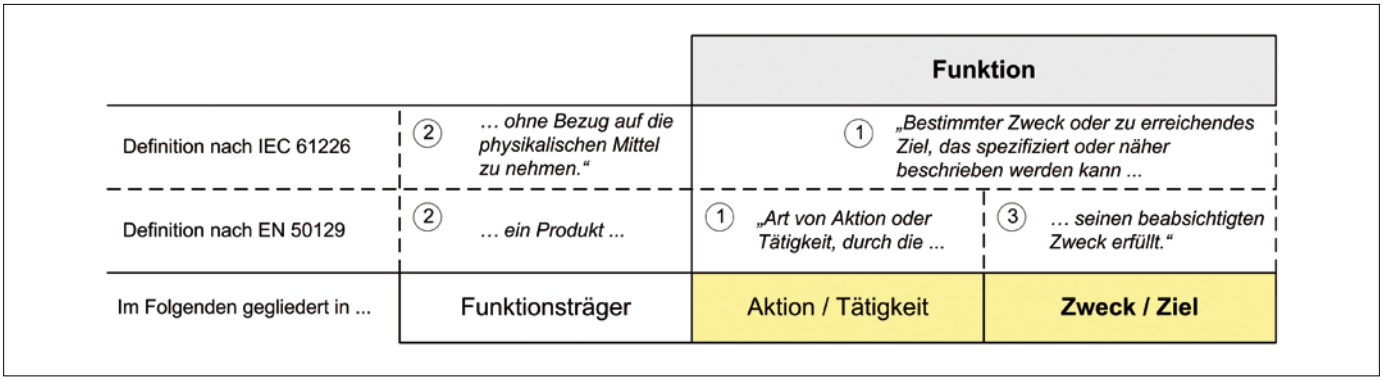


*Abbildung 5: Funktionen können durch den Zweck bzw. das Ziel ohne Bezüge auf ihren Funktionsträger definiert werden*

nur schwer im Rahmen von Risiko- und Sicherheitsanalysen eingesetzt werden. Für eine zielgerichtete Sicherheitsarbeit wird es in der Regel notwendig sein, genauer abzugrenzen, in welchen Situationen und insbesondere bei welchen betrieblichen Abläufen diese als gefährlich erkannten Zustände auftreten können. Nur dann können im Rahmen der Sicherheitsarbeit Maßnahmen festgelegt werden, mit denen das Eintreten der gefährlichen Zustände verhindert werden soll. Dies wird im Folgenden am Beispiel des gefährlichen Zustands „Nicht ordnungsgemäß anliegende Weichenzunge" erläutert.

Betrachtet man zum Beispiel den Prozess des Einstellens eines Fahrweges für eine Zug- oder Rangierfahrt, so besteht die Möglichkeit, dass die Weichenzunge zum Beispiel wegen eines Schottersteins nicht ihre ordnungsgemäße Endlage erreicht. Damit liegt der als gefährlich eingestufte Zustand „Nicht ordnungsgemäß anliegende Weichenzunge" vor.

Betrachtet man dagegen den Prozess einer Weicheninspektion, bei der unter anderem Verschleißmaße aufzunehmen sind, so können Nachlässigkeiten bei der Inspektion den gleichen gefährlichen Zustand nach sich ziehen. Es liegt also auf der Hand, dass die zu ergreifenden Maßnahmen zur Beherrschung der Gefährdung, den jeweils betrachteten Prozessen angepasst, unterschiedlich ausfallen werden. Beispielsweise würde man im Falle eines Schottersteins einer nicht ordnungsgemäß anliegenden Weichenzunge mit anderen Maßnahmen begegnen als im Falle einer nachlässig ausgeführten Inspektion. Während im ersteren Fall Zungenprüfer eine Maßnahme zur Beherrschung der Gefährdung sein können, können im zweiten Fall Schulungen des Personals zweckdienlich sein.

## Ableitung der Gefährdungen

Der vorstehend vorgenommene Vergleich der Arten von Gefährdungsbeschreibungen zeigt deutlich, weshalb es sinnvoll und auch notwendig ist, Gefährdungen auf der Basis von betrieblichen Prozessen als deren „Versagen" zu definieren. Die aus den Versagen resultierenden Zustände sind im Prinzip nur implizite Indikatoren, mit denen das Versagen als „gefährlich" oder „hemmend" beurteilt wird. Neben einer besseren Orientierung auf die zu ergreifenden Maßnahmen bildet ein solches Vorgehen auch die unterschiedlichen Verantwortungsbereiche besser ab. Gefährdungen werden deshalb auf der Basis der Funktionen, die ein System im Rahmen eines betrachteten Betriebsprozesses leisten soll, abgeleitet. Die von dem betrachteten System zu leistenden betrieblichen Funktionen müssen also vorab definiert werden. Die Funktionsdefinition ist ein wesentlicher Bestandteil der umfassenderen Systemdefinition, in der unter anderem auch die betrieblichen Anforderungen sowie Parameter und weitere Bedingungen, unter denen das System eingesetzt werden soll, festgelegt werden. Auf das Thema Systemdefinition wird in einem weiteren Beitrag ausführlich eingegangen. Zunächst soll hier der Begriff „Funktion" bzw. „Betriebliche Funktion" eingeführt werden.

## Betriebliche Funktionen

In dem Abschnitt über die Abgrenzung von Gefährdung gegenüber Fehlern und Ausfällen wurde gezeigt, dass Gefährdungen die Folgen von Fehlern und Ausfällen konkreter Systeme, deren Komponenten oder Personen sind. Folglich müssen auch die Funktionen, aus denen die Gefährdungen abgeleitet werden

https://doi.org/10.24355/dbbs.084-202005050941-0

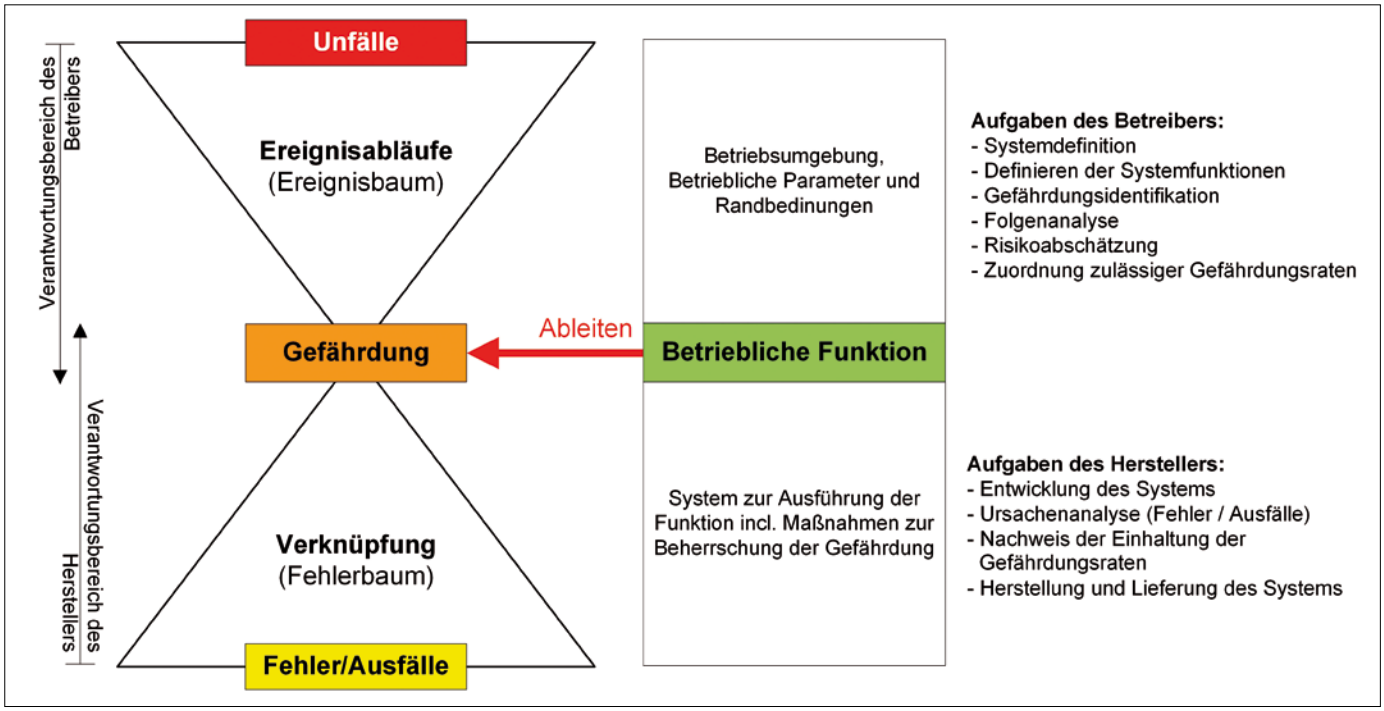


*Abbildung 6: Schnittstelle zwischen der Betreiber- und der Herstellerverantwortung*

sollen, Folgen der Arbeit dieser Systeme, Komponenten oder Personen sein. Sie sind quasi deren Ergebnisse. Aus dem Blickwinkel eines Betreibers betrachtet sind Funktionen die Ergebnisse, die mit einem System im Rahmen eines Betriebsprozesses bezweckt werden. Mit dem Stellen einer Weiche wird beispielsweise das Erreichen einer bestimmten Endlage bezweckt, die für eine bestimmte Zug- oder Rangierfahrt benötigt wird. Ob der Zweck „Erreichen einer bestimmten Endlage" mittels eines elektrischen oder pneumatischen Stellantriebs oder per Handhebel erreicht wird, spielt in der rein funktionalen Betrachtung keine Rolle, sondern wird durch andere Faktoren und Randbedingungen bestimmt. Betriebliche Funktionen können folglich ohne Bezüge auf ihren Funktionsträger definiert werden.

Der Gedanke, Funktionen ohne Bezüge zu ihren Funktionsträgern definieren zu können, ist auch in den einschlägigen Normen enthalten. So wird beispielsweise in der englischsprachigen IEC 61226[3)] Funktion als „bestimmter Zweck oder zu erreichendes Ziel, das spezifiziert oder näher beschrieben werden kann, ohne Bezug auf die physikalischen Mittel zu nehmen" definiert. Und die EN 50129[2)] definiert Funktion als „Art von Aktion oder Tätigkeit, durch die ein Produkt seinen beabsichtigten Zweck erfüllt". Beide Definitionen sind die Bezüge zu dem Zweck bzw. zu dem Ziel, der bzw. das mit einer Funktion erreicht werden soll (Abbildung 5).

Das Definieren von Funktionen, ohne konkret Bezug auf den Funktionsträger zu nehmen, deckt sich wiederum mit der in der Abbildung 2 dargestellten Schnittstelle zwischen den Verantwortungsbereichen von Betreibern und Herstellern. So wie der Betreiber dort auf der Ebene der Gefährdungen lediglich Vorgaben für die einzuhaltenden Gefährdungswahrscheinlichkeiten macht, nicht aber selbst deren Einhaltung nachweisen kann, so kann er auf dieser Ebene oft auch keine konkreten Vorgaben für die Realisierung des späteren Funktionsträgers machen. Dessen Entwicklung und Auslegung obliegt dem Hersteller, der neben dem Nachweis des Einhaltens der vorgegebenen Gefährdungswahrscheinlichkeiten auch zu zeigen hat, dass das System die betrieblich-funktionalen Anforderungen erfüllt.

## Ausblick

In diesem Beitrag wurden die Begriffe „Gefährdung" und „Betriebliche Funktion" als zentrale Elemente von Risiko- und Sicherheitsbetrachtungen herausgearbeitet. Ihre Bedeutung ist ihrer Lage an der Schnittstelle zwischen der Betreiber- und der Herstellerverantwortung geschuldet (Abbildung 6). Dies gilt sowohl für das Entwickeln komplett neuer System als auch für Änderungen am Eisenbahn im Sinne der EU-Verordnung 352/2009[1)]. In all diesen Anwendungsfällen sind die betrieblichen Funktionen zu definieren und die zugehörigen Gefährdungen zu identifizieren. Wesentliche Voraussetzungen für ein möglichst umfassendes und vollständiges Erfassen und Berücksichtigen aller relevanten Funktionen und Gefährdungen sind die Qualität der Systemdefinition und der Gefährdungsidentifikation. Auf diese beiden Punkte wird in einem weiteren Beitrag eingegangen werden. ■

**Quellen**

1) Europäische Gemeinschaft. Verordnung (EG) Nr. 352/2009 der Kommission vom 24.04.2009 über die Festlegung einer gemeinsamen Sicherheitsmethode für die Evaluierung und Bewertung von Risiken
2) EN 50129 Bahnanwendungen: Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Sicherheitsrelevante elektronische Systeme für Signaltechnik. Beuth Verlag GmbH, Berlin Oktober 2003
3) IEC 61226 Nuclear power plants – Instrumentation and control systems important to safety -Classification of instrumentation and control functions, International Electrotechnical Commission, 2005


https://doi.org/10.24355/dbbs.084-202005050941-0