Kapitel 2

Funktionssicherheitsanalyse

Begriff

Während der Erstellung und des Einsatzes eines Produktes können Fehler entstehen. Es können zum Beispiel während der Erstellung Softwarekomponenten falsch implementiert oder falsch spezifiziert werden. Im Einsatz können Datenkabel brechen oder Daten durch elektromagnetische Störungen verfälscht werden. Diese Fehler können unter Umständen gravierende Folgen wie z.B. Unfälle mit Personenschaden haben, wenn sie beim Einsatz des Produktes auftreten. Selbst geringere Folgen können noch einen negativen Einfluss auf den Umsatz und Gewinn eines Unternehmens haben ([Voe02], S. 2, Absatz 2). Zur Vermeidung von Fehlern ist deshalb die Analyse hinsichtlich der potentiellen Fehler eines Produktes eine wesentliche Aufgabe der Entwicklung ([Jon00]).[1] Eine Aktivität ist hierbei die *Funktionssicherheitsanalyse*.[2] Sie befasst sich mit den potentiellen Fehlern, die ein Produkt direkt nach seiner Fertigstellung haben kann oder die beim Einsatz eines Produktes entstehen können. Die in dieser Arbeit betrachteten Funktionssicherheitsanalysen sind in Bezug auf die Einsatzzeit der Produkte statisch, also die Analysen sind nach Fertigstellung des Produktes abgeschlossen und die Ergebnisse ändern sich während des Einsatzes nicht mehr.

Zweck

Die Ergebnisse der Funktionssicherheitsanalyse werden in Dokumenten festgehalten. Diese Ergebnisse unterstützen drei Aufgaben, die bei der Entwicklung sicherheitsrelevanter Produkte durchzuführen sind. Die Aufgaben und der spezifische Beitrag der Analyse sind folgende (siehe [Lev95], S. 289; [MK05], S. 282):

- *Entwicklung*: Die Betrachtung potentieller Fehler eines Systems, um diese oder deren Folgen zu eliminieren oder zu kontrollieren.
- *Operationelles Management*: Die Betrachtung potentieller Fehler eines Systems, in Hinblick auf eine Verbesserung der Richtlinien, der Formulierung

[1] Die Betrachtung von zwei Projekten im Automobil-Bereich hat gezeigt, dass der Aufwand für Funktionssicherheit mindestens ein Viertel der Entwicklungszeit in Anspruch nimmt.

[2] Der mehrdeutige Begriff Sicherheit wird in dieser Arbeit nicht als Angriffssicherheit (engl. Security) verstanden, sondern als Funktionssicherheit (engl. Safety).

Produkt *(Konstruktion)*	**Prozess** *(Nutzung)*	**Produktion** *(Fertigung)*
- Hardware	- Wartung	- Aufstellung
· Elektrik	· Konfiguration	- Chemie
· Mechanik	· Dokumentation	- Bearbeitung
· Schnittstellen	· Training	- Training
- Software	- Anwendung	
· SW-Funktionen	· Betriebsmodi	
· Hardwareschnittstellen	· Training	
- Funktionen	· Dokumentation	
· System	· Überlastung	
· Subsystem	· Nutzungsschnittstelle	

Tabelle 2.1: Unterteilung der Betrachtung eines Produktes (siehe [Eri05], S. 242)

von Sicherheitsvorschriften bzw. -hinweisen und der Steigerung der Motivation hinsichtlich der Effizienz und Zuverlässigkeit der Tätigkeiten beim Umgang mit dem Produkt

- *Zertifizierung*: Das Aufzeigen bzw der Nachweis der Funktionssicherheit eines Systems zur Akzeptanz der Öffentlichkeit oder anderen Institutionen.

Produktorientierung

Funktionssicherheitsanalysen können in drei sich ergänzende Kategorien unterteilt werden, die in Tabelle 2.1 aufgeführt sind (siehe [Eri05], S. 242). Die mit dem Präfix *Produkt* gekennzeichnete Kategorie befasst sich mit dem Aufbau des Produktes, also der Architektur und der Gestaltung der Implementierung. Sie betrachtet in einer White-Box-Sicht, welche Fehler in Produktteilen entstehen können und wie diese Fehler die Funktionalität des Produktes und somit die Umwelt beeinflussen können. Die Kategorie *Prozess* befasst sich mit den Aspekten der Nutzung und Wartung des Produktes. Das Produkt wird hierbei als eine Black-Box betrachtet, dessen Nutzungsschnittstelle im Vordergrund steht. Die Kategorie *Produktion* betrachtet Fehler der Maschinen, der Mitarbeiter und des Produktionsprozesses selbst.

✍ Diese Arbeit fokussiert sich auf die Produkt-Funktionssicherheitsanalyse. Im weiteren Verlauf des Kapitels wird deshalb der Begriff *Sicherheitsanalyse* als Synonym des Begriffs Produkt-Funktionssicherheitsanalyse verwendet. Dies heißt insbesondere, dass die Fehler, die sich auf die Nutzung und die Fertigung beziehen, nur dann betrachtet werden, wenn es zur Bewertung eines Fehlers notwendig ist.

Kapitelübersicht

Dieses Kapitel beschreibt Grundlagen der Sicherheitsanalyse sowie zwei der in der Industrie angewandten Verfahren. Abschnitt 2.1 definiert allgemein die grundlegenden Begriffe, die bei einer Sicherheitsanalyse auftreten. Dabei werden die Begriffe *Fehler* und *Funktionssicherheit* definiert. Abschnitt 2.2 beschreibt die Zusammenhänge der Sicherheitsanalysen mit dem Entwicklungsprozess. Schließlich stellen die Abschnitte 2.3 und 2.4 die Methoden *Fehler-Möglichkeit- und Einfluss-Analyse* und *Fehlerbau-*

manalyse vor, wie sie momentan in der Industrie Anwendung finden und in der Literatur beschrieben werden.

2.1 Definitionen (Terminologie)

Die Begriffe, die in dem Feld der Sicherheitsanalyse vorkommen, werden in diesem Abschnitt allgemein definiert. Im weiteren Verlauf der Arbeit (Kapitel 4) folgen formale Definitionen, die auf spezifische Sichten und Methoden hin spezialisiert sind. Die Definitionen der Begriffe zum Thema Sicherheitsanalyse sind nicht einheitlich (siehe [Lev95], [Eri05], [Bre01], [Ech90], [Thu04], [DIN04]). Ziel dieses Abschnitts ist die Hinführung zur Begriffswelt der Sicherheitsanalyse und die Erklärung, wie die Begriffe in dieser Arbeit verstanden werden. Im Wesentlichen orientieren sich die Definitionen an der IEC 61508 ([DIN04]). In Abschnitt 2.1.1 wird der Fehlerbegriff (Fehler, Versagen, Abweichung) definiert. Abschnitt 2.1.2 widmet sich dem Zusammenspiel von Fehlern als Kombination und in einer Ursache-Wirkungs-Beziehung. Abschnitt 2.1.3 definiert Begriffe zur Bewertung der Fehlerwirkung (Vorfall, Gefahr, Risiko) und definiert schließlich die Funktionssicherheit, welche für ein System bei der Sicherheitsanalyse geprüft wird.

2.1.1 Fehler

Fehler

Der grundlegende Begriff für eine Sicherheitsanalyse ist der des Fehlers. Auf dessen Definition wird die weitere Begriffswelt aufgebaut. Die Betrachtung des Fehlerbegriffs kann sowohl aus der Ereignis-Sicht wie aus der Zustands-Sicht erfolgen. Die Definition wird aus drei Teilen aufgebaut, welche separat definiert werden.[3]

Definition 2.1.1 (Fehler)
Ein *Fehler* ist ein Versagen (Def. 2.1.2), eine Abweichung (Def. 2.1.3) oder ein Fehlzustand (Def. 2.1.4). ⌟

Versagen

Ereignisse und deren kausale Zusammenhänge beschreiben den dynamischen Anteil eines Systems ([BS01]; [Lev95]; [Bal01]). In einem System treten Ereignisse auf, die Folgeereignisse implizieren. Das Soll-Verhalten einer Komponente ist dadurch definiert, dass sie auf eintretende Ereignisfolgen unter bestimmten Rahmenbedingungen entsprechende Ereignisfolgen liefert. Ein Versagen ist eine Abweichung vom Soll-Verhalten:

[3] In der Literatur findet man alternativ auch eine Auftrennung des Begriffs Fehler in falsches menschliches Handeln und Fehler von Maschinen ([Mus99],S.85). Fehler von Maschinen werden in nach Außen hin wahrnehmbare Fehler und in Defekte, die eine Ursache für die wahrnehmbaren Fehler sind, eingeteilt ([Mus99], S.41).

Definition 2.1.2 (Versagen)
Ein *Versagen* ist ein beobachtbares Verhalten eines Systems, welches nicht das spezifizierte Soll-Verhalten erfüllt.[4] ⌟

Beobachtbarkeit

Ein Versagen zeichnet sich dadurch aus, dass sich die Menge der Ereignisse und der kausalen Zusammenhänge des Soll-Verhaltens geändert hat. Es können nicht mehr nur die geplanten Ereignisabläufe im System ablaufen, sondern auch Abläufe stattfinden, in denen Fehlerereignisse vorkommen. Beobachtet man ein Versagen, so ist dieses daran zu erkennen, dass die Ausgaben eines Systems von den Soll-Ausgaben abweichen. Bezogen auf die Eingaben und Ausgaben eines Systems ist ein Fehler eine Abweichung:

Definition 2.1.3 (Abweichung)
Eine *Abweichung* ist eine Nichtübereinstimmung der Eingaben bzw. Ausgaben eines Systems mit den spezifizierten Soll-Eingaben bzw. Soll-Ausgaben.[5] ⌟

Die Definition einer Abweichung wird am Beispiel eines Steuergerätes einer Fahrwerks-Regelung verdeutlicht:

Beispiel 2.1.1 (Abweichung)
Ein Steuergerät hat unter anderem die Soll-Funktion, bei untersteuern des Fahrzeuges das passende Gegenlenken zu veranlassen (siehe Ausgabe (I)). Die Abweichung in Ausgabe (II) ist eine unerwünschte Abweichung, bei der die falsche Gegenlenkfunktion ausgewählt wird. Dies ist im Soll-Verhalten nicht vorgesehen. Ausgabe (III) ist ein Beispiel für eine Abweichung, welches das Ausbleiben einer Soll-Ausgabe ist. Hier leistet das Steuergerät seine Funktion nicht.

(I) (untersteuern →) Ausgabe: Kommando zum Gegenlenken (Modus Untersteuern)
(II) (untersteuern →) Ausgabe: *Kommando zum Gegenlenken (Modus Übersteuern)*
(III) (untersteuern →) Ausgabe: *(kein Kommando zum Gegenlenken)* ⌟

Zustands-Sicht

In der *Zustands-Sicht* wird das Verhalten eines Systems mit Zuständen und Zustandsübergängen (Transitionen) beschrieben ([Bal01]; [Lev95]). Ein System ist in einem Zustand und geht entsprechend einer ausgewählten Transition in einen anderen Zustand über. Das Soll-Verhalten einer Komponente wird definiert, indem für die Zustände (inklusive der Zustände der Eingabevariablen) die das System haben kann, jeweils nur bestimmte mögliche Folgezustände gegeben sind. Die zustandsorientierte Sicht lässt sich mit der ereignisorientierten Sicht kombinieren, in dem die

[4] [DIN04]: Beendigung der Fähigkeit einer Funktionseinheit, eine geforderte Funktion auszuführen.

[5] [DIN04]: Nichtübereinstimmung zwischen Rechenergebnissen, beobachteten oder gemessenen Werten oder Beschaffenheiten, und den betreffenden wahren, spezifizierten oder theoretisch richtigen Werten oder Beschaffenheiten.

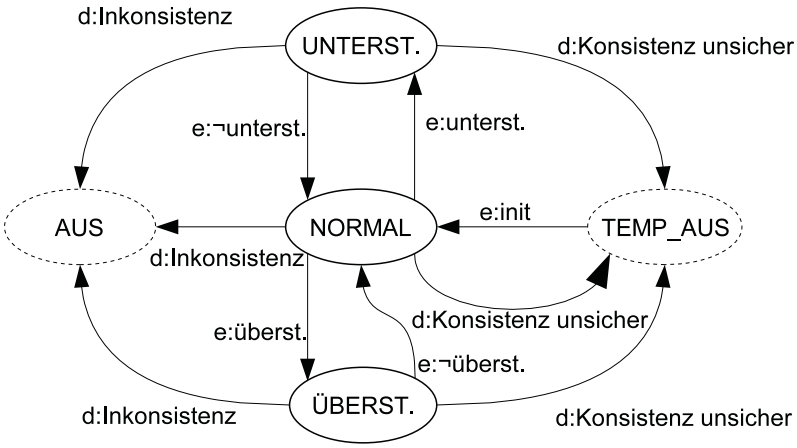

Abb. 2.1: Beispiel eines Automaten mit Fehlerzuständen

Zustandsübergänge mit Ereignissen verbunden werden (siehe [Bro98]). Die zustandsorientierte Sicht konzentriert sich auf den Zustand eines Systems, der ein Versagen eines Systems oder Abweichungen der Eingaben und Ausgaben verursacht. Es gilt folgende Definition:

Definition 2.1.4 (Fehlzustand)
Ein *Fehlzustand* ist ein interner Zustand, der ein Versagen verursachen kann.[6] ⌟

Beispiel 2.1.2 (Fehlzustand)
Abbildung 2.1 veranschaulicht die Definition des Begriffs Fehlzustand anhand des Steuergerätes aus Beispiel 2.1.1. Dieses schaltet abhängig von der Erkennung e der Fahrsituation in den jeweiligen Modus zur Stabilisierung der Fahrsituation. Die Erkennung der Fahrsituation wird von einer Diagnose d überwacht. Erkennt diese Unstimmigkeiten, so schaltet sie das System ab. In diesen Zustand sollte das System aber nie kommen, da die Stabilisierung dann nicht verfügbar ist (Fall III in Bsp. 2.1.1). Dieser unerwünschte Zustand ist ein Fehlzustand. Abhängig von der Diagnose kann er wieder verlassen werden (TEMP_AUS) oder nicht (AUS). Ebenso kann der unerwünschte Zustand eintreten, in dem das System, wie in Fall II in den Zustand Übersteuern geht, obwohl es eigentlich im Zustand Untersteuern sein sollte. ⌟

HW-Ausfall

Die Fehlzustände eines Systems können feiner unterschieden werden, um die Herkunft der Fehler besser zu verstehen und damit auch die Maßnahmen passend ableiten zu können. Eine Gruppe von Fehlern sind die physikalischen technischen Fehler der Hardware eines Systems. Diese treten zur Laufzeit auf und müssen meist mit passenden physikalischen Maßnahmen, wie der physikalischen Architekturgestaltung oder geeigneten Wartungsmaßnahmen vermieden werden.

[6] [DIN04]: nicht normale Bedingung, die eine Verminderung oder den Verlust der Fähigkeit einer Funktionseinheit verursachen kann, eine geforderte Funktion auszuführen.

Definition 2.1.5 (Hardwareausfall)
Ein *Hardwareausfall* ist ein Fehlzustand, der aus physikalischen Mechanismen in der Hardware resultiert und zum Versagen eines Systems führt.[7] ⌟

Erstellung

Die bisher beschriebenen Fehlzustände waren Zustände, die erst während Laufzeit des Systems aufgetreten sind. Als Komplement gibt es eine Menge von Fehlzuständen, die bereits bei der Inbetriebnahme gültig sind. Diese Fehlzustände kommen aus einer fehlerhaften Erstellung des Produktes. Hier handelt es sich also nicht um einen Systemzustand im Sinne einer Variablenbelegung, sondern um eine falsch definierte bzw. implementierte Funktionalität, die im Produkt fest verankert ist. Bei einer Fokussierung auf eine Produkt-Sicherheitsanalyse interessieren nur die Fehler in der Entwicklung des Produktes, die zur Nichterfüllung einer Spezifikation führen.

Definition 2.1.6 (systematischer Ausfall)
Ein *systematischer Ausfall* ist ein Fehlzustand, dessen Ursache im Entwurf oder der Fertigstellung eines Systems liegt.[8] ⌟

Wahrscheinlichkeit

Jeder Fehlzustand hat Zeiten, zu denen er gültig ist (siehe [MK05], S. 289 ff.). Häufig ist es die Aufgabe der Analyse, eine Vorhersage zu treffen, wie wahrscheinlich es ist, dass ein Fehler in einem Betrachtungszeitraum gültig ist. Der Betrachtungszeitraum kann je nach Bedarf spezifisch definiert sein. Es kann z.B. die absolute Zeit ab Entstehung des Produktes sein, aber auch die Ausführungszeit ([Mus99]). Diese Einschätzung für die Erscheinung eines Fehlers ist ein wesentlicher Faktor bei der Entscheidung entsprechende Sicherheitsmaßnahmen zu ergreifen.

Definition 2.1.7 (Fehlerwahrscheinlichkeit)
Die *Fehlerwahrscheinlichkeit* ist die Wahrscheinlichkeit, dass ein Fehlzustand in einem definierten Zeitraum gültig ist. (siehe [MK05], S. 289) ⌟

2.1.2 Zusammenspiel von Fehlern

Kombination

Bei der Sicherheitsanalyse können auch Kombinationen von Fehlern betrachtet werden. Je nach Ziel der Analyse macht es Sinn, die einzelnen Teilfehler der Kombination zu fokussieren, oder die Kombination als ein Ganzes zu nehmen. Für eine Ermittlung der Wirkung spielt z.B. die Gesamterscheinung des Fehlers eine Rolle, wobei die Teilfehler meist nicht interessant sind. Umgekehrt sind bei der Suche nach Maßnahmen zur Vermeidung einer Kombination die verschiedenen Teilfehler relevant. Es ergibt sich somit aus der Betrachtung heraus die Unterscheidung in Einfach- und Mehrfach-Fehler:

[7] [DIN04]: Ausfall, der zu einem zufälligen Zeitpunkt auftritt und der aus einem oder mehreren möglichen Mechanismen in der Hardware resultiert, die zu einer Verschlechterung der Bauteile führen.

[8] [DIN04]: Ausfall, bei dem eindeutig auf eine Ursache geschlossen werden kann, die nur durch eine Modifikation des Entwurfs oder des Fertigungsprozesses, der Art und Weise des Betreibens, der Bedienungsanleitung oder anderer Einflussfaktoren beseitigt werden kann.

Definition 2.1.8 (Einfachfehler)
Ein *Einfachfehler* ist ein Fehler, der als atomarer, nicht aus Teilfehlern kombinierter, Fehler betrachtet wird. ⌟

Definition 2.1.9 (Mehrfachfehler)
Ein *Mehrfachfehler* ist ein aus einer Menge von Einfachfehlern zusammengesetzter Fehler. ⌟

Ursache und Wirkung

Ein wesentlicher Bestandteil der Analyse eines Fehlers ist es, ihn mit anderen Fehlern in Bezug zu bringen. Zum Einen interessiert die Wirkung des Fehlers. Ein Fehler kann einen anderen Fehler zur Folge haben. Zum Anderen kann ein Fehler einen anderen Fehler als Ursache haben. Auf diese Weise lässt sich eine Kette von Fehlern beschreiben, die in einer Ursache-Wirkungs-Beziehung stehen. Diese Kette wird *Ursache-Wirkungs-Kette* genannt. Beschreibt man diese Beziehung als eine Relation, so stehen auf der linken Seite der Tupel die Ursachen und auf der rechten Seite die Folgefehler. Diese Relation kann im Detail verschieden ausgeprägt sein. Formale Beschreibungen der Ausprägungen sind in [Bre01] und [Thu04] zu finden. Eine auf diese Arbeit hin zugeschnittene Beschreibung wird in Kapitel 5 gegeben.

Definition 2.1.10 (Folgefehler (FF))
Ein *Folgefehler* (FF) ist ein Fehler, der unter bestimmten Bedingungen, die in einem System erfüllt sind, unausweichlich als Folge eines anderen Fehlers entsteht. (vgl. [Lev95]) ⌟

Definition 2.1.11 (Fehlerursache (FU))
Eine *Fehlerursache* (FU) ist ein Fehler, der unter bestimmten Bedingungen, die in einem System erfüllt sind, zu einem anderen Fehler geführt hat. (vgl. [Lev95] und [Kre06], S. 16) ⌟

Begrenzung der U-W-Ketten

Die Ursache-Wirkungs-Ketten können theoretisch beliebig lang gesponnen werden. Es ist sinnvoll, die Betrachtung der Ketten an bestimmten Punkten zu beenden. In Richtung der Wirkung werden die Ketten meist an einer gegebenen Systemgrenze oder bei besonderen Folgeereignissen wie einem Unfall (siehe Abschnitt 2.1.3) beendet. In Richtung der Ursachen werden die Ketten mit primären Fehlern beendet. Die Ursachen dieser primären Fehler werden nicht in der aktuellen Analyse betrachtet, sondern in anderen ergänzenden Analysen, wie der Nutzungsanalyse, der Entwickungsprozessanalyse und der Fertigungsanalyse. Bei der Analyse der Kette werden die Wahrscheinlichkeiten für die primären Fehler statistisch erhoben, wohingegen die Wahrscheinlichkeiten der Folgefehler aus denen der primären Fehler ermittelt werden können.

Definition 2.1.12 (Primärfehler (PF))
Ein *Primärfehler* (PF) ist ein Fehler, für den im gegebenen Betrachtungsraum keine Fehler als Ursache gegeben sind. (vgl. [Kre06], S. 18) ⌟

U-W-Ketten Die Ursache-Wirkungs-Ketten, können in zwei Richtungen aufgespannt werden. Die Wirkung kann erstens entlang der Systemhierarchie zur jeweils umgebenden Komponente verfolgt werden. Zweitens kann die Wirkung auf der gleichen Ebene der Systemhierarchie weiterverfolgt werden. Die in dieser Arbeit betrachteten Ketten sind folgende:

$$\text{Hardwareausfall} \xrightarrow{\textit{ist ein}} \text{Fehlzustand} \xrightarrow{PF \quad FF} \underset{\textit{Ebene i}}{\text{Versagen}} \xrightarrow{FU \quad FF} \underset{\textit{Ebene i-1}}{\text{Versagen}} \xrightarrow{FU \quad FF} \ldots$$

$$\text{systematischer Ausfall} \xrightarrow{\textit{ist ein}} \text{Fehlzustand} \xrightarrow{PF \quad FF} \underset{\textit{Ebene i}}{\text{Versagen}} \xrightarrow{FU \quad FF} \underset{\textit{Ebene i-1}}{\text{Versagen}} \xrightarrow{FU \quad FF}$$

$$\ldots$$

$$\underset{\textit{Ebene i}}{\text{Versagen}} \xrightarrow{PF \quad FF} \underset{\textit{Ebene i}}{\text{Abweichung}} \xrightarrow{FU \quad FF} \underset{\textit{Ebene i}}{\text{Abweichung}} \xrightarrow{FU \quad FF} \underset{\textit{Ebene i}}{\text{Abweichung}} \xrightarrow{FU \quad FF} \ldots$$

Fehlerklasse Für allgemeinere Aussagen, können Fehler in *Fehlerklassen* zusammengefasst werden. Eine Klasse ist hierbei über die gemeinsamen Eigenschaften aller in ihr enthaltenen konkreten Fehler bestimmt. Es kann zum Beispiel eine Klasse "Wert zu groß" alle die Fehler umfassen, bei denen eine Funktion zu große Werte liefert, aber die Latenzzeit verschieden lang ist. Anhand dieser Zusammenfassung ist es z.B. einfacher, die Wahrscheinlichkeit für einen Fehler der Klasse abzuschätzen, statt jeweils die Wahrscheinlichkeiten der konkreten Fehler abzuschätzen.

2.1.3 Bewertung der Fehler

Bewertung Ziel der Sicherheitsanalyse ist die Bewertung der Funktionssicherheit. Auf Basis der Begriffe des vorherigen Abschnitts, die sich auf die Beschreibung der Fehler konzentriert haben, werden nun die Begriffe hinsichtlich der Bewertung der Fehler definiert. Aufbauend auf den Bewertungen von Fehlern mittels Schaden und Risiko wird der Begriff Funktionssicherheit definiert.

Schaden als Folge Die Wirkung eines Fehlers kann in einer Ursache-Wirkungs-Kette angegeben werden. Um die Wirkung bewerten zu können, werden die Ketten bis hin zu speziellen aussagekräftigen Folgen untersucht. Ein aussagekräftiges Maß ist der Schaden. Entsprechend können für die Bewertung Folgen betrachtet werden, die einen Schaden zur Folge haben. Hierbei spricht man von gefährlichen Vorfällen.

Definition 2.1.13 (gefährlicher Vorfall)
Ein *gefährlicher Vorfall* ist ein unerwünschtes Ereignis, das einen Schaden zur Folge hat.[9] ⌟

Schadensbewertung In der obigen Definition ist offen gelassen, wie ein Schaden bewertet wird. Die Angabe der Stärke des Schadens hängt sowohl von dem Betrachter, wie auch von dem Bewertungsaspekt ab. Der Schaden wird in einer Metrik angegeben, die absolut

[9] [DIN04]: Gefährdungssituation, die zu einem Schaden führt.