KAPITEL 5

Probleme mit der Verwendung des Begriffs *Hazard* zur Risikoberechnung

Peter Ladkin

Anhand eines Beispiels zeigen wir, dass die Risikoberechnung mit Hilfe von Hazards, wie es in den Definitionen in Abschnitt 4.2 TODO gemacht wird, nicht zum intuitiv richtigen Ergebnis führt. Letzteres ist in diesem Fall jedoch unabhängig davon berechenbar.

5.1 Fünf Konzepte für Hazards

5.1.1 Auffassungen in System Safety und verwandte Ansichten

Die „System Safety“ Definition: Hazard-1

Als **Hazard-1** definieren wir Levesons Auffassung eines Hazards, wie sie auch in Abschnitt 4.2 TODO (4.2 haben wir nicht mehr!) beschrieben wird: [44]

> Ein **Hazard-1** ist ein Zustand eines Systems der, zusammen mit anderen Bedingungen in der Umgebung dieses Systems, unvermeidlich zu einem Unfall (Verlustereignis) führt.

Die entgegengesetzte Definition: Hazard-2

Wir haben gesehen, dass es sinnvoll sein kann einen Term für gefährliche Umgebungszustände eines Systems einzuführen. Mit diesem Term lassen sich Zustände beschreiben, die ein System eher versucht zu vermeiden (Flugzeuge versuchen beispielsweise Gewitterzonen, Berge oder Regionen mit hohem Verkehrsaufkommen zu vermeiden).

> Ein **Hazard-2** ist ein Zustand der Umgebung eines Systems der, zusammen mit einem bestimmten erreichbaren Zustand oder bestimmten erreichbaren Zuständen dieses Systems, unvermeidlich zu einem Unfall (Verlustereignis) führt.

Die Definition der „erhöhten Wahrscheinlichkeit“: Hazard-3

Einige Safety Ingenieure bevorzugen eine Hazard Definition, die einen Hazardzustand als einen Systemzustand mit einer deutlich erhöhten Wahrscheinlichkeit für einen eintretenden Unfall beschreibt. Demnach definieren wir:

> Ein **Hazard-3**
>
> ist ein Zustand eines Systems, in dem die Wahrscheinlichkeit eines Unfalls höher ist als in vorhergehenden Zuständen.

Die erweiterte System Safety Definition: Hazard-4

Wir haben gesehen, dass es manchmal effektiver ist Hazard-1 zu benutzen, und manchmal effektiver ist Hazard-2 zu benutzen. Daher ist es sinnvoll eine Definition zu haben, die einen Hazard als kombinierten Zustand von System und Umgebung beschreibt. Wir definieren:

> Ein **Hazard-4** ist Zustand eines Systems zusammen mit seiner Umgebung der, zusammen mit anderen Entwicklungen in der Umgebung des Systems, unvermeidlich zu einem Unfall (Verlustereignis) führt.

5.1.2 Die MIL-STD-882 Definition: Hazard-5

Die MIL-STD-882 Definition eines Hazards

Die MIL-STD-882 Definition eines Hazards beschreibt diesen als *eine Gegebenheit die vorausgesetzt ist, damit ein Unglücksfall eintreten kann* (Hierbei kann der „Unglücksfall“ mit dem hier bisher verwendeten „Unfall“ verglichen werden).

Die Zustandseigenschaft ist nicht eingeschränkt

Diese Auffassung eines Hazards unterscheidet sich deutlich von den vorher betrachteten. Zum einen beschreibt „Voraussetzung“ einen Teil eines Zustandes. Zum anderen, ist die Zustandseigenschaft nicht darauf beschränkt

- Teil eines Systemzustandes zu sein (Hazard-1);
- Teil eines Umgebungszustandes zu sein (Hazard-2).

Daher ist es angebracht, all diejenigen Zustandseigenschaften zu betrachten, die *sowohl* Elemente eines Systemzustands, *als auch* eines Umgebungszustandes beinhalten.

Fehlende Berücksichtigung der „Unvermeidbarkeit“

Weiterhin ist die Eigenschaft der Unvermeidbarkeit nicht berücksichtigt. Falls eine Gegebenheit eine Voraussetzung für einen Unfall ist, so ist diese *notwendig* ist damit der Unfall eintreten kann. Tritt ein Unfall unvermeidlich ein sobald diese Gegebenheit erfüllt ist, so ist diese *hinreichend* damit der Unfall eintritt. Die System Safety Definition sieht eine solche Gegebenheit also als notwendig an, die MIL-STD-882 Definition jedoch als hinreichend. Diese beiden Kriterien unterscheiden sich deutlich voneinander!

Letzterer Sachverhalt unterscheidet dieses Konzept von dem des Hazard-4

Das Fehlen des Unvermeidbarkeitskriterium unterscheidet die MIL-STD-882 Definition von der des Hazard-4.

Die Definition

Daher definieren wir:

> Ein **Hazard-5** ist Zustand eines Systems zusammen mit seiner Umgebung in dem die Wahrscheinlichkeit eines Unfalls höher ist als in vorhergehenden Zuständen.

5.2 Definition des Systems S

Die Objekte

Im betrachteten Universum gibt es drei Objekte: x, y und z – wir nennen sie „atomare Objekte“ – und damit auch die Objekte $x \oplus y$, $x \oplus z$, $y \oplus z$ und $x \oplus y \oplus z$.

Ihre Eigenschaften

Ein atomares Objekt kann genau drei Eigenschaften haben, die wir in der üblichen formalen Notation beschreiben und *1*, *2* und *3* nennen. Weiterhin schliessen sich diese Eigenschaften eines atomaren Objektes gegenseitig aus: Wenn *1* für x gültig ist, so können *2* und *3* nicht für x gültig sein. Das gleiche gilt auch für y und z sowie *2* und *3*. Ausserdem ist für jedes Objekt zu jeder Zeit eine dieser Eigenschaften gültig. Um genau zu sein, genau eine. Der Zustand des Universums kann also durch eine Auflistung beschrieben werden, welche Eigenschaften für welche Objekte gültig sind.

Ihre Relationen

Wir nehmen an, dass es weder binäre noch ternäre Relationen gibt, die von Bedeutung sind.

Die Zuweisungen

Die Menge der möglichen „atomaren“ Zuweisungen umfasst daher

1(x), 2(x), 3(x), 1(y), 2(y), 3(y),1(z), 2(z), 3(z).

In jedem Zustand ist genau eine Zuweisung pro Objekt wahr.

Die Zustände

Die Menge der Zustände zusammen mit ihrem Verhalten wird „Universum“ genannt. Möglichen Veränderungen am Universum sind einfach: Jedes Objekt im Zustand *1* kann übergehen in Zustand *2*, und von Zustand *2* in Zustand *3*; weitere Zustandsänderungen sind nicht möglich. Ausserdem nehmen wir an, dass diese Zustandsänderungen schrittweise passieren, d.h. dass keine zwei Zustandsänderungen zur gleichen Zeit eintreten (Diese Annahme dient nur der Bequemlichkeit und vereinfacht die Berechnung, wie im Folgenden gezeigt wird.).

Wahrscheinlichkeiten für Veränderungen

Nehmen wir an, dass jede mögliche Veränderung in jedem Zustand die gleiche Eintrittswahrscheinlichkeit hat. Ausgehend vom Zustand *112*, ist die Eintrittswahrscheinlichkeit der Zustände *212*, *122* und *113* nach einer Veränderung also jeweils 1/3. Ausgehend vom Zustand *213* haben die möglichen Nachfolgezustände *313* und *223* jeweils eine Eintrittswahrscheinlichkeit von 1/2, da z nicht mehr veränderlich ist. Ausserdem nehmen wir an, dass die Übergangswahrscheinlichkeiten nur durch den aktuellen Universumszustand beeinflusst werden: Die Vergangenheit ist irrelevant.

Das System und seine Umgebung

Wir definieren ein **System** S, bestehend aus den Objekten x, y. Objekt z stellt die Umgebung bzw. den Rest des Universums dar. (Dies bedeutet ausserdem, dass, wenn man so will, S auch das Objekt $x+y$ enthält. Weiterhin gibt es *gemischte* Objekte aus System und Umgebung, nämlich $x+z$ und $y+z$. Diese ontologischen Feinheiten brauchen uns hier aber nicht weiter zu beschäftigen, da sich jegliche Eigenschaften dieser Objekte logisch über die Eigenschaften von x, y und z definieren lassen.) Das System ist teleologisch: Der Startzustand ist *(11–)*, also der Systemzustand (*1(x) und 1(y)*), der Zielzustand ist *(13–)*, also die Universumszustände *131*, *132* oder *133*. *123* ist der einzige Verlustzustand. (TODO unity of severity?) Weiterhin nehmen wir an, dass die Wahrscheinlichkeit für den Zustand der Umgebung beim Start von S gleich verteilt ist; *111*, *112* und *113* sind mit einer Wahrscheinlichkeit von jeweils 1/3 gleich wahrscheinliche Universumszustände bei dem Start von S.

Das Verhalten des Systems

Im Folgenden wird die Funktionsweise von *S* beschrieben. Beginnend mit dem Startzustand *(11–)* „läuft“ (d.h. wechselt die Zustände) *S* so lange bis keine weiteren Aktionen mehr möglich sind. Während sich das System verändert, verändert sich auch die Umgebung. Resultiert eine Veränderung im Zustand *123*, so ist dies ein Verlustereignis. *S* ist erfolgreich, wenn es den den Zustand *13–* durchläuft, ohne dass der Zustand *123* eingetreten ist. Es wird sich zeigen, dass das System nicht sehr zuverlässig ist (Die Wahrscheinlichkeit dieses Ziel zu erreichen ist etwa 1/10) und die Wahrscheinlichkeit eines Verlustes eher hoch ist (etwa 1/3).

Das System, so wie das Universum, ist so einfach gehalten wie möglich. Es ist endlich, hat endlich vielen Zustände und zeigt endliches (terminierendes) Verhalten. Wir werden sehen, in wie fern die bisher gegebenen Definitionen für dieses System gültig sind. Sollen diese Definitionen für die Beschreibung komplexer Systeme verwendet werden, so muss die Beschreibung eines einfachen Systems wie *S* mit ihnen möglich sein.

Das Verhalten des Universums, zusammen mit den Wahrscheinlichkeiten, dass ein bestimmter Zustand des Universums eintritt, ist in Abbildung 5.1 gezeigt. Zustände des Universums sind dabei als Kreise dargestellt, Zielzustände des Systems werden durch Ovale beschrieben. Ein größeres Rechteck steht für den Verlustzustand, während die verschiedenen für die Berechnung der Hazards wichtigen Zustände als Rechtecke mit abgerundeten Kanten dargestellt sind. Hier sollte bemerkt werden, dass der Zielzustand *133* nur dann erreicht werden kann, wenn vorher einer der Zustände *132*, welcher selbst ein Zielzustand ist, oder *123*, der definierte Verlustzustand, durchlaufen wurde. Daher können wir *131* und *132* als die entscheidenden Zielzustände sehen. Um *133* zu erreichen muss entweder das Ziel schon erreicht worden, oder der Unfall eingetreten sein. Das betrifft jedoch die Zuverlässigkeit, nicht sie Safety Definitionen.

Startzustände

Der anfängliche Systemzustand ist (11–), die anfänglichen Universumszustände damit *111*, *112* und *113*; jeder mit einer Wahrscheinlichkeit von 1/3.

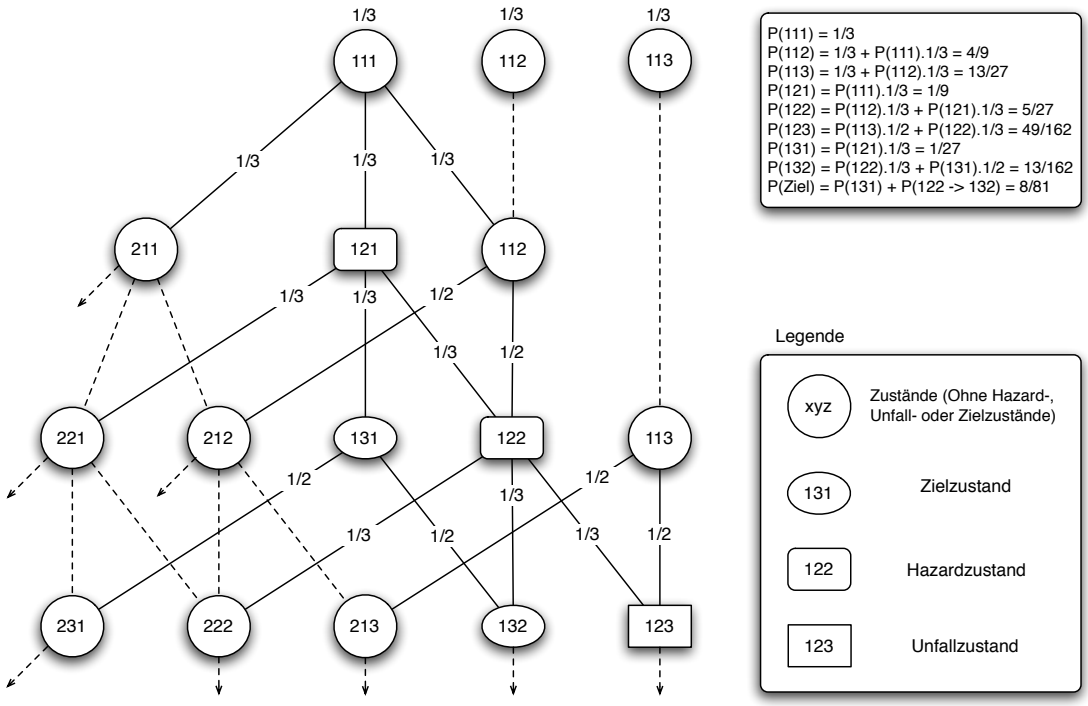

Abbildung 5.1: Das Beispielsystem, Zustands-Aktionsdiagramm mit Wahrscheinlichkeiten, Hazards und Zielen.

Unfälle

Ein Unfall ist definiert als ein Ereignis, das in einem Verlust resultiert. Der Verlustzustand ist 123. Dementsprechend gibt es genau zwei Ereignisse, die einen Unfall zur Folge haben. Das sind die Übergänge von $122 \rightarrow 123$ und von $113 \rightarrow 123$.

5.3 Hazard-4 und Hazard-1 Zustände berechnen

Es wird am einfachsten sein, die Hazardzustände in einer anderen als der eingeführten Reihenfolge zu berechnen.

5.3.1 Hazard-4 Zustände identifizieren

Hazard-4 Zustände sind Zustände des Universums, die einem Unfall unvermeidbar vorausgehen. Die offensichtlichsten Kandidaten sind die Vorgänger der zwei beschriebenen Unfälle 122 $\rightarrow$ 123 und 113 $\rightarrow$ 123, also *122* und *113*. Da *121* ohne Zutun des Systems in *122* resultiert, ist auch dieser Zustand ein Kandidat.

Kandidaten 121 und 122

Der einzig mögliche Ablauf für die Umgebung ist *1(z)* $\rightarrow$ *2(z)* $\rightarrow$ *3(z)*. Daher gilt:

- Wenn sich das Universum im Zustand 121 befindet und das System unverändert bleibt, so wird das Universum zwangsläufig 121 $\rightarrow$ 122 $\rightarrow$ 123 durchlaufen; ein Unfall ist unvermeidbar.
- Wenn sich das Universum im Zustand 122 befindet und das System unverändert bleibt, so wird das Universum zwangsläufig 122 $\rightarrow$ 123 durchlaufen; ein Unfall ist unvermeidbar.

Daher ist sind 121 und 122 Hazard-4 Zustände.

Kandidat 113

Ausgehend vom Zustand 113 ist ein Unfall nicht unvermeidbar, wie im folgenden erläutert wird. Die Umgebung kann sich nicht verändern. Solange sich das System nicht verändert, verbleibt das Universum ewig im Zustand 113, wodurch kein Unfall eintreten wird. 113 ist also kein Hazard-4 Zustand.

Ist 123 ein Hazard-4 Zustand?

Laut Definition ist ein Unfall ein Ereignis. Diese Unfälle sind 122 $\rightarrow$ 123 und 113 $\rightarrow$ 123. Da der Verlustzustand 123 kein Vorgänger dieser Ereignisse ist, ist 123 kein Hazard-4 Zustand.

Die Hazard-4 Zustände

Aus diesen Erläuterungen geht hervor, dass die Hazard-4 Zustände 121 und 122 sind.

5.3.2 Hazard-1 Zustände identifizieren

Der den Hazard-4 Universumszuständen 121 und 122 entsprechende Systemzustand ist (12–). Die Kandidaten für den ungünstigsten Zustand der Umgebung sind daher *1(z)* und *2(z)*. Beide sind unvermeidbare Vorgänger eines Unfalls, wie in Abschnitt 5.3.1 beschrieben. Es scheint, als gäbe es nicht viel was diese Zustände unterscheidet. Jede Veränderung der Umgebung macht den einen Zustand so schlecht wie den anderen; der eine ist ein unvermeidbare Vorgänger des anderen.

Ist *(11–)* ein Hazard-1 Zustand?

Ein weiterer Unfall ist 113 $\rightarrow$ 123. Es stellt sich daher die Frage, ob auch der Systemzustand *(11–)* ein Hazard-1 Zustand ist. Dies ist nicht der Fall. Der offensichtliche Kandidat für den ungünstigsten Zustand der Umgebung ist *3(z)*. Angenommen das Universum befindet sich im Zustand *113*, dann kann sich die Umgebung nicht mehr weiter verändern. Solange das System unverändert bleibt, tritt kein Unfall ein. Ein Unfall ist also nicht unvermeidbar.

5.3.3 Ein Unfall ohne vorhergehenden Hazard

Es ist möglich, dass ein Unfall eintritt, ohne dass vorher ein Hazardzustand durchlaufen wurde: Der Übergang von *113* zu *123* ist ein Unfall, obwohl *(11–)* kein Hazard-1 Zustand und *113* kein Hazard-4 Zustand ist.

5.4 Berechnen der Wahrscheinlichkeiten

Für die Berechnung der Hazard-3 und Hazard-5 Zustände ist es nötig, einige Wahrscheinlichkeiten zu berechnen.

Angewandte Wahrscheinlichkeitsberechnung

Wie die Startzustände des Systems *(11–)* haben auch die dazugehörigen Startzustände des Universums eine einheitliche Eintrittswahrscheinlichkeit. Da die Zustandsübergänge schrittweise ablaufen, lässt sich die Wahrscheinlichkeit eines bestimmten Systemverhaltens durch aufeinander folgende Multiplikation aller Wahrscheinlichkeiten

der einzelnen Zustandsübergänge dieses Verhaltens bestimmen.

Ein Hinweis zur Notation

Ich verwende die Notation *P(xyz)* um die Auftrittswahrscheinlichkeit eines Zustands *xyz* im ‚Verlauf' des Systems zu beschreiben. Da dies folgerichtig ein temporales Ereignis ist (Das System kann also nicht ewig in diesem Zustand verharren, aber auch nur zu bestimmten Zeiten), soll diese Notation nur als eine Abkürzung für *P(◇ xyz)* verstanden werden. *(◇ xyz)* steht hier für *‚eventuell xyz'*, d.h. *in einem zukünftigen Zustand, xyz*. *P(xyz → abc)* beschreibt die Auftrittswahrscheinlichkeit des Ereignisses *(xyz → abc)*, während sich das System im Zustand *xyz* befindet. Diese Standard Notation der bedingten Wahrscheinlichkeit ist tatsächlich nur eine Abkürzung für *P(◇(xyz → abc) / xyz)*. *P(xyz via abc)* drückt die Wahrscheinlichkeit aus, dass das System den Zustand *xyz* erreicht und dabei den Zustand *abc* durchläuft; dies ist eine Abkürzung für *P(◇ xyz and ◇ abc)*. Außerdem verwende ich noch die Notation *P(11a init → abc → ... → fgh)* um die Auftrittswahrscheinlichkeit eines Pfades zu beschreiben, wobei (11z → abc → ... → fgh) ein mit dem Startzustand beginnender Pfad oder einleitender Teilpfad ist. Weiterhin benötigen wir noch die Wahrscheinlichkeit, dass ein Pfad durchlaufen wird *nachdem* der erste Zustand dieses Pfades schon eingetreten ist. Diese wird beschrieben durch *P(abc start → abc → ... → fgh)*. Abschliessend drückt *P(abc|efg)* die bedingte Wahrscheinlichkeit aus, dass *abc* erreicht wird nachdem sich das System schon im Zustand *efg* befindet.

Berechnung der Verlustwahrscheinlichkeit anhand eines Universumszustandes

Im folgenden werden die Wahrscheinlichkeiten berechnet, dass ein Verlustzustand aus bestimmten gegebenen Universumszuständen hervorgeht.

$$
\begin{aligned}
P(123|111) = {} & P(111\textit{start} \rightarrow 121 \rightarrow 122 \rightarrow 123) \\
& + P(111\textit{start} \rightarrow 112 \rightarrow 122 \rightarrow 123) \\
& + P(111\textit{start} \rightarrow 112 \rightarrow 113 \rightarrow 123) \\
= {} & (1/3).(1/3).(1/3) + (1/3).(1/3).(1/3) + (1/3).(1/3).(1/2) \\
= {} & (1/27) + (1/27) + (1/18) \\
= {} & (7/54)
\end{aligned}
$$

$$
P(123|112) = P(112\textit{start} \rightarrow 122 \rightarrow 123)
$$

$$
\begin{aligned}
&+ P(112\textit{start} \rightarrow 113 \rightarrow 123) \\
&= (1/3).(1/3) + (1/3).(1/2) \\
&= (1/9) + (1/6) \\
&= (5/18)
\end{aligned}
$$

$$P(123|113) = (1/2)$$

$$
\begin{aligned}
P(123|121) &= P(121\textit{start} \rightarrow 122 \rightarrow 123) \\
&= (1/3).(1/3) \\
&= (1/9)
\end{aligned}
$$

$$
\begin{aligned}
P(123|122) &= P(122\textit{start} \rightarrow 123) \\
&= (1/3)
\end{aligned}
$$

$$P(123|123) = 1$$

Berechnung der Verlustwahrscheinlichkeit anhand eines Systemzustandes

Es folgen einige Berechnungen die Auskunft darüber geben, mit welcher Wahrscheinlichkeit der Verlustzustand aus verschiedenen Systemzuständen folgt. Da das System im Zustand (11–) startet, gilt:

$P(123\,|\,(11–)) = P(123)$

Außerdem gilt

$P(123\,|\,(13–)) = P(123\,|\,(21–)) = P(123\,|\,(22–)) = P(123\,|\,(23–)) = 0$

da der Verlustzustand aus diesen Systemzuständen unerreichbar ist.

Berechnung von P(123|(12–))

Die Berechnung von $P(123\,|\,(12–))$ ist etwas verzwickt. Dies liegt daran, dass einige Vorkommen des Unfalls $122 \rightarrow 123$ schon in $P(123\,|\,121)$ gezählt werden. Man muss darauf achten, diese Vorkommen nicht mehrfach zu erfassen wenn man von 122 ausgehend die Wahrscheinlichkeit von $122 \rightarrow 123$ bestimmt. Wir beginnen damit festzustellen, dass

- die schon gezählten Vorkommen genau diejenigen sind, die in 111*init* $\rightarrow$ 121 $\rightarrow$ 122 auftreten.
- die noch nicht gezählten Vorkommen den Pfaden 111*init* $\rightarrow$ 112 $\rightarrow$ 122 sowie 112*init* $\rightarrow$ 122 entstammen.

$$P(111\textit{init} \rightarrow 121 \rightarrow 122) = (1/3).(1/3).(1/3) = (1/27)$$

$$P(111\textit{init} \rightarrow 112 \rightarrow 122) = (1/3).(1/3).(1/3) = (1/27)$$

$$P(112\textit{init} \rightarrow 122) = (1/3).(1/3) = (1/9)$$

Daraus folgt:

P(122 *via* 112) = (4/27)
P(122 *via* 121) = (1/27)

Wir haben also einen von fünf Unfällen der Form 122 $\rightarrow$ 123 durch die Betrachtung von *P*(123 | 121) zählen können, die restlichen vier müssen noch betrachtet werden. Es folgt:

$$\begin{aligned} P(123|(12-) &= P(121 \rightarrow 122 \rightarrow 123) + (4/5).P(123|122) \\ &= (1/3).(1/3) + (4/5).(1/3) \\ &= 17/45 \end{aligned}$$

Betrachtung der einfachen Zustandswahrscheinlichkeiten

Wir benötigen die folgenden Zustandswahrscheinlichkeiten:

$$\begin{aligned} P(112) &= P(111 \rightarrow 112) \\ &\quad + P(112\textit{init}\ ) \\ &= (1/3).(1/3) + (1/3) \\ &= (4/9) \end{aligned}$$

$$\begin{aligned} P(113) &= P(111 \rightarrow 112 \rightarrow 113) \\ &\quad + P(112\textit{init}\ \rightarrow 113) \\ &\quad + P(113\textit{init}\ ) \end{aligned}$$

$$
\begin{aligned}
&= (1/3).(1/3).(1/3) + (1/3).(1/3) + (1/3) \\
&= (13/27)
\end{aligned}
$$

$$
\begin{aligned}
P(121) &= P(111 \rightarrow 121) \\
&= (1/3).(1/3) \\
&= (1/9)
\end{aligned}
$$

$$
\begin{aligned}
P(122) &= P(111 \rightarrow 121 \rightarrow 122) \\
&\quad + P(111 \rightarrow 112 \rightarrow 122) \\
&\quad + P(112\mathit{init} \rightarrow 122) \\
&= (1/3).(1/3).(1/3) + (1/3).(1/3).(1/3) + (1/3).(1/3) \\
&= (1/27) + (1/27) + (1/9) \\
&= (5/27)
\end{aligned}
$$

$$
\begin{aligned}
P(123) &= P(111 \rightarrow 121 \rightarrow 122 \rightarrow 123) \\
&\quad + P(111 \rightarrow 112 \rightarrow 122 \rightarrow 123) \\
&\quad + P(111 \rightarrow 112 \rightarrow 113 \rightarrow 123) \\
&\quad + P(112\mathit{init} \rightarrow 122 \rightarrow 123) \\
&= (1/3).(1/3).(1/3).(1/3) + (1/3).(1/3).(1/3).(1/3) \\
&= (1/3).(1/3).(1/3).(1/2) + (1/3).(1/3).(1/2) \\
&= (1/81) + (1/81) + (1/54) + (1/18) \\
&= (8/81)
\end{aligned}
$$

Berechnung der Wahrscheinlichkeiten von Systemzuständen

Weiterhin werden die folgenden Wahrscheinlichkeiten für Zustände des Systems benötigt, von denen ein Unfall erreichbar ist:

$$P((11-)) = 1$$

$$
\begin{aligned}
P((12-)) &= P(111 \rightarrow 121).(P(121|121) + P(121\mathit{start} \rightarrow 122)) \\
&\quad + P(111\mathit{init} \rightarrow 112 \rightarrow 122) \\
&\quad + P(112\mathit{init} \rightarrow 122) \\
&= (1/3).(1/3).(1 + (1/3)) + (1/3).(1/3).(1/3) + (1/3).(1/3) \\
&= (8/27)
\end{aligned}
$$

$P(123|(11-)) = P(123) = (8/81)$
$P(123|(12-)) = (17/45)$
$P(123|111) = (7/54)$
$P(123|112) = (5/18)$
$P(123|113) = (1/2)$
$P(123|121) = (1/9)$
$P(123|122) = (1/3)$
$P(123|123) = 1$
$P((11-)) = 1$
$P((12-)) = (8/27)$
$P(123) = (8/81)$
$P(121) = (1/9)$
$P(122) = (5/27)$
$P(112) = (4/9)$
$P(113) = (13/27)$

Abbildung 5.2: Zusammenfassung der Berechnungen

Es hat wenig Sinn die Wahrscheinlichkeiten anderer Systemzustände zu berechnen. Da ein Unfall von diesen Zuständen nicht eintreten kann, sind sie für uns im Moment nicht interessant.

5.5 Berechnen von Hazard-3 und Hazard-5 Zuständen

Wir sind nun in der Lage, Hazard-3 und Hazard-5 Zustände zu bestimmen. Wie zuvor beginnen wir wieder mit Hazard-5.

5.5.1 Bestimmen der Hazard-5 Zustände

Hazard-5 Zustände sind genau diejenigen Universumszustände, in denen die Wahrscheinlichkeit eines Unfalls höher ist als in vorhergehenden Zuständen. Anhand Abbildung 5.2 können wir die Kandidaten vergleichen.

Kandidat 111

111 ist ein Startzustand. Ein Startzustand hat keine Vorgänger. Daher kann keine sinnvolle Aussage über eine höhere Wahrscheinlichkeit gegenüber vorhergehenden Zuständen getroffen werden. 111 ist kein Hazard-5 Zustand.

Kandidat 112

Der einzige Vorgänger von 112 ist 111. Weiterhin ist 112 auch ein Startzustand und kann daher ohne Vorgänger auftreten. In diesem Fall kann keine sinnvolle Aussage über eine höhere Wahrscheinlichkeit gegenüber vorhergehenden Zuständen getroffen werden. Ansonsten ist $P(123|112) = (5/18) > (7/54) = P(123|111)$. Die Wahrscheinlichkeit eines Unfalls ist höher, und 112 damit ein Hazard-5 Zustand.

Kandidat 113

Der einzige Vorgänger von 113 ist 112. Weiterhin ist 113 auch ein Startzustand und kann daher ohne Vorgänger auftreten. In diesem Fall kann keine sinnvolle Aussage über eine höhere Wahrscheinlichkeit gegenüber vorhergehenden Zuständen getroffen werden. Ansonsten ist $P(123|113) = (1/2) > (5/18) = P(123|112)$. Die Wahrscheinlichkeit eines Unfalls ist höher. 113 ist ein Hazard-5 Zustand.

Kandidat 121

121 hat einen einzigen Vorgänger 111. $P(123|121) = (1/9) < (7/54) = P(123|111)$. Die Wahrscheinlichkeit eines Unfalls ist niedriger. 121 ist kein Hazard-5 Zustand.

Kandidat 122

Die Vorgänger von 122 sind 121 und 112. $P(123|122) = (1/3) > (1/9) = P(123|121)$. Die Wahrscheinlichkeit eines Unfalls ist höher. $P(123|122) = (1/3) > (5/18) = P(123|112)$. Die Wahrscheinlichkeit eines Unfalls ist höher. Die Wahrscheinlichkeit eines Unfalls ist höher ist als in beiden vorhergehenden Zuständen. 122 ist ein Hazard-5 Zustand.

Die Hazard-5 Zustände

Die Hazard-5 Zustände sind 112, 113 und 122.

5.5.2 Bestimmen der Hazard-3 Zustände

Die zwei Kandidaten sind, wie im vorher schon, (11–) und (12–), da der Unfall von anderen Zuständen aus unerreichbar ist.

Kandidat (11–)

(11–) ist der Startzustand. Ein Startzustand hat keine Vorgänger. Daher kann keine sinnvolle Aussage über eine höhere Wahrscheinlichkeit gegenüber vorhergehenden Zuständen getroffen werden.

Kandidat (12–)

(12–) hat einen einzigen Vorgänger (11–). $P(123|(12–)) = (17/45) > (8/81) = P(123|(11\text{-}))$. Die Wahrscheinlichkeit eines Unfalls ist höher. Da die Wahrscheinlichkeit eines Unfalls ist höher ist als in seinem vorhergehenden Zustand, ist (12-) ist ein Hazard-3 Zustand.

Die Hazard-3 Zustände

Wir haben (12–) als Hazard-3 Zustand identifiziert. Dadurch ist die Risikoberechnung in diesem Fall für Hazard-3 und Hazard-1 identisch.

Zusammenfassung

Abbildung 5.3 zeigt die identifizierten Hazardzustände für die unterschiedlichen Auffassung eines Hazards.

Hazard-1 : $(12-)$
Hazard-2* : $(12-)$
Hazard-3 : $(12-)$
Hazard-4 : 121 and 122
Hazard-5 : 112, 113 and 122

* Hier nocheinmal der Hinweis: Das Hazard-2 Beispiel ist das „Spiegelbild“, $S^{\dagger}$, des Systems S.

Abbildung 5.3: Hazardzustände für die Verschiedenen Auffassungen eines Hazards

5.6 Die Berechnung des Risikos anhand von Hazards

Since severity is unity - korrekt so? Da ein Verlust sich auf das ganze System bezieht, ist das zu erwartende Risiko einen Verlust zu erleiden einfach

$$1.P(123) = 1.(8/81) = (8/81)$$

Anhand des Hazards lässt sich Risiko wie folgt berechnen:

$$Risiko = \sum_{\text{Hazardzustände h}} P(h).P(123|h)$$

Wenn diese Berechnungen genau sind, sollten das Ergebnis (8/81) betragen. In der nun folgenden Berechnung werden wir die Notation $Risk_i$ für die Notation *Hazard-i* verwenden. Die dabei verwendeten Zahlen sind in Abbildung 5.2 zusammengefasst. Die verwendeten Hazardzustände werden durch Abbildung 5.3 beschrieben.

$$\begin{aligned} Risk_1 &= \text{P((12-)).P(123 | (12-))} \\ &= (8/27).(17/45) \neq 8/81 \end{aligned}$$

$$\begin{aligned} Risk_3 &= \text{P((12-)).P(123 | (12-))} \\ &= (8/27).(17/45) \neq 8/81 \end{aligned}$$

$$\begin{aligned} Risk_4 &= \text{P(121).P(123 | 121) + P(122).P(123 | 122)} \\ &= (1/9).(1/9) + (5/27).(1/3) \\ &= (6/81) = (2/27) \neq (8/81) \end{aligned}$$

$$\begin{aligned} Risk_5 &= \text{P(112).P(123 | 112) + P(113).P(123 | 113) + P(122).P(123 | 122)} \\ &= (4/9).(5/18) + (13/27).(1/2) + (5/27).(1/3) \end{aligned}$$

$$= (109/162) \neq (8/81)$$

Wir haben gezeigt, dass die Berechnung des Risikos durch die Kombination von Hazardwahrscheinlichkeit mit der Wahrscheinlichkeit eines Verlustes pro Hazard nicht zum passenden Ergebnis kommt, welches die Wahrscheinlichkeit eines Verlustes likelihood of loss simpliciter - wie zu übersetzen?. Die einzige Ausnahme hierbei ist die Berechnung des Hazard-2 – weswegen wir das Beispiel verändern. Wir nehmen das gleiche Beispiel für Hazard-2, vertauschen jedoch das System und seine Umgebung. Das bedeutet, das System ist nun z und seine Umgebung sind x und y. Dieses neue Beispiel nennen wir $S^{\dagger}$. Der Verlustzustand und die entsprechenden Wahrscheinlichkeiten werden ohne Veränderung übernommen. Die Berechnung des Risikos über Hazard-2 für System $S^{\dagger}$ ist identisch mit der Berechnung des Risikos über Hazard-1 für System S, da lediglich System- und Umgebungszustände miteinander vertauscht wurden und umgekehrt.

Zusammenfassung

Für keine der fünf betrachteten Auffassungen eines Hazards lässt sich eine Risikoberechnung anhand von Hazards, wie von Leveson definiert, durchführen [44].

5.7 Das Problem

5.7.1 Ein Risiko: Mehrfaches Erfassen

Die Probleme bei der Berechnung des Risikos der Systeme S und $S^{\dagger}$ anhand von Hazards werden teilweise durch mehrfaches Erfassen der Pfade hervorgerufen. Nämlich:

- Bei der Berechnung von $Risiko_1$ und $Risiko_3$ beinhaltet sowohl $P((12–))$ als auch $P(123\,|\,(12–))$ den Übergang $111init \rightarrow 121 \rightarrow 122$. Diese sind folglich nicht unabhängig.
- Bei der Berechnung von $Risiko_4$ berücksichtigt der Term $P(121).P(123\,|\,(121))$ einige Pfade die auch von $P(122).P(123\,|\,(122))$ berücksichtigt werden – wieder diejenigen, die den Übergang $121 \rightarrow 122$ beinhalten.
- Bei der Berechnung von $Risiko_5$ berücksichtigt der Term $P(112).P(123\,|\,(112))$ einige Pfade die auch von $P(113).P(123\,|\,(113))$ berücksichtigt werden – genau

diejenigen, die den Übergang $112 \rightarrow 113$ beinhalten.

5.7.2 Nicht allen Unfällen geht ein Hazard voraus

Obwohl der Unfall $122 \rightarrow 123$ laut aller angeführten Auffassungen eines Hazards in einem solchen begint, erreicht der Unfall $113 \rightarrow 123$ den Unfallzustand *ohne einen Hazard-1, Hazard-3 oder Hazard-4 Zustand zu passieren*. Aus diesem Grund fehlt das Unfallverhalten $113init \rightarrow 123$ in den Berechnungen dieser Risikobestimmungen. Hazard-5 ist die einzige Auffassung, die 113 als Hazardzustand erkennt. Wie oben erwähnt, leidet Hazard-5 jedoch darunter, Pfade mehrfach zu erfassen.

5.7.3 Zusammenfassung

Anhand zweier Beispielsysteme S und $S^{\dagger}$ und ihrer Umgebungen wurde versucht, eine Verknüpfung von der Wahrscheinlichkeit eines Hazards und der Wahrscheinlichkeit, dass ein Hazard zu einem Unfall (und dem damit einhergehenden Verlust) führt, zu finden. Die Untersuchungen haben gezeigt, dass es keinen sinnvollen Weg gibt eine akkurate Abschätzung des Risikos mittels der verschiedenen Konzepte eines Hazard (Hazard-1 bis Hazard-5) durchzuführen (Risiko kann in diesem Fall verstanden werden als die Wahrscheinlichkeit eines möglichen Verlustes in Kombination mit der Schwere eines solchen Verlustes). Das Konzept der Unfallschwere spielte bei diesen Betrachtungen keine Rolle, da das Problem in dem Versuch begründet ist, die Wahrscheinlichkeiten eines Hazards mit denen zu verbinden, dass ein Unfall aus einem Hazard resultiert. Die Schwierigkeiten wurden dabei teilweise durch das mehrfache Zählen von Pfaden, als auch durch die fehlende Berücksichtigung einiger Unfalltypen in Hazard Konzepten ausgelöst. Letzteres führt zu Systemverhalten, bei dem Unfälle ohne vorhergehende Hazards eintreten können.

5.8 Ein Versuch das Problem zu lösen

Lösung: Hazard-5 und unabhängige Hazards?

Obwohl dieses Beispiel kombinatorisch einfach ist, ist es schwer rein intuitiv etwas über seine Eigenschaften auszusagen. Dieses Beispiel wurde ganz bewusst entworfen um die Risiken zu demonstrieren, die sich sowohl hinter dem mehrfachen als auch

dem fehlenden Erfassen von Unfallpfaden verbergen. Das Risiko hinter dem mehrfachen Erfassen von Pfaden kann möglicherweise minimiert werden wenn sichergestellt wird, dass alle Phänomene die als Hazards gezählt werden unabhängig voneinander sind (Unabhängig im Sinne der Wahrscheinlichkeitstheorie). Mehrfaches Erfassen wird verursacht durch Situationen in denen das Universum den Zustand 121 erreicht, welcher nicht unabhängig davon ist, dass das System den Zustand 122 erreicht. Durch die Unabhängigkeit der Hazardzustände wird jedoch nicht das Problem des fehlenden Erfassens gelöst, welches durch Unfälle entsteht die passieren können ohne vorher einen dazugehörigen Hazardzustand durchlaufen zu haben. Wenn wir uns aber zurückerinnern – Hazard-5 ist in der Lage diese Zustände zu erfassen. Daher scheint eine Kombination von

- Verwendung des Hazard-5, und
- Sicherstellen, dass Hazards unabhängig voneinander sind

sinnvoll wenn es darum geht das Problem der Risikoberechnung mit Hilfe von Hazards zu lösen. An dieser Stelle sei nochmals erwähnt, dass beide Punkte notwendig sind: Die durch 112 und 113 gegebenen Hazard-5 Zustände sind nicht voneinander unabhängig. Die hier vorgestellte Lösung soll jedoch nicht als ultimative Lösung verstanden werden. Vielmehr werden hier einfach verschiedene Aspekte des Phänomens betrachtet.

Modifikationen am Konzept Risiko

Ein anderer Ansatz wäre, die gegebene Definition von Risiko zu verwenden; weiterhin zu schlussfolgern, dass die intuitive Auffassung von Risiko, (in diesem Fall) die Wahrscheinlichkeit eines Verlustes bestimmter Größe (TODO: given unit severity), nicht das am besten passende Konzept von Risiko ist. Dieser Schritt würde jedoch nur aus einem Grund gegen die Intuition sprechen, nämlich einer nicht weiter motivierten Konsistenz. Ausserdem besteht das Problem in einer anderen Form weiter. Die Wahrscheinlichkeit eines Verlustes muss errechnet werden, zum Beispiel um Wettchancen zu bestimmen. Das Problem ist jedoch, dass die vorgestellte Berechnungsmethode das nicht unter allen Umständen leisten kann.

Dem Verlust ausgeliefert

Wenn ich nun glaube, dass mein Risiko dem in der Definition entspricht und auch dementsprechend Wetten abgebe, dann tue ich dies anhand einer Einschätzung die jedoch nicht der tatsächlichen Wahrscheinlichkeit entspricht, dass ein Verlust eintritt. Daher kann ein Buchmacher eine Wettserie entwerfen auf die ich aufgrund meiner Risikoeinschätzung wohl eingehen würde – mit der ich auf lange Sicht jedoch garantiert Geld verlieren würde. Natürlich handelt es sich bei diesem Beispiel nur um eine Art zu verdeutlichen, dass mir eine falsch eingeschätzte Risikowahrscheinlichkeit nicht bei meinen Entscheidungen helfen kann meinen Verlust zu minimieren. Genau das ist es jedoch, was man sich von einer Risikoeinschätzung erhofft.

5.9 Motivationen für das Konzept des Hazard

Hazard-1

Wie wir gesehen haben, wird der Hazard-1 seit einiger Zeit im System Safety Ingenieurwesen in den USA verwendet, und wird aus dem Grund auch von Leveson unterstützt [44]. Das allein sollte für uns Grund genug sein, dieses Konzept zu berücksichtigen. Dennoch sollte man auch die Gründe dahinter sehen. Diese sind dadurch gegeben, dass ein Ingenieur bei einer Sicherheitsabschätzung eines teleologischen Systems zwar Kontrolle über den Zustand des Systems ausüben kann, nicht aber über die Zustände der Umgebung des Systems. Prophylaktische Maßnahmen können generell nur auf Umstände und Zustandskomponenten angewandt werden, die man auch kontrollieren kann. Aus diesem Grund muss die Behandlung von Hazards auf der Ebene von Systemzuständen erfolgen.

Hazard-2: Die Idee des Laien

Wenn ich in meinem Auto unterwegs bin, bin ich vermutlich geneigt einen auf die Strasse rollenden Fussball zusammen mit dem hinterherlaufenden Kind als Hazard zu bezeichnen. Genau so bin ich vermutlich geneigt, ein Schlagloch in der Strasse als Hazard zu betrachten. Beide Situationen sind Eigenschaften der Umgebung in der ich mich bewege, nicht des Autos und auch nicht des Fahrers. Wenn ich also mein Auto samt Fahrer als das System betrachte, dann sind diese „Hazards“ Eigenschaften der

Umgebung.

Wenn ich meine Auto auf übliche Art und Weise fahre, könnten diese Situationen – vielleicht sogar unvermeidlich – zu irgendeiner Art von Unfall führen, abhängig vom Zustand des Systems. Wenn ich beispielsweise nur mit 0,001 km/h unterwegs wäre, würden die Situationen nicht zu einem Unfall führen. Anders sähe es jedoch aus, wenn ich die normalerweise erlaubten 50 km/h fahren würde.

Hazard-1 und Hazard-2 für verschiedene Arten von Systemen?

Wenn man relativ geschlossene Systeme betrachtet, so wie ein Kraftwerk, ein Chemiewerk oder die Elektroverkabelung eines Hauses, ist es sinnvoll Hazards als Zustände des Systems zu verstehen. Es gibt jedoch komplexe Systeme, die zwangsläufig offen sind. Ein Flugzeug wird immer in bestimmten Wetter- oder Umgebungsgegebenheiten betrieben, die Teil seiner Umgebung sind. Es gibt keinen Systemzustand der einem Gewitter, das innerhalb weniger Minuten von Level 2 auf Level 4 umschlägt, entspricht. Daher ist es ratsam, einen solches Gebiet besonders im Auge zu behalten wenn es so kommt. Das ist die Begründung für Hazard-2. In den System Safety Definitionen gibt es kein äquivalentes Konzept zum Hazard-2, da es nicht möglich ist jeglichen Hazard-2 zu einem Hazard-1 zu reduzieren. Es ist jedoch schwer verstehen, wie auf die Verwendung des Hazard-2 in einigen Fällen verzichtet werden könnte.

Vielleicht beide zusammen: Hazard-4

Jegliche Überlegungen und Bestrebungen im Bereich der System Safety haben das Ziel, Kombinationen von Systemzuständen und Umwelteinflüssen zu vermeiden, die zu Unfällen führen. Wenn man all diese Zustände kennt, wie es bei Hazard-4 der Fall ist, lassen sich Hazard-1 und Hazard-2 Zustände von diesen berechnen, wie wir es für System *S* getan haben. Hazard-4 beinhaltet also sowohl mehr Informationen als Hazard-1 als auch Hazard-2. Letztere lassen sich jedoch aus Hazard-4 ableiten.

5.9.1 Abschwächen der Unvermeidbarkeitsforderung

Andere Definitionen eines Hazards halten daran fest, dass Hazards Zustände des Systems sind. Weiterhin geben sie die Forderung nach der Unvermeidbarkeit auf. Dies hat uns zu Hazard-3 und Hazard-5 geführt. Zustände nach einer erhöhten

Wahrscheinlichkeit zu beurteilen ist üblich, wenn es um Zuverlässigkeit geht. Hier wird zwar nicht nach Unfallwahrscheinlichkeit, aber nach Fehlerwahrscheinlichkeit beurteilt. Da Safety oftmals von der Zuverlässigkeit sicherheitskritischer Komponenten abhängt, sind diese miteinander verbunden.

Abgestufte Klassifikation

Ein Beispiel ist die kommerzielle Luftfahrt. Lloyd und Tye zeigen die verschiedenen Wahrscheinlichkeitskategorien wie sie für Zertifizierungsverfahren in der zivilen Luftfahrt in Grossbritannien verwendet werden [49]. Sie beschreiben, dass sowohl die U.S. Federal als auch die European Joint Aviation Regulations (JAR), 25 an der Zahl, Ereignisse in verschiedene Klassen einteilen. So werden Ereignisse als *wahrscheinlich* klassifiziert wenn ihre Eintrittswahrscheinlichkeit zwischen 10^{-5} und 1 liegt, *unwahrscheinlich* wenn ihre Eintrittswahrscheinlichkeit zwischen 10^{-9} und 10^{-5} liegt. Als *extrem unwahrscheinlich* werden Ereignisse mit einer Eintrittswahrscheinlichkeit kleiner als 10^{-9} gewertet. Wahrscheinliche Ereignisse werden in den JAR noch weiter unterteilt in *häufig* (zwischen 10^{-3} und 1) und *einigermaßen häufig* (zwischen 10^{-5} und 10^{-3}), unwahrscheinliche in *selten* (zwischen 10^{-7} und 10^{-5}) und *extrem selten* (zwischen 10^{-9} und 10^{-7}) [49, Tabelle 4-1].

Zweck einer abgestuften Klassifikation

Der Zweck einer solchen Klassifikation ist (war), ein Ereignis als *extrem unwahrscheinlich* einzustufen wenn dies aller Wahrscheinlichkeit nach innerhalb der Lebensdauer einer Flugzeugflotte nicht auftritt; als *extrem selten* wenn es einmal in der Lebensdauer einer Flugzeugflotte auftritt; als *selten* wenn es einmal in der Lebensdauer eines Flugzeuges und mehrere male pro Flottenleben auftritt; als *einigermaßen häufig* wenn es einige male in der Lebensdauer eines Flugzeuges auftritt. Eine Flugzeugflotte, so wurde angenommen, umfasse etwa 200 Flugzeuge, die jeweils etwa 50.000 Flugstunden in ihrer Lebensdauer absolvierten (Heutzutage sind wir eher mit Flottengrößen in der Ordnung von 1.000 bis 2.000 und Flugzeugen die mehr als 50.000 Stunden fliegen konfrontiert; zusammen eine Differenz um Faktor 10.).

Klassifikation von Auswirkungen

Auch die Auswirkungen sind klassifiziert. Die Klassen sind *geringfügig*, *bedeutend*, *gefährlich* und *katastrophal* und beziehen sich auf Schäden, Verletzte und Todesfälle.

Grundlage für die Zertifizierung

Als Grundlage für eine Zertifizierung ist (war) zu demonstrieren, dass *bedeutende*, *gefährliche* und *katastrophale* Auswirkungen dementsprechend höchstens *selten*, *extrem selten* und *extrem unwahrscheinlich* auftreten können.

Verschmelzung von Zuverlässigkeit und Safety

Bei der Grundlage für die Zertifizierung wurde versucht Fehlern Wahrscheinlichkeiten zuzuweisen, wie es eigentlich zur Klassifikation von Zuverlässigkeit gemacht wird. Wir haben jedoch bemerkt, dass Zuverlässigkeit und Safety über die Zuverlässigkeit von safetykritischen Systemen eng miteinander verbunden sind. So muss ein Flugzeug nach dem Ausfall mehrerer Motoren in einem bestimmten Radius um seine aktuelle Position landen, egal ob es dort einen passenden Flughafen gibt oder nicht. Wird ein an Bord ausbrechendes Feuer nicht effektiv genug gelöscht, so wird es sich innerhalb einer bestimmten Zeit ausbreiten und zu einer Katastrophe führen solange sich das Flugzeug zu diesem Zeitpunkt nicht am Boden befindet. Fehler in diversen zielgerichteten mechanischen Systemen, oder ein Totalausfall des Flugkontrollsystems, führen zwangsläufig zu einem Unfall. Dennoch können Zuverlässigkeit und Safety unterschieden werden: Ein Erkennungslicht am Unterboden ist ein safetykritisches Element; eine Leselampe im Passagierraum nicht. Die Zuverlässigkeit von letzterem hat keinen Einfluss auf die Safety.

5.9.2 Vermeidung problematischer Auffassungen

Die IFIP WG 10.4 Definitionen

Eine Reihe von Definitionen in [43] befasst sich mit Verlässlichkeit. Nach Ansicht der Mitglieder der IFIP WG 10.4 beinhaltet diese Safety. Überhaupt erwähnt werden jedoch die Konzepte Hazard und Risiko.

5.9.3 Klassifizierung von Risiko über Statistiken

Ein offensichtlicher Weg dieses Problem zu umgehen besteht wenn man sich in der unglücklichen Lage befindet genügend Unfälle erfahren zu haben um Risiken auf statistischem Wege aus der Vergangenheit errechnen zu können. Wir werden kurz auf eine plausible Möglichkeit eingehen, mit der eben dies erreicht werden kann, nämlich das U.S.A.F. Modell zur Klassifizierung von Unglücksfällen (Mishaps).

U.S. Air Force Unfälle als „Class A Mishaps“

Die von der U.S. Air Force verwendete Kategorie für die schwerwiegendsten Zwischenfälle ist die des *Klasse A* Unglücksfalls (*Class A Mishap*). Ein solcher Zwischenfall resultiert in dem Verlust von Menschenleben oder verursacht Schaden von mindestens $ 1 M. Diese Auffassung ist ähnelt der Definition der U.S. Federal Aviation Regulation, in der ein Unfall als schwere Verletzung oder der Verlust von Leben, oder „bedeutender Schaden“ an einem Flugzeug beschrieben ist („oder“ im inklusiven Sinn).

Diese Definition kann unintuitive Konsequenzen haben

Solche Unfälle haben sich in der Vergangenheit der militärischen Luftfahrt schon zugetragen, obwohl beide Flugzeuge wieder sicher landen konnten und dennoch ein Schaden von mehr als $ 1M entstanden ist [13]. (So zum Beispiel in Fällen in denen beträchtlicher Schaden entstanden ist, dieser aber reperabel ist und niemand getötet wurde.)

Die Unterscheidung zwischen Ereignissen und Ereignistypen

Leicht veränderte Parameter, sagen wir eine geringfügig andere relative Bewegung des Flugzeugs, hätten bei einem glimpflich ausgegangenen Ereignis katastrophale Konsequenzen haben können, wie zum Beispiel der Verlust beider Flugzeuge und Piloten. Aber was bedeutet es zu sagen, dass ein Ereignis andere Konsequenzen *haben können*? Eine mögliche Interpretation dieser Frage ist die Einordnung in eine Zwischenfallklasse, die der *Kollisionen im Flug*. Man kann auch weiter gehen und sagen: *Kollisionen im Flug zwischen zwei Flugzeugen vom Typ X im Formationsflug* oder sogar noch detaillierter: *Kollisionen im Flug zwischen zwei Flugzeugen vom Typ*

X im Formationsflug bei klarem Wetter, während sie Maneuver Y ausgeführt haben. Diese Klassifikationen definieren immer spezifischere und damit kleinere *Klassen* von Ereignissen. Sie sind *Ereignistypen*.

Verwenden der Unterscheidung

Ein individuelles Ereignis wie eine Kollision im Flug mit einem Schaden von $ 1.01M, nachdem aber beide Flugzeuge und Besatzungen sicher landen konnten, kann also entweder

- als ein individuelles Ereignis mit spezifischem Schaden, oder
- als Mitglied eines Ereignistyps, dessen Mitglieder im Schnitt alle katastrophale Unfälle sind

gesehen werden. Die Sichtweise hat maßgeblichen Einfluss darauf, wie mit diesem Ereignis umgegangen wird.

Unterschiedliche Klassifizierungen führen zu unterschiedlichen Vergleichen

Betrachten wir verschiedene Reaktionen auf die verschiedenen Klassifikationen.

1. Angenommen der Unfall wird als individuelles Ereignis mit spezifischem Schaden verstanden. Dann würde man es mit anderen Unfällen vergleichen, beispielsweise den folgenden.
   - Aufgrund von unangepasster Geschwindigkeit verliert ein Servicefahrzeug des Flughafens auf regennasser Fahrbahn kurzzeitig die Kontrolle und stößt mit einem geparkten Flugzeug zusammen.
   - Während einer Routinekontrolle zerstört eine Fehlanwendung von elektrischem Strom wichtige Avionikbauteile, die danach ersetzt und aufwändig getestet werden müssen.
2. Angenommen der Unfall wird Ereignis vom Typ *Kollision im Flug* verstanden. Die Folge wäre, dass dieser Unfall mit anderen Kollisionen im Flug verglichen würde, viele mit weitaus katastrophaleren Konsequenzen.

Unterschiedliche Vergleiche führen zu unterschiedlichen prophylaktischen Maßnahmen

Betrachten wir einen Moment Unfälle ohne Personenschaden. Wenn eine minderschwere Kollisionen im Flug die gleiche Klassifikation erfährt wie die falsche Handhabung eines Flughafenfahrzeuges oder die Fehlanwendung von elektrischem Strom während Wartungsarbeiten, könnte es sehr schwer sein Gemeinsamkeiten zu finden. Die Klassifikation dieser Zwischenfälle in Klasse A Unglücksfälle hat die Eigenschaften

- hauptsächlich ökonomisch zu sein, es geht um einen bestimmten Geldbetrag, und
- auf die Konsequenzen ausgerichtet zu sein, die Kosten für Regulierung oder Ersatz, nicht auf die Voraussetzungen.

Für die kausale Analyse des Ereignisses ist es jedoch viel wichtiger die Klassifizierung anhand der Eigenschaften, den Zustandsprädikaten, auszurichten. Diese sind

- entweder notwendige oder hinreichende Vorgänger des Ereignisses, oder aber
- unmittelbare Effekte.

Verschiedene Ansichten über prophylaktische Maßnahmen

- Die Reaktion des Management auf Unfälle ist von höchster Wichtigkeit. Daten müssen gesammelt werden, Um auf den Unfall reagieren zu können müssen Ressourcen zugewiesen werden, Verlaufsdaten müssen erfasst und später analysiert werden und die Resultate müssen in die betrieblichen Managementvorgänge einfliessen. Alle Analysten stimmen in der Auffassung überein, dass eine angemessene betriebliche Behandlung von Unfällen für den sicheren Betrieb von Systemen unerlässlich ist.
- Es sollte offensichtlich sein, dass Unfälle nur vermieden werden können, wenn ihre Ursachen beseitigt werden. Die Ursachen eines Unfalls können als eine Menge von einzeln notwendigen und gemeinsam hinreichenden Bedingungen angesehen werden, damit der Unfall so passieren konnte [51]. Einzeln notwendig bedeutet, dass der Unfall nicht passiert wäre wenn irgendeiner dieser Kausalfaktoren nicht eingetreten wäre. Eine Identifikation der Kausalfaktoren ermittelt also genau die Faktoren, die man beseitigen muss um in der Zukunft

Unfälle mit genau diesen Kausalfaktoren vollständig zu vermeiden.

Abgleichen der Ansichten

Daher kann die Behauptung aufgestellt werden, dass eine kausale Analyse unabdingbar, das *sine qua non*, jeder vorbeugenden Maßnahme ist. Dennoch verschlingt eine solche kausale Analyse Ressourcen und es muss darüber entschieden werden welchen Unfällen diese Ressourcen zugewiesen werden und welchen nicht. Die ökonomische Klassifikation von Unglücksfällen liefert eine praktische Richtlinie für das Management um Ressourcen auf die Unglücksfälle zu fokussieren, für die es gute ökonomische Argumente gibt warum sie vermieden werden sollten. Weiterhin wird eine politische Übereinstimmung mit solchen Entscheidungen dadurch vereinfacht. Dennoch muss darauf geachtet werden, Konzepte die hilfreich bei der kausalen Analyse sind nicht mit denen zu verwechseln, die bei der Zuweisung der Ressourcen helfen.

Bedeutsame und umbedeutsame Eigenschaften

Betrachten wir den Ereignistyp von Kollisionen in der Luft. Jeder einzelne Unfall hat genau bestimmbare räumlich-zeitliche Eigenschaften: Ein bestimmtes Teil eines Flugzeuges berührt ein Teil eines anderen zu einer bestimmten Zeit in einer bestimmten Zeitzone, in einer bestimmten Höhe und an einer präzisen geographischen Position (auch dann, wenn sich diese präzisen Koordinaten nicht so genau ermitteln lassen). Für den Unfall ist bedeutsam, dass es eine räumlich-zeitliche Überschneidung von Flugzeugteilen gab. Die Flugbahn der Flugzeuge und ihre Manövrierbarkeit sind für diese räumlich-zeitliche Überschneidung von kausaler Relevanz. Die Tatsache, dass sich dieser Unfall an genau einem bestimmten geographischen Punkt zugetragen hat und nicht 20 km (oder sogar 20m) weiter nördlich, wird dabei normalerweise als weniger wichtig erachtet da diese Information für die Dynamik der Flugzeuge ungenutzt bleibt.

Vorläufer eines Unfalls müssen kausale Vorläufer sein

Die kausale Analyse ist einstimmig als die vorherrschende Unfallanalysetechnik anerkannt. Ein bedeutender Grund für die Akzeptanz ist, dass es sowohl notwendig

als auch hinreichen für eine Vermeidung von wiederholten Unfällen ist dafür Sorge zu tragen, dass notwendige Bestandteile einer hinreichenden kausalen Gegebenheit in zukünftigem Verhalten gleicher oder ähnlicher Systeme in ihrer Umgebung ausbleiben.

Warum keine Korrelation?

Faktoren können eine hohe Korrelation mit Unfällen haben. Das bedeutet jedoch nicht, dass es eine bestimmte kausale Relation gibt. Dafür gibt es drei Gründe:

- Korrelation (oder wie Mill es genannt hat, *gleichzeitige variation* (concomitant variation) [53]) ist eine symmetrische Relation (wenn A mit B korreliert, dann korreliert auch B mit A), während ein kausaler Factor eine asymmetrische Relation ist (wenn A ein kausaler Faktor für B ist, dann kann B kein kausaler Faktor für A sein);
- Wenn sich A und B gleichzeitig verändern, dann könnte ein (eventuell undefinierter) gemeinsamer Kausalfaktor der Grund dafür sein;
- Weiterhin besteht die Möglichkeit, dass es einfach nur Zufall ist.

Korrelation fokussiert die Jagt nach der Kausalität

Die Identifikation von Korrelationen zwischen Faktoren hilft dabei, den Fokus der Aufmerksamkeit auf die Jagt nach der Kausalität zu richten. Kausalfaktoren korrelieren miteinander. Eine Identifikation der Korrelationen engt das Feld der möglichen Beziehungen ein, die bei der Identifikation von kausalen Verbindungen berücksichtigt werden müssen, ohne welche auszugrenzen.

Diese Methode ist nicht universell

Um jedoch statistische Korrelationen zu identifizieren, benötigt man eine hinreichende Anzahl von hinreichend ähnlichen Zwischen- oder Unfällen, oder aber eine hinreichende Menge an Beobachtungen des Verhaltens von Subsystemen. Diese könnten jedoch nicht immer verfügbar sein. Eine Situation in welcher diese verfügbar sind wäre die, in der die Safety mit der Zuverlässigkeit einer Systemkomponente korreliert und diese Komponente hinreichend analysiert wurde um Informationen über die

statistische Zuverlässigkeit zu erhalten. Solche Komponenten sind meistens „Safety Mechanismen“, auf deren Zuverlässigkeit die Safety des Systembetriebs basiert.

5.10 Zusammenfassung

Wir haben gesehen, dass selbst in einfachen Fällen wie den Systemen S und $S^{\dagger}$ ernsthafte Probleme mit den Begriffen Hazard und Risiko, so wie sie im Zusammenhang mit Systemen verwendet werden, existieren. Und dies sogar obwohl die Wahrscheinlichkeiten in S und $S^{\dagger}$ bekannt sind, die Wahrscheinlichkeiten für Veränderungen unabhängig von der Vergangenheit sind, das angenommene Schadensmodell trivial ist und Dauer nicht berücksichtigt wird.

Das dargelegte Argument beinhaltet drei Komponenten:

- Im Falle einer ganzheitlichen Unfallschwere (TODO unit severity) beschreibt das Risiko die Wahrscheinlichkeit eines Verlustes.
- Die Methode zur Berechnung eines Risikos über die Wahrscheinlichkeit eines Hazards in Kombination mit der Wahrscheinlichkeit, dass daraus ein Unfall resultiert, erfasst einige Pfade doppelt. Dies geschieht, wenn ein Hazardzustand unvermeidbar auf einen anderen folgt.
- Die Methode zur Berechnung eines Risikos über die Wahrscheinlichkeit eines Hazards in Kombination mit der Wahrscheinlichkeit, dass daraus ein Unfall resultiert, erfasst einige Pfade nicht. Dies geschieht, wenn ein Unfall eintritt ohne dass vorher einen Hazardzustand durchlaufen wurde.