Chapter 5

Problems Calculating Risk Via Hazard

We construct an example to show that the technique of calculating risk through hazard, as in the definitions in Section 4.2, does not give the intuitively correct answer, which in this case is separately calculable.

5.1 Five Notions of Hazard

5.1.1 The System Safety and Associated Notions

The "System Safety" Definition: Hazard-1 We denote by Hazard-1 the notion of hazard defined by [Lev95] and given in Section 4.2:

> A **Hazard-1** is a state of a system that, together with other conditions in the environment of the system, leads inevitably to an accident (loss event).

The Complementary Definition: Hazard-2 We have seen that it may make sense to have a term for a dangerous state of the environment that a system would like to avoid (an airplane avoiding thunderstorms, or mountains, or areas of dense traffic). Let us therefore define:

> A **Hazard-2** is a state of the environment of a system that, together with a particular reachable state or states of the system, leads inevitably to an accident (loss event).

The "Increased Likelihood" Definition: Hazard-3 Some safety engineers prefer to use a notion of hazard in which a hazard state is a system state in which there is a considerably increased likelihood of an accident happening. Accordingly, we define:

> A **Hazard-3** is a state of a system in which the likelihood of an accident is increased over the likelihood of an accident in precursor states.

The Enlarged System Safety Definition: Hazard-4 We have noted that sometimes one can use Hazard-1 effectively, and sometimes Hazard-2. It makes sense to consider whether one should define a hazard through a joint state of system and environment. We define

> A **Hazard-4** is a state of a system together with its environment that, together with other developments in the environment of the system, would lead inevitably to an accident (loss event).

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

The MIL-STD-882 Definition of Hazard The MIL-STD-882 definition of hazard is *a condition that is prerequisite to a mishap* (wherein 'mishap' is essentially the same as 'accident' as we have considered it).

The State Predicate is Not Restricted This is a different notion of hazard to those three we have considered previously. First, observe that by "condition" is meant part of the state. Second, the state predicate is not restricted to be

- part of the system state (Hazard-1);
- part of the environment state (Hazard-2).

It is thus appropriate to consider any state predicate, which may contain elements of system state *and* environment state.

"Inevitability" Is Not Predicated Furthermore, it does not contain within it the predicate of inevitability. If a condition is prerequisite to an accident, this means that the condition is *necessary* for an accident to occur. If an accident is inevitable, given the condition, this means that the condition is *sufficient* for an accident to occur. The system safety definition therefore requires the condition be necessary; the MIL-STD-882 definition that it be sufficient. These two criteria are very different!

This Distinguishes This Concept From That Of Hazard-4 Lack of the inevitability requirement distinguishes the MIL-STD-882 definition from that of Hazard-4.

The Definition We thus define:

> A **Hazard-5** is a state of a system together with its environment in which the likelihood of an accident is increased over the likelihood of an accident in precursor states.

5.2 Definition df the System S

The Objects There are three objects in the universe: x, y and z – let us call them 'atomic objects' – and thus also the objects $x \oplus y$, $x \oplus z$ and $y \oplus z$ and $x \oplus y \oplus z$.

Their Properties There are precisely three properties that may apply to any atomic object, which we shall write using standard formal notation, and we shall call *1*, *2*, and *3*. Furthermore, these properties hold exclusively of each object: if *1* holds of x, then *2* and *3* don't hold, and mutatis mutandis for *2*, *3* and y and z. And each object at any time has one of the properties; therefore, precisely one. The state of the universe may thus be described by specifying which property holds of which object.

Their Relations Let us suppose that there are no binary or ternary relations that are of significance.

The Assertions The collection of possible 'atomic' assertions is thus

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

and, of these, precisely one involving a given object is true in any state.

The States This collection of objects with their behavior will be called the 'universum'. The possible changes of the universum are simple: a change is possible from property *1* of any object to property *2* of that object; and from *2* to *3*; no other changes are possible. Let us also assume that changes are discrete: that no two changes happen simultaneously (this assumption is for convenience only; giving it up just complicates the arithmetic, as argued below).

Probability of Changes Assume that any possible change in state has an equal probability of happening. Thus in the state *112*, changes resulting in states *212*, *122* and *113* have each a probability 1/3 of happening; while in state *213*, changes resulting in states *313* and *223* each have probability of 1/2, because no change is possible to z. Let us also also assume that probabilities of transition are dependent only on what current state the universum is in: history is irrelevant.

The System and Its Environment We define a **system** S consisting of objects x and y; z constitutes the environment/rest of the universum. (This also means, if one so wishes, that S contains the object $x+y$; and that there are *mixed* objects, part system, part environment, namely $x+z$ and $y+z$. These ontological niceties need not concern us, since any properties of these objects may be defined logically from the properties of x, y and z.) The system is teleological: it starts in state *(11-)*, namely system state (*1(x) and 1(y)*), its goal state is *(13-)*, namely universum states *131*, *132* or *133*, and state *123* is a loss with a severity of unity (since it is the only loss). We assume there is an equal probability of S starting in any state of the environment; *111*, *112* and *113* are equiprobable universum states for the start of S, each with probability 1/3.

The Behavior of the System S works as follows. It starts in state *(11-)* and 'runs' (changes state) until no more actions are possible. As it changes, so does the environment. We suffer loss if the universum passes through state *123*, and we can consider S to have succeeded if it passes through state *13-* without me having suffered loss. We shall see that S is not very reliable (the probability of attaining its goal is about 1/10), and the chances of loss are quite high (about 1/3).

This system, indeed this universum, is just about as simple as could be. It is finite, with finitely many states and finite (terminating) behavior. We may see how the definitions given so far apply to this system. If we expect them to work in describing complex systems, we should be able to use them to describe such a simple system as S.

The behavior of the universum is shown in Figure 5.1, along with the probabilities that the universum enters a given state. States of the universum are shown in circles, with system goal states shown as ovals; the loss state as a larger rectangle; and the various states important for various calculations of hazard are shown as boxes with rounded corners. One should observe that one can attain the goal state *133* only by passing through *132*, already a goal state, or through *123*, the 'specified level of loss' state. We may regard *131* and *132* as the two goal states that count, since in order to reach *133*, we would have either achieved our goal already or suffered an accident. But this is a point concerning reliability, not the safety definitions.

Initial States The initial system state is (11−), so the initial univerum states are *111*, *112* and *113*; each has probability 1/3.

Accidents An accident is defined as an event that *results in* a loss. The loss state is 123. Accordingly, there are precisely two sorts of accident events, namely the transitions $122 \rightarrow 123$ and $113 \rightarrow 123$.

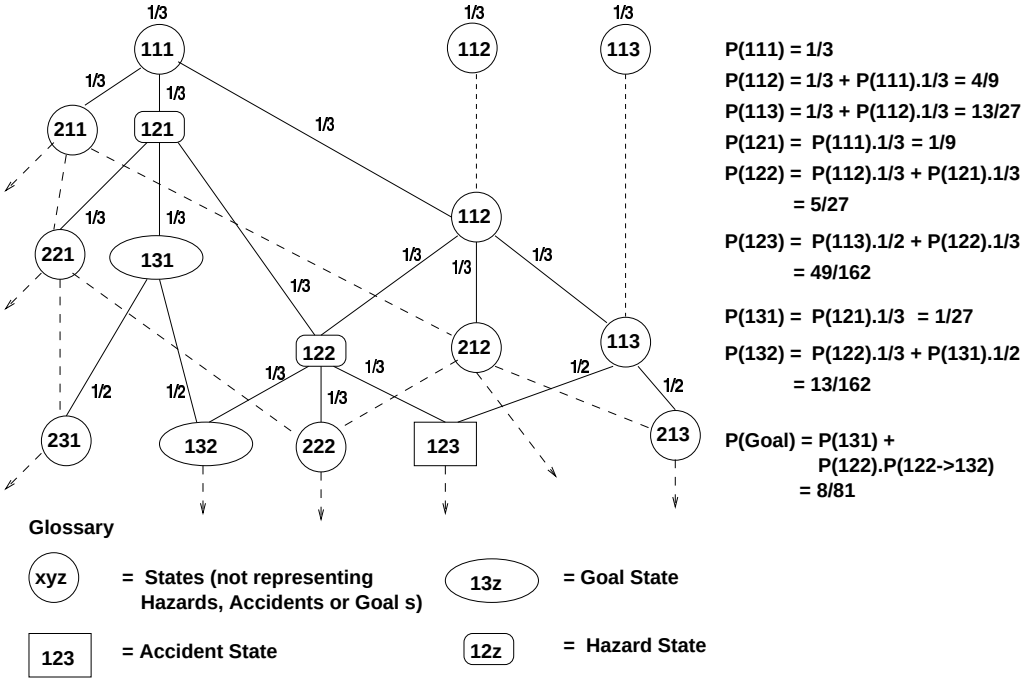

Figure 5.1: The Example System

5.3 Calculating Hazard-4 and Hazard-1 States

It will be easiest to calculate the hazard states for the various notions of hazard in a different order from that in which they were defined.

5.3.1 Identifying The Hazard-4 States

Hazard-4 states are universum states that are inevitable precursors of an accident. The two most obvious candidates are the preconditions of the two accidents *122* $\rightarrow$ *123* and *113* $\rightarrow$ *123*, namely *122* and *113*. Since *121* results in *122* without the system doing anything, *121* is a candidate also.

Candidates 121 and 122 There is no other place for the environment to go but to progress *1(z)* $\rightarrow$ *2(z)* $\rightarrow$ *3(z)*. Hence

- if the universum is in state 121 and the system does nothing, the universum will inevitably progress 121 $\rightarrow$ 122 $\rightarrow$ 123; an accident is inevitable;

- if the universum is in state 122 and the system does nothing, the universum will inevitably progress 122 → 123; an accident is inevitable.

Both 121 and 122 are therefore Hazard-4 states.

Candidate 113 An accident is not inevitable from the state 113, for the following reason. The environment cannot progress. If the system does nothing, the universum remains in state 113 for ever and no accident occurs. So 113 is not a Hazard-4 state.

Is 123 a Hazard-4 State? An accident is defined to be an event, and the two accidents are *122* → *123* and *113* → *123*. The loss state *123* is not a precursor of either of these two events, hence it is not a Hazard-4 state.

The Hazard-4 States The Hazard-4 states are thus 121 and 122.

5.3.2 Identifying the Hazard-1 States

The system state corresponding to the Hazard-4 universum states 121 and 122 is (12−). The candidates for "most unfavorable" environmental state are thereby *1(z)* and *2(z)*. They are both inevitable precursors of an accident, as argued in Section 5.3.1. There doesn't appear to be much to choose between them. The progression of the environment makes either equally as bad as the other; one is the inevitable precursor of the other.

Is *(11-)* a Hazard-1 State? 113 → 123 is also an accident. We should ask ourselves whether system state *(11-)* is also a Hazard-1 state. It is not. The obvious candidate for "most unfavorable environmental state" is 3(z). Suppose the universum to be in state *113*. The environment cannot change any more, so if the system does nothing, no accident occurs. An accident is therefore not inevitable.

5.3.3 An Accident Without a Preceding Hazard

Note that an accident can be suffered without going through a hazard state: the change *113* to *123* is an accident, but *(11-)* is not a Hazard-1 state and *113* not a Hazard-4 state.

5.4 Calculating Probabilities

We cannot calculate the Hazard-3 and Hazard-5 states without estimating some likelihoods. We do so now.

Performing Probability Calculations The universum states corresponding to the system initial state *(11-)* have equal probability of occurring as the initial state in the system's behavior. Since transitions occur discretely, the probability of occurrence of a specific system behavior may be obtained by multiplying together the probabilities along the path of transitions that the system takes.

A Remark on Notation I use notation *P(xyz)* to denote the probability of occurrence of a state *xyz* in the 'run' of the system; since this is logically a temporal event (the system cannot be in this state forever, but only at certain times), this is really shorthand for $P(\Diamond\ xyz)$, where $(\Diamond\ xyz)$ is to be read as '*eventually xyz*', that is, *in some future state, xyz*, as explained further in Section 7. $P(xyz \rightarrow abc)$ denotes the probability of occurrence of the event $(xyz \rightarrow abc)$ given that the system is in state *xyz*; using the standard notation for conditional probability, it is really a shorthand for $P(\Diamond(xyz \rightarrow abc)\ /\ xyz)$. *P(xyz via abc)* is the probability that the system attains state *xyz* and passes through *abc* on the way; it is shorthand for $P(\Diamond\ xyz\ and\ \Diamond\ abc)$. Finally, I use the notation $P(11a\ init\ \rightarrow abc \rightarrow \ldots. \rightarrow fgh)$, in which $(11z \rightarrow abc \rightarrow \ldots. \rightarrow fgh)$ is a path, or an initial segment of a path, commencing in the initial state, for the probability of occurrence of this path. We shall also need the probabilities that a path is followed *given that* we are already in the first state on the path. This is written $P(abc\ start\ \rightarrow abc \rightarrow \ldots. \rightarrow fgh)$. Finally, $P(abc|efg)$ is the conditional probability that *abc* will be reached, given that the system is already in *efg*.

Calculation of Loss Probability Given Universum State We shall need the following probabilities of entering the loss state given certain universum states.

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

$$\begin{aligned}
P(123|112) &= P(112start\ \rightarrow 122 \rightarrow 123) \\
&\quad + P(112start\ \rightarrow 113 \rightarrow 123) \\
&= (1/3).(1/3) + (1/3).(1/2) \\
&= (1/9) + (1/6) \\
&= (5/18)
\end{aligned}$$

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

$$P(123|121) = P(121start\ \rightarrow 122 \rightarrow 123)$$

$$= (1/3).(1/3)$$
$$= (1/9)$$

$$P(123|122) = P(122 start \rightarrow 123)$$
$$= (1/3)$$

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

Calculation of Loss Probability Given System State We shall need the following calculations of entering the loss state, given certain system states. Notice that since the system starts in a state $(11-)$, we have

$$P(123|(11-)) = P(123)$$

Also, we have

$$P(123|(13-)) = P(123|(21-)) = P(123|(22-) = P(123|(23-) = 0$$

since a loss state is unreachable from these system states.

Calculation of P(123 — (12-)) The calculation of $P(123|(12-))$ is a little tricky, because some of the accident occurrences $122 \rightarrow 123$ are counted already in $P(123|121)$ and we have to be careful not to count these again when assessing how likely it is that the accident $122 \rightarrow 123$ will happen when starting from state 122. We proceed by observing first that

- the ones we have already counted are those that come from $111 init \rightarrow 121 \rightarrow 122$.
- the ones we haven't already counted come via $111 init \rightarrow 112 \rightarrow 122$ plus those that come from $112 init \rightarrow 122$.

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

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

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

It follows that

$$P(122 \; via \; 112) = (4/27)$$

$$P(122\ \textit{via}\ 121) = (1/27)$$

so we have counted one out of five accidents $122 \rightarrow 123$ in considering $P(123|121)$ and we need to consider the other four-fifths. It follows that:

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

Likelihood of States Simpliciter We shall need the following state likelihoods.

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

$$\begin{aligned} P(113) &= P(111 \rightarrow 112 \rightarrow 113) \\ &\quad +P(112\textit{init}\ \rightarrow 113) \\ &\quad +P(113\textit{init}\ ) \\ &= (1/3).(1/3).(1/3) + (1/3).(1/3) + (1/3) \\ &= (13/27) \end{aligned}$$

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

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

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

Calculation of Likelihood of System States We shall also need the following likelihoods of system states from which an accident is reachable:

$P((11-)) = 1$

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

There is little point to calculating the likelihood of other system states. We shall not need them, since an accident is unreachable from them.

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

Figure 5.2: Summary of Calculations

5.5 Calculating Hazard-3 and Hazard-5 States

We are now in a position to determine the Hazard-3 and Hazard-5 states. We start as before with Hazard-5.

5.5.1 Determining the Hazard-5 States

Hazard-5 states are those universum states in which the likelihood of an accident is increased over the predecessors. Looking at Figure 5.2 lets us read off as follows

Candidate 111 111 is an initial state, but an initial state has no precursor, so one cannot meaningfully speak of an increased likelihood over precursors. 111 is not a Hazard-5 state.

Candidate 112 112 has as sole precursor 111. It is itself an initial state, but an initial state has no precursor, so one cannot meaningfully speak of an increased likelihood over precursors when it occurs as an initial state. $P(123|112) = (5/18) > (7/54) = P(123|111)$. The likelihood of an accident is increased, therefore 112 is a Hazard-5 state.

Candidate 113 113 has as sole precursor 112. It is itself an initial state, but an initial state has no precursor, so one cannot meaningfully speak of an increased likelihood over precursors when it occurs as an initial state. $P(123|113) = (1/2) > (5/18) = P(123|112)$. The likelihood of an accident is increased, therefore 113 is a Hazard-5 state.

Candidate 121 121 has as sole precursor 111. $P(123|121) = (1/9) < (7/54) = P(123|111)$. The likelihood of an accident is decreased, therefore 121 is not a Hazard-5 state.

Candidate 122 122 has as precursors 121 and 112. $P(123|122) = (1/3) > (1/9) = P(123|121)$. The likelihood of an accident is increased. $P(123|122) = (1/3) > (5/18) = P(123|112)$. The likelihood of an accident is increased. Since the likelihood of an accident is increased over the likelihood of an accident in either of its precursor states, 122 is a Hazard-5 state.

The Hazard-5 States The Hazard-5 states are thus 112, 113, and 122.

5.5.2 Determining the Hazard-3 States

The two candidates are (11−) and (12−) as before, since the accident is unreachable from other system states.

Candidate (11-) (11−) is the start state. It has no precursor, so so one cannot meaningfully speak of an increased likelihood over precursors.

Candidate (12-) (12−) has as sole precursor (11−). $P(123|(12-)) = (17/45) > (8/81) = P(123|(11-))$. The likelihood of an accident is increased. Since the likelihood of an accident is increased over the likelihood of an accident in its precursor state, (12−) is a Hazard-3 state.

The Hazard-3 States The Hazard-3 state we have identified is (12−). This makes calculations of risk identical in this case for Hazard-1 and Hazard-3.

Summary We summarise the Hazard states for each different notion of hazard in Figure 5.3.

Hazard-1 : (12−)
Hazard-2* : (12−)
Hazard-3 : (12−)
Hazard-4 : 121 and 122
Hazard-5 : 112, 113 and 122
* Recall that the Hazard-2 example is the "mirror", $S^{\dagger}$, of System S.

Figure 5.3: Hazard States For Each Notion of Hazard

5.6 The Calculation df Risk Via Hazard

Since severity is unity, the risk that we shall suffer loss is simply

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

The calculation of risk via hazard that we are supposed to perform is:

$$Risk = \sum_{Hazard\ states\ h} P(h).P(123|h)$$

and were these calculations to be accurate, we should obtain (8/81). Let us now perform these calculations, using the notation $Risk_i$ for the notion Hazard-i. The numbers we use are summarised in Figure 5.2. The hazard states we use are summarised in Figure 5.3.

$$Risk_1 = P((12-)).P(123|(12-))$$

$$= (8/27).(17/45) \neq 8/81$$

$$Risk_3 = P((12-)).P(123|(12-))$$

$$= (8/27).(17/45) \neq 8/81$$

$$Risk_4 = P(121).P(123|121) + P(122).P(123|122)$$

$$= (1/9).(1/9) + (5/27).(1/3)$$

$$= (6/81) = (2/27) \neq (8/81)$$

$$Risk_5 = P(112).P(123|112) + P(113).P(123|113) + P(122).P(123|122)$$

$$= (4/9).(5/18) + (13/27).(1/2) + (5/27).(1/3)$$

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

We have shown that the calculation of risk through combining hazard likelihood with likelihood of loss per hazard doesn't yield the appropriate figure, which is likelihood of loss *simpliciter*. The only exception is the calculation for Hazard-2, and for that we alter the example. For Hazard-2, we take the same example, but interchange system and environment. That is, the system becomes z and the environment x and y. Call this new example System $S^\dagger$. The loss state and its likelihood remains the same. The calculation of risk through Hazard-2 for System $S^\dagger$ is identical to the calculation of risk through Hazard-1 for System S, since we have just swapped system and environment, and thus system states for environment states and vice versa.

Conclusion The calculation of risk through hazard according to the definitions in [Lev95]do not work for any of the five notions of hazard we have considered.

5.7 The Problem

5.7.1 The Risk of Overcounting

The problems with calculating risk through hazard on Systems S and $S^\dagger$ come about partly through overcounting the paths. Namely,

- in the calculation of $Risk_1$ and $Risk_3$, both $P((12-))$ and $P(123|(12-))$ include a component assessing the likelihood of the transition $111init \rightarrow 121 \rightarrow 122$. They are thus not independent.

- In the calculation of $Risk_4$, the term $P(121).P(123|121)$ counts some of the same paths as $P(122).P(123|122)$, again those that contain the transition $121 \rightarrow 122$.

- In the calculation of $Risk_5$, the term $P(112).P(123|112)$ counts some of the same paths as $P(113).P(123|113)$, namely those that contain the transition $112 \rightarrow 113$.

5.7.2 Not All Accidents Occur Through Hazards

Although the accident $122 \rightarrow 123$ starts in a hazard state for each of the different notions of hazard, the accident $113 \rightarrow 123$ attains a loss state *without passing through a Hazard-1, Hazard-3 or Hazard-4 state*. Thus the accident behavior $113init \rightarrow 123$ is omitted from the count that each of these risk assessments make. Hazard-5 is the only notion of hazard which includes 113 as a hazard state, but it suffers from overcounting problems as noted above.

5.7.3 Summary

We have used System S and System $S^{\dagger}$and their environments to demonstrate that there is no reasonable way via the notions of Hazard-1 through Hazard-5 to combine hazard probability with likelihood that a hazard state will result in an accident (along with severity of loss) to obtain an accurate estimate of risk, understood as the likelihood of loss (combined with severity). The concept of severity played no role in the argument; the problem lies in the attempt to combine hazard probabilities with likelihood that an accident will result. The problem lies partly in overcounting, and partly in undercounting accidents that occur in system behaviors that do not pass through a hazard state.

5.8 Trying To Fix It

Solution: Hazard-5 Plus Independence of Hazards? Although this example is combinatorially simple, intuition does not help a great deal in guessing its properties. It was deliberately constructed in order to demonstrate the risks of overcounting and undercounting. The risk of overcounting can perhaps be mitigated by trying to assure that all phenomena to be counted as hazards are independent of each other, in the sense of probability theory. It is because the situation of the universum entering state 121 is not independent of it entering 122 that we overcount. However, ensuring independence of hazard phenomena does not solve the undercounting problem, whereby accidents can happen without passing through a corresponding hazard state. But recall that Hazard-5 captured these states. This may suggest to some that a combination of

- employing the concept Hazard-5, and
- ensuring that identified hazards are independent

might be a useful solution to the problem of calculating risk through hazard. Note that both are needed: the Hazard-5s posed by 112 and 113 are not independent of each other. We will not go so far as to favor this solution. Rather, we prefer here simply to discuss the phenomenon.

Altering the Concept of Risk Another move would be to take the definition of risk as it is given; and conclude that the intuitive concept of risk as (in this case) likelihood of loss given unit severity is not the most appropriate concept of risk. But this would be a move to contradict intuition for the sake of otherwise unmotivated consistency. Besides, the problem remains in another form. We need to calculate the likelihood of loss, for example to calculate betting odds, and the problem is that the proposed calculation method cannot render this in all circumstances.

This Leaves One Open To Loss If I believe my risk is as in the definition, and I bet according to this, then I am betting according to some assessment of probability that is different from the actual probability that a loss state will occur. A bookmaker can thus construct a series of bets that I am prepared to accept according to my assessment of risk but which I am guaranteed to lose money on in the long run. This is of course only a way of phrasing the fact that if I incorrectly assess the probability of loss, I may make decisions which do not minimise my loss. This is not what one hopes for from a risk assessment.

5.9 Motivating The Conceptions of Hazard

Hazard-1 As we have seen, Hazard-1 is that used in System Safety engineering in the U.S. for some time, and that espoused for that reason by [Lev95]. This is reason enough for us to consider it. However, one should also note the rationale behind it, which is that in the safety assessment of a teleological system is that the the engineer has control over the system state but not over the environmental state. Any prophylactic measures can only be applied to circumstances and state components over which one has control. Therefore, hazard reduction must be applied to the system state.

Hazard-2: The Layman's Idea While driving my car, I am inclined to call a football bouncing into the road with a child running after it a hazard. I am also inclined to call a pothole in the road a hazard. Both of these are predicates of the environment in which I am driving, not of my car and its driver. If I consider my car with driver to be the system, these "hazards" are environmental predicates.

If I am driving my car in a more or less standard manner, these conditions could lead to - or would inevitably lead to - some sort of accident, depending on the system state. For example, if I am driving at 0.001 kph, the situations above would not lead to accidents, whereas they would if I am driving at the generally allowable 50kph.

Hazard-1 and Hazard-2 for Different Sorts of Systems? When considering a relatively closed system, such as a power plant or chemical plant, or

electrical wiring in a building, it makes sense to conceive of hazard states as being system states. However, some complex systems are unavoidably open. An aircraft has to operate in weather and in terrain that is part of its environment. There is no system state which corresponds to a thunderstorm going from Level 2 to Level 4 within a matter of a few minutes, and it is wise to single out this area of the environment for special attention when it happens. This is the rationale for Hazard-2. The system safety definitions have no equivalent concept to that of Hazard-2, since there is no obvious way to reduce Hazard-2 to Hazard-1 in general, but it is hard to see how the use of Hazard-2 can be avoided in some cases.

Maybe Both At Once: Hazard-4 The point of considering and designing for system safety, however, is to avoid combinations of environmental conditions and system states leading to accidents. If one knows all such states, as in Hazard-4, then one can calculated Hazard-1 and Hazard-2 states from them, as we did for System S. Therefore Hazard-4 contains more information than either Hazard-1 or Hazard-2, and these latter are recoverable from it.

5.9.1 Weakening the Inevitability Requirement

Other definitions of hazard preserve its feature as a property of system states, but give up the insistence on inevitability. This led us to Hazard-3 and Hazard-5. Judging states by increased likelihood, not of accidents but of failure, is common in reliability engineering. Since safety may often depend on the reliability of safety-critical components, these are connected.

Discrete Classification An example is commercial aviation. Lloyd and Tye [LT82] explain the various different likelihood categories used in civil aviation certification in the U.K. They note [LT82, Table 4-1] that both U.S. Federal and European Joint Aviation Regulations, in their parts 25, classify events as *probable* if their likelihood of happening lies between 10^{-5} and 1, *improbable* if between 10^{-9} and 10^{-5}, and *extremely improbable* if smaller than 10^{-9}; the JARs additionally classify probable events into *frequent* (between 10^{-3} and 1) and *reasonably probable* (between 10^{-5} and 10^{-3}), and improbable events into *remote* (between 10^{-7} and 10^{-5}) and *extremely remote* (between 10^{-9} and 10^{-7}).

The Purpose of the Discrete Classification The purpose is (was) to classify an event as *extremely improbable* if it was unlikely to arise during the life of a fleet of aircraft; *extremely remote* if it was likely to arise once during fleet life; *remote* if likely to arise once per aircraft life, and several times per fleet life; *reasonably probable* if likely to arise several times per aircraft life. Fleet sizes were assumed to be about 200 aircraft, with each aircraft flying 50,000 hours in

its life (nowadays, we are seeing fleet sizes are of the order of 1,000 to 2,000, and aircraft flying more than 50,000 hours, altogether about a factor of 10 difference).

Classification of Effects Effects are also classified into *minor*, *major*, *hazardous* and *catastrophic*, according to damage, injuries and deaths.

The Certification Basis The certification basis is (was) to demonstrate that *major*, *hazardous* and *catastrophic* effects could occur at most with *remote*, *extremely remote* and *extremely improbable* frequencies respectively.

Reliability and Safety Conflated The certification basis attempted to assign probabilities to failures, which is a technique for reliability classification, but we have noted that reliability and safety are closely linked via reliability of safety-critical components. For example, multiple engine failures entail that the aircraft must land within a certain radius of its position, whether there is a suitable airport there or no. A fire on board that is not effectively extinguished will spread within a certain time, and be catastrophic unless the aircraft is on the ground at this time. Failure of various specific mechanical parts, or total failure of the flight control system, lead inevitably to an accident. However, reliability and safety may still be distinguished: a recognition light on the underbelly is a safety-critical item; a reading lamp in passenger class is not. The reliability of the latter is not a safety issue.

5.9.2 Avoidance Of The Problematic Notions

The IFIP WG 10.4 Definitions The series of definitions in [Lap92] concerned with dependability, which is taken by members of the IFIP WG 10.4 to include safety, does not include the concepts of hazard and risk at all.

5.9.3 Classifying Risk Through Statistics

An obvious way to avoid the problem is to have had the misfortune to have had sufficiently many accidents that one can calculate risks on a statistical basis from history. Let us briefly consider one plausible way in which this might be done, namely the U.S.A.F. mishap classification scheme.

U.S. Air Force Accidents as "Class A Mishaps" The most severe category of incident defined by the U.S. Air Force is a *Class A* mishap. This is a mishap resulting in loss of life or more than $ 1M in damage. This is similar to the U.S Federal Aviation Regulations definition, in which an accident is defined to be severe injury or loss of life, or "substantial damage" to an aircraft (the "or" is inclusive).

This definition may have unintuitive consequences Such accidents have occurred in military aviation in which both aircraft returned safely with more than $ 1M in damage [Gar98]. (This would be a case in which considerable damage was done, but no one died and the damage was repairable.)

The Distinction Between Events and Event Types With a slight change in parameter, say, a slightly different relative motion of the aircraft, then the event that occurred could have had catastrophic consequences. For example, loss of both aircraft with pilots. What does it mean to say that an event *could have had* other consequences? One way of interpreting this is to note that there is a class of incidents, *mid-air collisions* to which this event belongs. One can even go further and say: *mid-air collisions between two aircraft of type X in formation flying* or even more detailed: *mid-air collisions between two aircraft of type X in formation flying in clear weather, performing manoeuver Y*. These classifications define ever more precise and thus smaller *classes* or collections of events. These are *event types*.

Using the Distinction An individual event such as a mid-air collision with $1.01M damage but in which both aircraft and crew returned safety can be viewed either

1. as an individual event with specified damage; or
2. as a member of an event type whose average member is a catastrophic accident

How we view this event can have considerable influence on how we would treat it.

Different Classification Leads to Different Comparisons Consider the different reactions to the different classifications.

1. Suppose we treated the accident as an individual event with specified damage. Then we would be comparing with other events in which, say,
   - a ground service vehicle ran into a parked aircraft because it was travelling too fast for wet conditions and momentarily lost directional control; or
   - a misapplication of electrical power during routine service fried essential aircraft avionics and required thorough test and replacement
2. Suppose we considered the accident as an event belonging to the type *midair collision*. Then we would be comparing with other midair collisions, many with much more catastrophic consequences.

Different Comparisons Lead to Different Prophylactic Measures Let us for the moment consider non-injurious accidents. If a midair collision with minor consequences is classified together with midhandling of a ground vehicle or misapplication of electrical current during maintenance, we may be hard put to find similarities. The classification of these incidents into Class A mishaps uses a predicate which is

- primarily economic, an amount of money, and
- oriented towards consequences, the cost of management or replacement, rather than preconditions.

An incident classified in the according to the features, the state predicates, that were

- either necessary or sufficient precursors of the event, or else
- immediate postconditions

is of much more importance for the causal analysis of the event.

Different Views on Prophylaxis

- Management response to accidents is of the utmost importance. Data must be collected, resources allocated to response, trend data must be classified and analysed over time, and the results incorporated into institutional management procedures. All analysts agree uniformly that appropriate institutional treatment of accidents is crucial to safe systems operation.
- It should be evident that accidents themselves can only be avoided by mitigating their causes. The causes of an event can be regarded as a collection of individually necessary and jointly sufficient conditions for the event to have occurred [Mac74]. That they are individually necessariy means that if any one of these causal factors had not pertained, the event would not have happened. Identifying the causal factors identifies those factors which, were they to be avoided in the future, would avoid entirely future accidents with exactly those causal features.

Reconciling The Views An argument may thus be made that causal analysis is essential to, the *sine qua non* of, any prophylaxis. However, performing such a causal analysis requires allocation of resources and a decision must be made as to which incidents those resources should be allocated and to which not. The economic classification of mishaps is thus a practical guide to management, focusing resources on those mishaps for which there is a good economic argument to be made for avoidance, and thus encouraging political agreement with such decision. Care must be taken, however, not to confuse concepts which aid in causal analysis with concepts which aid in resource allocation.

Predicates That Matter, And Predicates That Don't Consider the event type of midair collisions. Each individual accident will have precisely locatable spatio-temporal features: such-and-such an aircraft part touched another part at a precise time in a precise time zone, in a precise altitude and geographical location (even if these precise coordinates are not so precisely determined). It is significant for the accident that there was spatio-temporal overlap of parts. The trajectories of the aircraft and their manoeuverability are regarded as causally relevant to this spatio-temporal overlap. The fact that it happened over the precise geographical point that is did and not 20 km, or even 20m, to the north, is usually regarded as less relevant, since nothing about the dynamics of the aircraft makes use of this information.

Allowing Revision of This Judgement It may be, however, that the exact geographical location is relevant; perhaps because of sun position and location of reflectors on the ground and position of the aircraft relative to the reflected image of the sun, one pilot was temporarily blinded and lost the precise dynamic control over his aircraft that formation flying requires. So revision of *a priori* judgements of causal relevance must remain an open possibility. However, in the example above, it should be clear that relative position (or angle) of sun, the presence of ground reflectors, and the requirement of perfect pilot vision for manoeuvering are pertinent causal factors, and the translation of the ground reflector and the aircraft 20m to one side of the (relative) coordinate frame does not affect causality.

Precursors to An Accident Must Be Causal Precursors Causal analysis is uniformly accepted as the predominant accident analysis technique. A significant justification for this acceptance is that in order to avoid repeat accidents, it is both necessary and sufficient that a necessary part of a sufficient causal condition for the accident be absent from future behavior of the same or similar systems in their environment.

Why Not Correlates? Factors may have high correlation with accidents. However, correlation does not mean that there is a specific causal relation, for three reasons:

- Correlation (or, as Mill called it, *concomitant variation* [Mil73a]) is a symmetric relation (if A correlates with B, then B correlates with A), whereas being a casual factor is an asymmetric relation (if A is a causal factor of B, then B cannot be a causal factor of A);
- if A and B vary concomitantly, then that may be because they have a (maybe unidentified) causal factor in common;
- the possibility remains that it could just be chance.

Correlat on Focuses the Hunt For Causality Identifying correlation between factors helps to focus attention in the hunt for causality. Causal factors will be correlated, so identifying correlations narrows the potential relationships to be considered in identifying causal relations, without excluding any.

This is Not a Universal Method However, in order to identify statistical correlations, one needs a sufficient number of sufficiently similar incidents or accidents, or a sufficient number of observations of subsystem behavior. These may not always be available. One circumstance in which these would be available are in a case in which safety is correlated with reliability of a system component, and sufficient analysis of this component has been performed to be able to identify a statistical reliability. Such components are most likely "safety mechanisms", on whose reliability the safety of the system operation is predicated.

5.10 Summary

We have seen that, even for a simple case such as System S and System $S^{\dagger}$, there are serious problems with the notions of hazard and risk as used about systems. This despite probabilities in S and $S^{\dagger}$ being determinate, with probabilities of change independent of history, and assuming trivial severity and ignoring duration.

There are three components to the argument as presented:

1. Risk in the case of unit severity is likelihood of loss;
2. Calculating risk through hazard likelihood combined with likelihood that an accident will result overcounts some paths in the case in which one hazard state inevitably leads to another,
3. Calculating risk through hazard likelihood combined with likelihood that an accident will result omits to count the likelihood of accidents which occur without passing through a hazard state.