# Insights

## What is a Hazard?

Hazards, their identification, and eventual resolution play a key role in safety assurance. This paper is prompted by the variations we see in hazard understanding that lead to inconsistent use of hazards and the effective management of the risks they relate to. Hence, we revisit here what may be a well-defined area, with the intent to refresh thinking and re-establish the underlying points.

Definitions of a hazard vary, and this may lead to some variance of understanding from the start, so in this paper we will go back to the underlying principles.

### Fundamental Context

The idea is that the hazard is a situation set up by a system, which could lead to an accident. A system operates within an environment. Accidents occur in the environment, whereas hazards occur on the system/environment interface or boundary. Consider Figure 1 as an example.

A hazard can lead to an accident in the environment - perhaps in the presence of other conditions in that environment. The hazard sits on the system/environment interface because, from the systems perspective, all the preconditions for the hazard are satisfied and there is nothing more required for the hazard to exist. From the environment's perspective, the hazard may lead to an accident if a number of other things occur.

Consider an example most will be familiar with (referring to the states and conditions labelled in Figure 1):

- **Environment:** Kitchen
- **System:** Cleaning
- **Hazard:** Wet floor open to public
- **State A:** Wet floor after being cleaned
- **State B:** Area not isolated
- **Condition C:** Someone enters kitchen
- **Accident:** Person falls over

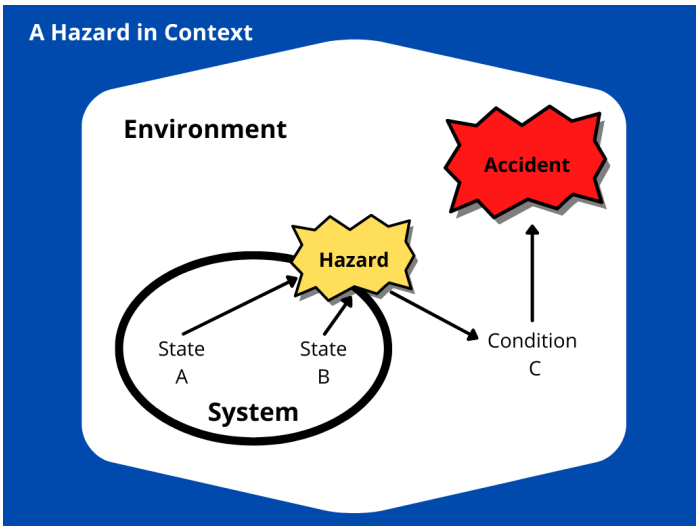


**Fig. 1 - A hazard in context**

The example is a 'cartoon' (a “ludicrously simplistic, unrealistic portrayal”) we use here to allow us to make the points about hazards using an example that can be easily understood.

The basic premise of the example is that the system of cleaning will involve washing the floor and leaving it to dry. The hazard of a wet floor exists whilst the floor is drying. Should a person enter the area while it is still drying, there is a good chance a fall and (possible) injury will occur.

We can use this simple example to demonstrate a few things:

1. **The hazard and the accident are different**. Someone may enter the area or they may not, the cleaning system cannot (as described so far) control the movements of people in the kitchen area. Hence the hazard is “wet floor open to public” which may then lead to the accident “Person falls over”.
2. **The states that set up the hazard are under the control of the system**. State A “Wet Floor after being cleaned” is unavoidable and would normally be expected to occur. State B “Area not isolated” may depend on the specific context. In a work environment, it may be part of the system to isolate areas with signs, in a domestic environment this is less likely.
3. **The hazard and the causes are different**. The hazard is not “Wet floor after being cleaned” because we also require the area to be open to people to walk through for there to be a hazard.
4. **The hazard sits on the interface between the system and the environment**. Symbolically this is the point at which the system effects its environment. If we take the causal states alone: State A "Wet floor after being cleaned" and State B "Area not isolated" the first seems like a normal state of affairs (if you are thinking it’s the hazard – hold that thought!) and the second prompts the question: “Why would we need to isolate?”. Removing both states would result in an unclean and unusable area. While this removes our hazard, it also removes any benefit of having the area at all (clean or otherwise).

Causes (like the states A and B) could relate to faults, design oversights, application constraints, unidentified side effects or lots of things that could feasibly by related to the system. It is only when we understand how these internal characteristics of the system can contribute to a hazard at the boundary with the environment that we can see how the system contributes to risk.

Finding the states that trigger hazards may not be easy or straightforward, as most realistic systems have many states. If we understand why the system might be unsafe by identifying hazards, we can then see how the multitude of states within the system could contribute to the hazard. This reinforces the value and importance of a good hazard identification process, as the hazards will lead us to the causes. Once we know the causes, we can consider how to control those causes.

Of course, there is an issue with the example above. If you considered the scenario, there is a good chance that the idea occurs that State A “Wet floor after being cleaned” is the 'real' hazard. It is the wet floor that causes the problem, and we only isolate people because of the cleaning and the resulting wet floor. The isolation is more of a control for the known hazard of a wet floor. So, the cause is the hazard, which negates point 3 above. Have we deceived you?

This is resolved by thinking of hazards in relation to the specific system of interest. Following systems engineering – it is possible to break down a system into its constituent subsystems. In this way, each subsystem could be argued to have hazards on its interface to the broader system. We will illustrate this below by extending the cleaning example to illustrate the point.

### System Hierarchy

We can break down the cleaning system in our example to consist of two subsystems.

1. **Washing**: Where all aspects of getting the floor clean are dealt with.
2. **Drying and finishing**: Where all aspects of finishing the floor and returning it to use are dealt with.

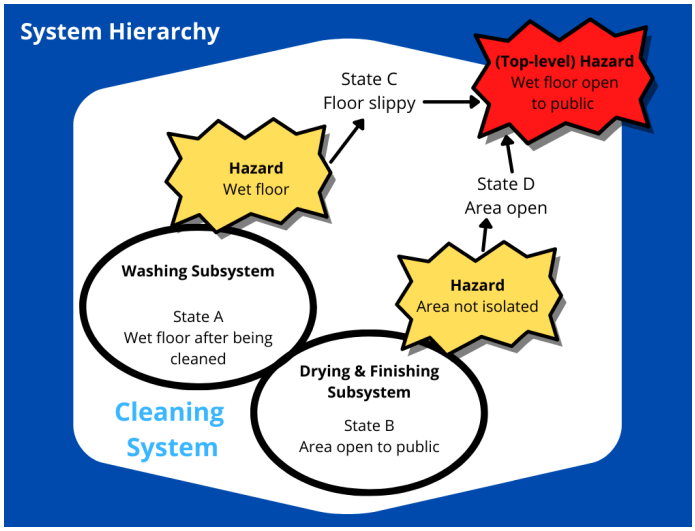


**Fig. 2 - System hierarchy**

We could represent the situation as shown in Figure 2 (a development of Figure 1).

Here the washing subsystem has a hazard "Wet floor" which exists within its immediate environment – the cleaning system - and this leads to the consequence of State C "Floor slippy". Similarly, the drying and finishing subsystem has a hazard in the same environment of "Area not isolated", leading in consequence to the State D: "Area open".

The eventual hazard (we shall use the phrase "top level" hazard for reasons that are hopefully clear from Figure 2) "Wet floor open to public" is caused in the environment by the combination of States C and D. This helps to illustrate a few more points relating to hazards:

1. **Hazards can be pitched at the level of systems decomposition we are focusing on**. But they will always exist at the system boundary of the specific system we focus on.
2. **In a systems hierarchy, hazards at a subsystem level may be the causes of the hazard at the system level**. And in turn, the system level hazard will have implications in the environment.

So, in effect, the idea that the hazard is "Wet floor" are vindicated. In this example and having knowledge that firms that clean generally take the precaution of isolating wet areas suggests that, in practical terms, the hazard would only likely occur if there was a failing in the secondary system that controls the drying process to isolate the area. Hence, we get a better picture of the true situation that leads to the hazard in the environment. This is useful as to reduce the risk we could look at both:

- **Controls to reduce the wet floors hazard**: perhaps dry cleaning techniques or procedures that reduce the time it takes to dry the floor reducing exposure time of the hazard.
- **Controls to reduce the 'open to public' hazard**: ensuring cleaning takes place at quiet times, providing barriers to areas to reinforce closed status.

This leads to another significant point:

- **By undertaking this analysis, we can be more specific about how to determine which controls might be effective in reducing the risk at a subsystem level.** This leads to a reduction at the system level.

## Summary

Hazard analysis is the central and vital part of safety assurance. The process should be systematic, it should relate to the system under assessment, and support a view that the safety risks of deployment have been managed So Far As Is Reasonably Practicable (SFAIRP).

This paper has discussed the concept of hazards and how this relates to systems architecture. Following this concept allows a better understanding of how states within a subsystem can escalate to become system level hazards. This provides a better understanding of the chain of events that leads to a hazard occurring in the context of a specific system architecture.

This also ensures that the causes of the hazard can be traced to subsystems and specific controls identified as well as understanding which events are outside of the system definition and are conditions of the environment. With this analysis in place, we can be clearer about what we mean when we talk about a 'hazard' and how it depends on the specific context.

**Steve Dawkins | Principal Consultant**

Acmena


## CONTACT US

**+61 (0) 478 814 324**
**enquiries@acmena.com.au**
**www.acmena.com.au**

Acmena Group Pty Ltd
PO BOX 220
Ashgrove West
Brisbane, QLD 4060
ABN: 37 158 514955
ACN: 158 514 955