Chapter 7

Defining Changes

Before starting work on a change, your organisation must define the aims, extent and context of the change.

7.1 Guidance from volume 1

This is often done in a requirements specification.

If you are in doubt about the aim, extent or context of the change, you will also be in doubt about claims for its safety.

When you define a change you should also find out which authorities will have to approve your safety case.

7.2 General

Understanding the aims, extent and context of a change is fundamental to successful ESM. Any change to the railway can be regarded as introducing a new *system,* or changing an existing one. Understanding the boundary between this system and its environment is a pre-requisite to understanding how the system might contribute to an accident (that is understanding what its *hazards* are).

Figure 7-1 illustrates the relationship between the system boundary, hazards and accidents.

The system or equipment may consist of software, hardware, people and procedures.

The environment consists of any anything that could influence, or be influenced by, the system or equipment. This will include anything to which the system connects mechanically, electrically or by radio but may also include other parts of the railway that can interact through electromagnetic interference, or thermal interchange. The environment will also include people and procedures that can affect, or be affected by, the operation of the system or equipment.

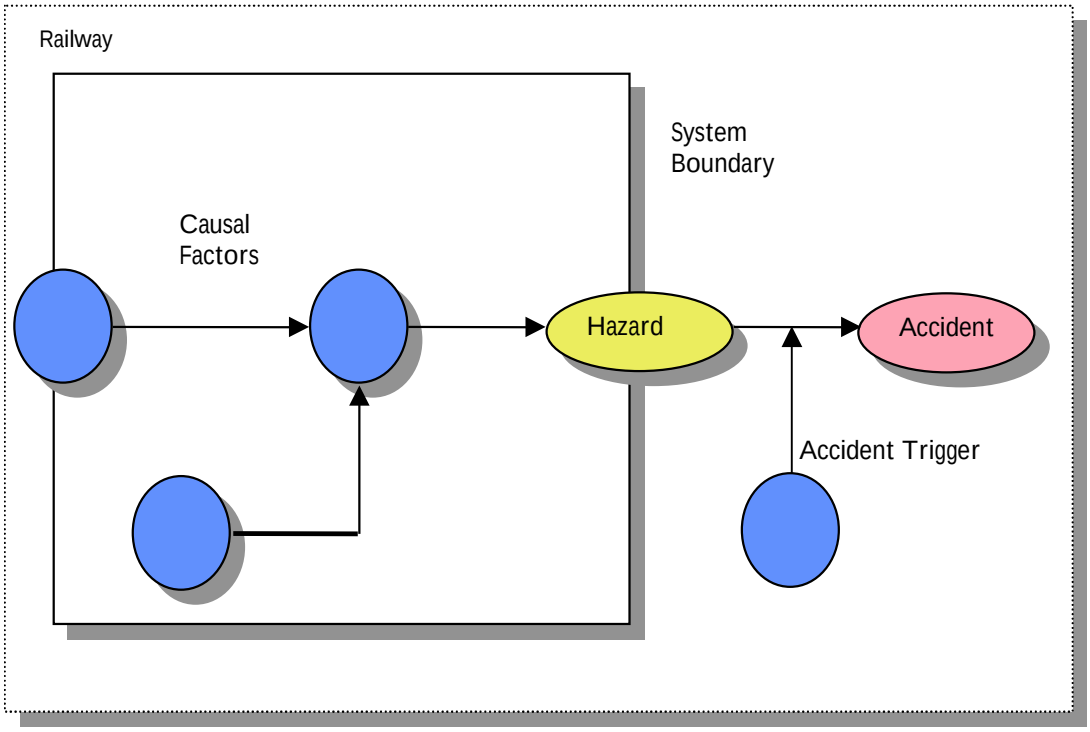

Figure 7-1 - The system boundary in safety analysis

The aims, extent and context of a change should already be defined in a requirements specification but, if they are not, you should clarify them before starting to proceed with safety analysis. If there is not sufficient information available to completely define the change, then explicit assumptions should be made. These assumptions will need to be confirmed at some later stage in the lifecycle of the change and this confirmation should be planned.

The aims, extent and context may change during the life of the system or equipment. You should monitor them for change and, if they do change, you should review all affected ESM activities and rework them as necessary.

This chapter is written for:

- Project Managers, and
- anyone involved in performing or reviewing a risk assessment.

7.3 The supplier chain

Any railway involves a network of stakeholders. The ultimate services to the public are provided by railway operators, including train operators, station operators and infrastructure controllers. However they rely on suppliers in order to do this, their suppliers rely on other suppliers and so on.

It may be the case that the overall safety of the railway depends upon the weakest link in this chain.

Figure 7-2 shows an example of this state of affairs. A train operator relies on a train supplier to provide them with trains. The train supplier, in turn relies on other companies to supply train components, such as the driver's display. Of course this is just a small fragment of a much more complex network of suppliers.

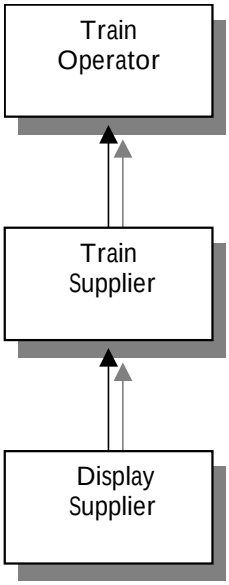

Figure 7-2 - A railway supply chain

There is a hierarchy of systems associated with this network of suppliers, as illustrated in Figure 7-3. This shows that System B (a train, perhaps) is part of the railway as a whole and System A (the driver's display, perhaps) is part of System B.

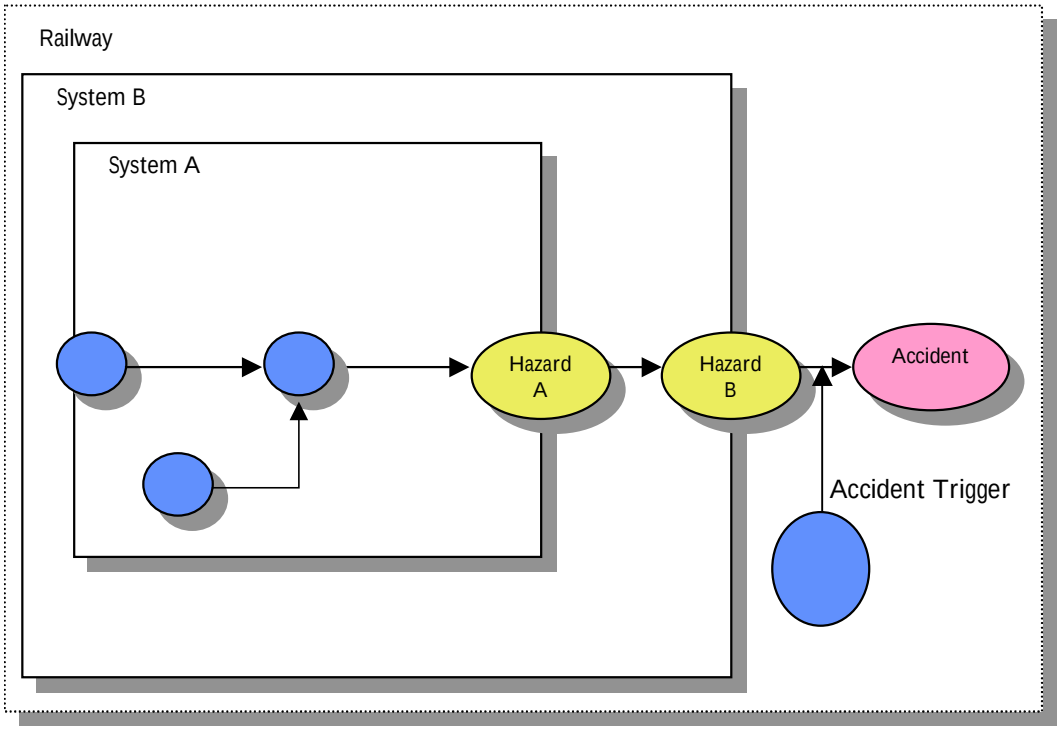

Figure 7-3 - The system hierarchy

The suppliers of both system A and system B need to carry out ESM but they will use different system boundaries and, as a result, concentrate on different hazards.

System B provides the environment for system A. The supplier of system B should, therefore, provide the supplier of system A with information that the latter needs to carry out ESM, including relevant hazards, risks and safety requirements associated with System B. This is discussed further in chapter 6.

7.4 Product development

A product manufacturer may not know all the environments in which their product may be considered for application. In general, they proceed by making informed assumptions (from their own knowledge and by talking to likely customers) about the environment that their product will experience (see Figure 7-4). These assumptions should be made explicit and written down. When it comes to preparing a Safety Case for a specific application, a large part of the work required will be to check that these assumptions hold in the application in question.

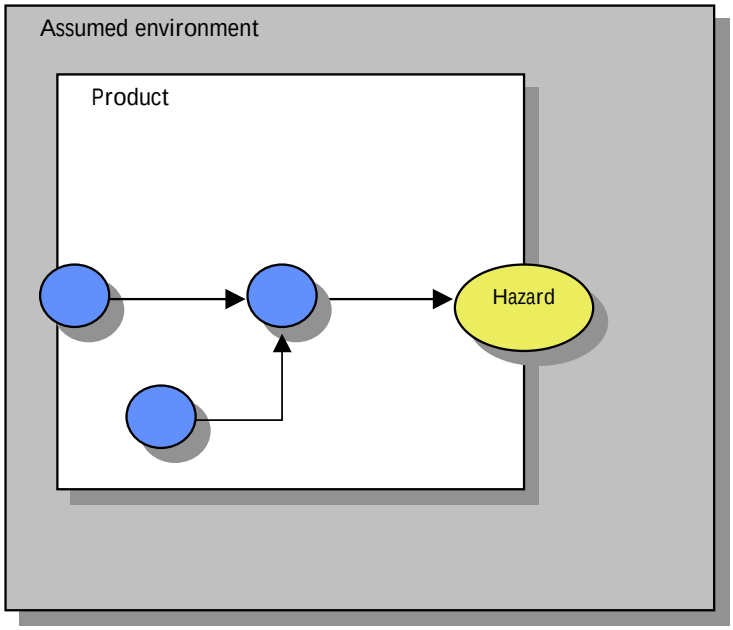

Figure 7-4 - Product development

7.5 Related Guidance

Chapter 6 provides guidance on the information that should be provided to suppliers, to allow them to carry out effective safety analysis.