ACCIDENT ANALYSIS AND BARRIER FUNCTIONS

Erik Hollnagel, IFE (N)

Version 1.0, February 1999

Table of Contents

ACCIDENT ANALYSIS AND BARRIER FUNCTIONS

Abstract. This report presents an analysis of the barrier concept, as it has been used in accident analysis. On the most basic level, the function of a barrier is either to **prevent** an action from taking place, or **protect** the system and the people in it from the consequences. Even though the concept of a barrier has been used in accident analysis for more than 20 years, there have only been a few attempts of formalising the concept and of developing systematic classifications of barriers. After reviewing the main prior treatments of the barrier concept, a systematic classification is proposed based on the distinction between a barrier system and a barrier function. Four different barrier systems are defined, called physical, functional, symbolic, and immaterial. The use of this classification is illustrated by several examples. The report continues by considering the relation between accidents and barrier analysis. It is proposed that a special form of event representation is used, called an accident tree. The accident tree combines the advantages of the classical fault tree with the time line. The use of the accident tree for barrier analysis is illustrated by two larger examples. Finally, the relation between the barrier concept and the error modes used by the Cognitive Reliability and Error Analysis Method (CREAM) is discussed. This leads to the need to distinguish between personal and systemic error modes, and a proposal for a revised classification is presented.

1. INTRODUCTION

The purpose of accident analysis is to look for the events and conditions that led to the final outcome, that is to find the set of probable causes (Woods et al., 1994). The outcome of the accident analysis is usually a description of one or more chains of interacting causes that are seen as constituting a satisfactory explanation. Complementary to that, the accident can also be described as a set of barriers that have failed, even though the failure of a barrier only rarely is included in the set of identified causes. A barrier, in this sense, is an obstacle, an obstruction, or a hindrance that may either (1) prevent an action from being carried out or an event from taking place, or (2) thwart or lessen the impact of the consequences. In the former case the purpose of the barrier is to make it impossible for a specific action or event to occur. In the latter case a barrier can achieve its purpose, for instance by slowing down the uncontrolled release of matter and energy, limiting the reach of the consequences or weakening them in other ways. These simple considerations suggest that it is possible to make a basic distinction between barriers that **prevent** and barriers that **protect**.

Barriers are important for the understanding and prevention of accidents in two different, but related, ways. Firstly, the very fact that an accident has taken place means that one or more barriers have failed – either because they did not serve their purpose adequately or because they were missing or dysfunctional. The search for barriers that have failed should therefore be an important part of accident analysis. Secondly, once the aetiology of an accident has been

determined and the causal pathways identified, barriers are used as a means to prevent that the same, or similar, accidents take place in the future. In order to facilitate this, the consideration of barrier functions should be a part of system design.

1.1 A Few Examples

One simple example of different types of barriers is provided by industrial robots on, e.g., a production line. Industrial robots are often surrounded by a fence or a cage, which serves the purpose of preventing people from accidentally getting too close to the robot and possibly being hit by it. (Industrial robots today have no awareness of what takes place in their surroundings, except that which has been specified as part of their function. The cage is therefore necessary to provide a physical or material barrier.) At times it may, however, be necessary to enter the cage to maintain or reprogram the robot. In such cases the act of opening the door to the cage may cause the robot to stop, either by abruptly switching off the power or by guiding it to a halt or a safe neutral position. Whereas the cage constitutes a material or physical barrier, the opening of the door constitutes a functional barrier. Finally, there may be warnings or safety rules that forbid personnel to come close to a moving robot. This would constitute an organisational barrier, i.e., a rule that may or may not be combined with the cage. This small example illustrates how several types of barriers can be applied in the same situation, and suggests that multiple barriers usually are necessary to prevent an unwanted event from taking place.

Another simple example is the railing or fence running along a road. The purpose of this barrier is to prevent cars from going off the road. The barrier, which clearly is a physical structure, is effective to the extent that it is able to withstand the impact of a car, which in turn depends on the weight and speed of the car. However, on many smaller roads the railing is replaced either by cat's eyes or posts with reflective marks placed along the road boundary. These serve - especially at night - as a way to show drivers where the edge of the road is. Although the purpose of the barrier is the same, i.e., to prevent the driver from going off the road, it is achieved in a completely different manner. Technically speaking, the barrier function is the visual Gestalt of a line or an edge, that serves as a perceptual demarcation.[1] If, therefore, the posts are too far from each other the barrier will be unable to serve its purpose since the physical barrier, the posts, are incapable withstanding the impact of a car hence preventing it from going off the road.

A third example is the launch control of an Inter-Continental Ballistic Missile (ICBM). It obviously is important that an ICBM is not launched by accident, and several barriers are therefore included in the system. Firstly, the command to launch may require independent authentication by two or more people. Secondly, the launch control has to be armed either by using separate keywords or keys. Thirdly, the launch requires the simultaneous pressing of two

[1] Note that the railing combines the perceptual demarcation and the physical hindrance. Thus if the railing cannot be seen, e.g., at night, it will only partly fulfil its function.

buttons that are too far apart for one person to reach both at the same time. This barrier is interesting because it actually combines several different barriers into one, namely physical distance, synchronisation (the need to press buttons at the same time)[2], and communication or collaboration (the need to plan to work together). Clearly, if a larger number of barriers are combined into an aggregated barrier, the less likely it is that the barrier is broken or malfunctions in other ways.

A final example is the use of Automatic Train Control (ATC) in train driving. The purpose of the ATC is to ensure that certain situations do not occur, e.g. that a train drives through a stop signal[3], or that the speed of the train is higher than allowed. This is achieved by having transponders on the track which will indicate the current conditions as the train passes by. If, for instance, the train is supposed to stop, and the train driver for some reasons fails to do so, then the ATC will take over and activate the brakes. The ATC thus serves as a barrier against a failure of the train driver, and effectively takes over the train driver's functions. Yet almost paradoxically, the train driver may also serve as a safeguard or back-up if the ATC is temporarily not functioning or if it fails. In this situation, the train driver can take over control and drive the train manually. This is a situation that is common to practically all conditions where automation is introduced as part of the control of a process.

1.2 Barriers And Accidents

The presentation of the examples has indirectly illustrated the different ways in which the term "barrier" can be used, referring to either the type or nature of a barrier, its function, its purpose, etc. In daily language the precise meaning of the single term "barrier" is, hopefully, clear from the context. For the purpose of a more systematic use, as part of accident analysis and system design, it is necessary to clarify the various meanings of the term "barrier" and to propose a more precise terminology.

Barriers, using the term in a general sense, may be characterised in several different ways. One is with regard to their temporal relation to an actual or hypothetical accident. Barriers that are intended to work **before** a specific initiating event takes place, serve as a means of **prevention**. Such barriers are supposed to ensure that the accident does not happen, or at least to slow down the developments that may result in an accident (cf. Svenson, 1991). Barriers that are intended to work **after** a specific initiating event has taken place serve as means of **protection**. These barriers are supposed to shield the environment and the people in it, as well as the system itself, from the consequences of the accident. Barriers may either be **active** or **passive**.

---

[2] Strictly speaking, the need to synchronise the activation of the buttons resides in the electronics of the system, rather than in the physical spacing of the buttons. The physical distance between the buttons would, however, not be an effective barrier unless it was also necessary to press the two buttons simultaneously.

[3] This condition happens so frequently that it has given rise to a special name: Signals Passed At Danger (SPAD), e.g., Horberry et al. 1994.

If a barrier is active, it means that it entails one or more functions, the effects of which achieve the purpose of the barrier. If a barrier is passive or inactive, it means that it serves its purpose by existing rather than by actively doing something. In relation to prevention, an active barrier, such as a blinking warning light, may hinder that an action is carried out, while a passive barrier, such as wire fence, may block access to a dangerous area. In relation to protection, an active barrier, such as a sprinkler system, serves to reduce or deflect the consequences, whereas a passive barrier, such as a fire wall, contains or holds the consequences.

Consider, for instance, a nuclear power plant, where there are multiple barriers to prevent an initiating event from taking place - specifically to prevent operators from taking an incorrect course of actions. This may include features of the interface design, procedures, organisational rules, etc. The commonly most dreaded result of such an initiating event is the uncontrolled release of radioactive material following damage to the reactor core. If such a release of radioactive material takes place, then the containment building serves as a passive protective barrier, hindering the radioactive material being spread to the environment. The difference between prevention and protection is illustrated in Figure 1.

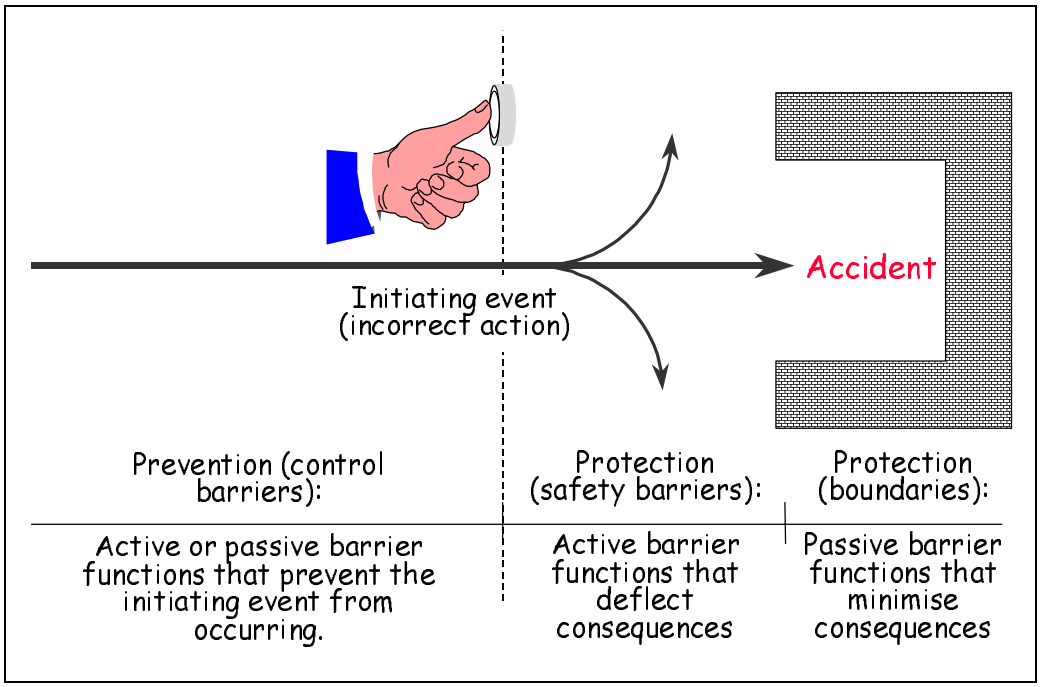

Figure 1: Prevention and protection.

This distinction between preventive and protective barriers is obviously relative to the occurrence of the initiating event. In some cases the very same barrier may therefore be either preventive or protective, depending on the point of view. To take a simple example, a door leading into a room with dangerous equipment or materials may serve as a preventive barrier in the sense that it may hinder people from entering the room, and as a protective barrier in the case of an explosion or a fire. The barrier that prevents the transportation of physical matter, i.e., the door, is, of course, the same in both cases.

2. USE AND DESCRIPTION OF BARRIERS

The notion of a barrier can be considered both in relation to a method or a set of guidelines for identifying barriers, and in relation to a way of systematically describing or classifying barriers. The two aspects are dependent, since the method for analysis necessarily must refer to a classification scheme, regardless of whether the analysis is a retroactive or a predictive one (Hollnagel, 1998). The present report mainly considers the issue of the classification scheme, with some suggestions for how it can be linked to analysis methods.

Despite the importance of barriers in accident analysis, only a small number of studies have actually studied them. The main ones are described in the following.

2.1 The Barrier Concept In Risk Analysis

Taylor (1988) provided a representative account of barriers as the concept has been applied by practitioners of risk analysis. The context was a general discussion of the techniques applicable to assess the safety of weapon systems. A barrier was straightforwardly defined as "equipment, constructions, or rules that can stop the development of an accident". The examples provided included a distinction between three types of barriers called **passive**, **active**, and **procedural**. Passive barriers, such as firewalls and distance (spatial separation), would work because of their physical characteristics and would always be ready to use. Active barriers, such as safety switches and fire extinguishing equipment, would require some kind of activation before they could be used. Finally, procedural barriers, such as instructions for use of equipment, would require a mediating agent in order to be effective. The general concept of a barrier was illustrated by a diagram similar to the representation used by the AEB model, which is described in a following section (Section 2.2).

Taylor also provided an extensive discussion of the requirements to barrier quality, as summarised by Table 1. The criteria are mixed in the sense that some of them, such as the adequacy requirements, are relevant for any kind of barrier, while others, such as the availability requirements, mainly apply to active barriers.

Table 1: Requirements to barrier quality

Quality / criterion	Specific requirement
Adequacy	Able to prevent all accidents within the design basis. Meet requirements set by appropriate standards and norms. Capacity must not be exceeded by changes to the primary system. If a barrier is inadequate, additional barriers must be established.
Availability, reliability	All necessary signals must be detectable when barrier activation is required. Active barriers must be fail-safe, and either self-testing or tested regularly. Passive barriers must be inspected routinely.
Robustness	Able to withstand extreme events, such as fire, flooding, etc. The barrier shall not be disabled by the activation of another barrier. Two barriers shall not be affected by a (single) common cause.
Specificity	The effects of activating the barrier must not lead to other accidents.

	The barrier shall not destroy that which it protects.

The classification of barriers - as passive, active, or procedural - and the pragmatic requirements to barrier quality, very much reflect the use of barriers in a proactive sense. As such it represents concerns that unarguably are significant, and which must be recognised by any serious attempt to classify barriers. The criterion of specificity is in particular interesting, since it hints at the possible negative side-effects that some types of barriers may have, for instance the undesired effects of automation, such as de-skilling or complacency. Despite the obvious value of this line of work it has, unfortunately, received little attention outside the field of risk analysis, and the impact has therefore been less than deserved.

2.2 The AEB Model

In terms of basic principles for classification, Svenson (1991) described the evolution leading to an accident as a chain or sequence of failures, malfunctions, and errors. Referring to this, a distinction was made between barrier functions and barrier systems.

> "A barrier function represents a *function* (and not, e.g., an object) which can arrest the accident evolution so that the next event in the chain is never realized. *Barrier systems* are those maintaining the barrier function. Such systems may be an operator, an instruction, a physical separation, an emergency control system, and other safety-related systems, components, and human factors-organizational units."
>
> (Svenson, 1991,p. 501)

More generally, a **barrier function** can be defined as the specific manner by which the barrier achieves its purpose, whereas a **barrier system** can be defined as the foundation or substratum (or embodiment) for the barrier function, i.e., the organisational and/or physical structure without which the barrier function could not be accomplished.[4] The use of the barrier concept should be based on a systematic description of various types of barrier systems and barrier functions, for instance as a classification system. This will help to identify specific barrier systems and barrier functions and to understand the role of barriers, in either meaning, in the history of an accident.[5]

The distinction between barrier systems and barrier functions was used as the basis for a general Accident Evolution and Barrier Function (AEB) model (Svenson, 1991). This model

[4] Compared to the system analytic distinction between "why", "what", and "how", the "why" corresponds to the purpose of the barrier, the "what" to the barrier function, and the "how" to the barrier system.

[5] In daily language the use of the term "barrier" is largely synonymous with the notion of a barrier function. This practice will be continued throughout this report.

represented the development of an accident as a sequence of steps belonging to either the human factors / organisational system or the technical system, cf. Figure 2. Each step represents either, (1) the failure or malfunction of a component or, (2) an incorrectly performed function within each system, and the barrier functions are used to indicate how the development of the accident could be arrested. (In Figure 2 barrier functions are shown as two parallel lines "//".)

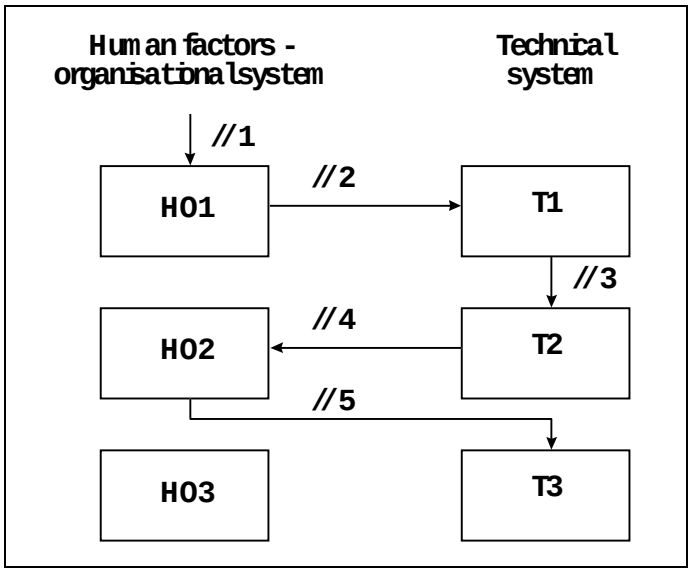

Figure 2: The Accident Evolution and Barrier (AEB) function model

The AEB model proposed three different barrier systems, namely physical, technical, and human factors/organisational (Svenson, 1991, p. 501). Barrier functions were discussed in relation to a specific incident, but there was no proposal for a systematic classification of functions. The paper did, however, include an interesting discussion of the factors that may affect the strength of barrier functions, similar to the discussion of robustness by Taylor (1988).

Using the concepts of the AEB model, an extensive study looked for the barriers that existed in a given system (the refuelling process in a nuclear power plant) and analysed the reliability of the existing barrier functions (Kecklund et al., 1996). In the analysis of the refuelling process, a considerable number of barriers were found. It was proposed that the barriers could be assigned to one of the following three groups: human, technical, and human/organisational. (Note that this differs from the barrier systems proposed by Svenson, 1991.) An example of a human barrier would be that an operator should check the condition of a system or device before using it. An example of a technical barrier would be that two systems should be aligned before a process could be started, for instance in terms of a mechanical interlock. Finally, an example of a human/organisational barrier would be the issuing of a work order or work permit.

Despite the relatively large number of specific barriers found in this study, they only represented a few categories - or, in the terminology used here, they represented a small

number of barrier functions. Thus, human barrier functions were all related to visual inspection or checking of the conditions of the system, or device, to be used. In these cases the human barrier functions served to prevent a technical failure. The study identified two types of barrier functions related to the technical system: (1) the lack of indication that two systems were locked, and (2) the blocking of the manoeuvre of one piece of equipment by the incorrect position of another. These were seen as technical barrier functions that prevented human failures. (The first can also be described as a lack of signal – due to the absence of a pre-condition, and the second as a physical obstruction.) Finally, three human/organisational barriers were identified: (1) permission to work, (2) check of information consistency between two persons, and (3) an administratively forbidden zone.

2.3 Barriers And MORT

Another study of barriers is found in the work on barrier analysis related to the Management Oversight and Risk Tree (MORT) programme. The MORT approach (cf. Knox & Eicher, 1983) describes a technique for a comprehensive investigation of occupational accidents as well as a technique to analyse safety programmes. The MORT approach is based on the use of a formal decision tree that integrates a wide variety of safety concerns in a systematic fashion. The MORT chart describes, in an orderly manner, all the potential causal factors for the accidents that can occur in a system. An important part of this is obviously the relation between energy transportation (or energy releases) and barriers.

The MORT barrier analysis (Trost & Nertney, 1985) makes a distinction between control barriers and safety barriers. The difference is that the control barriers relate to the wanted or intended energy flows, whereas the safety barriers relate to the unwanted or unintended energy flows.

- Examples of **control barriers** are: conductors; approved work methods; job training; disconnection switches; pressure vessels; etc.

- Examples of **safety barriers** are: protective equipment; guard-rails; safety training; work protection code; emergency contingency plans; etc.

Control and safety barriers do not match precisely the categories of barrier systems and barrier functions proposed above, but rather seem to describe the purpose or objective of a barrier. Control barriers can also be thought of as **facilitators**, i.e., means by which correct functions and actions can be ensured. Facilitating the correct functions is, of course, a way of preventing the incorrect function from occurring.[6]

[6] In addition to the distinction between preventive and protective barriers, one may also consider the function of facilitators as a way of encouraging the correct actions, hence as a barrier against incorrect actions. This is important in a discussion of the proactive use of barriers in system design, but will not be part of the present report.

In terms of the elimination of hazards in a system, MORT lists four approaches in order of importance. These are: (1) elimination through design; (2) installation of appropriate safety devices (barriers); (3) installation of warning devices (alarms); (4) development of special procedures to handle the situation. This ordering seems to reflect the different nature of the barriers, i.e., the degree to which they are material or organisational. This issue is discussed further below.

Corresponding to the discussion above (cf. Figure 1), MORT makes a distinction between three different barrier purposes, which are called **prevention**, **control**, and **minimisation**. This reflects a temporal view of systems and accidents, in the sense that the preventive barriers are present in the system independent of the task, control barriers work as part of the task (cf. above), and minimisation barriers work after the incident or accident. The latter category thus corresponds to the notion of protective barriers described in Figure 1.

MORT also proposes a distinction between several different types of barriers. These are: (1) physical barriers; (2) equipment design; (3) warning devices; (4) procedures / work processes; (5) knowledge and skills; and (6) supervision. This is more elaborate than the three-way distinction by Svenson (1991) and Kecklund et al. (1996) into human, technical, and human/organisational barriers. There is, however, a clear mapping between the two proposals. Of the three barrier systems defined by the AEB model, the technical barriers correspond to types 1-3 in MORT, the human barrier corresponds to type 6, and the human/organisational barrier corresponds to types 4 & 5. The notion of a barrier type in MORT therefore seems to correspond to the notion of a barrier function in the AEB model.

Finally, the MORT barrier analysis also discusses how barriers may be unable to achieve their purpose, either because they fail as such or because of other reasons. It is pointed out that barriers can be impractical, that they can fail outright, or that they can be overlooked or ignored. Altogether, the essence of the MORT barrier analysis can be summarised as shown in Figure 3.

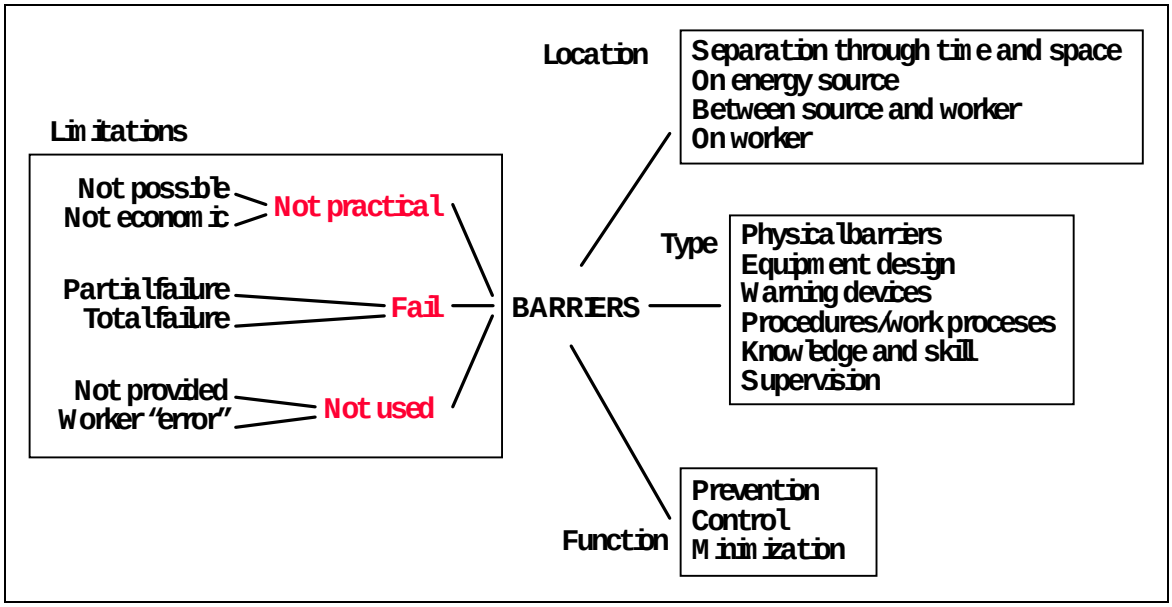

Figure 3: Summary of MORT barrier analysis.

2.4 Barriers In Software Systems

A more recent discussion of the barrier concept has been provided by Nancy Leveson, in her book on safeware (Leveson, 1995). In the later parts of the book, the issue of hazard reduction is described, and three main approaches are presented: controllability, barriers, and failure minimisation. These are the same terms used by the MORT approach, although they are used to describe different types of barriers. Compared to MORT, Leveson therefore seems to be using the concept of barriers in a somewhat narrower sense. The difference may be due to the fact that MORT was developed to analyse hazards and barriers related in systems with energy flows, whereas Leveson discusses barriers in relation to software systems mostly.

According to Leveson, a distinction can be made between three types of barriers called lockout, lockin, and interlock, respectively. A **lockout** "prevents a dangerous event from occurring or prevents someone or something from entering a dangerous area or state" (Leveson, 1995, p. 422). A lockout is thus a kind of shield or defence, which either prevents a specific initiating event from taking place, or prevents an agent from getting into the system. One example is the ways to shield a system from electromagnetic interference (EMI). This can happen either by reducing the source of the EMI, by separating the target system from the source, or by establishing a barrier, such as an interference filter, around the target system. Another example is the concept of authority limitation, which is a lockout that can prevent specific actions from being carried out. An example of that is the different access rights that may exist for a system, often implemented by means of passwords or other types of access codes.

A **lockin** is defined as something that maintains a condition, or preserves a system state. A lockin can be physical, such as walls, doors, cages, safety belts, containers, etc. They can also

be functional in the sense that they maintain a specific system state or condition. The classical example of that is Watt's governor, which served to maintain a constant speed of rotation; more generally a lockin can be seen as a feedback controlled device that can maintain a desired system state.

Finally, an **interlock** serves "to enforce correct sequencing or to isolate two events in time" (Leveson, 1995, p. 426). An interlock can work by inhibiting (or preventing) an event from occurring by establishing a set of either pre-conditions or execution conditions. An example of a pre-condition is that it may only be possible to start the engine of a car with automatic transmission if the gear selector is in the "Park" position. An example of an execution condition is the "deadman" button in trains. An interlock can also work by enforcing a certain sequence of actions or events, although in principle this is functionally equivalent to defining a pre-condition for an action. Interlocks are common on many systems, and may be implemented either by hardware or, increasingly, by software.

The barrier types used by Leveson (1995) can be seen as derived from the limiting and protecting functions that commonly are used in process automation. These are: interlocks, defined as above; controllers or lockins; limiters, which ensure that predefined standard operating values are not exceeded; protections, which ensure that predefined safety critical values are not exceeded; and finally programmes, which can be regarded as interlocks but for more complex functions or systems. In designing process automation these functions are usually thought of as a way to ensure a specific performance, rather than as barriers, but the two points of view are obviously complementary.

Compared to the approaches to barrier analysis described above, Leveson mainly describes different types of barrier functions. This may be because the domain is systems which include or a based on software. It is natural in such cases to be concerned with preventive rather than protective barriers, and to focus on barrier functions rather than barrier systems since it is the transportation of information, rather than mass or energy, that is the greatest concern.

2.5 Barriers And Latent Failure Conditions

The notion of a barrier also plays a role in the analysis and explanation of organisational accidents. It is a common finding that accidents in complex systems can de described as a combination of active failures and latent failure conditions (Reason, 1995; 1997). The defining feature of **latent failure conditions** is that they are present within the system well before the onset of a recognisable accident sequence. The influence of latent failure conditions in complex well-defended, low-risk, high-hazard systems, such as nuclear power plants, chemical process plants, modern aircraft, etc., gives rise to multiple-failure accidents that have their remediable root causes in basic organisational processes such as design, construction, procedures, maintenance, training, communication, human-machine interfaces and the like (Reason, 1992). Latent failure conditions are seen in contrast to active failures which are the local triggering events that usually are accepted as the immediate causes of an accident.

Latent failure conditions can have several different causes such as organisational or managerial decisions, design failures or deficiencies, maintenance failures or deficiencies, and slow degradation of system functions or resources (e.g. corrosion, small leaks) which are undetected. Latent failure conditions typically belong to one of the following three categories: lack of barriers, lack of resources, and precarious conditions. **Lack of barriers** means that a designed prevention against an accident either is not functional. **Lack of resources** means that the necessary means to counter or neutralise an event are missing. A simple example is that the spare tyre may be flat; a more complex one is that there may be insufficient power to start the emergency diesels or power emergency lights. Finally, **precarious conditions** means that parts of the system have become unstable so that only a small active failure is needed to release the latent condition; the analogy is that of an avalanche or any other supercritical system. Figure 4 illustrates how barriers can be affected by latent failure conditions (cf. Reason, 1995).

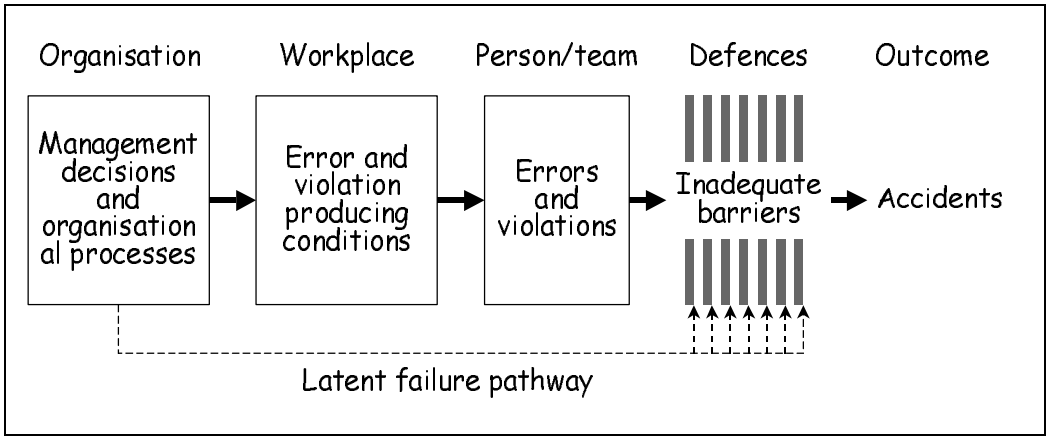

Figure 4: A model of organisational accident causation.

In this usage of the barrier concept, the lack of a barrier corresponds completely to the notion of a preventive barrier as it is generally used, whereas the lack of resources in some cases may correspond to the notion of a protective barrier. For instance, if the water pressure is too low in a sprinkler system, then the protective barrier against a fire is effectively lost. In the case of preventive barriers a further distinction is made between physical barriers and functional barriers such as procedures and rules. There is, however, no further attempt to characterise and classify barriers in more detail.

It is possible to extend the concept of a latent system condition to include, for instance, a lack of appropriate training. The ability of the people in a system to respond appropriately to a situation is crucial, whether they are operators, maintenance staff, or management. In the case of an unexpected incident or a disturbance, the ability to respond appropriately may be the most important barrier against worsened consequences. The lack of adequate training may be seen as a latent system condition which weakens a barrier, even though it may not be reasonable to see it as a latent failure condition. The reason for this is that it may be neither possible nor reasonable to attribute the latent condition to an identifiable event or decision. This becomes even more obvious if one considers more intangible conditions such as the age profile of the staff in an organisation. The knowledge and experience of the staff may be

considered a barrier in some sense, and this barrier may be lost if a large proportion of the experienced staff retires without being replaced. The aging of a population of operators may thus result in a precarious system condition.

In general, latent conditions are important for the availability and reliability of active barriers, such as in the defence-in-depth principle. A discussion of the difference between latent system conditions and latent failure conditions is clearly interesting but will not be pursued here, since it will take us too far away from the more concrete notion of a barrier that was the starting point.

2.6 Barriers And Field Theory

Outside the field of accidents and risks the concept of a barrier has been used by Kurt Lewin as part of his field theory. Lewin (1951; org. 1942) discussed how learning can be described in terms of various forces and how, for instance, punishment as a repelling force is effective only if there is a barrier strong enough to prevent the individual from leaving the field. Even though the context was entirely different from that of the present paper, barriers were used with the same meaning, i.e., as something that prevents an action from taking place.

3. CLASSIFICATION OF BARRIERS

The descriptions above have shown how an analytical description of barriers can be based on several different concepts, such as their origin, their purpose, their location, and their nature. Each of these are considered separately in the following.

3.1 Classification Based On The Origin Of Barrier

In terms of their origin, barrier systems can be produced either by the organisation or the individual. (Conceivably, a physical barrier system may also come about by an act of nature, such as the Great Barrier reef, although this is hardly the outcome of an intention. It is also possible that a barrier function may be generated by an artefact, provided it contains a reasonable level of intelligence. We will, however, refrain from further speculations in this direction.) It is nevertheless the exception that barrier functions or barrier systems are created by an individual *qua* individual, except during abnormal conditions, emergencies, etc. Since barriers should reflect a systematic and comprehensive analysis of risks and weaknesses in the system as a whole and be able to serve their purpose in a representative range of conditions, it is unlikely that they will be based on the transitory needs and intentions of an individual.[7] In

[7] If individuals feel compelled to introduce barriers for normal working conditions it is usually an indication that the organisation does not function adequately. It may nevertheless happen in fluctuating environments, such as construction sites.

any case, since the notion of the origin of a barrier system is limited to very few categories, it is not considered an appropriate basis for a comprehensive classification system.

3.2 Classification Based On Purpose Of Barrier

It has already been mentioned that barriers may serve several different purposes, e.g., being preventive, controlling, protective or minimising. Kecklund et al. (1996) discussed how a barrier may serve to prevent a human failure, i.e., an incorrectly performed action by a human, or a technical failure. Another example is the ubiquitous confirmation dialogue box that is part and parcel of the Windows interface. The dialogue box is a barrier to prevent people from making elementary mistakes, such as deleting the wrong file or neglecting to save a piece of work. The MORT approach also identified three different purposes of a barrier. The purpose of a barrier system or function may, however, be relative to the onset of the accident or event, and is therefore not the best criterion to use as the basis for a categorisation.

3.3 Classification Based On Barrier Location

In the barrier analysis that is part of the MORT technique (Trost & Nertney, 1985), a distinction is made between where in the system a barrier is located.[8] According to this, a barrier can either be placed on the source, between the source and the worker or the exposed targets, on the worker or the target, or work by means of a separation in time or space. For example, separating in time a source of combustion from a source of ignition is a very effective barrier that may prevent a fire or an explosion. This distinction of barrier locations is, of course, only applicable to barriers that have some kind of physical reality, and is therefore not adequate as the basis for a more comprehensive classification.

3.4 Classification Based On Barrier Nature

This leaves the nature of barriers as a possible starting point for developing a categorisation. The nature of barriers is principally independent of their origin, their purpose (e.g., as preventive or protective), and their location. In terms of their nature, barrier systems can range from physical hindrances (walls, cages) to ethereal rules and laws. One approach to a classification of barrier systems could be to use the following four main categories.

- **Material, or physical, barriers**. These are barriers that physically prevent an action from being carried out or an event from taking place, hence correspond to the physical barriers in the MORT analysis. Material or physical barriers may also block or mitigate the effects of an unwanted event, cf. Figure 1. Examples of material barriers are buildings, walls, fences, railings, bars, cages, gates, containers, fire curtains, etc. A

[8] In the terminology used here, it would be the location or focus of the barrier function.

material barrier presents an actual physical hindrance for the action or event in question and although it may not prevent it under all circumstances, it will at least slow it down or delay it. A material barrier can withstand forces up to a certain maximum beyond which it is no longer effective. A door or a wall may be broken down, a dike may be flooded, a container may burst, etc. Another characteristic of material barriers is that they do not have to be perceived or interpreted by the acting agent in order to work.[9] They can therefore be used for energy and material, as well as people.

- **Functional (active or dynamic) barriers**. A functional barrier works by impeding the action to be carried out, for instance by establishing an interlock, either logical or temporal (cf. Leveson, 1995). A functional barrier effectively sets up one or more pre-conditions that have to be met before the action can be carried out. These pre-conditions need not be interpreted by a human, but may be interrogated or sensed by the system itself, for instance an automatic safety device such as an airbag. A functional barrier may therefore not always be visible or discernible, although its presence often is indicated to the user in one way or another, and although it may require one or more actions to be overcome. A lock, for instance, is a functional barrier, whether it is a physical lock that requires the use of a key or a logical lock that requires some kind of password or identification. Functional barriers correspond to the categories of equipment design and supervision proposed by the MORT analysis.

  Although a functional barrier often sets up a pre-condition, it is not generally the case that all pre-conditions are barriers. It is, for instance, a pre-condition for starting a car engine that the battery is charged, but it would be an improper use of the terminology to say that an uncharged battery is a barrier against driving. A pre-condition, such as a low battery charge, may be an obstacle to a normal function, without being a barrier to an abnormal function. This issue is raised again below in the discussion of the relation between barriers and communication.

  Note also that there is an important difference between a functional barrier and a barrier function. A functional barrier is a type of barrier system, and represents the set of barrier functions that are of the same nature. A barrier function is the specific manner by which the barrier system achieves its purpose, and this mode of description can therefore be applied to all possible barrier systems.

- **Symbolic barriers**. The defining characteristic of a symbolic barrier is that it requires an act of interpretation in order to achieve its purpose, hence an "intelligent" agent of some kind that can react or respond to the barrier. Alternative terms may therefore be conceptual or perceptual barriers. Whereas the railing along a road is both a physical and a symbolic barrier, the reflective posts or markers are only a symbolic barrier: they indicate where the edge of the road is, but unlike the railing they are insufficient to prevent a car from going off the road. All kinds of signs and signals are symbolic

[9] This can be testified by anyone who have walked into a glass door.

barriers, specifically visual and auditory signals. The same goes for warnings (by text or by symbol), warnings devices (cf. the MORT typology), interface layout, information presented on the interface, visual demarcations, etc.

Whereas a functional barrier works by establishing an actual pre-condition that must be met by the system, or the user, before further actions can be carried out, a symbolic barrier indicates a limitation on performance that may be disregarded or neglected. The indication of maximum speed on a sign is a symbolic barrier, but the automatic breaking activated by the ATC if the signal is missed, is a functional barrier. Even though a functional barrier may include a pre-condition, that pre-condition need not be interpreted in the same sense as a symbol does.

- **Immaterial barriers**. The final class of barriers are the immaterial ones. This means that the barrier is not physically present or represented in the situation, but that it depends on the knowledge of the user in order to achieve its purpose. Immaterial barriers are usually also represented in a physical form such as a book or a memorandum, but are often not physically present when their use is mandated. Typical immaterial barriers are: rules, guidelines, safety principles (safety culture), restrictions, and laws. In industrial contexts, immaterial barriers are largely synonymous with organisational barriers, i.e., rules for actions that are imposed by the organisation, rather than being physically, functionally or symbolically present in the system. Immaterial barriers correspond to the MORT types of procedures / work processes, knowledge and skills.

It is clearly possible to realise several barrier systems and functions in the same physical artefact or object. For instance, a door may have on it a written warning and may require a key to be opened. Here the door is a physical barrier system, the written warning is a symbolic barrier system, and the lock requiring a key is a functional barrier system. It may, in fact, be the rule rather than the exception that several different barrier systems and functions are used together to achieve a common purpose.

3.5 A Classification Of Barriers

The following Table 2, presents a classification of the barriers that are commonly found in the general literature. Each barrier is described with regard to the underlying barrier **system**, i.e., one of the four main classes as defined above, and the specific barrier **function** (or **mode**), i.e., the more specific nature of the barrier. The list of barriers presented here is unlikely to be exhaustive, but hopefully sufficiently extensive to be of some practical use.

Table 2: Barrier systems and barrier functions.

Barrier system	Barrier function	Example
Material, physical	***Containing*** or protecting. Physical obstacle, either to prevent transporting something **from** the present location (e.g., release) or **into** present location (penetration).	Walls, doors, buildings, restricted physical access, railings, fences, filters, containers, tanks, valves, rectifiers, etc.
	Restraining or preventing movement or transportation.	Safety belts, harnesses, fences, cages, restricted physical movements, spatial distance (gulfs, gaps), etc.
	Keeping together. Cohesion, resilience, indestructibility	Components that do not break or fracture easily, e.g. safety glass.
	Dissipating energy, protecting, quenching, extinguishing	Air bags, crumble zones, sprinklers, scrubbers, filters, etc.
Functional	***Preventing*** movement or action (*mechanical, hard*)	Locks, equipment alignment, physical interlocking, equipment match, brakes, etc.
	Preventing movement or action (*logical, soft*)	Passwords, entry codes, action sequences, pre-conditions, physiological matching (iris, fingerprint, alcohol level), etc.
	Hindering or impeding actions (spatio-temporal)	Distance (too far for a single person to reach), persistence (dead-man-button), delays, synchronisation, etc.
Symbolic	***Countering,*** preventing or thwarting actions (visual, tactile interface design)	Coding of functions (colour, shape, spatial layout), demarcations, labels & warnings (static), etc. *Facilitating correct actions may be as effective as countering incorrect actions.*
	Regulating actions	Instructions, procedures, precautions / conditions, dialogues, etc.
	Indicating system status or condition (signs, signals and symbols)	Signs (e.g., traffic signs), signals (visual, auditory), warnings, alarms, etc.
	Permission or authorisation (or the lack thereof)	Work permit, work order.
	Communication, interpersonal dependency	Clearance, approval, (on-line or off-line), in the sense that the lack of clearance etc., is a barrier.
Immaterial	***Monitoring***, supervision	Check (by oneself or another a.k.a. visual inspection), checklists, alarms (dynamic), etc.
	Prescribing: rules, laws, guidelines, prohibitions	Rules, restrictions, laws (all either conditional or unconditional), ethics, etc.

The classification of barriers is not always a simple matter. A wall is, of course, an example of a physical barrier system and a law is an example of an immaterial barrier system. But what about something like a procedure? A procedure by itself is an instruction for how to do something, hence not primarily a barrier (except in the sense that performing the right actions rules out performing the incorrect ones, cf. the notion of facilitation). Procedures may, however, include warnings and cautions, as well as conditional actions (pre-conditions). Although the procedure may exist as a physical document, other formats are also possible, such as computerised procedures. The procedure therefore works by virtue of its contents or

meaning rather than by virtue of its physical characteristics. The warnings, cautions, and conditions of a procedure are therefore classified as examples of a symbolic barrier system, i.e., they require an act of interpretation in order to work.

Immaterial barriers are often complemented by symbolic barriers. For instance, general speed limits as given by the traffic laws are supplemented by road signs (a symbolic barrier system) and at times enforced by traffic police (performing the immaterial monitoring function, perhaps supplemented by physical barriers such as road blocks or speed bumps). Material barriers may also be complemented by symbolic barriers to encourage their use. Seat belts are material barriers, but can only serve their purpose if they are actually used. In commercial aeroplanes, the use of the seat belt is supported by both static cautions (text, icons) and dynamic signals (seat belt sign), as well as verbal instructions, demonstrations, and visual inspection. In private cars the material barrier is normally only supported by the immaterial barrier, i.e., the traffic laws, although some models of cars also have a warning signal. On the whole, the result is less than satisfactory, especially since the use of a safety belt seems to be influenced by cultural norms as well.

3.6 Humans As Barriers

Humans are in many ways a special type of barrier, although it is not necessary to go so far as considering humans as a barrier in its own right. Humans can, for instance, constitute a physical barrier, as in the case of a doorman at a night club or a phalanx of police (appropriately described as a human wall). Humans can also be a functional barrier, e.g. a sentry requiring a password. In the case of symbolic barriers, humans can in some cases serve as symbols, as e.g. a traffic policeman. Other examples may be found in myths and legends. Humans are, of course, always required to interpret the barrier and to carry out or guide the appropriate response. Finally, humans are also needed to effectuate the immaterial barriers since these, by definition, must exist in the minds of the people they are supposed to affect.[10] One might go so far as to say that except for physical barriers and some functional barriers, humans are necessary for the purpose of the barrier to be accomplished. Specifically, humans - as individuals or as organisations - are a fundamental part of understanding how barriers can fail.

3.7 Social Barriers

New section?

[10] It might also be suggested that humans can be immaterial barriers, e.g., as the father figure in psychoanalysis. It is arguable, however, whether this is not really a symbolic barrier, and in any case it is of limited practical value for accident analysis and barrier design.

3.8 The Examples Revisited

The examples given in Section 1.1 can be used to illustrate the principles of the classification described above.

- The cage around an industrial robots is a physical barrier system that contains the robot and prevents people from coming near it. The door in the cage is also a physical barrier, and has the same purpose. The lock on the door, which stops the robot when the door is opened, is a functional barrier system and the function is to prevent the robot from moving. (The lock is a lockout in the terminology used by Leveson, 1995.) Finally, the safety rules that forbids personnel to come close to a moving robot constitute an immaterial barrier. The safety rule may be supported by a symbolic barrier, such as a written warning or a sign, or a painted separation line on the floor.

- The railing or fence running along a road is a physical barrier system that restrains the cars and stops them from going off the road (provided the cars do not go too fast or are too heavy). Since seeing or observing the railing is used by car drivers to stay on the road, the railing is also a symbolic barrier system. On roads where the railing is replaced by posts or markers, these represent a symbolic but not a material barrier system, although the function (preventing) is the same.

- The design of the launch control of an Inter-Continental Ballistic Missile include several barrier systems and functions. The rules for authorisation of the launch command represent an immaterial barrier system (monitoring), whereas the authorisation code itself represents both a functional barrier system (preventing) and a symbolic one (permission). The need to use separate keywords or keys represents a functional barrier system that prevents an action. The spatial separation of the firing or launch buttons represents a material or physical barrier that also prevents an action from taking place. Note, however, that this is only effective because two actions must occur simultaneously. The need of synchronisation represents a functional barrier system and the barrier function is that of prevention.

- In the case of the automatic train control system, the ATC itself is a functional barrier system that serves, e.g., to prevent the movement of the train. (In addition, the ATC also serves as a symbolic barrier system, since it provides the train driver with information about the current constraints on driving and the status of signals.) As mentioned in the example, the driver also serves as a functional barrier system for the ATC, since the driver is expected to be able to control the train manually should the ATC temporarily be out of order or fail. An uncontrolled event therefore takes place only if both the ATC and the train driver fail to perform their function appropriately. (An example of that is provided by the Lammhult accident described below.) The situation is, however, slightly complicated because either system is supposed to serve as a barrier for the other, i.e.,

there is a reciprocal dependency, as shown in Figure 5.[11] This is a type of relation that may potentially lead to problems, for instance if the train driver is not aware that he is supposed to take over for the ATC. In this case both system fail at the same time, despite the best intentions behind the design.

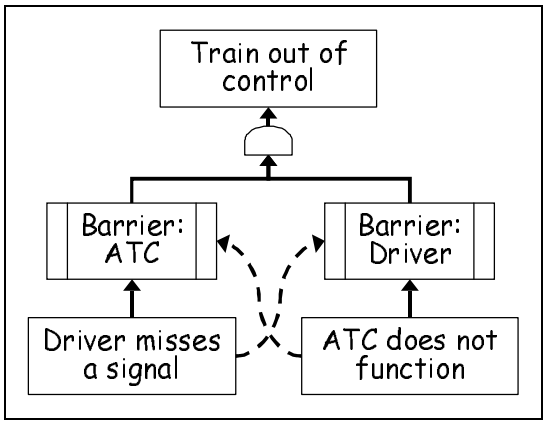

Figure 5: Reciprocal barrier dependency

The use of multiple barrier systems and functions is a way of ensuring that a single failure does not lead to an unwanted event or accident in a system. The multiple barriers may be combined in various ways, for instance according to the defence-in-depth principle These concerns, which were addressed by the requirements described by Taylor (1988), become very important when barriers are used proactively in the design of safety functions. The discussion below, however, considers another aspect, namely how to address the issue of barriers in accident analysis.

3.9 Barriers And Communication

The barrier concept is strongly associated with the flow of mass and energy, where barriers serve as a way of preventing an undesired flow from taking place. A barrier may, however, at times also be an obstacle to normal functioning, for instance in the flow of information and control. In such cases a barrier is not primarily a safety feature, but may rather contribute to the occurrence of failures and accidents.

Accidents are often due to missing information or the lack of communication. Consider, for instance, the case where an event report is produced after an accident or an incident. If the report is not properly processed and analysed, but merely filed, the organisation will be unable to make the appropriate changes, for instance by strengthening existing barriers or developing new ones. It will therefore remain vulnerable to accidents or incidents of the same type. In such cases the failure to communicate the lessons learned may be due to barriers in the system,

[11] An alternative representation would be to show a conjunction of a failure and the inverse of a barrier function.

although these barriers are hindrances or obstacles to a desired function rather than ways of preventing an undesired one. Another common example is the transmission of information from one work shift to another, where such information may either be incomplete or misunderstood. In general, if information is missing it is not because a barrier has failed, but rather because there has been one where the should not.

Although this difference in the use of barrier concept may seem paradoxical, that is really not the case. The difference is caused by a contrast in perspective, so to speak. In the case of functions relating to the flow and storage of mass and energy, barriers are considered in relation to the prevention of an unwanted flow. In the case of functions relating to the flow of communication (information) and control, barriers are considered in relation to the prevention of a desired or needed flow. In both cases, the concept of a barrier may actually be used either way. For instance, a clot of blood may prevent the normal circulation of blood, hence be an undesirable barrier. Similarly, unwanted information, such as propaganda, may be prevented by deliberately jamming the transmission. This difference in perspective may be due to the fact that mass and energy flows usually have well-defined ducts or channels in a system, and that their efficacy can easily be measured or gauged. Communication (information and control) are less easy to channel and measure and we are furthermore usually interested in the effects rather than the physical flow of bits of information as such. Yet the effects of communication are more difficult to measure than the effects of mass and energy flows, especially when something goes wrong. In the case of water leaking from a tank the laws of physics tells us that it must flow into something else. We know that the amount of mass and energy should be constant, and if we find that something is missing or unaccounted for, we rightly get worried. For communication there is nothing that corresponds in a simple manner to a constant “volume” of information or control, information theory notwithstanding (Shannon & Weaver, 1969). We may know that a message is generated and transmitted, but it is less easy to determine whether it is received or whether parts of it are lost on the way. The differences in perspective means that the search for, and classification of, barriers cannot be the same in the two cases.

4. ACCIDENTS AND BARRIER ANALYSIS

In order for a classification system to be useful, it must be closely associated to a method. This goes for a classification of barriers as well as anything else (Hollnagel, 1998). In the case of barriers, there is a actually need of three different sets of methods. One set of methods is needed for the identification of barriers in accident analysis. Another set is needed for the identification of barriers under normal circumstances, e.g., as part of a system safety survey or a risk analysis. Finally, a third set of methods is needed for the specifications of barriers for system design. Only the first will be discussed here.

For the purpose of an accident analysis, or the retroactive use of the barrier concept, barrier identification is generally carried out in a rather *ad hoc* fashion. The common practice in risk analysis is to look for know barriers - similar to the search for latent failure conditions, sneak paths, or failure modes - and this approach has simply been applied to accident analysis as well. The principal disadvantage of that is the barrier analysis in this way is carried out on its own,

rather than as an integral part of the general accident analysis method. Although risk analysis has some similarities to accident analysis, it is clearly not a complete accident analysis method by itself, since it does not address aspects such as accounting for the interaction between the various elements of the socio-technical system, or describing the common performance conditions. It is therefore necessary to find a way of incorporating a systematic classification of barriers into common accident analysis methods.

4.1 Fault Trees And Accident Trees

Since barriers relate to functions or events, a natural starting point is a description of the accident in terms of the events that, individually or in a combination, can lead to the observed outcome. Barriers must always be seen in relation to a potential flow of mass, energy, and information (or control), and it is therefore natural to base the analysis on a representation of possible sequences of functions or events such as a time-line or a flow diagram. This approach was used by Kecklund et al., 1996, to analyse the reliability of barriers in the refuelling process in a nuclear power plant. The advantage of the time-line description is that it clearly shows the order in which the events occurred. The main disadvantage is that it usually only shows a single line of action, hence makes it more difficult to see how concurrent or parallel paths came together in the accident. It is, however, entirely possible to use a representation based on multiple time-lines.

Another possibility is to base the analysis on a generic fault tree representation, such as the "anatomy of an accident" structure shown in Figure 6 (Green, 1988). This shows how an accident occurs as the result of a sequence of events and failures, where the failures easily may be interpreted as a lack of appropriate barriers.

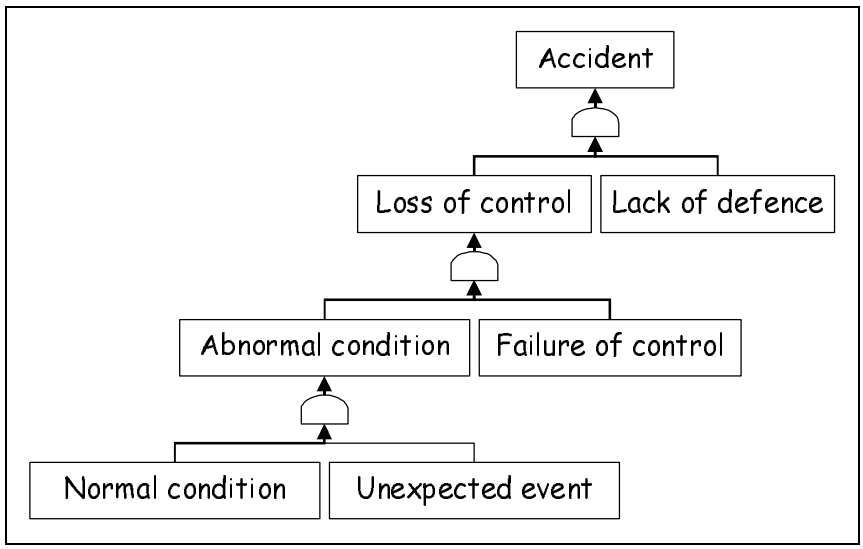

Figure 6: The "anatomy of an accident"

The fault tree is normally used as a basic technique in risk analysis for technical systems and was first proposed in 1961 (cf. Leveson, 1995). The standard approach is to start from a top

event, which in Figure 6 is denoted as the accident, and try to list all the possible conditions of faults that conceivably could lead to the top event. The search is thus a backward expansion of the fault tree from the top event (which properly speaking is the root) until all the basic events have been found. The expanded fault tree shows how individual events and failures may combine to produce the top event. The combinations can be either conjunctive (AND conditions) or disjunctive (OR conditions). Once the fault tree has been constructed possible barriers can be explored simply by considering each of the branches of the tree.

The fault tree does not necessarily indicate the temporal relation between events, such as the time-line does. Thus, in Figure 6, it is entirely possible that the "failure of control" or "lack of defence" happens prior to the occurrence of the "unexpected event". The reason for that is that the fault tree is used mostly to describe possible or hypothetical events, where the logical combination of conditions is more important than the order in which they occur. In accident analysis, the order of events is usually known in great detail, and it is therefore reasonable to include this information in the graphical representation. The outcome of an accident analysis can conveniently be represented in the form of a tree which is a combination of a fault tree and a time-line.[12] The top event is given as the accident or outcome that actually happened. The tree is simplified or reduced in the sense that it only represents the events and failures that actually happened; in contrast to that, the full fault tree shows all the possible events and failures that could lead to the (same) top event. To distinguish it from the fault tree, this representation of the outcome of the analysis can be called an **accident tree**. Most accident analysis methods, including CREAM, can easily be adjusted to show the outcome as an accident tree.

4.2 Two Examples

This section presents two examples of how an accident analysis can be combined with a description of barriers and barrier failures. The examples do not represent a completely developed methodology, but illustrate the main principles.

4.2.1 Cadarache Water Spill

As an example of an accident tree, consider the events at the French Cadarache nuclear power plant which led to the release of lightly contaminated water to the environment. The sequence of events was roughly as follows:

- Some person forgot to turn off a tap in a basin meant for rinsing eyes.
- After a while, the water in the basin overflowed and spilled into a storage tank. The tank was slowly filled up, but the overflow alarm of the tank failed.

[12] It may therefore also be considered as a specific instance of a fault tree.

- When the overflow tank became full, water spilled into a low level radiation tank. The overflow alarm of this tank also failed to work.
- As a result 10-12 m^3 of water spilled out on the floor and flowed into the sump.
- For some reason, the pump from the sump was connected to an outside rainwater tank, rather than to a tank for industrial waste. The net result was therefore that the contaminated water ended up in the wrong place.

An accident tree, as shown in Figure 7, can represent this series of events. The flow of events is shown from left to right, in accordance with the conventional way of representing time. The relative positions of the individual events show their relative temporal order, e.g., the filling up of the storage tank that creates an overflow condition precedes the failure of the tank overflow alarm. The accident tree does not indicate why the overflow alarms were out of order, as this information was not available in the description of the accident.

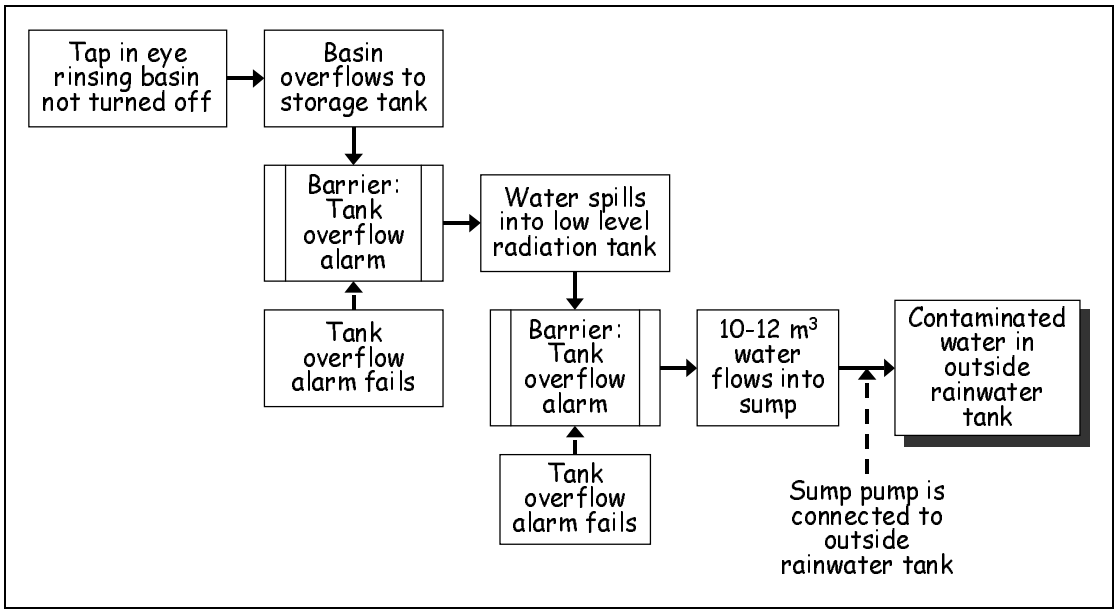

Figure 7: Accident tree for Cadarache spill.

This accident, or rather incident since it is hardly serious enough to be classified as an accident, shows the usual features of a number of functions failing at the same time. In terms of barriers, there were clearly several barriers built into the system, yet all of them failed. Going through the accident tree, the first thing that happened was that the tap for the eye rinsing basin was not turned off after use. In terms of error modes (cf. below) this can be classified as an omission of an action, which belongs to the category of "sequence" error modes in CREAM. It is thus very likely to be a failure of a symbolic barrier for regulating actions, i.e., the instruction or procedure for using the tap. Although there apparently were no functional barriers for this error mode, it is possible to suggest several. For instance, a timing device that automatically

turns off the tap after a while. Or changing the operating of the tap to require a sustained activation of, e.g., a pedal.[13]

The next two steps both involve the occurrence of an overflow condition in two tanks where in both cases the overflow alarms failed to function. Here there were functional barriers in the system, but they were not operational or available. The final step is that the pump from the sump was incorrectly connected to the outside rainwater tank. This is a latent condition rather than an event. It is shown in Figure 7 by a dotted line pointing to the path between the two events involved (water flowing into the sump and water ending up in the outside rainwater tank), rather than as an event related by a logical conjunction. Here it is again easy to suggest ways in which the occurrence of the latent condition could have been prevented, e.g. by having different fittings on the two tanks, by using colour codes or clear labels, etc.

In this case the analysis directly identified two barriers that had been broken, i.e., the failing overflow alarms. As shown in the description above it is also rather easy to suggest barriers that might have prevented the top event, although that is not the purpose of the accident analysis *per se*.

4.2.2 Lammhult Train Accident

Another, and less clear cut, example is the derailing of a train that happened at the Lammhult in Sweden in June, 1985. The contents of this incident is as follows:

- The train arrived at the station about 3 minutes too early and was directed into a side-tack to allow for the passage of another train. The signals indicated that the speed of entry into the side-track should be 40 km/h. According to the automatic registration from the train engine, the actual speed was 96-98 km/h. As a result, the last part of the train was derailed as it passed onto the side-track.

- During the following investigation, the train driver at first admitted that he had observed the signal, but that the train probably was going too fast. Later he denied having observed the signal, although acknowledging that the speed of the train was too high when it entered the side-track.

- The investigation after the incident did not reveal any malfunctioning of the signalling system. It was confirmed that the correct signal, 40 km/h had been given. It was not possible to find any mechanical defects of either the rails nor the wagons which could have caused the derailing.

- The standard speed of the train should have been 90 km/h, corresponding to the norms for the wagons carried by the train. The automatic registration from the train engine showed that the actual speed for most of the journey has been higher than 95 km/h.

[13] It would have to be a pedal, since presumably the hands were used as part of rinsing the eyes.

Apparently, the train driver mistakenly thought that the standard speed of the train was 100 km/h "as usual". The technical investigation also indicated, firstly, that the ATC system had been set with the wrong values for the train and, secondly, that it had not been engaged, despite denials from the train driver. The automatic registration showed that the emergency brakes had been activated twice, at one time leading to a full stop, although the train driver did not admit that this had happened. The activation of the emergency brakes would occur if the ATC was not engaged and the train driver "lost" the dead-man button. A re-enactment of the journey with the ATC engaged showed that the train correctly slowed down to 40 km/h when passing the signal and stopped at the station.

- Finally, it was found that the train driver did not carry the appropriate written instructions on the train (line book and order of the week).

In this case the outcome of an analysis can be shown as the "tree of causes" in Figure 8.[14] The analysis uses the concepts of error modes described in the Cognitive Reliability and Error Analysis Method (CREAM, cf. Hollnagel, 1998). As an analysis method, CREAM defines a recursive search for links between consequents (or "consequences") and antecedents (or "causes"), using a set of pre-defined groups of antecedent-consequent relations. The analysis starts by a specific event, which is described in terms of a finite set of error modes. The error modes refer to the ways in which the execution of an action can fail or go wrong, either in relation to the person acting or to the systemic consequences.

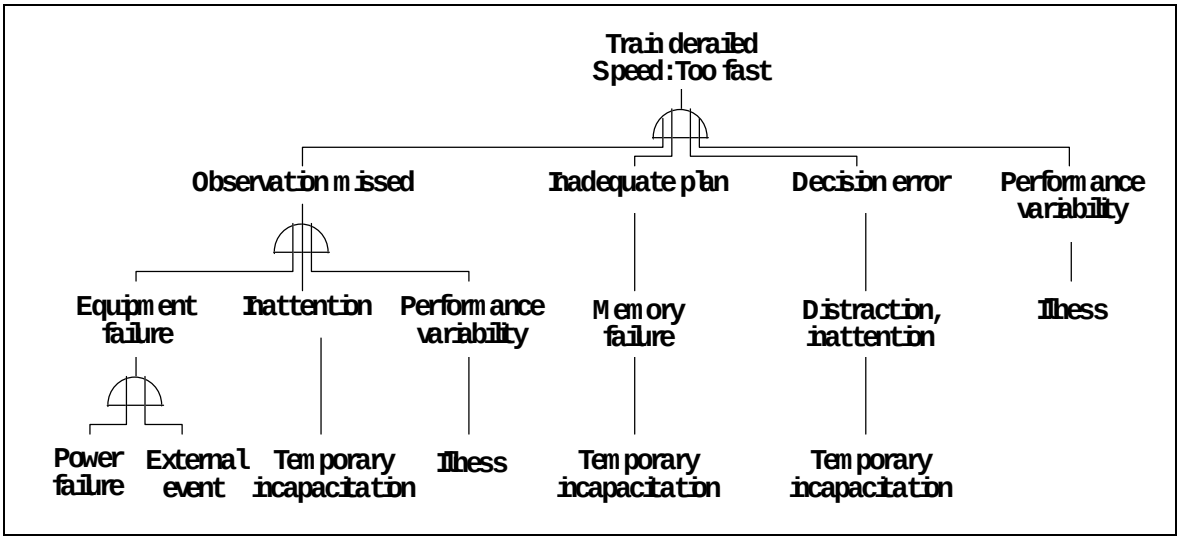

Figure 8: "Tree of causes" for the Lammhult derailing.

[14] For the sake of the example it is not critical whether the outcome of the analysis is correct, in the sense that it points to the "true" cause. The example is used only to illustrate how a barrier analysis can be combined with the accident analysis.

In Figure 8 the starting point for the analysis is the actual derailing of the train, which can be seen as corresponding to the error mode "speed: too fast".[15] According to the analysis on the first level of explanation there are four possible, and independent, ways in which this might have happened. These are: *(1) observation missed*, *(2) inadequate plan*, *(3) decision error*, and *(4) performance variability*.

Firstly, the train driver may have "missed the observation" of the signal. The evidence on that is not clear, but it was established after the accident that the signal functioned normally, even though the train driver did not respond to it as required. The continued analysis of this possibility shows that the signal could have been missed for several reasons, such as a spurious failure, because the train driver was inattentive when the train passed the signal, or because he was temporarily functioning on a subnormal level due e.g. to a passing illness. The explanation in terms of "performance variability" also occurs as the fourth possibility on the first level of analysis. The two remaining candidate possibilities are "inadequate planning" on behalf of the train driver, or a "decision error". Given the other information from the investigation, the most likely explanation seems to be in terms of inadequate planning. It appears that the train driver throughout the journey had misunderstood the conditions under which he was driving, and that he was not paying full attention to what happened around him.

In the event, the actual derailing was a combination of missing the signal and the ATC not working. Since the ATC is intended to be a functional barrier against the outcome of incorrectly performed actions, the failure of the barrier was an important contributor to the accident. In this case the barrier failed because the equipment had not been activated, which in turn can be seen as an omission that happened at an earlier point in time. Similarly, it appears from the description of the accident that the train was going too fast even at the time it reached the signal. The outcome is therefore an accident tree as shown in Figure 9. In this accident tree, the outcome of the "tree of causes" is included as the descriptions of the conditions that led to the actual events.

[15] Strictly speaking, the derailing is the final consequences, while the excessive speed is the immediately preceding cause. This can also be interpreted as the error or failure mode for the train.

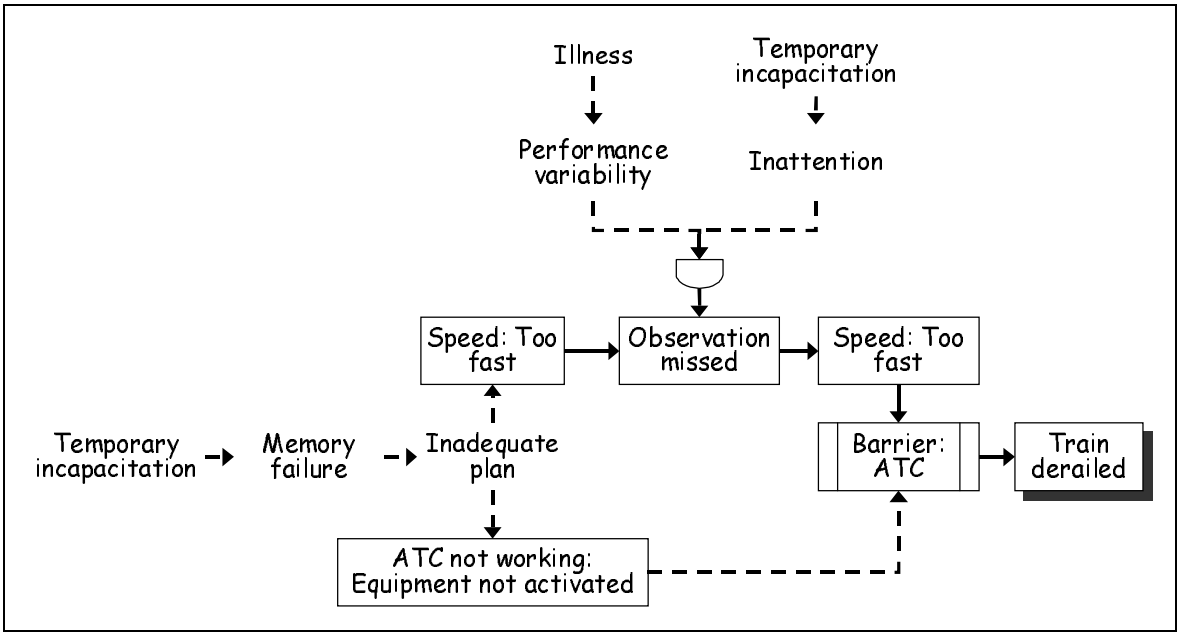

Figure 9: Accident tree for Lammhult derailing

The accident tree in Figure 9 differs from the "tree of causes" in Figure 8 in the following ways. Firstly, the main events are arranged according to their temporal relation. Secondly, the top event, the derailing, is now described as the result of the high speed followed by the failure of the functional barrier, i.e., the ATC system. The high speed, is in turn explained by the missed observation, which can be attributed to either performance variability or inattention. The reason for the ATC not working was probably that the system had not been activated, which can further be seen as the result of inadequate planning by the train driver. This inadequate planning also led to the train having too high a speed throughout the journey, hence at the time when the signal was passed. It thereby achieves the status that corresponds to a common mode error in a fault tree.

This accident typically shows that a number of functions failed at the same time. In terms of barriers, the main functional barrier built into the system is the ATC, but this failed since it had not been activated. Apparently, there were no barriers against driving the train without the ATC and no adequate facilitators for remembering to activate the ATC. The signal is an important symbolic barrier for the train driver, but as the signal was not observed it could not achieve its purpose. The signal is also part of the ATC as a functional barrier, since the signal provides the pre-condition for automatically activating the brakes. However, as the ATC was not activated, the pre-condition was not registered. Finally, there was also a failure of communication, or a breach of procedures, since the train driver had not brought the line book and order of the week with him to the train. There did, however, not seem to be any other ways in which this symbolic barrier was implemented.

4.3 Barrier Analysis And Event Trees

Just as the fault tree, and the accident tree, is the generic way of representing the outcome of a retrospective accident analysis, so the event tree is the generic representation used in risk prediction, e.g., Probabilistic Safety Assessment / Probabilistic Risk Assessment (PSA/PRA) and Human Reliability Assessment (HRA). The event tree shows the possible consequences of a specific initiating event in the form of a binary branching tree. For such event trees, barriers are uncomplicated to insert, since they are the ways in which failures can be prevented. Thus, every "failure" branch of the event tree is a potential place for one or more barrier functions. The effect of barriers on the analysis is to reduce the overall failure probabilities - or to introduce possible ways of recovering from a function failure. The event tree representation is, however, not well suited for accident analysis, and will therefore not be considered further here.

Another representation of a predictive analysis is the AEB functional model that was shown in Figure 2. The AEB model is basically a single, i.e., non-branching, sequence of actions or events, although these may be grouped to show how they relate to different main categories. The AEB model, as the event tree, is well suited for identifying barriers that may possibly prevent a specific development from taking place. It is, however, not efficient as a way of identifying barriers in an accident analysis, since it does not depict parallel or alternative event sequences as, for instance, the accident tree or the fault tree do.

5. BARRIERS, ERROR MODES, AND "ERROR CAUSES"

The analysis of barriers can either be treated as a separate step on top of a conventional accident analysis, or be included in the accident analysis. The two examples presented above basically illustrated how a barrier analysis could be used to further elucidate the outcome of an accident analysis. From a practical point of view it is preferable that the two types of analysis are combined, since the accident analysis can provide the barrier analysis with a detailed description of the events, whereas that barrier analysis quite possibly can enrich the categories used by the accident analysis.

The specific accident analysis approach considered here is CREAM (Hollnagel, 1998). This entails a recursive analysis method together with a non-hierarchical set of categories organised in a number of classification groups. The outcome of CREAM is an accident tree, as illustrated by the analysis of the derailing at Lammhult. The classification groups defines the links between specific "causes", called antecedents, and "effects", called consequents. These links are used by the recursive analysis method to generate the possible sets of events that may have led to the observed outcome.

The barrier analysis can be combined with CREAM in a rather simple manner by noting that the antecedents can be used as the starting point for defining barriers. The accident tree shown in Figure 9, contains four sequences of events, where each step is an antecedent to the one before it. Together these define 13 antecedent links, although some of them are identical. Consider, for instance, the link <Speed: too fast> ⇐ <Observation missed>, disregarding for

the moment that it is part of a conjunctive condition. If it could have been insured, that the observation of the signal had not been missed, then this link would have been impossible. The question is therefore whether it is possible to define an appropriate barrier for this antecedent link. One possibility would be to show the signal in the driver's cabin rather than along the track[16]; another to use a multi-model presentation (e.g., sound and light); a third to make the strength of the signal relative to the threshold defined by the ambient conditions (noise, illumination), etc.

For links that refer to physical or technical functions it will be relatively easy to think of appropriate barriers. For links that refer to human performance and conditions, such as most of the links in Figure 9, barriers may be more difficult to find. Consider, for instance, the link <Inadequate plan> ⇐ <Memory failure>; since the occurrence of a memory failure may depend on a host of conditions and other events, it is not easy to suggest an effective barrier. Neither is it reasonable to say that any specific barrier has failed in this case. An alternative approach would therefore be to consider how the system could be modified or redesigned so that this specific link did not play so important a role. That would, however, take us into the area of accident prevention, and therefore not be discussed here.

The accident tree in Figure 9 includes three pairs of logical links or combinations, two being conjunctive and one disjunctive. Disjunctive links show multiple ways in which a specific "effect" or consequent can come about and therefore indicate points of vulnerability, hence also points where barriers may be considered. The presence of a disjunctive link is, however, not itself an indication of a broken barrier. Conjunctive links, on the other hand, are good indicators of barriers that have failed, and may directly refer to barriers that are part of the system design. In Figure 9, the link <Observation missed> ∧ <Inadequate plan>, points to a non-technical failure, where either component constitutes a barrier against a failure of the other one. It is, for instance, conceivable that the speed would not have been too high if the train driver had adequately planned the journey, despite missing the observation of the signal; or conversely, if he had observed the signal, despite having an inadequate plan. In this case the train driver did not follow the correct procedure, hence broke a symbolic barrier.

The other conjunctive link in the analysis of the Lammhult derailing is [<Observation missed> ∧ <Inadequate plan>] ∧ <ATC not activated>. Here the second component is a technical barrier that is part of the safety system design, and the analysis therefore directly points to a failure of this barrier to function. The proposed classification may be used to describe the barrier more specifically as a preventive barrier function in a functional barrier system, cf. Table 2. This barrier did not fail because the specific pre-condition was missing (e.g., the signal from the ATC beacon), but because a general pre-condition had not been met, i.e., that the ATC system had been activated. The analysis this suggests that it might be worthwhile to consider this condition further - given, of course, that this type of accident occurs frequently enough to justify the efforts and resources needed.

---

[16] In practice this is achieved via the ATC, although the presentation is not analogous to the actual signal. In the present case this solution was ineffective because the ATC had not been activated.

5.1 Barriers And Error Modes

The analysis of the barriers for the Lammhult example suggests that the barrier analysis is based on the accident tree that results from the accident analysis, and that this is done during the accident analysis rather than afterwards. The advantage of that is that the barrier analysis may improve the precision of the accident analysis, and point to possible critical links. In practical terms, the barrier classification should be combined with the classification groups of CREAM, probably as an additional category (i.e., in addition to antecedents and consequents).

Another change of CREAM may be to combine the barrier concept with the notion of error modes. CREAM contains eight basic error modes for human actions, where each specific error mode can be interpreted as the breaking of a barrier. However, in analysing accidents it is recommended to start from the manifestations on the level of system functioning rather than on the level of human performance. In Figure 9, for instance, the manifestation is "speed to high" which may be due to the failure of a human function or to the failure of a technical function, hence the possible failure of a technical barrier. It is therefore necessary to consider whether the eight basic error modes need to be extended to be fully able to characterise the performance (failures) of the joint system. The outcome of this consideration is shown in Table 3.

Table 3: Human and systemic error modes.

	Human error mode	**Systemic error mode**
Timing	Action performed too early or too late	Position reached too early or too late. Equipment not working as required.
Duration	Action performed too briefly or for too long	Function performed too briefly or for too long. System state achieved too briefly or held for too long
Distance	Object/control moved too short or too far	System or object transported too short or too far
Speed	Action performed too slowly or too fast	System moving too slowly or too fast Equipment not working as required.
Direction	Action performed in the wrong direction	System or object (mass) moving in the wrong direction
Force / power / pressure	Action performed with too little or too much force.	System exerting too little or too much force. Equipment not working as required.
		System or component having too little or too much pressure or power.
Object	Action performed on wrong object	Function targeted at wrong object
Sequence	Two or more actions performed in the wrong order,	Two or more functions performed in the wrong order,
Quantity and volume	None	System/object contains too little or too much or is too light or too heavy.

As shown by Table 3, all the eight error modes defined for human functions can be applied to system functions or systems states by reformulating the definitions (third column). Note that in three cases (referring to timing, speed, and force) a new error mode has been added, called

"equipment not working as required". The use of that has already been illustrated in the analysis of the Lammhult accident. It was also found necessary to introduce a ninth error mode referring to discrepancies in mass and volume, which is only applicable to system functions or states. The reason for this is that the primary function of a system often is to transport mass and energy (or information), and that incorrect quantity and volume therefore are highly relevant error modes.

6. CONCLUSION

This report has presented an overview of the barrier concept as it has been applied by different fields and by various researchers and practitioners. A number of specific proposals for classifications of barriers have been outlined, and based on these a specific classification has been described. The classification makes a distinction between barrier functions and barrier systems. A barrier function is defined as the specific manner by which the barrier achieves its purpose, whereas a barrier system is defined as the foundation or substratum (or embodiment) for the barrier function, i.e., the organisational and/or physical structure without which the barrier function cannot be accomplished.

Four different types of barrier systems were defined, being **physical** or material barrier systems, **functional** barrier systems, **symbolic** barrier systems, and **immaterial** barrier systems respectively. A basic distinction between barrier functions is whether they are **preventive** or **protective**. This reflects whether the barrier function is intended to work before the occurrence of an accident or after it has happened. It is furthermore possible to describe a number of generic barrier functions, such as: containing, restraining, keeping together, dissipating, preventing, hindering, regulating, indicating, permitting, communicating, monitoring, and prescribing. There is no simple one-to-one correspondence between barrier functions and barrier systems, nor between barrier functions and their use as either preventive or protective barriers. It is, in fact, practically the norm that several barrier systems and barrier functions are combined to achieve a given purpose. This can either provide a measure of redundancy, or an effective defence-in-depth.

The presentation of the barrier classification was followed by a discussion of how a barrier analysis can be combined with an accident analysis. The common way of representing the outcome of an accident analysis is by a format similar to a fault tree, which for practical purposes was called an accident tree. The accident tree provides an excellent basis for a systematic investigation of the barriers that may have failed during an accident, and the barrier analysis can be combined with the accident analysis to improve the focus and the description of events. The retrospective use of barrier analysis is closely linked to the predictive use, but the application of the barrier classification to accident prevention, e.g. as a part of system design, has not been considered in this report but is postponed to a later occasion.

Finally, the steps needed to include the barrier analysis with the retrospective use of CREAM were discussed. This will result in a revision of the CREAM error modes, as well as an

extension of the details of the classification groups. The work will be undertaken in the near future.

This report has focused on the use of the barrier classification for accident analysis, i.e., a retrospective application. It is clear that the barrier concept also plays an essential role in system design, since incorporating the appropriate barriers generally insures system safety. A discussion of this use of barriers must, however, be conducted separately, at a later stage.

7. ACKNOWLEDGEMENTS

This report has been written as part of the project TRAIN - Traffic Safety and Information Environment for Train Drivers - funded by Banverket (Swedish National rail Administration). I am grateful for comments and encouragement to earlier drafts of this paper from members of the project team (Marie Green, Lena Kecklund, Erik Lindberg), and from Ola Svenson.

8. REFERENCES

Green, A. E. (1988). Human factors in industrial risk assessment - some early work. In L. P. Goodstein, H. B. Andersen & S. E. Olsen (Eds.), *Task, errors and mental models*. London: Taylor & Francis.

Hollnagel, E. (1995). The art of efficient man-machine interaction: Improving the coupling between man and machine. In: J.-M. Hoc, P. C. Cacciabue & E. Hollnagel (Eds.), *Expertise and technology: Cognition & human-computer co-operation*. Lawrence Erlbaum.

Hollnagel, E. (1998). *Cognitive reliability and error analysis method*. Oxford, UK: Elsevier Science.

Horberry et al, 1994) SPAD

Kecklund, L. J., Edland, A, Wedin, P. & Svenson, O. (1996). Safety barrier function analysis in a process industry: A nuclear power application. *Industrial Ergonomics*, *17*, 275-284.

Knox, N. W. & Eicher, R. W. (1983) *MORT user's manual* (DOE 76/45-4). Idaho Falls, Idaho: EG&G Idaho, Inc.

Leveson, N. (1995). *Safeware. System safety and computers*. Reading, MA: Addison-Wesley Publishing Company.

Lewin, K. (1951). Field theory and learning. In D. Cartwright (Ed.) *Field theory in social science. Selected theoretical papers by Kurt Lewin*. New York: Harper Torchbooks.

Reason, J. T. (1992). The identification of latent organisational failures in complex systems. In J. A. Wise, V. D. Hopkin & P. Stager (Eds.), *Verification and validation of complex systems: Human factors issues.* Berlin: Springer Verlag.

Reason, J. R. (1995). A systems approach to organizational error. *Ergonomics, 38,* 1708-1721.

Reason, J. T. (1997). *Managing the risks of organizational accidents*. Aldershot, UK: Ashgate.

Shannon, C. E. & Weaver, W. (1969). *The mathematical theory of communication*. Chicago: University of Illinois Press.

Svenson, O. (1991). The accident evolution and barrier function (AEB) model applied to incident analysis in the processing industries. *Risk Analysis, 11*(3), 499-507.

Svenson, O. (1997). *Safety barrier function analysis for evaluation of new systems uin a process industry: How can expert judgment be used?* In: Proceedings of Society for Risk Analysis Europe Conference, Stockholm, June 15-18, 1997.

Taylor, R. J. (1988). *Analysemetoder til vurdering af våbensikkerhed*. Glumsø, DK: Institute for Technical Systems Analysis.

Trost, W. A. & Nertney, R. J. (1985). *Barrier analysis* (DOE 76-45/29). Idaho Falls, Idaho: EG&G Idaho, Inc.