Modeling Safety Barriers and Defense in Depth with Mulitlevel Flow Modeling

Lind, Morten

Published in:
Proceedings of First International Symposium on Socially and Technically Symbiotic Systems

Publication date:
2012

Modeling Safety Barriers and Defense in Depth with Multilevel Flow Modeling

Morten Lind

Department of Electrical Engineering, Technical University of Denmark, Kongens Lyngby, Denmark
(Tel: +45-4525 3566, E-mail: mli@elektro.dtu.dk)

Abstract: The barrier concept plays a central role in design and operation of safety critical processes. In plant design barriers are provided as means of prevention to avoid critical process conditions which may be harmful to the environment. In plant operations barriers may be established and maintained through control actions in order to limit the consequences of critical plant events

The barrier concept has had a significant practical value for industry by guiding the design thinking of safety engineers. The provision of material barriers preventing the release of radioactive materials from the reactor core to the environment is accordingly a basic principle of nuclear safety design. The application of barriers is furthermore an integral part of the defence in depth principle applied by nuclear industry. Here several barriers are combined with reliability techniques such as redundancy and diversity to create systems with a high level of safety. Chemical industries apply similar techniques for protection of the environment against the release of toxic materials.

The paper explores different ways barriers can be represented in Multilevel Flow Modeling (MFM). One of the existing flow functions in MFM is a barrier function. It is shown that other barrier types can be represented and that their combination into barrier chains may be used to analyze and design levels of safety in automated processes. Suggestion for further research on barrier modeling with MFM are included.

Keywords: Safety, Barriers, Defence in Depth, Multilevel Flow Modeling.

1. INTRODUCTION

The concept of a barrier plays a central role in design and operation of safety critical processes. In process design barriers are provided as countermeasures to avoid critical process conditions which may be harmful to the environment. In plant operations and control barriers may be established and maintained through counteractions limiting the consequences of critical plant events.

The barrier concept has had a significant practical value for industry by guiding the design thinking of safety engineers. The provision of material barriers preventing the release of radioactive materials from the reactor core to the environment is accordingly a basic principle of nuclear safety design. The application of barriers is furthermore an integral part of the defence in depth principle applied by nuclear industry [1]. The application of several barriers to build layered defence structures is here combined with reliability techniques such as redundancy and diversity to create systems with a high level of safety. Chemical industries apply similar techniques for protection of the environment against the release of toxic materials [2].

The barrier concept has also been the subject of study by systems analysts and researchers. A challenge faced by both analysts and researchers has been that the barrier concept, although useful, is not particularly well defined.

The present paper will describe how MFM can be used to represent different types of barrier. The use of MFM for modeling safety barriers is a relatively unexplored research topic. The paper will present the status of current work on using MFM for modeling safety functions at DTU and show how it relates to existing research on barriers. Being the first paper on the topic it is also the aim to provide directions for further work.

The barrier concept is included in Multilevel Flow Modeling (MFM) [3] as one of the flow functions used to compose functional structures representing the functions involved in processing material and energy flows. The use of barriers in MFM to represent safety aspects of the sodium cooled Japanese Monju nuclear plant is presented in Lind et. al. [4]. This model clearly reflects the use of the barrier concept to model safety features of nuclear power plant. It also demonstrates the principle of defense in depth by a series of barriers separating the functions of the primary and secondary sodium cooling loops and the water steam cycle. Yoshikawa et. al. [5] proposes that such an MFM model could be used for on line risk monitoring.

We will show in the paper that MFM includes ways to represent other types of barrier which are relevant for capturing other aspects of safety in complex automated plants. First we will review current research on barriers and defence in depth.

2. BARRIERS AND DEFENCE IN DEPTH

The nuclear industry and other industries as well apply two basic safety design principles for the technical, organizational and the administrative functions in industrial plants. The first principle is to establish active or passive barriers against severe disturbances or hazards. The second principle is “defence in depth” which implies that several barriers are connected in chains so that each chain should

then be broken before the harmful incident occurs as illustrated in Fig. 1. These principles are applied in design of both hardware and software, in the planning of plant operation and in the overall qualitative assessment on management level. Control systems often serve as active barriers in the defence in depth structure.

The barrier concept plays therefore a central role in the design and operational philosophy of safety related industries. However, the barrier concept is often used uncritical and without rigor and hinders therefore a more formalized analysis and evaluation of plant safety. The problem can be illustrated by Fig. 1. Here each barrier (the vertical bars) in the defense structure (prevention, control, protection. mitigation) is implemented by a variety of different mechanisms. It becomes therefore difficult to define what the common characteristics of barriers are across all these mechanisms. Even though the barrier concept seems good for framing the safety problem it is accordingly too abstract to be useful for a more formal rigorous analysis.

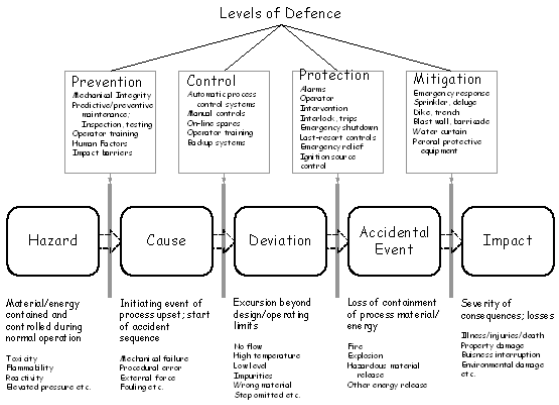


Fig 1. The principle of defense in depth

2.1 Defining barriers

An early influential study of the barrier concept was done by Haddon [6]. One of the aims among researchers has been to develop systematic techniques for barrier analysis which could be used by industry and its regulators in the assessment of plant safety [7]. Another interest has been to use barrier concepts in accident analysis [8].

Haddon's analysis of countermeasure strategies mentions a whole range of ways to create barrier structures in a variety of practical contexts. Hollnagel extends the meaning of the concept to encompass several meanings including material, functional, symbolic and immaterial barriers. Petersen [9] see this variety of meanings as a problem for the analysis and proposed a causal model to clarify the concept.

2.1.1 MORT

According to the MORT (The Management Oversight and Risk Tree) system safety programme [7] the basic ingredients of an accident are :

- the energy flow or environmental condition that does the harm;
- the vulnerable people or objects that can be hurt by that energy flow or environmental condition;
- the failure or lack of the barriers and controls that are designed to keep them apart; and
- the events and energy flows that lead into the final accident phase.

Like Haddon [6] the MORT programme uses an energy-barrier concept. A distinction is made between *safety* and *control barriers*. Safety barriers is concerned with control of unwanted energy flows and control barriers are concerned with the control of wanted energy flows. A barrier can be both a control barrier and a safety barrier.

Examples of safety barriers are: protective equipment, guardrails, safety training, work permit, and emergency plans. Examples of control barriers are: conductors, approved work methods, job training, disconnect switch, and pressure vessels.

Note that, compared to Haddon [6] the MORT programme generalizes the barrier concept. Haddon uses of the barrier concept only as a material separation of harmful energy and the target.

The analytical description of barriers in the MORT programme is based on concepts such as *function*, *location* and *type*. The function of a barrier can be prevention, control or minimization. A barrier can be located on the energy source, between the source and the worker, on worker, and separation through time and space. The different types of barriers are physical barriers, equipment barriers, warning devices, procedures/work processes, knowledge and skill, and supervision.

Furthermore, a strategy for dealing with hazards is described. The priority of actions is:

1. Elimination through design selection.
2. Installation of safety devices (barriers).
3. Installation of warning devices for timely detection (barriers).
4. Development of special procedures enabling the equipment operator to handle the situation (barriers).

2.1.2 Barrier types

Hollnagel has introduced a distinction between different barrier types and an extension in applications. He defines a barrier as an obstacle, an obstruction or a hindrance that may 1) prevent an action from being carried out or an event from taking place, or 2) prevent or lessen the impact of the consequences. Note that this definition marks a generalization of the concept of a barrier as it is not restricted to an energy-based concept.

Hollnagel also distinguish between the *barrier function* defined as the specific manner by which the barrier achieves its purpose from a *barrier system* which is defined as the substratum or foundation for the barrier function, i.e. the organizational and/or physical structure without which the barrier could not be accomplished.

Hollnagel define four barrier types: material, functional, symbolic and immaterial barriers.

- *Material barriers* that physically prevent an action from being carried out or the consequences from spreading. Examples of material barriers are buildings, walls, fences and railings.
- *Functional (or active or dynamic) barriers* that works by impeding the action to be carried out, for instance by establishing a logical or temporal interlock. A functional barrier effectively sets up one or more preconditions that have to be met before something can happen. Examples of functional barriers are: a lock (physical or logical)
- *Symbolic barriers* that require an act of interpretation in order to achieve its purpose. Hence, such barriers presume an "intelligent" agent that can react or respond to the barrier.
- *Immaterial barriers* that are not physically present in the situation but depend on the knowledge of the user to achieve their purpose. Immaterial barriers are usually also present in a physical form such as a book or a memorandum, but physically present when the use is mandated.

The material and the functional barriers are relevant in relation to the prevention of an action of a physical system or the prevention of the happening of the consequences of such an action. Symbolic barriers are relevant for human machine interaction. But as we shall see later, symbolic barriers are also involved in MFM when modeling automated safety controls.

2.1.3 Barriers and countermeasures

Petersen developed a novel approach for the analysis of safety [9]. Here the barrier concept is substituted by a causal account based on countermeasures. The principle can be explained by Fig. 2 showing the conditions required for the execution of an action A by an agent and directed towards an object (patient). Assuming that the action A is not wanted, the figure can be used to identify all the countermeasures which can be used in order to prevent the action for being succeeding. We can ensure that the agent does not have the capability to act and we can ensure that the object is not liable to undergo the change resulting from A. These are conditions for the potentiality of the action. We can also ensure that there is no opportunity to act be separating the agent and object in time or space (opportunity) and we can ensure that conditions which trigger the action does not occur (the actualization). Note that several of these countermeasures can be used together to obtain a high level of safety.

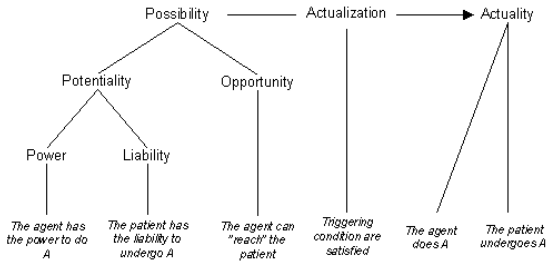


Fig. 2 Phases of an action [14]

When MFM is used for modeling safety we will actually need both Hollnagel´s and Petersen´s barrier concepts. As will be demonstrated below we can relate to Hollnagel´s barrier types. The countermeasures introduced by Petersen are related to recent extensions of MFM with roles [12]. However, here we will only be able to provide a preliminary analysis highlighting some of these aspects.

3. MULTILEVEL FLOW MODELLING

3.1 Overview

Multilevel flow modeling is a modeling methodology for process and automation design and for reasoning about fault management and control of complex plants. MFM concepts and symbols are shown in Fig. 3 including an extension with the concept of threat required for proper modeling of goals and functions required for safety. Recent work extends MFM with roles [12] but is not included here. The reader is referred to [3,11] for a detailed introduction to MFM.

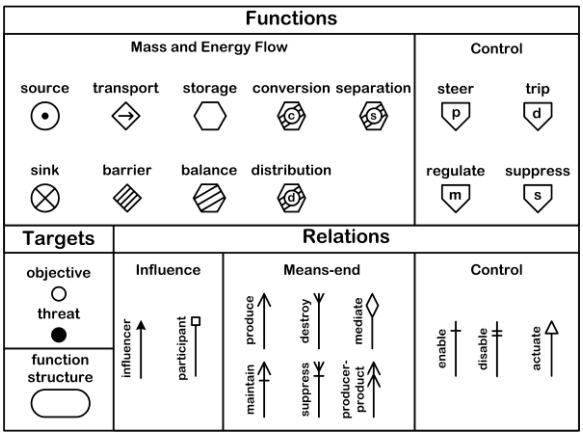


Fig. 3. MFM concepts with a safety related extension (threat).

It is seen that the flow functions in MFM includes a barrier concept. This barrier represents the function of a system which prevents the flow of material or energy. Since we will identify other types of barrier in MFM below this will be called a flow barrier. A mass flow barrier belongs clearly to Hollnagel category of material barriers. But energy flow barriers (e.g. heat insulation) do not seem to fit naturally in his categories. With some interpretation they may belong to functional barriers.

But MFM includes other concepts such as suppress and destroy relations and trip and suppress control functions which we will show are related to the wider definition of barrier concepts introduced above. We need therefore to review the use of these MFM concepts in order to explain their relevance for modeling barriers.

The first step in the review is a reconsideration of the meaning of objectives and means-end relations. This will lead to the introduction of *threats* in MFM. The concept of a threat clarify the proper use of suppress and destroy relations and of the safety related control functions in MFM. The second step is to show the relevance of these results for representing different types of barriers in MFM.

We need also a third step considering the levels of knowledge representation in MFM introduced in the analysis of causal reasoning presented in [13]. As part of this analysis event barriers were identified but not included in the paper. They will be discussed below.

3.2 Reviewing the meaning of MFM objectives

An objective in MFM represents a desirable future or existing situation or state. Objectives are related to the functions provided by the plant designer which are the means to produce or maintain the objective. The means-end relations produce and maintain are available in MFM and are used to represent situations where an agent seeks to promote a situation which is desirable. This desirable situation is expressed in the objective.

It is realized that objectives and the produce and maintain relations are constituents of the same conceptual scheme dealing with promoting desirable situations. Within this scheme there are two possible syntactical combinations shown in Fig. 4 (the label xx refer to the so-called main function inside the flow structure fs1).

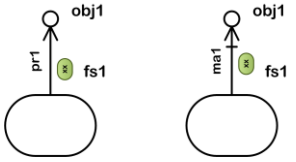


Fig. 4. Means-end relations for promoting objectives

MFM make also distinctions between process objectives and control objectives. The distinction between these two types of objectives is not reflected in separate modeling concepts or symbols but reflected by the context in which they appear as shown in Fig. 5.

The control functions in Fig. 5 (pco1 and mco1) promote the achievement of process objectives (obj1 and obj2). The control objectives (cob1 and cob2) specifies requirements to the means and manner of control. The syntax of control structures are described in [11].

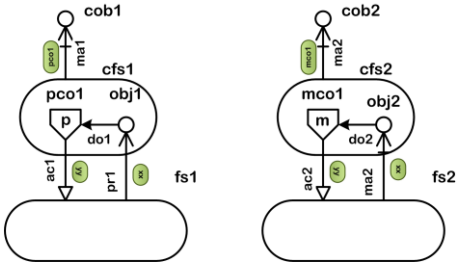


Fig. 5. Control structures in MFM include both process and control objectives.

3.3 Introduction of threats

Objectives are accordingly situations or states which are being promoted by the decisions of the process designer or the actions of a control agent. However designing or acting for reasons of safety deal with avoiding harmful situations. Such situations are obviously not promoted but opposed by proper actions. We need therefore also to consider actions which oppose situations or states which imply a risk or are undesirable by being in conflict with the values of the designer or the control agent.

These situations or states will be called threats and represented by a black circle in MFM (see Fig. 3). Like an objective, a threat is referring to a situation or state. But unlike an objective which refers to a desirable situation, a threat refers to something which is undesirable or a hazard. The distinction between objectives and threats express value related preferences of the process designer or the control agent. Objectives and threats share a common property of being situations which are the target of the designer's decisions and the agent action. We have therefore introduced a super-ordinate concept "target" as part of the generic MFM concepts (Fig. 3). Fig. 6 shows how threats are combined with destroy and suppress relations and the means or countermeasures used to oppose them (the main functions labeled "xx").

The concept of threat introduced here is related to the countermeasures provided by the designer. Threats can also be defined in an operational context in relation to the evaluation of dynamic situations e.g. in the management of alarms [15] but will not be addressed here.

Fig. 6. Means-end relations used to represent connections between countermeasures (the means) and threats (the undesirable ends).

3.3.1 Inconsistent intentions

By the introduction of threats we can ensure the consistency of representations of intentional structures in MFM. Intentions are considered consistent if they are rational in the sense that there is no conflict between the end and the means taken to achieve the ends.

We can illustrate this idea of consistency by Fig. 7 showing four schematic MFM models which are inconsistent. The structures shown in Fig. 4, 5 and 6 are consistent.

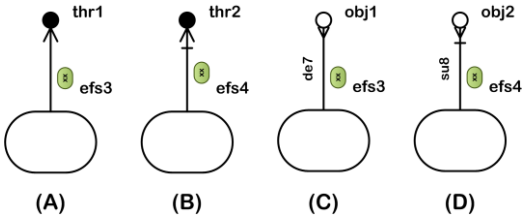


Fig. 7. MFM models representing inconsistent intentions.

Models A and B in Fig. 7 are inconsistent because a rational agent would not produce or maintain a situation or state which is a threat (except for sabotage which we exclude here). In a similar way the models C and D should be considered inconsistent because a rational agent would not destroy or suppress a situation which is an objective.

Note that there may be conflicts among two agents if the objective of one of the agent is a threat for the other agent. Such situations are not inconsistent and would be relevant to consider in future research but will not be discussed further here.

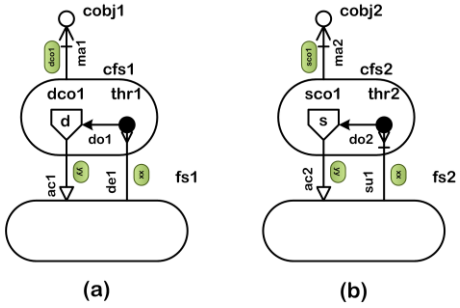


Fig. 8. Control functions contribute to elimination (A) or suppression (B) of threats

3.3.2 Threats and control functions

Control functions in MFM [11] can also be combined with threats as shown in Fig. 8 and Fig. 9. The control functions in Fig. 8 contribute to the elimination (a) or suppression (b) of threats thr1 and thr2. In Fig. 9 the control functions suppress situations with unstable dynamics in a steering (a) and a regulation (b) control task (the threats cthr1 and cthr2).

Control structures can accordingly be connected with both objectives and threats at the same time and thereby reflect the typical complexity of a control situation which often includes process states that should be promoted and opposed in combination with situations of instability (threats) which should be avoided or eliminated.

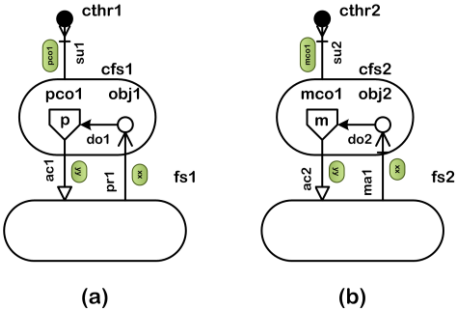


Fig. 9. Threats can also relate to the performance of control functions.

3.3.3 Threats and conditions

Enablement and disablement conditions can be combined with objectives as shown in Fig. 10 (A and B). Threats also combine with enablement and disablement as shown (C and D).

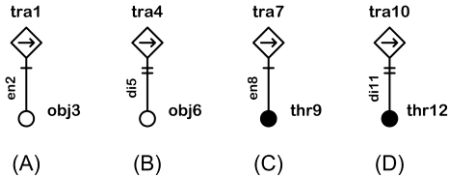


Fig.10. A flow function can be conditioned (enabled or disabled) by an objective or a threat.

3.4 Levels of representation in MFM

It has been shown in [13] that the knowledge provided for causal reasoning in a MFM model related to four separate but interdependent levels of specification. An overview of these levels is presented in Table 1.

On the most fundamental level 1 state dependency relations represent cause-effect and logic relations between states of process objectives and functions. On level 2 we find influence, means-end and control relations which are used to represent potentials for interaction between states of objectives and functions. They comprise a separate level of representation which is more abstract than level 1 by only indicating

the existence of a state dependency relation between two flow functions and not the specific state dependency relations which are represented on level 1.

Table 1. Process knowledge in MFM is organized into four levels of specification

Level	Knowledge category		
4	Paths	Event propagation paths	
3	Patterns	Influence patterns	Means-end and control patterns
2	Relations	Influence relations	Means-end and control relations
1	Dependencies	State dependency relations	

Of particular importance for the present paper is the distinction between the two types of influence relations "influencer" and "participant" on level 2 (see Fig. 3). The participant relation is used in situations where the state of a transport function is independent on changes in the state of the functions it is connected with through the participant relation. This means that a change in the state of a storage function or a barrier which is connected with the transport through a participant relation cannot propagate to the transport. This means that the participant relation can be seen as an *event barrier*.

On level 3 we find influence and means-end relations combining functions and goals into MFM patterns on level 3. MFM patterns are generic combinations of goals and functions and are the building blocks of propagation paths on level 4.

3.5 Event barriers

Event propagation within a flow-structure reflects the general behavior of mass and energy flow systems. It is derived from the bidirectional propagation of events between storage, balance, transport and barrier flow functions.

Event propagation paths determine the potential for interaction between plant functions and are therefore relevant for both process and control system design or in general for reasoning about dynamic situations dealing with the confinement and control of disturbances.

Fig. 11. An example illustrating the use of influence relations (ca7, pa9, ca8, pa10 and pa11) in a flow structure.

Flow functions are interconnected within flow structures by two types of influence relations called direct and indirect influences (Fig. 11). The influences define a *potential* for interaction between flow functions. They do not define the *actual* dependencies between states of the functions which are defined by state dependency relations (level 1).

Direct influences represent situations where a change in the state of a transport function has an effect on the state of its neighboring storage or balance functions. Direct influences are exemplified in Fig. 11 by considering the effects of a changed flow in transport function tra9 on its neighboring storage functions sto2 and sto3.

Assuming that the flow provided by tra9 is changed the state of storage sto2 and sto3 is changed. These influences on the state of sto2 and sto3 caused by changes in tra9 are called direct influences and are expressions of the potential of transport functions for changing mass or energy balances. The arrow inside the transport function tra9 is an explicit representation of the direct influence which go in both upstream and downstream directions (tra9 will influence sto2 upstream and sto3 downstream).

Direct influences are only mentioned here in order to distinguish them from indirect influences which are highly relevant for the present discussion of barriers. More details about the causal implications of direct influences can be found in [13].

An indirect influence represents a situation where the change of the state of a storage or a balance may have an effect on the state of their connected transport functions. Indirect influences represent accordingly interactions between potential and actualized changes in mass or energy flows. As an example, if the content of mass in sto3 in Fig. 11 is changing it may influence the transport tra10 by changing the flow rate. The accumulated mass in sto3 represents a potential for flow and the resulting change in the transport tra10 is its actualization. This indirect influence of sto3 on the state of tra10 is represented by an arrow pointing from sto3 towards tra10 (ca9 in Fig.11). Since the storage actively influences the transport the relation is called an *influencer*. In other situations storages will not influence the state of the transports but passively deliver or receive the flows. This type of indirect influence is represented in MFM by a so-called participant relation depicted as a directed relation with a box indicating the transport function in question (pa9, pa10 and pa11 in Fig. 11).

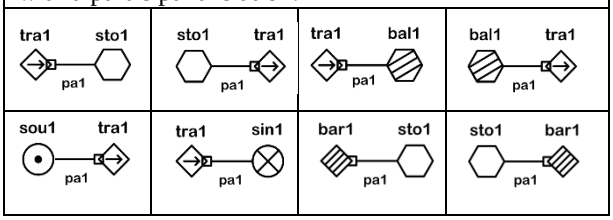
3.5.1 Patterns of indirect influence

Influence relations combine MFM flow functions into patterns of indirect influence (level 3 in table 1) which are basic building blocks of event propagation paths (level 4). Influence patterns are divided into two main groups. In one group the patterns are composed of two flow functions which are related by an influence relation. The other group comprising patterns with two or more transport functions and/or barriers connected to a balance are discussed by Lind [13] but will not be discussed here. Furthermore we will also ignore patterns with influencer relations since they are irrelevant for the present discussion

about event barriers. In the following we will accordingly only discuss the patterns of indirect influence created by participant relations.

The possible patterns with two flow functions connected by a participant relation are shown in table 2. The combinations are restricted by the MFM syntax which does not allow interconnections of e.g. two transport or two storages etc. The syntax defines combinations of functions which are meaningful in the sense of process semantics.

Table 2. MFM Patterns with transport, barrier, storage, balance, source or sink functions connected with a participant relation.



We will show in the following that these patterns in some cases prevent changes of the state in one of the flow functions to propagate to the other one in the pattern. These cases define accordingly a set of event barriers. We will also show that the event barriers combine in chains. The event barriers introduced below fit in the category of functional barriers in Hollnagel´s taxonomy.

3.5.2 Upstream and downstream propagation

MFM distinguish between propagation of changes in upstream or downstream directions [13]. The distinction is related to the direction of mass or energy flow which is indicated in the transport function. The distinction is important because events can propagate in the same direction as the flow (downstream) or it can propagate in the opposite direction (upstream). The two situations lead to different event barriers and will be therefore be discussed separately.

3.5.2.1 Upstream event barriers

We have here identified three different situations from table 2 involving event barriers (Fig. 12).

The cases are: a) preventing propagation of a storage event upstream to a connected transport function, b) preventing propagation of a balance event upstream to a connected transport function, and c) preventing propagation of a storage event to a connected barrier. A brief explanation of each case is given below.

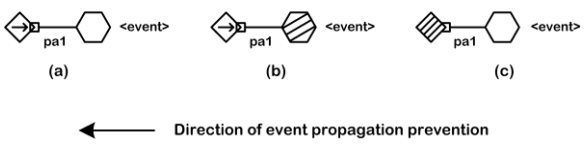


Fig. 12. Upstream event barriers

Storage and transport (a)

A storage event (i.e. a change of its state) cannot propagate *upstream* to the connected transport. This lack of influence on the state of the transport is what the participant relation (pa1) signifies. This pattern accordingly represents an event barrier.

Balance and transport (b)

A balance event (e.g. a leak or unbalance) cannot propagate *upstream* by influencing the state of transport functions. This lack of influence on the state of the transport is what the participant relation (pa1) signifies. This pattern accordingly represents an event barrier.

Storage and barrier(c)

A storage event cannot here propagate *upstream* by influencing the state of a connected barrier (similar to a). This lack of influence on the state of the transport is what the participant relation (pa1) signifies. This pattern accordingly represents an event barrier.

3.5.2.2 Upstream event barrier paths

It is clear that upstream event barriers combine into barrier paths as exemplified in Fig. 13 where a storage (sto1) event is prevented from propagating to the connected transport (tra2) and where a leak in the balance (bal1) is prevented from propagating to the next transport (tra1) upstream. Note that an upstream path is always is associated with a node from where the event is assumed to originate (here sto1).

These barriers paths are of interest in understanding interactions between several barriers and the principles involved in building defence in depth structures.

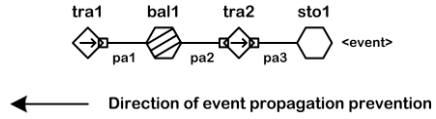


Fig. 13. An upstream event barrier path combining patterns in Fig. 12

Of particular interest would be to develop rules for reasoning about event barrier failures. Thus the consequence of a failure of the barrier related to pa3 in Fig. 13 would be that the storage event propagates to the transport function tra2. This event would then transfer to the first transport tra1 through the balance bal1 but is prevented by pa1. These rules for reasoning about barrier failure are presently not included in the reasoning systems for MFM based root cause analysis under development [13].

3.5.2.3 Downstream event barriers

As for upstream propagation we will also here consider three different cases of event barriers. They are shown in Fig. 14.

The cases are: a) preventing propagation of a storage event downstream to a connected transport function, b) preventing propagation of a balance

event downstream to a connected transport function, and c) preventing propagation of a storage event to a connected barrier. A brief explanation of each case is given below.

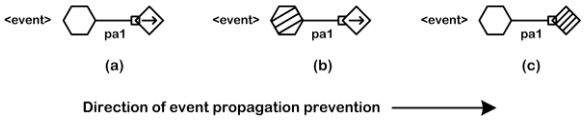


Fig. 14. Downstream event barriers.

Storage and transport (a)

A storage event (i.e. a change of its state) cannot propagate *downstream* to the connected transport. This lack of influence on the state of the transport is what the participant relation (pa1) signifies. This pattern accordingly represents an event barrier.

Balance and transport (b)

A balance event (e.g. a leak or unbalance) cannot propagate *downstream* by influencing the state of transport functions. This lack of influence on the state of the transport is what the participant relation (pa1) signifies. This pattern accordingly represents an event barrier.

Storage and barrier(c)

A storage event cannot here propagate *downstream* by influencing the state of a connected barrier (similar to a). This lack of influence on the state of the transport is what the participant relation (pa1) signifies. This pattern accordingly represents an event barrier.

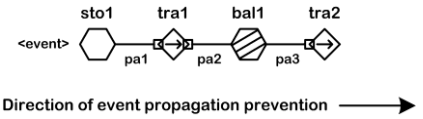


Fig. 15. A downstream event barrier path combining barriers in Fig. 14.

3.5.2.4 Downstream event barrier paths

The downstream event barriers in Fig. 14 combine into barrier paths as exemplified in Fig. 15 where a storage (sto1) event is prevented from propagating downstream to the connected transport (tra1) and where a leak in the balance (bal1) is prevented from propagating to the transport (tra2) upstream. Note that a downstream path is always is associated with a node from where the event is assumed to originate (here sto1).

As mentioned above, these barrier paths and the rules for their composition are of interest in understanding interactions between several barriers and for the development of formalized principles for analysis and construction of levels of defence.

3.6 Other barrier types in MFM

In the following we will explain how MFM can represent other types of barrier.

Two of the control functions in Fig. 3 can actually be seen as barriers. This is illustrated by Fig. 16 (identical to Fig. 8) which includes two simplified MFM models containing destroy or trip (dco1) and suppresses (sup1) control functions. The trip function (dco1) eliminates the threat (thr1) and is therefore a barrier against counteragents which otherwise may realize the threat. Similarly, the suppress function (sup1) prevents that the threat thr2 becomes realized by acting as a barrier against counteragents. The inclusion of disturbances in MFM models are discussed by Heussen [16].

The trip and suppress control functions should accordingly be seen as a barriers. Both of these barriers belong to Hollnagel's functional category.

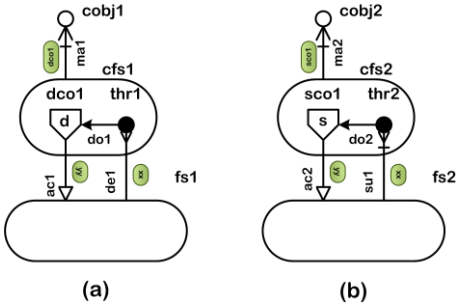


Fig. 16. Control structures in MFM models include symbolic and functional barriers (according to Hollnagel's types).

The threats themselves may also be seen as barriers as they require an act of interpretation in order to achieve their purpose. In MFM this interpretation is expressed by the type of control function related to the threat.

In summary, each of the examples (a and b) in Fig. 16 contains two barriers. The first barrier is the threat which is symbolic as it requires interpretation by the control agent in order that the corresponding situation is eliminated (a) or prevented (b). The control functions (dco1 and sco1) are the countermeasures provided against the threat and is therefore the second barrier.

The MFM representations of barriers in Fig. 16 accordingly signify that two measures are taken by the system designer to prevent a threatening situation. The first is to inform a potential control agent that the situation is a threat (and not an objective). The second is that a control action is provided to cope with the threat.

Above we have discussed the various ways by which MFM can represent barriers. It has been concluded that the barrier types included in MFM may be seen as instances of the more abstract barrier types defined in Hollnagel's taxonomy.

4 DEFENCE IN DEPTH AND MFM

In the following we will discuss the relevance of the findings presented above for the principle of defence in depth [1]. We will focus exclusively on the idea of providing levels of defence in the plant and its control systems. We will not discuss aspects related to diversity and the distinctions between functional and structural redundancy even though these aspects also may be addressed by MFM (see e.g. [12]).

4.1 An Example

We will use a simple process example to demonstrate how MFM can combine barriers and represent their interrelations. The example shown in Fig. 17 is a generic heat transfer system and is taken from [4]. This system has been used to build an MFM model of the MONJU nuclear power plant which has several interacting heat transfer subsystems of this type.

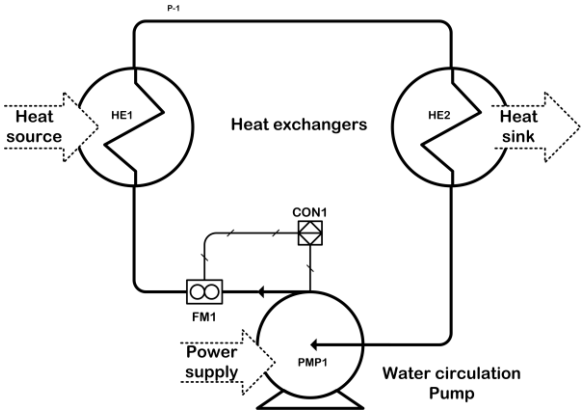


Fig. 17. A generic heat transfer system

The heat transfer system contains two heat exchangers HE1 and HE2 connected with a water circulation loop. The purpose of the water loop is to transfer heat from the secondary side of HE1 to the primary side of HE2. The water is circulated by a pump. The circulation flow is controlled by a control system CON1. An MFM model of the example as shown in Fig. 17 is presented in [4].

For the purpose of the present discussion the example will be extended by assuming that there is a risk of overheating the fluid on the secondary side of HE2. An additional safety related control system is therefore provided to monitor the temperature and respond with protective actions if the temperature gets too high. We will assume that the control system will change the setpoint of the flow controller. This additional control system is not shown in Fig. 17.

Fig. 18 show the MFM model with the extensions required to include the temperature controller. The extensions comprise the control structure cfs2 modeling the temperature controller including the threat thr1 which may be expressed by a temperature limit (related to the accumulation of heat in HE2 represented by the energy storage function sto4. The temperature control system is actuating (ac2) the transfer of energy (tra1) inside the pump.

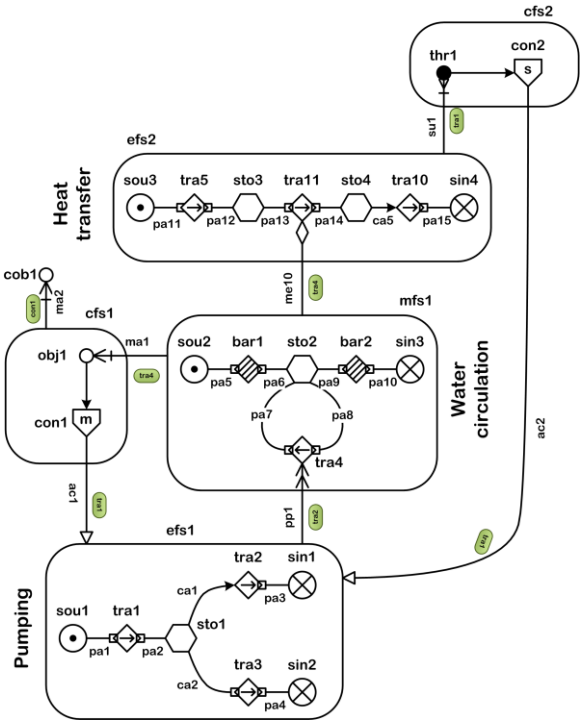


Fig. 18. MFM model of the generic heat transfer system including a control system suppressing high temperature in HE2.

4.1.2 Barrier types in the example

It is realized that the MFM model contains several barrier types. First of all there are two flow barriers included in the mass flow structure mfs1. These two barriers represent the functions of the piping inside HE1 and HE2 respectively. These pipes prevent the fluid contained in the primary side of the heat exchangers to enter their secondary side. It is also seen that the amount of water accumulated in the circulation loop (the state of sto2) will not affect the barriers such as creating a leak due to the pressure created (indicated by pa6 and pa9).

In addition to the flow barriers in mfs1 we also see several examples of event barriers in in efs2 and efs1. Two examples of particular interest are the event barriers defined by the participant relations pa13 and pa14 and the flow functions they connect in energy flow structure efs2. These event barriers show that changes in the energy transferred from the secondary side of HE1 (sto3) to the primary side of HE2 (sto4) can only be performed by changing in the circulation flow (tra1, tra4 to tra11 following the means-end relations between efs1, mfs1 and efs2).

This illustrates that MFM model can be used to study the interaction between different types of barrier in the system (ignoring the fact that the somewhat counter intuitive result of the analysis may indicate that the model is not entirely correct!).

We also see that the temperature controller introduce two barriers as explained above i.e. the threat (thr1) and the control function (con2). It is realized that these two barriers are interrelated with the energy flow barriers in efs1 mentioned above through a chain of means and ends incorporating the a chain of means-and ends including the pumping, circulation and energy transfer functions.

The MFM model can accordingly reflect composite barrier structures in a system. However, it is also seems as if the organization of the barriers not always can be described as simple chains or levels of defense. More complex structures are to be involved. MFM may be an efficient tool for the analysis and design of these structures.

5. CONCLUSIONS

This paper is of an exploratory nature. It investigates how MFM can be used to model barriers and analyze defence in depth in safety critical process. The paper is the first published on this topic.

The paper demonstrates that MFM models can represent several barrier types and their composition in levels of defence. The concept of threat is introduced as an extension of MFM. The extension was required in order to clarify the semantics and to be able to extend the barrier types covered by MFM.

Further research work is required including also the development of rules for reasoning about barrier structures and their failures. This research is required in order to make MFM useful as a tool for systematic analysis and design of level of defence.

6. ACKNOWLEDGEMENT

The paper includes previously unpublished joint work of the author and Johannes Petersen reviewing the barrier concept. Petersen's contribution to this review is acknowledged. Sten Bay Jørgensen and Niels Jensen from the DTU functional modeling group contributed to the identification of event barriers by reflective comments during the development of the causal analysis published in [13].

REFERENCES

[1] IAEA. Defence in Depth. International Atomic Energy Agency INSAG-10, Vienna, 1996.

[2] DOE. DOE Handbook: Chemical Process Hazards Analysis. US Department of Energy DOE-HDBK-1100-2004, February 1996.

[3] M. Lind. An Introduction to Multilevel Flow Modeling. International Journal of Nuclear Safety and Simulation, 2011, 2(1), 22-32 .

[4] M. Lind, H. Yoshikawa, S. B. Jørgensen, M. Yang, K. Tamayama, K. Okusa. Multilevel flow modeling of Monju Nuclear Power Plant. International Journal of Nuclear Safety and Simulation, 2011, 2(3).

[5] H.Yoshikawa, M. Yang, M. Hashim, M. Lind, and Z. Zhang, "Design of Risk Monitor for Nuclear Reactor Plants, International Journal of Nuclear Safety and Simulation, **2(3),** pp.265-273(2011).

[6] W. Haddon. Energy Damage and the Ten Count ermeasure Strategies. Human Factors, 1973, 15(4), 355-366.

[7] W. Trost and R. J. Nertney. Barrier Analysis. SCIE-DOE-01-TRAC-29-95, Scientec INC, Technical report, August 1995.

[8] E. Hollnagel. Accidents and Barriers. Proc. 7th Conference on Cognitive Science Approaches to Process Control (CSAPC99). Villeneuve dÁsc, France, 21-24 September 1999, 175-180.

[9] J. Petersen. Countermeasures and Barriers. Proc. 2005 Annual Conference of European Association of Cognitive Ergonomics (EACE´05), Chania Greece, September 29-October 1, 43-50.

[10] M. Lind. Modeling Goals and Functions of Control and Safety Systems. Nordic Nuclear Safety Research NKS-114, October 2005.

[11] M. Lind. Control functions in MFM: basic principles. International Journal of Nuclear Safety and Simulation, 2011, 2, June 2011.

[12] M. Lind. Knowledge Representation for Integrated Plant Operation and Maintenance. 7´th American Nuclear Society Int. Topical Meeting in Nuclear Plant Instrumentation, Control and Human-Machine Technologies NPIC&HMIT, Las Vegas, Nevada, November 7-11, 2010.

[13] M. Lind. Reasoning about Causes and Consequences in Multilevel Flow Modeling. Proc. European Safety and Reliability Conference, ESREL 2011, Troyes France, September 18-22, 2011.

[14] M. Lind. Possibilities for Action. Technical Report CHMI-7-2000, Center for Human Machine Interaction, Risø National Laboratory, Denmark. 2000.

[15] T. Us, N. Jensen, M. Lind and S. B. Jørgensen. Fundamental Principles of Alarm Design. Proceedings 4´th International Symposium on Cognitive Systems Engineering Approach to Power Plant Control (CSEPC2008), Harbin China, 2008.

[16] K. Heussen and M. Lind. Representing Causality and Reasoning about Controllability of Multilevel Flow Systems. Proceedings IEEE International Conference on Systems, Man and Cybernetics SMC 2010, 2010.