SAFETY-BARRIER DIAGRAMS FOR DOCUMENTING SAFETY OF HYDROGEN APPLICATIONS

Duijm, N.J.[1] and Markert, F.[2]
Systems Analysis Department, Risø National Laboratory,
Technical University of Denmark, P.O. Box 49, DK-4000 Roskilde, Denmark,
[1] nijs.j.duijm@risoe.dk,
[2] frank.markert@risoe.dk

ABSTRACT

Safety-barrier diagrams have proven to be a useful tool in documenting the safety measures taken to prevent incidents and accidents in process industry. In Denmark they are used to inform the authorities and the non-experts on safety relevant issues as safety-barrier diagrams are less complex compared to fault trees and are easy to understand. Internationally there is a growing interest in this concept with the use of so-called "bow-tie" diagrams, which are a special case of safety-barrier diagrams. Especially during the on-going introduction of new hydrogen technologies or applications, as e.g. hydrogen refueling stations, this technique is considered a valuable tool to support the communication with authorities and other stakeholders during the permitting process. Another advantage of safety-barrier diagrams is that there is a direct focus on those system elements that need to be subject to safety management in terms of design and installation, operational use, inspection and monitoring, and maintenance. Safety-barrier diagrams support both quantitative and qualitative or deterministic approaches. The paper will describe the background and syntax of the methodology and thereafter the use of such diagrams for hydrogen technologies are demonstrated.

1 INTRODUCTION

During the recent years, there is a growing interest to develop and to introduce new energy technologies because the fossil fuel based technologies are considered to have adverse effects on the climate (green house effect), are assumed to soon have reached their peak production capacity and because of other political reasons e.g. for many countries to reach a higher level of self-supply being less dependent on third countries to cover the energy demands. The application of hydrogen-based technologies is considered to be a promising solution especially for the intermediate storage of electricity produced by wind turbines and solar cells that both depend on fluctuating primary energies as wind and sun-light, respectively. Another application is in the transport sector with a future vision of hydrogen-driven vehicles. This involves building of a very large net of refueling stations. Safety is an essential aspect in the reshaping of our known infrastructure into one compatible with the new sustainable energy forms. The goal must be to build new infrastructures providing at least the same or better societal and individual safety compared to the present situation. The approach is international and very complex. Therefore, good and easy to understand communication about the safety aspects of new technologies has to be established. Safety-barrier diagrams have proven to be a useful tool in Denmark in documenting the safety measures taken to prevent incidents and accidents in process industry. Internationally there is a growing interest in the concept of safety barriers and the use of so-called "bow-tie" diagrams, which are a special case of safety-barrier diagrams. Safety-barrier diagrams use the same logic as classical fault trees and event trees, but basic events and logic related to the functioning of safety systems are encapsulated in a single item, which diminishes the number of symbols in the graph, turning fault trees and event trees into diagrams that are much easier to understand by non-expert stakeholders. Especially during the early introduction of hydrogen technology, this technique can support the communication with e.g. authorities and other stakeholders during the permitting process. Another advantage of safety-barrier diagrams is that there is a direct focus on those system elements that need to be subject to safety management in terms of design and installation, operational use, inspection and monitoring, and maintenance. Safety-barrier diagrams support both quantitative and qualitative or deterministic approaches.

The paper will reflect on the concept of safety barriers in relation to safety management, and describe the background and syntax of safety-barrier diagrams. Thereafter we will demonstrate the use of safety-barrier diagrams using an example taken from a FMEA study on a liquefied hydrogen refueling station [1].

2 SAFETY BARRIERS

The concept of "safety barriers" has gained interest from risk management practitioners. In this paper we consider terms like "safeguards", "layers of protection" and "lines of defense" to be synonymous with safety barriers. A recent discussion of safety barriers can be found in Sklet [2] and Hollnagel [3]. Following Harms-Ringdahl [4] we make use of the notion of a barrier function to define a safety barrier [5,6]:

- A barrier function is a function planned to prevent, control, or mitigate the propagation of a condition or event into an undesired condition or event;

- A safety barrier is a series of elements that implement a barrier function, each element consisting of a technical system or human action.

Some safety barriers implement the barrier function by the mere presence of their elements (e.g. a tank pit or a firewall), these are called passive safety barriers. Other safety barriers perform an action in response to a certain state or condition, these are called active barriers. Active barriers always include a sequence of "Detection–Diagnosis–Action". Most safety barriers involve several elements or components to fulfill the barrier function. Figure 1 shows an example of a system to prevent overfilling where an operator has to respond to an alarm by pressing a button to close a valve. From this example it is clear that the alarm is only a part of a safety barrier: without the other elements it will not prevent the overfilling.

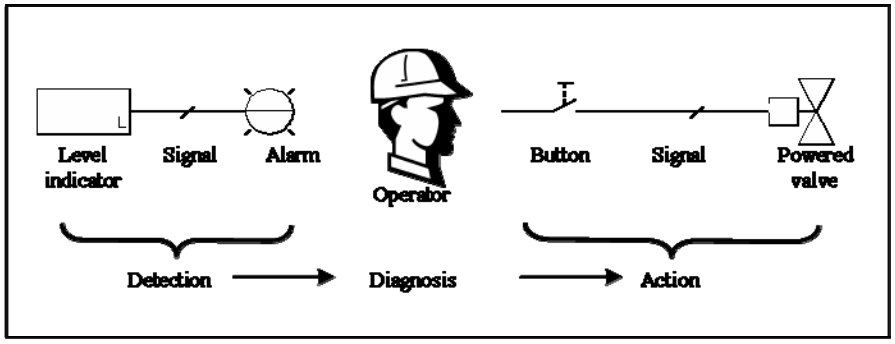

Figure 1 Example of a safety barrier to avoid overfilling involving instrumentation, data transmission, alarm, human action and a powered actuator

Barrier functions and safety barriers are directly related to the event sequence or accident scenario, and they do not include possible influencing factors that affect the barrier performance, such as higher-level safety-management related issues of training, maintenance, procedures, etc. Technical/physical safety barriers are normally easy to identify, but in case the safety barrier involves human action (e.g. an operator response to an alarm) one should be careful to differentiate between the action itself (that implements the barrier function) and all factors that support the operator in taking the right action, such as proper procedures or rules, training, and unambiguous presentation of information. These latter issues in themselves cannot prevent the accident sequence but can be of big importance for the successful functioning of the safety barrier. For that reason recent research focuses on the relation between safety management (which has to provide for training, procedures, ergonomics, maintenance, etc.) and safety barrier performance [7,8].

3 SAFETY-BARRIER DIAGRAMS

A barrier diagram is a graphical presentation of the evolution of unwanted events (initiating events or conditions) through different system states depending on the functioning of the safety barriers intended to

prevent this evolution. A barrier diagram represents possible (accident) scenarios. It is a directed, acyclic graph within the framework of mathematical graph theory similar to event trees, fault trees, cause-consequence diagrams and Bayesian networks, to which the barrier diagrams are closely related.

Using the terminology of graph theory, the barriers are the nodes or vertices of the graph. The edges between the nodes correspond to conditions or states of the system: on the left-hand side of a barrier, such a condition is the condition or event that triggers the barrier to function (condition on demand) while normally the condition on the right-hand side is the condition when the barrier has failed (condition on failure). Alternatively other states on the right-hand side can be defined, corresponding to different responses of the barrier, but usually only two barrier outcomes are considered, viz. success or failure. E.g. for a pressure relief valve, the successful deployment leads to a release of material, which is not a normal condition and therefore may be included in the barrier diagram giving rise to an alternative scenario (i.e. an alternative path through the barrier diagram). We use the graphical notation for barriers with two states on the right-hand side as in Figure 2.

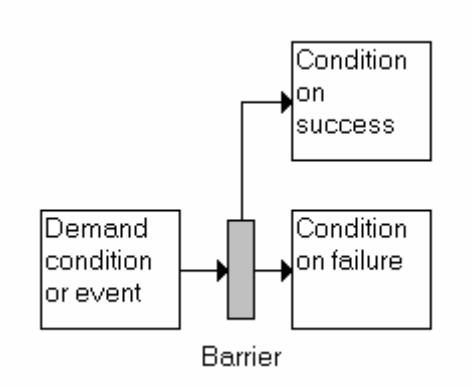

Figure 2 Graphical representation of a safety barrier in safety-barrier diagrams with two output conditions

Logically, the barrier represents an AND gate, i.e. the condition on failure occurs when the demand condition occurs and the barrier fails, see Figure 3. Note that in this presentation one cannot show the condition on success without introducing a new input condition ("barrier works on demand") and a new logical gate. One of the main advantages of barrier diagrams is their relative simplicity as compared to fault trees and event trees, which makes them useful for communication with non-experts.

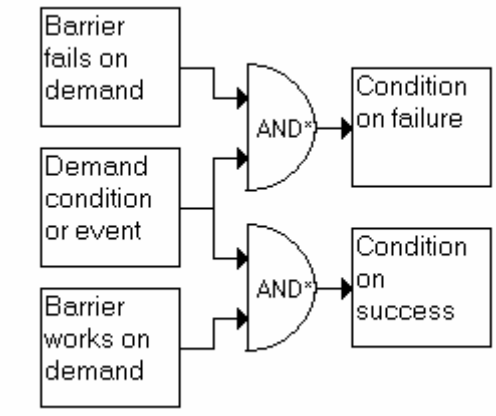

Figure 3 Representation of the barrier from Figure 2 by means of a fault tree

The syntax of safety-barrier diagrams is discussed in more detail in Duijm [5,6]. We mention the most important properties of safety-barrier diagrams here:

- Safety barriers and conditions in a safety-barrier diagram are unique. Safety barriers respond to specific demand conditions, and the output conditions of safety barriers are also uniquely defined given the demand condition and the barrier. As a consequence, a given barrier with its demand and output conditions can only appear once in a diagram. This does not exclude that a condition can trigger more than one barrier (barriers can share demand conditions) nor that conditions can be the output of more than one barrier (barriers can share output conditions). When two barriers share the same demand condition, both barriers are triggered simultaneously, i.e. the parallel paths through the diagram do not exclude each other (as opposite to the parallel paths that originate from the alternative success or failure outputs of one barrier; these paths are mutually exclusive as in an event tree). When barriers share an output condition, the joining of the paths represents an "OR" gate, i.e. the condition appears when at least one of the barriers proceeds to the shared output condition.

- Safety-barrier diagrams can be split into smaller diagrams. These diagrams are said to be connected. The only condition for a set of connected diagrams is that the joint diagram is acyclic and directed and that the conditions and barriers in this joint diagram are unique.

- The probability of conditions in a safety-barrier diagram can be derived from the probability of the initial conditions and the probabilities of failure on demand of the barriers. In general, algorithms developed for fault tree analysis can be used. But in case the (joint) diagram does not include diverging-converging paths (paths that split at one point and that join again later), and if all barriers and initial conditions are independent, it is possible to propagate the probability of the conditions through the diagram without the need for more advanced algorithms.

Many safety barriers include several elements that are necessary to perform the barrier function, as described in the previous section. Though the barriers themselves are unique, elements in these barriers don't need to be unique. In practice many barriers depend on the same systems, like power supply, control systems or single operators. In that case the functioning of the barriers is no longer independent of each other and the simple propagation of probability can no longer be applied. Furthermore, for a qualitative assessment, it is useful to be able to identify which barriers share common elements.

4 EXAMPLE: DESCRIPTION OF A REFUELLING STATION

To demonstrate the use of safety-barrier diagrams, we have taken the example of a hydrogen refueling station. A hydrogen refueling station consists of a number of technical systems to fulfill the overall function to refuel road vehicles. There are different options for the refueling station with regards to supply and storage at the station. Hydrogen can be delivered by trucks or can be produced on-site e.g. by electrolysis. Hydrogen can be stored in liquefied or pressurized form. In our example we have taken the case of a refueling station were the hydrogen is delivered in liquid cryogenic form by a truck. This needs unloading facilities at the station. In Figure 4 a typical hydrogen refueling station is shown as it is described in the CEC FMEA study [1]. This refueling station exists of an unloading facility, a cryogenic storage tank where the main bulk of hydrogen is stored, an evaporator to gasify the hydrogen, a compressor and a small high-pressure hydrogen storage installation followed by the refueling facility to fill the pressure tank of the vehicles.

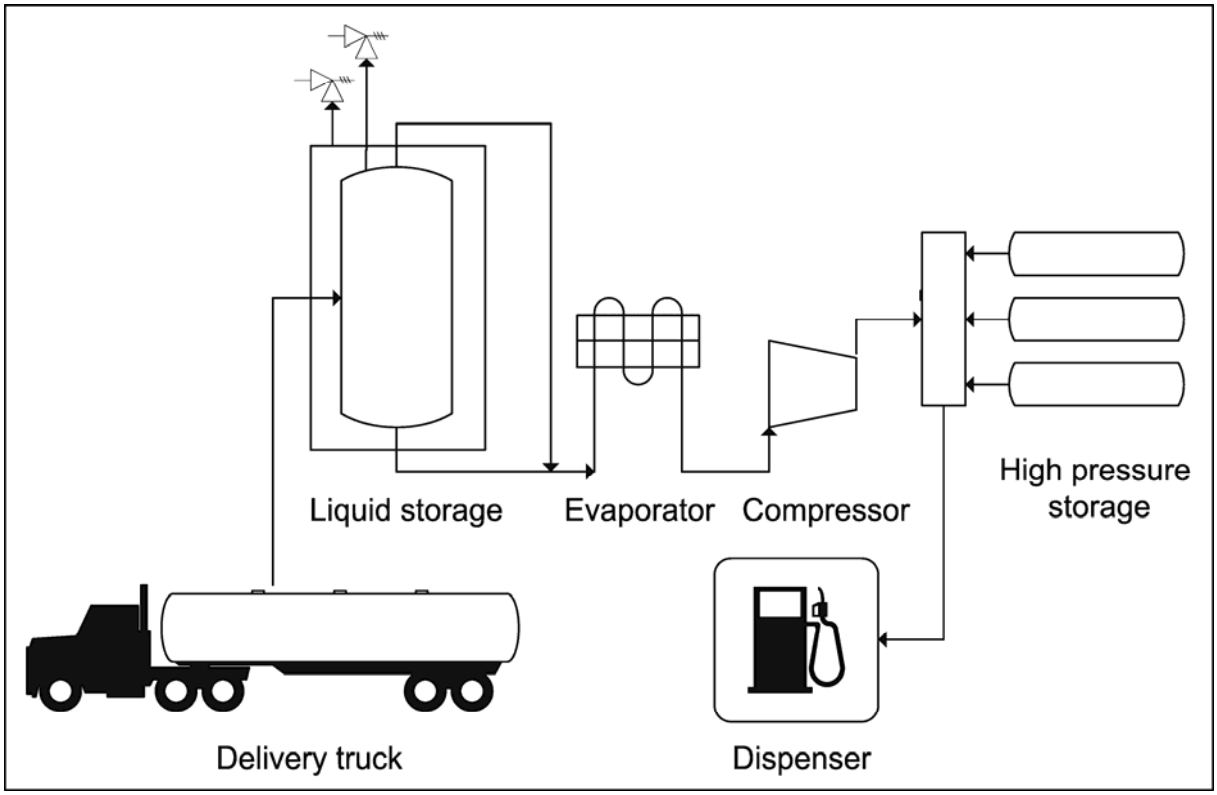

Figure 4 Process flow diagram for a hydrogen refuelling facility with cryogenic delivery

5 SAFETY ASSESSMENTS BY MEANS OF BARRIER DIAGRAMS

As an example, the FMEA analysis made for the liquid hydrogen fuelling station as described in the section above [1] has been used as the basis for two barrier diagrams: One for the truck unloading action, and one for the liquid storage tank, see Figure 5 and Figure 6, respectively. The software (”SafeBar” developed by Risø) used to draw these safety-barrier diagrams requires that all barriers are classified based on a predefined barrier classification. In this case we used the barrier classification as proposed by the ARAMIS project [9], that discriminates eleven different barrier types, covering passive (permanent) and active barriers with different levels of automation and human action. This classification proves to be very helpful, because it forces the analyst to consider “complete” active barriers, i.e. barriers that contain the full “detect – diagnose – act” sequence. The referenced FMEA study mentions some examples where controls only include the “detect” part of the barrier, such as hydrogen sensors. When drawing up these barrier diagrams, one should consider what preventive or mitigative action could follow when the sensors detect hydrogen (such as closing down all the transfer operations at the station), and in what state the facility would be when either the sensors work or when they fail to detect the explosive gas cloud.

Please note that the original FMEA-study as well as the safety-barrier diagrams presented here do not include the possible fire and explosion risks following a release of hydrogen.

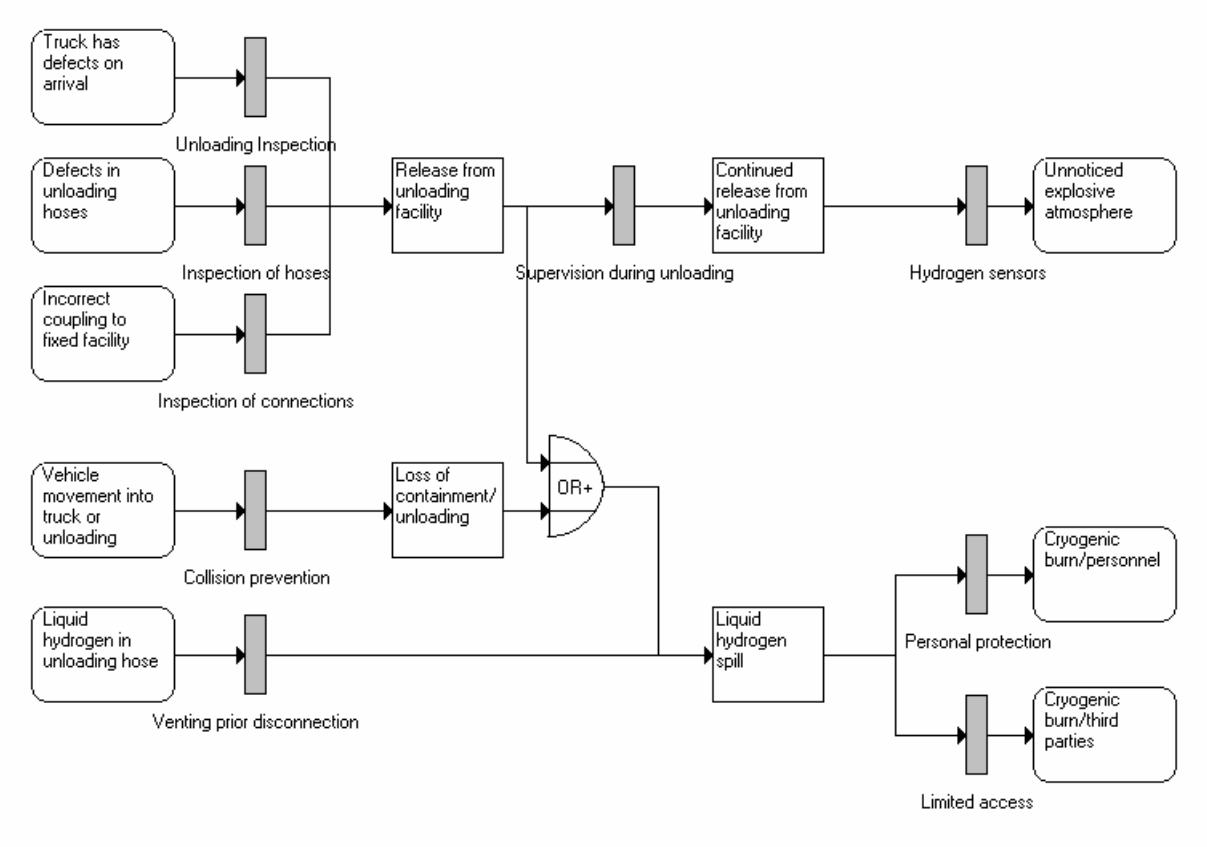

Figure 5. Safety-barrier diagram for the unloading of a liquid hydrogen truck at a refuelling station on the basis of the FMEA study in [1]

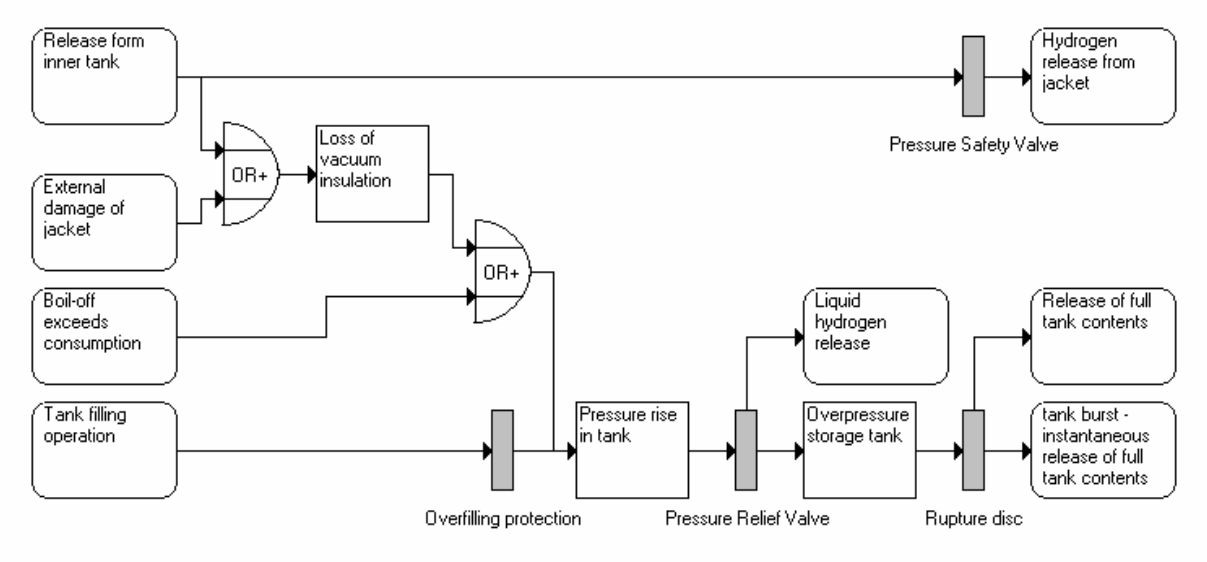

Figure 6. Safety-barrier diagram for the liquid hydrogen storage tank at the refuelling station on the basis of the FMEA study in [1]

Lists of the barriers and their classifications and detailed descriptions can be extracted from the software, and results are presented in Table 1 and Table 2. These tables can be automatically generated on the basis of the descriptions and information that are managed by the previously mentioned software tool. Here another

example of barrier classification can be discussed. The FMEA study suggests that impact from other vehicles with the unloading truck can be prevented by the driver putting caution cones around the truck. According to the ARAMIS classification, this would be an “activated barrier - warned (Human action based on warning, sign, alarm)” with the additional remark that the signs (cones) are temporary. Such a barrier is vulnerable to two failure modes: the cones are not placed or the vehicle ignores the warnings. A more robust option would be a combination of collision-resistant barriers (e.g. concrete poles, steel barrier) around the unloading facility in combination with a collision-resistant temporary barrier (fence) on the access way to the truck's unloading position.

Normally, safety-barrier diagrams are used to describe and document the final implementations of the safety measures, but the previous example shows that safety-barrier diagrams also can be used during the design and specification phase, where the barrier “blocks” can represent the more abstract barrier function (see section 2), in this case “Collision Prevention”, prior to decisions about how these barrier functions can be implemented in practice.

Table 1. Overview of safety barriers included in the diagram for unloading of the liquid hydrogen truck

Barrier Name	**Barrier Type according to ARAMIS**	**Description**
Unloading Inspection	Activated Barrier - Procedural (Observation of local conditions not using instruments)	On arrival of the truck, the truck is inspected visually for defects by driver or station operator (need to be decided who). The mitigation action what to do in case defects are noted need to be included.
Hydrogen sensors	Activated Barrier - Warned (Human Action based on passive warning)	Hydrogen sensors are located near the unloading facility The sensors themselves do not mitigate the presence of an explosive atmosphere, so a follow up has to be found in terms of alarms, evacuation, close down of unloading operation, close down of potential ignition sources
Inspection of hoses	Activated Barrier - Procedural (Observation of local conditions not using instruments)	Inspection of hoses before unloading/connection
Inspection of connections	Activated Barrier - Procedural (Observation of local conditions not using instruments)	Connections are inspected before unloading action is started
Supervision during unloading	Activated Barrier - Procedural (Observation of local conditions not using instruments)	The unloading action is monitored by personnel. Note that the personnel may become disabled by freeze burn - consider additional remote monitoring Deviations of the unloading lead to aborting the unloading action
Personal protection	Temporary Passive Barrier - Put in place (and removed) by person	Unloading operator and truck driver have donned protective clothing against cryogenic burn ("Nomex suit")

Barrier Name	Barrier Type according to ARAMIS	Description
Limited access	Activated Barrier - Warned (Human Action based on passive warning)	A safety distance around the truck and unloading facility where access is prohibited to third parties and personnel not involved in the unloading action Barrier can be enforced by signs, lights (when unloading) and supervision of personnel
Venting prior disconnection	Activated Barrier - Procedural (Observation of local conditions not using instruments)	Unloading hoses need to be vented prior to disconnection
Collision prevention	Temporary Passive Barrier - Put in place (and removed) by person /Permanent Passive Barrier/Activated Barrier - warned	Temporary Passive Barrier The unloading facility can be protected against external impacts such as third party traffic by: a) caution cones, b) concrete poles, and c) impact resistant movable fences/barriers

Table 2. Overview of safety barriers included in the diagram for the liquid hydrogen storage tank

Barrier Name	Barrier Type according to ARAMIS	Description
Overfilling protection	Activated Barrier - Manual (Human action triggered by active hardware detection)	Overfilling protection may consists of several independent systems, instruments, alarms and human intervention
Pressure Relief Valve	Activated Barrier - Hardware on demand	The inner tank is provided with two pressure relief valves. The release will be vented to a safe location (vertical upwards and well above the ground level) These relief valves will be able to handle pressure rise due to normal evaporation rates in the tank by venting vapour. Overfilling will cause the PRV's to dump liquid as well. Capacity will probably be too limited to handle full loss of insulation.
Rupture disc	Activated Barrier - Hardware on demand	On the line to the Pressure Relief Valve a rupture disc is mounted, that will release the tank pressure if the pressure rises above the set pressure of the PRV's. The release will be vented to a safe location (vertical upwards and well above the ground level)
Pressure Safety Valve	Activated Barrier - Hardware on demand	A pressure safety valve is mounted on the vacuum space between outer jacket and inner tank, that releases at 0 psig (0 barg, i.e. atmospheric pressure)

6 CONCLUSIONS

The methodology of safety-barrier diagrams has been introduced and exemplified by the safety analysis of two sections of a hydrogen refueling station. Safety-barrier diagrams offer a good overview of the safety precautions that are included in the different sections, and the consequences of the failure of these

precautions. The logic framework used for safety-barrier diagrams and the use of a classification for the different safety barriers forces the analysts to consider the completeness of the barriers (in terms of the detect-diagnose-act sequence) and the role of the safety barrier in the system.

The safety-barrier diagrams allow both quantitative and qualitative assessments to be made. Qualitative assessments can be based on requirements that consequences of certain severity need to be counteracted by a minimum number of safety barriers – the more severe the consequence, the more safety barriers are required.

The presentation by means of safety-barrier diagrams is simpler, and thereby easier to understand by non-experts than other graphical methods such as fault trees or event trees. Therefore safety-barrier diagrams are excellent means for documenting system safety and for communication with authorities and other stakeholders.

Safety-barrier diagrams support hazard analysis; they do not support or replace the preceding phase of hazard identification, for which exist a range of more suitable methods, such as FMEA or HAZOP

To support risk analysis by means of safety-barrier diagrams, Risø National Laboratory develops a software tool ("SafeBar") that manages the graphical presentation as well as the other information and descriptions of the safety barriers and system states. It is expected that this type of information system will support management of the safety barriers by keeping track of specifications, use, inspection and maintenance of these safety barriers.

ACKNOWLEDGEMENTS

The partial financial support from the NoE HySafe (SES6-CT-2004-502630) is gratefully acknowledged.

REFERENCES

1. Venkatesh S, Unnasch S, Powars C, Ozog H, Woody J.; Failure modes and effects analysis for hydrogen fueling options. Sacramento, California: California Energy Commission; 2004.
2. Sklet S.; Safety barriers: Definition, classification, and performance. *Journal of Loss Prevention in the Process Industries* 2006;19(5):494-506.
3. Hollnagel E. ; Barriers and Accident Prevention. Hampshire, UK: Ashgate; 2004.
4. Harms-Ringdahl L.; Assessing safety functions--results from a case study at an industrial workplace. *Safety Science* 2003;41(8):701-720.
5. Duijm NJ.; Safety-barrier diagrams, to be presented. ESREL, Stavanger, 25-27 June 2007
6. Duijm NJ.; Safety-barrier diagrams as a safety management tool (submitted for publication). *Reliability Engineering & System Safety* 2007
7. Duijm NJ, Goossens, LHJ.; Quantifying the influence of safety management on the reliability of safety barriers. *Journal of Hazardous Materials* 2006;130(3):284-292.
8. Aven T, Sklet S, Vinnem JE.; Barrier and operational risk analysis of hydrocarbon releases (BORA-Release): Part I. Method description. *Journal of Hazardous Materials* 2006;137(2):681-691.
9. Guldenmund FW, Hale AR, Goossens LHJ, Betten J, Duijm NJ.; The development of an audit technique to assess the quality of safety barrier management. *Journal of Hazardous Materials* 2006;130(3):234-241.