SafetyBarrierManager, a software tool to perform risk analysis using ARAMIS's principles

Duijm, Nijs Jan

Published in:
Risk Analysis and Management – Trends, Challenges and Emerging Issues: Proceedings of the 6th International Conference on Risk Analysis and Crisis Response (RACR 2017)

Publication date:
2017

Document Version
Peer reviewed version

Paper accepted for presentation at the 6th International Conference on Risk Analysis and Crisis Response (RACR-2017), June 5-9, 2017, Ostrava-Prague, Czech Republic

SafetyBarrierManager, a software tool to perform risk analysis using ARAMIS's principles

Nijs Jan Duijm

Technical University of Denmark DTU, Department of Management Engineering, Produktionstorvet 424, DK 2800 Kgs. Lyngby, Denmark, email nidu@dtu.dk
Nicestsolution, Baunegaardsvej 16, DK 4040 Jyllinge, Denmark, email nicestsolution@duijm.dk

Abstract

The ARAMIS project resulted in a number of methodologies, dealing with among others: the development of standard fault trees and "bowties"; the identification and classification of safety barriers; and including the quality of safety management into the quantified risk assessment.

After conclusion of the ARAMIS project, Risø National Laboratory started developing a tool that could implement these methodologies, leading to SafetyBarrierManager. The tool is based on the principles of "safety-barrier diagrams", which are very similar to "bowties", with the possibility of performing quantitative analysis. The tool allows constructing comprehensive fault trees, event trees and safety-barrier diagrams. The tool implements the ARAMIS idea of a set of safety barrier types, to which a number of safety management issues can be linked. By rating the quality of these management issues, the operational probability of failure on demand of the safety barriers can be calculated. The paper will give a short description of the features of the tool, with emphasis on the methodologies that originate from the ARAMIS project.

The paper will also address developments and experiences over the last years, which have inspired additional features. This includes a discussion of the use of generic management issues as opposed to concrete safety measures targeted at specific safety barriers, which includes a discussion of the basic philosophy in the ARAMIS methodology of dealing with safety management. The adjustments to the barrier typology is also discussed.

Introduction

The ARAMIS methodology is based, among others, on a set of standardized fault trees and the concept of safety barriers, which can be presented in a bow-tie diagram. At the end of the ARAMIS project, Risø National Laboratory concluded that they did not have access to a tool that in a user-friendly way could present these fault trees or bowties, nor implement safety barriers in a logic and consistent way. At the time, Danish process industry used the concept of "safety-barrier diagrams" widely, but these diagrams were always constructed manually, or by using the drawing capabilities of spreadsheet tools like Excel®.

Safety-barrier principles

Since the ARAMIS project, the concept of safety barriers has become widely known. There is a plethora of definitions around. In many contexts, the term "safety barrier" is used for any safeguard or risk-reducing measure that decreases the probability of consequence of an accident. In our methodology we limit the notion of "safety barrier" to those risk-reducing measures that acutely and autonomously respond to a potentially dangerous situation, i.e. safety barriers perform unplanned actions. In contrast, many other risk-reducing measures consists of actions that are planned or scheduled in advance, and where there is no direct relationship in time between the carrying out of the action, and a potentially dangerous situation being pertinent. Such safety actions are in our framework considered to be "safety-management measures", or in short: "management measures". Of course, there is a relation between the management measures and the safety barriers. The chance of successful deployment of the safety barrier depends on the proper design, installation, inspection, maintenance and replacement of the safety barrier, and, in so far the safety barrier comprises human action, in providing the proper education, competence, training, procedures, etc. to be able to take the right decisions at the right time.

Useful definitions make use of the concept of a "barrier function". This means that there may be different ways of implementing a barrier function: a specific safety barrier is just one such possibility. A often referred definition of a safety barrier is (Sklet, 2006):

- A *barrier function* is a function planned to prevent, control, or mitigate undesired events or accidents
- A *barrier system* is a system that has been designed and implemented to perform one or more barrier functions

Safety-barrier diagrams

The "SafetyBarrierManager" tool uses safety-barrier diagrams to show accident sequences. Following the definition, the function of a safety barrier is to abort a potentially dangerous situation. Such functioning can be showed graphically as a response to a potentially dangerous development, the *Demand Condition*, avoiding the dangerous outcome, the *Condition on Failure*, which would occur if the barrier was not present, or is not working properly. A successful deployment of the barrier may lead to the *Condition on Success*, see Figure 1. Figure 1 can be interpreted as a minimal example of a safety-barrier diagram. Depending on the complexity of the system, one can add more conditions or events, and more safety barriers.

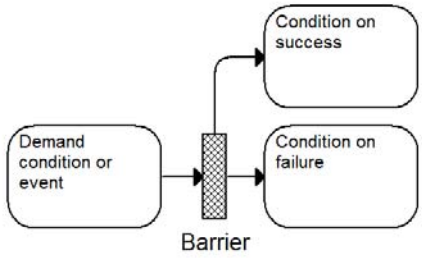

Figure 1 Definition of a safety barrier.

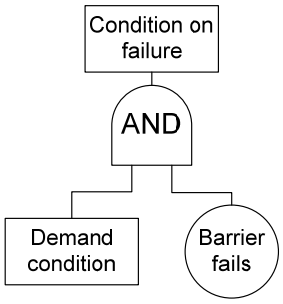

Figure 2 Fault tree representation of the safety barrier.

A safety-barrier diagram is a simplified cause-consequence diagram (Nielsen, 1971). It shows the sequence of possible events as an accident scenario. As the diagram shows a sequence of (potential) events, the order of the events, and thus the order of the safety barriers, has meaning, and the risk analyst shall consider the order of the barriers and events.

The safety-barrier diagram is very similar to the "bowtie" diagrams, which the ARAMIS project mentioned. Although the aspect of sequence was not addressed in the ARAMIS project, it is noted that common bowtie diagrams, including tools to graph bowtie diagrams, do not represent sequences of events, and indeed, sequential ordering of barriers is often not applied. Consequently, these bowties do not distinguish between the barriers that act in immediate response to potentially hazardous conditions and the risk reducing measures or safety management measures that are scheduled. Both types of risk reducing measures, the "real" barriers and the "safety management measures" may appear side by side in these bowtie diagrams.

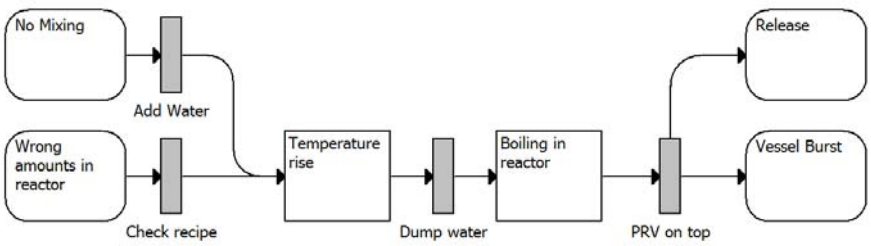

Figure 3 Example of a safety-barrier diagram

As an example, Figure 3 shows a barrier diagram for a run-away reaction in a batch reactor. The "SafetyBarrierManager" tool includes the logic to ensure that safety barriers are properly placed between the

Demand Condition and a Condition on Failure or a Condition on Success. Each safety barrier represents a simplified fault tree as shown in Figure 2. The logic is discussed in more detail in (N J Duijm, 2009). Due to the strict implementation of the logic, for each condition in the diagram it is possible to derive a fault tree that has this condition as top event. This is used to calculate the probability or expected frequency of the conditions. The Probability of Failure on Demand (PFD) of the safety barriers and the probability or expected frequency of the initial conditions are the inputs for that calculation.

Safety management: how it affects safety-barrier quality

The "SafetyBarrierManager" tool forces the risk analyst to assign a "safety-barrier type" to each safety barrier that is introduced in the safety-barrier diagram. The safety-barrier types belong to a predefined set of types. ARAMIS developed such a set of safety-barrier types, see Table 1. Barrier types 1-4 are normally considered to be "passive" barriers (there is no detection function), while types 5-11 are considered "active" barriers. By forcing the risk analyst to assign a barrier type, and thus compare the barrier with a description of a barrier type, we hope to minimize the use of incomplete barriers. Incomplete barriers are typically barriers where either detection (e.g. a "shut-down valve") or action (e.g. an alarm) is missing.

Table 1 Barrier typology as developed in ARAMIS (Andersen et al., 2004)*. Examples are mentioned for each type. N/A: Not Applicable; H: Hardware; S: Software; B: Behavioural, S: Skill-based; R: Rule-based; K: Knowledge-based.*

No.	Barrier type	Examples	Detect	Diagnose	Act
1	Permanent passive control	Pipe/hose wall, anti-corrosion paint, tank support, floating tank lid	N/A	N/A	H
2	Permanent passive barrier	Bund, dyke, railing, fence, blast wall, lightning conductor	N/A	N/A	H
3	Temporary passive	Barriers round repair work, blind flange, helmet/gloves/ goggles	N/A	(B)	H
4	Permanent active	Active corrosion protection, heating/cooling system, ventilation, explosion venting, inerting system	N/A	(B)	H
5	Activated/on demand	Pressure relief valve, interlock with "hard" logic, sprinkler installation, pressure/temperature/level control	H	H	H
6	Activated - automated	Programmable automated device, control system or shutdown system	H	S	H
7	Activated - manual	Manual shutdown in response to instrument reading or alarm, donning breathing apparatus or calling fire brigade on alarm	H	B.SRK	B/H
8	Activated - warned	Donning personal protection equipment in danger area, refraining from smoking, keeping within white lines, opening labelled pipe,	H	B.R	B
9	Activated - assisted	Using an expert system	H	S/B.RK	B/H
10	Activated - procedural	Follow start up/shutdown procedure, adjust setting of hardware, warn others to evacuate, empty & purge line before opening, lay down water curtain	B	B.SR	B/H
11	Activated - emergency	Response to unexpected emergency, improvised jury-rig during maintenance, fight fire	B	B.K	B/H

The other function of the barrier type is to enable to link the safety barrier to a set of management functions. Depending on the type of barrier, different actions will determine the quality of the barrier: barriers that depend on hardware require inspection and maintenance; barriers that depend on human behaviour require training, procedures and resource planning. Table 2 shows the list of "management issues" as proposed by ARAMIS. This table also shows the "weight factors" that describe how important the management issue is for ensuring the integrity of the safety barrier of the given type.

Table 2 Management issues and weight factors for adjusting safety-barrier performance as proposed by (Nijs Jan Duijm & Goossens, 2006)

ARAMIS management issue	ARAMIS weight factor $B_{i,k}$			
	Barrier types (Table 1)			
	1, 2, 4, 5, 6 (Hardware)	3, 8 (Temporary)	7, 9, 10 (Behaviour - R/S)	11 (Behaviour - K)
0 Safety Culture	0%	8%	15%	25%
1 Manpower planning & availability	0%	29%	58%	87%
2 Competence & suitability	0%	36%	72%	100%
3 Commitment, compliance & conflict resolution	0%	10%	20%	33%
4 Communication & coordination	0%	25%	50%	83%
5 Procedures, rules & goals	0%	9%	18%	40%
6 Hard/software purchase, build, interface, install	43%	22%	0%	0%
7 Hard/software inspect, maintain, replace	17%	8%	0%	0%

Based on an audit of the safety management system according to the ARAMIS methodology as described in (Guldenmund, Hale, Goossens, Betten, & Duijm, 2006), for each of the safety management issues a quality rating can be obtained: 100% for a perfectly functioning management issue and 0% if the management issue fails to meet any of its requirements. Given a design PFD of each safety barrier, i.e. the best (lowest) obtainable PFD assuming that all conditions and support functions are according to specifications, it is now possible to derive the operational PFD given the quality of the safety management according to the audit (Nijs Jan Duijm & Goossens, 2006):

$$\log(PFD_{operational,k}) = \left(1 - \sum_{i=0}^{7} (1 - S_i) \cdot B_{i,k}\right) \cdot \log(PFD_{design,k}) \quad (1)$$

Here S_i is the rating (between 0 and 1, with 1 for perfect rating) of management issue i, and $B_{i,k}$ the weight factor of management issue i for barrier type k, as presented in Table 2.

Table 3 Example of ratings for safety management issues.

Safety Management Issue	Rating
0 Safety Culture	75% (default)
1 Manpower planning & Availability	100%
2 Competence & suitability	86%
3 Commitment, compliance & conflict resolution	80%
4 Communication & coordination	85%
5 Procedures, rules & goals	80%
6 Hard/software purchase, build, interface, install	100%
7 Hard/software inspect, maintain, replace	80%

Table 4 The management weights and ratings as listed in Table 2 and Table 3 applied to the barrier diagram in Figure 3.

Type	Name	Design PFD	Operational PFD	Frequency using design PFD (per year)	Frequency using operational PFD (per year)
Initiating event	No mixing			0.021	(idem)
Barrier	Add water	0.02	0.0639		
Initiating event	Wrong amounts in reactor			0.01	(idem)
Barrier	Check recipe	0.1	0.1963		
Intermediate event	Temperature rise			0.00142	0.003305
Barrier	Dump water	0.02	0.0248		
Intermediate event	Boiling in reactor			$8.649 \cdot 10^{-5}$	$13.61 \cdot 10^{-5}$
Barrier	PRV on top	0.001	0.001265		
Consequence	Release			$8.641 \cdot 10^{-5}$	$13.59 \cdot 10^{-5}$
Consequence	Vessel Burst			$8.649 \cdot 10^{-8}$	$17.21 \cdot 10^{-8}$

Table 3 and Table 4 demonstrate the effect of reduced management quality when applied to the barrier diagram in Figure 3. The ratings in Table 3 have been have been taken from the example in the ARAMIS User Guide (Andersen et al., 2004). As can be seen, even modest reductions in management efficiency from 100% down to 80% may double the expected frequency of the worst consequence.

New developments – an alternative safety-barrier classification

During a number of studies, it was found that the barrier-type classification originally introduced by ARAMIS could be improved. This leads to the classification in Figure 4.

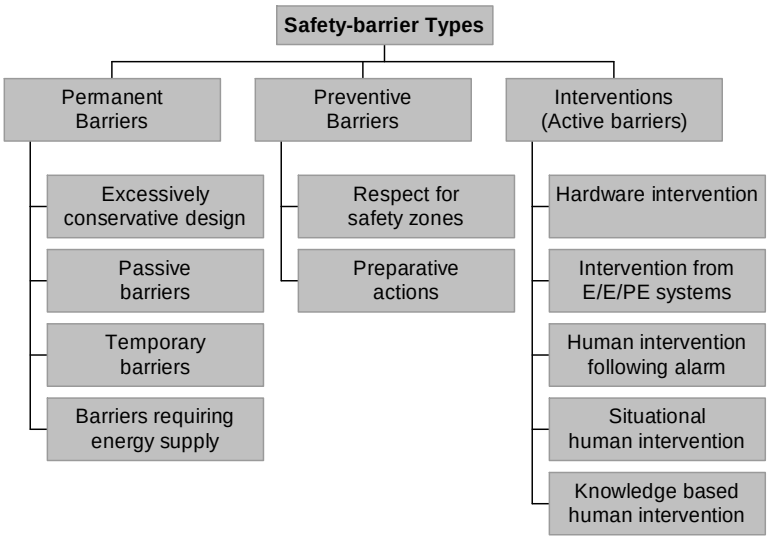

Figure 4 A new safety-barrier classification

- The type “Excessively conservative design” replaces the ARAMIS passive “control” barrier. “Controls” in the sense of the equipment and actions necessary to perform the primary process should not be considered as safety barriers. Failure of a primary process control is an initiating event, not a barrier failure. In order to allow for primary process controls with “built-in” aspects that are specifically added for a better safety performance, the “excessively conservative design” is included as a “barrier” instead. This barrier covers e.g. extra wall thickness and mechanical redundancy such as double steering rods.
- An extra group “preventive barriers” is introduced. This group is a kind of grey area between safety management measures and “real” barriers. They are not “real” barriers because they are invoked before the threatening situation occurs, so they can be considered “planned” actions. On the other hand, they represent actions closely linked to the daily operations and performed by the operators at the sharp end. After a number of studies, it turned out that these actions best could be introduced in the barrier diagram as safety barriers. The group includes the behavior of “respecting safety zones”, e.g. refrain from entering danger zones. It also includes “preparative actions”, e.g. venting tanks before entering (which was barrier type No. 8 in ARAMIS’s typology).
- On the other hand, the five different barrier types covering human intervention are reduced to three (type No.9 is removed while type No. 8 is moved into the “Preparative actions”, see above).

New developments – risk reducing measures

The philosophy of the ARAMIS project was to deal with safety management through an abstract, top-level approach. This was justified by the consideration that an evaluation of a management system by means of a management audit always would be based on selective spot checks of the management system. Therefore, efforts were aimed at ensuring how spot checks of the management system could be used to provide general statements on the effectiveness of all safety barriers. This is established through a direct link between top-level management issues and safety barriers as expressed in formula (1)

However, an industrial risk analyst drawing up barrier diagrams has access and knowledge of the detailed safety measures that link to specific safety barriers. Such safety measures can be e.g. inspection and maintenance plans, competence requirements for specific functions and tasks, and detailed procedures how to handle alarms and deviations. For an industrial risk analyst it is straightforward to link the detailed safety measures to the safety barrier. It is of importance to demonstrate (e.g. to the authorities) that such measures have been taken to ensure the integrity of the barrier. Each measure fits within a management issue, but that link is of lesser importance to the risk analyst in this context.

Figure 5 shows how the SafetyBarrierManager tool displays the detailed management measures linked to the barriers, but also to the initiating events in the example in Figure 3: Avoiding initiating events from happening, by ensuring the integrity of the primary process controls, is equally important as ensuring the integrity of the safety barriers.

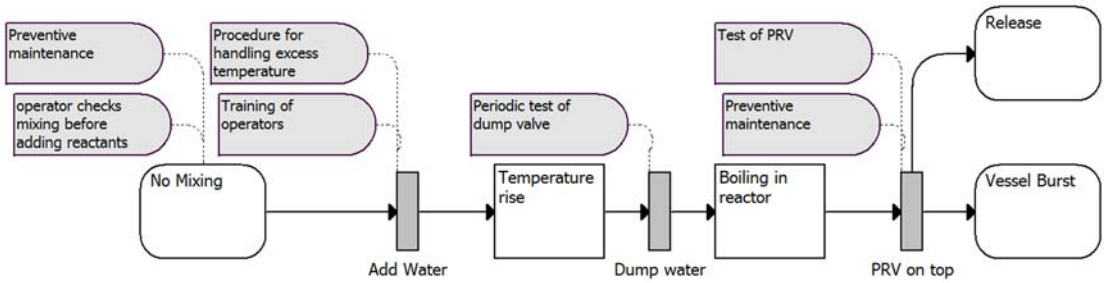

Figure 5 Safety-barrier diagram showing safety-management measures that a) prevent the initiating events or b) ensure the integrity of the safety barriers.

Discussion

The "SafetyBarrierManager" tool implements a number of the methodologies developed during the ARAMIS project. The tool is helpful in both qualitative assessments (showing implemented risk reducing measures) and quantitative assessments (by calculating the expected frequency of consequences).

Experiences gained by using this tool has initiated some changes and provoked the need for additional features. There is still a need for better understanding of the relation between safety management and the quality of safety barriers, and the role safety management may have as a common cause factor for the simultaneous failure of barriers, as has been suggested in (Markert, Duijm, & Thommesen, 2013).

References

Andersen, H., Casal, J., Dandrieux, A., Debray, B., de Dianous, V., Duijm, N. J., … Tixier, J. (2004). *ARAMIS User Guide*. Retrieved from http://safetybarriermanager.com/files/aramis/ARAMIS_FINAL_USER_GUIDE.pdf

Duijm, N. J. (2009). Safety-barrier diagrams as a safety management tool. *Reliability Engineering and System Safety*, *94*(2), 332–341.

Duijm, N. J., & Goossens, L. H. J. (2006). Quantifying the influence of safety management on the reliability of safety barriers. *J.Haz.Mat.*, *130*(3), 284–292.

Guldenmund, F. W., Hale, A. R., Goossens, L. H. J., Betten, J. M., & Duijm, N. J. (2006). The Development of an Audit Technique to Assess the Quality of Safety Barrier Management. *J.Haz.Mat.*, *130*(3), 234–241.

Markert, F., Duijm, N. J., & Thommesen, J. (2013). Modelling of safety barriers including human and organisational factors to improve process safety. In *Proc. 4th Int. Symp. on Loss prevention and safety promotion in the process industries* (pp. 283–288). Florence, Italy.

Nielsen, D. S. (1971). *The Cause/Consequence Diagram Method as a Basis for Quantitative Accident Analysis* (Vol. Risø-M-137). Roskilde: Danish Atomic Energy Commision, Risø.

Sklet, S. (2006). Safety barriers: Definition, classification, and performance. *Journal of Loss Prevention in the Process Industries*, *19*(5), 494–506.