MPMM

Maintenance Performance
Measurement and Management

Proceedings of Maintenance Performance Measurement and Management (MPMM) Conference 2014

Risk Management based on the Assessment of Safety Barriers

[1]José Sobral; [2]Carlos Guedes Soares

[1] jsobral@dem.isel.ipl.pt; [2] c.guedes.soares@centec.tecnico.ulisboa.pt

[1] Mechanical Engineering Department, ISEL – Instituto Superior de Engenharia de Lisboa Lisboa, Portugal

[1,2] Centre for Marine Technology and Engineering (CENTEC), Instituto Superior Técnico, Universidade de Lisboa, Av. Rovisco Pais, 1049-001 Lisboa, Portugal

***Abstract* – The present paper deals with safety barriers, describing their characteristics and presenting a new classification for them based on their type and operating mode. While the assessment of safety barriers performance is often achieved by tests or inspections in order to determine the probability of failure on demand (PFD) and detect the so-called hidden failures, a new methodology to evaluate the adequacy of a safety barrier is proposed by linking the safety integrity level of an assessed safety barrier with the probability of occurrence of the hazardous event that it should protect. Based on the study of all possible safety function failures there is a selective approach to determine the ones classified as dangerous undetected in a way to use them on the determination of the PFD. Applying the methodology proposed it is also possible to estimate the probability of occurrence of a hazardous situation, once it depends on the simultaneity of happening the initiating event and the safety barrier fault, when a demand occurs. The impact of a specific safety barrier assessment on risk can thus be evaluated.**

Keywords—safety barrier, probability of failure on demand, safety integrity level.

I. Introduction

In complex and technological industrial systems when some control variables go out of their natural range it can be a sign of failure of some equipment or process. To face this type of events and avoid the escalation of an incident or accident it is common to implement systems called safety barriers which function is to prevent the occurrence of such events or disable the evolution of their effects. If these functions are not accomplished it is considered a safety barrier's failure and then the consequences could be catastrophic in almost cases.

So, it is essential to assure that safety barriers have high availability and high reliability to keep risk under acceptable limits. The assessment of safety barriers availability and the reliability analysis of their functions are fundamental issues to take into account when, for example, someone wants to assure a high level of safety onsite or reduce the consequences of dangerous phenomenon or hazardous events on people, business or environment.

Most accidents result from a combination of an unexpected event and a dysfunctional or missing barrier. Usually, when an accident occurs the question is how could it happen if we had several safety features in place to face it? So it is essential to understand how those safety barriers failed in the course of an accident.

Several studies about safety barriers have been performed in a large range of industries and with different purposes.

Kecklund *et al* [1] presented a study with a general model for the reliability analysis of existing barrier functions in the refuelling process at the annual outage of a nuclear power plant (NPP) assuming on that study the technology-human interaction. Harms-Ringdahl [2] describes a method for accident investigation based on the concept of safety function, resulting on the proposal of some safety improvements. This author applied the referred method to five different incidents where around 40 safety functions were identified for each case and less than a half had worked when it was necessary. In this work the main attention is on common workplaces rather than major hazard installations. In other study safety barrier diagrams were developed as a tool for modelling safety of hydrogen applications just to document measures taken to prevent incidents and accidents in process industry [3]. Some works deal with operating situations and apply the notion of safety integrity level of a barrier at specific cases as the safety evaluation in complex guided transportation systems [4] or estimation of this parameter for safety related systems in high speed trains [5].

In this paper a deep reflection is done about safety barriers regarding different interpretations about some concepts and terminology in the existing literature. Based on this analysis a simple and coherent classification is made being possible to apply it to the majority of the safety barriers. A new methodology is also proposed in a way to evaluate the adequacy of a safety barrier for a specific hazard. This methodology is innovative since it links the safety integrity level of an assessed safety barrier with the probability of occurrence of the hazardous event that it should protect. Based on this relationship and using a risk acceptability matrix the adequacy of the safety barrier is evaluated.

The paper is structured in five Sections. The second focuses on the definition of safety barrier, safety function and safety barrier classification. Section III describes some safety integrity requirements and how to develop a safety barrier assessment. Section IV presents a methodology to assess safety barriers and illustrates it with a demonstrative example. Section V presents some conclusions and suggests future

ISBN 978-972-8954-42-0 | http://dx.doi.org/10.14195/978-972-8954-42-0_22

works that can be done on the field of safety regarding the management of safety barriers and the proposed methodology.

II. Safety barriers

The definition of safety barrier is not unanimous and different interpretations can be seen on literature. Sometimes this kind of features and characteristics are called defences or energy models. Types and classification of safety barriers can also promote some discussion. For example, a division of hard and soft defences was made by Reason, where the former include physical barriers and alarms and the later refers to regulation, procedures and training [2]. For this reason, and according to the author, defence is a wider concept than barrier. The concept of "defence-in-depth" is also discussed meaning successive layers of protection.

Regarding an interesting work done by Sklet [6] about safety barriers definition, classification and performance, it has been concluded that either in literature or standards there are not universal definitions for terms like safety barrier, defence, layer of protection analysis (LOPA), safety function or other related terms.

II.1. Safety barrier and safety function

In accordance to his review Sklet [6] defines safety barriers as physical and/or non-physical means planned to prevent, control or mitigate undesired events or accidents. It is distinct of a safety function that means a function planned to prevent, control or mitigate undesired events or accidents and so describes the purpose of safety barriers with a direct and significant effect. Usually, a safety function is described with a verb and a noun (e.g. "open valve"). A barrier system is a system designed and implemented to perform one or more barrier function. Hollnagel [7] distinguishes between what barriers "do" and what barriers "are", pointing out the first situation as the safety function and the last one as the way to achieve the referred function, meaning the barrier system by itself.

Duijm [8] defines in a simple way a safety barrier as a series of elements that implement a barrier function, where each element consists of a technical system or a human action.

In accordance to Dianous and Fiévez [9] safety barriers can be physical and engineered systems or human actions based on specific procedures or administrative controls. Sometimes these two types are interchangeable and work together to keep the effectiveness of the safety function. So, safety barrier is related to the way how the safety function is accomplished.

II.2. Safety barrier classification

Concerning safety barrier classification, several interpretations can be seen when observing the literature available. There is not a consensus about safety barrier classification. Dianous and Fiévez [9] define four main categories for safety barriers:

- Active barriers – Barriers automated or activated manually and always require a sequence of detection-diagnosis-action. This sequence can be performed using hardware, software and/or human actions;
- Passive barriers – Barriers with permanent functioning where there is no need for human actions and energy or information sources (e.g. firewall, corrosion prevention systems or inherent safe design);
- Human actions – Barriers which effectiveness is related with the knowledge of the operator. These human actions rely on the use of the human senses, effective communication, thinking, rules, guidelines and safety principles and may be part of the detection-diagnosis-action sequence;
- Symbolic barriers – Barriers that need an interpretation by a person in order to achieve their purpose (e.g. passive warnings).

Hollnagel [7] also presents four types of systems or barriers, but with a different notation:

- Physical (or material) barrier – Barrier that prevents the event occurrence or mitigates the effects by blocking the transportation of mass, energy or information from one place to another (e.g. walls, containers, fire curtains);
- Functional barrier – Barrier that creates one or more pre-conditions that have to be met before an action can be carried out (e.g. interlock system);
- Symbolic barrier – Barrier that works indirectly through their meaning, requiring an interpretation by someone (e.g. signals, warnings or alarms);
- Incorporeal barrier – Barrier that it is not a physical barrier, depends on the knowledge of the user and is often related to organisational barriers (e.g. rules for actions).

Independent of their classification, safety barriers can be represented in a bowtie diagram, where preventive and protective safety functions are included. Figure 1 shows those safety barriers on both sides of the diagram.

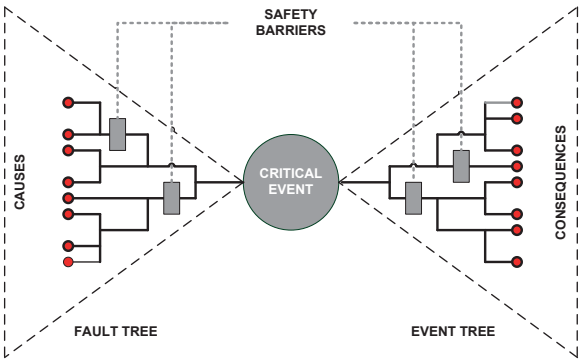

Fig. 1. Bowtie diagram for safety barriers

In this paper it was established and assumed a safety barrier classification based on two factors:

- Type of barrier – what barrier "is";

- Mode of operation of the barrier – how it "operates".

The different types and modes proposed on this paper are shown on Figure 2. This classification was used in the demonstrative example of Section IV.

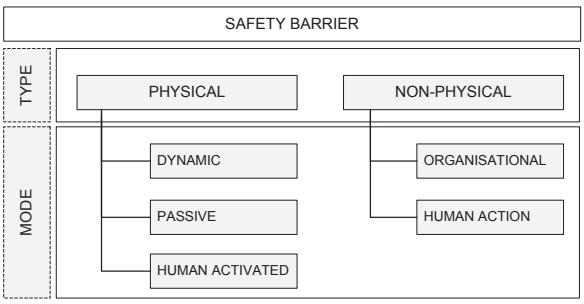

Fig. 2. Safety barrier classification

The "type" of safety barrier defines if it is a physical or a non-physical system. It means that a physical safety barrier is something that exists whether its function could be preventive or protective. The "mode" is related with the way how it acts when a demand happens.

A dynamic safety barrier corresponds to an automated system that is expected to operate changing from a dormant state to a living state and without human intervention (e.g. an automated sprinkler system or an automated shutdown valve).

A passive safety barrier is intended as static system that remains in the same state and usually is a design system with protective function (e.g. a fire wall).

A human activated safety barrier is a physical system that needs to be activated by someone. This is what differentiates a human activated safety barrier from a dynamic safety barrier.

By other side, an organisational safety barrier is related to training, safety procedures and internal rules and regulations established to avoid an accident or incident or to minimise the effects of the consequences (e.g. evacuation procedure).

At last, a human action safety barrier is any human actuation that not involves the use of physical systems (e.g. workplace cleaning).

III. Safety Integrity Requirements

IEC 61508 [10] standard represents a guide for design, validation and verification of a safety instrumented system (SIS) which fundamental purpose is to bring the plant or equipment to a safe state if an undesirable events occurs. The probability of a SIS satisfactory perform the required safety function under all the stated conditions within a specific time interval is called safety integrity. This standard defines four discrete levels for safety integrity named "safety integrity level" (SIL). In this scope a "SIL 4" corresponds to the higher level of safety integrity and "SIL 1" to the lowest one. The hardware safety integrity requirements include an estimation of the probability of failure on demand (PFD) or probability of failure per hour (PFH), when a low or high demand (or even continuous) mode occurs, respectively [11].

Table I shows the safety integrity levels according IEC 61508 for the two situations above mentioned.

Table I. Safety Integrity Levels (SIL)

SIL	Low demand mode (average probability of failure on demand)	High demand or continuous mode (probability of a dangerous failure per hour)
4	10^{-5} - 10^{-4}	10^{-9} - 10^{-8}
3	10^{-4} - 10^{-3}	10^{-8} - 10^{-7}
2	10^{-3} - 10^{-2}	10^{-7} - 10^{-6}
1	10^{-2} - 10^{-1}	10^{-6} - 10^{-5}

Jin *et al* [12] refer the IEC 61508 to define a low demand when the demand rate is less than once per year and less than twice the functional test frequency giving the example of emergency shutdown systems (ESD), fire and gas detection systems, process shutdown systems (PSD) and airbag systems installed in cars. For high demand systems the referred authors give the example of dynamic positioning (DP) systems for ships and offshore platforms, anti-lock braking systems (ABS) and railway signalling systems.

The IEC 61508 refers a "low demand mode" when the safety function is only performed on demand, in order to transfer the equipment under control (EUC) into a specified safe state, and when the frequency of demands is no greater than one per year. A high demand mode refers the situation where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is greater than one per year. Continuous mode is where the safety function retains the EUC in a safe state as part of normal operation.

The PFD is related to safety unavailability of the system and corresponds to the fraction of time that the system is unavailable to perform its function when the plant is operating. It can be modelled by several classical tools and methods such as Fault Tree Analysis (FTA), Markov Analysis (MA) and Reliability Block Diagrams (RBD), among others [13].

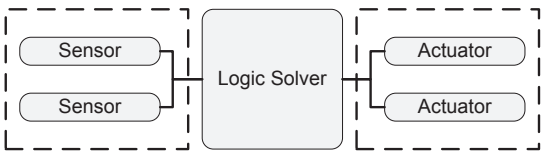

Fig. 3. Structure of a Safety Instrumented System (SIS)

Usually a SIS is presented as a structure with three main sub-systems, as shown in Figure 3. The first sub-system is related with the input elements present to detect the occurrence of a hazardous event such as sensors, switches, detectors, etc. The second sub-system concerns a logic solver

ISBN 978-972-8954-42-0 | http://dx.doi.org/10.14195/978-972-8954-42-0_22

or logic unit which is the element that will decide what to do (programmable logic devices, multi-agent structure, etc…). Finally, the last sub-system, including actuators (shutdown valves, cut-off energy devices, etc.) as the elements responsible for performing one or more safety instrumented functions (SIF), in accordance with the decision previously taken.

III.1. Safety barrier parameters

Risk control criteria are linked to the frequency and the severity of accident scenarios. The assessment of the frequency of occurrence of dangerous events is often based on statistical data. However, each analysis must be carried out with carefully because the available information is based on averaged data from different types of installation.

Usually, safety barriers are submitted to self-diagnostic and periodic tests or inspections. A dangerous failure puts the safety related system into a hazardous or failed condition. This happens, for example, due to existence of a hidden failure not detected by any kind of monitoring technique and only detected at the next test or inspection. A safe failure means a failure without the hazardous potential. When the dangerous failure is detected by some monitoring technique or self-tests, that is called as a dangerous detected failure. The following rates, assumed to be constant are then defined [14]:

- λ_{DU} = Dangerous undetected failure rate;
- λ_{DD} = Dangerous detected failure rate;
- λ_{SU} = Safe undetected failure rate;
- λ_{SD} = Safe detected failure rate;
- λ_S = Safe failure rate (detected + undetected);
- λ_D = Dangerous failure rate (detected + undetected);
- μ_{DD} = Repair rate (for dangerous detected failure).

Concerning the IEC 61508 some qualitative requirements can also be undertaken related to the architectural constraints that could limit the achievement of a determined SIL. These constraints could be the ability of a functional unit to continue to perform a function in the presence of faults or Fault Tolerance (FT) or the Safe Failure Fraction (SFF) which is a parameter that gives the fraction of overall hardware failure rate of the device considered as "safe", given by:

$$SFF = \frac{\lambda_S + \lambda_{DD}}{\lambda_S + \lambda_D} \quad (1)$$

The SFF value can be used to obtain a type of architecture for a given SIL (concerning the hardware fault tolerance) or can be applied to quantify the maximum expected SIL for a given architecture (type of SIS complexity) [14].

The ratio of the dangerous detected failure rate with respect to the total dangerous failure rate is called the "Diagnostic Coverage" (DC) and is an important parameter to be taken into account once dangerous failures early detected allows avoiding or mitigating undesirable situations.

$$DC = \frac{\lambda_{DD}}{\lambda_D} \quad (2)$$

Reference should also be made to a similar standard, known as ANSI/ISA-S84.01-1996, because it is still a guidance document in the United States (US), considered by the US Environmental Protection Agency (EPA) and the Occupational Safety and Health Administration (OSHA) as a generally accepted good industry practice. Based on this assumption it is mandatory that any US based instrumented system specified after march 1997 must be designed and developed in compliance with this standard [15] [16].

The dangerous undetected (DU) failure rate is due to failures related to non-safe situations and is influenced by the Diagnostic Cover factor.

$$\lambda_{DU} = (1 - DC).\lambda_D \quad (3)$$

The periodic activity of safety barrier testing has the objective to find dangerous undetected failures or hidden failures and so achieve and improve the safety integrity level of the system.

The test interval (τ) should be, by one side the shortest one in a way to detect potential hidden failures, but by another side this kind of frequency brings higher cost and eventually increases the probability of human error induced during the referred tests. In general DU failures of the SIS are not detected immediately and are also referred to as dormant failures [17] [18].

After determining the PFD, a discrete SIL level is defined (Table I). Each SIL number represents a bounded interval for the probability of failure on demand (PFD). Some people assume the PFD as the average value of the unreliability function over an inspection period, but others interpret that as the steady state unavailability. In this later concept it is necessary to apply a Markovian approach just to observe the behaviour of the SIS in a continuous time, including the inherent repair rates.

Some studies introduce the concept of safety-related uncertainty when determining the safety integrity level (SIL). Xu *et al.* [19] state that the conventional global sensitivity analysis (GSA) is inappropriate to handle overall uncertainty when safety related uncertainty is of interest. The authors present and discuss four methods to measure it and compare with GSA. GSA is a useful technology to determine which parameters influence the output the most when uncertainty in the parameters is propagated through the model. It can identify critical parameters and rank them with respect to reliability and risk.

III.2. Layer of protection analysis

The layer of protection analysis (LOPA) is a method for determining the needed SIL of a SIS. This method can be applied after the HAZOP (Hazard and Operability) analysis where the identified consequences are classified for severity level. During the HAZOP analysis the various process deviations are analysed and the possible consequences are determined. To reduce or mitigate the effect of the consequences of the hazardous event some safeguards or barriers are designed. LOPA is a semi-quantitative methodology that can be used to identify safety barriers that

meet the independent protection layer (IPL) criteria and work as extrinsic safety systems (active or passive systems). Summers [20] states some examples of IPL:

- Standard operating procedures;
- Basic process control systems;
- Alarms with defined operator response;
- Safety instrumented systems;
- Pressure relief devices;
- Blast walls and dikes;
- Fire and gas system;
- Deluge systems.

In accordance with the same author, LOPA provides specific criteria and restrictions for the evaluation of IPL, eliminating the subjectivity of qualitative methods and substantially less cost than fully quantitative techniques.

The IPL must meet the independence, specificity, dependability and auditability requirements. It means that the IPL must be completely independent of the initiating event. The probability of failure on demand (PFD) of an IPL is a measure of the risk reduction that can be obtained. For SIS the PFD is observed as the SIL level.

III.3. Safety barrier assessment

Several methods related to barrier assessment and several variants can be found in literature. Methods such as the energy model, the Management Oversight and Risk Tree (MORT) method, the Accident Evolution and Barrier (AEB) analysis or the more classical Fault Tree Analysis (FTA) or Event Tree Analysis (ETA) are some of the methods used to study safety barriers.

The determination of the PFD of the safety functions are carried out according to the principles derived from the safety integrity level concept available in IEC 61508 [10] and IEC 61511 [21] standards knowing the reliability of the safety barrier. IEC 61508 is a generic standard common to several industries that states requirements for safety systems, while IEC 61511 was developed to the process industry.

In accordance with the regulations of Petroleum Safety Authority (PSA) in Norway, the performance of barriers can be seen as comprising three elements [22]:

- Functional requirements - Qualities such as capacity and efficiency related to the effect that the barrier has on the event/accident chain given that it functions;
- Integrity requirements - Qualities such as availability and reliability related to the barrier's ability to function when required and/or demanded;
- Vulnerability requirements – Qualities related to robustness and the barrier's ability to withstand relevant accidental loads.

Hollnagel [7] presents several different possible points to evaluate the quality of a safety barrier:

- Efficiency – how well the safety barrier meets its intended function;
- Resource needs – cost to design, develop and maintain a safety barrier;
- Robustness – related to reliability, measures how well a barrier can withstand the variability of the environment;
- Implementation delay – corresponding to time from safety barrier conception till its implementation;
- Availability – whether the barrier can fulfil its purpose when needed;
- Evaluation – how easy is the determination if the safety barrier works as expected;
- Independence – the safety barrier doesn't depend on human actuation to achieve its purpose.

The ARAMIS project presents three criteria for the assessment of the performance of safety barriers [9]:

- Effectiveness - is the ability of a safety barrier to perform a safety function during a determined period of time, in a non-degraded mode and in specified conditions. It is usual to present the effectiveness as a percentage or probability of the performance of the defined safety function;
- Response time - is related to the period between the straining of the safety barrier and the complete achievement of the safety function performed by the safety barrier;
- Level of confidence - is related to its reliability and is inversely proportional to the probability of failure on demand (PFD). It corresponds to the reliability of the barrier to perform properly the required safety function according to a specific effectiveness and response time under the stated conditions within a stated period of time.

The level of confidence of a safety barrier is based on some qualitative factors such as:

- The independence of the safety barrier (with causes and regulation systems);
- The architecture of the safety barrier (according to the complexity of the subsystems);
- The proven concept of the barrier (tested, experienced);
- The existence of periodic tests.

The level of confidence of a subsystem relies on two parameters:

- The Safe Failure Fraction (SFF) – Ratio between the frequency of failure corresponding to a safe failure and the frequency of failure of total failures;
- The Fault Tolerance (FT) – Linked to the capacity of the barrier to keep its safety function although the failure of one or more subsystems that belong to the safety barrier. It is usually kinked to the existence of redundancies. A Fault Tolerance of "1" means that if one component is defective, the safety function remains operational.

ISBN 978-972-8954-42-0 | http://dx.doi.org/10.14195/978-972-8954-42-0_22

In this case, the referred IEC 61508 and IEC 61511 standards divide the subsystems into two main classes or types:

- Type "A" – Simple Subsystem – If the failure modes of all safety barrier components are well defined;
- Type "B" – Complex Subsystem – If the failure mode of at last one component is not well defined.

The qualitative criteria for these two types of constraints are presented in Table II:

TABLE II. ARCHITECTURAL CONSTRAINTS

Safe Failure Fraction (SFF)	Fault Tolerance (FT)					
	Type "A"			Type "B"		
	0	1	2	0	1	2
SFF<60%	LC 1	LC 2	LC 3	na	LC 1	LC 2
60%<SFF<90%	LC 2	LC 3	LC 4	LC 1	LC 2	LC 3
90%<SFF<99%	LC 3	LC 4	LC 4	LC 2	LC 3	LC 4
SFF≥99%	LC 4	LC 4	LC 4	LC 3	LC 4	LC 4

na = not applicable

For example:

- For a simple (type "A") SIS, with a 1oo2 architecture and a SFF of 75%, it is expected a SIL 3 or LC 3 (maximum);
- For a complex (type "B") SIS, with a SFF of 80% and a desired SIL 2 or LC 2, it is recommended a FT of 1, with an architecture of 1oo2.

The quantitative criteria are related to the probability of failure of the subsystems (type "A" or "B") and depends on the mode of operation (low demand or high demand or continuous mode), as presented on Table I. On the level of confidence concept there is a correspondence between the LC and the SIL numbers.

The level of confidence of the safety barrier is then achieved assuming the lowest level of confidence of the analysed subsystems. Langeron *et al.* [14] and Guo and Yang [23] go a little bit further explaining how to determine the SIL/LC for series and parallels arrangements of subsystems in a way to achieve the global SIL/LC for a system (safety barrier).

IV. METHODOLOGY PROPOSED

Following the previous Sections and all the theoretical and practical issues analysed, a methodology to assess safety barriers is proposed in this Section. In simultaneous a demonstrative example is presented to show the applicability of the methodology to a real safety barrier.

The demonstrative example is based on a common safety system that is present in almost industrial facilities and commercial or residential buildings. This system acts in a protective mode, facing the undesirable consequences of a fire and so it is called "fire fighting system". The equipment under control (EUC) is assumed to be the facility or the building itself and the safety barrier is the "fire pumping system". Its safety function (SF) is to pressurize water to the fire extinguishing system. This equipment can be assessed assuming it as an independent protection layer (IPL) and applying the structure of a safety instrumented system (SIS) (see Figure 3).

In accordance with the classification proposed in this paper in Section II.2, this safety barrier is classified as:

- Type = Physical;
- Mode = Dynamic.

Based on these principles and regarding all the equipment design details and operating mode, the three subsystems of the SIS were defined as shown in Table III.

TABLE III. SAFETY BARRIER SUBSYSTEMS

Subsystem	ID	Individual Function
Sensor System	Pressure Switches	Detect a pre-selected pressure level and transmit an electric signal to the Control System. It includes two starter pressure switches (one per pump) and two security pressure switches (one per pump).
Logic System	Control System	Receive the electric signal from the Pressure Switches and give order to activate the Pressurization System (one jockey pump and one of the two main pumps).
Actuator System	Pressurization System	Receive the order from the Control System and put a determined flow of water at a determined pressure (design characteristics) on the hydraulic fire fighting system (extinguishing system).

The following step of the methodology is to describe all subsystem failure modes. At this stage a team work and a historic of failure analysis is fundamental once both potential and registered failures are essential to complete this part of the methodology. This is a kind of a partial failure mode and effects analysis (FMEA).

After this, the next step is to classify the safety function failure. To do so, it must be fulfilled for all identified failure modes the degree of severity as "safe" or "dangerous" and the degree of detectability as "yes" or "no". Based on the combination of these two factors the safety function failure could be classified as shown in Table IV.

TABLE IV. SAFETY FUNCTION FAILURE CLASSIFICATION

Severity	Detectability	Safety Function Classification
Safe	Yes	SD – Safe Detected
Safe	No	SU – Safe Undetected
Dangerous	Yes	DD – Dangerous Detected
Dangerous	No	DU – Dangerous Undetected

From this classification all the dangerous undetected failure modes are selected and analysed at the next stage. For each one a dangerous undetected failure rate is achieved and based on the test interval (τ) of the subsystem an individual PFD_i is determined.

$$PFD_i = \frac{\lambda_{DU}.\tau}{2} \quad (4)$$

The PFD_{SS} of each subsystem is reached assuming the highest individual PFD_i.

$$PFD_{SS} = \max(PFD_i) \quad (5)$$

The safety barrier probability of failure on demand (PFD_{SB}) is then determined by the sum of the subsystems probability of failure on demand (PFD_{SS}) once the failure of the safety barrier could happen due to a failure on the Sensor System **or** on the Logic System **or** on the Actuator System.

$$PFD_{SB} = \sum PFD_{SS} \quad (6)$$

Based on the PFD_{SB} and on Table I the safety integrity level (SIL) is determined.

The next step is to estimate the probability of occurrence of the initiating event (POIE). At the present example the initiating event is the existence of a "fire". The estimated probability value is then allocated into one of five levels according to Table V.

TABLE V. PROBABILITY OF OCCURRENCE OF INTITIATING EVENT (POIE)

Level	ID	Probability [occur./year]
Very High	VH	p > 1
High	H	0,5 < p < 1
Moderate	M	0,1 < p < 0,5
Low	L	0,001 < p < 0,1
Very Low	VL	p < 0.001

Finally, the acceptance of the safety barrier is based on the determined SIL and on the POIE. If the result falls into a red zone of the matrix represented on Table VI it is not acceptable and something must be done (e.g. implement measures to reduce the POIE or increase the SIL value of the safety barrier). If it falls on the yellow zone it is acceptable but with remarks (meaning that an accurate analysis should be done on that cases). Obviously the green zone is the desirable one meaning that we have a safety barrier integrity level adequate to accomplish the safety function for the considered hazard.

It is also possible to determine the probability of a hazardous situation taking into account the POIE and the SIL corresponding to the PFD_{SB}.

$$PHS = PFD_{SB}.POIE \quad (7)$$

In accordance to the proposed methodology a simple tool was developed bringing automated and reliable results.

TABLE VI. ACCEPTABILITY MATRIX

POIE	SIL			
Very High	4	3	2	1
High	4	3	2	1
Moderate	4	3	2	1
Low	4	3	2	1
Very Low	4	3	2	1

V. CONCLUSIONS AND FUTURE WORK

This study illustrates how risk can be managed through safety barriers assessment. Some standards related to the assessment of safety barriers and safety functions were referred and some misunderstanding around concepts and their interpretation was clarified. It was proposed a classification for safety barriers according to their type and operation mode.

In the present work some requirements that must be fulfilled to achieve the necessary integrity level were mentioned and it was shown how to reach them.

Based on the theory and on previous works about safety barriers, safety instrumented systems and risk management a new methodology to assess safety barriers was proposed. In this methodology it is possible to identify dangerous undetected failure modes and determine the probabilities of those failures occur. Once determined such parameters it is possible to calculate the probability of failure on demand for the entire safety barrier.

Furthermore the study has shown that some innovation is brought with this methodology when the probability of occurrence of initiating event (POIE) is also considered and when the decision on acceptance of a safety barrier is based on both indicators, the SIL and the POIE.

Based on this work some studies can be developed in the future, including at the model the consideration of architectural constraints, repair rate times, self-diagnostic of failures (diagnostic coverage) and other methods to determine the probability of individual failures according to the period established to test the barrier as well as other influencing factors.

REFERENCES

[1] Kecklund, L, Edland, A., Wedin, P. and Svenson, O., "Safety barrier function analysis in a process industry: A nuclear power application", International Journal of Industrial Ergonomics, vol. 17, pp. 275-284, 1996.

[2] Harms-Ringdahl, L., "Analysis of safety functions and barriers in accidents", Safety Science, vol. 47, pp. 353-363, 2009.

[3] Duijm, N. and Markert, F., "Safety-barrier diagrams as a tool for modelling safety of hydrogen applications", International Journal of Hydrogen Energy, vol. 34, pp. 5862-5868, 2009.

[4] Beugin, J., Renaux, D. and Cauffriez, L., "A SIL quantification approach based on an operating situation model for safety evaluation in complex guided transportation systems", Reliability Engineering and System Safety, vol. 92, pp. 1686-1700, 2007.

[5] Wenjin, Z., Nan, L. and Xinwei, L., "Estimating Technology of Safety Integrity Level of Safety-Related Systems in High-speed Train", IERI Procedia, vol. 1, pp. 172-177, 2012.

ISBN 978-972-8954-42-0 | http://dx.doi.org/10.14195/978-972-8954-42-0_22

[6] Sklet, S., "Safety barriers: Definition, classification, and performance", Journal of Loss Prevention in the Process Industries, vol. 19, pp. 494-506, 2006.

[7] Hollnagel, E., "Risk+barriers=safet?", Safety Science, vol. 46, pp. 221-229, 2008.

[8] Duijm, N., "Safety-barrier diagrams as a safety management tool", Reliability Engineering and System Safety, vol. 94, pp. 332-341, 2009.

[9] Dianous, V. and Fiéviez, C., "ARAMIS project: A more explicit demonstration of risk control through the use of bow-tie diagrams and the evaluation of safety barrier performance", Journal of Hazardous Materials, vol. 130, pp. 220-233, 2006.

[10] IEC, "IEC 61508: Functional safety of electrical, electronic and programmable electronic safety-related systems – Parts 1-7", International Electrotechnical Comission, Geneva, 2002.

[11] Catelani, M., Ciani, L. and Luongo, V., "The FMEDA approach to improve the safety assessment according to the IEC 61508", Microelectronics Reliability, vol. 50, pp. 1230-1235, 2010.

[12] Jin, H., Lundteigen, M. and Rausand, M., "Reliability performance of safety instrumented systems: A common approach for both low and high-demand mode of operation", Reliability Engineering and System Safety, vol. 96, pp. 365-373, 2011.

[13] Torres-Echeverría, A., Martorell, S. and Thompson, H., "Modelling and optimization of proof testing policies for safety instrumented systems", Reliability Engineering and System Safety, vol. 94, pp. 838-854, 2009.

[14] Langeron, Y., Barros, A., Grall, A. and Bérenguer, C., "Combination of safety integrity levels (SILs): A study of IEC 61508 merging rules", Journal of Loss Prevention in the Process Industries, vol. 21, pp. 437-449, 2008.

[15] Summers,A., "Viewpoint on ISA TR84.0.02 – simplified methods and fault tree analysis", ISA Transactions, vol. 39, pp. 125-131, 2000.

[16] Beckman, L., "Expanding the applicability of ISA TR84.02 in the field", ISA Transactions, vol. 39, pp. 357-361, 2000.

[17] Hokstad, P., "Demand rate and risk reduction for safety instrumented systems", Reliability Engineering and System Safety, vol. 127, pp. 12-20, 2014.

[18] Sobral, J., "Utilização da metodologia RAMS na análise de barreiras de segurança de instalações industriais de risco elevado", Doctoral Thesis, FEUP - Faculdade de Engenharia da Universidade do Porto, 2010.

[19] Xu, M., Chen, T. and Yang, X., "The effect of parameter uncertainty on achieved safety integrity of safety system", Reliability Engineering and System Safety, vol. 99, pp. 15-23, 2012.

[20] Summers, A., "Introduction to layers of protection analysis", Journal of Hazardous Materials, vol. 104, pp. 163-168, 2003.

[21] IEC, "IEC 61511: Functional safety: Safety Instrumented Systems for the Process Sector", International Electrotechnical Comission, Geneva, 2003.

[22] Hauge, S., Krakenes, T., Habrekke, S., Johansen, G., Merz, M. and Onshus, T., "Barriers to prevent and limit acute releases to sea – SINTEF A20727 Report", SINTEF, 2011.

[23] Guo, H. and Yang, X., "A simple reliability block diagram method for safety integrity verification", Reliability Engineering and System Safety, vol. 92, pp. 1267-1273, 2007.