ELSEVIER

Journal of Hazardous Materials 130 (2006) 220–233

Journal of Hazardous Materials

www.elsevier.com/locate/jhazmat

ARAMIS project: A more explicit demonstration of risk control through the use of bow–tie diagrams and the evaluation of safety barrier performance

Valérie de Dianous [a,*], Cécile Fiévez [b]

[a] *INERIS, Direction des Risques Accidentels, Parc technologique Alata, BP2 60 550 Verneuil en Halatte, France*
[b] *Faculté Polytechnique de Mons, Major Risk Research Centre, 56 rue de l'épargne 7000 Mons, Belgium*

Available online 16 August 2005

Abstract

Over the last two decades a growing interest for risk analysis has been noted in the industries. The ARAMIS project has defined a methodology for risk assessment. This methodology has been built to help the industrialist to demonstrate that they have a sufficient risk control on their site.

Risk analysis consists first in the identification of all the major accidents, assuming that safety functions in place are inefficient. This step of identification of the major accidents uses bow–tie diagrams. Secondly, the safety barriers really implemented on the site are taken into account. The barriers are identified on the bow–ties. An evaluation of their performance (response time, efficiency, and level of confidence) is performed to validate that they are relevant for the expected safety function. At last, the evaluation of their probability of failure enables to assess the frequency of occurrence of the accident. The demonstration of the risk control based on a couple gravity/frequency of occurrence is also possible for all the accident scenarios.

During the risk analysis, a practical tool called risk graph is used to assess if the number and the reliability of the safety functions for a given cause are sufficient to reach a good risk control.

Keywords: ARAMIS; Risk control; Risk analysis; Safety barriers; Bow–tie

1. General introduction

Over the last two decades, a growing interest for risk analysis has been noted in the industries. Indeed, some recent technological accidents like Enschede (2000), Toulouse (2001) or Lagos (2002) have led the public to wonder or even mistrust both the industry and the regulatory authorities in their risk-informed decisions. These accidents have raised the need for more transparent decision-making processes.

Risk-based decisions of course require some reliable scientific input from risk analyses. However, noteworthy variations exist in the results of different risk analysis, what may affect any relevant and local decision. That is why emerges today the need for a methodology giving consistent rules to identify accident scenarios, to demonstrate their risk control, to select accident scenarios.

Among the different features of the ARAMIS project, this paper focuses on how the use of bow–tie diagrams and evaluation of the performance of the safety barriers can lead to a more explicit demonstration of risk control.

In a first step, all the major hazard accidents have to be identified. In the ARAMIS project, bow–tie diagrams are used for the identification of these accidents [1].

In a second step, among all the major hazard accidents identified, a demonstration that the scenarios have sufficient risk control must be performed. The demonstration is made using safety barriers as explained in this paper. The criteria for risk control is linked to the couple grav-

* Corresponding author. Tel.: +33 3 44 55 69 13; fax: +33 3 44 55 62 95.
E-mail addresses: valerie.dedianous@ineris.fr (V. de Dianous), cecile.fievez@fpms.ac.be (C. Fiévez).
URL: www.ineris.fr.

0304-3894/$ – see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.jhazmat.2005.07.010

ity/frequency of occurrence of the different accident scenarios. However, during the ARAMIS project, difficulties were encountered to assess frequency of occurrence of dangerous phenomena. Indeed, an inventory of the probabilistic data sources was carried out. It showed that very generic frequency ranges are usually used in these data sources, both for critical events and causes. These generic figures have to be considered very cautiously; indeed, they may have been averaged from different kinds of plants and substances, the safety systems are not clearly identified in figures and the global level of safety of the plants considered is unknown. Eventually, the use of generic figures do not underline the efforts made by the industrialists on their specific site both in prevention and mitigation, and in their safety management system.

An alternative method was also proposed, which really takes into account the safety barriers implemented on the industrial site. Indeed, the ARAMIS project proposes the assessment of the frequency of occurrence of the accident scenarios starting from the original frequency of occurrence of the deep causes and by reducing it taking into account the probability of failure of the safety functions identified on each scenario. An evaluation of these barriers is performed to validate that they are relevant for the expected safety function and to assess their probability of failure. After the evaluation of the frequency of occurrence of the different dangerous phenomena, it is possible to define if a scenario has a sufficient, insufficient or unacceptable risk control. During the risk analysis, a practical tool called risk graph is used to assess if the number and the reliability of the safety functions for a given cause are sufficient to reach an adequate risk control.

The ARAMIS project is based on existing methodologies (IEC 61508 [3], IEC 61511 [4] and LOPA [5]).

The developing methodology of risk assessment has been tested on different European industrial sites during the year 2004. These test cases have enabled the partners to improve the methodology by taking into account the former lacks.

2. Identification of the major accident hazards using bow–ties

The identification of major accident hazards likely to occur on an industrial site is the first step of the risk analysis. The identification of major accident hazards is performed in the ARAMIS project by the methodology MIMAH [2], abbreviation of Methodology for the Identification of Major Accident Hazards. Major accident hazards correspond to the worst accidents likely to occur on a site, assuming that no safety barriers are installed or that they are inefficient. The methodology is based mainly on the use of bow–tie diagrams (Fig. 1), centred on a critical event and composed of a fault tree on the left and of an event tree on the right. It should be noted that a critical event is generally defined as a loss of containment (LOC) or a loss of physical integrity (LPI).

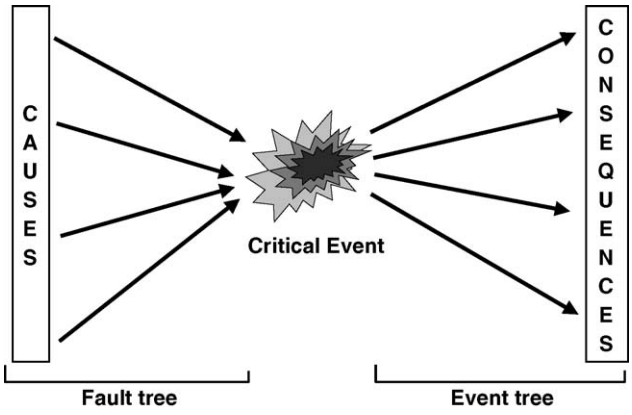


Fig. 1. General scheme of the bow–tie.

The bow–tie concept is gaining in popularity and is believed to offer a good overview of the different accident scenarios considered. Indeed, all the causes and consequences of an accident are clearly identified on the bow–ties. Moreover, the bow–tie is a tool particularly adapted to represent the influence of safety systems on the evolution of accident scenarios. Safety systems, technical or organisational, can be placed on the different branches of the bow–tie. Prevention safety systems are found on the fault tree side, and mitigation systems are found on the event tree side. The bow–tie enables to quickly visualise what safety function acts on a scenario, as illustrated in Fig. 2. When the evaluation of the frequencies of occurrence of each scenario is performed, the most critical cause or scenario appears clearly.

Note that in the following "dangerous phenomenon" corresponds to the last level on the right of the bow–tie, describing the nature of the accident consequences (for example, a pool fire, a vapour cloud explosion, a toxic cloud, etc.).

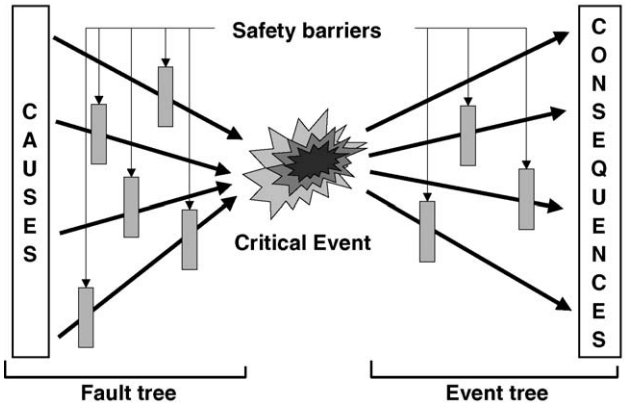


Fig. 2. Complete bow–tie with identification of prevention or mitigation safety functions.

3. Identification and evaluation of safety functions and barriers

3.1. Why taking into account safety functions and barriers?

Standard risk analysis methods propose to assess the frequency of occurrence of a major accident and to decide from this evaluation whether the risk is acceptable or not (sufficient risk control or not). The ARAMIS project has kept this principle and has based the definition of reference accident scenarios on the couple gravity/frequency of occurrence [1].

The methodology proposed by ARAMIS takes into account the safety barriers implemented on the industrial site. The principle is to assess the frequency of occurrence of the dangerous phenomena starting from the original frequency of occurrence of the deep causes of the accident and by reducing it taking into account the probability of failure of the safety functions really implemented on site. The calculations of the probabilities of failure of the safety functions are carried out according to the principles derived from the safety integrity level concept (SIL) available in IEC 61508 [3] and IEC 61511 [4] standards and according to the known reliability of the safety barriers.

Taking into account safety functions and barriers has three main purposes:

- It prompts the industrialists to invest in safety barriers (prevention or mitigation); indeed, the barriers will influence the risk level of a plant what would not be the case by using generic figures of frequency of occurrence for equipment failures;
- The identification of the safety functions in the bow–ties is completed by the evaluation of their performance; the industrialist is encouraged to better know its safety functions, what is favourable to a better level of safety on site;
- The analysis with the barriers helps the industrialists to identify more clearly which scenarios have an insufficient level of risk control, as explained in Section 4 of this paper.

3.2. Definition and typology of a safety function

A safety function is a technical or organisational action, and not an object or a physical system. The generic safety functions can be expressed by actions to be achieved. It is an action to be achieved in order to avoid or prevent an event or to control or to limit the occurrence of the event. This action is realised thanks to safety barriers defined in Section 3.3.

In the fault tree, the different possible actions of safety functions are to avoid, to prevent the occurrence of an event, to limit the size of an event or to reduce the probability of an event. In the event tree, the different possible actions of safety functions are to avoid, to prevent or to reduce the consequences of the critical event and to mitigate its effects on the surroundings of the equipment (individuals, neighbouring equipment and environment). In the fault tree, the safety functions may decrease the frequency of an event, whereas in the event tree, the safety functions may reduce the frequencies and/or the consequences of dangerous phenomena and mitigate their effects.

The safety function is the "what" needed to assure, to increase and/or to promote safety.

Four main verbs of action are defined for the safety functions. Definitions for these four safety functions are presented in Table 1. It should be noted that, in these definitions, an event can be each kind of event encountered in the bow–tie, both on fault and event tree sides. For some functions ("to control" and "to limit"), a detection action is often included in the global safety function.

3.3. Definition and typology of a safety barrier

The safety barriers can be physical and engineered systems or human actions based on specific procedures or administrative controls. The safety barrier directly serves the safety function. So, a safety barrier can be the action of an operator, a prevention system (layer of protection to prevent the corrosion), an emergency control system (pressure safety valve), a physical system (retention bund, wall), safety-related system (fire extinguisher). The engineered and physical systems and the human actions are sometimes interchangeable and/or work together to maintain the effectiveness of the safety function.

The safety barriers are the "how" to implement safety functions.

Four main categories of safety barriers are defined. The categories are useful for the evaluation of the safety barrier management [6].

- *Passive barriers*: Barriers always in functioning (permanent), no need of human actions, energy sources or information sources. Passive barriers may be physical barriers (retention bund, wall, ...), permanent barriers (corrosion prevention systems) or inherently safe design.
- *Activated barriers*: These barriers set up preconditions that need to be met before the action can be carried out. So, these barriers must be automated or activated manually to work or these barriers can be mechanical barriers that require an activation (hardware) to achieve their function. Activated barriers always require a sequence of detection – diagnosis – action. This sequence can be performed using hardware, software and/or human actions.
- *Human actions*: The effectiveness of these barriers is relied on the knowledge of the operator in order to reach the purpose. Human actions are to be interpreted broadly, including observations by all senses, communication, thinking, physical activity and also rules, guidelines, safety principles, ... Human actions may be part of a detection – diagnosis – action sequence.
- *Symbolic barriers*: These barriers need an interpretation by a person in order to achieve their purpose. The typical example can be passive warnings (like keeping out of

Table 1
Typology of safety functions

Safety function	Definition	Example
To avoid	To make the event impossible	In the fault tree, to avoid an impact on a vessel
"To avoid" safety functions may only act upstream of any kind of event in such a way this event can never occur. The event is avoided by suppressing the intrinsic conditions that causes the event, by adding generally a passive, permanent, physical barrier. This kind of safety function cannot depend on the functioning of any other safety function		
To prevent	To hinder, to put obstacles on the way of occurrence of the event	In the fault tree, to prevent the corrosion of a vessel
		In the event tree, to prevent the vapourisation of a pool, or to prevent the ignition of a flammable cloud
"To prevent" safety functions may only act upstream of any kind of event in such a way the occurrence of this event is reduced (but not absolutely avoided). This safety function will only reduce (of one or more order of magnitude) the frequency of an event.		
To control	In the fault tree, to control = to bring back the system to a "safe" state	In the fault tree, to control the overfilling of a liquid storage
	In the event tree, to control = to get the event under control and return to a "safe" state	In the event tree, to control the pool dispersion
"To control" safety functions may act upstream of an event in the fault tree (in response to a drift which may lead to the event and/or in response to upstream events—feedback, control loops). "To control" safety functions may also act downstream of an event in the event tree (the event occurred but can be definitively stopped). A part of this safety function is nearly always a detection		
"To limit" or "To reduce" or "To mitigate"	To limit = to limit the event in the time and/or in the space, or to reduce its magnitude, or to mitigate the effects of a dangerous phenomenon on the neighbouring equipment, on the human beings or on the environment	In the fault tree, to reduce the overpressure in the reactor
		In the event tree, to reduce the liquid flow, to reduce the concentration of the toxic cloud, or to limit the duration of a leak, to limit liquid vapourisation
"To limit" or "to reduce" or "to mitigate" safety functions may act downstream of an event. As a matter of fact, the event must have occurred to be limited or reduced or mitigated. It provides no control. A detection is sometimes part of the "limit" safety function		
These limitation functions can be of three different kinds. They can aim at limiting the amount of energy or hazardous substances or, more generally, the amplitude of dangerous phenomena constitutive of the critical event		

prohibited areas, opening labelled pipes, refraining from smoking . . .)

3.4. Taking into account safety barriers in the bow–tie

For the identification of the safety barriers, the method proposed is to review systematically the fault tree and the event tree. Each event of the trees, branch per branch, must be examined and the following question should be asked: "Is there a safety barrier which avoids, prevents, controls or limits this event?" If yes, the safety barrier must be placed on the branch. The barrier will generally be placed upstream of an event if it avoids or prevents this event. If it controls or limits this event, it has to be placed downstream.

According to the typology of the safety function, the effect on the scenario will be different, as explained in the following paragraphs.

3.4.1. "Avoid" barriers

This kind of barrier implies that the event located just downstream is supposed impossible.

For example, Fig. 3 shows a part of a fault tree leading to a large breach in an equipment. Overpressure in this equipment could occur due to temperature increase, being caused by the thermal radiation due to a domino effect (fire in the adjacent unloading unit). The safety barrier considered is the large distance between the unloading unit and the equipment, which corresponds to an "avoid" barrier. It is thus proposed to represent the barrier as shown in Fig. 3.

The branch could have been completely deleted from the fault tree, but this is not recommended. Indeed, if the barrier disappears (for example, here if the unloading unit is moved), the tree drawn with the method proposed in Fig. 3 will always be up-to-date and the hazard due to the unloading unit will always be kept in mind. Otherwise, the deleted cause could be forgotten later if the barrier is no more relevant.

3.4.2. "Prevent" or "control" barriers

For these barriers, the rule is: "If the level of confidence of a barrier on a branch is equal to LC, then the frequency of the downstream event on the branch is reduced by a factor 10^{-LC}".

Fig. 4 gives an example of a complete drawing of the tree generated by a safety barrier. Two branches are derived from the safety barrier, one in case of failure of the safety barrier, and one in case of success. In this second case, the accident corresponding to the studied critical event is stopped, and thus the branch can be deleted. The practical drawing (Fig. 5) is thus simpler and will only take into account the case of failure of the safety barrier. The frequency of the downstream event is thus reduced by a factor 10^{LC} since the barrier has a level of

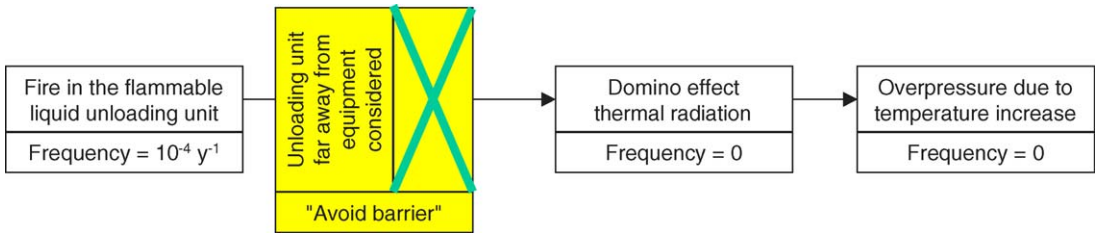


Fig. 3. "Avoid barrier" in the fault tree.

confidence equal to LC. It can be noted that for some barriers, the working of the barrier can lead to another type of critical event. For example, the release of a safety pressure valve will lead to a critical event called "medium" leak, compared to the critical event "catastrophic rupture" in case of the burst of the equipment due to overpressure. The working of the barrier will be a cause to the "medium" leak.

In these drawings (Figs. 4 and 5), the barrier is placed downstream of the event because the example considers a "control" barrier. A "prevent" barrier should have been placed upstream of the event.

3.4.3. "Control" barrier in the event tree

In the event tree, the "control" barriers can control, stop the evolution of a branch. It depends on the level of confidence of these barriers. An example of the influence of control barriers is shown in Fig. 6, for two independent control barriers.

It can be concluded that a "control" barrier introduces a kind of OR gate in the event tree. One branch concerns the successful action of the barrier, and leads to a safe situation where the accident is under control. The other branch concerns the failure of the safety barrier, allowing the further development of the scenario. The frequency of the event on this branch is equal to the frequency of the event upstream of the barrier, multiplied by 10^{-LC} (where LC is the level of confidence of the barrier, explained in Section 3.5).

3.4.4. "Limit" barrier in the event tree

The limitation/mitigation barriers have an indirect influence on the transmission probabilities and they can reduce the major effects of dangerous phenomena, for example, by limiting the flow rate and the release time, the pool area, the vapourisation time or in diluting the toxic/flammable concentrations, . . .

In the event tree, when a limitation/mitigation barrier is considered, two branches must be built, one if the barrier succeeds and an other one, if the barrier fails. Both branches have to be kept in the event tree, because they will lead to two different dangerous phenomena, one with less severe consequence but a higher frequency, and the other one

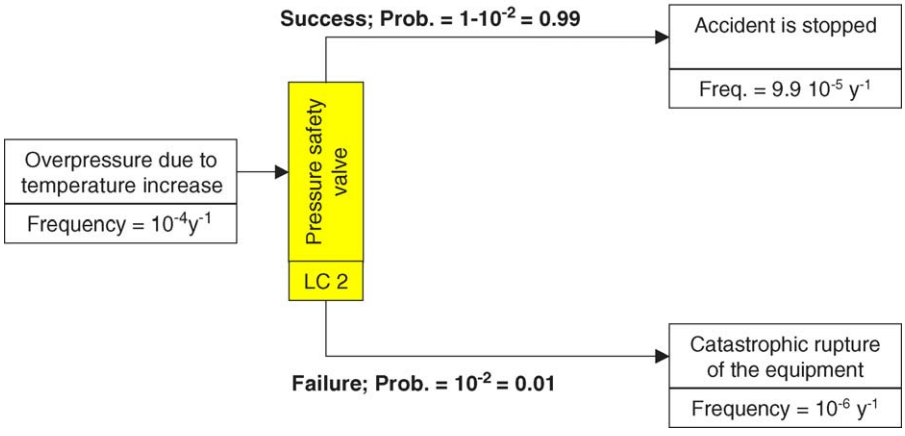


Fig. 4. "Prevent" or "control" barriers in the fault tree—complete drawing (example).

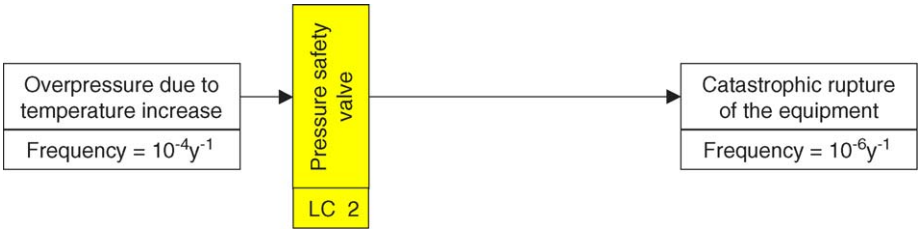


Fig. 5. "Prevent" or "control" barriers in the fault tree—simple drawing (example).

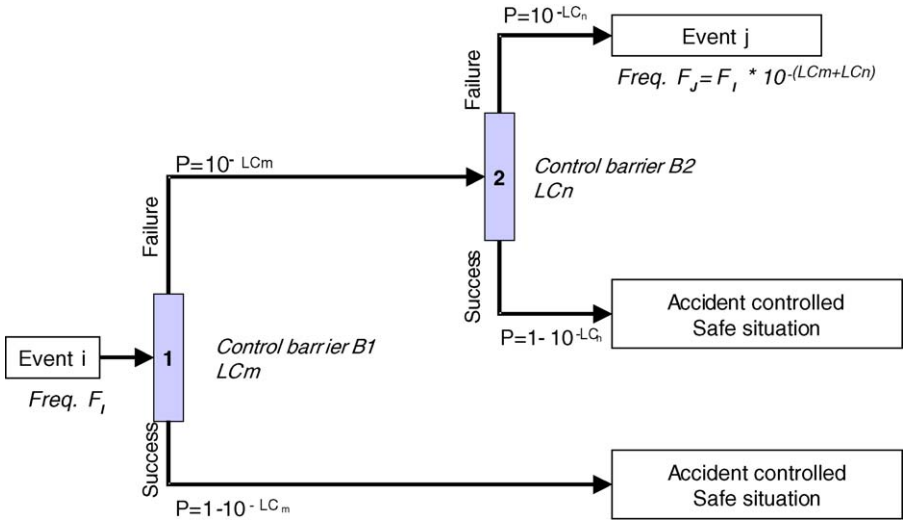


Fig. 6. "Control" barriers—influence on the calculation of frequencies of events in term of level of confidence.

with more severe consequence but a lower frequency. The frequency calculation is linked to the level of confidence of the safety barrier.

For example, in the case of a toxic dispersion, a self-closing valve coupled to a detection system can reduce the effects of the toxic cloud. We have thus two types of consequences: the one resulting from a whole toxic cloud with the probability of non-functioning of the limitation safety system, and the other with a smaller toxic cloud with mitigated effects and a smaller severity of the dangerous phenomenon (DP) (see Fig. 7). The characteristics of the DP differ in terms of limitation of the effects or not, and also in terms of frequency.

3.5. Evaluation of the performance of a safety barrier

Before taking into account the safety barriers in the bow–tie as explained in Section 3.4, it is necessary:

- To demonstrate that the given safety function and the related barriers are relevant to avoid, to prevent, to control or to mitigate the event. The assessment of the performance of the barriers is performed through the study of three criteria that are effectiveness, response time and level of confidence. If the barrier is not considered relevant, it is not kept as a barrier.
- To estimate the probability of failure of the safety function by decomposing the function in different barriers. The probability of failure of each barrier is linked to the level of confidence.

The different criteria are detailed in this section.

3.5.1. Minimal requirements for safety barriers

During risk analysis, different safety functions are identified and decomposed into several safety barriers. It is necessary to make sure that the safety barriers are relevant to perform the expected safety function. To be considered as relevant, a safety barrier must first meet the following requirements:

- The *effectiveness* of the safety barrier must be demonstrated and adapted to the scenario. The effectiveness is the ability for a technical safety barrier to perform a safety function for duration, in a non-degraded mode and in specified conditions. The effectiveness is either a percentage or a probability of the performance of the defined safety function. If the effectiveness is expressed as a percentage, it may vary during the operating time of the safety barrier. For example, a valve that would be not completely closed on safety demand would not have an effectiveness of 100%. To assess the effectiveness of a safety barrier, it is necessary to take an interest in the design of the barrier. In this way, the barrier must be designed in appliance with codes, rules, ... and the design must be adapted to the characteristics of the products and the environment The characteristics of its design must be in accordance with the related function. Assessment of effectiveness may be performed during risk analysis by considering data and experience from suppliers or industrialists, tests on site, norms and technical guides, calculation data sheets of the barriers.
- The *response time* must be in accordance with the kinetics of the scenario of the considered major hazard accident. The response time is the duration between the straining of the safety barrier and the complete achievement (which is equal to the effectiveness) of the safety function performed by the safety barrier. The response time can be assessed for technical barriers from data from industrialists, experience, standards and technical guides. For human barriers, the response time may depend on different criteria (training of the operator, easy diagnostic in case of an accident, access to a barrier, knowledge of the operator about what he has to do in case of an accident).

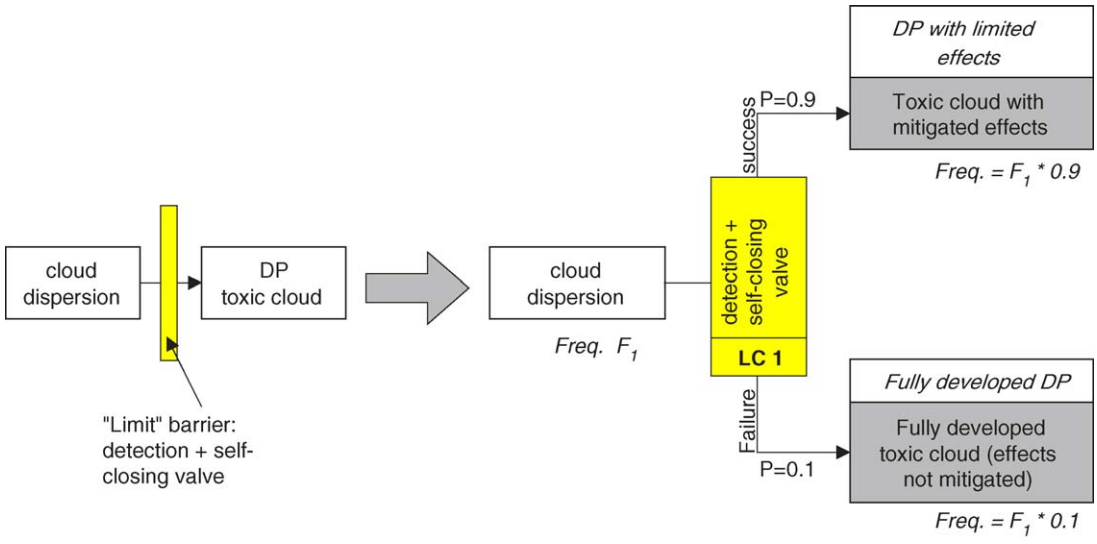


Fig. 7. Influence of a limitation barrier on the effects of dangerous phenomena.

- The *level of confidence* of the barriers is linked to its reliability. The level of confidence of a safety barrier is inversely proportional to the probability of failure on demand of the barrier. It corresponds to the reliability of the barrier to perform properly a required safety function according to a given effectiveness and response time under all the stated conditions within a stated period of time. Actually, this notion is inspired from the notion of safety integrity level defined in IEC 61511 [4] for safety instrumented systems and it has been enlarged to all types of safety barriers, including human barriers, passive barriers.

However, before making a quantitative estimation of the level of confidence, qualitative parameters should be studied to estimate further the level of confidence:

- the independence of the safety barrier with the causes and with the regulation systems (to reduce common failure mode);
- the architecture of the safety systems (to check if redundancy or common failure mode exist, if safety barriers are fail-safe, if it is possible to shunt a safety function);
- the "proven" concept of the barrier that is to say that the concept is well-known (experienced) (otherwise, it may be necessary to perform more tests on site to check the quality of the barrier);
- the existence of periodic tests in accordance with experience of industrialists or suppliers and the existence of a schedule of maintenance operations with the view to maintain the characteristics of the safety barrier in time.

These three different parameters (effectiveness, response time, level of confidence) are estimated for each barrier, and a combination of the different barriers is then made to assess the global characteristics of the safety function. If the safety function is not considered as relevant, it is not kept on a branch of the bow–tie.

3.5.2. Estimation of the level of confidence of a safety barrier

The level of confidence of a safety barrier depends on two criteria:

- the first one, qualitative (architectural constraints);
- the second one, quantitative (probability of dangerous failure).

The processing for the two criteria are made according to the principles defined in the IEC 61508 [3] and IEC 61511 [4] standards.

3.5.2.1. Architectural constraint. A first estimation of the level of confidence of a barrier is made by analysis of its architecture. According to the complexity of the subsystems composing the barrier, a class of confidence is proposed in IEC 61508 and 61511. A subsystem is a component of a safety barrier, for example, a detector, a valve.

To determine the level of confidence for a subsystem, two parameters are used:

- The *safe failure fraction* (SFF), which is the ratio between the frequency of failure of the component leading to a safe position to the frequency of total failures. A safe position is a failure that does not have the potential to put the safety barrier in a hazardous or fail-to-function state.
- The *fault tolerance* (FT), which is linked to the capacity of the barrier to keep its safety function in case of failure of one or more system composing the barrier. Fault tolerance is linked to the *redundancy*. For example, a fault tolerance of 1 means that if one component is defective, the safety function remains operational.

Then, the class of confidence depends on the complexity of the subsystems, as defined in IEC 61508 [3] and IEC 61511 [4] standards. A subsystem is simple (type A in Table 2) if the failure modes of all constituent components are well-defined.

Table 2
Architectural constraints for the type A (all the failure modes are well-known)

Safe failure fraction (SFF)	Fault tolerance		
	0	1	2
<60%	LC 1	LC 2	LC 3
60–<90%	LC 2	LC 3	LC 4
90–<99%	LC 3	LC 4	LC 4
≥99%	LC 4	LC 4	LC 4

Table 3
Architectural constraints for the type B (all the failure modes are not known)

Safe failure fraction (SFF)	Fault tolerance		
	0	1	2
<60%	Non-possible	LC 1	LC 2
60–<90%	LC 1	LC 2	LC 3
90–<99%	LC 2	LC 3	LC 4
≥99%	LC 3	LC 4	LC 4

It is, for example, mechanical devices like. A subsystem is complex (type B in Table 3) if the failure mode at least of one constituent component is not well-defined. It is, for example, complex systems like processors, subsystems hardware.

The qualitative criteria corresponding to architectural constraints for the subsystems (types A and B) are, respectively, defined in Tables 2 and 3. These tables are issued from the IEC 61508 standard [3].

3.5.2.2. Quantitative criteria for the estimation of the level of confidence. The quantitative criteria correspond to the probability of failure for the subsystems (types A and B) and depends on the mode of operation (low demand or continuous mode). The link between the level of confidence and the probability of dangerous failure are defined in Tables 4 and 5. These tables are issued from the IEC 61508 standard [3].

Table 4
Level of confidence: failure measures for a safety function, allocated to a safety barrier operating in low demand mode of operation (from EN 61508)

Level of confidence	Low demand mode of operation (average probability of failure to perform its design function on demand)
LC 4	$\geq 10^{-5}$ to $<10^{-4}$
LC 3	$\geq 10^{-4}$ to $<10^{-3}$
LC 2	$\geq 10^{-3}$ to $<10^{-2}$
LC 1	$\geq 10^{-2}$ to $<10^{-1}$

Table 5
Level of confidence: failure measures for a safety function, allocated to a safety barrier operating in high demand or continuous mode of operation (from EN 61508)

Level of confidence	High demand or continuous mode of operation (probability of a dangerous failure per hour)
LC 4	$\geq 10^{-9}$ to $<10^{-8}$
LC 3	$\geq 10^{-8}$ to $<10^{-7}$
LC 2	$\geq 10^{-7}$ to $<10^{-6}$
LC 1	$\geq 10^{-6}$ to $<10^{-5}$

Table 6
Definition of the level of confidence for barriers

Level of confidence of a barrier	Risk reduction factor	Equivalent probability of failure on demand (PFD)	Equivalent probability of failure per hour
4	10000	$\geq 10^{-5}$ to $<10^{-4}$	$\geq 10^{-9}$ to $<10^{-8}$
3	1000	$\geq 10^{-4}$ to $<10^{-3}$	$\geq 10^{-8}$ to $<10^{-7}$
2	100	$\geq 10^{-3}$ to $<10^{-2}$	$\geq 10^{-7}$ to $<10^{-6}$
1	10	$\geq 10^{-2}$ to $<10^{-1}$	$\geq 10^{-6}$ to $<10^{-5}$

3.5.3. Global level of confidence of a safety function

The safety functions identified on the bow–tie have been divided in different safety subsystems (for example, detection, treatment of the information, action like closing of valves, ...). Each subsystem is divided in different barriers (for example, detection can be performed both by human detection and by a gas detector). For each barrier, the level of confidence is assessed by means of the criteria explained above. Then, each subsystem (detection, treatment of the information, action) can be evaluated by taking also into account the architecture (potential redundancy...) and the probability of a dangerous failure of each barrier. The time response and the effectiveness of the subsystem are also a combination of the parameters of the different barriers.

The global level of confidence of the safety function is then calculated from the level of confidence of the different subsystems in the same way. The level of confidence of the safety function is the smallest level of confidence of the different subsystems. The time response and the effectiveness of the safety function are also a combination of the parameters of the different subsystems.

It should be noted that LC 4 safety systems are nearly never encountered in process industry.

The level of confidence of the barrier is linked to a risk reduction factor as detailed in Table 6.

4. Demonstration of the risk control and use of risk graph

The risk analysis has the purpose to demonstrate that the site has a good level of risk control. The risk control is built on the reduction of the frequency of occurrence of the major dangerous phenomena taking into account the safety barriers, so that the dangerous phenomena are defined with an acceptable couple gravity/frequency of occurrence.

By taking into account the safety barriers on the bow–tie, ARAMIS provides an explicit demonstration of the risk control: the method is based on the existing safety barriers on the site, the criteria for assessment of the level of confidence are clear.

During a risk analysis, it is possible to define risk reduction goals for a set of barriers so that the considered scenario is expected to have a good level of risk control. This is performed thanks to a tool called the risk-graph and inspired from the IEC 61511 standards [4]. It has been adapted to fit

the purpose of the ARAMIS project. The advantage of the graph risk is that it enables to perform recommendation during risk analysis in case that some scenarios have insufficient risk control.

4.1. Principles and use of the risk graph

The purpose of the risk graph is to precise for a given scenario and a given cause, according to the expected consequences of the dangerous phenomena associated to the critical event, the level of confidence of the safety barriers required to have an good risk control. All the safety barriers on the fault or event tree have to be considered. The requirement for the level of confidence is a global level of confidence obtained by adding the levels of confidence of all the barriers.

The risk graph gives the goals on the levels of confidence of the barriers identified on a scenario to have an acceptable risk control on this scenario. The figures given in the risk graph depends on the risk matrix [1] that defines for each risk analysis the thresholds of acceptability of the couple gravity/frequency of occurrence of the accidents.

An example of risk graph is presented in Fig. 8, and the main definitions of the terms used in the graph are summarised in Table 7.

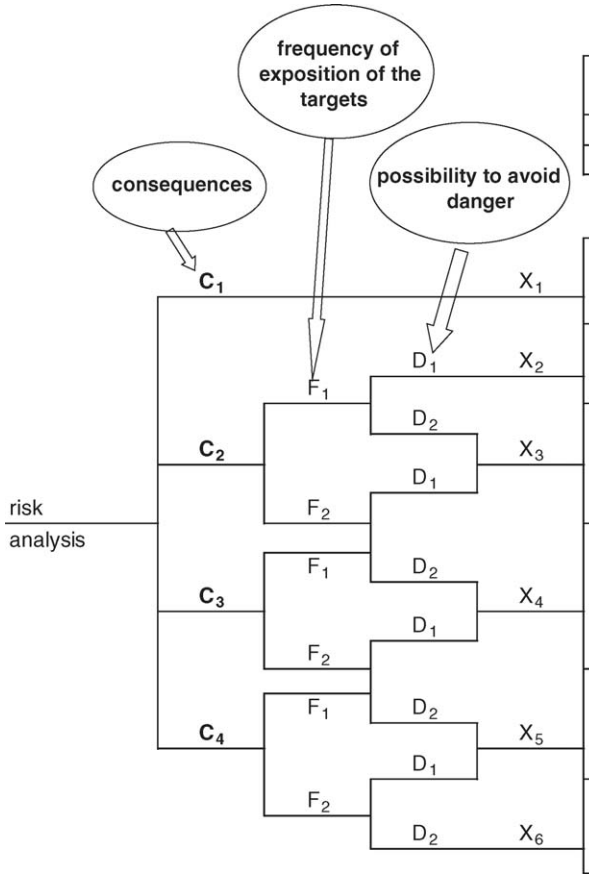
The risk graph can be used in the following way: for a given bow–tie and for a given initiating event (or a whole group of initiating events linked by a "AND" gate):

- The consequences of the accident are assessed through the parameter C, taking into account the dangerous phenomenon with the higher consequences for the given critical event and the given initiating event and assuming that all safety barriers are inefficient. Definitions of the class of consequences are given in reference [1].
- The frequency of exposition of targets during the operation (F_1 or F_2) and the possibility or not to avoid the danger (D_1 or D_2) must be determined.
- The level of frequency of the given initiating events has to be assessed as explained in reference [1].

Thanks to these four parameters (C, F, D and P), the required level of confidence can be determined by the risk-graph. The way to assess the required level of confidence is shown in the example of Section 4.2.

4.2. Example of demonstration of risk control

This paragraph presents an example of how bow–tie and evaluation of the safety barriers lead to demonstrate risk



FREQUENCY OF THE INITIATING EVENT (per year)			
$10^{-2}<F\leq10^{-1}$	$10^{-3}<F\leq10^{-2}$	$10^{-4}<F\leq10^{-3}$	$F\leq10^{-4}$
1	2	3	4

P_1	P_2	P_3	P_4
---	---	---	---
a	---	---	---
1	a	---	---
2	1	a	---
3	2	1	a
4	3	2	1

Fig. 8. Risk graph, definition of objectives in order to demonstrate the control of risk.

Table 7
Main definitions for the risk graph

C_n	Potential consequence of the dangerous phenomena, defined by the severity of the accident and the vulnerability of the environment; C_n is ranking from C_1 (low consequences) to C_4 (major consequences) *Note 1:* at the step of the project when risk graph is useful, C_n is just estimated; no calculation of severity or vulnerability index has been made
$F_{1/2}$	Frequency of exposition of the targets during the operation: F_1, for the studied operation, targets are few exposed to the risk (less than 10% of the duration of the operation) F_2, for the studied operation, targets are very exposed to the risk (more than 10% of the duration of the operation) *Note:* target may be environment, persons on site or outside the site. The more important the effects of the accident are, the more the number of persons involved will increase and the frequency of exposition may increase
$D_{1/2}$	Possibility to avoid damage, by intervention or evacuation D_1, long kinetic and intervention/evacuation clearly defined and personnel warmed that safety barriers are not efficient D_2, in the other cases
$P_{1/2/3/4}$	Frequency of the initiating event leading to a given critical event. (or a whole group of initiating events linked by a "AND" gate) P_4 (very low frequency: $F \leq 10^{-4}$ year^{-1}) P_3 (low frequency: 10^{-4} year$^{-1} < F \leq 10^{-3}$ year^{-1}) P_2 (medium frequency: 10^{-3} year$^{-1} < F \leq 10^{-2}$ year^{-1}) P_1 (high frequency: 10^{-2} year$^{-1} < F \leq 10^{-1}$ year^{-1})
–	No safety requirements
a	No safety requirements for safety barriers
b	Unacceptable situation; there is need to redesign the process or make prevention more effective
1–4	Level of confidence of safety barriers

control. A fictitious and quite simplified example has been considered. The equipment chosen here is pressure storage of toxic gas located in a high-inhabited environment.

4.2.1. Major accident scenario

The considered accident scenario is a large leak of toxic gas from a gas pipe. The leak may be due to two independent causes: an operator error (wrong valve opened) or a domino effect (impact due to missiles). For the sake of simplification, only two causes are considered in the examples. The accident scenario is represented in Fig. 9. A very simplified bow–tie for this example is shown in Fig. 10.

The downstream flow is not considered (the product being consumed in a reactor).

The safety technical function consists in a safety instrumented system (SIS) composed with two pressure detectors (D_A and D_B), one logic controller and one automatic emergency shut-down valve (ESV). Besides, an additional water curtain (manual action) is at the disposal of the operator.

4.2.2. Identification of safety functions and safety barriers

For the example, the relevant safety functions are the following ones:

- to prevent operator error,
- to prevent impact on the pipe,
- to limit the gas release from pipe,
- to limit the gas dispersion.

In this particular case, the safety barriers shown in Table 8 achieve these safety functions.

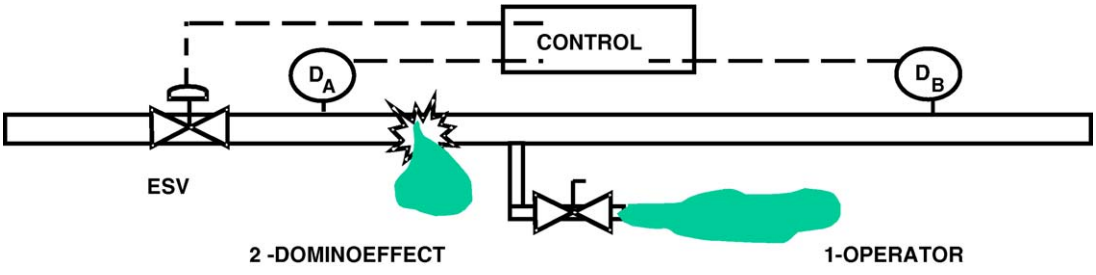


Fig. 9. Large leak of toxic gas.

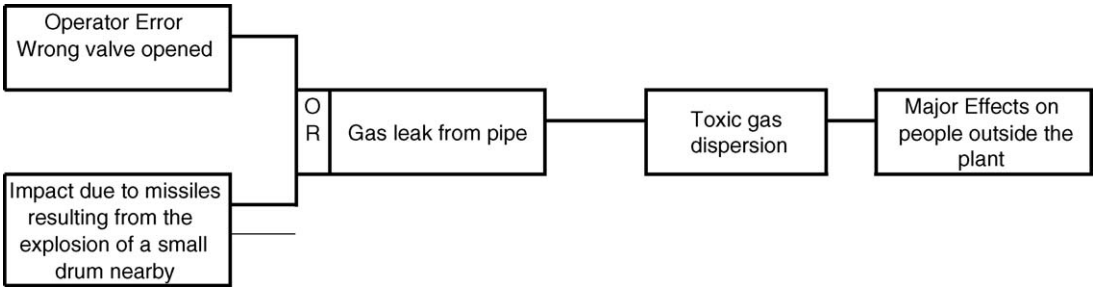


Fig. 10. Simplified bow–tie.

Table 8
Identification of safety functions and safety barriers

Safety function	Safety barriers for the cause "error operator"	Safety barriers for the cause "domino effect"
To prevent operator error	Training of the operator Indications on pipes to identify them Procedure (check whether pipe is empty with pressure detection devices)	
To prevent impact on pipe		In this case, no safety barriers
To limit the gas release	Differential measure of flow rate in the pipe Logic controller One automatic shut-down valve at each extremity of the pipe	Differential measure of flow rate in the pipe Logic controller One automatic shut-down valve at each extremity of the pipe
To limit the gas dispersion	Mobile water curtains (manual)	Mobile water curtains (manual)

4.2.3. Safety requirements

The risk graph can be used to define the requirement of the level of confidence for each cause (see Fig. 11).

4.2.3.1. Cause 1: Error of the operator. Due to the crowded surroundings of the plant, the assessment of the consequences for the toxic cloud leads to a consequence class C_4. The targets are supposed exposed to the risk more than 10% of the duration of the operation. Therefore, we set $F = F_2$. We consider here that the accident leads to the dispersion of a toxic cloud but that the effects of this cloud are observed after a few minutes. We assume that people have the possibility to detect this cloud and to get confined in order to avoid damage. In consequence, we set $D = D_1$. To identify the safety requirements, it is then important to assess the frequency of the initiating events of the scenario. The frequency of an operator error is assessed to 10^{-1} year^{-1} that is to say, we set $P = P_1$. Considering $C = C_4$, $F = F_2$ and $D = D_1$, the level of confidence is defined in line X_5 on the risk graph presented in Fig. 11. For $P = P_1$, the level of confidence required for the safety barriers is 3.

4.2.3.2. Cause 2: Domino effect. The parameters C, F and D may be the same as for the previous cause. However, the frequency of occurrence of domino effect should be assessed and should be lower than 10^{-1} year^{-1}, leading to a lower requirement for level of confidence of the safety barriers. This cause is not studied any longer.

4.2.4. Evaluation of performances of safety functions

The previous steps have determined the required level of confidence for the considered accident scenario, the large leak of a toxic gas due to an operator error. It is then necessary to check whether the safety level on the plant meets the identified requirements.

4.2.4.1. Effectiveness and response time of safety barriers. Among the four safety functions previously identified for the two causes (see Table 8), three apply for the cause "operator error ", the function "to prevent impact on pipe" being not adapted for this cause.

After this identification, it is important to check that these barriers are relevant for the considered scenario, by considering first their response time and effectiveness:

- The influence of actions designed to prevent the operator error is quite clear since, if they are correctly applied, they should totally avoid the possibility of a leak. Therefore, this first barrier (training + procedures) is considered as effective if properly achieved. The effectiveness of the prevention function can be considered to 100%. The probability of operator error is included in the level of confidence of this barrier.
- The safety chain with the differential measure of flow rate and shut-down valves has an effectiveness sufficient to detect the leak due to the opening of a wrong valve; indeed, the differential measure of flow rate can detect variation higher than 10%, which is representative of a valve kept opened. Besides, the response time is acceptable compared to the kinetics of the scenario; indeed, thanks to calculations and on-site tests, the overall response time has been assessed to 30 s. This response time is sufficient to completely limit the damage due to the leak.
- The mobile water curtains might have an influence on the dispersion of the cloud. This influence is hard to define since it depends on various parameters such as the direction of the jet, of the wind ... Besides, these mobile curtains must be triggered manually and this operation takes at least a few minutes, which is too long regarding the kinetics of the scenario. Therefore, this safety barrier is not selected as relevant.

4.2.4.2. Levels of confidence of safety barriers. Following the criteria specified for the performance evaluation of safety barriers, the effectiveness, response time and level of confidence for each safety barrier are assessed as shown in Table 9.

Table 9
Effectiveness, response time and level of confidence of safety barriers

Safety barriers	Effectiveness (%)	Response time (s)	LC
To prevent the operator error			
Training + procedures	100	–	1
To limit the gas release			
Differential measure of flow rate in the pipe	90	5	2
Logic controller	100	5	2
Shut-down valve (one at each extremity of the pipe)	99	20	1

4.2.4.3. Levels of confidence of safety functions. The levels of confidence of safety barriers allow to define the level of confidence of safety functions according to the architecture of these barriers. For training and procedures (operator answer with stress) (LC = 1), it seems reasonable to consider an overall level of confidence equal to 1 for the safety function "To prevent operator error". For the safety function "To limit the gas release", it is important to consider the architecture of the safety barriers. The system is so decomposed as shown in Fig. 12. Following the criteria specified for the evaluation of the performance of safety functions, for the global safety function, a level of confidence of 1, an effectiveness of 90% and a response time of 30 s will be considered.

4.2.5. Comparison of safety requirements and actual safety performances

The safety requirements for the scenario of leak due to human error are equivalent to an overall level of confidence of 3 (LC = 3) according to the risk graph (see Fig. 11). In the example, we only have one safety function with LC = 1 in prevention (to prevent operator error) and one safety function with LC = 1 in limitation. So the sum is only two. The requirements for an acceptable risk are not reached.

This result shows that safety improvements are necessary to achieve a sufficient risk control for this accident scenario. Several improvements could be suggested:

- To improve the prevention of the leak thanks to training, procedures in order to increase the level of confidence, . . .
- To improve the limitation of the gas release by adding new safety barriers or improving the existing ones. This solution will be further discussed for the architecture and the shut-down valve clearly appears as a weak point.
- To lower consequences thanks to heavy modifications of the process such as the use of a less toxic gas, the use of pipe with less important diameter . . . These modifications are sometimes difficult to achieve specially on existing plants. These measures tend to reduce risk at the source.

In this particular case, it appears more convenient to improve the safety level of the existing safety chain. This can be achieved either by using best quality valves with higher safety failure fraction or to add an identical valve in order to be tolerant to the fault of one valve (redundancy). With an extra valve, the level of confidence associated to the safety chain is equal to 2 and together with the safety function of prevention (level of confidence = 1), it allows to reach the requirements targeted.

The previous result showed that with the adding of an identical shut-off valve, the performances of safety barriers were good enough to prevent the occurrence of C_4 consequences of the accident. The influence of safety barriers can be represented in the bow–tie, as indicated in Fig. 13.

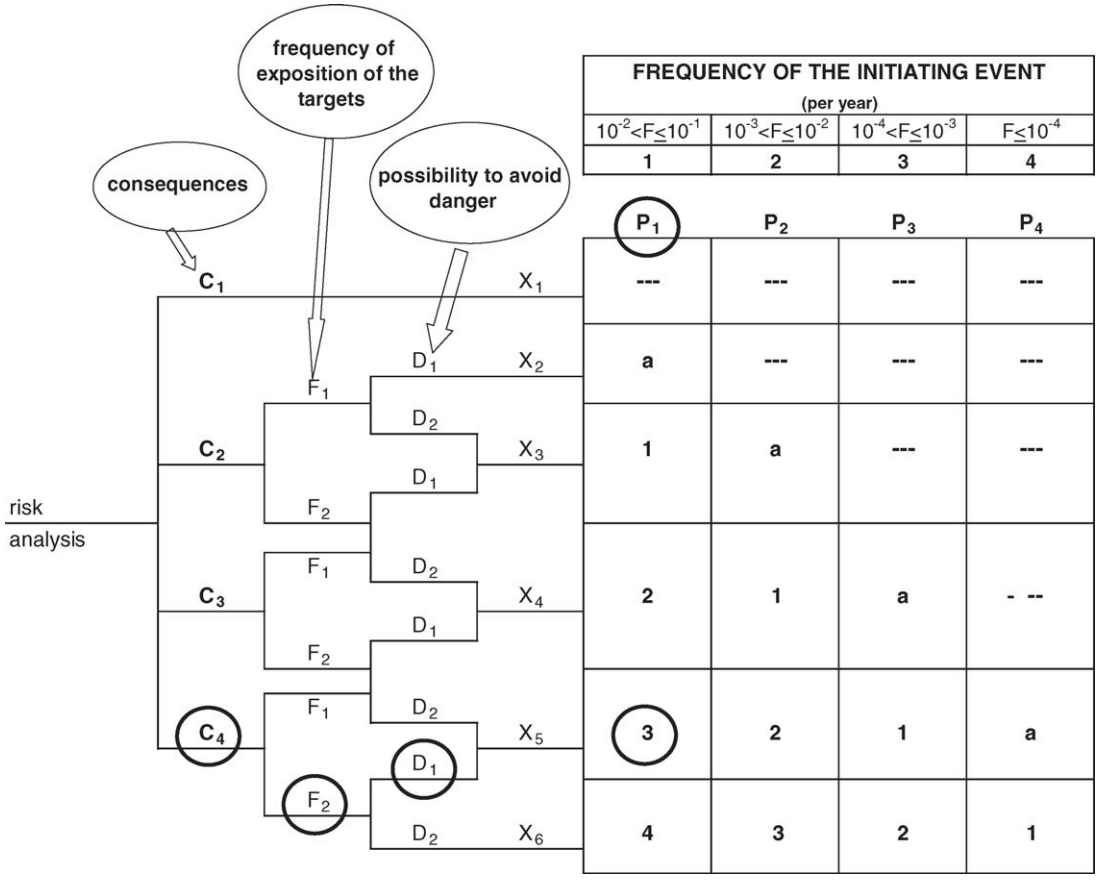


Fig. 11. Risk graph for the scenario—cause "operator error".

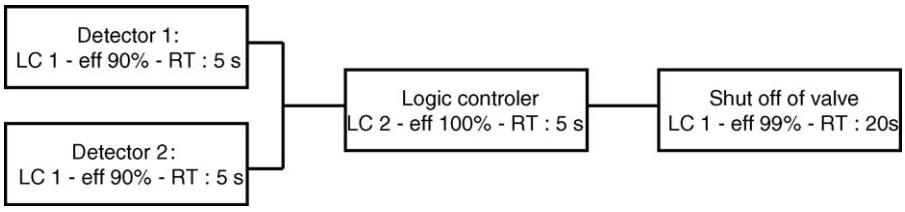


Fig. 12. Architecture of safety function (level of confidence of 1, effectiveness of 90%, response time of 30 s).

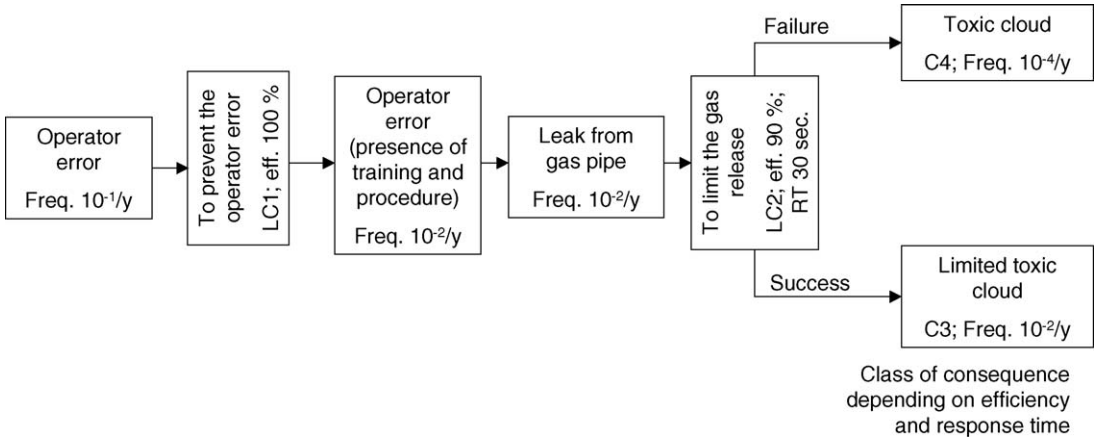


Fig. 13. Bow–tie with the influence of safety barriers.

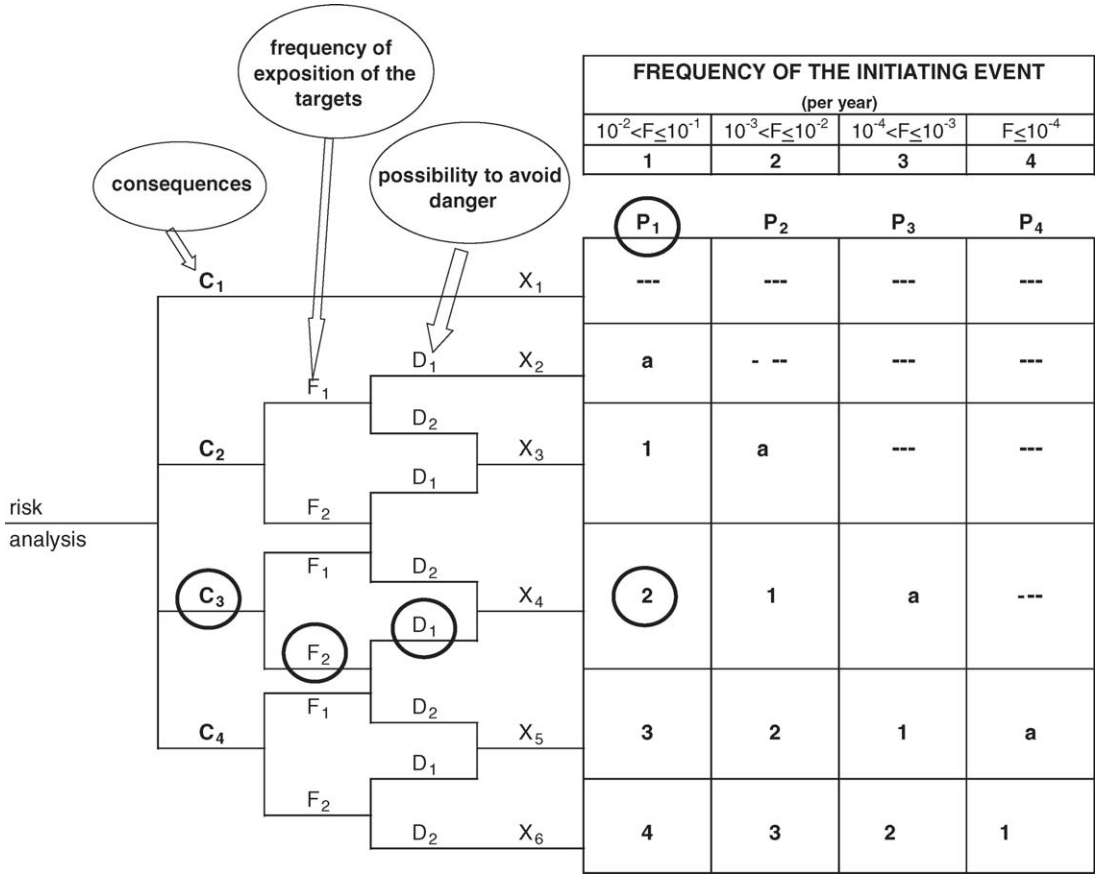


Fig. 14. Risk graph for the scenario – cause “operator error” – residual scenario.

4.2.6. Checking of effectiveness and response time

However, as the response time (30 s) of the chain cannot be totally neglected, it is, therefore, worth checking whether the residual consequences need to be controlled or not. In this case, we assume that a 30 s release leads to C_3 consequences. Since these consequences remain quite severe, they may need to be controlled. In order to assess the safety level required for this residual scenario, we can refer to the risk graph; in this case, the safety function "To limit the gas release" is of course not taken into account since we consider in the residual scenario that the safety function works properly. The class of consequence is reduced from 4 to 3; taking into account the same parameters than for the basis scenario, the requirement of level of confidence is reduced to 2 as illustrated in Fig. 14. The safety function "to prevent" does not allow meeting the requirement; additional measures are still needed. In this case, additional prevention functions may be planned or a better function "to limit" may be installed, with a lower time response with the view to reduce the class of consequence from a class 3 to a class 2.

5. Conclusions

The risk analysis has the purpose to demonstrate that an industrial site has a good level of risk control. The risk control is built on the reduction of the frequency of occurrence of the major dangerous phenomena by taking into account the safety barriers, so that the dangerous phenomena are defined with an acceptable couple gravity/frequency of occurrence.

The ARAMIS project proposes to use bow–ties diagrams that give a clear overview of the cause and consequences of an accident. The safety barriers are identified on the bow–ties showing precisely on what scenarios they act and how they reduce the frequency of occurrence of the major accident or how they lead to a decrease in the effects of an accident.

By taking into account the safety barriers on the bow–tie, ARAMIS provides an explicit demonstration of the risk control: the method is based on the existing safety barriers on the site and the criteria for assessment of the level of confidence are clearly defined. It offers an alternative way to the traditional risk-based and consequence-based methodologies for risk analysis using generic figures of frequency of occurrence of events or of causes.

An advantage of this methodology is that it appears clearly for the industrialists which barriers have an influence on risk control and/or have to be improved. It gives them reasons to invest in safety measures. The necessary evaluation of the performance of the safety barriers enables the industrialist to better know their safety functions, what is favourable to a better level of safety on site. Besides, the competent authorities have comprehensive rules to assess risk control and to check more precisely the barriers involved in the reduction of the risk. Demonstration to the public is made easier.

The use of the risk graph during risk analysis enables to perform recommendations in case that some scenarios have insufficient risk control.

It must be kept in mind that prevention remains preferable to mitigation measures. It is not acceptable to have a reduced frequency of occurrence only by mitigation measures; it is better to try to prevent the critical event. However, because complete exhaustiveness in the identification of the causes is impossible, it is also preferable to have mitigation measures on a site.

Acknowledgements

The work presented in this paper has been elaborated in the frame of the EU project "Accidental Risk Assessment Methodology for Industries" (ARAMIS), co-ordinated by INERIS (F) and including EC-JRC-IPSC-MAHB (I), Faculté Polytechnique de Mons (B), Universitat Politècnica de Catalunya (E), ARMINES (F), Risø National Laboratory (D), Universita di Roma (I), Central Mining Institute (PL), Delft University of Technology (NL), European Process Safety Centre (UK), École des Mines de Paris (F), École des Mines de Saint Etienne (F), École des Mines d'Alès (F), Technical University of Ostrava (CZ) and Jozef Stefan Institute (Si). The project is funded under the Energy, Environment and Sustainable Development Programme in the Fifth Framework Programme for Science Research and Technological Development of the European Commission.

References

[1] C. Delvosalle, C. Fiévez, A. Pipart, B. Debray, ARAMIS project: A comprehensive methodology for the identification of reference accident scenarios in process industries, J. Hazard. Mater. 130 (3) (2006) 200–219.

[2] C. Delvosalle, C. Fiévez, A. Pipart, H. Londiche, B. Debray, E. Hubert, Aramis project: effect of safety systems on the definition of reference accident scenarios in SEVESO establishments, in: Proceedings of the 11th International Symposium Loss Prevention and Safety Promotion in the Process Industries, Praha, Czech Republic, 31 May–3 June, 2004.

[3] IEC, IEC 61508, Functional safety of electrical, electronic and programmable electronic safety-related systems, parts 1–7, International Electrotechnical Commission, Geneva, 1998.

[4] IEC, IEC 61511, Functional safety instrumented systems for the industry sector, parts 1–3, International Electrotechnical Commission, Geneva, 2001.

[5] Layer of Protection Analysis, Simplified Process Risk Assessment Center for Chemical Process Safety (CCPS), American Institute of Chemical Engineers (AIChE), New York, 2001, ISBN 0-8169-0811-7.

[6] F. Guldenmund, A. Hale, L. Goosens, J. Betten, N.J. Duijm, The development of an audit technique to assess the quality of safety barrier management, J. Hazard. Mater. 130 (3) (2006) 234–241.