ELSEVIER

Journal of Hazardous Materials 130 (2006) 200–219

Journal of Hazardous Materials

www.elsevier.com/locate/jhazmat

ARAMIS project: A comprehensive methodology for the identification of reference accident scenarios in process industries

Christian Delvosalle [a,*], Cécile Fievez [a], Aurore Pipart [a], Bruno Debray [b,1]

[a] *Faculté Polytechnique de Mons, Major Risk Research Centre, 56 rue de l'épargne, 7000 Mons, Belgium*
[b] *INERIS, Accidental Risk Division, Parc Technologique ALATA, BP2, 60550 Verneuil-en-Halatte, France*

Available online 26 August 2005

Abstract

In the frame of the Accidental Risk Assessment Methodology for Industries (ARAMIS) project, this paper aims at presenting the work carried out in the part of the project devoted to the definition of accident scenarios. This topic is a key-point in risk assessment and serves as basis for the whole risk quantification.

The first result of the work is the building of a methodology for the identification of major accident hazards (MIMAH), which is carried out with the development of generic fault and event trees based on a typology of equipment and substances. The term "major accidents" must be understood as the worst accidents likely to occur on the equipment, assuming that no safety systems are installed.

A second methodology, called methodology for the identification of reference accident scenarios (MIRAS) takes into account the influence of safety systems on both the frequencies and possible consequences of accidents. This methodology leads to identify more realistic accident scenarios. The reference accident scenarios are chosen with the help of a tool called "risk matrix", crossing the frequency and the consequences of accidents.

This paper presents both methodologies and an application on an ethylene oxide storage.

Keywords: ARAMIS project; Accident scenarios; Risk analysis; Bow-tie approach; Seveso

1. Introduction

In process industries, the identification of possible accident scenarios is a key-point in risk assessment. However, especially in a deterministic approach, mainly worst cases scenarios are considered, often without taking into account safety devices used and safety policy implemented. This approach can lead to an over-estimation of the risk-level, and does not promote the implementation of safety systems.

One of the aims of the ARAMIS project is to develop a methodology able to face this problem. This paper describes methods and tools to identify major accidents (without considering safety systems), then to study deeply safety systems, causes of accidents and (qualitative) probabilities, in order to be able to identify reference accident scenarios, which take into account safety systems.

In order to reach this goal, two main complementary methods are used. Both were developed during the ARAMIS project.

The first one, the methodology for the identification of major accident hazards (MIMAH) allows to identify which major accidents are likely to occur, on the basis of equipment considered and properties of substances handled. The term "major accident hazards" must be understood as the worst accident scenarios, assuming that no safety systems (including safety management systems) are installed or that they are ineffective.

The second method is called methodology for the identification of reference accident scenarios (MIRAS). The deep study of causes of accident, probability levels and safety

* Corresponding author. Tel.: +32 65 37 44 03; fax: +32 65 37 44 07.
E-mail addresses: christian.delvosalle@fpms.ac.be (C. Delvosalle), cecile.fievez@fpms.ac.be (C. Fievez), aurore.pipart@fpms.ac.be (A. Pipart), bruno.debray@ineris.fr (B. Debray).

[1] At the time these results were produced, Bruno Debray was employed by the SITE division of the Ecole Nationale Supérieure des Mines de Saint-Etienne, France, which is also member of the ARAMIS consortium.

0304-3894/$ – see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.jhazmat.2005.07.005

systems allows to define with this method scenarios more realistic than the major accident hazards. These reference accident scenarios (RAS) represent the *real* hazardous potential of the equipment, taking into account the safety systems (including safety management system).

These methods are composed of several steps which are described in this paper and simultaneously applied on a fictitious example, i.e. an ethylene oxide storage. This substance is a toxic and flammable one. To simplify the example, only the fault tree and the event tree for the critical event "breach (large) on shell in liquid phase" associated with this equipment will be fully detailed according to these two methodologies.

2. Methodology for the identification of major accident hazards (MIMAH)

2.1. Introduction—the bow-tie approach

MIMAH means "methodology for the identification of major accident hazard". The objective of MIMAH is to identify all the potential major accident scenarios which can occur in a process industry. The main tool on which MIMAH is based is the bow-tie (Fig. 1). This tool will be largely developed in the different steps of the methodology.

A bow-tie is centred on a critical event. A critical event (CE) is generally defined as a loss of containment (LOC) or a loss of physical integrity (LPI). The left part of the bow-tie, named fault tree, identifies the possible causes of a critical event. The right part of the bow-tie, named event tree, identifies the possible consequences of a critical event.

In MIMAH, seven steps have to be followed. A general overview of these steps is shown in Fig. 2.

2.2. MIMAH step 1: collect needed information

In order to identify major accident scenarios, data must be collected. Some data have to be gathered before the beginning of the analysis, and some others can be collected during the different steps. First of all, general data about the plant are needed, such as plant layout, description of processes, description of equipment and pipes. It is also necessary to obtain information about the substances stored or handled, and their hazardous properties. It must also be stressed that a close exchange of data with industrialists will be helpful during the fifth step, devoted to the construction of fault trees.

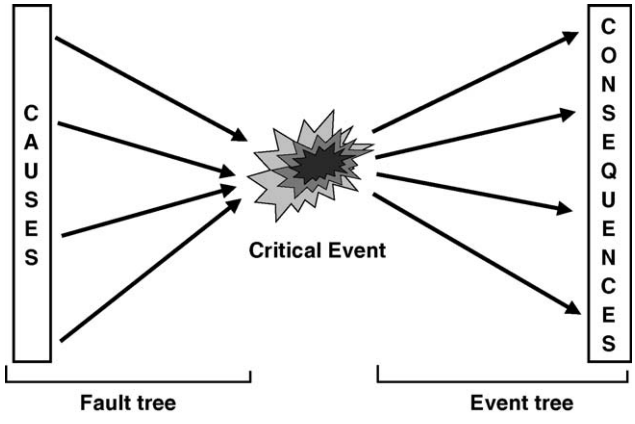

Fig. 1. General scheme of the bow-tie.

In our example, we consider an ethylene oxide storage. This horizontal cylindrical vessel (volume: 230 m^3, filling rate: 80%) is operated at 5 °C and 6.5 bar (including a nitrogen pad). The ethylene oxide is in two-phase state and is extremely flammable (R12) and toxic by inhalation, in contact with skin and if swallowed (R23).

2.3. MIMAH step 2: identify potentially hazardous equipment in the plant

On the basis of information collected, a list of the hazardous substances present in the plant must be drawn up. To achieve this, MIMAH proposes a typology of hazardous substances based on the Seveso II Directive [1] and on the risk phrases found in the 67/548/EC Directive [2].

A list of equipment containing these substances must then be drawn up. ARAMIS proposes 16 equipment categories. The list of defined equipment is presented here after:

- *Storage equipment*: mass solid storage (EQ1), storage of solid in small packages (EQ2), storage of fluid in small packages (EQ3), pressure storage (EQ4), padded storage (EQ5), atmospheric storage (EQ6), cryogenic storage (EQ7);
- *Transport equipment*: pressure transport equipment (EQ8), atmospheric transport equipment (EQ9);
- Pipes networks (EQ10);
- *Process equipment*: intermediate storage equipment integrated into the process (EQ11), equipment devoted to the physical or chemical separation of substances (EQ12), equipment involving chemical reactions (EQ13), equipment designed for energy production and supply (EQ14), packaging equipment (EQ15), other facilities (EQ16).

Finally, it is necessary to precise in which physical state the substance can be found in the equipment (solid, liquid, two-phase, gas/vapour).

A three-fold typology (hazardous substances, physical state, equipment) is thus used. The result of this step is the list of potentially hazardous equipment identified on the plant. Table 1 shows such a list, with one line devoted to the ethylene oxide storage studied in this paper.

2.4. MIMAH step 3: select relevant hazardous equipment

Among the potentially hazardous equipment identified in the previous step, it is then necessary to select the relevant hazardous equipment; it means those which participate significantly to the risk created by the plant.

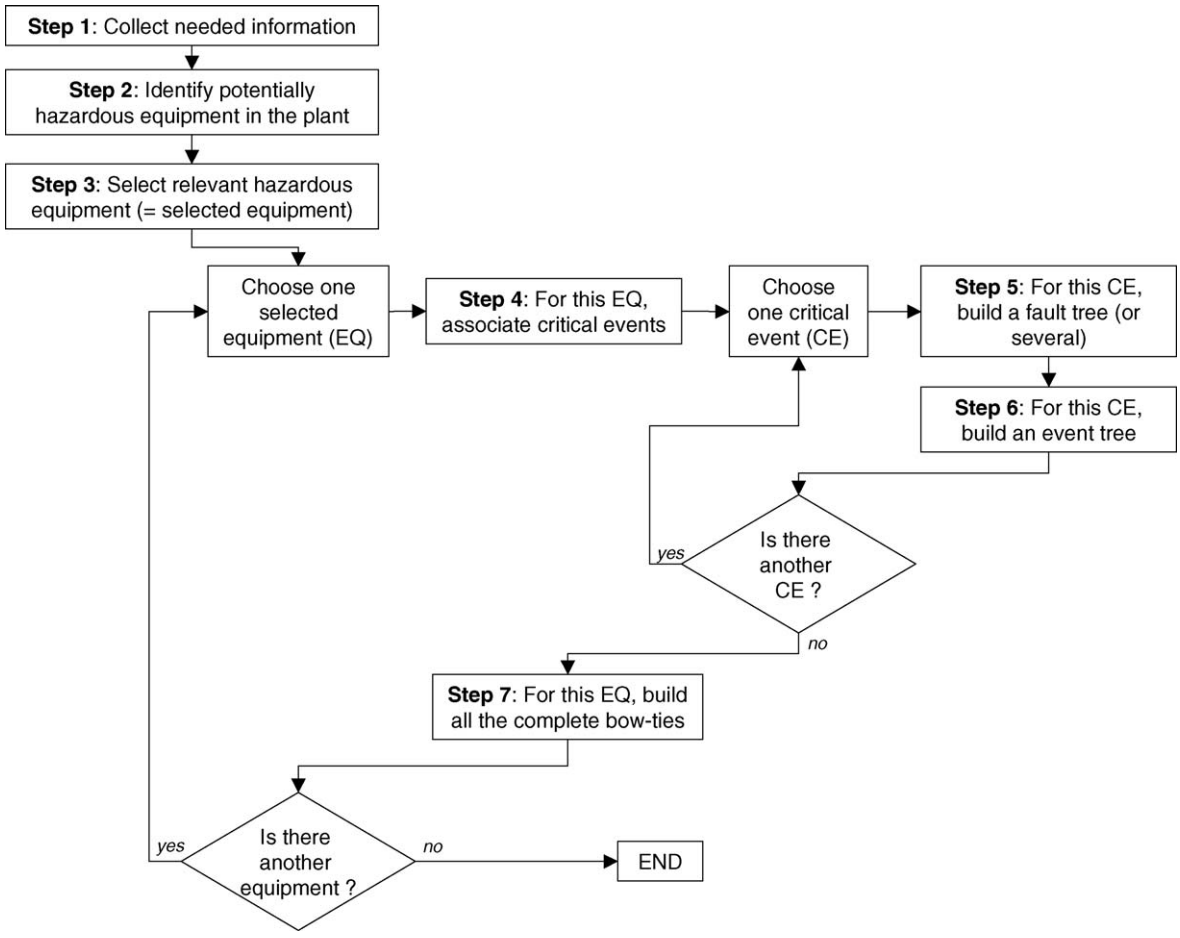

Fig. 2. General overview of the MIMAH steps.

The principle for the selection of relevant hazardous equipment is the following one: "an equipment containing hazardous substances will be selected as a relevant hazardous equipment if the quantity of hazardous substance in this equipment is higher or equal to a threshold-quantity."

The threshold depends on the hazardous properties of the substance, its physical state, its vapourisation tendency and eventually its location with respect to another hazardous equipment (possible domino effects).

The method for the selection of relevant hazardous equipment is a part of the "Vade-Mecum" proposed by the Walloon Region [3], which is a guideline for the writing of the Seveso safety report.

The method for the selection of equipment must not be applied blindly. Any additional equipment considered as

Table 1
List of potentially hazardous equipment

Name of the substance	Risk phrases	Name of the equipment	Type of equipment	State of the substance
Substance 1	R11	D-283	EQ6: Atmospheric storage	Liquid
		Stream 2	EQ10: Pipe	Liquid
Substance2	R23	T-305	EQ7: Cryogenic storage	Liquid
		Stream 5	EQ10: Pipe	Gas
Substance 3	R26	R-102	EQ12: Equipment involving chemical reaction	Gas
Ethylene oxide	R12, R23	Truck for unloading	EQ8: Pressure transport equipment	Two-phase
		Stream 4 (Unloading pipe)	EQ10: Pipe	Liquid
		T-310 (ethylene oxide storage)	EQ4: Pressure storage	Two-phase
Substance 5	R8	R-254	Eq13: Equipment devoted to the physical or chemical separation of substances	Solid
		T-256	EQ1: Mass solid storage	Solid

Table 2
Application of the method for the selection of relevant hazardous equipment

No. of equipment	Equipment	Type of equipment	Substance	Physical state	Boiling T (p atm) in °C or decomposition temperature for solid	Service T in °C	Risk phrases	Hazard classification	Contained quantity M (kg)	Reference mass Ma (kg)
1	D-283	EQ6: Atmospheric storage	Substance1	Liquid	126	25	R11	F+	5000	10000
2	Stream 2	EQ10: Pipe	Substance1	Liquid	126	25	R11	F+	200	10000
3	T-305	EQ7: Cryogenic storage	Substance2	Liquid	−34	−34	R23	T	35000	10000
4	Stream 5	EQ10: Pipe	Substance2	Gas	−34	85	R23	T	460	1000
5	R-102	EQ12: Equipment involving chemical reaction	Substance3	Gas	7.5	80	R26	T+	25	100
6	Truck of unloading	EQ8: Pressure transport equipment	Ethylene oxide	Two-phase	11	5	R12, R23	F,T	25000	10000
7	Stream 4 (Unloading pipe)	EQ10: Pipe	Ethylene oxide	Liquid	11	15	R12, R23	F,T	4200	10000
8	T-310 (ethylene oxide storage)	EQ4: Pressure storage	Ethylene oxide	Two-phase	11	5	R12, R23	F,T	54660	10000
9	R-254	EQ13: Equipment devoted to the physical or chemical separation of substances	Substance5	Solid	210	20	RB	O	350	10000
10	T-256	EQ1: Mass solid storage	Substance5	Solid	210	20	R8	O	20000	10000

No. of equipment	S1 coefficient (for the liquids) = 10 exp ($T_s - T_b$/100)	S2 coefficient (for liquids) = T_b/(−50) if T_b < °C	S coefficient (for liquids) = S1 + S2	Mass M_b (kg) = Ma/S	Selection if $M >= M_b$	Distance D from the nearest selected equipment (m)	Name of the nearest selected equipment	S3 = (0.02D) exp3	M_c (kg) = S3 × M_b	Selection if D < 50 m and $M > M_c$
1	0.10	0	0.10	100000	No	2	Cryogenic storage	0.1	10000	No
2	0.10	0	0.10	100000	No					
3	1.00	0.68	1.68	5952	Yes					
4			1.00	1000	No					
5			1.00	100	No					
6	0.87	0	0.87	11482	Yes					
7	1.10	0	1.10	9120	No					
8	0.87	0	0.87	11482	Yes					
9			1.00	10000	No					
10			1.00	10000	Yes					

dangerous due to the properties of the substance and/or the particular conditions inside or outside the equipment, can be selected as a relevant hazardous equipment and studied according to the MIMAH methodology.

To use this method, the following data are needed for each equipment identified as potentially hazardous in the step 2:

- name of the equipment;
- type of equipment;
- substance handled;
- physical state;
- boiling temperature (in °C);
- service temperature (in °C);
- risk phrases;
- hazardous classification;
- mass contained in the equipment (in kg) or, for flow through equipment (as pipes), the mass released in 10 min.

It is then possible to build a table with these data and the results of calculations required by the method (see the example presented in Table 2).

The result of this step is the selection of relevant hazardous equipment with a mass of hazardous substance higher or equal to a mass threshold. These selected equipment will be studied in the following steps of the MIMAH methodology.

2.5. MIMAH step 4: for each selected equipment, associate critical events

The centre of a bow-tie is the critical event (CE). For fluids, the critical event is generally defined as a loss of containment (LOC). For solids and more especially for mass solid storage, we would rather use loss of physical integrity (LPI), considered as a change of chemical and/or physical state of the substance.

MIMAH considers 12 different critical events which are specified hereunder:

- decomposition (CE1);
- explosion (CE2);
- materials set in motion (entrainment by air) (CE3);
- materials set in motion (entrainment by a liquid) (CE4);
- start of fire (LPI) (CE5);
- breach on the shell in vapour phase (CE6);
- breach on the shell in liquid phase (CE7);
- leak from liquid pipe (CE8);
- leak from gas pipe (CE9);
- catastrophic rupture (CE10);
- vessel collapse (CE11);
- collapse of the roof (CE12).

Table 3
Values for the size of breaches and leaks

Size of breach/leak	CE6 and 7: breaches diameter of the breach	CE8 and 9: Leaks Diameter of the leak
Large	100 mm diameter	Full bore rupture
Medium	35–50 mm diameter or diameter of the fitting	22–44% of the pipe diameter
Small	10 mm diameter	10% of the pipe diameter

For CE6–9, concerning breaches and leaks, it will be seen in Section 2.6 that three sizes of breach/leak will be defined: large, medium and small. It is then important to give figures for these sizes. MIMAH proposes to consider, by default, sizes for which generic frequencies of critical event can be found in the literature. Proposed values are detailed in Table 3.

Two matrices are used in order to define which critical events must be associated with a given equipment containing a given substance:

- one matrix crossing the type of equipment and the 12 potential critical events;
- one matrix crossing the physical state of the substance considered and the 12 potential critical events.

In our example, the equipment type considered is a pressure storage EQ4, handling a substance which physical state is STAT3 (two-phase). The critical events likely to occur on pressure storage are given in the matrix EQ-CE. Those likely to occur with a substance in two-phase state are given in the matrix STAT-CE. The combination of these information gives as result that six critical events (see Table 4) must be retained

Table 4
Critical events retained

		CE 1 decomposition	CE2 explosion	CE3 materials set in motion (entrainment by air)	CE4 materials set in motion (entrainment by a liquid)	CE5 start of a fire (LPI)	CE6 breach on the shell in vapour phase
Pressure	EQ4					X	X
Two-phase	STAT3					X	X
Results						X	X

		CE7 breach on the shell in liquid phase	CE8 leak from liquid pipe	CE9 leak from gas pipe	CE10 catastrophic rupture	CE11 vessel collapse	CE12 collapse of the roof
Pressure	EQ4	X	X	X	X	X	X
Two-phase	STAT3	X	X	X	X	X	X
Results		X	X	X	X	X	X

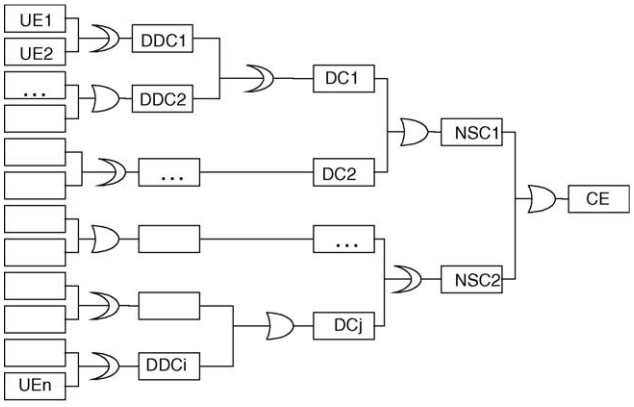

Fig. 3. Structure of the fault tree.

and associated with the pressure storage of ethylene oxide (two-phase state substance).

2.6. MIMAH step 5: for each critical event, build a fault tree

2.6.1. Objective

The objective of this step is to obtain a fault tree for each critical event identified during the previous step. The method suggests to start with the generic fault trees proposed by MIMAH. Each generic fault tree should be considered as a list of possible causes and could be modified to be adapted to actual characteristics of the equipment.

2.6.2. The generic fault trees

The general structure of the fault tree is shown in Fig. 3. The fault trees were limited to five levels linked by AND or OR gates according to the following logical sequence: combinations of undesirable events (UE) lead to detailed direct causes (DDC) which, when combined, lead to direct causes (DC) which cause necessary and sufficient conditions (NSC) provoking the critical event (CE).

MIMAH proposes 14 generic fault trees. In summary, it can be said that each critical event is associated with a generic fault tree, and that a separate fault tree is provided for each size of breach/leak.

The generic fault trees proposed by MIMAH were built following a deductive sequence, i.e. from the critical event to the undesirable events. The first step led to the identification of necessary and/or sufficient causes of the critical event. Only physical phenomena were considered at this stage. The second step involved the identification of direct causes that could lead to the occurrence of NSC's. The causes at this level were, for most of them, the causes usually considered in the accident databases such as erosion, corrosion, overpressure. In the next level called detailed direct causes, the immediate causes of the direct causes are detailed. For example, at this level the causes of corrosion are considered. They can involve the environment which can be corrosive and/or the material constitutive of the equipment which can present a poor resistance to corrosion. In the last level it was tried to propose very generic causes, called undesirable events making the link with human behaviour and organisational deficiencies which are potential causes for a very large variety of events [4].

2.6.3. Fault trees associated with identified critical events

The generic fault trees can (and should) be modified in order to be adapted to the actual characteristics of the equipment studied. For the application of the MIMAH methodology, the generic fault trees must not be used blindly but they should be used as checklists and as support for further discussions. Indeed, these fault trees must be adapted according to the design, the operating conditions, the actual external conditions of the equipment. Some causes in fault tree may be removed or some causes more specific to process or to equipment, like "loss of utility", "reverse flow", may be added and an agreement may be obtained on some causes.

It is also possible to built several fault trees for a same critical event according to the life phase of the equipment (during start-up, maintenance, shut-down, ...) because the causes can be different than the ones in operating phase.

Finally, the generic fault trees are not in opposition with other methods of risk analyses (like HAZOP or other systematic methods to identify the causes of an accident but also the risk analysis made on site). Besides, they seem complementary methods to the proposed generic fault trees in order to identify other possible causes.

2.6.4. Example

The fault tree for the critical event "large breach on shell in liquid phase" associated with the ethylene oxide storage is presented in Fig. 4 as example. This fault tree, while fictitious and simplified, is a realistic one.

2.7. MIMAH step 6: for each critical event, build an event tree

2.7.1. Structure of the event tree

The right part of the bow-tie, named event tree, identifies the possible consequences of a critical event. The structure of the event tree is shown in Fig. 5.

The critical event CE, such as a pipe failure, leads to secondary critical events SCE (for example, a pool formation, a jet, a cloud, ...), then to tertiary critical events TCE (for example, a pool ignited, a pool dispersion, a jet ignited, ...) which lead to dangerous phenomena DP. Thirteen DP are defined in the methodology: poolfire, tankfire, jetfire, VCE, flashfire, toxic cloud, fire, missiles ejection, overpressure generation, fireball, environmental damage, dust explosion, boilover and resulting poolfire. Major events (ME) are defined as the significant effects from the identified dangerous phenomena on targets (human beings, structure, environment, ...). The possible significant effects are thermal radiation, overpressure, missiles, toxic effects (on the humans or on the environment).

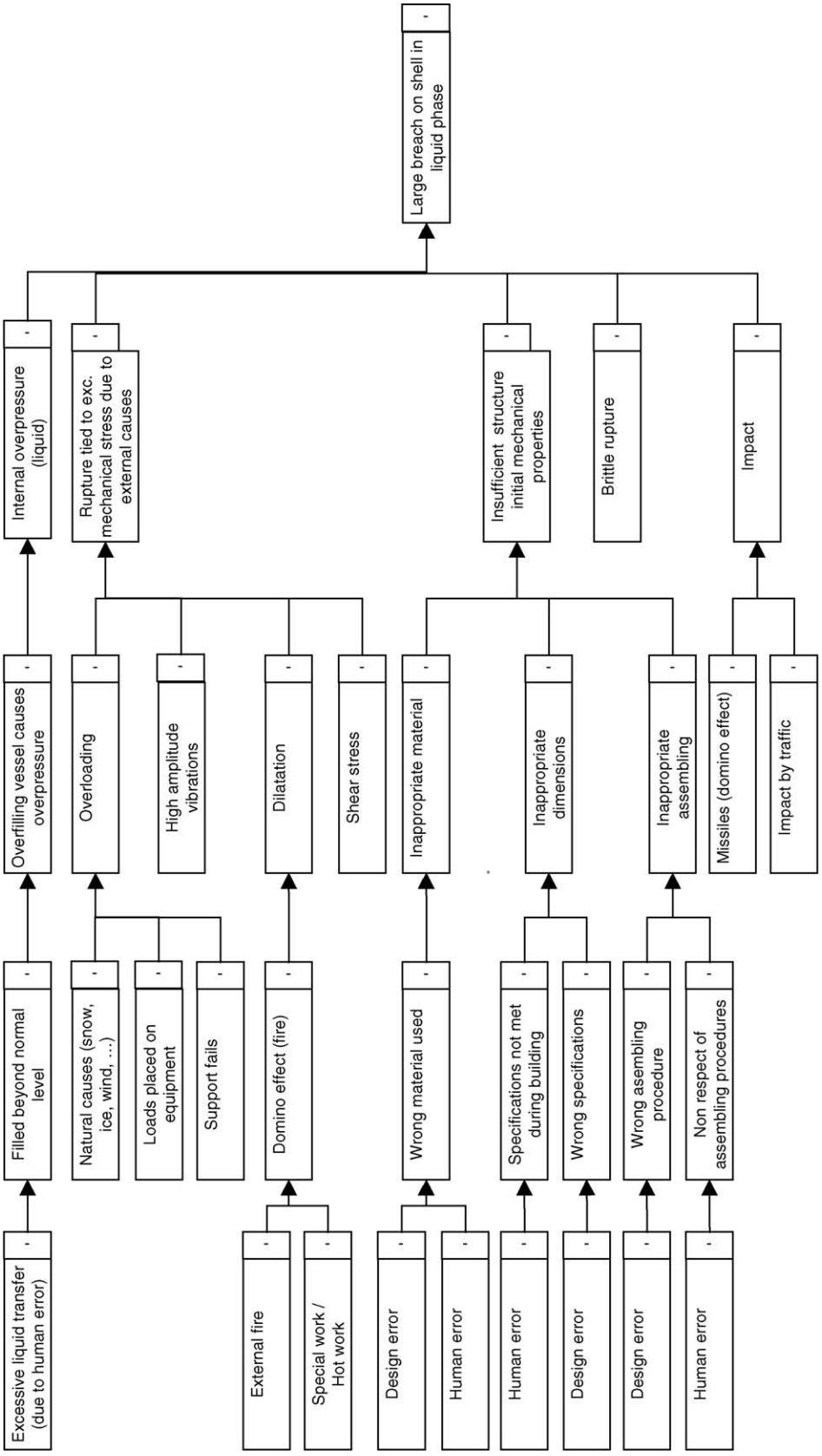

Fig. 4. Adapted fault tree for "large breach on shell".

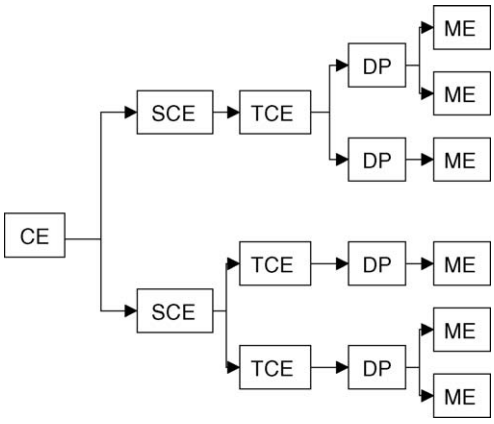

Fig. 5. Structure of the event tree.

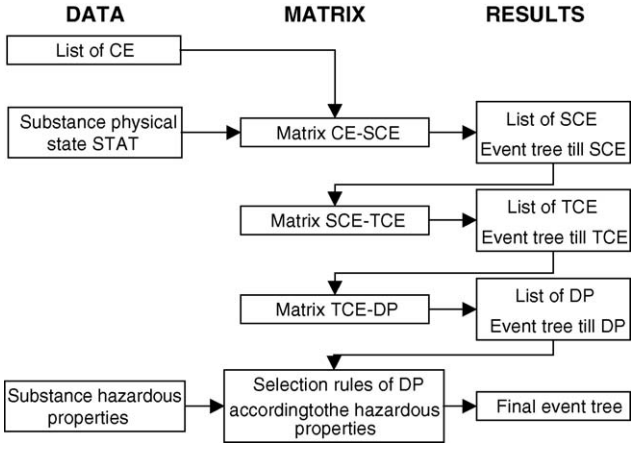

Fig. 6. Summary of the steps followed for the construction of the event trees.

2.7.2. Method of construction of the event tree

For each critical event studied, an event tree is build with an automatic method based on matrices. The data needed are the critical event considered, the physical state and the hazardous properties of the substance.

A schematic overview of the method for the building of the event trees is shown in Fig. 6. An extensive description of the method can be found in [5].

2.7.3. Example

The event tree obtained with MIMAH for the critical event "large breach on shell in liquid phase" associated with the ethylene oxide storage is shown in Fig. 7.

2.8. MIMAH step 7: for each selected equipment, build the complete bow-ties

The MIMAH methodology ends with the construction of complete bow-ties for each selected equipment. Each bow-tie is obtained by the association of a critical event, its corresponding fault tree on the left and its corresponding event tree on the right.

These bow-ties, result of the whole MIMAH method, are major accident scenarios, assuming that no safety systems (including safety management systems) are installed or that they are ineffective. They are the basis for the application of the MIRAS methodology.

3. Methodology for the identification of reference accident scenarios (MIRAS)

3.1. Objectives and main steps of MIRAS

The objective of MIRAS is to choose reference accident scenarios (RAS) among the major accident hazards identified with MIMAH. The reference scenarios will be those which have to be modelled in order to calculate the severity of a plant [6], which in turn will be compared with the vulnerability of the surroundings of the plant.

In order to define these RAS, the MIRAS methodology will take into account:

- the safety systems installed on and around the equipment;
- the safety management system;
- the frequency of occurrence of the accident;
- the potential consequences of the accident.

This goal will be reached by means of the eight steps presented in Fig. 8. The whole development has to be performed for each bow-tie built with MIMAH.

3.2. MIRAS step 1: collect needed data

Compared to the data collected for the MIMAH part, additional data will be required during the MIRAS application. Some of them can be pointed out here, for example values for frequencies/probabilities of initiating events, safety systems and procedures applying to the equipment studied, information for the assessment of the level of performance of the safety barriers, ignition probabilities if relevant, etc.

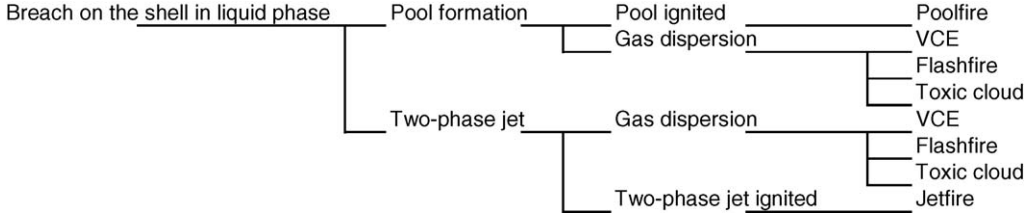

Fig. 7. Event tree for the CE7 "breach on shell in liquid phase" taking into account the risk phrases.

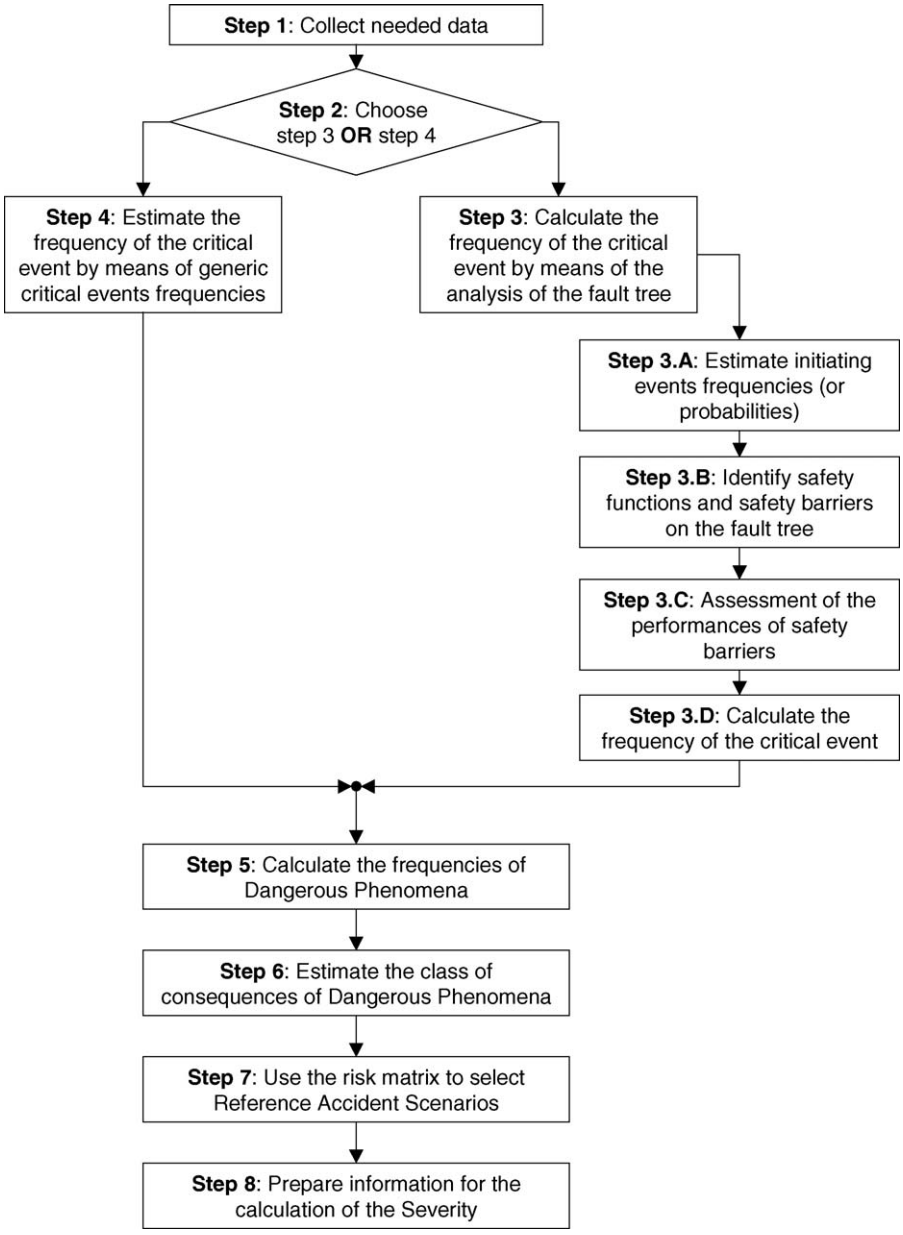

Fig. 8. General overview of the steps of MIRAS (steps to be applied for each bow-tie built with MIMAH).

3.3. MIRAS step 2: make a choice between step 3 or step 4

Steps 3 and 4 have the same goal: estimate the frequency per year of the critical event for the considered bow-tie.

The first choice is to make a complete analysis of the fault tree in taking into account the influence of safety barriers in order to calculate the frequency of the critical event. This way is presented in step 3. The alternative way is to estimate directly the frequency of the critical event. This way is presented in step 4.

The first way should be preferred if the data are available. Even if this method is more time-consuming, it allows to take into account the safety systems related to the prevention of critical events (those located on the left-side part of the bow-tie). In the second way, the prevention level of the plant is no more considered, but the time required for the analysis is shorter.

3.4. MIRAS step 3: calculate the frequency of the critical event by means of the analysis of the fault tree

If this way is chosen, four steps have to be followed. Firstly, the frequencies (or probabilities) of the initiating events (left-end of the fault tree) must be assessed. Secondly, safety barriers influencing the events in the fault tree must be identified. Thirdly, the performance of these safety barriers must be assessed. And finally, all these parameters have to be

Table 5
Qualitative definitions of initiating events frequencies

Frequency of occurrence per year		Class
Qualitative definition	Quantitative definition	Ranking
Very low frequency: unlikely to occur	$F \leq 10^{-4}$ year^{-1}	F_4
Low frequency: the critical event (for the given cause) might happen. It has already happened in similar installations (once by 1000 years)	10^{-4} year$^{-1} < F \leq 10^{-3}$ year^{-1}	F_3
Medium frequency: the critical event (for the given cause) might happen. It has already happened in similar installations or on the site (once by 100 years)	10^{-3} year$^{-1} < F \leq 10^{-2}$ year^{-1}	F_2
Possible—high frequency; may happen. Has already happened in the site (once during 10 years)	10^{-2} year$^{-1} < F \leq 10^{-1}$ year^{-1}	F_1
Likely—very high frequency: has already happened several times in the site	$F \geq 10^{-1}$ year^{-1}	F_0

taken into account to calculate the frequency of the critical event.

3.4.1. MIRAS step 3.A: estimate initiating events frequencies (or probabilities)

The objective of this step is to provide frequency (probability) figures for the initiating events, defined as the first causes upstream of each branch leading to the critical event in the fault tree.

ARAMIS gives an overview of data available for the frequencies (or probabilities) of initiating events. Precise data and explanations can be found in the full ARAMIS report [7] and cannot be reproduced here due to limited extend of this paper. However, some remarks should be brought to the fore here.

- There is obviously a lack of data in this field. The synthesis of published data shows that there is a great discrepancy in figures found, and in the quantity of data available for the different kind of initiating events.
- When possible, it is recommended to use plant specific data if they are available. Or, at least, to try to estimate the frequencies of initiating events with the plant staff, with the help of qualitative frequencies given in Table 5.

For the sake of the example, the estimated frequencies of initiating events are written down in the fault tree: "large breach on shell in liquid phase" (see Fig. 9). The estimated frequencies are invented but remain realistic.

3.4.2. MIRAS step 3.B: identify safety functions and safety barriers on the fault tree

In order to identify the safety systems which have an influence on the occurrence of the accident, the concept of safety functions and safety barriers was introduced. A typology of safety functions and safety barriers was also defined in order to facilitate the identification and the assessment of performances of these barriers. More details about the exact definitions of these concepts are given in [8].

Starting from the fault tree built with MIMAH, the objective is to obtain a fault tree on which safety barriers are placed at the right place. To achieve this goal, it is proposed to review systematically the fault tree.

Each event of a tree, branch per branch, must be examined and the following question should be asked: "Is there a safety barrier which avoids, prevents or controls this event ?". If yes, this safety barrier must be placed on the branch. The barrier will be placed upstream of an event if it avoids or prevents this event. If it controls this event, it has to be placed downstream. This identification can (should) be made with the industrialists (operators, safety officers, . . .), with the help of "process and instrumentation diagrams" and "flow diagrams" or with any other existing documentation. The ARAMIS full report [7] proposes a check-list of safety functions and barriers on all the events of the bow-tie.

The various safety functions and barriers placed on the fault tree "large breach on shell in liquid phase" are given in the Fig. 10 for the considered example.

3.4.3. MIRAS step 3.C: assessment of the performances of safety barriers

Once the safety barriers have been identified and placed on the fault tree, it is necessary to assess the influence of these barriers on the frequency of the critical event.

First of all, it must be stressed that a barrier must fulfil some minimum requirements to be considered as a relevant safety barrier. These requirements are explained in [8].

When a barrier is considered as relevant, its performance is defined according to three parameters:

- its level of confidence (LC) linked to its probability of failure on demand (PFD);
- its adequate capacity to take the required action (specific size or volume, physical strength, etc.) or effectiveness (E);
- its response time (RT).

The definitions and the way to assess these parameters are explained in details in [8].

In a first step, the assessed level of confidence is the "design" level of confidence. This means that the barrier is supposed to be as efficient as when its was installed, to have the same response time and the same level of confidence.

But the performance of the safety barrier could decrease during the lifetime of an installation. This could occur for multiple reasons; for example, a bad inspection program, a loss of knowledge of the operators, the clogging up of some devices, ... All these reasons can be related to the quality of the safety management system.

In a second step, it is thus needed to assess the quality of the safety management system and its influence on the

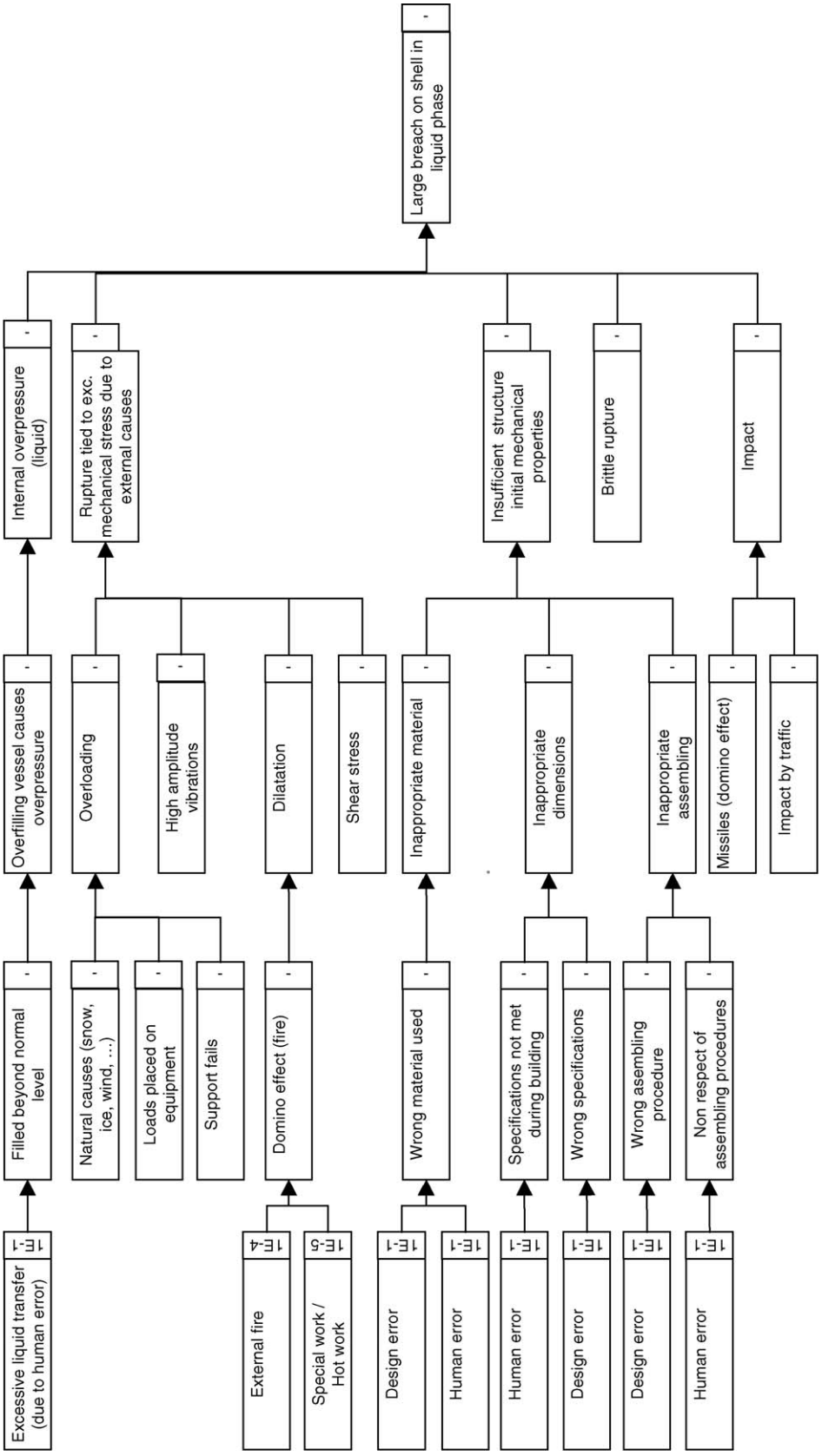

Fig. 9. Frequencies of initiating events on the fault tree.

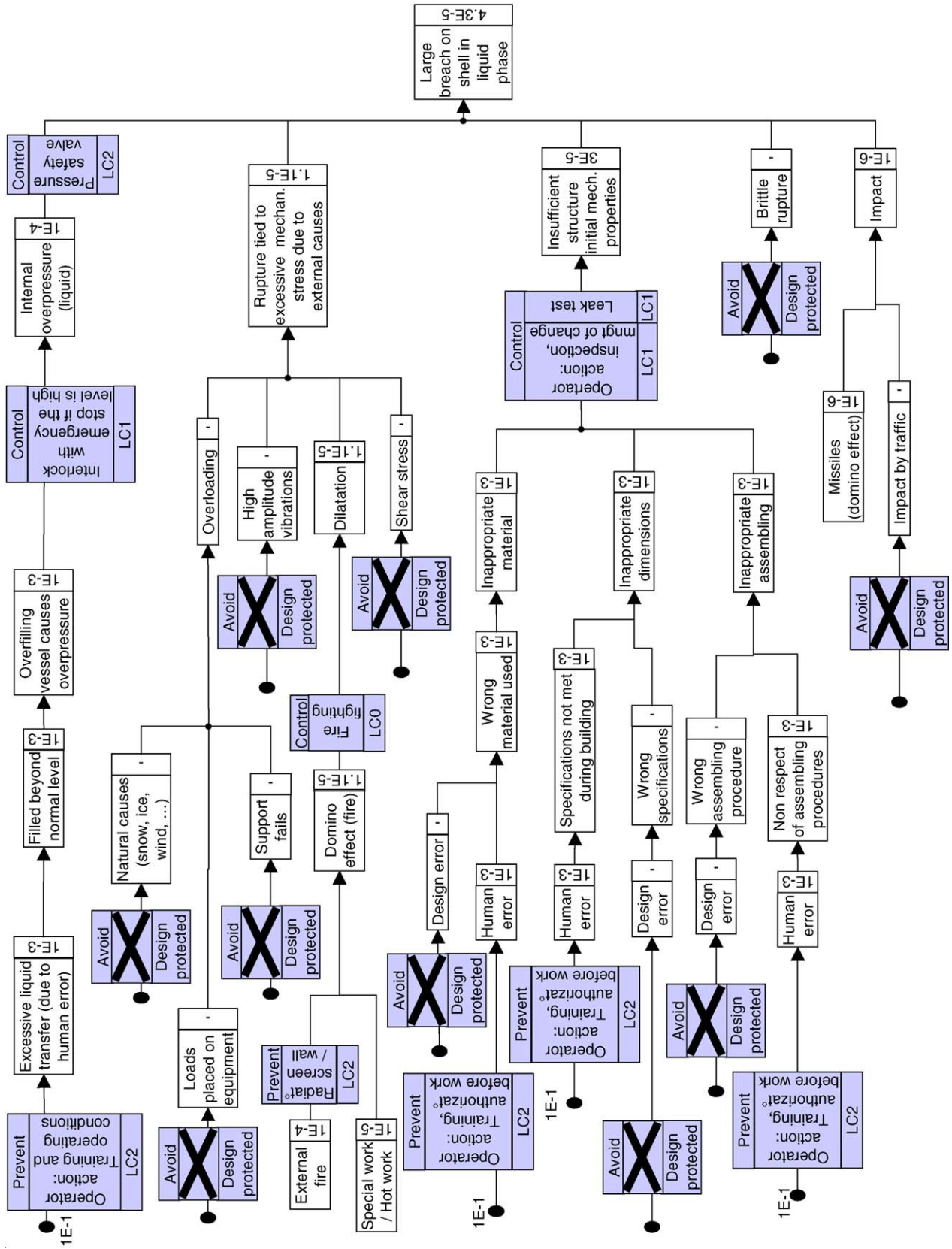

Fig. 10. Fault tree with the frequency of CE "large breach on the shell in liquid phase".

performances of the safety barriers. The tools for the management audit are described in an other ARAMIS part [9]. One of the aims of the audit is to verify if the safety barriers are enough inspected and maintained. If it is not the case, the level of confidence of safety barriers will be decreased according to the results of the audit. This will give the "operational" level of confidence of the safety barrier.

Details about the modifications of the performances of the safety barriers according to the quality of the safety management system should be found in the ARAMIS part related to the safety management system [9].

In the example, only the "design" levels of confidence of the safety barriers were estimated. These levels are written down in the fault tree "large breach on shell in liquid phase" (see Fig. 10).

Let us note that the "design protected" avoid barriers are, in fact, prevention barriers with a very high level of confidence (of course obvious evidence is required). Causes protected by such barriers can be ignored in the calculation of the critical event frequency.

3.4.4. MIRAS step 3.D: calculate the frequency of the critical event

After the evaluation of the initiating events characteristics, the identification of the safety barriers and the evaluation of their performances, it is possible, at this stage, to analyse the fault tree in order to calculate the frequency of the associated critical event. The analysis will be made by a gate-to-gate method. However, this step may be complex and some rules should be kept in mind in order to avoid error in the predicted critical event frequency. Detailed explanations about these calculations can be found in the literature (e.g. [10]).

This method starts with the initiating events of the fault tree and proceeds upward toward the critical event in taking into account the safety barriers on the fault tree.

The ways to take into account the effects of safety barriers are explained in details in [8]. The main principles are explained hereafter. The "avoid" barriers imply that the event located just downstream is supposed impossible. The corresponding branch will thus not influence the critical event frequency anymore. For the "control" and "prevent" barriers, the rule is the following: "If the level of confidence of a barrier on a branch is equal to n, then the frequency of the downstream event on the branch is reduced by a factor 10^n."

The frequencies of the various events in the fault tree and, finally, of the critical event, taking the safety barriers into account, can thus be calculated. The results for the example are presented in Fig. 10. In the example, the estimated critical event frequency is 4.3×10^{-5} year^{-1}. This value, which is obtained for a fictitious example, seems reasonable.

3.5. MIRAS step 4: estimate the frequency of the critical event by means of generic critical events frequencies

If the frequency of the critical event cannot be calculated on the basis of the analysis of the fault tree (step 3), another possibility is to evaluate it by means of generic critical event frequencies.

During the ARAMIS project, a bibliographic review was performed about published data on this subject. MIRAS provides a table summarising the data collected, and proposes values or ranges of values for the different critical event frequencies, depending on the kind of equipment considered [7]. An extract of this table is shown here (Table 6).

The frequencies have a generic character and they are given for a "standard" security level. However, in the literature, the "standard" security level is not specified. This means that the reader has to be careful when handling these figures.

When a range of frequency values is provided, a figure should be chosen in the range, rather a high value if the safety level is poor, or rather a low value if the safety level is good. Information found in the literature do not allow to give more precise guidance on the choice of a precise value.

3.6. MIRAS step 5: calculate the frequencies of dangerous phenomena

The objective, at this stage, is to proceed step by step in the event tree to obtain, as output, the frequency of each dangerous phenomenon. First of all, the transmission probabilities in the tree will be discussed and the safety barriers related to the event tree side will be taken into account, both in terms of consequences and frequency of dangerous phenomena.

3.6.1. Evaluation of the transmission probabilities in the event trees (rain-out, ignition probabilities, probability of VCE/flashfire)

In the event trees, several binary choices need to be translated in terms of conditional probabilities: for example, is there an immediate ignition or not ? If not, is there a delayed ignition or not ? In case of delayed ignition of a vapour cloud, will it end in a vapour cloud explosion (VCE) or a flashfire?

As the probabilities of ignition and the probability of VCE depend on a lot of parameters (e.g. the flammability of the substance, the source term, the presence and the type of ignition sources, the meteorological conditions, the obstruction of site, ...), these parameters and these probabilities should be discussed with the industrialists on site. To help the reader, ARAMIS proposes some conservative values of probabilities. An extract of the ARAMIS proposals is shown in Tables 7 and 8.

3.6.2. Influence of safety barriers in the event tree

The objective is now to identify safety barriers on the event tree, and then to quantify their influence.

For the identification of the safety barriers, the method proposed is identical to the one used for the fault tree: it is proposed to review systematically the event tree. Each event of the tree, branch per branch, must be examined and the following question should be asked: "Is there a safety barrier which

Table 6
Generic frequencies of critical events (extract)

Failure frequency (/year)		Breach on the shell in vapour phase		Breach on the shell in liquid phase		Leak from liquid pipe		Leak from gas pipe	
		CE6		CE7		CE8		CE9	
Pressure storage	EQ4	10mm	5 E-05	10mm	5 E-05	All fittings	0.15 E-3	All fittings	0.15 E-3
		35mm	5 E-06	35mm	5 E-06				
		50mm	1 E-06	50mm	1 E-06				
		100mm	5 E-07	100mm	5 E-07				
Atmospheric storage **(single containment)**	EQ6			10mm	1 E-04	Same values as for a pipe			
				35mm	1.8 E-05				
				50mm	5 E-06				
				100mm	5 E-06				
Pressure transport equipment	EQ8	Largest connection	5E-07	Largest connection	5 E-07	Full bore rupture of hose	4 E-06 /hour	Full bore rupture of hose	4 E-06 /hour
		10mm	1.1 E-04- 1.3 E-05	10mm	1.1 E-04 - 1.3 E-05	10% of the nominal diameter (ND)	4 E-05 /hour	10% of ND	4 E-05 /hour
		35mm	4.4 E-06	35mm	4.4 E-06	Full bore rupture of arm	3 E-08 /hour	Full bore rupture of arm	3 E-08 /hour
		50mm	5 E-05	50mm	5 E-05	10% of ND	3 E-06 - 3 E-07 /hour	10% of ND	3 E-06 - 3 E-07 /hour
		100mm	3 E-06	100mm	3 E-06				
Pipe	EQ10					**/year and /m**	ND <75mm	75mm< ND <150mm	ND >150mm
						10% of ND	1.18 E-05	2.5 E-06	1.75 E-06
						22% of ND	7.93 E-06	1.11 E-06	6.5 E-07
						44% of ND	3.3 E-06	4.62 E-07	2.7 E-07
						Full bore rupture	1.22 E-06	3.5 E-07	1.18 E-07

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 prevents this one. If it controls or limits this event, it has to be placed downstream. This identification can (should) be made with the industrialists (operators, safety officers, . . .), with the help of "process and instrumentation diagrams" and "flow diagrams" or with any other existing documentation.

The performance of the safety barriers identified must then be assessed. The procedure is also the same as for the barriers in the fault tree. To be considered as relevant, a barrier must meet some minimum requirements expressed in [8]. Then,

Table 7
Probability of immediate ignition

Source term		Substance	
Continuous (gas jet) (kg/s)	Instantaneous (gas puff) (kg)	Gas (low reactive)	Gas (average or high reactive)
<10	<1000	0.02	0.2
10–100	1000–10000	0.04	0.5
>100	>10000	0.09	0.7

Table 8
Probability of VCE (compared to flash fire), according to the obstruction when the delayed ignition occurs

Obstruction	Probability of VCE
Low	0.1
Medium	0.5
Strong	2/3

the "Design" level of confidence, the effectiveness and the response time have to be evaluated.

An operational level of confidence has to be assessed, reflecting the influence of the quality of the safety management system.

Finally, the safety barriers related to the event tree side have to be taken into account, both in terms of consequences and frequencies of dangerous phenomena, as explained in [11]. Briefly, it can be pointed out that the prevention and control barriers decrease the transmission probability between two events and influence the dangerous phenomena frequencies. The limitation barriers reduce the consequences of dangerous phenomena in limiting the source term or in limiting their effects. In the event tree when a limitation barrier is met, two branches appear, one if the barrier fails with a probability equal to the probability of failure on demand (PFD) of the barrier and an other if the barrier succeeds with a probability equal to (1-PFD).

The probability of failure on demand (PFD) of a safety barrier is equal to 10^{-n}, n being the level of confidence of the barrier.

3.6.3. Example

Thanks to these various types of probabilities and the evaluation of safety barriers, the frequency of dangerous phenomena associated with each critical event identified by MIMAH can be calculated. The event tree following the critical event "large breach on shell in liquid phase" on the ethylene oxide storage is shown in Fig. 11. In this figure, the frequencies of dangerous phenomena are calculated and the limitations of the source term and/or effects of dangerous phenomena by the limiting safety barriers are also specified.

3.7. MIRAS step 6: estimate the class of consequences of dangerous phenomena

The selection of reference accident scenarios is based on the evaluation of the frequency of dangerous phenomena together with their potential consequences. At this stage, it is thus necessary to evaluate roughly the consequences of each dangerous phenomenon.

The evaluation of the potential consequences is only qualitative. A quantitative assessment will be made in the ARAMIS part devoted to the calculation of the Severity, but this step can only be made after the selection of reference accident scenarios.

The qualitative assessment of the consequences of dangerous phenomena is based on four classes of consequences defined in Table 9. These classes are defined according to potential consequences in term of domino effects, effects on human targets and effects on the environment.

Even if the material and financial damages are considered as criteria for the notification of an accident at the European Commission in the SEVESO II Directive, it should be noted that they are not retained as criteria for the definition of consequence classes defined in Table 9. As a matter of fact, the severity and vulnerability mappings do not take financial aspects into account.

Thus, for each dangerous phenomenon obtained during the development of the event trees, a class of consequence must be chosen according to the definitions given in Table 9. It should be noted that, due to the presence of safety barriers, dangerous phenomenon can be "fully developed" or "limited":

- a dangerous phenomenon with a "limited source term" means that the consequences of the critical event are limited by a successful safety barrier (for example by limiting the size of the pool or the release duration);

Table 9
Class of consequences

Consequences			Class
Domino effect	Effect on human target	Effect on environment	Ranking
To take into account domino effects, the class of consequences attributed to the studied dangerous phenomenon will be increased to the class of the secondary dangerous phenomenon that the first can bring about by domino effects	No injury or slight injury with no stoppage of work	No action necessary, just watching	C_1
	Injury leading to an hospitalisation >24 hours	Serious effects on environment, requiring local means of intervention	C_2
	Irreversible injuries or death inside the site, reversible injuries outside the site	Effects on environment outside the site, requiring national means	C_3
	Irreversible injuries or death outside the site	Irreversible effects on environment outside the site, requiring national means	C_4

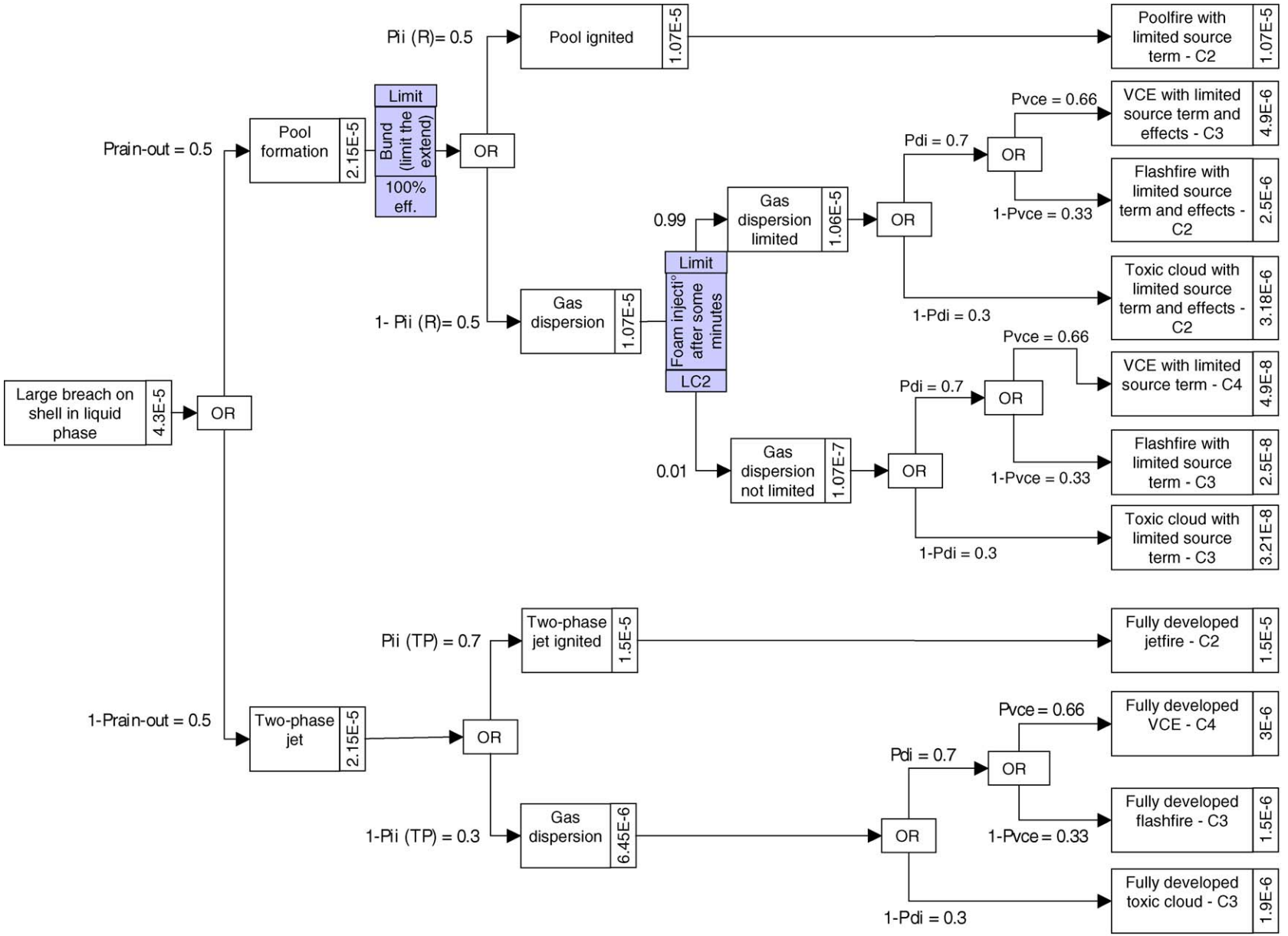

Fig. 11. Event tree with the frequencies of dangerous phenomena for the large breach on shell in liquid phase.

Table 10
Rough class of consequences of "fully developed" dangerous phenomena

Dangerous phenomena	Consequence class
Poolfire	C2
Tankfire	C1
Jetfire	C2
VCE	C3 or C4 (according to the released quantity)
Flashfire	C3
Toxic cloud	C3 or C4 (according to the risk phrases; C4 for very toxic substances)
Fire	C2
Missile ejection	C3
Overpressure generation	C3
Fireball	C4
Environmental damage	To judge on site
Dust explosion	C2 or C3 (according to the substance and the quantity)
Boilover and resulting poolfire	C3

- a dangerous phenomenon with "limited effects" means that a limiting barrier acts in the event tree, but not directly influencing the source term (for example a water curtain which limits the quantity of gas constituting the cloud);
- a "fully developed" dangerous phenomenon means that no safety system limits the consequences of the critical event and no safety system mitigates the effects.

Obviously, a dangerous phenomenon can be defined as "with a limited source term" and "with limited effects" if the two kinds of barriers are present and are successful.

For "fully developed" dangerous phenomena, rough consequence classes given in Table 10 could be used. If the dangerous phenomenon is "limited", the "fully developed" class of consequence could be decreased, according to the type of limiting systems and always referring to the definitions of Table 9.

Among the three categories of consequences (human, environmental and domino effects), the most serious one has to be taken as final consequences class. This choice is conservative.

The output of this step is a list of dangerous phenomena associated with each critical event identified by the MIMAH methodology. The frequency of each dangerous phenomenon was calculated in step 5, and thanks to step 6, a class of consequence is associated with each dangerous phenomenon found in the event trees (see Fig. 11).

3.8. MIRAS step 7: use the risk matrix to select reference accident scenarios

The objective of this step is to select the reference accident scenarios which will be modelled in the calculation of the severity. The tool used here is a risk matrix (Fig. 12). The *X*-axis corresponds to the four consequence classes, and the *Y*-axis corresponds to the frequency of the dangerous phenomena. Three zones are defined in this matrix.

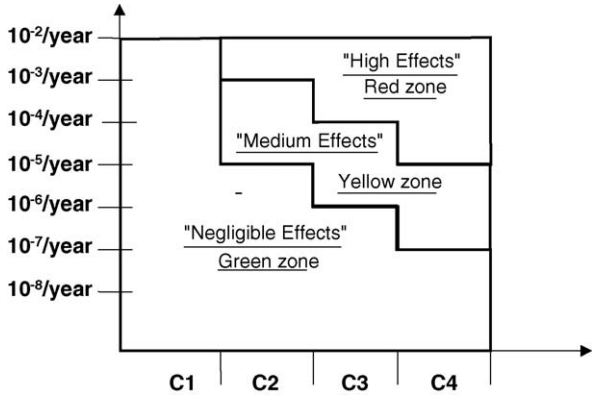

Fig. 12. Risk matrix.

- The lower green zone ("negligible effects" zone) corresponds to dangerous phenomena with a low enough frequency and/or consequences which will probably have no actual effects on the severity.
- The intermediate yellow zone ("medium effects" zone) corresponds to dangerous phenomena which will probably have actual effects on the severity and will then be selected to be modelled for the severity calculations. These dangerous phenomena correspond to reference accident scenarios.
- The upper red zone ("high effects" zone) corresponds to very dangerous phenomena which will surely have actual effects on the severity. Corresponding accident scenarios should be revisited in order to put additional safety systems in place. However, if nothing is changed, these dangerous phenomena shall be selected, in their present state, to be modelled for the severity calculations. Of course, these dangerous phenomena correspond to reference accident scenarios.

Each dangerous phenomenon resulting from the bow-ties must be placed in the risk matrix, according to its frequency and its class of consequence. dangerous phenomena in yellow and red zones have to be modelled for the severity calculations.

From the results presented in the event tree (see Fig. 11), each dangerous phenomenon identified in our example are placed in the risk matrix, according to its frequency and its class of consequence (see Fig. 13).

Thus, it appears that six reference accident scenarios (corresponding to the reference dangerous phenomena located in the "yellow" or "red" zones) will have to be modelled for the severity calculations:

- fully developed jetfire;
- fully developed VCE;
- fully developed flashfire;
- fully developed toxic cloud;
- poolfire with limited source term;
- VCE with limited source term and effects.

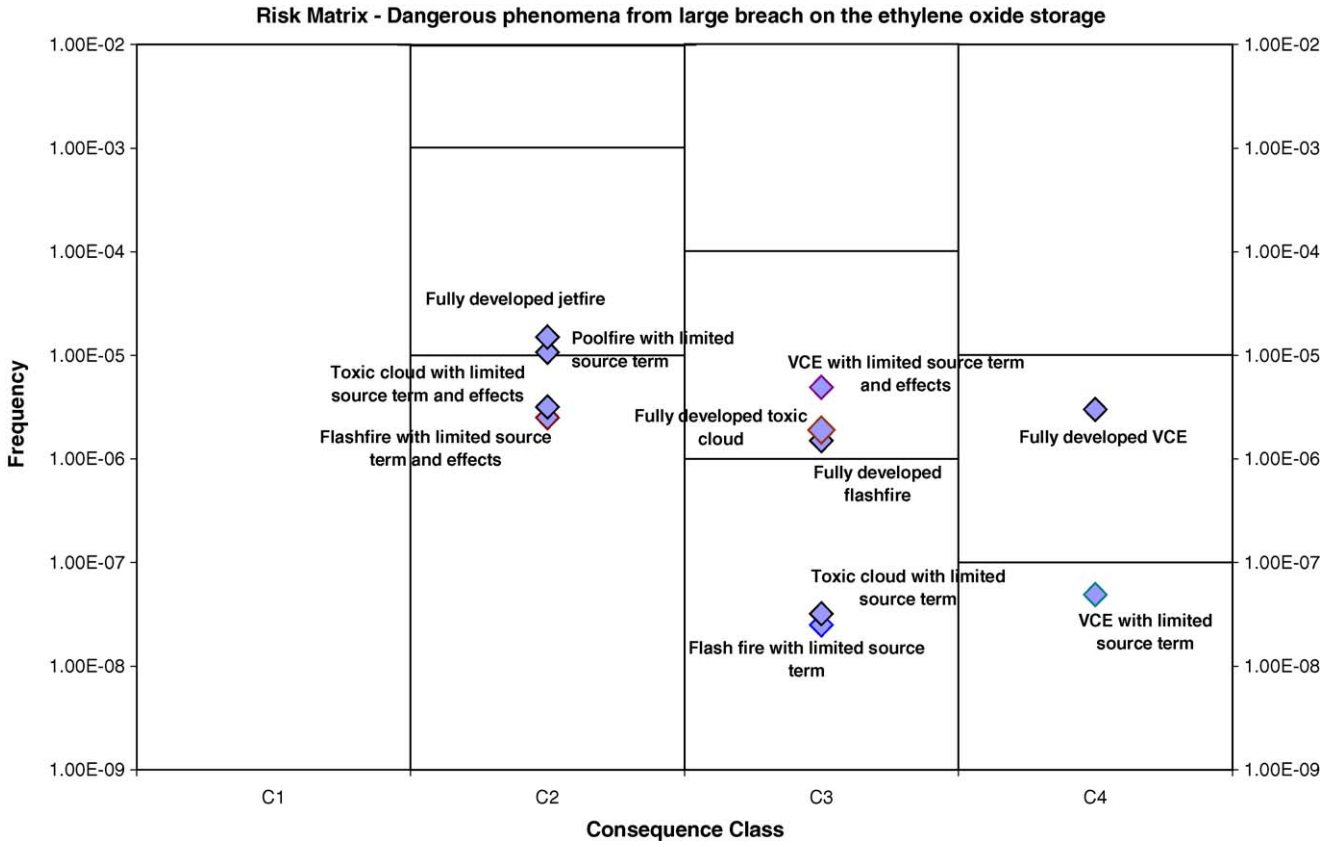

Fig. 13. Risk matrix with dangerous phenomena from large breach on shell in liquid phase.

The risk matrix should not be used blindly. One can always choose to model a scenario located in the green zone if it is believed necessary to do so. At the very worst, this will only be time consuming but also offer the possibility to appreciate the real impact of questionable scenarios. It should be reminded that this risk matrix is actually not a guide for the acceptability of risk, but it is only a guidance to select reference accident scenarios which have to be modelled for the calculation of the severity.

3.9. MIRAS step 8: prepare information for the calculation of the severity

The last bow-ties obtained by the MIRAS methodology (including the influence of safety systems), the risk matrix with all dangerous phenomena and the reference accident scenarios will be used for the calculation of the severity index S [6].

For each reference accident scenario (a dangerous phenomenon located in the yellow or red zone of the risk matrix), the information needed for the severity calculations are the equipment characteristics (volume, height of liquid, operating conditions, ...), the properties and the quantity of the substance, the characteristics of the critical event (e.g. diameter of the breach, release time, ...), the characteristics of safety barriers which may affect the severity modelling, the description of the site surroundings, the meteorological conditions, ...

4. Discussion

The result of this work is a comprehensive methodology. An extended documentation describes each step to be followed, and numerous tools and concrete figures are provided [7].

In the MIMAH part, several tools can be put to the fore:

- A method gives information on how to identify potentially hazardous equipment on a plant, and how to select relevant hazardous equipment, which are likely to influence the global risk level of the plant.
- MIMAH is based on a bow-tie analysis. Instructions are given to select adequate type of loss of containment or other kind of accidents likely to occur on equipment (centre of the bow-tie).
- For each kind of equipment, guidelines help to identify possible causes of accidents and to structure them in fault trees (left part of the bow-tie).
- A tool helps to build automatically event trees (right part of the bow-tie), depending on the kind of equipment considered, the hazardous properties of the substance handled and its physical state.

- All these tools allow to identify major hazard potential of a plant.
- With the second method, called MIRAS, safety devices and safety management are taken into account to identify accurately the risk level. Again, several tools are available.
- Reference accident scenarios are selected on the basis of their frequency and their potential consequences. Precise criteria are provided.
- The calculation of the frequency of scenarios starts from the estimation of the frequency of initiating events at the left end of the fault tree. Numerous figures are provided to assess these frequencies.
- Moving to the right in the bow-tie, tools and figures are also provided to evaluate some transmission probabilities, i.e. ignition probabilities.
- Everywhere in the bow-tie, the development of an accident can be prevented, stopped, controlled with the help of safety barriers, technical and management ones. MIRAS proposes precise definitions of what is a safety barrier, how they can be placed on a bow-tie, how to assess their efficiency and what is their influence on the development of an accident, in terms of both frequency and consequences.

These methods have been tested in five chemical plant across Europe. Feed-back from these case studies is included in the tools presented in this paper and thus the method is believed to be consistent and applicable. Moreover, besides the final objective which is to identify reference accident scenarios, the ARAMIS methodology offers a great number of parallel outcomes resulting from the wide variety of tools mentioned above.

5. Conclusions

A part of the work carried out for the ARAMIS project was devoted to the identification of reference accident scenarios in process industries. Two complementary approaches are used, firstly the methodology for the identification of major accident hazards (MIMAH), and secondly the methodology for the identification of reference accident scenarios (MIRAS).

MIMAH allows to select the relevant hazardous equipment on a plant, which are likely to influence the risk level of the plant. According to a bow-tie approach and on the basis of the equipment type, the substance handled, its physical state and hazardous properties, the major accidents are identified through generic fault and event trees.

In MIRAS, safety devices and policies are taken into account to identify scenarios more realistic than the major accident hazards, the reference accident scenarios. A "barrier approach" is applied on the bow-ties. Everywhere in the bow-tie, the development of an accident can be prevented, stopped, controlled with safety barriers. Their efficiency and their influence on both frequency and consequences of the accident are estimated.

In parallel, different frequencies/probabilities (frequencies of initiating events and of critical events, transmission probabilities) are studied all along the branches of the fault and the event tree.

Finally, the reference accident scenarios are selected thanks to a "risk matrix" crossing the frequency and the potential consequences of accidents. The risk matrix identifies accident scenarios with actual effects on the severity, called "reference accident scenarios", and points out accident scenarios not adequately protected and needing additional safety systems.

The application to an example, an ethylene oxide storage, shows that these methodologies are consistent and applicable.

Acknowledgements

The results presented in this publication have been elaborated in the frame of the EU project ARAMIS (Accidental Risk Assessment Methodology for IndustrieS), contract no EVG1-CT-2001-00036, co-ordinated by INERIS (F) and including EC-JRC-IPSC-MAHB (I), Faculté Polytechnique de Mons—MRRC (B), Universitat Politecnica de Catalunya—CERTEC (SP), ARSMINES (F), Risø National Laboratory (DK), Univertsita di Roma—Dipartimento Ingegneria Chimica (I), CMI—Safety Management and Technical Hazards (PL), Delft University of Technology, Safety Science Group (NL), European Process Safety Centre (UK), Ecole des Mines de Paris—Pôles Cindyniques (F), Ecole des Mines de St Etienne—SITE (F), Ecole des Mines d'Alès—LGEI (F).

The programme is organised within the Energy, Environment and Sustainable Development Programme in the fifth Framework Programme for Science Research and Technological Development of the European Commission.

References

[1] Council Directive 96/82/EC of 9 December 1996 on the control of major accident hazards involving dangerous substances, Off. J. Eur. Commun. L 10 (1997) 13–33 (14 January).
[2] Council Directive 67/548/EEC of 27 June 1967 on the approximation of laws, regulations and administrative provisions relating to the classification, packaging and labeling of dangerous substances, Off. J. P 196 (1967) 0001-0098 (16 August).
[3] Ministry of Walloon Region, Belgium, Vade Mecum: Spécifications techniques relatives au contenu et à la présentation des études de sécurité, Direction Générale des Ressources Naturelles et de l'Environnement, Cellule Risque d'Accidents Majeurs, 2000.
[4] B. Debray, C. Delvosalle, C. Fiévez, A. Pipart, H. Londiche, E. Hubert, Defining safety functions and safety barriers from fault and event trees analysis of major industrial hazards, in: Proceedings ESREL, Berlin, Germany, 14–18 June 2004.
[5] C. Delvosalle, C. Fiévez, A. Pipart, J. Casal Fabrega, E. Planas, M. Christou, F. Mushtaq, ARAMIS Project: Identification of reference accident scenarios in SEVESO establishments, in: Proceedings ESREL, Maastricht, The Netherlands, 16–18 June 2003, pp. 479–487.

[6] J. Casal, E. Planas, A. Vallée, A proposal for mapping risk severity of a plant, J. Hazard. Mater. 130 (3) (2006) 242–250.
[7] C. Delvosalle, C. Fiévez, A. Pipart, Aramis project, Deliverable D1C WP1, Project report issued for the European Commission, July 2004.
[8] V. de Dianous, C. Fiévez, ARAMIS project: A more explicit demonstration of risk control through the use of bow-tie diagrams and the evaluation of safety barrier performance, J. Hazard. Mater. 130 (3) (2006) 220–233.
[9] F. Guldenmund, A. Hale, L. Goossens, 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.
[10] Centre for Chemical Process Safety (CCPS), Guidelines for Chemical Process Quantitative Analysis, American Institute of Chemical Engineers, Center for Chemical Process Safety, New York, 1989.
[11] C. Delvosalle, C. Fiévez, A. Pipart, B. Debray, H. Londiche, ARAMIS project: Effect of safety systems on the definition of reference accident scenarios in SEVESO establishments, in: Proceedings Loss Prevention, Prague, Czech Republic, 31 May–3 June, 2004.

Glossary

Effectiveness of a safety barrier: the effectiveness is the ability for a technical safety barrier to perform a safety function for a 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 which would be not completely closed on safety demand would not have an effectiveness of 100%.

Level of confidence of a safety barrier: the probability of failure on demand 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 similar to the notion of SIL (Safety Integrity Level) defined in IEC 61511 for Safety Instrumented Systems but applies here to all types of safety barriers.

Response time: 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.

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

Safety function: a safety function is a technical or organisational action, and not an object or a physical system. 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 will be realised thanks to a safety barrier. The safety function is the "what" needed to assure, increase and/or promote safety.