The European Commission
Community Research
Energy, Environment and Sustainable Development

PROPOSAL FOR THE 5TH FRAMEWORK PROGRAMME

ARAMIS

ACCIDENTAL RISK ASSESSMENT METHODOLOGY FOR INDUSTRIES
IN THE CONTEXT OF THE SEVESO II DIRECTIVE

Contract number : EVG1 – CT – 2001 – 00036

Deliverable D.1.C.

WP 1

Faculté Polytechnique de Mons
Major Risk Research Centre
Prof. C. Delvosalle
Ir C. Fiévez, Ir A. Pipart

F.P.Ms
MAJOR RISK RESEARCH CENTRE

July 2004

TABLE OF CONTENTS

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 report 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 is the **Methodology for the Identification of Major Accident Hazards (MIMAH)**. The MIMAH methodology defines the maximum hazardous potential of an installation. The term "Major Accident Hazards" must be understood as the worst accidents likely to occur on this installation, assuming that no safety systems (including safety management systems) are installed or that they are ineffective. The major accident hazards identified are only linked with the type of equipment studied and the properties of chemicals handled.

The second method is called **MIRAS (Methodology for the Identification of Reference Accident Scenarios).** This method studies the influence of safety devices and policies on scenarios identified by the MIMAH methodology. The deep study of causes of accident, probability levels and safety systems allows to define 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).

The Reference Accident Scenarios have then to be modelled to obtain the **severity** mapping, which has to be compared with the **vulnerability** mapping of the surroundings of the plant.

The aspects of management, severity and vulnerability are dealt with in other parts of the ARAMIS project. In addition to the identification of Reference Accident Scenarios, they constitute the risk assessment methodology called ARAMIS.

This report is mainly devoted to the explanation of MIMAH and MIRAS contributions to the ARAMIS project. By means of the different steps described, the reader will be able to define, for a given process plant, the Reference Accident Scenarios which have to be taken into account.

A Glossary of the main terms used in this report is presented in appendix 1

2. Methodology for the identification of major accident hazards (MIMAH - Construction of bowties without safety barriers)

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 the MIMAH methodology is based is the **bow-tie** (Figure 1). This tool will be largely developed in the different steps of the methodology.

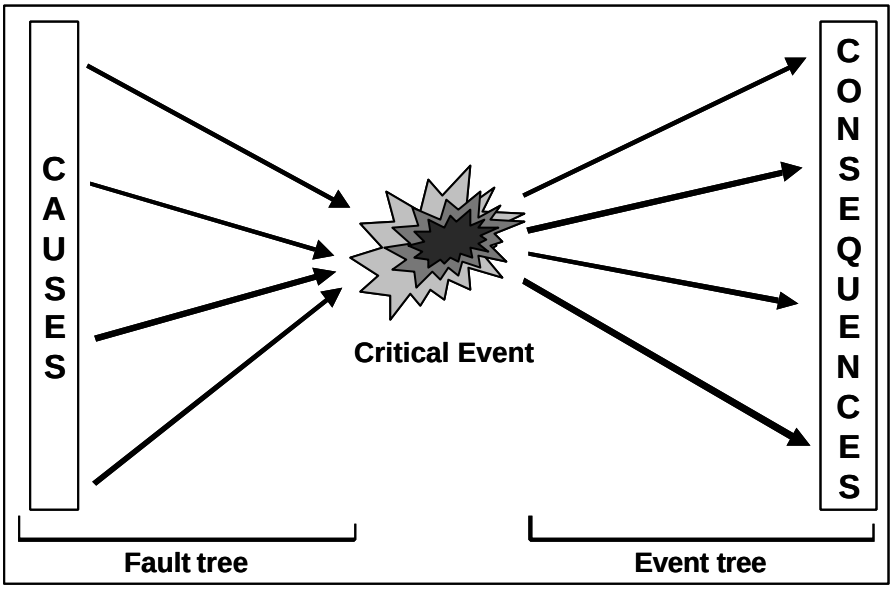

Figure 1: General scheme of the bow-tie

A bow-tie is centred on a critical event. A **Critical Event** 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.

2.2 Main steps of MIMAH

In MIMAH, 7 steps have to be followed:

- Step 1: Collect needed information
- Step 2: Identify potentially hazardous equipment in the plant
- Step 3: Select relevant hazardous equipment
- Step 4: For each selected equipment, associate critical events
- Step 5: For each critical event, build a fault tree
- Step 6: For each critical event, build an event tree
- Step 7: For each selected equipment, build the complete bow-ties

A general overview of the steps involved in MIMAH is shown in Figure 2.

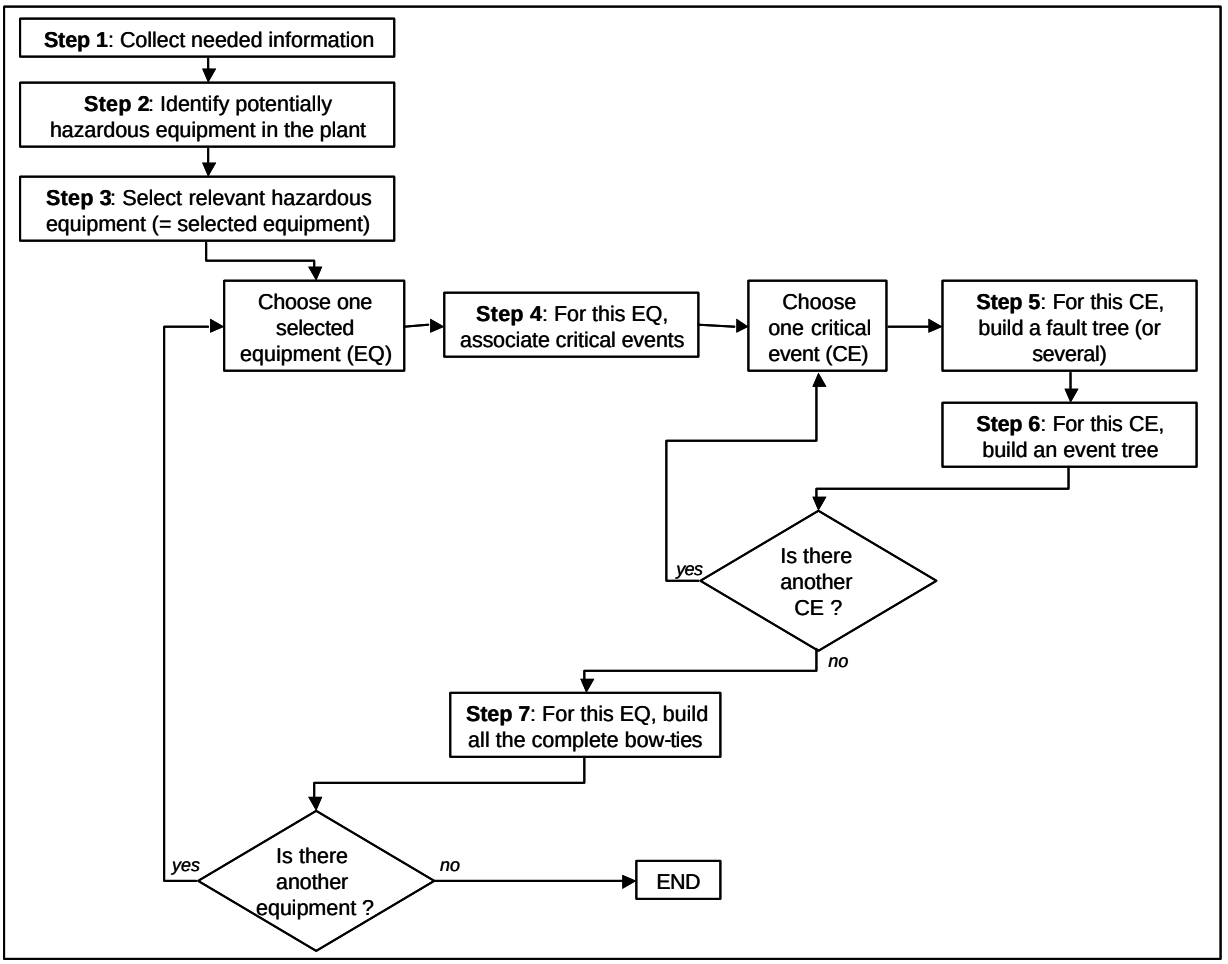

Figure 2: General overview of the MIMAH steps

2.3 MIMAH Step 1: Collect needed information

In order to identify major accident scenarios, many data must be collected. The list given in Table 1 describes the minimum data needed to achieve MIMAH.

The user can choose to collect all the data at the same time, or to collect data progressively when they are needed. In Table 1, the needed data are linked to the step during which they will be used.

Table 1: Data needed for MIMAH (step by step)

Step	Description of data needed
Step 1: Collect needed information	General data about the plant (in order to have an overview of the plant and of the processes) • Plant layout • Brief description of processes • Brief description of equipment and pipes
Step 2: Identify potentially hazardous equipment in the plant	• List of substances stored or handled in the plant, associated with the list equipment concerned • Hazardous properties of the substances
Step 3: Select relevant hazardous equipment	For each potentially hazardous equipment: • name of the equipment • size (volume, dimension) • service pressure and temperature • substances handled • substance state • quantity of substance "in" the equipment (in kg for contents or in kg/s for flows) • substance hazardous properties (risk phrases, hazard classification) • substance boiling temperature For this step, PFD should be useful (especially for flow rates through equipment)
Step 4: For each selected equipment, associate critical events	No additional data
Step 5: For each critical event, built a fault tree	*This step requires a review of possible causes of accidents. Strictly speaking, no additional data is required, but a meeting with industrialists concerned could be fruitful. It could be necessary to use risk assessment methods during this step.*
Step 6: For each critical event, built an event tree	No additional data

Step	Description of data needed
Step 7: For each selected equipment, build the complete bow-ties	No additional data

If available, results from previous risk analysis or the safety report required by the Seveso II Directive could be a good source of information and should be asked for.

2.4 MIMAH Step 2: Identify potentially hazardous equipment in the plant

2.4.1 INTRODUCTION

On the basis of information collected (see paragraph 2.3), **a list of the hazardous substances present in the plant** must be drawn up (paragraph 2.4.2). In a second step, it is necessary to draw up **a list of equipment containing these substances**, and to specify in which **physical state** the substance can be found in the equipment (paragraph 2.4.3). A threefold typology (hazardous substances, physical state, equipment) is thus used.

2.4.2 DRAW UP A LIST OF HAZARDOUS SUBSTANCES PRESENT IN THE PLANT

All the hazardous substances having one or several risk phrases mentioned in the typology of hazardous substances (Table 2) should be considered.

In Table 2, the hazardous properties of substances are classified in categories according to the SEVESO II Directive (96/82/EC) and, for each category, risk phrases are associated (namely as defined in the 67/548/EC Directive, see also remarks under the table).

Table 2: Typology of hazardous substances

Category	Risk phrases	
Very toxic	R26	Very toxic by inhalation
	R100(3)	Emit very toxic vapours when it is on fire (*)
Toxic	R23	Toxic by inhalation
	R101(3)	Emit toxic vapours when it is on fire (*)
Oxidising	R7	May cause fire (organic peroxides)
	R8	Contact with combustible material may cause fire
	R9	Explosive when mixed with combustible material

Category	Risk phrases	
Explosive	R1	Explosive when dry. (*)
	R2	Risk of explosion by shock, friction, fire or other sources of ignition
	R3	Extreme risk of explosion by shock, friction, fire or other sources of ignition
	R4	Forms very sensitive explosive metallic compounds.(*)
	R5	Heating may cause an explosion. (*)
	R6	Explosive with or without contact with air. (*)
	R16	Explosive when mixed with oxidising substances. (*)
	R19	May form explosive peroxides. (*)
	R44	Risk of explosion if heated under confinement. (*)
	R102(3)	Pyrotechnic substance
Flammable	R10	Flammable
	R18	In use, may form flammable/explosive vapour-air mixture. (*)
Highly flammable	R10	Flammable (in particular conditions of temperature and pressure) (1)
	R11	Highly flammable
	R17	Spontaneously flammable in air
	R30	Can become highly flammable in use. (*)
Extremely flammable	R10	Flammable ($T > T_{éb}$) (2)
	R11	Highly flammable ($T > T_{éb}$) (2)
	R12	Extremely flammable
React violently with water	R14	Reacts violently with water
	R15	Contact with water liberates extremely flammable gases
	R29	Contact with water liberates toxic gas
	R14/15	Reacts violently with water, liberating extremely flammable gases
	R15/29	Contact with water liberates toxic, extremely flammable gas
React violently with another substance	R103(3)	Contact with an other substance liberates toxic gas (*)
	R104(3)	Contact with an other substance liberates very toxic gas (*)
	R105(3)	Contact with an other substance liberates flammable gas (*)
	R106(3)	In case of contact with an other substance, can explode (*)

Category	Risk phrases	
Dangerous for the environment (aquatic environment)	R 50	Very toxic to aquatic organisms: (96h CL50 (fish) ≤ 1 mg/l or 48h CE50 (daphnia) ≤ 1 mg/l or 72 h CL50 (algae) ≤ 1 mg/l)
	R51	Toxic to aquatic organisms (96h CL50 (fish): 1mg/l < CL50 ≤ 10 mg/l or 48h CE50 (daphnia): 1mg/l < CE50 ≤ 10 mg/l or 72 h CL50 (algae): 1mg/l < CI50 ≤ 10 mg/l).
Dangerous for the environment (non-aquatic environment)	R54	Toxic to flora. (*)
	R55	Toxic to fauna. (*)
	R56	Toxic to soil organisms. (*)
	R57	Toxic to bees. (*)
	R59	Dangerous for the ozone layer. (*)

(1) In order to take into account the definition of "highly flammable substance" in the SEVESO II Directive relating to substances which have a flash point lower than 55 °C and which remain liquid under pressure, where particular processing conditions, such as high pressure or high temperature, may create major-accident hazards, the flammable substances in particular conditions of temperature and pressure with the risk phrase R10 are considered as highly flammable substances (risk phrase R11) as in the SEVESO II Directive.

(2) In order to take into account the definition of extremely flammable substance in the SEVESO II Directive relating to liquid substances and preparations maintained at a temperature above their boiling point, the flammable substances with the risk phrase R10 and the highly flammable substances with the risk phrase R11 at a temperature superior at boiling point are considered as extremely flammable substances (risk phrase R12) as in the SEVESO II Directive.

(3) Some risk phrases do not have an "official" number. For their easy handling, numbers were added. They are easily recognisable by their number higher than 100.

(*) The star indicates risk phrases not retained in the Seveso II Directive, but which have to be considered in this method.

2.4.3 DRAW UP THE LIST OF EQUIPMENT IN WHICH HAZARDOUS SUBSTANCES CAN BE FOUND

To divide roughly a site in several parts, the notion of **unit** is introduced. The unit is defined as a part of an establishment forming a logical set, geographically separated from the other parts of the establishment (for example by a wall of an open space). Four kinds of units are defined:

- **Storage unit**: unit used for the storage of raw materials, intermediate goods, manufactured products or waste products.

- **(Un)loading unit**: unit used for inlet and outlet of substances in the establishment, involving transport equipment.
- **Pipes networks**: piping linking different units are considered as "pipes networks" (for example a pipe linking an unloading unit and a storage unit, or linking a storage unit and a process unit), as well as pipes feeding the flare.
- **Process unit**: unit used for the processing of substances or for the production of energy used in the establishment.

For each identified hazardous substance and each unit of the plant, it is necessary to draw up **a list of equipment which may contain these substances** (eventually substances which may be generated in this equipment). The equipment must be classified according the typology of equipment defined in Table 3. In this table, 16 types of equipment have been defined .

It is also necessary to define in which **physical state** the substance can be found in the equipment (solid, liquid, two-phase, gas/vapour).

Table 3: Typology of equipment

N^r	Type of equipment	Definition
Storage units		
EQ1	Mass solid storage	Storage of solid substances in the form of powder or pellets. These substances may be stored in bulk or in silos (solid products storage in form of "small" bags are not taken into account here).
EQ2	Storage of solid in small packages	Low capacity storage of solid in bags and in storage tanks with individual volume smaller than ≅ 1 m³.
EQ3	Storage of fluid in small packages	Low capacity storage of fluid as carboys, drums and all storage tanks with individual volume is smaller than ≅ 1 m³.
EQ4	Pressure storage	Storage tanks working at ambient temperature and at a pressure above 1 bar (pressure exerted by the substance, eventually with an inert gas). The substance stored can be a liquefied gas under pressure (two phase equilibrium) or a gas under pressure (one phase).
EQ5	Padded storage	Storage tanks working at ambient temperature and at a pressure above 1 bar (the pressure is exerted by a pad of inert gas) and containing a substance in a liquid state.
EQ6	Atmospheric storage	Storage tanks working at ambient temperature and pressure and containing a substance in a liquid state.
EQ7	Cryogenic storage	Storage tanks working at atmospheric pressure or at a lower pressure and at a low temperature. The substance stored is a refrigerated liquefied gas.

N^{r}	Type of equipment	Definition
	(Un)loading units	
EQ8	Pressure transport equipment	Transport equipment working at ambient temperature and at a pressure above 1 bar (pressure exerted by the substance, eventually with an inert gas). The substance stored can be a liquefied gas under pressure (two phase equilibrium) or a gas under pressure (one phase).
EQ9	Atmospheric transport equipment	Transport equipment working at ambient temperature and pressure and containing a substance in a liquid state.
	Pipes networks	
EQ10	Pipe	Piping linking different units of the plant are considered as "pipe" (for example a pipe linking an unloading unit and a storage unit, or linking a storage unit and a process unit), as well as pipes feeding the flare. Piping inside a unit (for example inside a storage farm, or between two process equipment of the same process unit) are not considered as "pipe". They are integral part of the equipment to which they are linked.
	Process units	
EQ11	Intermediate storage equipment integrated into the process	Storage equipment which can be found inside a process unit, as a mass solid storage, a pressure storage, a padded storage, an atmospheric storage, a cryogenic storage.
EQ12	Equipment involving chemical reactions	Equipment in which a chemical reaction occurs, for example a reactor.
EQ13	Equipment devoted to the physical or chemical separation of substances	Equipment in which a physical or chemical separation occurs, for example a distillation column, an absorption column, a liquid – liquid extraction equipment, a centrifuge, a filter, a separator, a dryer, a sieve, a classifier, etc
EQ14	Equipment designed for energy production and supply	Equipment providing energy, for example furnaces; boilers, direct-fired heated exchangers
EQ15	Packaging equipment	Equipment dedicated to the packaging of material. Packages are not included here, but only the packaging system
EQ16	Other facilities	Equipment not classified among the previous categories, for example pumps, heat exchangers, compressors, gas expansion facility, mixers, blenders, etc

2.4.4 CONCLUSION FOR THE IDENTIFICATION OF POTENTIALLY HAZARDOUS EQUIPMENT

As result of this step, a table should be obtained with the following columns:

- Name of the substance
- Hazardous properties of the substance (Risk phrases)
- Name of the equipment in which the substance can be found
- Type of the concerned equipment
- State of the substance in the concerned equipment

This table constitutes the list of potentially hazardous equipment identified on the plant.

Remark:

Some equipment could be considered as hazardous one because they are likely to cause a domino effect but do not contain an hazardous substance (for example a boiler which can generate missiles in case of explosion but which only contains water). These equipment **are not considered as potentially hazardous** in this methodology. They will be taken into account in the fault tree when the possible causes of accident on neighbouring equipment will be examined.

2.5 MIMAH Step 3: Select relevant hazardous equipment

The principle for the selection of relevant hazardous equipment is the following:

> ***An equipment containing hazardous substances will be selected as 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 possibility of vaporisation and eventually its location with respect to another hazardous equipment in case of possible domino effects.

The method for the selection of relevant hazardous equipment is described in the appendix 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.

The method must not be applied blindly. If an equipment can be dangerous by the presence of an hazardous substance and by the operating conditions inside the equipment, it can be selected as a relevant hazardous equipment and studied according the MIMAH methodology.

2.6 MIMAH Step 4: For each selected equipment, associate critical events

2.6.1 DEFINITION OF THE CRITICAL EVENTS

The centre of a bowtie is the **critical event**. The **Critical Event** is generally defined as a **Loss of Containment (LOC)**. This definition is quite accurate for fluids, as they usually behave dangerously after release. 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 substances.

MIMAH considers 12 different critical events which are defined in Table 4.

Table 4: List of critical events

	Critical events	Definition
CE1	Decomposition	This critical event concerns only *solid substances*. It corresponds to a change of chemical state of the substance (Loss of Physical Integrity, LPI) by action of a energy/heat source or by reaction with a chemical substance (incompatible reagent). The decomposition of the substance leads, as secondary and tertiary critical events, to an emission of toxic products or to a delayed explosion of flammable gas formed (reaction not spontaneous but can be violent). This critical event concerns only *mass solid storage*
CE2	Explosion	This critical event concerns only **explosive** *solid substances* with "explosive" risk phrases (e.g. R2, R3, R6 …). It corresponds to a change of physical state of the substance (LPI) by action of an energy/heat source or by action of a chemical source (incompatible reagent). This change of state implies a combustion of a solid with overpressure generation (or an explosion) due to a violent and spontaneous reaction. This critical event concerns *only mass solid storage*. In case of substance stored in a closed vessel, an explosion (or an explosive decomposition of solid) is considered as an internal cause of overpressure leading to a loss of containment (for example catastrophic rupture or breach on the shell). In this case, the loss of containment is the critical event considered in the bow-tie.
CE3	Materials set in motion (entrainment by air)	This critical event is reserved for a potentially mobile solid, to a fragmented solid (powder, dust,..) exposed to the ambience (e.g. fragmented solid in an open storage or in conveyor belts) and occurs due to the presence of an air vector (e.g. too high ventilation,…)

	Critical events	Definition
CE4	Materials set in motion (entrainment by a liquid)	This critical event is reserved for a potentially mobile solid exposed to the ambience (e.g. fragmented solid in an open storage or in conveyor belts) and occurs due to the presence of a liquid vector (e.g. flooding, liquid escaping from an other equipment,…)
CE5	Start of fire (LPI)	This critical event corresponds to the specific reaction between an oxidising substance and a flammable or combustible substance or to the autonomous decomposition of an organic peroxide leading to a fire. This critical event concerns only substances having a risk phrase describing a *loss of physical integrity* leading to a fire. These risk phrases are R7, "May cause fire (organic peroxides)"; R8, "Contact with combustible materials may cause fire" excluding any other risk phrase. This event can also be associated with pyrotechnic substances.
CE6	Breach on the shell in vapour phase	This critical event is a hole with a given diameter on the shell in vapour phase (above the liquid level if a liquid phase exists) of an equipment, leading to a continuous release. This hole can be due to a mechanical stress due to external or internal causes, to a deterioration of mechanical properties of the structure,… This critical event includes also a breach on an equipment where a solid material is in suspension in air or in gas.
CE7	Breach on the shell in liquid phase	This critical event is a hole with a given diameter on the shell in liquid phase (under the liquid level) of an equipment, leading to a continuous release. This hole can be due to a mechanical stress due to external or internal causes, to a deterioration of mechanical properties of the structure,…
CE8	Leak from liquid pipe	This critical event is a hole with a diameter corresponding to a given percentage of the nominal diameter of the pipe. It can also be a leak from a functional opening on the pipe: flanged joints, pump seals, valves, plugs, seals,… This leak occurs on a pipe carrying a liquid substance.
CE9	Leak from gas pipe	This critical event is a hole with a diameter corresponding to a given percentage of the nominal diameter of the pipe. It can also be a leak from a functional opening on the pipe: flanged joints, pump seals, valves, plugs, seals,… This leak occurs on a pipe carrying a gaseous substance. This critical event includes also a leak on an equipment where a solid material is in suspension in air or in gas.

	Critical events	Definition
CE10	Catastrophic rupture	A catastrophic rupture is the complete failure of the equipment leading to the complete and instantaneous release of the substance. **A BLEVE is also a catastrophic rupture in particular operating conditions.** Depending on the circumstances, the catastrophic rupture can lead to overpressure generation and missiles ejection.
CE11	Vessel collapse	A vessel collapse is the complete failure of the equipment leading to the complete and instantaneous release of the substance. It is due to a **decrease of the internal pressure** in the vessel leading to the collapse of the vessel under the effect of atmospheric pressure. The vessel collapse **does not lead** to overpressure generation nor missiles ejection.
CE12	Collapse of the roof	The collapse of the roof may be due to a decrease of the internal pressure in the vessel leading to the collapse of the mobile roof under the effect of atmospheric pressure. The collapse of the roof is specially considered for atmospheric storage.

For CE6, 7, 8 and 9, concerning breaches and leaks, it will be seen later (see paragraph 2.7.3) that three sizes of breach / leak will be defined: large, medium and small. It is then important to give figures for these sizes. ARAMIS 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 5.

Table 5: 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 to 50 mm diameter Or diameter of the fitting	22 to 44 % of the pipe diameter
Small	10 mm diameter	10 % of the pipe diameter

2.6.2 ASSOCIATION OF CRITICAL EVENTS TO RELEVANT HAZARDOUS EQUIPMENT

Appendix 3 gives the description of the method used to associate critical events and relevant hazardous equipment.

In brief, it should be noted that 2 matrices are used:

- 1 matrix crossing the type of equipment and the 12 potentials critical events
- 1 matrix crossing the physical state of the substance considered and the 12 potentials critical events

As explained in appendix 3, these matrices allow, for each relevant hazardous equipment, to determine which critical events must be retained.

The result of this step is thus, for each hazardous equipment selected, to associate a list of critical events.

2.7 MIMAH Step 5: For each critical event, build a fault tree

2.7.1 STRUCTURE OF THE FAULT TREE

The general structure of the fault tree is shown in Figure 3. The fault trees were limited to five levels linked by AND or OR gates according to the following logical sequence :

> Combination 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).

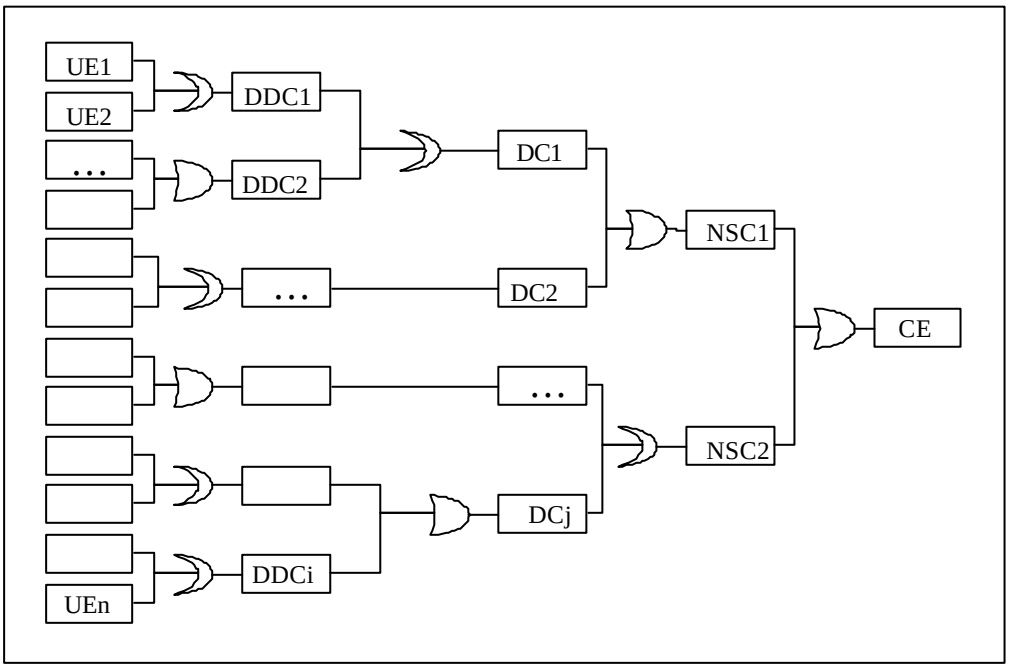

Figure 3: Structure of the fault tree

The events which constitute the fault tree, from the left to the right, are explained below:

- The **Undesirable Events** designate the deepest level of causes in the fault trees. The UE are, most of the time, generic events which concern the organisation or the human behaviour, which can always be ultimately considered as a cause of the critical event.

- The **Detailed Direct Causes** are either the events that can provoke the direct causes or, when the labelling of the direct cause is too generic, the detailed direct cause provides a precision on the exact nature of the direct cause.
- The **Direct Causes** are the immediate causes of the Necessary and Sufficient Causes (NSC). For a given NSC, the list of direct causes tends to be as most complete as possible.
- The **Necessary and Sufficient Causes** designate the immediate causes that can provoke a critical event. For a given critical event, the list of NSC is supposed to be exhaustive. This means that the critical event will occur if at least one of the NSC is fulfilled.

2.7.2 METHOD OF CONSTRUCTION OF THE FAULT TREE

MIMAH proposes 14 generic fault tree (see list in Table 6). This paragraph intends to give some information to the reader about the way the fault trees were built.

The fault trees were built following a deductive sequence, i.e. from the critical event to the undesirable event. For each event in the tree, at any level, the procedure involves the identification of its potential immediate causes taking into account the functions or elements usually present in the system or its surroundings.

The first step led to the identification of **necessary and/or sufficient causes** of the critical event. Only technical aspects were considered at this stage. For example, the immediate conditions for thermal decomposition to occur is that a thermal sensitive material is used and that it is put in presence of some heat source.

The second step involves the identification of the causes that could lead to the NSCs. These are called **direct causes**. Again a technical approach of the phenomena is used. The labelling of the direct causes is very generic. The causes considered at this level are, for most of them, the causes usually considered in the accident databases. Direct causes such as erosion, corrosion, overpressure are considered here.

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 as much as possible very generic causes making the link with human behaviour and organisational aspects. Human error is a potential cause for a very large variety of events. The human error is never a direct cause of a rupture but rather of its direct causes or even detailed direct causes. For example a human error can be at the origin of an overfilling leading to an overpressure which creates too large a stress on the structure which breaks. For these reasons we have tried to make human error appear only in the last level (**undesirable event**) and to reserve the previous levels to the technical consequences of human error.

Human error can happen at different steps of the plant's life cycle : conception, manufacturing, building, maintaining, operating. Human error can also take different aspects : unconscious error, disobedience to rules or procedures, malicious intervention.

2.7.3 GENERIC FAULT TREES

MIMAH proposes 14 generic fault trees. They can be found in details in appendix 4. Table 6 presents which fault tree is associated with which critical event.

Table 6: List of generic fault tree for each critical event

Nr CE	Critical event	Generic fault tree (FT)
CE1	Decomposition	FT Chemical decomposition FT Decomposition tied to a punctual ignition source FT Thermal decomposition
CE2	Explosion	FT Explosion of an explosive material FT Explosion (violent reaction)
CE3	Materials set in motion (entrainment by air)	FT Materials set in motion (entrainment by air)
CE4	Materials set in motion (entrainment by a liquid)	FT Materials set in motion (entrainment by a liquid)
CE5	Start of fire (LPI)	FT Start of fire (Loss of Physical Integrity)
CE6	Breach on the shell in vapour phase	FT Large breach on shell or leak from pipe FT Medium breach on shell or leak from pipe FT Small breach on shell or leak from pipe
CE7	Breach on the shell in liquid phase	FT Large breach on shell or leak from pipe FT Medium breach on shell or leak from pipe FT Small breach on shell or leak from pipe
CE8	Leak from liquid pipe	FT Large breach on shell or leak from pipe FT Medium breach on shell or leak from pipe FT Small breach on shell or leak from pipe
CE9	Leak from gas pipe	FT Large breach on shell or leak from pipe FT Medium breach on shell or leak from pipe FT Small breach on shell or leak from pipe
CE10	Catastrophic rupture	FT Catastrophic rupture
CE11	Vessel collapse	FT Vessel collapse
CE12	Collapse of the roof	FT Collapse of the roof

Remarks:

Some critical events have several possible fault trees.

- For the CE1 (Decomposition): the 3 fault trees must be built separately. However, the event tree will be the same for the 3 fault trees.
- For the CE2 (Explosion): the 2 fault trees must be built separately. However, the event tree will be the same for the 2 fault trees.
- For the CE6, 7, 8 and 9 (Breaches and Leaks), the 3 fault trees must be built separately. The generic event trees are the same for CE6 and CE9 (release in gaseous phase) and for CE7 and CE8 (release in liquid phase), but must also be studied separately because the consequences of a small, medium or large breach or leak will not be identical.

2.7.4 FAULT TREES ASSOCIATED TO IDENTIFIED CRITICAL EVENTS

The objective of the fifth step is, for each critical event associated with a selected equipment, to built a fault tree. With the help of Table 6, the reader can choose which fault tree must be considered according to the critical event studied. If several fault trees are mentioned for a single critical event, each fault tree must be taken into account.

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 for a given equipment. They can be modified according to the design, the operating conditions, the actual external conditions of the equipment. According to these conditions, some causes of fault tree may be removed or added and an agreement may be obtained on some causes.

Moreover, even if the list of direct causes and necessary and sufficient causes is, as a whole, exhaustive, it is not necessarily the case for the list of detailed direct causes or undesirable events due to the large variety of existing equipment design and of operating conditions. **So, some other causes, like "loss of utility", "Reverse flow", or causes more specific to process or to equipment can be added in some cases.**

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. Some causes can be removed or added. Moreover, some safety barriers will be maybe not presented or activated during these phases or there are more manual operating procedures than in operating phase, which can be more automated.

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). Besides, the HAZOP method seems a complementary method to the proposed generic fault trees in order to identify same possible causes, especially for process equipment (like reactor, distillation column, unit of process). It is also possible to use the risk analysis already made on the site.

In brief, the reader should make the following actions:

- for each critical event, consider one or more generic fault tree(s) according to the information given in Table 6;
- each generic fault tree should be considered as a check list of possible causes and could be modified (add or remove causes) to become adapted to actual characteristics of the equipment;
- if other risk assessment methods give additional causes, these have to be included in the fault tree.

2.8 MIMAH Step 6: For each critical event, build an event tree

2.8.1 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 Figure 4.

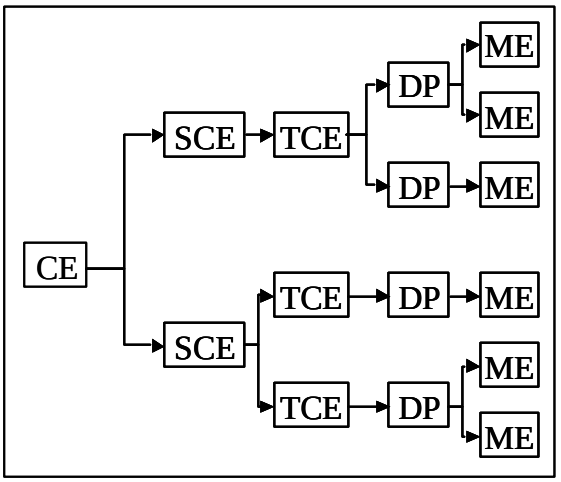

Figure 4: Structure of the event tree

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 leads 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 the following ones:

- ✓ Thermal radiation
- ✓ Overpressure
- ✓ Missiles
- ✓ Toxic effects (on the humans or on the environment)

2.8.2 METHOD OF CONSTRUCTION OF THE EVENT TREE

The method for the construction of event trees is fully explained in appendix 5. 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.

For the critical events for which several fault trees have been generated (see Table 6), only one event tree will be built per critical event.

A schematic overview of the method for the building of the event trees is shown in Figure 5.

It should also be noted that an excel file is available on the ARAMIS web site, including a program which allows to automatically generate the event trees.

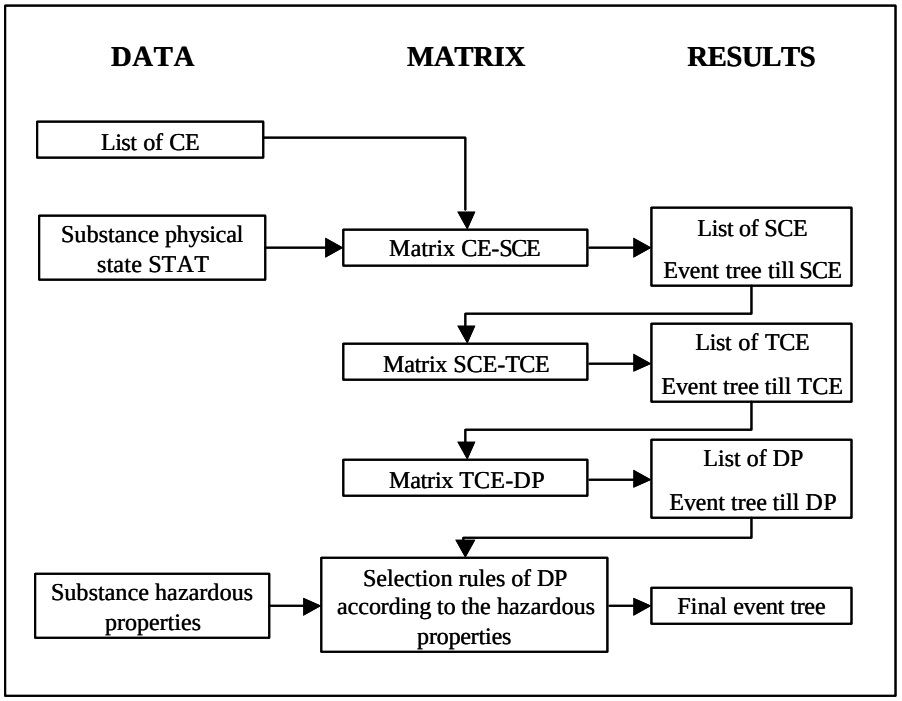

Figure 5: Summary of the steps followed for the construction of the event trees

2.8.3 REMARKS

- The events trees obtained can be modified if some events are not possible for the given equipment and for the actual external/internal conditions. For example, a jetfire is not realistic if the pressure inside the equipment is very near the atmospheric pressure.
- AND and OR gates are implicitly present in event trees but are not drawn at this stage. This will be explained in paragraph 3.11.2, page 44.

2.9 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, according to the scheme of a bow-tie shown in Figure 1, page 6.

For each selected equipment, the number of bow-ties is equal to the number of fault trees developed. This number can be higher than the number of critical events because, for some critical events, more than one fault tree has to be built.

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 - Construction of bowties with the safety barriers)

3.1 Introduction (objectives and main steps of MIRAS)

The objective of MIRAS is to **choose Reference Accident Scenarios** 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**, which in turn will be compared with the **vulnerability** of the surroundings of the plant.

MIRAS 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 possible consequences of the accident

MIRAS will follow 8 steps. The whole development has to be performed for each bow-tie built with MIMAH. The succession of the steps is shown in Figure 6

- Step 1: Collect needed data
- Step 2: Make a choice between step 3 or step 4
- Step 3: Calculate the frequency of the critical event by means of the analysis of the fault tree
    - Step 3.A: Estimate initiating events frequencies (or probabilities)
    - Step 3.B: Identify safety functions and safety barriers on the fault tree
    - Step 3.C: Assessment of the performances of safety barriers
    - Step 3.D: Calculate the frequency of the critical event
- or Step 4: Estimate the frequency of the critical event by means of generic critical events frequencies
- Step 5: Calculate the frequencies of Dangerous Phenomena
- Step 6: Estimate the class of consequences of Dangerous Phenomena
- Step 7: Use the risk matrix to select Reference Accident Scenarios
- Step 8: Prepare information for the calculation of the Severity

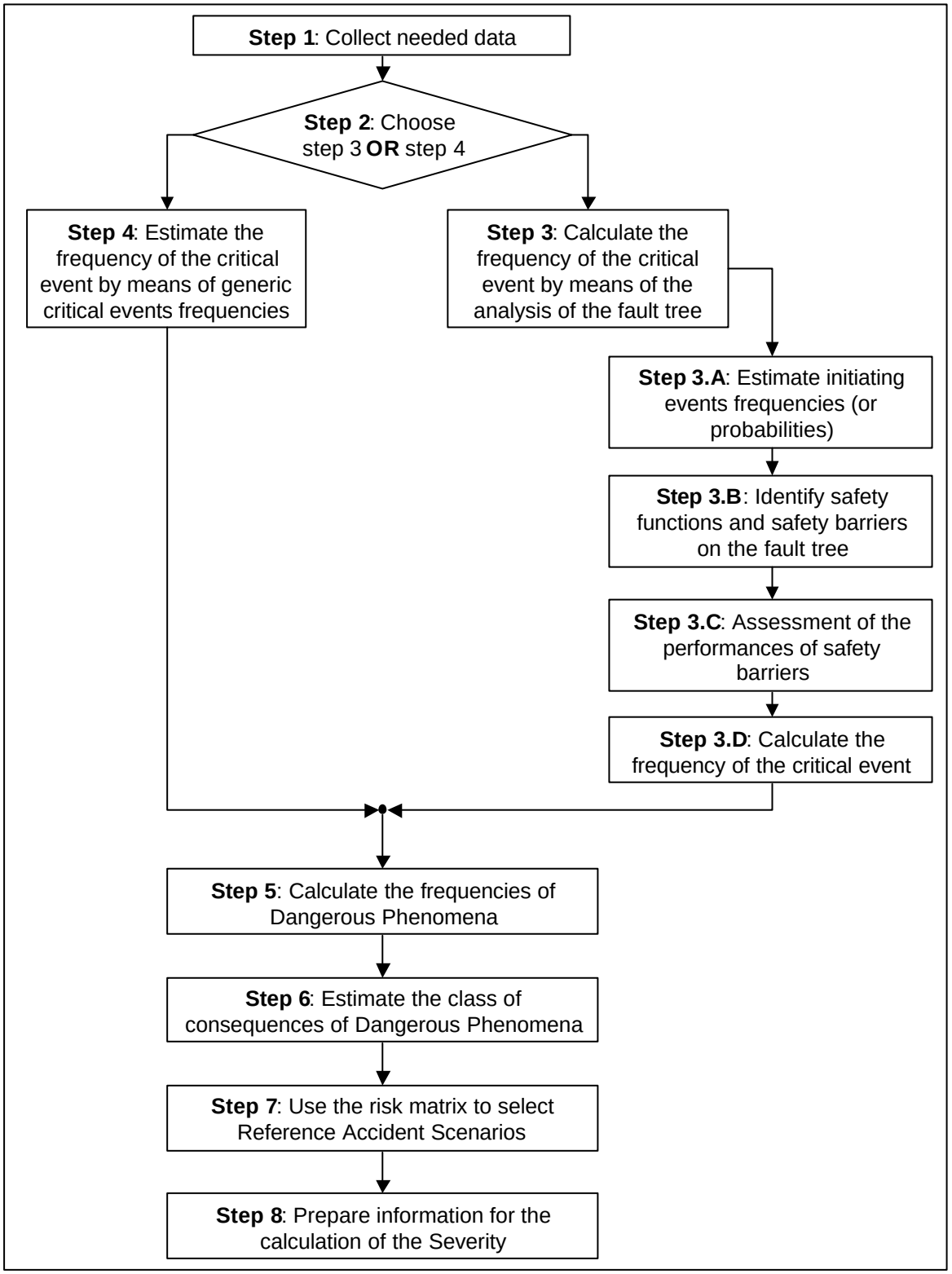

Figure 6: General overview of the steps of MIRAS (steps to be applied for each bow-tie built with MIMAH)

3.2 General overview of MIRAS

The objective of MIRAS is to obtain, for a given plant, Reference Accident Scenarios (RAS) which will be modelled to compute the Severity characterising the plant. The RAS will be chosen on the basis of a risk matrix crossing the level of consequences of the Dangerous Phenomena and their frequency per year. According to its position in the matrix, each Dangerous Phenomenon will be retained or not as a RAS.

To achieve this goal, its is necessary, for each bow-tie built with MIMAH, to:

- obtain the frequency per year of the critical event, either by an analysis of the fault tree or by using generic critical events frequencies;
- classify the possible consequences of the Dangerous Phenomena identified in the event tree;
- take into account the safety systems, the safety management and their effects, in terms of frequencies of accidents and also in terms of level of consequence;
- develop the event tree built with MIMAH to take into account the safety systems and the "transmission" probabilities (e.g. the probabilities of ignition).

This goal will be reached by means of the 8 steps presented in paragraph 3.1 and discussed below.

3.3 MIRAS Step 1: Collect needed data

Additional data will be required all along the MIRAS steps. The list of information needed is given in Table 7.

Needed data are linked with the step during which they will be used. The reader can choose to collect all the data at the same time, or to collect data progressively when they are needed.

Table 7: Data needed for the MIRAS part

Step	Description of data needed
Step 1: Collect needed data	See below
Step 2: Make a choice between step 3 or step 4	No additional data

Step	Description of data needed
Step 3: Calculate the frequency of the critical event by means of the analysis of the fault tree	A meeting with industrialists concerned could be fruitful to achieve this step. • Fault trees built during the MIMAH part • Initiating events frequencies / probabilities • Safety barriers on the fault tree side; to be identified on the basis of the check lists of appendix 8, with the help of Process Instrumentation Diagrams, with the results of risk assessment previously performed (like HAZOP) • Information for the evaluation of performance of safety barriers: architecture of the barriers, probability of failure on demand, response time, etc
Step 4: Estimate the frequency of the critical event by means of generic critical events frequencies	No additional data
Step 5: Calculate the frequencies of Dangerous Phenomena	A meeting with industrialists concerned could be fruitful to achieve this step. • Event trees built during the MIMAH part • Ignition probabilities • Safety barriers on the event tree side; to be identified on the basis of the check lists of appendix 8, with the help of Process Instrumentation Diagrams, with the results of risk assessment previously performed (like HAZOP) • Information for the evaluation of performance of safety barriers: architecture of the barriers, probability of failure on demand, response time, etc
Step 6: Estimate the class of consequences of Dangerous Phenomena	No additional data
Step 7: Use the risk matrix to choose Reference Accident Scenarios	No additional data
Step 8: Prepare information for the calculation of the Severity	• Characteristics of equipment for which one (or several) Reference Accident Scenarios has been retained (for example dimensions of the vessel, size of the bund, … see the complete list in paragraph 3.14) • Wind rose and meteorological conditions • Description of the site surroundings (populated area including schools, hospitals, …)

3.4 MIRAS Step 2: Make a choice between step 3 or step 4

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

The frequency of the critical event can be obtained in two ways:

1. The first choice is to make a complete analysis of the fault tree, starting from the frequencies (or probabilities) of the initiating events and 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.

2. The alternative way is to estimate directly the frequency of the critical event with the help of data given in appendix 10. 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). With the second way, the quality of the prevention is no more considered, but the time required for the analysis is shorter.

The reader has then to make a choice between step 3 (paragraphs 3.5 to 3.9) or step 4 (paragraph 3.10).

3.5 MIRAS Step 3: Calculate the frequency of the critical event by means of the analysis of the fault tree

If the reader chooses this way, he has to follow 4 steps. 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 will be identified. Thirdly, the performance of these safety barriers will be assessed. And finally, all these parameters will be taken into account to calculate the frequency of the critical event.

3.6 MIRAS Step 3.A: Estimate initiating events frequencies (or probabilities)

The objective of this step is to provide frequency (probability) figures to be placed at the beginning of the fault tree, for the bow-tie studied.

The initiating events are defined as the first causes upstream of each branch leading to the critical event in the fault tree (on the left end of the bowtie). The initiating event can thus be an undesirable event, a detailed direct cause, etc … according to the level of development of the fault tree. The initiating event is the one placed the most on the left.

Appendix 7 gives an overview of data available for the frequencies (or probabilities) of initiating events. The reader should refer to this appendix for precise data and explanations, but some remarks should be brought to the fore here.

- There is obviously a lack of data in this field. Appendix 7 tries to give an overview and a synthesis of published data, but it appears 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 8. Figures estimated could then be compared with published frequencies summarized in appendix 7.

Table 8: 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	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 $< F \leq 10^{-3}$ /year	F_3
Low 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 $< F \leq 10^{-2}$ /year	F_2
Possible – High frequency May happen. Has already happened in the site (once during 10 years)	10^{-2} /year $< F \leq 10^{-1}$ /year	F_1
Likely – Very high frequency Has already happened several times in the site	$F \geq 10^{-1}$/year	F_0

- In the fault trees, it appears that a great number of initiating events are related to human error. It seems then important to draw the attention of the reader on the considerations developed in appendix 7 on this topic.

These frequencies will be expressed in frequency per year. Even if other units could be used, the unit "year^{-1}" will be the more convenient for the following steps.

Result of this step:

After this step, the estimated frequencies (year^{-1}) (or probabilities) of any initiating events have to be indicated on the bow-tie studied.

3.7 MIRAS Step 3.B: Identify safety functions and safety barriers on the fault tree

The objective of this step is to identify the safety systems which have an influence on the possibility of occurrence of the critical events. The concrete realisation of this objective is explained in paragraph 3.7.5. Before that, the concept of **safety functions and safety barriers** has to be introduced. Definitions are provided and a typology of safety functions and barriers is defined.

With these tools, the reader will be able to identify the safety functions and barriers related to the fault tree being analysed, and will be able to place these barriers at the right place in the fault tree.

A check-list, given in appendix 8, helps the reader to identify the functions and barriers associated with each type of event which can be found in the generic fault and event trees.

This approach has many common points with the LOPA method (Layer Of Protection Analysis, see reference 9).

3.7.1 DEFINITION OF A 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 defined in paragraph 3.7.3.

In the fault tree, the different possible actions of safety functions are to avoid or prevent the occurrence of an event or 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, prevent or 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 the consequences of dangerous phenomena and mitigate their effects.

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

3.7.2 TYPOLOGY OF SAFETY FUNCTIONS

The generic safety functions (as well for fault trees as for event trees) can be expressed by actions to be achieved. Four main verbs of action are defined (with eventually some synonyms but obviously other synonyms may be used). Definitions for these four safety functions are presented in Table 9. It should be noted that, in these definitions, an event can be each kind of event encountered in the bow-tie (i.e. undesirable event, detailed direct cause, direct cause, necessary and sufficient cause, critical event, secondary critical event, tertiary critical event, dangerous phenomenon, major event).

It should be noted that, for some functions ("to control" and "to limit"), a **detection** action is often included in the global safety function.

Table 9: 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 which 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 vaporization of a pool. 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 event tree, to control = to get the event under control and return to a "safe" state.**	In the fault tree, to control the overfilling of a liquid storage. In the event tree, to control the pool dispersion.

Safety function	Definition	Example
	"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. In the event tree, to limit the duration of a leak, to limit liquid vaporisation.
	"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.	

3.7.3 DEFINITION 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,…), a 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.

3.7.4 TYPOLOGY OF SAFETY BARRIERS

Four main categories of safety barriers are defined in order to make easier the assessment of the influence of safety management system on these barriers.

1. **Passive barriers**: barriers always in functioning (permanent), no need to human actions, energy sources and information sources. Passive barriers may be physical barriers (retention bund, wall,…), permanent barriers (corrosion prevention systems) or inherently safe design.

2. **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.

3. **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.

4. **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 prohibited areas, opening labelled pipes, refraining from smoking,…)

According to these 4 main categories of safety barriers, a typology of safety barriers is defined in Table 10, based on the components (hardware, software, and human action) involved in the sequence *"detection - diagnosis - action"*.

This typology will be used to quantify the influence of the safety management on the quality of the barriers. The reader should then refer to the report dealing with the assessment of the safety management system for further details.

Table 10: 11 types of safety barriers

Category of barriers	N	Barrier	Examples	Detect	Diagnose/ activate	Act
PASSIVE	**1**	*Permanent – passive –* MORT control	*Pipe/hose wall, anti-corrosion paint, tank support, floating tank lid, viewing port in vessel*	none	none	Hardware
	2	*Permanent – passive –* MORT barrier	*Bund, dyke, drainage sump, railing, fence, blast wall, lightning conductor, bursting disc*	none	None	Hardware

Category of barriers	N	Barrier	Examples	Detect	Diagnose/ activate	Act
	3	*Temporary – passive* Put in place (and removed) by person	*Barriers round repair work, blind flange over open pipe, helmet/gloves/safety shoes/goggles, inhibitor in mixture*	none	None (human must put them in place)	Hardware
	4	*Permanent – active*	*Active corrosion protection, heating/cooling system, ventilation, explosion venting, inerting system*	none	none (may need activation by operator for certain process phase)	Hardware
ACTIVATED	**5**	*Activated – hardware on demand –* MORT barrier or control	*Pressure relief valve, interlock with "hard" logic, sprinkler installation, p/t/level control*	hardware	hardware	Hardware
	6	*Activated – automated*	*Programmable automated device, control system or shutdown system*	hardware	software	Hardware
	7	*Activated – manual* Human action triggered by active hardware detection	*Manual shutdown or adjustment in response to instrument reading or alarm, evacuation donning breathing apparatus or calling fire brigade on alarm, action triggered by remote camera, drain valve, close/open (correct) valve*	hardware	human	human/ remote control
	8	*Activated – assisted* Software presents diagnosis to the operator	*Using an expert system*	hardware	software - human	human/remote control

Category of barriers	N	Barrier	Examples	Detect	Diagnose/ activate	Act
SYMBOLIC	**9**	*Activated – warned* Human action based on passive warning	*Donning ppe in danger area, refraining from smoking, keeping within white lines, opening labelled pipe, keeping out of prohibited areas*	hardware	human	human
HUMAN	**10**	*Activated – procedural* Observation of local conditions not using instruments	*(Correctly) follow start up/shutdown/batch process procedure, adjust setting of hardware, warn others to act or evacuate, (un)couple tanker from storage, empty & purge line before opening, drive tanker, lay down water curtain*	human	human	human/ remote control
	11	*Activated – emergency* Ad-hoc observation of derivation /improvisation of response	*Response to unexpected emergency, improvised jury-rig during maintenance, fight fire*	human	human	human/ remote control

3.7.5 IDENTIFICATION OF SAFETY BARRIERS ON THE FAULT TREE ANALYSED

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 barriers identified must be classified according the typology shown in Table 10, in order to be able later to take into account the quality of the safety management ("operational" level of confidence, see paragraph 3.8.2).

A complete example is shown in appendix 15. A shorter one (not on a full fault tree) is shown in Figure 7. It should be noted that, to simplify the drawing, the OR gates are not represented.

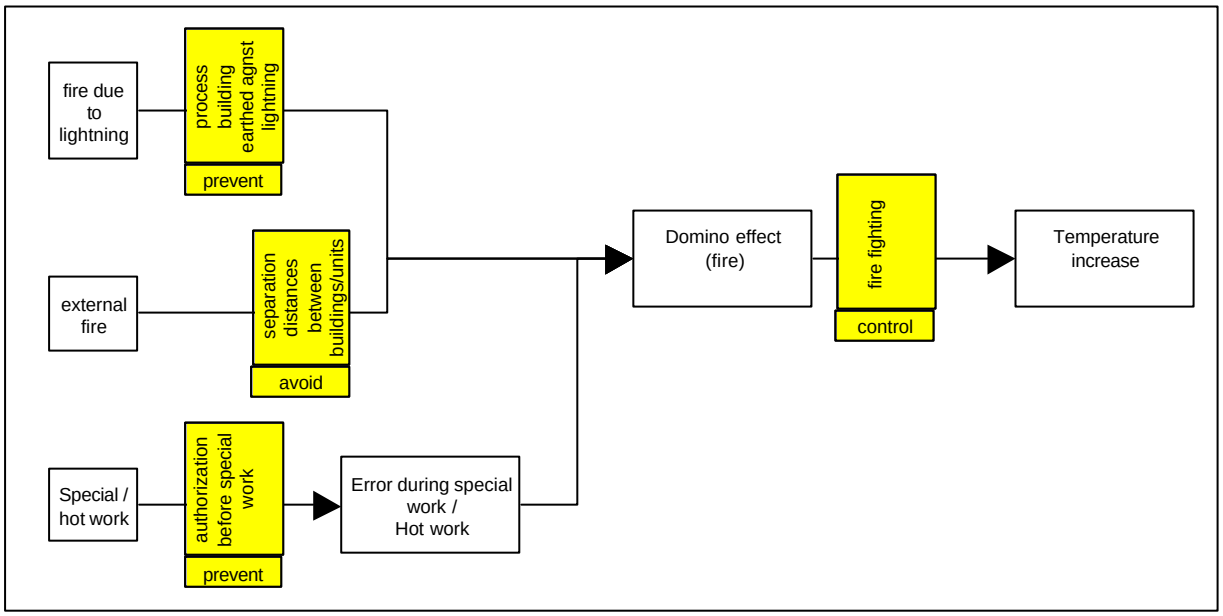

Figure 7: Short example of barriers placed on a branch of a fault tree

3.7.6 REMARKS

- The barriers for control and for limitation will be often associated to a detection system, which is an integral part of the barrier.

- When the safety barriers are not yet implemented on the equipment (for example in a design or a modification phase), it is also possible to start from safety functions in order to identify which safety barriers could be added to the system. An other tool, called the "risk graph" is also helpful to determine the number of barriers necessary to efficiently place under control a possible cause of accident. Further details are given in chapter 4, devoted to the possible use of the ARAMIS method for the identification of scenarios.

- A checklist of possible safety functions and safety barriers upstream and downstream of each event of the bow-ties has been built. This checklist can be found in appendix 8. With the help of this checklist of functions and barriers, it is possible to compare them to actual functions and

barriers implemented in a plant. They can also be used to define what should be implemented on a new plant or to improve an unsatisfactory safety level in an existing plant.

3.8 MIRAS Step 3.C: Assessment of the performances of safety barriers

3.8.1 DEFINITION OF THE PERFORMANCE OF A SAFETY BARRIER

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.

The performance of a safety barrier is defined according to three parameters:

- Its **level of confidence** (LC) linked to its probability of failure on demand (PFD). The **level of confidence of a safety barrier** is 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.
- Its adequate capacity to take the required action (specific size or volume, physical strength, etc.) or **effectiveness** (E). 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%.
- Its **response time** (RT). 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 way to assess these parameters is explained in details in appendix 9.

3.8.2 "DESIGN" AND "OPERATIONAL" LEVEL OF CONFIDENCE - LINK WITH THE SAFETY MANAGEMENT SYSTEM

In a first step, the level of confidence assessed with the help of instruction given in appendix 8 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 or probability of failure on demand.

But the performance of the safety barrier could decrease when time is going. 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 performances of the safety barriers. The tools for the management audit are described in an other ARAMIS document. 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.

During the management audit, several criteria will be studied and weights will be allocated at each criterion according to the 11 types of safety barriers (see paragraph 3.7.4). The weights associated to evaluation criteria will be different depending on whether it is a passive or active barrier, or an human one.

Details about the modifications of the performances of the safety barriers according to the quality of the safety management system are available in the ARAMIS report related to the safety management system.

3.8.3 OUTPUT OF THIS STEP

At the end of this step, additional information will have been collected for the safety barriers:

- for each safety barrier, it will have been decided if this safety barrier meet the minimum requirements expressed in appendix 9. If yes, the barrier is relevant and can be placed on the bow-tie, but will not be taken into consideration if it should not be the case;
- for the relevant safety barriers, the performances are assessed, that means that the reader has evaluated the level of confidence, the response time and the effectiveness of the safety barrier.

3.9 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. Guidelines for Chemical Process Quantitative Risk Analysis, ref. 12). Some basic rules are summarised in the next paragraph.

3.9.1 BASIC RULES FOR THE ANALYSIS OF THE FAULT TREE

The gate-by-gate method starts with the initiating events of the fault tree and proceeds upward toward the critical event. All inputs to a gate must be evaluated before calculating the gate output. All the bottom gates must be computed before proceeding the next higher level.

The mathematical relationships used in the gate-to-gate approach are summarised in Table 11.

Table 11: Rules for gate-by-gate fault tree calculation

(ref. 12, F = Frequency, P = Probability)

Gate	Input pairing	Calculation for output	Units
OR	P_A OR P_B	P(A OR B) $= 1 - (1-P_A)*(1-P_B)$ $= P_A + P_B - P_A*P_B$ $\cong P_A + P_B$	
	F_A OR F_B	F(A OR B) $= F_A + F_B$	y^{-1}
	P_A OR F_B	Not permitted	
AND	P_A AND P_B	P(A AND B) $= P_A*P_B$	
	F_A AND F_B	Not permitted, change to F_A and P_B	
	F_A AND P_B	F(A AND B) $= F_A*P_B$	y^{-1}

Remarks

- When a OR gate has several inputs, they are added (the approximation due to omitting coproduct terms is often negligible for small probabilities and is conservative)
- Several probability terms, but only one frequency, may be brought into an AND gate (eventually, some frequencies must be converted into probabilities).

A special attention should be paid to common-cause failures which may affect various events in the fault tree. If a common-cause failure appears in two branches of a fault tree joined by a AND gate, the final result of the gate-by-gate method could be incorrect. The common-cause failure (power failure, for instance) should be taken into account only once !

The ways to take into account the effects of safety barriers is presented in the following paragraphs.

3.9.2 TAKING INTO ACCOUNT THE SAFETY BARRIERS OF THE FAULT TREE

3.9.2.1 "Avoid" barriers

This kind of barrier implies that the event located just downstream is supposed impossible. The corresponding branch will thus not influence the critical event frequency anymore.

For example, Figure 8 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 Figure 8.

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 Figure 8 will always be up-to-date and the hazard due to the unloading unit will always be kept in mind. Otherwise, the cause deleted could be forgotten later if the barrier is no more relevant.

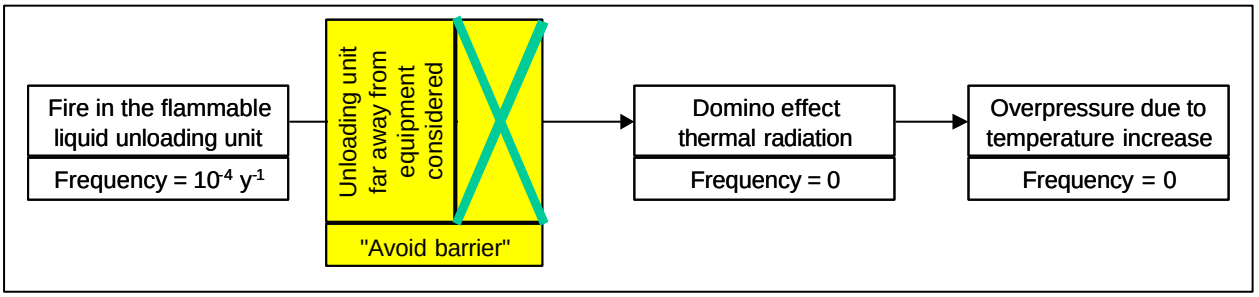

Figure 8: "Avoid" barrier in the fault tree

3.9.2.2 "Prevent" or control" barriers

For these 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.

An example is shown in Figure 9 where the complete drawing of the tree is shown. 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 is stopped and thus the branch can be deleted.

The practical drawing (Figure 10) 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^n after a barrier having a level of confidence equal to n.

In these drawings (Figure 9 and Figure 10), 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.

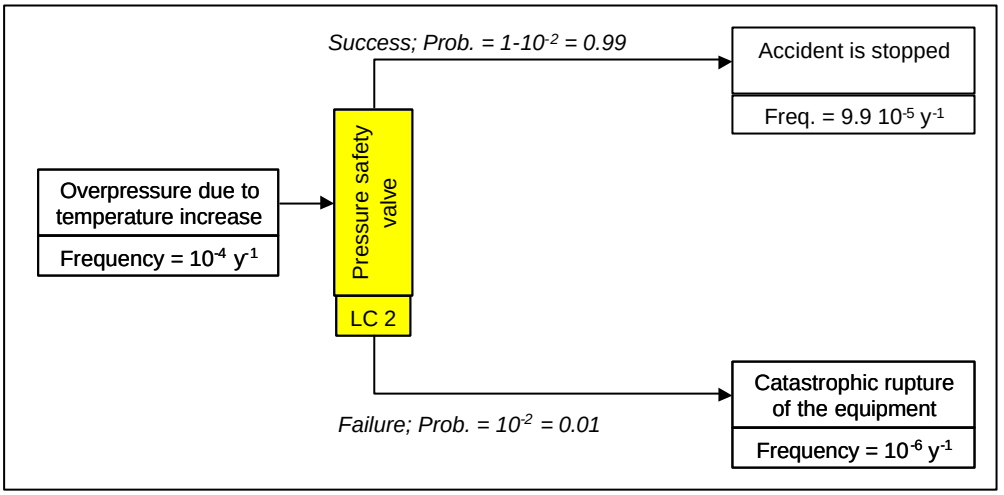

Figure 9: "Prevent" or "control" barriers in the event tree – complete drawing (example)

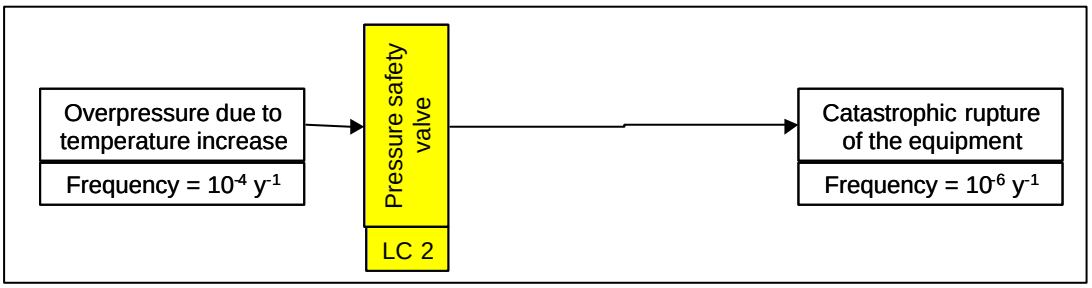

Figure 10: "Prevent" or "control" barriers in the event tree – simple drawing (example)

3.9.2.3 Combinations of several safety barriers

In principle, the level of confidence of independent barriers acting on the same event are additive. That means that, if we have a barrier with LC = m and another barrier with LC = n, the global reduction factor for the downstream event is equal to $10^{(m + n)}$.

Practically, this is true but has to be applied carefully. When combining safety barriers, the reader should especially pay attention to the following points:

- Is there a common failure mode for the barriers ? If yes, they cannot be considered as fully independent.

- Is there a common subsystem for two different barriers ? For example, a gas detector could serve to activate an isolating valve, and the same detector could also activate the sprinkler system. If this subsystem (gas detector) has a LC = 1, then the isolation system has a LC1 at maximum, the sprinkler system has a LC1 at maximum. The combination of the two safety systems has a LC1 at maximum and not a LC2, because the gas detector is common to both safety barriers.
- The architecture of the barriers should be studied deeply in order to identify common subsystems (as shown above), but also to examine redundancy. In the same example, the sprinkler could be also activated by a flame detector, this with a LC1. In this case, it can be considered that the sprinkler system is independent from the isolation system and thus when combining the two safety barriers a global LC2 is obtained.

  The representation of the different subsystems (detection, transmission, action parts) is interesting to assess quickly the performance of the safety barriers, but a weak point could be missed (for example an electro-valve common to several barriers).

3.9.2.4 Remark

A complete example of fault tree with safety barriers, and with the calculation of the frequency of the critical event is developed in appendix 15.

3.9.3 OUTPUT OF THIS STEP

The output of this step is the frequency (per year) of the critical event, taking into account the safety barriers on the fault tree.

If the frequency of the critical event with the safety barriers is lower than **10^{-7}/year**, there is no need to apply the following steps. The frequency of the critical event is low enough. The major accident scenario is thus enough controlled on the fault tree side and will not lead to a reference accident scenario.

3.10 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), an other possibility is to evaluate it by means of generic critical event frequencies.

Appendix 10 gives the results of a bibliographic review of published data on this subject. At the end of the appendix, a table summarises the data collected, and proposes values or ranges of values for the different critical event frequencies, depending on the kind of equipment considered.

The frequencies given in appendix 10 have a GENERIC character; the number of safety barriers included in these figures, the age of the equipment and the state of the art at the time of failure are not known. The generic frequencies 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.

3.11 MIRAS Step 5: Calculate the frequencies of Dangerous Phenomena

3.11.1 INTRODUCTION

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, some basic rules for the calculation of frequencies in the event tree will be reminded. In a second step, the transmission probabilities in the tree will be discussed. Finally, during the third step, safety barriers related to the event tree side will be taken into account, both in terms of consequences and frequency of dangerous phenomena.

3.11.2 BASIC RULES FOR THE CALCULATION OF FREQUENCIES IN THE EVENT TREE – AND AND OR GATES

In the generic event trees built with the MIMAH methodology, there is no AND / OR gates explicitly drawn. In fact, these gates are implicitly included in the event trees.

AND gates are located between an event and its simultaneous consequences (for example a breach on a two-phase storage, under the liquid level, has two consequences occurring simultaneously – a two-phase jet and a pool formation). These outcomes are linked by a AND gate.

If the events are tied by an "AND" gate, the frequency upstream the "AND" gate is transmitted to all the branches downstream.

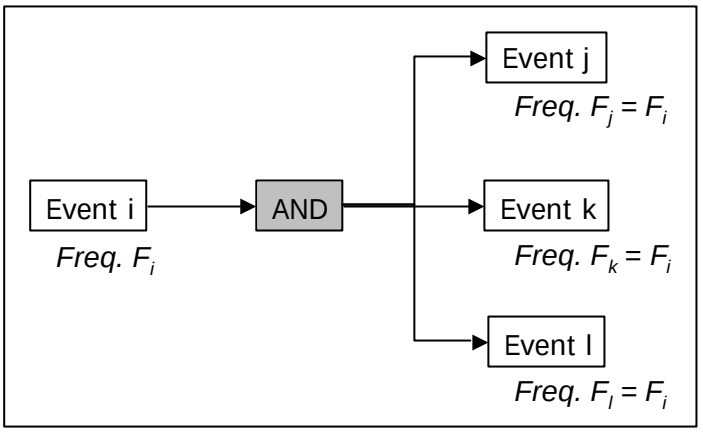

Figure 11: "AND" gate

OR gates appear downstream an event if one of the consequent events may occur and the others not. For example, if we consider the pool formation, a direct ignition can occur and we have then the "pool ignited" phenomenon, and in the other case we have the dispersion of the gas.

Events linked by a OR gate are mutually exclusive.

The frequency of each event downstream a OR gate may be determined by multiplying the upstream event frequency by the "transmission" (conditional) probability along the path leading to that outcome. Thus the probabilities associated with each branch must sum to 1.

For instance, if there are only two downstream events, the transmission probability of one branch may be P_1 and the transmission probability of the other branch, P_2, is equal to $1-P_1$. This is illustrated in Figure 12.

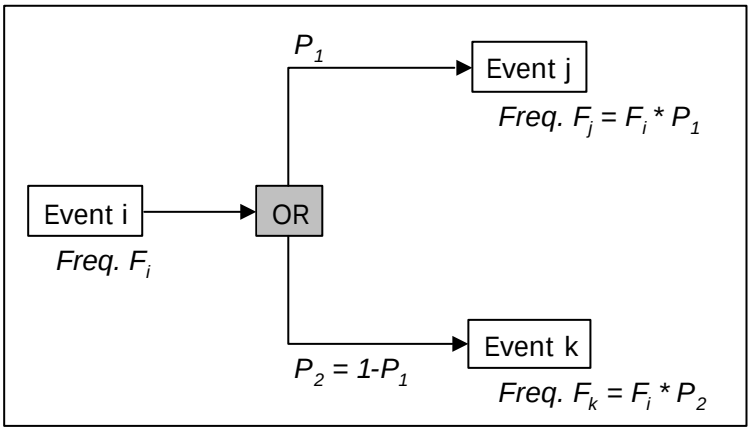

Figure 12: "OR" gate

Appendix 11 gives detailed information about these gates. Moreover, generic trees built with MIMAH for the different critical events and the different physical states of substances are detailed, and gates are explicitly indicated.

3.11.3 EVALUATION OF THE TRANSMISSION PROBABILITIES IN THE EVENT TREES (RAIN-OUT, IGNITION PROBABILITIES, PROBABILITY OF VCE/FLASHFIRE)

When OR gates appear in the event tree, figures for the transmission probabilities linked with these gates must be assessed. Having a look in all the generic event trees, it should be noted that different situations may arise:

- The **probability of rain-out**, which is partly tied to the probability that a jet is turned toward an obstacle. The position of the leak on the equipment, the wind direction, the presence of obstacles may influence this probability.
- The **probability of immediate ignition**, which depends on the flammability of the substance, the source term, the presence of ignition sources around the equipment, some safety barriers which prevent the ignition (explosion proof area,…), …
- The **probability of delayed ignition**, which depends on the flammability of the substance, the source term, the direction in which the cloud disperses, the presence of ignition sources and the type of ignition sources inside the flammability limits of the cloud (function of meteorological conditions), some safety barriers which prevent the ignition (explosion proof area,…),…
- The **probability of VCE**, which depends on the obstruction of site in the direction in which the cloud will be dispersed. This probability is higher for a zone with strong obstruction.

As the probabilities of ignition and the probability of VCE depends on a lot of parameters, these parameters and these probabilities should be discussed with the industrialists on site. For a first approximation, the reader should take conservative values for the delayed ignition and the probability of VCE which depend on the wind rose and meteorological conditions (stability class, wind velocity,..).

To help the reader, some values of probabilities are given in appendix 12.

3.11.4 INFLUENCE OF SAFETY BARRIERS IN THE EVENT TREE

3.11.4.1 Overview

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 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 event. If it controls or limits this event, it has to be placed downstream.

This identification can be made with the industrialists (safety officers, operators, …), with the help of "process and instrumentation diagrams" and "flow diagrams" or with any other existing documentation. Appendix 8 gives a check-list of safety functions and barriers on all the events of the bow-tie.

The reader must then **assess the performance of the safety barriers** identified. The procedure is also the same as for the barriers in the fault tree. To be considered as relevant, a barrier must meet the minimum requirements expressed in appendix 9. Then, the level of confidence, the effectiveness and the response time have to be evaluated.

The barriers identified must be classified according the typology shown in Table 10, in order to be able later to take into account the quality of the safety management. This will be made by modifying the design level of confidence of a barrier due to the quality of the safety management system, to obtain an **"operational" level of confidence** (see paragraph 3.8.2).

Depending on the type of barrier (prevention, control, limitation), the method to **take this barrier into account in the event tree** will be different. Explanations are given in the following paragraphs.

3.11.4.2 "Prevent" barrier

In the event tree, the prevention barriers are mainly related to the probability of ignition. They do not have to be placed directly in the trees, but serve qualitatively to evaluate the probability of ignition. Further information are given in appendix 12.

3.11.4.3 "Control" barrier

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 Figure 13, for two independent control barriers.

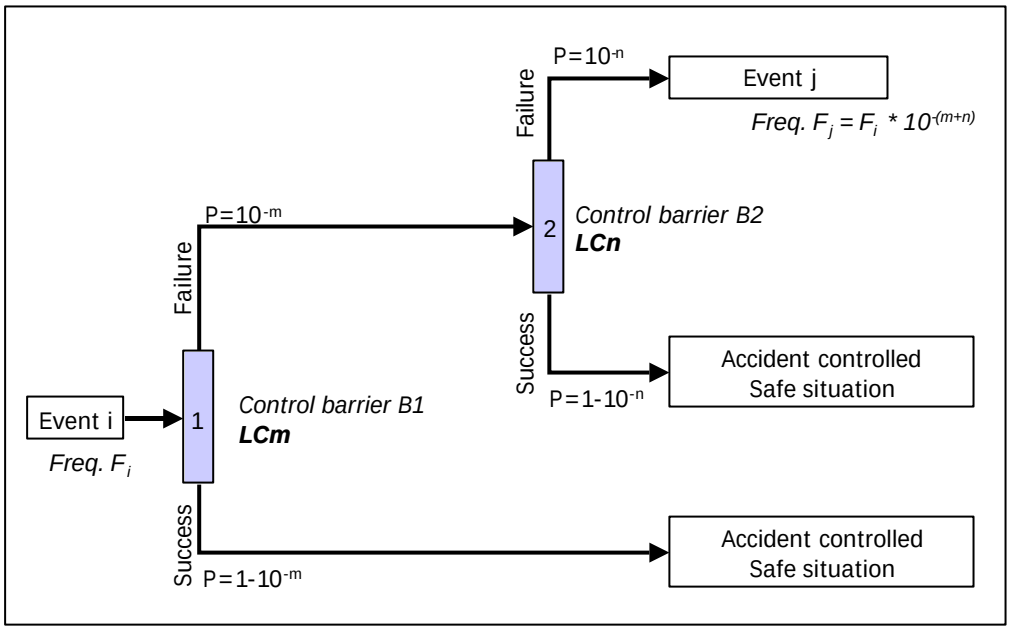

Figure 13: "Control" barriers – influence on the calculation of frequencies of events in term of level of confidence

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).

3.11.4.4 "Limit" barrier

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 vaporization 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 different dangerous phenomena, one with less severe consequence but a higher frequency, and the other one with more severe consequence but a lower frequency. The frequencies calculation is linked with the level of confidence of the safety barrier.

It is worthwhile to precise the different kind of dangerous phenomena which can be obtained in event trees influenced with "limit" safety barriers.

- 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)
- a **Dangerous Phenomenon with "limited effects"** means that a limiting barrier acts in the event tree, but not directly after the critical event (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 both kinds of barriers are present and are successful.

These details will be useful when the consequences of the dangerous phenomena will be evaluated (see paragraph 3.12).

Examples

For example, in the case of a leak on a liquid pipe, a detection of the leak coupled with a self-closing valve can limit the duration of the leak to five minutes. We have thus two types of consequences: the one resulting from an unlimited leak with the probability of non-functioning of the limitation safety barrier, and the other with a leak limited in duration, thus a smaller pool and a smaller severity of the associated dangerous phenomena. The characteristics of the DP differ in term of limitation of the consequences of the critical event or not, and also in terms of frequency.

The corresponding part of the event tree is shown in Figure 14.

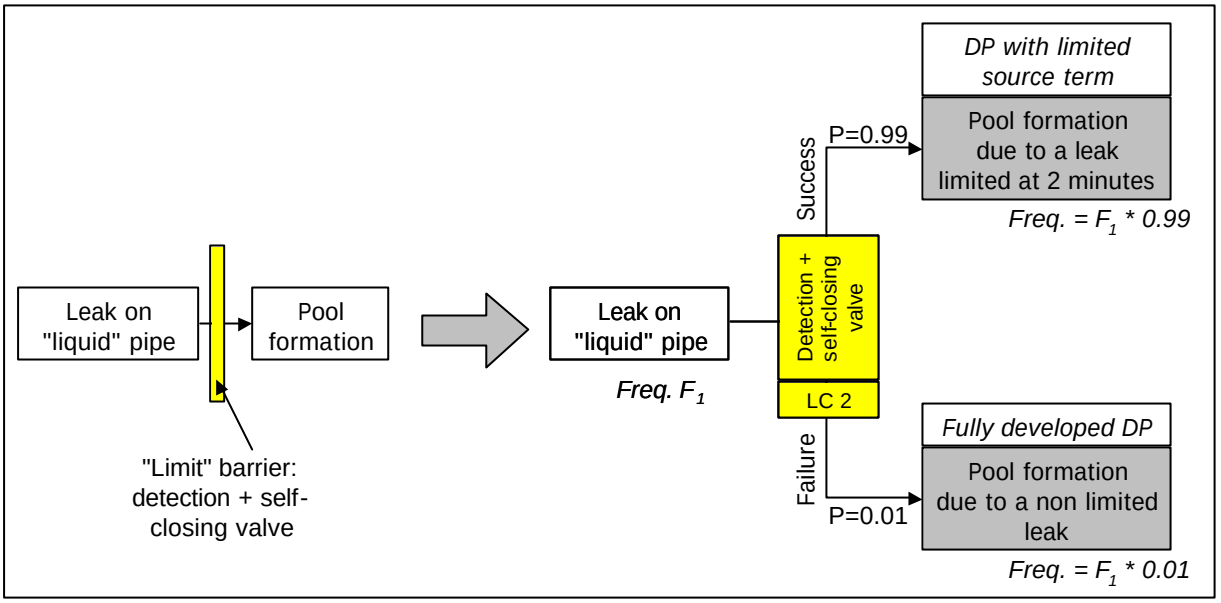

Figure 14: Influence of a limitation barrier on the consequences of the critical event

An other example: in the case of a toxic dispersion, water curtain 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 (see Figure 15). The characteristics of the DP differ in term of limitation of the effects or not, and also in terms of frequency.

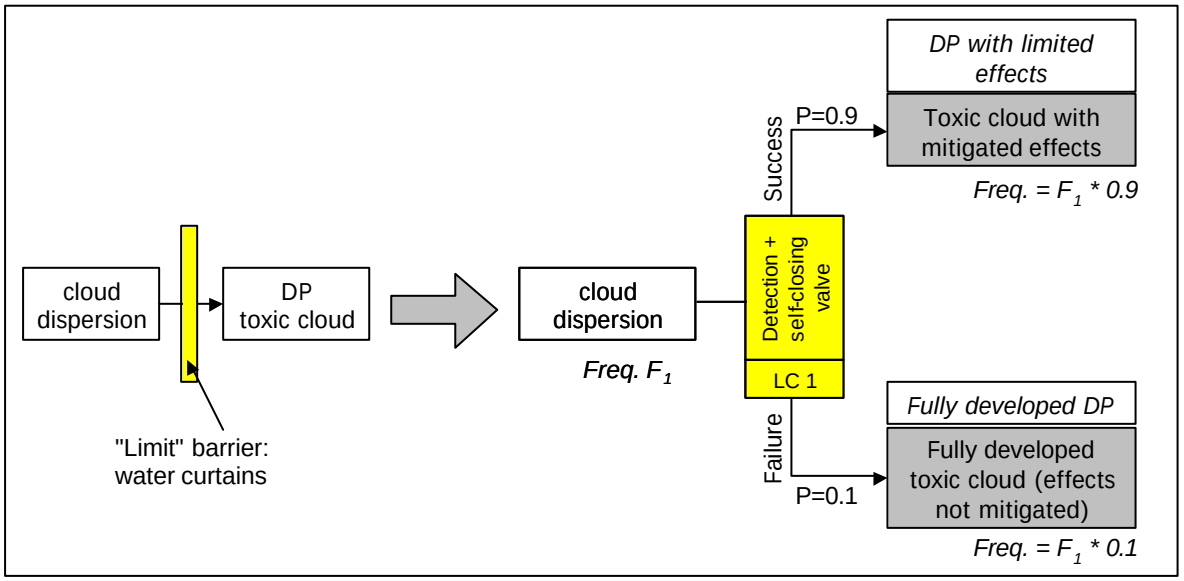

Figure 15: Influence of a limitation barrier on the effects of dangerous phenomena

3.11.5 OUTPUT OF THIS STEP

The output of this step is a list of dangerous phenomena (DP) associated to each critical event identified by the MIMAH methodology. The frequency of each dangerous phenomenon is calculated, and limitations are taken into account (DP with a limited or not limited source term, limitations or not of the effects).

A full example is given in appendix 15.

3.12 MIRAS Step 6: Estimate the class of consequences of Dangerous Phenomena

3.12.1 DEFINITIONS OF CONSEQUENCE CLASSES

The selection of Reference Accident Scenarios is based on the evaluation of the frequency of Dangerous Phenomena, and of their potential consequences. At this stage, it is thus necessary to evaluate roughly the consequences of each Dangerous Phenomenon.

This 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 12. These classes are defined according to potential consequences in term of domino effects, effects on human targets and effects on the environment.

Table 12: Class of consequences

CONSEQUENCES			CLASS
Domino effect	**Effect on human target**	**Effect on environment**	**Ranking**
See note under **Table 12**	No injury or slight injury with no stoppage of work	No action necessary, just watching	C_1
See note under **Table 12**	Injury leading to an hospitalisation > 24 hours	Serious effects on environment, requiring local means of intervention	C_2
See note under **Table 12**	Irreversible injuries or death inside the site, Reversible injuries outside the site	Effects on environment outside the site, requiring national means	C_3
See note under **Table 12**	Irreversible injuries or death outside the site	Irreversible effects on environment outside the site, requiring national means	C_4

Note for domino effects : Let us consider a Dangerous Phenomenon, noted DP1, likely to induce a domino effect and the Dangerous Phenomenon, noted DP2, caused by this domino effect. For example a Vapour Cloud Explosion (DP1) could cause the rupture of a pipe due to the overpressure generated, the leak of flammable liquid and then a poolfire feeded by the liquid flowing from the ruptured pipe (DP2). The consequences classes for DP1 and DP2 will be evaluated only on the basis of their potential human and environmental effects. If it appears that the consequence class for DP2 is higher than the consequence class for DP1, then the consequence class for DP1 shall be raised to the consequence class of DP2.

Remark:

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, they are not retained as criteria for the definition of consequence classes defined in Table 12. 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 12. It should be reminded 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)
- a **Dangerous Phenomenon with "limited effects"** means that a limiting barrier acts in the event tree, but not directly after the critical event (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, the reader could use rough consequence classes given in Table 13. If the Dangerous Phenomenon is "limited", the "fully developed" class of consequence could be decreased by the reader, according to the type of limiting systems and always referring to the definitions of Table 12.

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

Table 13: Rough class of consequences of "fully developed" Dangerous Phenomena

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

3.12.2 OUTPUT

The output of this step is a list of dangerous phenomena (DP) associated to 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 to each dangerous phenomenon found in the event trees**.

3.13 MIRAS Step 7: Use the risk matrix to select Reference Accident Scenarios

3.13.1 INTRODUCTION: THE RISK MATRIX

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 (Figure 16). 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:

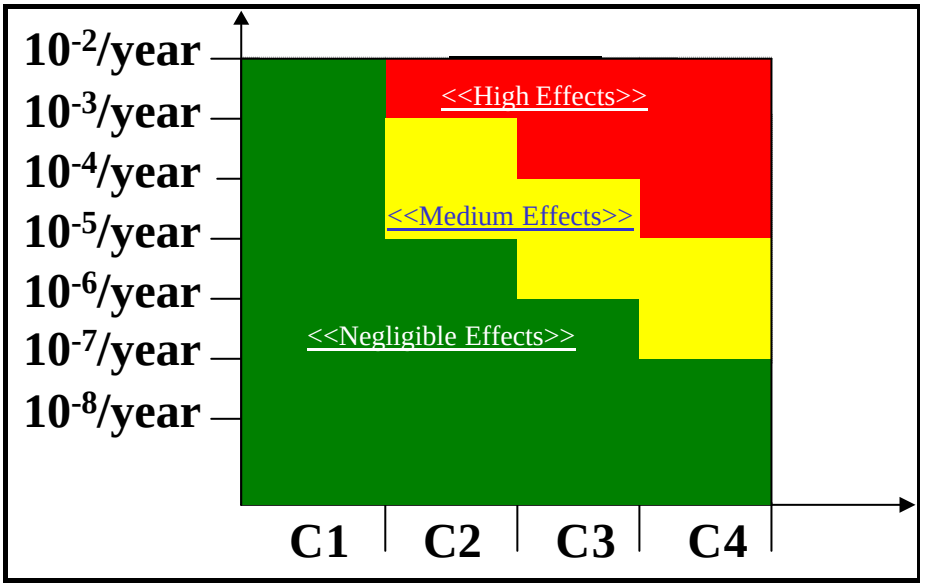

Figure 16: Risk matrix

- ✓ 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.

3.13.2 APPLICATION OF THE RISK MATRIX

Each Dangerous Phenomenon resulting from the bow-ties must be placed in the risk matrix, according its frequency and its class of consequence.

Dangerous Phenomena in yellow and red zones have to be modelled for the severity calculations.

3.13.3 COMMENTS

Appendix 13 explains how the risk matrix was built.

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.

3.14 MIRAS Step 8: Prepare information for the calculation of the Severity

The last bowties 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 given to people involved in the calculation of the severity index S.

For each reference accident scenario (a dangerous phenomenon located in the yellow or red zone of the risk matrix), the information to collect for the severity calculations are described here under:

- ✓ The equipment type

- ✓ The design/rupture pressure and design/rupture temperature of the equipment
- ✓ The height of liquid (if relevant)
- ✓ The properties of the hazardous substance (substance state, physical and chemical properties, hazardous properties, risk phrases)
- ✓ The quantity of substance available
    - Mass in the equipment
    - Flow entering in the equipment
- ✓ The operating conditions inside the equipment (temperature, pressure)
- ✓ The bow-tie with the fault tree, the branches leading to reference accident scenarios (DP in yellow or red zone) in the event tree and with the efficient safety barriers.
- ✓ The critical event
    - For a breach: localisation, diameter, liquid height above the hole and release time
    - For a leak on a pipe: localisation and diameter of the leak; dimensions of the pipe (length, diameter); release time
    - For the calculation of the rain-out, the presence of obstacles in the direction of the two-phase jet (if any)
- ✓ The dangerous phenomenon with its frequency (frequency per year)
- ✓ The ignition sources on the site, it is necessary to verify the presence of ignition sources in the flammability zone of the cloud
- ✓ The wind rose
- ✓ The average meteorological conditions on the site (stability class, wind velocity, temperature, pressure, humidity, cloud coverage,...)
- ✓ Presence of safety barriers which affect the severity modelling (presence of a bund, equipment inside a building, presence of a scrubber, injection of foam on a pool (which limits the vaporization time), efficient systems which dilute a toxic or flammable cloud,…)
- ✓ Characteristics of these safety barriers (bund, building, emergency scrubber, …)
- ✓ Description of the site surroundings, including localisation of the schools, hospitals,..
- ✓ …

4. Use of the ARAMIS methodology for the identification of scenarios in design phase

All the methods developed during the ARAMIS project in view of the identification of Reference Accident Scenarios can be applied on an existing plant or equipment. But they can also be used in a design phase.

In addition, another special tool was also developed during this ARAMIS project: the **Risk Graph**. This tool is fully explained in appendix 14. In summary, it can be said that the risk graph is a tool inspired from IEC 61508. Its purpose is to define for a given scenario and a given cause, according to the consequences of the dangerous phenomena associated to the critical event, the level of confidence of the safety barriers required to have an acceptable risk.

This tool can thus be particularly helpful in design phase, to identify the global performance requirements of safety barriers that have to be placed on an equipment in order to obtain an acceptable risk.

Information given in appendix 8 are also especially interesting in design phase, since this appendix shows (non-exhaustive) **check-lists of safety barriers** which can be used to avoid, prevent, control or limit all kinds of events encountered in the generic bow-ties.

5. Conclusion

This report describes a full methodology for the identification of Reference Accident Scenarios. 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 first to identify the potential hazardous equipment on a plant and to select relevant hazardous equipment. Then, a step by step method allow to build complete bow-ties representing the major accident hazards.

In a second step, **MIRAS** selects Reference Accident Scenarios by means of criteria related to the frequency of dangerous phenomena and their potential consequences. These criteria are synthesised in a risk matrix. A great part of the MIRAS method is devoted to the evaluation of frequencies and probabilities in the trees. The key topic is the **influence of the safety systems** on these frequencies / probabilities, and also on the possible consequences of the accident scenarios.

The most obvious usefulness of this method is the possibility to identify Reference Accident Scenarios, taking into account the safety systems, technical ones as well as safety management system.

But the outputs of MIMAH and MIRAS are much more than that. In particular, the following results can be put to the fore:

- MIMAH allows to draw a list of all potential hazardous equipment on the plant, and to select the relevant ones
- MIMAH allows to identify critical events on any kind of equipment
- On the basis of generic fault trees, MIMAH allows to identify causes of critical events and to built adapted fault trees
- MIMAH offers a tool to build automatically event trees, in which the hazardous properties of the substances are taken into account
- MIRAS gives the opportunity to identify and deeply analyse the safety systems present on an equipment. Performances of these systems can be evaluated.
- The influence of safety systems on frequencies and consequences of accident scenarios is clearly shown here, by means of a systematic method.
- The risk matrix, as well as the risk graph, offers the possibility to point out accident scenarios not adequately protected and needing additional safety systems.

This method has been tested in five chemical plant across Europe. Feed-back from these case studies is included in the tools presented here and thus the method is believed to be consistent and applicable. It is sure that concepts and tools are not simple, but authors are confident that, thanks to the various results which can be obtained with MIMAH and MIRAS, the game is worth the candle.

6. References

1. "Deliverable D.1.A. - Methodology for the Identification of Major Accident Hazards, and associated safety tools - Summary", Projet ARAMIS - 5th Framework Program of the European Community, 53 pages, July 2003, Mons (Belgique), (Delvosalle C., Fiévez C., Pipart A., Debray B., Hubert E., Cauffet F., Londiche H., Casal J., Planas E., Kirchsteiger C., Mushtaq F.).

2. "Deliverable D.1.B. - Probabilistic aspects and Methodology for the Identification of Reference Accident Scenarios- Summary", Projet ARAMIS - 5th Framework Program of the European Community, 53 pages, January 2004, Mons (Belgique), (Delvosalle C., Fiévez C., Pipart A., Debray B., Piatyszek E.., Cauffet F., Londiche H.).

3. "Deliverable D.3.A.: Method for the assessment of technical safety barriers (draft report version 1)", 65 pages, April 2003, Ineris-DRA (France), (Hourtolou D., Bouchet S., Bernuchon E.).

4. "Risk analysis: Tools for evaluation of safety barriers", 16 pages, February 2004, Ineris-DRA (France), (Dedianous V., Hourtolou D.).

5. "Defining safety functions and safety barriers from fault and event trees analysis of major industrial hazards", Bruno Debray, Christian Delvosalle, Cécile Fiévez, Aurore Pipart, Henry Londiche, Emmanuel Hubert, ESREL 2004, Berlin, Allemagne, 14-18 juin 2004

6. IEC. 1998. IEC 61508, Functional safety of electrical, electronic and programmable electronic safety-related systems, parts 1-7. *International Electrotechnical Commission, Geneva.*

7. IEC. 2001. IEC 61511, Functional safety instrumented systems for the process industry sector, parts 1-3. International Electrotechnical Commission, Geneva.

8. Guidelines for Safe Automation of Chemical Processes. *American Institute of Chemical Engineers, Center for Chemical Process Safety, New York, 1993.*

9. Layer of Protection Analysis: Simplified Process Risk Assessment. American Institute of Chemical Engineers, Center for Chemical Process Safety, New York, 2001.

10. Personal Communication from ARAMIS WP3 - see Deliverable D.3.C.

11. Personal Communication from ARAMIS WP3 - see Deliverable D.3.C.

12. AIChE, CCPS, Guidelines for Chemical Process Quantitative Analysis, American Institute of Chemical Engineers, New York, 1989

7. List of appendices

1. Glossary
2. Methodology for the selection of equipment to be studied
3. Method to associate critical events and relevant hazardous equipment
4. Generic fault trees
5. Methodology for the building of generic event trees (MIMAH)
6. Generic event trees generated by MIMAH
7. Frequencies and probabilities data for the fault trees
8. Checklist of safety functions and barriers
9. Assessment of the performances of safety barriers
10. Generic frequencies data for the critical events
11. AND and OR gates, and notations in the event tree
12. Probability aspects in the event tree
13. Risk Matrix
14. The Risk graph
15. Application of MIMAH and MIRAS : A fictitious example