The European Commission
Community Research
Energy, Environment
and Sustainable Development

PROJECT UNDER 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

USER GUIDE

Institut National de l'Environnement Industriel et des Risques (INERIS)	FRANCE
Joint Research Center - European Commission	ITALY (EU)
Faculté Polytechnique de Mons	BELGIUM
Universitat Politecnica de Catalunya	SPAIN
Risoe National Laboratory	DENMARK
Universita di Roma "La Sapienza"	ITALY
Central Mining Institute	POLAND
Technische Universiteit Delft	THE NETHERLANDS
IChemE - EPSC	UNITED KINGDOM
ARMINES : Ecole Nationale Supérieure des Mines de Paris	FRANCE
ARMINES : Ecole Nationale Supérieure des Mines de St Etienne	FRANCE
ARMINES : Ecole Nationale Supérieure des Techniques Industrielles et des Mines d'Alès	FRANCE
Jozef Stefan Institute	SLOVENIA
VSB - Technicka Univerzita Ostrava	CZECH REPUBLIC

Main contributors to this document : H.Andersen, J.Casal, A.Dandrieux, B. Debray, V.De Dianous, N.J.Duijm, C.Delvosalle, C.Fievez, L.Goossens, R.T.Gowland, A.J.Hale, D.Hourtolou, B.Mazzarotta, A.Pipart, E.Planas, F.Prats, O.Salvi, J.Tixier.

Additional information on http://aramis.jrc.it

December 2004

CONTENTS

Preface

Risk Assessment for industrial activity is becoming increasingly important everywhere, particularly in the densely populated regions of Europe. Decisions balancing risks created by an activity towards people and environment require tools to be made available to all involved stakeholders. For these decisions to be made, there need to be some accepted methodologies based on science and wherever possible, measurable parameters. To gain credibility and widespread use, the methodologies need to have a number of attributes:

- *Use state of the art methods to study processes to predict potential hazardous events and their likelihood.*
- *Use state of the art or best practice calculation methods for effects of toxic releases, fire, explosion and environmental impact.*
- *Utilise information which is wherever possible specifically applicable to the enterprise local environment and socio-economic situation, recognising special factors such as vulnerability.*
- *Use best available data for properties of materials, processing parameters, failure rates (Hardware, Software and Human Factors)*
- *Have 'transparent' processes which allow users or regulating authorities to understand, validate and comment on in a consistent manner.*
- *Achieve consistency so that different analysts derive substantially the same results when analysing similar operations.*
- *Enhance existing methodologies by improving the assessment of such important parts of the overall subject such as Safety Management Systems, Emergency Response and the Vulnerability of the potentially affected zones.*

The ARAMIS project team believes that the methodology described in this guidance addresses these and contributes in a major way to the goal of improving risk assessment. ARAMIS method offers a realistic choice for industry and regulators who have not yet settled their detailed policies. For those who have established their policies, ARAMIS has additional functionality within its tools which can enhance existing risk assessment. These are integral assessment tools within ARAMIS which can be extracted and used in conjunction with other methodologies such as comprehensive Quantitative Risk Assessment (QRA), or Deterministic Assessment thus enhancing results available to the users and reviewers. These tools elucidate the parameters which can be managed to reduce risk, allowing improvements to influential factors such as Inherently Safer Design and Safety Management Systems.

Consistency accuracy and credibility of risk assessment outcomes remain elusive goals. ARAMIS is a significant step in this direction.

Richard Gowland, Director of the European Process Safety Centre

Acknowledgements

The authors of the present document and, beyond, the members of the ARAMIS consortium thank the European Commission for its financial support in the framework of the the Energy, Environment and Sustainable Development Programme in the 5th Framework Programme for Science Research and Technological Development of the European Commission.

The ARAMIS project was also co-funded by state and private institutions from the different countries of the consortium members. Let them all be thanked for their contribution to this project.

Our gratitude is also addressed to the members of the Review Team who dedicated time and attention to assessing the results of this research program : Mrs. Helga KATZER, Mrs. Homa AMINI, Mrs. Jasmina KARBA, Mrs. Elisabeth KRAUSMANN, Mrs Ruth COUTTO, Mr. Bruno CAHEN, Mr. Peter VANSINA, Mr. Jean Paul LACOURSIERE, Mr. Jos POST, Mr. Jochen UTH, Mr. Michael STRUCKL, Mr. Pat CONNEELY, Mr. Lajos KÁTAI-URBÁN, Mr. Pablo LERENA, Mr. Richard GOWLAND, Mr. Jacques CALZIA, Mr. Michalis CHRISTOU, Mr. Juergen WETTIG, Mr. Axel WOLTER, Mr. Francisco José RUIZ BOADA, Mr. Peter ALBERTSSON.

INERIS as co-ordinator of this program thanks all the members of the consortium who have contributed to the success of this research and now constitute the basis of an expertise network on industrial safety and the prevention of major accidents.

INERIS, as initiator and co-ordinator of the project, would like to thank very warmly Mr Stuart Duffield (former head of Major Accident Hazard Bureau - JRC) and Mr Jürgen Wettig (DG.ENV) who strongly supported the ideas contained in ARAMIS and the final goal to develop a convergent risk assessment method with a large number of partners coming from countries applying different approaches.

Glossary

The words defined in the glossary are asterisked (*) in the principal text.

Audit: A systematic examination or review whether the actual condition and situation (of safety management) is in agreement with the stated requirements

Blast*:* overpressure originated by an explosion (bar).

BLEVE: explosion resulting from the failure of a vessel containing a liquid at a temperature significantly above its boiling point at normal atmospheric pressure.

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,…

Critical Event (in the bow-tie): 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. The Critical Event is the centre of the bow-tie.

Dangerous phenomenon (in the bow-tie, event tree side): event following the tertiary critical event (for example, the pool fire after the ignition of a pool). Examples of Dangerous Phenomena are a Vapour Cloud Explosion, a flash fire, a tank fire, the dispersion of a toxic cloud, etc.

Dangerous Phenomenon with a "limited source term": Dangerous Phenomenon for which 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)

Dangerous Phenomenon with "limited effects": Dangerous Phenomenon for which 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).

Delivery system: Delivery systems are structural parts of the **safety management system***. Delivery systems provide the required resources (behaviour and hard- or software) that is needed for optimal performance of a barrier throughout its life cycle

"fully developed" Dangerous Phenomenon: Dangerous Phenomenon for which no safety system limits the consequences of the critical event and no safety system mitigates the effects

Effectiveness of a safety barrier: The effectiveness is the ability of a 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 not completely close on a safety demand (either because of hardware design or design of the method to close it by hand) would not have an effectiveness of 100%.

Event tree: Right part of the bow-tie, identifying the possible consequences of the critical event

Fault Tolerance: It is linked to the capacity of the barrier to keep its safety function in case of failure of one or more system composing the barrier. Fault tolerance is linked to the *redundancy*. For example, a fault tolerance of 1 means that if one component is defective, the safety function remains operated.

Fault tree: Left part of the bow-tie, identifying the possible causes of the critical event

Flash fire: rapid combustion of a cloud of flammable gas/vapour mixed with air.

GIS*:* geographical information system.

Hazardous substance: The SEVESO II Directive defines a hazardous substance as a substance, mixture or preparation listed in Annex 1, Part 1, of the SEVESO Directive or fulfilling the criteria laid down in Annex 1, Part 2, of the SEVESO II Directive and presents as a raw material, product, by-product, residue or intermediate, including substances which may be generated in case of accident;

Finally, a hazardous substance is a substance whose toxicity, flammability, instability or explosivity may induce hazard for people, environment or equipment. The used hazardous properties are based on the hazardous categories of the SEVESO II Directive and the risk phrases of the 67/548/EEC Directive.

Initiating event: the first causes upstream of each branch leading to the critical event in the fault tree (on the left end of the bow-tie).

Level of confidence of a safety barrier: the probability of failure on demand to perform properly a required safety function according to a given effectiveness and response time under all the stated conditions within a stated period of time. 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, including those relying on human behaviour full or in part.

The **"design" level of confidence** is assessed with the help of instruction given in appendix 8. 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.

The **"operational" level of confidence** includes the influence of the safety management system. The value could be lower than the "design" one if some problems are identified during the audit of the safety management system.

Levels of effects: qualitative categories of the effects of accidents.

Lower flammability limit (LFL): minimum concentration of flammable gas or vapour in air at which the flame propagates through the mixture

MIMAH: Methodology for the Identification of Major Accident Hazards

MIRAS: Methodology for the Identification of Reference Accident Scenarios

Missiles: fragments of a vessel ejected by an explosion.

Overpressure: rapid increase of pressure originated by an explosion (bar).

Pool fire: combustion of a pool of liquid fuel; a pool fire can also happen in a tank containing liquid fuel.

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).

Radiation: thermal radiation from a flame (kW m^{-2}).

Relevant hazardous equipment: equipment containing a quantity of hazardous substance higher or equal to a threshold–quantity.

Response time: duration between the straining of the safety barrier and the complete achievement (which is equal to the effectiveness) of the safety function performed by the safety barrier.

Risk index: a measure, quantitative or qualitative, oriented to integrate into a numerical value or a descriptive adjective, a set of factors which have an influence on the hazards or the risk of a system.

Risk severity index: risk index as defined by Eq. 1 (Section 7.2.2).

Safe Failure Fraction: It is the ratio between the frequency of failure of the component leading to a safe position to the frequency of total failures. A safe position is a failure which does not have the potential to put the safety barrier in a hazardous or fail-to-function state.

Safety barrier: The safety barriers can be physical and engineered systems or human actions based on specific procedures or administrative controls. The safety barrier directly serves the safety function. The safety barriers are the "how" to implement safety functions.

Safety culture: The set of shared and interconnected beliefs, norms and practices among members of a work group [or organisation] that have an impact – actual or potential – on the safety of the operations of the group [organisation].

Safety function: A safety function is a technical or procedural action, and not an object or a physical system. It is an action to be achieved in order to avoid or prevent an event or to control or to limit the occurrence of the event. This action will be realised thanks to a safety barrier. The safety function is the "what" needed to assure, increase and/or promote safety.

Safety Integrity Level (SIL): ranking of the Level of Confidence* according to standards IEC 61508 and IEC 61511 on functional safety of electrical/electronic/programmable electronic safety-related systems. SIL is defined as $SIL = -{}^{10}\log(PFD)$, where PFD is Probability of Failure on Demand

Safety management: the set of management activities that ensures that hazards are effectively identified, understood and minimised to a level that is reasonably achievable. *In the framework of ARAMIS, this can be extended to include:* The set of management activities that ensure that safety barriers are specified and that these safety barriers perform as designed and required.

Safety management system: The documented set of principles, scheduled tasks, procedures, and responsibilities that ensures effective safety management and its continuous improvement. *Or, adapting the definition of a quality management system (ISO 9000)*: that part of the overall management system that includes organizational structure, planning activities, responsibilities, practices, procedures, processes and resources for developing, implementing, achieving, reviewing and maintaining the safety policy.

Secondary Critical Event (in the bow-tie, event tree side): event following the critical event (for example, the formation of a pool after a breach on a vessel)

Target : element of the environment of the industrial site that can undergo an impact in case of a major accident occurring in the plant. Three main categories of targets have been defined : human targets, material targets and the natural environment.

TEEL: Temporary Emergency Exposure Limits.

Tertiary Critical Event (in the bow-tie, event tree side): event following the secondary critical event (for example, the ignition of a pool after the formation of a pool).

Threshold levels: limit values for the different levels of effects, as defined in Table 23.

1. Introduction

1.1 Context and history of ARAMIS

At the time the ARAMIS project was beginning, some recent technological accidents like Enschede (2000), Toulouse (2001) or Lagos (2002) had led the public to wonder or even mistrust both the industry and the regulatory authorities in their risk-informed decisions. These accidents had raised the need for more consistent and transparent decision-making processes.

Risk-based decisions, of course, require some reliable scientific input from risk analyses. But from one risk analyst to the next, noteworthy variation exist in the results, which would affect any relevant and local decision. This was put in evidence by the ASSURANCE project. That is why has emerged the need for a methodology giving consistent rules to select accident scenarios and taking into account safety management effectiveness for risk control demonstration. In the context of Seveso II directive, there is also an underlying need for a method that could reach a consensus amongst risk experts throughout Europe.

The potential end users of ARAMIS are numerous but the most concerned are the industry, the competent authorities and the local authorities. If all of them have an interest in the same risk management process, their needs are slightly different.

Industry needs a method to identify, assess and reduce the risk and demonstrate the risk reduction as required by the Art.9 of the SEVESO directive. This method and the demonstration have to be accepted by the competent authorities. The approach also has to bring useful information about the ways to reduce the risk and to manage it daily.

The competent authorities need to be able to assess the safety level of the plant, particularly through the safety report. They need to know which scenarios to select for modelling of consequences.

Both need to assess the influence of the management on the safety level. The industry to be able to improve its management to reduce the risk, and the competent authority to assess a true risk level which takes into account this major influencing factor. More than 50% of the major accidents have indeed causes related with human and organisational factors. This is a sufficient reason to take these aspects specifically into account.

The local authorities (municipalities) are interested in land use planning issues. They need to have a clear report on the risks their population is facing. They also want to get information that can be used for decision making. Basically, their role relates to the reduction of vulnerability either by limiting the number of targets (people, infrastructure, environment) exposed to the risk or by introducing obstacles between the source and these targets. They also need to trust the industry and competent authorities when they propose a risk contour based on an accident scenario.

The aim of ARAMIS is to answer all these needs :

- Enable the demonstration that hazards are identified and risk properly managed, by taking into account also the efficiency of the management system ;

- Provide information for the decision making process related to land use planning and emergency planning ;

- Present a clear approach understandable by the public.

It is also to make the convergence between the deterministic approach and the probabilistic approach with a method that meets the expectations of both the industry, the competent authorities and the local authorities.

ARAMIS overall objective is to build up a new Accidental Risk Assessment Methodology for IndustrieS that combines the strengths of both deterministic and risk-based approaches. Co-funded under the 5th EC Framework Programme, this three-year project started in January 2002. Three years later, the basic methodology is achieved and aims at becoming a supportive tool to speed up the harmonised implementation of SEVESO II Directive in Europe. This user guide intends to expose the major features of the methodology and to provide ARAMIS potential users the essential elements to implement the methodology.

1.2 Overview and outline of the user guide

ARAMIS is divided into the following major steps that are described more extensively in the main chapters of the present user guide.

- Identification of major accident hazards (MIMAH)

- Identification of the safety barriers and assessment of their performances

- Evaluation of safety management efficiency to barrier reliability

- Identification of Reference Accident Scenarios (MIRAS)

- Assessment and mapping of the risk severity of reference scenarios

- Evaluation and mapping of the vulnerability of the plant’s surroundings

The last chapter is dedicated to the potential use of ARAMIS for further applications and fields of research.

Each of the major steps of the ARAMIS methodology are described briefly hereunder and are summarised in Figure 1.

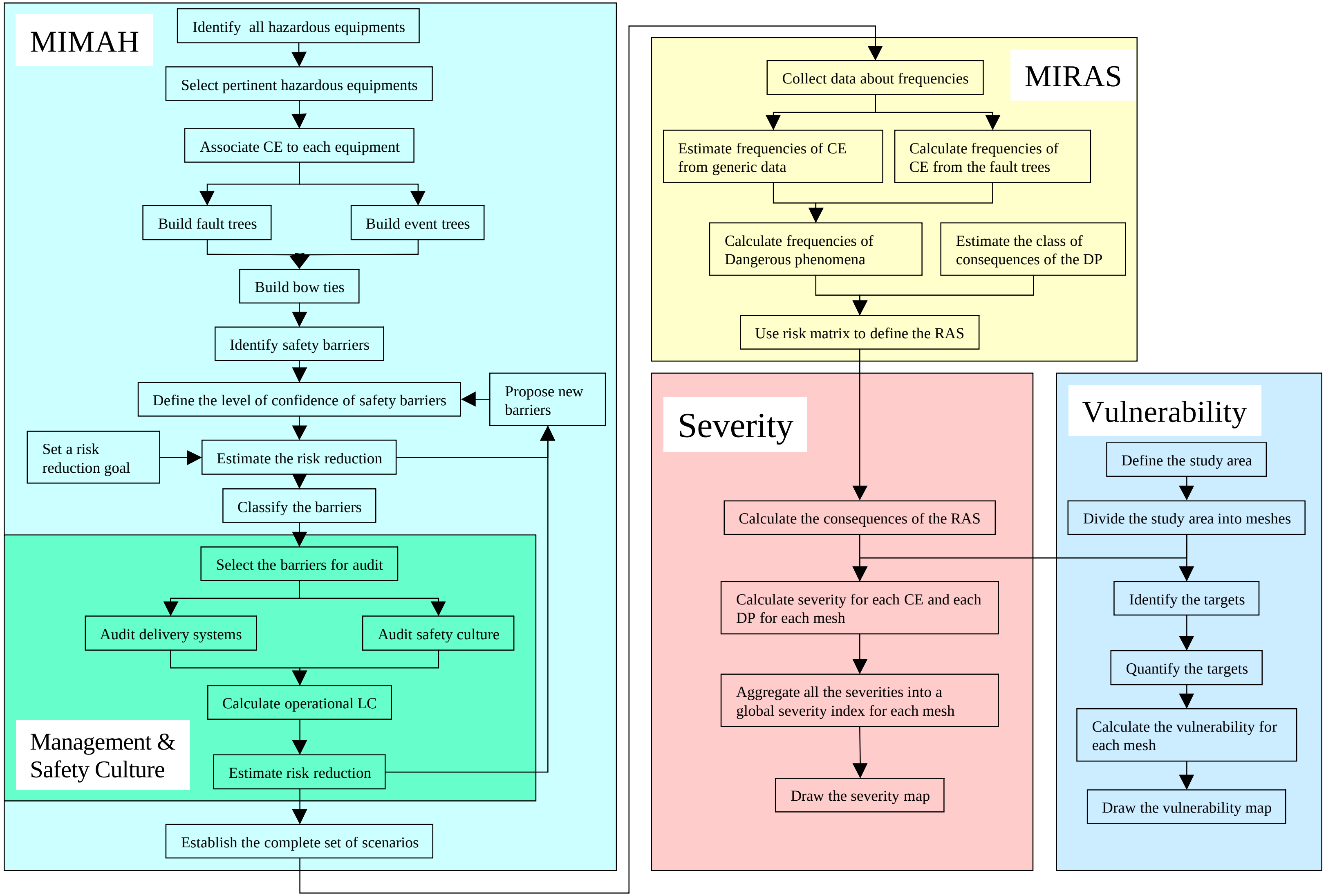


Figure 1 : general overview of the ARAMIS methodology

1.2.1 Methodology for the identification of the major accident hazards (MIMAH) [Chapter 2]

MIMAH [Chapter 2] is the method for the identification of major accident hazards. It is based mainly on the use of the bow-tie, centred on a critical event and composed of a fault tree on the left and an event tree on the right.

MIMAH provides a comprehensive methodology to collect the information needed to identify potentially hazardous equipment in the plant and to select relevant hazardous equipments susceptible to generate major accidents. In a second time, the list of potential critical events associated with each equipment is generated. Fault trees and event trees are build for each critical event on the basis of the generic trees proposed by the methodology. The set of a fault tree and an event tree constitutes the bow tie, which, at this step of the process is considered without any safety barrier. Bow-ties are assumed to be built during a risk analysis on site, with a working group.

This has the advantage to make an explicit distinction between hazard and risk. This first step of the method allows really the identification of hazards. The next step aims at identifying the risks which result from the hazard scenarios and the failure of safety barriers.

1.2.2 Identification of the safety barriers and assessment of their performance [Chapter 3]

This second step of the methodology is intended to give an acute estimation of the risk level and to promote the implementation of safety systems. In this step, the effects of safety systems are taken into account in terms of frequency of the accident and also in terms of level of consequences. It involves the identification of safety functions and safety barriers resulting from an analysis of the bow tie.

The influence of safety barriers is determined in assessing their performances (level of confidence, efficiency and time response in accordance with the scenario).

A risk reduction goal, defined in terms of aggregated confidence level, is assigned to each scenario in order to reach an acceptable level of risk during risk analysis.

1.2.3 Evaluation of safety management efficiency to barrier reliability [Chapter 4]

The management has a strong influence on the capacity to control the risks. The aim of ARAMIS is to provide tools to assess the safety management system and the safety culture and take them into account by the competent authorities as well as to help the plant operator to define the objectives and characteristics of the SMS (safety management system). The approach adopted in ARAMIS consists in focusing the requirements of the management system on the life cycle of the safety barriers resulting from the previous steps of the risk analysis procedure. This life cycle includes the following steps : design, installation, use, maintenance, improvement. For each of them, ten important structural elements of the safety management organisation have been identified and can be assessed together with a set of eight cultural factors. Questionnaires were developed for the auditing of these management and cultural aspects.

1.2.4 Identification of Reference Accident Scenarios (MIRAS) [Chapter 5]

Once the major accident scenarios have been assessed (step MIMAH) and the safety barriers have been quoted (and modified according to the results of the audits and safety questionnaires), their consequences must be evaluated. The aim of MIRAS is to Identify the Reference Accident Scenarios (RAS) which will be taken into account for the calculation of the severity index. The principle is to select only the scenarios corresponding to dangerous phenomena with a frequency and/or consequences which may have actual effects on the severity. A risk matrix was developed to guide this selection together with guidelines for estimating the frequency of occurrence of the scenarios (either by an analysis of the fault tree and the barrier performance or by the use of generic frequencies) and for estimating the consequence class of dangerous phenomena.

1.2.5 Assessment and mapping of the severity [Chapter 6]

Once the Reference Accident Scenarios have been selected, the methodology implies to assess the severity of these scenarios. The aim is to be able to build severity maps so that the effect of an accident can be crossed with the vulnerability of the surroundings. A severity index was developed considering four effect levels so that the results of various risk analysis can be compared. This Risk Severity Index S for a whole installation is a combination of the specific risk severity indexes associated to each of the critical events considered and their frequencies. The specific risk severity indexes are build by considering all the consequences a critical event can have and their associated probabilities. A GIS tool was developed to draw the risk severity maps, which will then be crossed with vulnerability maps.

1.2.6 Evaluation of the vulnerability [Chapter 7]

The last step of the ARAMIS methodology is dedicated to the assessment of the vulnerability. A vulnerability index has been build as a linear combination of the number of different types of targets including human, environmental and material targets. Each category of target has been assigned a weight for each of the physical effects representative of its relative vulnerability. A GIS tool was developed for the building of the vulnerability maps. Their crossing with the severity maps will be useful for land use planing and risk reduction decisions involving the suppression or protection of the targets.

1.3 Structure of the user guide

In the following chapters, each step of the methodology is explained in a short and synthetic manner. Reference is made to the ARAMIS documents in which the reader can obtain more detailed information. Examples are given to illustrate the methodology. These examples are mainly extract of the test study cases or derived from other real cases. They allow the reader to understand in a very concrete manner how the methodology can be applied and what the results are.

1.4 Link with other available ARAMIS documents (http://aramis.jrc.it)

Chapters 2, 3 and 5 of this document present the main steps in order to apply the Methodology for the Identification of Major Accident Hazards (MIMAH) and the Methodology for the Identification of Reference Accident Scenarios (MIRAS). The methodologies are fully developed and explained in the following document:

- "Deliverable D.1.C. - Report presenting the final version of the Methodology for the Identification of Reference Accident Scenarios", ARAMIS Project - 5th Framework Program of the European Community, 59 pages + 15 appendices, July 2004, Mons (Belgium), (Delvosalle C., Fiévez C., Pipart A.)

Two other documents are available and consist in preliminary reports, which describe how the tools used in MIMAH and MIRAS have been developed:

- "Deliverable D.1.A. - Methodology for the Identification of Major Accident Hazards, and associated safety tools - Summary", ARAMIS Project - 5th Framework Program of the European Community, 53 pages, July 2003, Mons (Belgium), (Delvosalle C., Fiévez C., Pipart A., Debray B., Hubert E., Cauffet F., Londiche H., Casal J., Planas E., Kirchsteiger C., Mushtaq F.).
- "Deliverable D.1.B. - Probabilistic aspects and Methodology for the Identification of Reference Accident Scenarios - Summary", ARAMIS Project - 5th Framework Program of the European Community, 53 pages, January 2004, Mons (Belgium), (Delvosalle C., Fiévez C., Pipart A., Debray B., Piatyszek E.., Cauffet F., Londiche H.).

Chapter 6 presents the method for calculating the risk severity index. This method as well as the preparatory works to build the severity index S is fully described in the following documents

- Deliverable D.2.A “Parameters composing the severity index” WP 2: Severity evaluation Casal, J.; Planas, E.; Delvosalle, C.; Fiévez, C.; Pipart, A.; Lebecki, K.; Rosmus, P.; Vallee, A.
- Deliverable-D2B "Methodology for the calculation of the risk severity index" WP 2 UPC
- Deliverable D.2.C “THE RISK SEVERITY INDEX” WP 2: Severity evaluation Casal, J.; Planas, E.; Delvosalle, C.; Fiévez, C.; Pipart, A.; Lebecki, K.; Rosmus, P.; Vallee, A

Chapter 4 presents the method to assess the safety management efficiency and the safety culture. Its main features are fully developed in the following documents.

- Deliverable D.3.B "Methodology to determine a Safety Management Efficiency Index ", Nijs Jan Duijm, Henning Boje Andersen, Andrew Hale, Louis Goossens, Frank Guldenmund

Chapter 7 exposes the method for calculating and mapping the vulnerability of the surroundings. This method and the tools that were developed to implement it are described in the following documents.

- Deliverable D.4.A “Guide describing the methodology to calculate the spatial vulnerability index V” WP 4: Environment vulnerability Tixier J., Dandrieux A., Dusserre G., Mazzarotta B., Di Cave S., Bubbico R., Londiche H., Debray B., Hubert E., Rodrigues N.
- Deliverable D.4.B “Interface for using GIS for data acquisition and mapping” MAPINFO v7.0 and Géoconcept Expert v4.2 WP 4: Environment vulnerability Tixier J., Dandrieux A., Dusserre G., Londiche H., Debray B., Hubert E., Rodrigues N.
- Deliverable D.4.C «Software for determining the environmental vulnerability index based on G.I.S. information » MAPINFO v7.0 and Géoconcept Expert v4.2 WP 4: Environment vulnerability Tixier J., Dandrieux A., Dusserre G., Londiche H., Hubert E., Rodrigues N.

1.5 List of main articles and publications

Many articles were written by the ARAMIS partners during the project and edited in conference proceedings or scientific journals. These articles bring useful complimentary information to understand the evolution of the concepts and tools of ARAMIS and their implementation. The list below is far from being exhaustive.

[Hourtolou 03] Hourtolou, D. and Salvi, O., ARAMIS Project: development of an integrated accidental risk assessment methodology for industries in the framework of SEVESO II directive, Bedford, T. and Gelder, P. H. A. J. M. van, Safety & Reliability - ESREL 2003, pp. 829-836, 2003

[Delvosalle 04] C. Delvosalle, C. Fiévez, A. Pipart, H. Londiche, B. Debray, E. Hubert, Aramis Project: Effect of safety systems on the definition of reference accident scenarios in SEVESO establishments, Proceedings of the LP2004, Loss prevention conference, Prague, May-June 2004.

[Debray 04] B. Debray, C. Delvosalle, C. Fiévez, A. Pipart, H. Londiche, E. Hubert, Defining safety functions and safety barriers from fault and event trees analysis of major industrial hazards, PSAM7-ESREL2004 conference, Berlin, June 2004.

[Planas 04] E. Planas, J. Casal, ARAMIS project: application of the severity index, Proceedings of the LP2004, Loss prevention conference, Prague, May-June 2004.

[Duijm 04] N. J. Duijm, M. Madsen, H. B. Andersen, L. Goossens, A. Hale, D. Hourtolou, ARAMIS project: Effect of safety management's structural and cultural factors on barrier performance, Proceedings of the LP2004, Loss prevention conference, Prague, May-June 2004.

[Tixier 04] J. Tixier, A. Dandrieux, G. Dusserre, R. Bubbico, L. G. Luccone, B. Mazzarotta, B. Silvetti, E. Hubert, Vulnerability of the environment in the proximity of an industrial site, Proceedings of the LP2004, Loss prevention conference, Prague, May-June 2004.

[Hourtolou04] D.Hourtolou, B. Debray, O. Salvi, ARAMIS project: Achievement of the integrated methodology and discussion about its usability from the case studies carried out on real test Seveso II sites. Proceedings of the LP2004, Loss prevention conference, Prague, May-June 2004.

[Duijm 04] N.J. Duijm, H.B. Andersen, A. Hale, L. Goossens, D. Hourtolou, Evaluating and Managing Safety Barriers in Major Hazard Plants, PSAM7-ESREL2004 conference, Berlin, June 2004.

[Duijm 03] Duijm, N.J., Madsen, M.D., Andersen, H.B., Hale, A.R., Goossens, L., Londiche, H., and Debray, B., Assessing the effect of safety management efficiency on industrial risk, Bedford, T. and Gelder, P. H. A. J. M. van, Safety & Reliability - ESREL 2003, pp. 575-581, 2003

[Delvosalle 03] Delvosalle, C., Fiévez, C., Pipart, A., Casal Fabrega, J., Planas, E., Christou, M., Mushtaq, F., ARAMIS project: Identification of Reference Accident Scenarios in SEVESO establishments, T. and Gelder, P. H. A. J. M. van, Safety & Reliability - ESREL 2003, pp. 479-487, 2003

2. Methodology for the Identification of Major Accident Hazards (MIMAH - Construction of bowties without safety barriers)

The Methodology for the Identification of Major Accident Hazards (MIMAH) 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, the physical state and the hazardous properties of chemicals handled.

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.

In order to prepare the application of ARAMIS and in particular, of MIMAH, a preliminary visit is necessary to meet the plant operator for a first contact, to explain the objectives of ARAMIS and to collect the data needed to start MIMAH (see paragraph 2.1).

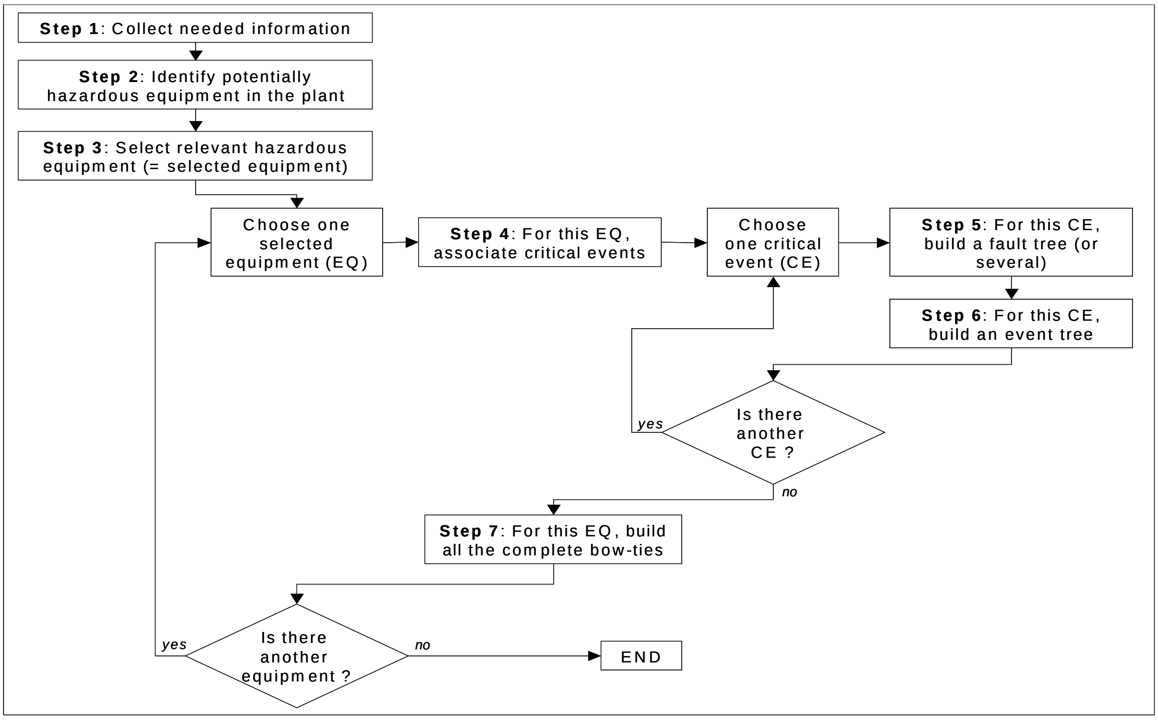


Figure 2: General overview of MIMAH steps

2.1 Collect needed information

The list of minimum data needed to achieve the Methodology for the Identification of Major Accident Hazards, MIMAH, is the following one:

- ✓ 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
  - List of substances stored or handled in the plant, associated with the list equipment concerned
  - Hazardous properties of the substances (risk phrases, hazard classification)
- ✓ 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 boiling temperature

2.2 Select relevant hazardous equipments

2.2.1 Purpose

The purpose of the method for the selection of relevant hazardous equipment is to select equipment on which the identification of major accident scenarios will be performed. It must be reminded that, before applying this method, a list with equipment containing potentially hazardous substances must be drawn (see paragraph 2.2.2).

2.2.2 Identify potentially hazardous equipments in the plant (MIMAH Step 2)

On the basis of information collected (see paragraph 2), a **list of hazardous substances**(*) present in the plant, which have one or several risk phrases mentioned in the typology of hazardous substances (see Table 1), must be drawn up.

Table 1: Typology of hazardous substances (Extract of *Table 2 of D.1.C. (MIMAH Step2) [1])*

Category	Risk Phrases
Very toxic	R26, R100
Toxic	R23, R101
Oxidising	R7, R8, R9
Explosive	R1, R2, R3, R4, R5, R6, R16, R19, R44, R102(*)
Flammable	R10, R18
Highly flammable	R10, R11, R17, R30
Extremely flammable	R10, R11, R12
React violently with water	R14, R15, R29, R14/15, R15/29
React violently with another substance	R103, R104, R105, R106
Dangerous for the environment (aquatic environment)	R 50, R51
Dangerous for the environment (non-aquatic environment)	R54, R55, R56, R57, R59

The risk phrases of the handled substances will be also taken into account in the building of event trees.

In a second step, it is necessary to draw up a **list of equipments containing these substances**, and to specify in which **physical state** (two-phase, liquid, gas/vapour or solid) the substance can be found in the equipments.

---

[*] The words with an asterisk are defined in the glossary.

The equipment must then be classified according to the typology of equipment. 16 types of equipment have been defined:

Table 2: Typology of equipment (Extract of *Table 3 of D.1.C.[1], MIMAH Step 2*)

#	**Type of equipment**
EQ1	Mass solid storage
EQ2	Storage of solid in small packages
EQ3	Storage of fluid in small packages
EQ4	Pressure storage
EQ5	Padded storage
EQ6	Atmospheric storage
EQ7	Cryogenic storage
EQ8	Pressure transport equipment
EQ9	Atmospheric transport equipment
EQ10	Pipe
EQ11	Intermediate storage equipment integrated into the process
EQ12	Equipment involving chemical reactions
EQ13	Equipment devoted to the physical or chemical separation of substances
EQ14	Equipment designed for energy production and supply
EQ15	Packaging equipment
EQ16	Other facilities

The result of the selection is will be a table 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

2.2.3 Select relevant hazardous equipments (= selected equipments) (MIMAH Step3)

Each equipment containing an hazardous substance will be selected as a relevant hazardous equipment(*) **if the mass of hazardous substance in this equipment is higher or equal to a mass threshold**. 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 equipments in case of possible domino effects.

The method for the selection of relevant hazardous equipments is fully described in *Appendix 2 of D.1.C., paragraph 2 [1] (available at http://aramis.jrc.it).* This method is based on the "VADE MECUM" methodology used in Walloon Region, in Belgium (DGRNE, 2000) *[2]*.

To use this method, the following data are needed for each equipment identified as potentially hazardous, obtained by the step 2 of MIMAH (see paragraph 2.2.2):

- ✓ Name of the equipment
- ✓ Type of equipment
- ✓ Substance handled
- ✓ Physical state
- ✓ Boiling temperature (in °C)
- ✓ Service temperature (in °C)
- ✓ Risk phrases
- ✓ Hazardous classification
- ✓ Mass contained in the equipment (in kg) or, for flow through equipment (as pipes), the mass released in 10 minutes

The rules described hereafter must be followed to calculate the mass threshold for the selection of hazardous equipments.

1. Define a reference mass Ma (kg) according to the properties of the substance

Table 3 : reference masses

	Reference mass Ma (kg)		
Properties of the substance	**Solid**	**Liquid**	**Gas**
1 Very toxic	10.000	1.000	100
2 Toxic	100.000	10.000	1.000
3 Oxidizing	10.000	10.000	10.000
4 Explosive (definition 2a annex 1 Seveso II Directive)	10.000	10.000	---
5 Explosive (definition 2b annex 1 Seveso II Directive)	1.000	1.000	---
6 Flammable	---	10.000	---
7 Highly flammable	---	10.000	---
8 Extremely flammable	---	10.000	1.000
9 Dangerous for the environment	100.000	10.000	1.000
10 Any classification not covered by the properties given above in combination with risk phrases R14, R14/15, R29	10.000	10.000	---

2. Adjust the mass reference of liquid according to the possibility of vaporisation

For liquids, the reference mass Ma given in the table above must be divided by a S coefficient.

A new reference mass Mb is then found: $Mb = \frac{Ma}{S}$

An equipment will be selected if the mass contained M is higher than the reference mass Mb.

- S is the sum of the coefficient S_1 and the coefficient S_2.
  S must be included in the interval 0.1 – 10.
  $$\begin{array}{|llll} 0.1 \leq S \leq 10 & & & \\ \text{If} & S < 0.1 & \text{then} & S = 0.1 \\ \text{If} & S > 10 & \text{then} & S = 10 \end{array}$$
- S_1 coefficient takes into account the difference between the service temperature T_p (°C) and the boiling temperature at atmospheric pressure T_{eb} (°C) according to: $S_1 = 10^{(T_p - T_{eb})/100}$
- S2 coefficient is only applied to process with a service temperature lower than 0°C, according to: $S_2 = \frac{Teb}{(-50)}$. In other cases (positive service temperature), S_2 = 0.
  Temperatures are expressed in Celsius degrees.

3. Adjust the reference mass in case of domino effect hazard

For equipment not selected previously (M < Mb), then the following reasoning is applied: Equipment containing **explosive or flammable substances** must also be selected as hazardous equipment:

- **if** it is located at less than 50 m from an equipment selected as hazardous following rules explained in paragraphs 1 and 2;
- **AND if** it contains a mass of hazardous substance higher than a reference mass Mc calculated as: $M_c = S_3 \cdot M_b$

$$\text{with} \begin{cases} 0.1 \le S_3 \le 1 \\ S_3 = (0.02 \cdot D)^3 \end{cases}$$

D is the distance (expressed in m) between the two equipment.

S_3 must be included in the interval 0.1 – 1.

$$\left| \begin{array}{llll} 0.1 \le S_3 \le 1 & & & \\ \text{If} & S_3 < 0.1 & \text{then} & S_3 = 0.1 \\ \text{If} & S_3 > 1 & \text{then} & S_3 = 1 \end{array} \right.$$

The result of the method is the selection of relevant hazardous equipment for which the mass of substance is higher or equal to the mass threshold. The selected equipment are studied according to MIMAH.

2.2.4 Discussion

A first visit on site is necessary in order to explain the method for the selection of equipment, to collect the missing data and to discuss with the plant operator about equipment selected a priori.

The method for the selection of equipment must not be applied blindly. If an equipment is judged hazardous due to the presence of an hazardous substance and/or by the operating conditions inside the equipment, it can be selected as a relevant hazardous equipment and studied according to MIMAH, even if the mass in the equipment is lower than the threshold. Moreover, some equipment near the plant boundaries could be selected due to their effects on close targets.

2.3 Develop Bow-ties

2.3.1 Purpose

The purpose of MIMAH is to identify all the potential major accident scenarios which can occur in a process industry.

The main tool on which MIMAH is based, is the **bow-tie** (Figure 3**).** A bow-tie is centred on a critical event. The left part of the bow-tie, named **fault tree**, identifies the possible causes of a critical event. The right part, named **event tree**, identifies the possible consequences of a critical event.

2.3.2 Associate critical events to relevant hazardous equipment (MIMAH Step 4)

Appendix 3 of D.1.C. [1] 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 potential critical events considered in MIMAH:

Table 4: matrix equipment type (EQ) – critical events (CE)

		CE1 Decomposition	CE2 Explosion	CE3 Materials set in motion (entrainment by air)	CE4 Materials set in motion (entrainment by a liquid)	CE5 Start of a fire (LPI)	CE6 Breach on the shell in vapour phase	CE7 Breach on the shell in liquid phase	CE8 Leak from liquid pipe	CE9 Leak from gas pipe	CE10 Catastrophic rupture	CE11 Vessel collapse	CE12 Collapse of the roof
Mass solid storage	EQ1	X	X	X	X	X							
Storage of solid in small packages	EQ2					X					X		
Storage of fluid in small packages	EQ3					X	X	X			X		
Pressure storage	EQ4					X	X	X	X	X	X		
Padded storage	EQ5					X		X	X		X	X	
Atmospheric storage	EQ6					X		X	X		X	X	X
Cryogenic storage	EQ7					X	X	X	X	X	X	X	
Pressure transport equipment	EQ8					X	X	X	X	X	X		
Atmospheric transport equipment	EQ9					X		X	X		X	X	
Pipe	EQ10					X			X	X			
Intermediate storage equipment integrated in the process	EQ11	X	X	X	X	X	X	X	X	X	X	X	X
Equipment devoted to the physical or chemical separation of substances	EQ12					X	X	X	X	X	X		
Equipment involving chemical reactions	EQ13					X	X	X	X	X	X		
Equipment designed for energy production and supply	EQ14					X	X	X	X	X	X		
Packaging equipment	EQ15			X	X	X			X	X			
Other facilities	EQ16					X	X	X	X	X	X		

1 matrix crossing the physical state of the substance considered and the 12 potential critical events :

Table 5: matrix substance state (STAT) – critical events (CE)

		CE1 Decomposition	CE2 Explosion	CE3 Materials set in motion (entrainment by air)	CE4 Materials set in motion (entrainment by a liquid)	CE5 Start of a fire (LPI)	CE6 Breach on the shell in vapour phase	CE7 Breach on the shell in liquid phase	CE8 Leak from liquid pipe	CE9 Leak from gas pipe	CE10 Catastrophic rupture	CE11 Vessel collapse	CE12 Collapse of the roof
Solid	STAT1	X	X	X	X	X	X			X	X		
Liquid	STAT2					X		X	X		X	X	X
Two-phase	STAT3					X	X	X	X	X	X		
Gas / Vapour	STAT4					X	X			X	X		

By crossing these two matrices, it is possible to associate a list of critical events for each hazardous equipment selected in accordance with the state of the handled substance.

2.3.3 For each critical event, build a fault tree (MIMAH Step 5)

MIMAH proposes 14 generic fault trees(*), presented in *Appendix 4 of D.1.C. [1].* The structure and the method of construction of fault trees are given in the *deliverable D.1.C. (MIMAH Step 5) [1]*.

Table 6 presents which fault tree is associated with which critical event.

Table 6: List of generic fault trees 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

Nr CE	Critical event	Generic fault tree (FT)
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

The generic fault trees identified for each critical event 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. Moreover, if other risk assessment methods raise additional causes, these have to be included in the fault tree.

2.3.4 For each critical event, build an event tree (MIMAH Step 6)

For each critical event studied, an event tree(*) is built 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 (risk phrase).

The method for the construction of event trees is fully explained in *Appendix 5 of D.1.C.[1].* It should be noted that an excel file, MIMAH2.xls, is available on the ARAMIS web site, including a program which allows to automatically generate the event trees. The methodology will be explained here according to its main principles.

Firstly of all, for a critical event associated to a selected equipment (see paragraph 2.3.2), it is useful to know which secondary critical event(s) occur(s) after a given critical event. This will depend on the physical state of the handled substance: a same critical event can give rise to different secondary critical events for different substance states. A matrix linking the critical events (CE), the substance state (STAT) and the secondary critical events (SCE) is thus built.

In the same way, matrices linking the secondary critical events (SCE) with the tertiary critical events (TCE), and then tertiary critical events (TCE) and dangerous phenomena (DP) are defined. The crossing is independent of the physical state of the substance.

The list of dangerous phenomena is the following one:

DP1: Poolfire	DP8: Missiles ejection
DP2: Tankfire	DP9: Overpressure generation
DP3: Jetfire	DP10: Fireball
DP4: VCE	DP11: Environmental damage
DP5: Flashfire	DP12: Dust explosion
DP6: Toxic cloud	DP13: Boilover and resulting poolfire
DP7: Fire	

Lastly, the hazardous properties (risk phrases) of the handled substance have to be taken into account in order to select appropriate dangerous phenomena. This selection leads to the deletion of some branches of the event tree. Additional conditions have to be used for that purpose (see *Appendix 5 of D.1.C., paragraph 4 [1]*). The event trees obtained can be modified if some events are not possible for the given equipment and for the actual external/internal conditions.

So, MIMAH 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 (MIMAH Step 7). Each bow-tie represents a major accident hazard which can occur on the selected equipment. The Figure 4 presents an example of a bow-tie centred on the critical event "Breach on shell in liquid phase".

2.3.5 Discussion

The bow-ties associated to each relevant hazardous equipment are major accident hazards, 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 Methodology for the Identification of Reference Accident Scenarios, MIRAS.

During the construction of bow-ties, a second visit on site is recommended to discuss with the operators about the generic bow-ties built with MIMAH which are tools in order to ensure a better exhaustiveness and are used as checklists. The research of real causes and consequences of accidents with the operators can be made from generic bow-ties but also with the help of other risk analysis tools (like HAZOP or other systematic risk analysis methods to identify the possible causes of an accident).

Besides, the HAZOP method seems a complementary method to the proposed generic fault trees in order to identify some possible causes, especially for process equipment. It is also possible to use risk analyses already made on the site.

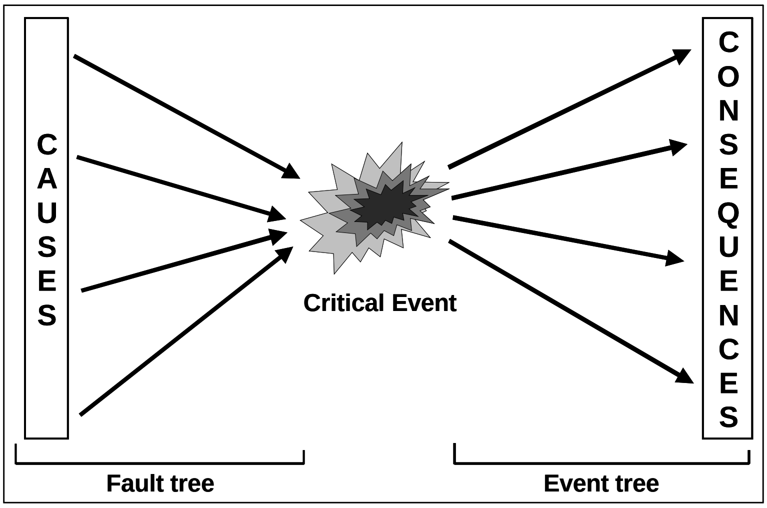


Figure 3 : General scheme of the bow-tie

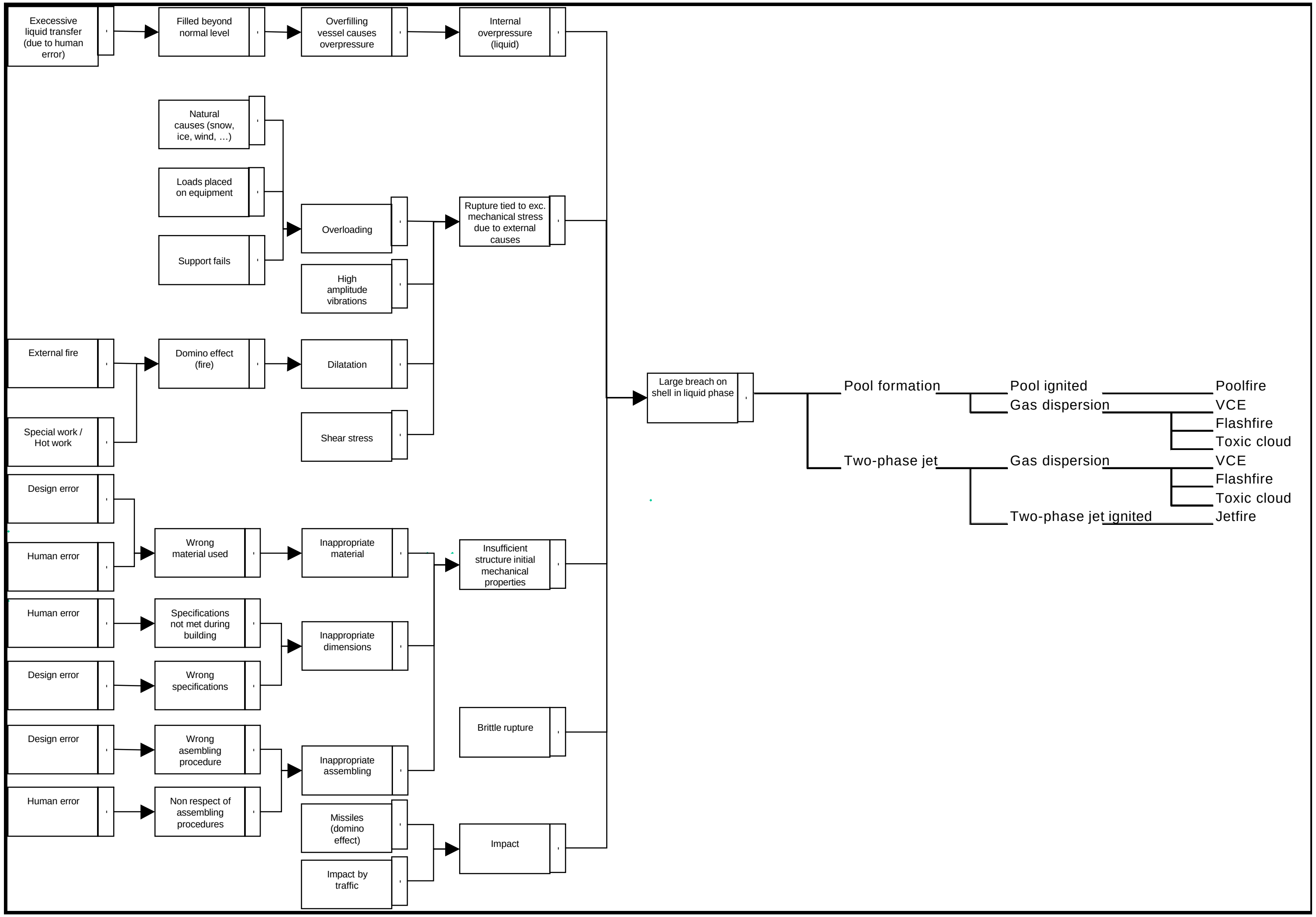


Figure 4:Example of bow-tie

3. Identification of the safety barriers and assessment of their performances

3.1 Purpose

To consider only the major accident scenarios can lead to an over-estimation of the risk level and does not promote the implementation of safety systems. To face this problem, it is necessary to focus on the influence of safety systems and safety management in the definition of accident scenarios. This approach is intended to give an acute estimation of the risk level and to promote the implementation of safety systems.

The purpose of this step is to identify the safety systems which have an influence on the possibility of occurrence of critical events, on the consequences of the accident and to obtain a bow-tie on which safety barriers are placed at the right place. Once the safety barriers have been identified and placed on the bow-tie, it is necessary to assess their performances (level of confidence, efficiency and response time) and to verify if the safety barriers reach the safety requirements to obtain an acceptable risk.

3.2 Identify safety functions and barriers

This step is carried out thanks to the concept of safety functions(*) and safety barriers(*).The safety functions are technical or organisational functions, and not objects. They are expressed in terms of actions to be achieved. Four main verbs of action are defined: **to avoid, to prevent, to control and to limit**. These actions have to be realised thanks to safety barriers. The safety barriers are physical and engineered systems or human actions. The safety function is the **"what"** needed to assure, increase and/or promote safety. The safety barrier is the **"how"** to implement safety functions.

To identify the safety functions and barriers, each event of a bow-tie, branch per branch, must be examined and the following question should be asked: "Is there a safety barrier which avoids, prevents, controls or limits this event ?". If yes, 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 or limits this event, it has to be placed downstream.

3.3 Level of confidence of a safety barrier

The **level of confidence(*) of a safety barrier (LC)** is the probability of failure on demand to perform properly a required safety function according to a given **effectiveness (E)(*)** and **response time (RT)(*)** under all the stated conditions within a stated period of time. Actually, this notion is inspired from the notion of SIL (Safety Integrity Level) defined in IEC 61511 [3] for Safety Instrumented Systems and has been enlarged to all types of safety barriers.

The **level of confidence** will be estimated for a **whole safety barrier** (and not for a single device), including if necessary the different subsystems composing the barrier (detector, treatment system, action). For each subsystem, level of confidence, effectiveness and response time will be estimated and combined to calculate a global level of confidence of the barrier.

A subsystem can be either of type A or of type B. The definition of each type is presented below:

A subsystem is of type A if :

the failure modes of all components are well defined, **AND** the behaviour of the subsystem under fault conditions can be completely determined, **AND** dependable failure data from field experience exists for the subsystem, sufficient to show that the required target failure measure is met.

Example: mechanical devices like valves

A subsystem is of type B if :

the failure mode of at least one component is not well defined, **OR** the behaviour of the subsystem under fault conditions cannot be completely determined, **OR** no dependable failure data from field experience exists for the subsystem, sufficient to show that the required target failure measure is met.

Example: complex systems like processors, subsystem hardware.

To reach a level of confidence, the safety barrier must comply with two criteria, the first one, qualitative (architectural constraints) and the second one, quantitative (probability of dangerous failure).

The qualitative criteria corresponding to architectural constraints for the subsystems (type A and type B) are defined in

Table 7 and

Table 8. These tables are extracted from the IEC 61508 standard [4].

For the type A : all the failure modes are well-known.

Table 7: Architectural constraints for the type A

SFF: **Safe Failure Fraction**	**Fault Tolerance**		
	0	**1**	**2**
< 60%	LC 1	LC 2	LC 3
60% - < 90%	LC 2	LC 3	LC 4
90% - < 99%	LC 3	LC 4	LC 4
≥ 99%	LC 4	LC 4	LC 4

For the type B: all the failure modes are not known

Table 8: Architectural constraints for the type B

SFF: **Safe Failure Fraction**	**Fault Tolerance**		
	0	**1**	**2**
< 60%	Non possible	LC 1	LC 2
60% - < 90%	LC 1	LC 2	LC 3
90% - < 99%	LC 2	LC 3	LC 4
≥ 99%	LC 3	LC 4	LC 4

The quantitative criteria corresponding to the probability of failure for the subsystems (type A and type B) and depending of demand mode of operation are defined in the

Table 9 and Table 10.

Table 9: Level of confidence: failure measures for a safety function, allocated to a safety barrier operating in low demand mode of operation (from IEC 61508)

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

Table 10: Level of confidence: failure measures for a safety function, allocated to a safety barrier operating in high demand or continuous mode of operation (from IEC 61508)

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

The global level of confidence of the whole barrier is equal to the smallest one of the subsystems composing the barrier.

The **effectiveness (E)** 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 **response time (RT)** 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 effectiveness and the response time can not be known by a generic way and are given by data from suppliers, experience, norms, technical guides and data sheets.

The way to assess these three parameters is explained in details in *Appendix 9 of D.1.C. [1]* and some examples are given in the paragraph 3.5. hereunder. Before to assess the performances of safety barriers, each safety barrier identified must meet the following minimum requirements expressed (see Appendix 9 of D.1.C. [1], paragraph 2):

- components of safety barriers must be independent from regulation systems (common failures of safety and regulation systems are not acceptable); this criterion is applicable in case of two systems in place for the same function;
- design of the barriers must be made in appliance with codes, rules... and design must be adapted to the characteristics of the substances and the environment ;
- barriers must be of a “proven” concept, that is to say that the concept is well known (experienced). Otherwise, it may be necessary to perform more tests on site to check the quality of the barrier

- barriers must be tested with a defined frequency. Frequency of the tests will be based on experience of operators or suppliers.
- barriers must have a schedule of preventive maintenance.

The previously assessment of the performance of the barriers including the analysis of the architecture (if barriers independent, safe-failed…), the existence of periodic tests, is important to decide if the safety barriers can be considered as relevant and can be placed on the bow-tie and if their level of confidence can be assessed.

3.4 Set a risk reduction goal

A tool, called "Risk Graph" and based on the principles of the IEC 61508/61511 standards, has been developed. For a given cause in the bow-tie, depending on its frequency of occurrence and its potential consequences (due to the phenomenon the most dangerous which the cause can lead), the required level of confidence of safety barriers for the studied scenario is identified in order to have an acceptable risk.

This tool is fully described and explained in *Appendix 14 of D.1.C. [1]*. The Risk Graph is specially useful in a design phase, in order to evaluate the importance of safety systems which have to be put in place. It can also be used for existing equipment, in order to verify if the safety systems are sufficient to protect the possible scenarios.

The conclusions obtained from the Risk Graph can not be the same than the ones of the Risk Matrix. The Risk Graph considers separately each branch of the bow-tie (from a cause to a dangerous phenomenon). The Risk Matrix considers the set of dangerous phenomena in the bow-tie in aggregating the causes.

3.5 Example

This paragraph gives some examples of levels of confidence for some safety barriers according to the type of barrier: passive, active or human actions.

3.5.1 Passive barriers

The passive barriers are defined as functioning in permanence, not requiring any human actions, energy sources and information sources to achieve their function. In the ARAMIS methodology, it has been decided to allot to any passive barrier a generic Probability of Failure on Demand (PFD), which is a value comparable to a Level of Confidence (LC) but taken out of some accident databases and learnt from accidents.

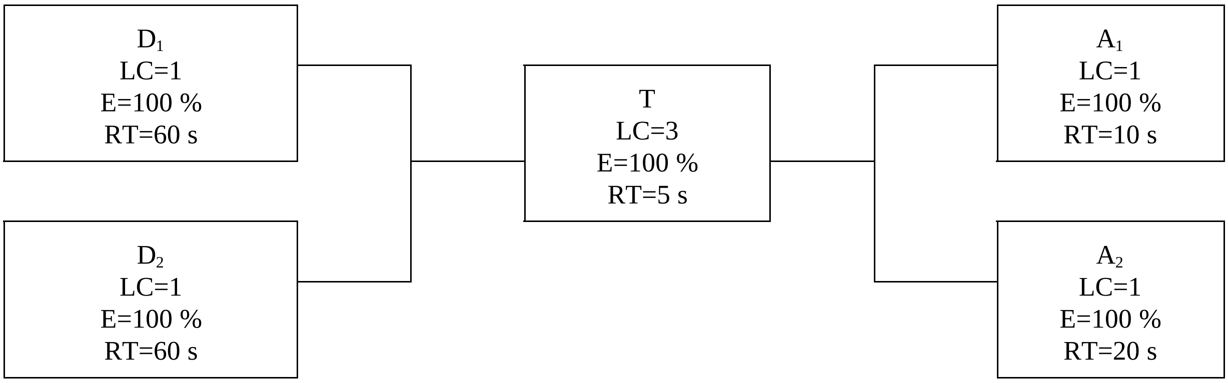
Table 11: Examples of LC for passive barriers

Generic passive safety barrier	PFD from Literature and Industry (no dimension)	Level of Confidence of the barrier
Dike (efficient retention capacity and watertight)	$10^{-2} – 10^{-3}$	2
Fire-proofed wall (efficient maximum duration)/ blast wall / bunker	$10^{-2} – 10^{-3}$	2
Rupture disk (efficient conception pressure and maintenance)		2
Intrinsic safety disposition (thickness, material quality,…) tied to design		4

These levels of confidence for the passive barriers are examples and can be modified by complementary criteria tied to the security management (like the procedures of bund emptying, the maintenance…)

3.5.2 Active barriers

The active barriers are composed of three subsystems in chain: a detection system (D), a treatment system (T) (logic solver, relay, mechanical device, interlock, human…) and an action (A) (mechanical, instrumented, human…). Figure 5 gives a generic example of combination of LC for one specific safety barrier.



LC = 1 (E=100 %, RT=75 s) or
LC = 2 (E= 100 %, RT=85 s)

Figure 5: Generic configuration for LC combinations

Some examples of values of level of confidence, effectiveness, response time for given subsystems are presented in Table 12. Effectiveness and response time must be adapted for each plant.

Table 12: Examples of LC, E and RT for subsystems

System	LC	Response time	Eff
Safety shut-off valve	1	10 to 50 s (1)	100%
Auto-tested valve	2		
Safety relief valve *(2)*	1 *(2)*		
Pressure switch	1	< 5 s	
Extraction fan	1	< 30 s	
Gas Sensor in confined zone	/	15 s to 1,5 min (3)	100%
Classical Relay	1	< 5 s	100%
Safety Programmable Logic Controler (certified)	See its certification	< 5 s	100%

(1) The value depends on the type and on the operating conditions of the system

(2) For safety relief valve, the value of 2 is generally adopted

(3) The value depends on the type of gas

3.5.3 Human actions

As for the passive barriers, the principles of IEC 61508/61511 standards for the assessment of level of confidence can not therefore be applied. In the ARAMIS methodology, it has been decided to associate to human actions a generic probability of failure on demand (PFD), which is derived in an equivalent level of confidence (LC).

Table 13: Examples of LC for human actions

Human barriers	PFD (from literature, industry)	Level of confidence
Prevention	10^{-2} (PFD)	LC 2
Normal operation	10^{-2} (PFD)	LC 2
Intervention	10^{-1} (PFD)	LC 1

These levels of confidence for the human barriers are examples. Some other criteria can modify this level of confidence (like the time needed to the operator to act, the stress generated by the intervention,…)

3.6 Discussion

The **identification of safety barriers** to be placed on the bow-ties can (should) be made with the plant operator (workers, safety officers …) during the second visit on site, with the help of "process and instrumentation diagrams" and "flow diagrams" or with any other existing documentation.

A checklist, available in *Appendix 8 of D.1.C.[1],* helps the reader to identify the functions and barriers in the bow-ties. It 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 according to the **"Risk Graph"**.

Moreover, it should be stressed that, in a first step, the level of confidence assessed with the help of instruction given in Appendix 9 of D.1.C. is the **"design" level of confidence**. This means that the barrier is supposed to be as efficient as when it was installed. But the performances of the safety barrier could decrease when time is going according to the quality of the safety management system.

In a second step, it is thus needed to classify the safety barriers identified according to the typology shown in *Table 10 of D.1.C. (MIRAS Step 3.B.) [1]*. This typology is used to assess the influence of the safety management system on the performances of safety barriers. The reader should then refer to the paragraph 4 dealing with the assessment of the safety management system for further details.

4. Evaluation of the influence of safety management efficiency on barrier reliability

4.1 Purpose

Safety management* applied in a Major Accident Prevention Policy leads to the definition of actions related to technical, human and organisational factors. The operational goal of safety management is to provide and maintain the barriers (being technical or behavioural) at a maximum level of effectiveness, as defined in their specification. The barriers' effectiveness depends on the organisational and management framework (maintenance, adequacy of procedures, education, safety attitudes of personnel, etc) against accidents. Safety management contains a large number of responsibilities, tasks and functions.

Safety management affects the probability of occurrence of the scenarios. Therefore the purpose of evaluating safety management is to assess the effectiveness of safety management in preventing accidents.

In the ARAMIS project, the activity of minimising risks is considered to be performed mainly by means of the concept of implementing and maintaining safety barriers. So safety management includes:

- Hazard and risk analysis, in order to identify and understand hazards and risks; and
- Selection, implementation and maintenance of safety barriers, as the means of minimising the risks.

The MIRAS methodology (see the chapter 5) based on generic fault and event trees (bowties) assists the risk analysis process in a Seveso-II establishment. Part of the outcome of the risk analysis activity is the identification of existing safety barriers, and (if applicable) identification of the need to implement further safety barriers.

When all necessary safety barriers are identified and selected, the next task of safety management is to ensure the effectiveness of the safety barriers during their lifetime, i.e. the life cycle of the barriers needs to be managed.

4.2 The ARAMIS safety management evaluation concept

The ARAMIS methodology for assessment of **safety management*** is based on a concept that recognises a number of structural elements in the **safety management system*** and the influence of a number of **safety culture*** factors. This concept is described in chapter 2 of "Methodology to determine a Safety Management Efficiency Index - Deliverable D.3.B"*[5]*.

The structural factors and the relation with the life cycle of a specific **safety barrier*** can be visualised as in Figure 6. In order to fulfil the functions corresponding to each of the structural factors, the safety management system needs to include a "**delivery system***" for each structural factor. The assessment of the structural factors is carried out by means of a safety **audit***. The audit addresses the elements 1 and 3 to 10 of Figure 6 explicitly, while a "mapping" exercise is performed to elicit the distribution of responsibilities (element 2). This "mapping" identifies what parts – of the site-dependent implementation - of the safety management system deal with the delivery systems as identified in Figure 6.

The structural factors of safety management are discussed in detail in chapter 2 and 3 of "Methodology to determine a Safety Management Efficiency Index - Deliverable D.3.B"*[5]*, and in the ARAMIS Audit Manual (Annex A to the above mentioned report). The steps or "boxes" in the separate delivery systems are described in the ARAMIS Audit Manual.

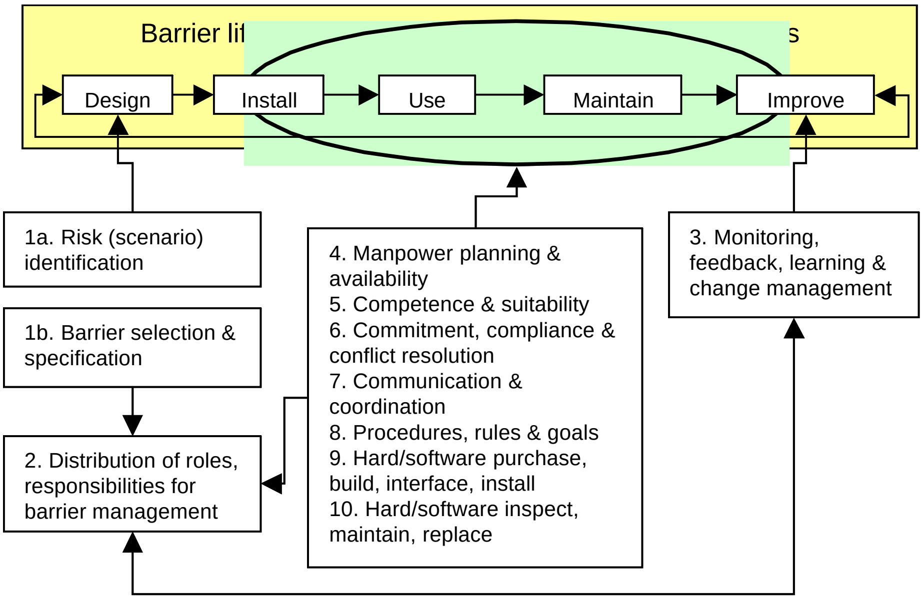


Figure 6 : Structural elements of the safety management organisation in relation to the task of managing the life cycle of safety barriers. The ellipse indicates the focus of the assessment with respect to identifying the effectiveness of safety barriers.

The safety management system or structure includes the principles (policies), plans, responsibilities, etc. It provides the top-down formal framework for safety management. A good safety management structure is a necessary condition for effective safety management. But effective safety management will also depend on the informal beliefs, norms and practices, i.e. the **safety culture*** of the work force (bottom-up). The safety culture determines how well the scheduled tasks and procedures are performed and adhered to.

Therefore, safety culture is another issue included in the safety management evaluation. In conjunction with the structural elements of the organisation's safety management, we recognise that there is a set of safety-culture elements that affect how well the safety management functions are performed. We recognise the following set of eight cultural factors:

Learning and willingness to report. This is a broad factor that comprises employees' willingness / reluctance to report accidents and incidents, their perception of feedback from reporting and dissemination of lessons learned. It overlaps with trust in leadership with regard to "just culture". Associated with this factor are single items that may reveal why reporting is not satisfactory: reasons for not reporting.

Safety prioritisation, rules and compliance. This broad factor comprises several factors and single indicators including use of and familiarity with rules and instructions; the prioritisation of safety versus productivity and ease of work; the extent to which and the circumstances under which safety procedures may be violated

Leadership involvement and commitment. This dimension concerns both the avowed involvement and commitment of management and supervisors and team leaders as well as employee perception of their commitment and involvement

Risk and human performance limitation perception. This factor, the items of which may vary according to the type of work domain, concerns management and employee awareness of hazards, risks and human error potentials (fatigue, automation etc.) relevant to their work.

Felt responsibility. This factor concerns employee perception of who is responsible for safety at work including felt ownership of responsibility

Trust and fairness. This factor involves management's trust in employees and, crucially, employees' trust in top management's and their immediate leader's and employee perception of fairness in the workplace

Work team atmosphere and support. This is a broad factor that comprises employees' perception of teamwork and the 'spirit' in their respective teams; the extent to which the team gives its members support and help; and the extent to which respondents are willing to speak up and warn each other of dangers.

Motivation, influence and involvement. This broad factor comprises four batteries concerned with perceptions of (i) work as meaningful; (ii) own influence on work planning and execution; (iii) motivation and involvement; and (iv) feeling informed and finding work predictable

The evaluation of safety management of a specific hazardous site is performed by a combination of:

1. An audit of the safety management system using the concept of the 10 structural elements and focussing on how the site-dependent safety management system addresses a set of selected, representative safety barriers (i.e. it is concretised in relation to real, existing on-site safety barriers), and
2. A questionnaire-based investigation of the safety culture among the employees of the site.

The next chapter describes step-by-step the activities to perform the evaluation and the required documentation.

4.3 Stepwise description of the evaluation process

The evaluation process is visualised in a flow chart in Figure 7. The steps are described in the following sections.

4.3.1 Step 1 Collect all barriers and nominal LC values

The safety management evaluation builds on the risk analysis performed using the MIRAS methodology (see chapter 5). MIRAS produces a list of accident scenarios (visualised by bowties) and identifies safety barriers. For these barriers the “design” **Level of Confidence*** is assessed (see Annex 9 to D.1.C *[1]*). This information is the input to the safety management evaluation process.

4.3.2 Step 2 Classify barriers

The safety management actions necessary to implement and maintain a barrier depend on the properties of the barrier and what elements constitute the barrier (hardware, software, or human behaviour). As a consequence, the assessment of safety management needs to consider these barrier properties; therefore a classification scheme for safety barriers is set up that groups barriers together. The classification scheme is presented in Table 14. This scheme is identical to the table included in MIRAS (Table 10 in D.1.C *[1]*), and the tables in the ARAMIS Audit Manual. Experience from the test cases indicated that the classification is not trivial – the descriptions in the table included herein are slightly extended to accommodate for some of the difficulties.

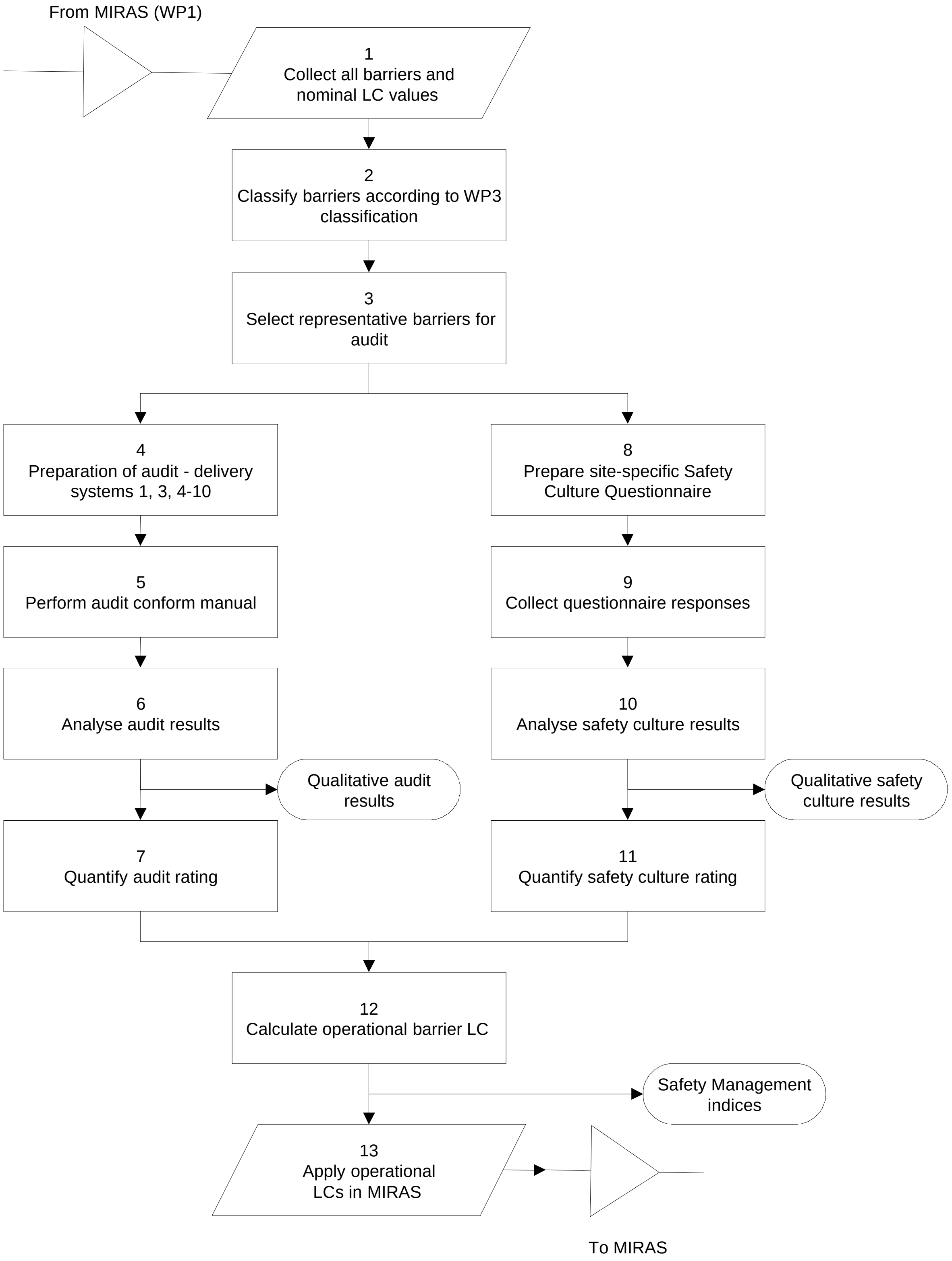


Figure 7 : Flowchart of the safety management evaluation

Table 14 : Classification of barriers in the ARAMIS safety management evaluation.

	Barrier	Examples	Detect	Diagnose/ Activate	Act
1	*Permanent – passive – control*[1]	Wall of pipe, hose or tank; anti-corrosion paint; tank support; floating tank lid; flange connection; seals; viewing port in vessel	None	None	Hardware
2	*Permanent – passive – barrier*	Tank bund, dyke, drainage sump, railing, fence, blast wall, lightning conductor,	None	None	Hardware
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 or cooling system, ventilation, system to maintain inert gas in equipment.	None	None (may need activation by operator for certain process phases)	Hardware
5	*Activated – hardware on demand – barrier or control*	Pressure relief valve, interlock with “hard” logic, sprinkler installation, electro-mechanic pressure, temperature or level control	Hardware	Hardware	Hardware
6	*Activated – automated*	Programmable automated device, control system or shutdown system	Hardware	Software	Hardware

---

[1] The difference between “control” and “barrier” follows from the terminology of the (MORT) methodology[6]. A control is acomponent that is necessary to perform the primary process, but which serves also to control hazards (e.g. a pipe wall, a level control), a barrier is a component that is installed solely to prevent or mitigate hazards (a tank bund, a pressure relief valve).

(Table continued)

7	*Activated – manual* Human action triggered by active hardware detection(s)	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 (Skill-, Rule- or Knowledge-based)	Human/ remote control
8	*Activated – warned* Human action based on passive warning	Donning personal protection equipment in danger area, refraining from smoking, keeping within white lines, opening labelled pipe, keeping out of prohibited areas	Hardware	Human (Rule-based)	Human
9	*Activated – assisted* Software presents diagnosis to the operator	Using an expert system	Hardware	Software – human (Rule- or Knowledge-based)	Human/ remote control
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 (Skill- or Rule-based)	Human/ remote control
11	*Activated – emergency* Ad-hoc observation of deviation + improvisation of response	Response to unexpected emergency, improvised jury-rig during maintenance, fight fire	Human	Human (Knowledge-based)	Human/ remote control

The classification should be done for all identified barriers, because it is necessary to know the classification in order to calculate the operational **level of confidence*** during step 12**.**

The classification needs to be performed with care. Difficulties arise easily. Bursting plates are often classified as passive barriers, but in fact they need to be activated (pressure above burst-pressure to rupture the material) in order to perform their safety function, so they can be classified as class 5. An inert gas above a flammable liquid can be considered as a passive barrier (class 2) but it is required to be put in place after filling or other handling operations, and a system is required to provide, distribute, and purge the inert gas, so classifications as class 3 or 4 may be correct. In case of doubt, the barrier classification be based on which safety management structures (delivery systems) are most important for the implementation and maintenance of the barrier in question. The relation between the barrier and the relevant parts of the safety management structure – and thus the corresponding elements of the audit - are depicted in Figure 8.

4.3.3 Step 3 : Select representative barriers for the audit

The management of each scenario and every barrier cannot be assessed because it would generally take too much time. A responsible choice should be made, based on severity and impact.

The result of this step is a set of scenarios and barriers that serves as a point of reference for the audit. The quality of management of these barriers will be assessed during the audit and will be generalised to the whole barrier management system and will be quantified subsequently.

This step is discussed in detail in the ARAMIS Audit Manual as Step 1 of the audit process.

The classification in Table 14 should be used as basis for this choice of barriers and at least one example from each category should be used as example by the different delivery systems for which it is significant. Some guidance on this is as follows (numbers are those indicating type of barrier in Table 14 – where numbers are separated with a slash (/), an example can be chosen out of either of the two [or one of the several] types):

- For the **hardware** life cycle protocols at least the following types: 1, 2, 3, 4, 5, 6/9, 7, 8
- For **procedures** and **commitment**: 3/8, 7/10, 9, 11
- For **competence**: at least one at each level of Skill/Rule/Knowledge
- For **communication**: 3/7/9/10/11 requiring coordinated action of more than one person
- For **availability**: 3, 7/10, 11

Figure 8 shows which delivery systems, and therewith which audit activities, are important for the different types of barriers. Barriers consist often on several elements, and a reasonable choice has to be made what elements will be addressed during the audit for each selected barrier.

If the barrier is made up of active hardware the emphasis must be on inspection, monitoring and adjustment.

If the barrier consists of passive hardware elements the audit should almost exclusively concentrate on construction and installation, with some concern for maintenance, to ensure the passive barrier is not compromised by modifications and is kept functioning to specifications.

If the barrier has behavioural elements these can be audited using the behavioural delivery systems:

- The procedures, which describe the required behavioural in relation to the barrier
- The availability of individuals whose required behaviour forms (an element of) the barrier function
- The competence of individuals to carry out the required behaviour
- The commitment of individuals to carry out the required behaviour at the right moment, with the right care and alertness in order to control the risk
- The necessary communication and coordination in cases where more than one individual's behaviour is responsible for the effectiveness of the barrier.

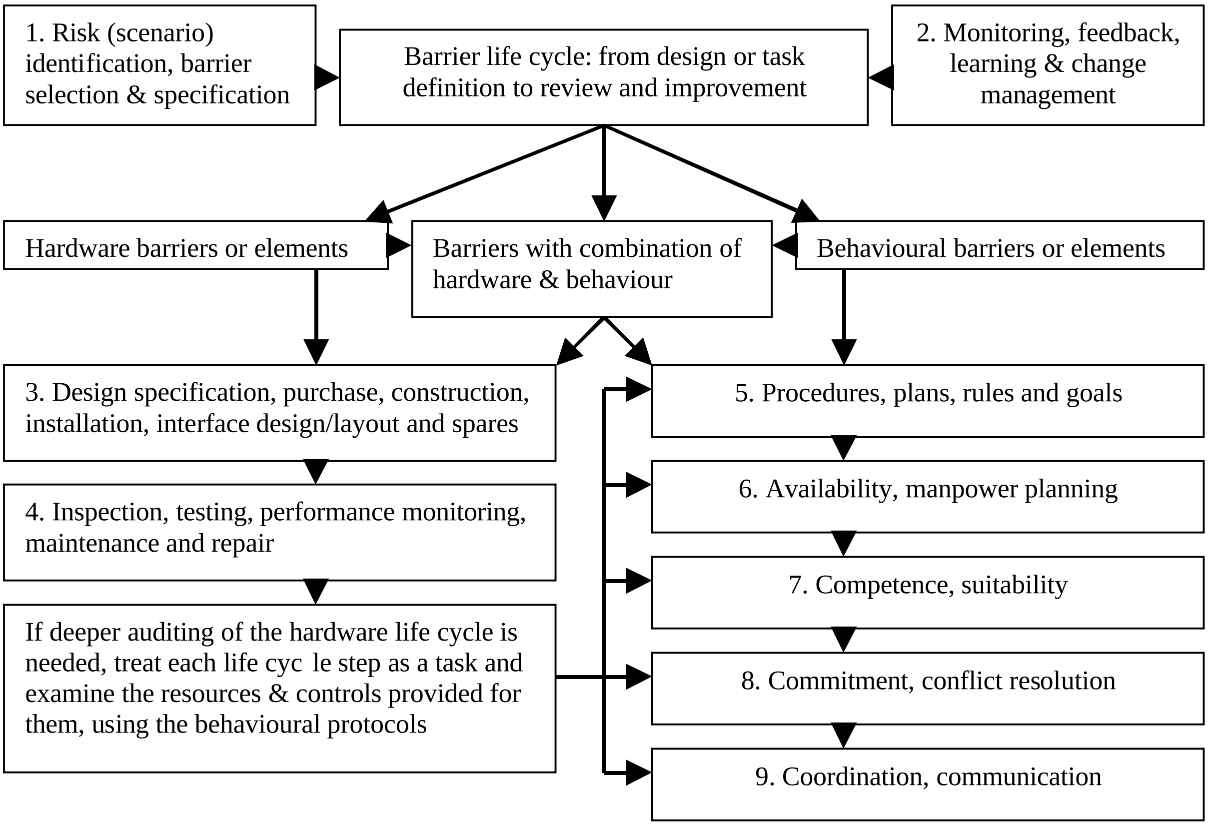


Figure 8 : The relationship of barrier types and management influences for installed, existing barriers.

4.3.4 Step 4 : Prepare the audit

The most important activity for the preparation of the audit is the mapping of the company's specific safety management system on the ARAMIS safety management structure. It involves the linking of the different components of the ARAMIS audit depicted in Figure 6 to the relevant parts of the Safety Management System of the company under investigation.

The mapping should be based on documentation of the company, as well as interviews conducted during the pre-audit visit. The interviews are needed either to verify the audit team's initial impressions or to add to the information from the available documentation if this does not provide enough information to conduct the mapping exercise. The mapping should make clear *who* will be asked *what* during the audit.

The mapping is described in detail in the ARAMIS Audit manual as step 2 of the audit process.

4.3.5 Step 5 : Perform the audit.

The ARAMIS audit covers four areas that are separated in the ARAMIS barrier management system structure (Figure 6 and Figure 8). It depends on the particular company that is assessed to what extent these areas are also managed by different local safety systems. The mapping performed in the previous step should have provided a clear picture of the distribution of these areas of safety management at the plant.

The four areas of assessment are:

1. Audit of the process by which the decisions were arrived at for choosing the barriers
2. Audit of the hardware (aspects of the) barriers using the life cycle steps, and going, where necessary, into the relevant delivery systems associated with them
3. Audit of the behavioural/procedural barriers using the relevant delivery systems
4. Audit of the learning and change management system

The auditor may decide not to separate topics 2 and 3 when actually conducting the audit, especially when dealing with the operation of barriers with both hardware and behavioural elements.

This step is described in detail in the ARAMIS Audit Manual as step 3 of the audit process, and uses the descriptions of the delivery systems in the annexes 2 to 10 and the tools (annex 11) of the ARAMIS Audit Manual.

4.3.6 Step 6 : Analysis of the audit results

The assessment should include an evaluation of the quality of the choices the company has made for fulfilling each of the safety functions that has been identified in the chosen scenarios. In other words, has the company used state-of-the-art techniques in controlling the company-specific hazards. This would mean that the probability of barrier failure is As Low As Reasonably Achievable (ALARA principle) using available technology and non-excessive costs.

The audit addresses the "boxes" (see the description of the delivery systems in the annexes 2 to 10 of the ARAMIS Audit Manual) and the links between them. The quality of these boxes and links is expressed on (preferably) a five-point scale. Results are visualised by colour-coding the graphs displaying the delivery systems (green=best, red=worst, in the manual there is a proposal to reduce the five-point scale to a three-point colour scale). This colour coding provides a qualitative feedback to the company, together with a (written) list of specific findings of the audit team. The feed back to the company is described in section 7 of the ARAMIS Audit Manual. The report on the audit is described in section 9 of the ARAMIS Audit Manual.

It should be stressed, that the qualitative results of the audit may be more relevant to the company (and other stakeholders, like the Competent Authorities) than the quantification, as the qualitative results provide immediate information on specific safety management issues that can be improved or should be altered.

4.3.7 Step 7 : Quantification of the audit results

In order to evaluate the impact of safety management on the risk level of the site, the results of the audit are quantified. The evaluation addresses an existing plant site with existing, installed safety barriers; this means that the focus is on the safety management delivery systems that affect the operational safety of the plant (see the ellipse in Figure 6). This excludes "risk analysis" and "learning and change" and leaves seven elements with direct impact on the Level of Confidence of the safety barriers (see Figure 8).

The audit process leads to a rating on a qualitative 5-point scale for the individual boxes within the delivery systems. This scale is transposed to a numerical rating with equal distance between the qualitative ranks, where the best rank corresponds to a numerical rating of 100%, and the worst rank corresponds to a numerical rating of 20%.

For the rating of the delivery system as a whole, the ratings of the individual boxes are combined. This is done in the following way: A number of delivery systems contains one or two "dominant" boxes. For these delivery systems, the rating is expressed as:

Rating delivery system as a whole = Lowest value of:

The lowest rating of any dominant box;

The average of ratings of all boxes.

For those boxes where no dominant boxes identified, the rating is the average of the ratings of all boxes.

Now there is one group of delivery systems where all boxes are assumed to contribute equally to the failure of the delivery system, these delivery systems are:

a. Manpower planning

b. Communication

c. Purchase/install

And there is one group of delivery systems where a few boxes are assumed to contribute dominantly to the failure of the delivery system:

d. Procedures (*box 5*: communicate, train, execute rules; and *box 8*: evaluate rule effectiveness)

e. Competence (*box 2*: define suitability & competence needed for behaviour)

f. Commitment (*box 2*: assess & modify behavioural antecedents & consequences)

g. Inspect & maintain (*box 2*: define maintenance concepts & plans; and *box 7*: execute maintenance & repair)

The result of this step is a numerical rating between 20% and 100% of all the seven elements that are assumed to have a direct impact on the Level of Confidence of the safety barriers. These are shown again here:

1. Manpower planning & availability
2. Competence & suitability
3. Commitment, compliance & conflict resolution
4. Communication & coordination
5. Procedures, rules & goals
6. Hard/software purchase, build, interface, install
7. Hard/software inspect, maintain, replace

The numerical ratings are denoted S_1 to S_7 for later reference. An Excel tool is provided (http://aramis.jrc.it), work sheet 1 in the “ARAMIS rating sheet.xls”, that transfers the ratings per box (on a scale from 1 to 5, 5 being the “best” rating) to the numerical ratings S_1 to S_7.

4.3.8 Step 8 : prepare a site specific Safety Culture Questionnaire

Annex B to “Methodology to determine a Safety Management Efficiency Index - Deliverable D.3.B” contains the generic “Safety Culture Questionnaire for Process Industries” (**SCQPI***) This questionnaire is available in different languages (English, French, Danish, Dutch, Slovenian and Czech). The questionnaire needs to be adjusted at some minor points before it can be distributed to the employees of the plant. These adjustments are the following:

- Name, function, phone number of the on-site responsible person for the survey (on page 1 of the questionnaire)
- It should be checked that the terminology used for different types of incidents and accidents correspond with the (reporting) practice at the site (page 2)
- Under Items 7 and 8, the locally used names at the site for: *supervisor / shop floor manager*, *safety engineer/officer*, *work group leader / team leader*, and *the work group / the team* need to be inserted (page 4 and 5)

- It is possible to add a number of open questions on specific items, but these require separate analysis.
- The demographic section should be adjusted to suit the target plant, and care should be made not to request information which, in combination, may jeopardise the anonymity of responses

The employees that will answer the questionnaire investigation need to be selected. On one hand, the group (s) should be large enough to obtain statistically significant results, i.e. individual groups (work teams, shifts, or employees with similar functions or positions) should be no smaller than 15 persons (also to guarantee that individual responses can not be identified), on the other hand. large groups require more resources (time of the employees – though the time required for analysis depends only on the number of groups that may be of interest to compare).

In principle all employees that work at or in direct relation to the hazardous equipment should be included in the investigation, i.e. field and control-room operators, maintenance and cleaning personnel, engineers, etc. It may be useful to identify responses from different groups in order to develop effective management intervention, and therefore, the groups to be compared should be listed in the demographic section. However, differences among groups at a given site do not enter into the computation of the ARAMIS safety culture index.

The conditions for filling out and returning the questionnaire need to be made very clear to the employees. These conditions include:

- All responses are anonymous
- No information at individual level will be reported
- Feedback will be given to employees about the results of the safety culture survey

It can be beneficial to include the support from union officials from the plant in order to obtain the co-operation and interest from the employees. The primary objective of the questionnaire is to collect information that can be used to improve the safety performance of the plant (adequate protection for the life and health of workers in all occupations, is one of the purposes of the unions).

4.3.9 Step 9 : Collect questionnaire responses

The most efficient approach for collecting questionnaire responses is by arranging one or more sessions for (different groups of) the employees where, during about one hour, the employees may fill in their answers in the questionnaires and return them directly. The response rate decreases drastically when the questionnaires are filled out home on a voluntary basis and are returned by (pre-paid postage) mail or submitted in identical envelopes to collection boxes at the plant.

4.3.10 Step 10 : Analysis of safety culture results

Responses to each of the single questions will be given in the form of level of agreement (or similar) on a five-point rating scale. The results are reported by presenting the distribution of the answers over the five-point scales graphically, grouped in batteries. It is recommended that results of a survey be compared with the results from the ARAMIS five-site reference sample (N=255).

By comparing the results with the reference group, relative strengths and weaknesses in the safety culture may be identified, and the company can use this information to address possible causes and conditions for particular findings, and develop intervention measures to remedy those.

It should be stressed, that the qualitative results of the safety culture investigation may be more relevant to the company (and other stakeholders, like the Competent Authorities) than the quantification, as the qualitative results provide immediate information on specific safety management issues that, e.g. can be improved or should be altered.

4.3.11 Step 11 : Quantify the safety culture rating

The following steps contain the instructions for computing the Safety Culture Index $S_0{}^k$, for a given new sample *k*. In Table Table 15 is provided a table of means and standard deviations obtained from the five-site European reference sample.

The following abbreviations are used:

μ_i^{REF} = the mean of the *i'th* item of the reference sample (the five test cases)

σ_i^{REF} = the standard deviation of the *i'th* item of the reference sample

μ_i^{NEW} = the mean of the *i'th* item of some new target sample

Steps

1. Responses to each item (question) of the questionnaire groups 1, 3, 5, 6, 9, 10, 11 shall be coded into a scale of 1, 2, ... 5 in the following way [groups 2, 4, 7, and 8 do not count towards the safety culture index; similarly, item 3.14 shall also be excluded]: For all items, assign 1 to the left-most response value “strongly agree” or “to a very high degree”, 2 to the second, and finally 5 to the right most value. For items 1.9, 3.6, 3.7, 3.8, 3.9, 3.10, 3.11, 3.12, 3.13, 5.6, 5.7, 6.2, 9.1, 9.3, 9.8, 9.9, 9.10, 10.7, the assignment shall be reversed so that “strongly agree” and “to a very high degree” are assigned to 1, and so on. The reversal will ensure that the direction of positive and negative response values in terms of attitudes and perceptions.

2. For each item *i*, compute the sample mean μ_i^{NEW}

3. Based on the reference sample data of Appendix A containing, for each item, the mean and the standard deviation, the y-score of the target sample shall be computed as follows. First, the y-score for each item *i* is computed:

   $$y_i^{NEW} = (\mu_i^{NEW} - \mu_i^{REF}) / \sigma_i^{REF}$$

   from which the mean y-score Y^{NEW} for all items can be produced

   $$Y^{NEW} = 1/71 \cdot \sum_{1=i}^{71} y_i^{NEW}$$

4. Finally, the transformation of the y-score of the target sample *k* to the Safety Culture Index, $S_0{}^k$ is made as follows :

   $S_0{}^k = 1$ if $Y^{NEW} \geq 1$;

$S_0^{\,k} = 0.25 \cdot Y^{NEW} + 0.75$ if $-3 < Y^{NEW} < 1$;

$S_0^{\,k} = 0$ if $Y^{NEW} \leq -3$

(It may be noted that for the reference sample the Safety Culture Index, $S_0^{\,REF} = 0.75$ *by definition).*

Table 15 : means and standard deviations for items (questions) of the ARAMIS safety culture questionnaire obtained from the case studies

Item no. *	Mean	Std. Deviation	Item no. *	Mean	Std. Deviation	Item no. *	Mean	Std. Deviation
Item01.1	2,159	0,985	Item05.1	1,836	0,740	Item10.1	2,600	0,921
Item01.2	1,659	0,676	Item05.2	1,940	0,660	Item10.2	2,756	0,929
Item01.3	1,823	0,815	Item05.3	2,060	0,778	Item10.3	2,302	0,757
Item01.4	1,740	0,689	Item05.4	2,506	0,894	Item10.4	2,300	0,780
Item01.5	2,043	0,811	Item05.5	2,720	0,787	Item10.5	2,298	0,777
Item01.6	2,097	0,852	Rev05.6	2,390	0,966	Item10.6	2,541	0,910
Item01.7	2,664	0,913	Rev05.7	2,308	0,988	Rev10.07	2,808	0,919
Item01.8	2,492	1,039	Item06.1	2,520	0,902	Item10.8	2,480	0,841
Rev01.9	2,669	1,008	Rev06.2	2,484	0,842	Item11.1	2,622	0,998
Item01.10	2,332	0,872	Item06.3	2,344	0,777	Item11.2	3,317	0,915
Item01.11	2,068	0,869	Item06.4	2,534	0,966	Item11.3	3,162	0,910
Item01.12	2,574	0,850	Item06.5	2,404	0,756	Item11.4	2,980	0,994
Item03.1	1,853	0,617	Item06.6	2,716	0,833	Item11.5	2,177	0,715
Item03.2	2,376	0,815	Rev09.1	2,855	1,006	Item11.6	2,045	0,621
Item03.3	2,204	0,842	Item09.2	2,414	0,834	Item11.7	2,052	0,752
Item03.4	2,321	0,886	Item09.3	3,590	0,938	Item11.8	2,967	0,927
Item03.5	2,641	0,959	Item09.4	2,258	0,886	Item11.9	2,544	0,768
Rev03.6	2,679	1,084	Item09.5	2,265	0,784	Item11.10	2,492	0,942
Rev03.7	2,353	1,029	Item09.6	2,602	0,842	Item11.11	2,722	0,990
Rev03.8	2,131	0,987	Item09.7	2,237	0,765	Item11.12	2,801	0,989
Rev03.9	2,702	1,050	Rev09.8	2,270	0,914	Item11.13	2,269	0,845
Rev03.10	2,438	1,043	Rev09.9	2,258	0,798			
Rev03.11	2,151	0,934	Rev09.9	2,258	0,798			
Rev03.12	2,810	1,050	Rev09.10	2,177	1,024			
Rev03.13	2,737	0,981	Item09.11	2,500	0,800			
			Item09.12	2,691	0,873			

(*"Rev" = item for which response values have been reversed)

4.3.12 Step 12 : Calculate the operational Level of Confidence of the barriers

The **design*** (also referred to as *nominal* or *optimal*) **Level of Confidence*** or SIL (**Safety Integrity Level***) in the case of hardware barriers or an equivalent generic performance level in the case of behavioural barriers should be allocated to the actually implemented barriers. This figure will anchor the safety management assessment. The assessment of the structural and cultural elements will lead to a rating of the extent to which the management system elements fail to meet the requirements. This means that for safety culture and any of the 7 distinguished delivery systems, a rating of the performance compared to optimal performance will be given, leading to the set of values (management indexes) S_i. The simplest model for the operational LC for a safety barrier (or safety barrier component[2]) of type *k* is the following:

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

Here S_i represents the final rating for the delivery corresponding to structural element *i* including audit and safety culture assessments, $B_{i,k}$ represents an array of weight factors linking the importance of the delivery system *i* to the barrier type *k* in question, with $B_{i,k} \geq 0$ for all *k* and *i* (If sum over Bi larger than 1, then the result has to be maximized to 0).

With this result, and remembering that the LC is defined as $LC = -{}^{10}\log(PFD)$, the expected frequency of all relevant accident scenarios can be reviewed using the actual probabilities of failures on demand of the barriers that are identified in the bowtie. These expected frequencies include the assessment of the safety management system.

An Excel tool is provided, work sheet 2 in the “ARAMIS rating sheet.xls”, that transfers the ratings (from step 7 and 11 above) to the reduction in Level of Confidence for any of the eleven types of barriers **(for the time being, the weight matrix included in this tool is for exploratory exercises only!)**

4.3.13 Step 13 : Apply the operational Level of Confidence in the risk assessment methodology (MIRAS)

For all barriers that are included in the scenarios recognised by MIRAS, the reduction in design Level of Confidence can be calculated using step 12. The resulting *operational* Levels of Confidence will then be used in the calculation of the expected frequency of the accident scenarios. The final result presents the risk level of the company including the evaluation of the safety management.

4.4 Example

As an example, the following tables present rating sheets for one of the case studies. The grey cells in the sheets are the cells where the findings of the audit team are put in. The totals provide the rating (in percent of best performance) per delivery system (“risk analysis” and “learning” are not considered explicitly in the barrier analysis, and quantification is not provided here).

The next table provides the “ARAMIS Safety Management Efficiency Calculation” for a relief valve (barrier type 5) with a design Level of Confidence of 3. The results from the audit rating are automatically transferred to a reduction of the Level of Confidence to 2.7. (the result from

---

[2] The probability of failure on demand of a barrier is approximately (rare event approximation) the sum of the probabilities of failure on demand of the serial barrier components.

the Safety Culture investigation has to be included manually in the green cell). **The reduction of course depend on the weight factors B, which is set to 50% for both "purchase and installation" and "inspection and maintenance" for the sake of this example. The final weight factors have to be defined by means of (among others) expert opinion.**

Table 16 : Rating sheet filed with the results from one case study (first half)

ARAMIS Delivery system	Step No.	Steps	Rating (1-5)
Distribution of roles, responsibilities for barrier management		***Quantification not necessary***	
	1	Make inventory of primary & secondary business processes	4
	2	Identify accident scenarios	4
	3	Prioritise (quantify) risk per scenario	4
	4	Identify required safety functions	4
	5	Allocate barrier functions on grounds of HF & effectiveness	4
	6	Specify appropriate & effective barriers & define performance criteria and working conditions (LCA) for them	4
	7	Plan and provide resources for barrier life cycle effectiveness	4
	8	Monitor barrier performance, evaluate and learn	
Monitoring, feedback, learning & change management		***Quantification not necessary***	
	1	Collect information over state of the art of barrier design & management	4
	2	Record barrier state & performance	5
	3	Record incidents & accidents with, & failures of barriers & management	4
	4	Audit management system relating to barrier performance	2
	5	Assess data & propose changes in barrier choice, design & management	5
	6	Inventory of plans for changes in processes	5
	7	Assess risks of proposed changes & need for (changed) barriers	5
	8	Inventory of plans for organisational changes	
	9	Assess risks of proposed changes for allocation of tasks related to barriers	3
	10	Decide on changes, implement & evaluate	4

ARAMIS Delivery system	Step No.	Steps	Rating (1-5)
1 Manpower planning & availability		**Total:**	**100%**
	1	Assess manpower needs for tasks	5
	2	Plan to match supply & demand	5
	3	Identify pool of contractors	5
	4	Hire pool of own staff	5
	5	Hire contractors	5
	6	Rooster staff/contractors including holiday etc. coverage	5
	7	Arrange emergency cover & call-out	5
	8	Evaluate manpower plan & learn	5
2 Competence & suitability		**Total:**	**86%**
	1	Task analysis of behaviour as element of barrier or its management	4
	2	Define suitability & competence needs for behaviour	5
	3	Allocate task to own or contractor staff	4
	4	Select appropriate staff/contractors	5
	5	Devise/revise training programme	4
	6	Train staff/contractors	4
	7	Assess that competence has been acquired	5
	8	Monitor task performance	4
	9	Evaluate competence	4
	10	Refresher training	4

Table 17 : Rating sheet filed with the results from one case study (second half)

ARAMIS Delivery system	Step No.	Steps	Rating (1-5)
3 Commitment, compliance & conflict resolution		**Total:**	**80%**
		[Establish policy & assess company cultural maturity]	
	1	Analyse, specify & agree critical behaviours	5
	2	Assess & modify behavioural antecedents & consequences (equipment, work environment, systems, training, risk perception)	4
	3	Put incentives, supervisory & social control in place	5
	4	Implement measures to ensure commitment & provide feedback	5
	5	Review, evaluate impact, learn	5
4 Communication & coordination		**Total:**	**85%**
	1	Analyse communication & coordination needs	5
	2	Develop communication & coordination channels and procedures	4
	3	Use communication & coordination channels & procedures	4
	4	Monitor, evaluate & improve communication & coordination system	4
5 Procedures, rules & goals		**Total:**	**80%**
	1	Define where rules are necessary	4
	2	Develop applicable rules	4
	3	Write & approve rules	4
	4	Promulgate, train, execute rules	4
	5	Monitor use of rules	5
	6	Enforce use of rules	5
	7	Evaluate rule effectiveness (errors/violations)	4
	8	Modify rules	5

ARAMIS Delivery system	Step No.	Steps	Rating (1-5)
6 Hard/software purchase, build, interface, install		**Total:**	**100%**
	1	Specify barriers, equipment, tools, spares incl. HF considerations	5
	2	Choose to buy or fabricate	5
	3	Plan resources for fabrication	5
	4	Fabricate incl. HF	5
	5	Make inventory & selection of suppliers	5
	6	Select & order equipment, materials	5
	7	Receive, check & store orders & purchases	5
	8	Check requisition & issue	5
	9	Install & adjust, incl. HF	5
	10	Register performance, evaluate & learn	5
7 Hard/software inspect, maintain, replace		**Total:**	**80%**
	1	Risk Analysis	4
	2	Define maintenance concept & plans (Maintenance/Inspection)	5
	3	Document equipt. & plans	5
	4	Plan resources & methods	5
	5	Execute inspection & testing	5
	6	Schedule maintenance/repair	4
	7	Execute maintenance & repair (isolate – check – handover – execute – check – handover - restart)	4
	8	Report, Record, Evaluate, Learn	4

Table 18 : Safety management efficiency results for a safety relief valve

ARAMIS Safety Management Efficiency Calculation							
Barrier:		Safety relief valve					
Barrier type:		5	Activated – hardware on demand – barrier or control				
	Design Barrier Level of Confidence:	**3**					
	Ratings:			**Reduction factors**			
0	Safety Culture			0%			
1	Manpower planning & availability	100%		0%			
2	Competence & suitability	86%		0%			
3	Commitment, compliance & conflict resolution	80%		0%			
4	Communication & coordination	85%		0%			
5	Procedures, rules & goals	80%		0%			
6	Hard/software purchase, build, interface, install	100%		0%			
7	Hard/software inspect, maintain, replace	80%		10%			
	Operational Barrier Level of Confidence:	**2,70**					

4.5 Discussion

4.5.1 Who can perform the audit and the SCQPI?

Originally, the project aimed at providing a method that could be used by the competent authorities as well as by the industry themselves and not only by external auditors. The ARAMIS review group has expressed doubts whether the audit could be performed by industry itself (as an internal audit). There are no technical reasons that prohibit the ARAMIS audit manual to be used for an internal audit, and it is up to the authorities to accept results of an internal audit to be used as basis for the (quantified) safety management efficiency evaluation.

As the SCQPI is a fixed instrument, with little room for subjective interpretations (as compared to the audit), industry itself can perform and supervise the SCQPI investigation.

4.5.2 How reliable is the calculation of the reduction of the Level of Confidence due to deficiencies in safety management?

The presumed effect of deficiencies in safety management on the reduction of design values of the Level of Confidence of safety barriers is not confirmed by any objective data. The “Purple book” [7] touches on the issue in different contexts. The general influence of safety management efficiency on failure rates is not included due to uncertainty – on the other hand, the presence of either more or less (physical?) safety measures compared to “state of the art” allows for a factor of ca 5 in decrease and increase of the failure rate of pressure vessels, respectively.

The suggested direct coupling of the rating of safety management and safety culture to the barrier’s Level of Confidence is a simplification of reality, but introduced because it is even harder to quantify the “real” links in between, as indicated in the graph below.

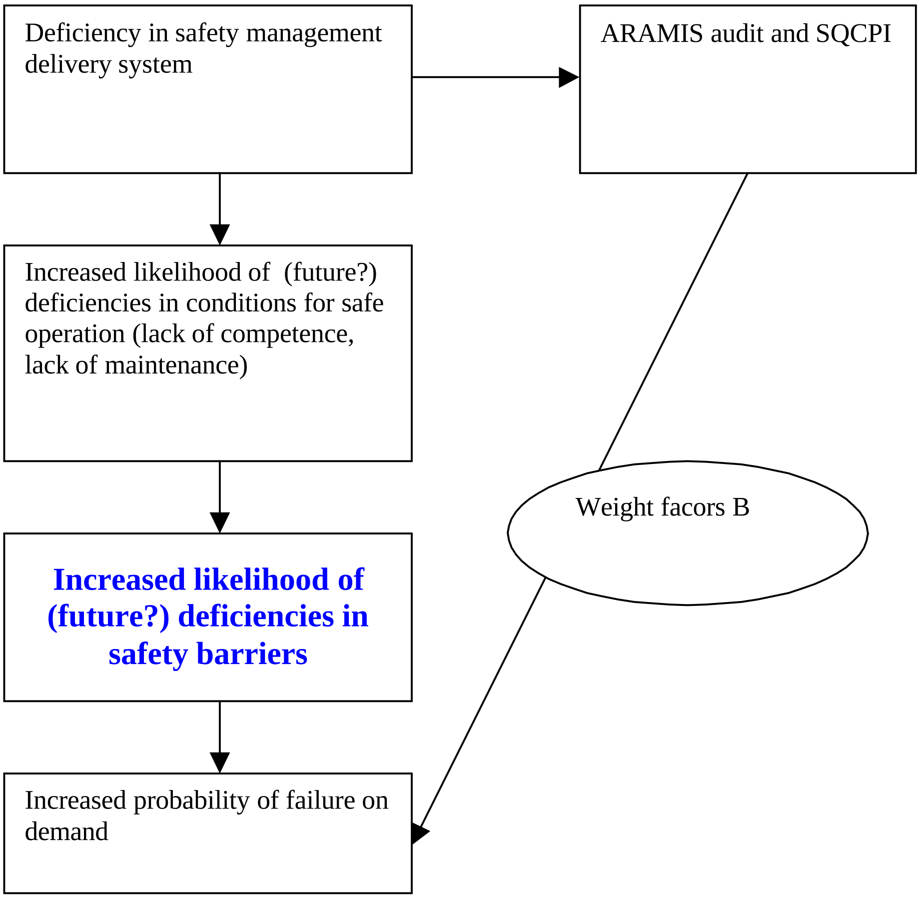


Figure 9: Relation between the management system and the probability of failure of a given safety related component and link with ARAMIS audit and safety culture questionnaire

The most important short-cut is that the present methodology presumes that deficiencies in the *process* of safety management are directly linked to deficiencies of the safety barriers, while the actual causal relationship is that the deficiencies in the *output* of safety management that drive the probability of failures in the barriers.

On the other hand, it is the *process* of safety management that can provide the indication whether the safety barriers are likely to keep their present level of confidence in future, in other words, the *process* of safety management gives an outlook of the safety level in future conditions.

It is beyond doubt, that the present set of weight factors only provides a very rough indication of the expected reduction of Level of Confidence due to deficiencies in safety management, and future efforts in the field are necessary, though data collection will be extremely difficult due to the nature of the problem.

4.5.3 Should the safety management efficiency evaluation be included in the risk assessment?

The ARAMIS review group has expressed that some authorities will refrain from introducing quantified safety management evaluations in the risk assessment. The argument is that management is changing fast, so the risk assessment – and the decisions on e.g. land-use planning – would not be robust.

The arguments against this reasoning are:

1. Current risk assessments tend to be based on optimal, design values for the Level of Confidence of safety barriers. The inclusion of the safety management evaluation leads to more conservative risk estimates, and as such the results would actually be more robust with respect to future conditions. Neglecting the safety management efficiency means actually neglecting the possible degradation of the safety barriers under the presumably volatile safety management regimes.

2. As presented in the previous section, the *process* of safety management is the (only) element that provides indication about the expected future state of the safety barriers, i.e. the future risk level. Accepting a risk assessment that includes a safety management evaluation gives the authorities a more explicit reference for plant inspections – and enables the authorities to put explicit requirements on specific items of safety management.

5. Methodology for the Identification of Reference Accident Scenarios (MIRAS)

5.1 Purpose

The purpose of the Methodology for the Identification of Reference Accident Scenarios (MIRAS) is to **choose Reference Accident Scenarios** (RAS) among the Major Accident Scenarios identified with MIMAH in the paragraph 2.3. The RAS will be modelled to compute the Severity characterising the plant (see paragraph 6).

MIRAS takes 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 follows 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 10:

- 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

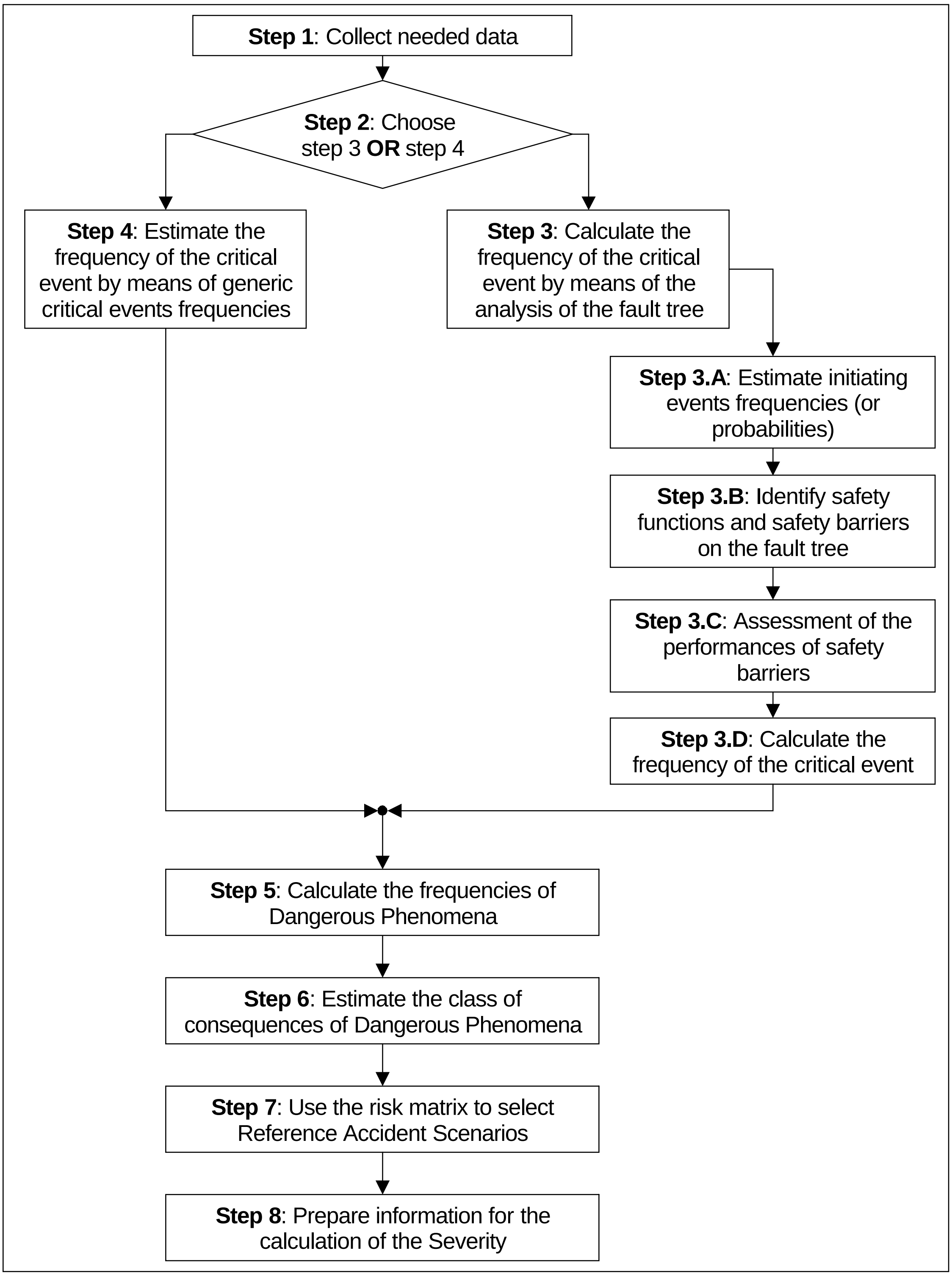


Figure 10: General overview of MIRAS steps (steps to be applied for each bow-tie built with MIMAH)

5.2 Collect needed data (MIRAS Step 1)

Additional data will be required all along the MIRAS steps. The list of information needed is given in *Table 7 of D.1.C. (MIRAS Step 1) [1].*

5.3 Calculate the frequency of the critical event (MIRAS Step 2 and 3 or 4)

Step 3 and step 4 have the same goal: estimate the frequency per year of the critical event for the considered bow-tie. So in the step 2 of MIRAS, the reader has then to make a choice between step 3 or step 4.

In the **step 3 of MIRAS**, firstly, the frequencies (or probabilities) of the initiating events(*) must be assessed. *Appendix 7 of D.1.C. [1]* gives an overview of data available for the frequencies (or probabilities) of initiating events. However, it is recommended to use plant specific data if they are available or to estimate them with the plant staff, with the help of qualitative frequencies given in Table 19 (*Table 8 of D.1.C. (MIRAS Step 3.A.) [1]).*

Table 19: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 (once by 1000 years)	10^{-4} /year < $F \leq 10^{-3}$ /year	F_3
Low frequency (once by 100 years)	10^{-3} /year < $F \leq 10^{-2}$ /year	F_2
Possible – High frequency (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

Secondly, the identification of safety barriers in the fault tree (*MIRAS Step 3.B.*) and the evaluation of their performances (*MIRAS Step 3.C.*) must be realised (see paragraphs 3.2 and 3.3).

Finally, with these data, it is possible 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 and will take into account the safety barriers on the fault tree, as explained in the *deliverable D.1.C. (MIRAS Step 3.D) [1]*.

Briefly, 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.

In parallel, the influence of safety barriers on the accident scenario (the bow-tie) is taken into account. The **"avoid" barrier** implies that the event located just downstream is supposed impossible. The corresponding branch will thus not influence the critical event frequency anymore. The **prevention and control barriers** decrease the transmission probabilities between two events in the fault tree and influence the critical event frequency. Indeed, 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}.

If the frequency of the critical event cannot be calculated on the basis of the analysis of the fault tree, an other possibility is to evaluate it by means of generic critical event frequencies. It is the **step 4 of MIRAS**. *Appendix 10 of D.1.C. [1]* gives the results of a bibliographic review of published data on this subject.

5.4 Calculate the frequencies of dangerous phenomena (MIRAS Step 5)

The objective is to proceed step by step in the event tree to obtain, as output, the frequency of each dangerous phenomenon(*).

First of all, in the generic event trees built with MIMAH, there is no AND/OR gate explicitly drawn. In fact, these gates are implicitly included in the event trees. AND gates are located between an event and its simultaneous consequences. OR gates appear downstream an event of one of the consequent events may occur and the others not. *Appendix 11 of D.1.C. [1]* gives detailed information about the gates.

Secondly, when OR gates appear in the event tree, figures for the transmission probabilities linked with these gates must be assessed. The transmission probabilities can be the following ones: probability of rain-out, probability of immediate ignition, probability of delayed ignition or probability of VCE. To help the reader, some values of transmission probabilities are given in *Appendix 12 of D.1.C. [1]*

Finally, safety barriers related to the event tree side will be taken into account, both in terms of consequences and frequency of dangerous phenomena, as explained in the *deliverable D.1.C. (MIRAS Step 5) [1]*. Briefly, it can be pointed out that the prevention and control barriers decrease the transmission probability between two events by their level of confidence and influence so the dangerous phenomena frequency. The limitation barriers reduce the consequences of dangerous phenomena in limiting the source term or in limiting their effects. In the event tree when a limitation barrier is met, two branches must be built, one if the barrier fails with a probability equal to the probability of failure on demand (PFD) and an other one, if the barrier succeeds with a probability equal to (1-PFD). The PFD of a safety barrier is equal to 10^{-n}, *n* being the level of confidence of the barrier. 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 output of this step is a list of dangerous phenomena (DP) associated to each critical event identified by MIMAH. The frequency of each dangerous phenomenon is calculated, and the limitations of source term or of effects due to limiting safety barriers are taken into account.

5.5 Estimate the class of consequences of dangerous phenomena (MIRAS Step 6)

The selection of Reference Accident Scenarios (RAS) is based on the evaluation of the frequency of dangerous phenomena, together with their potential consequences. So, the consequences of each dangerous phenomenon have to be evaluated qualitatively. This evaluation will be based on the four classes of consequences defined in Table 20 and will take into account the presence of limiting safety barriers on the event tree (see *deliverable D.1.C (MIRAS Step 6) [1]*).

Table 20: Class of consequences

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

Table 21 gives the rough class of consequences of "fully developed" dangerous phenomena(*). This table must be used only as orientation.

Table 21: Rough class of consequences of "fully developed" Dangerous Phenomena

Dangerous phenomena	*Consequence class*
Poolfire	C2
Tankfire	C1
Jetfire	C2
VCE	C3 or C4 (according to the released quantity)
Flashfire	C3
Toxic cloud	C3 or C4 (according to the risk phrases – C4 for very toxic substances)
Fire	C2
Missiles 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

5.6 Select the Reference Accident Scenarios (MIRAS Step 7)

The selection of RAS is obtained thanks to a tool, called "Risk Matrix" crossing the frequency and the potential consequences of accidents (see Figure 11). Three zones are defined in the risk matrix:

the lower green zone ("Negligible effects" zone), the intermediate yellow zone ("Medium effects" zone) and the upper red zone ("High effects" zone).

Each dangerous phenomenon resulting from bow-ties must be placed in the risk matrix, according to its estimated frequency and class of consequences. **Dangerous Phenomena in yellow and red zones are the Reference Accident Scenarios and have to be modelled for the severity calculations**.

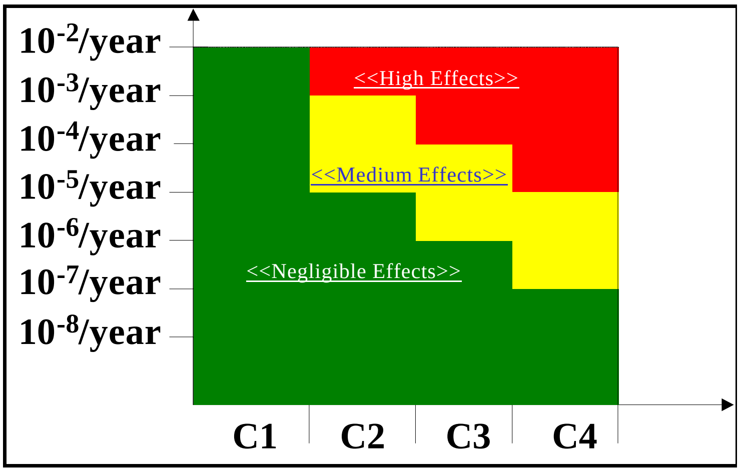


Figure 11: Risk matrix

5.7 Example

For the bow-tie presented as example (see paragraph 2.3.4), the calculation of the frequency of CE7 "Large Breach on shell in liquid phase" from the fault tree, taking into account the estimation of initiating events frequencies, the identification of safety barriers and the evaluation of their performances is shown on Figure 12.

In Figure 13, the frequencies of dangerous phenomena taking into account the safety barriers and the transmission probabilities in the event tree are calculated and indicated on the event tree studied previously as example (see paragraph 2.3.4).

After having qualitatively assessed the consequence classes of dangerous phenomena, these ones are placed in the Risk Matrix (see Figure 14).

Thus, in the example considered here, it appears that six Reference Accident Scenarios (corresponding to dangerous phenomena located in the "yellow" or "red" zones) will have to be modelled for the severity calculations.

5.8 Discussion

The data needed for the application of MIRAS, as the determination of initiating events frequencies/probabilities, the identification of safety barriers, the evaluation of their performances and the assessment of transmission probabilities, can be obtained and discussed during the second visit on site.

The figures given as orientations in the appendices 7, 10 and 12 of D.1.C. should not be used blindly because they have a generic character. There are a lot of uncertainties on these values, the origin of these data are not very precise and their application conditions are not known.

In MIRAS, the deep study of causes of accidents, probability levels and safety systems allows to define scenarios more realistic than the Major Accident Hazards. The RAS represent the real hazardous potential of the equipment, taking into account the safety systems (including safety management system). The RAS will be given to people involved in the calculation of the severity index S with the information needed to perform the modelling (see *deliverable D.1.C. (MIRAS Step 8) [1]*).

It should be reminded that the risk matrix is actually not a guide for the acceptability of risk, but it is only a guidance to select reference accident scenarios. 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.

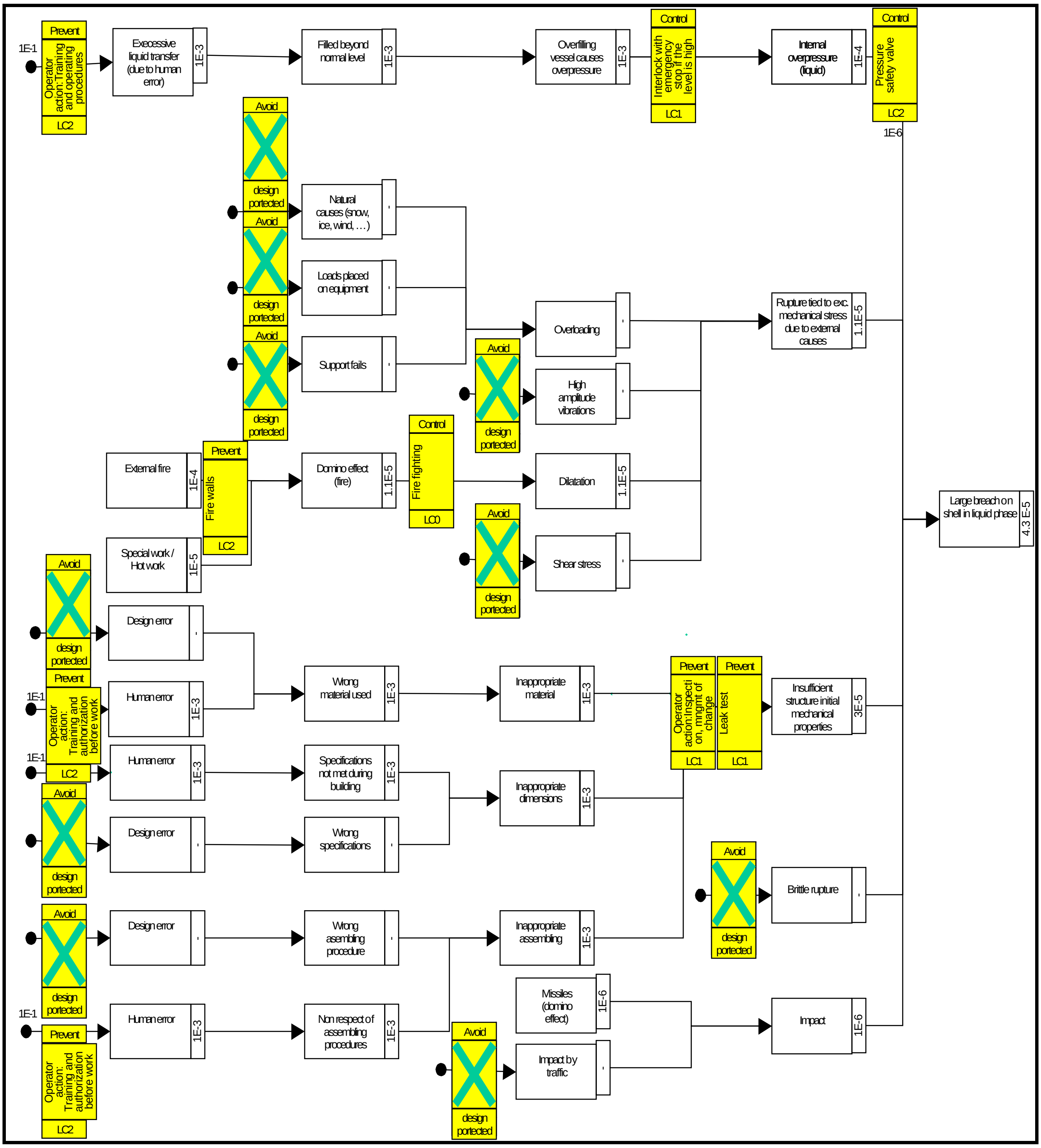


Figure 12: Fault tree with the frequency of CE7 "Large breach on shell in liquid phase"

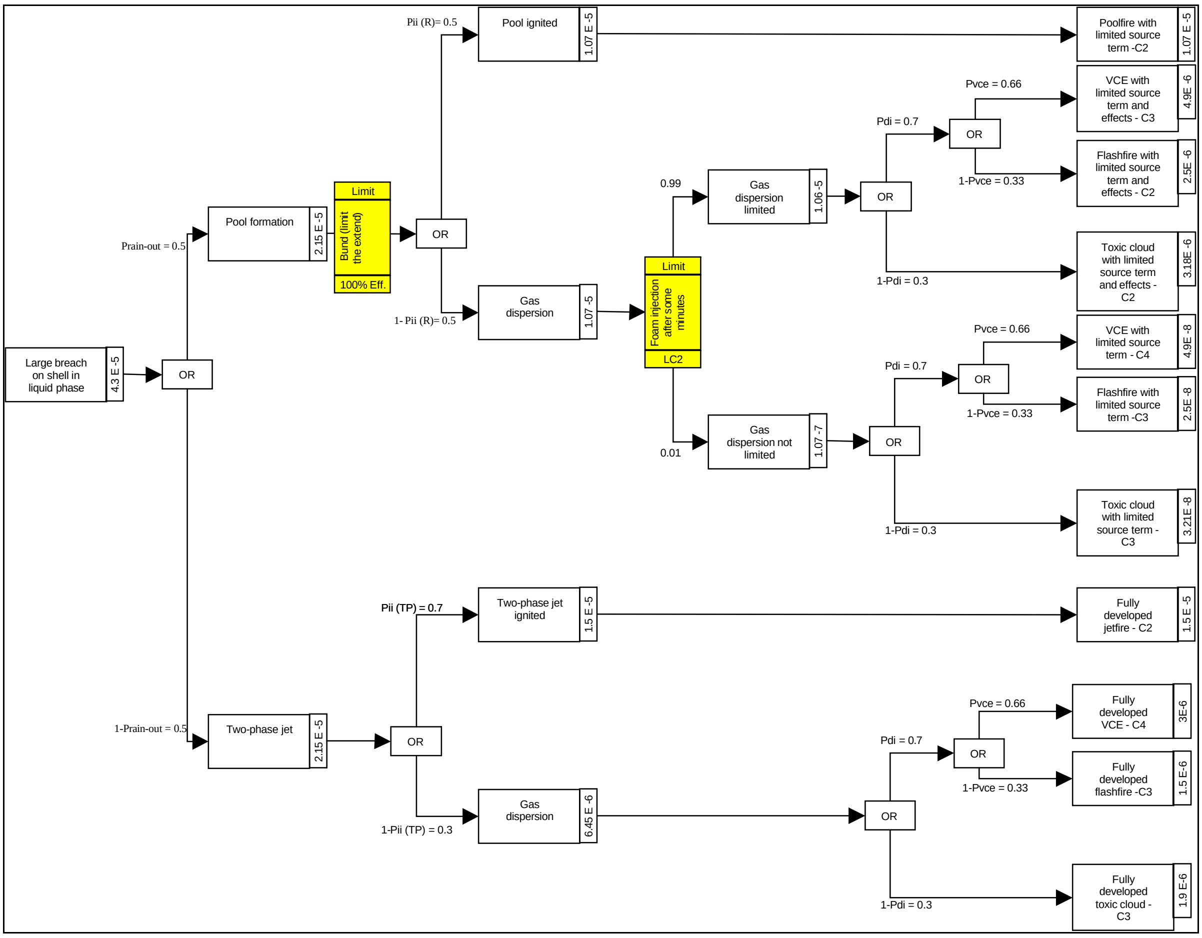


Figure 13: Event tree with the frequencies of DP

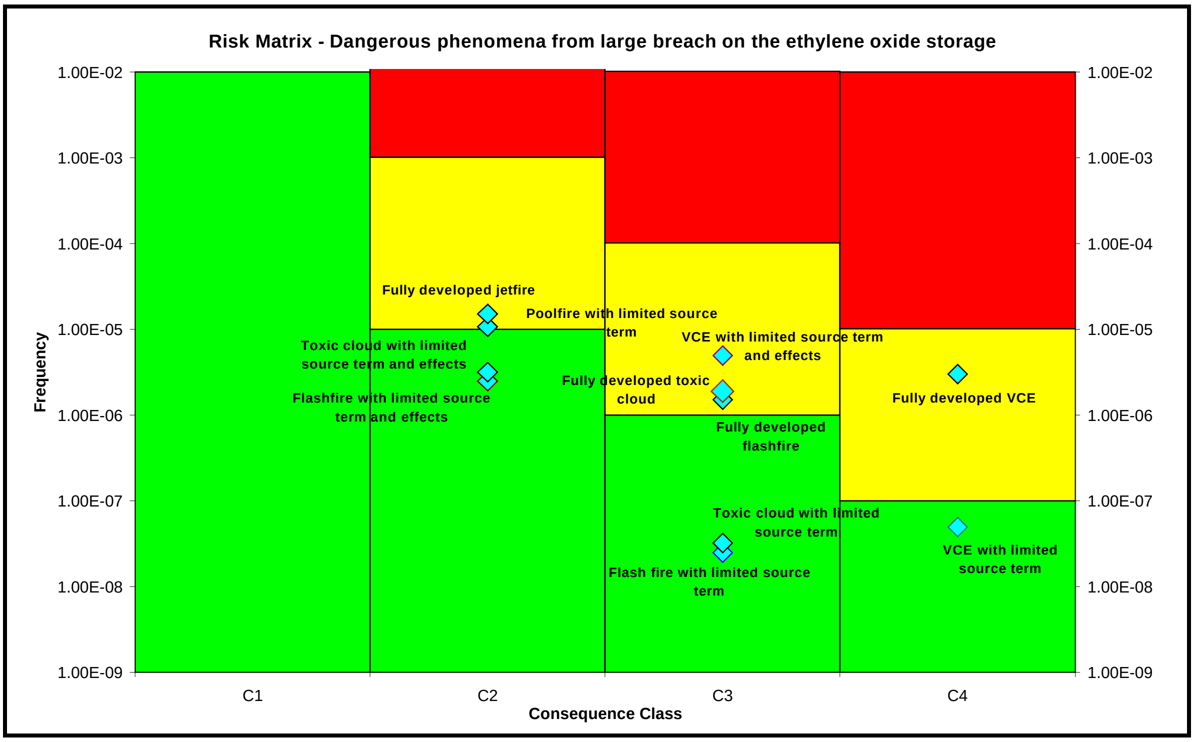


Figure 14: Risk matrix with DP from CE7 "Large breach on shell in liquid phase"

6. Mapping the risk severity of reference scenarios

6.1 Purpose

One of the targets of the ARAMIS methodology is the characterization of the risk level through an integrated risk index composed with independent parameters related to the severity evaluation of scenarios, the prevention management effectiveness and the environment vulnerability estimation describing the sensitivity of the potential targets located in the vicinity of the SEVESO II establishments.

Therefore, a parameter allowing the evaluation of the severity of the scenarios -taking into account only their effects- has been deviced. This parameter, which has been named Severity Index (*S*), is completely independent from the other parameter developed in the context of the ARAMIS project, the Vulnerability Index (*V*).

In this section the methodology for the calculation of the Risk Severity Index (S) is described and the results from a typical example case are calculated and used to “map” the risk on a given zone. The complete methodology is described in the deliverable D.2.C [8].

6.2 The risk severity index

A risk index is a measure, quantitative or qualitative, oriented to integrate into a numerical value or into a descriptive adjective, a set of factors which have an influence on the hazards or the risk of a system.

The Risk Severity Index (S) is based on a set of Dangerous Phenomena (DP) and their corresponding Major Events (ME), identified through the application of the MIMAH methodology (Methodology for the Identification of Major Accident Hazards) developed in the frame of ARAMIS. It takes into account as well an uniform set of threshold levels concerning the diverse accident effects.

6.2.1 Threshold levels

Four levels of effects are considered (see Table 22), which in some way are representative of the criteria used by in the diverse European countries.

Table 22: Levels of effects considered

Level of effect	*Description*
1	Small or non effects
2	Reversible effects
3	Irreversible effects
4	Start of lethality and/or domino effects

Several effects are considered :

a). Thermal radiation

Continuous radiation

Threshold values are shown for 60 s exposure time, if another exposition time is considered the values in Table 23 will change taking into account the concept of dose.

Instantaneous radiation

In this case the threshold values are related to the concentration of flammable material in the cloud.

b). Blast effects

Four ranges of maximum overpressure are used. In this case the time has no influence on the dose which is directly the value of the maximum overpressure.

c). Missiles

The thresholds for missiles ejection consider only two possibilities: maximum level of effects (4) for any point at a distance smaller than the distance were the 100% of the missiles are found, and the minimum level (1) for higher distances.

d). Toxic effects

TEEL* values (Temporary Emergency Exposure Limits) [9] are used.

Table 23 summarizes the values of the thresholds corresponding to the four levels of effects to be used in the definitions of the Risk Severity Index. It should be pointed out that it does not intend the proposal of new harmonized threshold levels, as this is a decision corresponding to each country and is not the objective of the ARAMIS project. Table 23 is only for use in the context of this project and the severity index proposed can be applied to any other threshold values.

Table 23: Definition of the thresholds for the diverse levels of effects.

Level of effects	**Radiation(1)** (kW/m^2)	**Instantaneous Radiation**	**Blast (mbar)**	**Missiles(2) (%)**	**Toxic effects**	**Description**
1	< 1.8	< 0.5·LFL	< 30	0	< TEEL-1	Small or non effects
2	1.8 – 3		30 – 50		TEEL-1 – TEEL-2	Reversible effects
3	3 – 5		50 – 140		TEEL-2 – TEEL-3	Irreversible effects
4	> 5	= 0.5·LFL	> 140	100	>TEEL-3	Start of lethality and/or domino effects

(1) For 60 s exposure
(2) Range distance of the indicated percentage of missiles.

All the effects represented in Table 23 make reference only to humans or structures but not to the environment. Nevertheless, the most important effect on the environment will be mainly due to toxic substances and in this case a reference concentration level for the affected target should be taken into account.

6.2.2 The risk severity index

The Risk Severity Index for a given critical event, S_{CE} , is a combination of the Specific Risk Severity Indexes, S_{DP}, associated to each of the dangerous phenomena that the critical event has, as in this way the probabilities of occurrence can be taken into account:

$$S_{CE}(d) = \sum_{i=1}^{n} \left(P_{DP_i} \cdot S_{DP_i}(d) \right) \qquad \text{Eq. 1}$$

In this expression n is the total number of dangerous phenomena (DP) associated to the critical event; P_{DPi} is the probability of occurrence of the DP_i; and $S_{DPi}(d)$ is the specific severity index associated to the DP_i.

The value of S_{CE} will usually range between 0 and 100 (Table 24) although in some cases it could be greater than 100 (for example when the sum of the probabilities corresponding to the DP is greater than 1)[3], especially for low values of d.

Table 24: Specific Risk Severity index value as a function of the level of effects

S_{DP}	***Level of effects***
0 – 24	1
25 – 49	2
50 – 74	3
75 – 100	4

The Risk Severity Index for a whole installation, S, is a combination of the Risk Severity Indexes associated to each of the critical events considered and their frequencies of occurrence:

---

[3] This situation can occur when a cautious approach is applied when defining the probabilities of dangerous phenomena

$$S(d) = \sum_{j=1}^{m} \left(f_{CE_j} \cdot S_{CE_j}(d) \right) \qquad \text{Eq. 2}$$

In this expression *m* is the total number of critical events (*CE)* associated to the installation; f_{CEj} is the frequency of occurrence of the CE_j; and $S_{CEj}(d)$ is the risk severity index associated to the CE_j.

The values obtained after the application of Eq. 2 are not in the range 0-100 and the scale defined in Table 24 can not be applied any more. The values obtained will usually range between 0-1.2. These values are normalized in order to have them between 0-1000. The following scale applies:

Table 25. Scale for the Risk Severity Index of an installation

S value	***Risk Severity Index Level***
S = 750	Extremely high
300 = S < 750	High
50 = S < 300	Medium
S < 50	Low

The value of *S* changes as a function of the distance; in this way, maps of severity can be constructed around an installation. In order to represent the S values on the GIS, five distances are proposed to be calculated for each dangerous phenomena involved (see Table 26).

Table 26. Relationship between the S value and the distance where this value is reached

S_{DP}	***distance***
0	d_o
25	d_1
50	d_2
75	d_3
100	d_4

Once the distances d_o to d_4 have been found through the application of the models, the value of *S* at any distance can be obtained by applying lineal equations inside each range (see Table 27).

The values of S_{DP}, S_{CE} and *S*, are evaluated in each mesh of the treated zone directly with the Severity GIS Tool developed specifically. The user only needs to find the distances d_0 to d_4 for each DP considered on the installation and introduce them into the GIS in order to obtain the maps and the values of the risk severity indexes on a given point.

Table 27. Lineal equations for S_{DP}

Equation		
$S_{DP} = \frac{25}{(d_1 - d_0)} \cdot x - \frac{25 \cdot d_0}{(d_1 - d_o)}$	$d_1 < x < d_o$	Eq. 3
$S_{DP} = \frac{25}{(d_2 - d_1)} \cdot x + \frac{(25 \cdot d_2 - 50 \cdot d_1)}{(d_2 - d_1)}$	$d_2 < x < d_1$	Eq. 4
$S_{DP} = \frac{25}{(d_3 - d_2)} \cdot x + \frac{(50 \cdot d_3 - 75 \cdot d_2)}{(d_3 - d_2)}$	$d_3 < x < d_2$	Eq. 5
$S_{DP} = \frac{25}{(d_4 - d_3)} \cdot x + \frac{(75 \cdot d_4 - 100 \cdot d_3)}{(d_4 - d_3)}$	$d_4 < x < d_3$	Eq. 6

6.3 Calculating risk severity values

The general procedure to obtain the Risk Severity Index corresponding to a Reference Accidental Scenario (RAS) or a critical event (CE) is given in Figure 15. An example of the calculation is given in section 7.5.[4]

---

[4] Note : The case studies have shown that the global severity index is very sensitive to the number of critical events considered. The previous steps of the methodology must have been followed very cautiously to assure a good significance of this result.

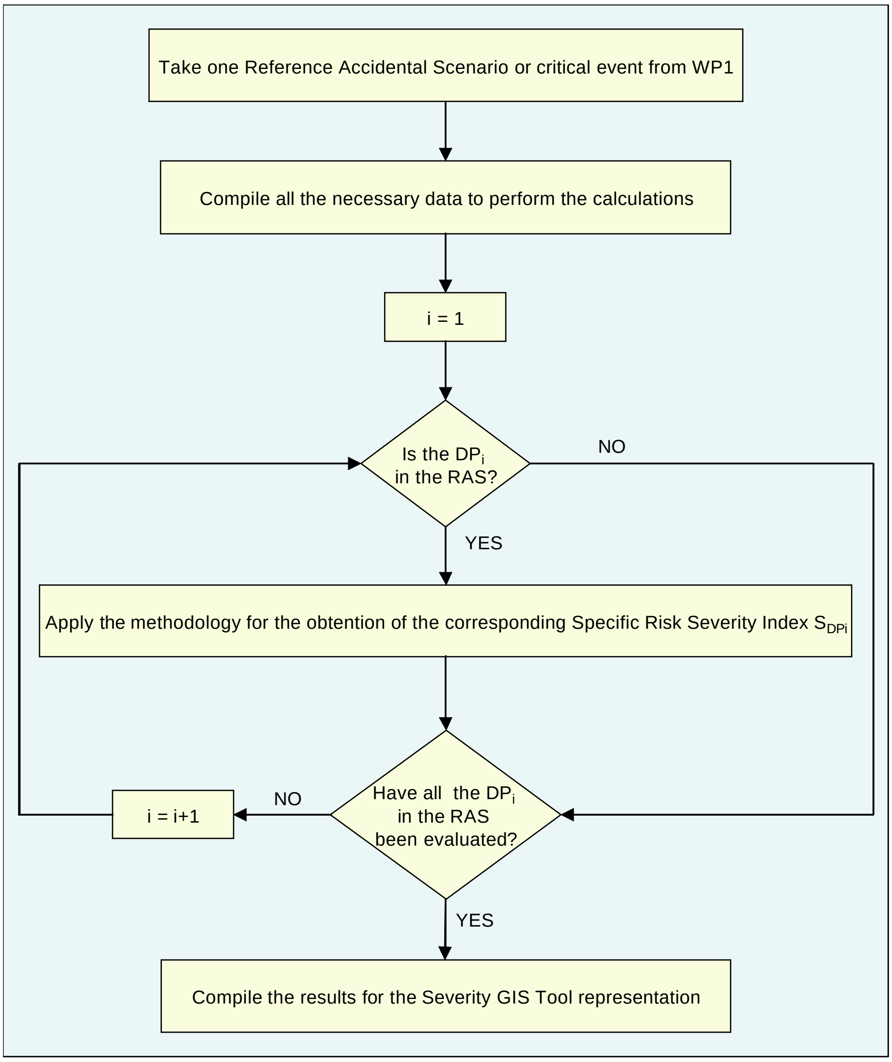
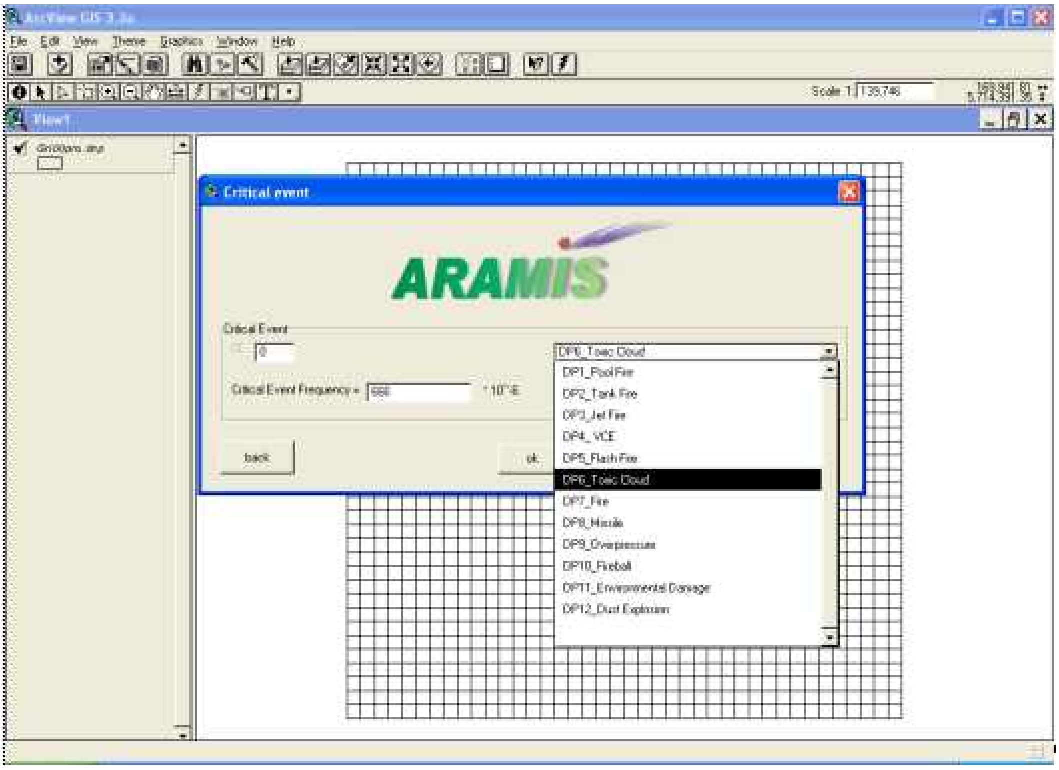


Figure 15 : Schematic representation of the global methodology to obtain the Risk Severity Index.

6.3.1 GIS Severity Mapping Procedure

The procedure prepared with the GIS tool ArcView® assists the user to obtain severity maps. The first step is the projection of the selected grid (see Vulnerability Mapping) and the input of the data concerning wind direction probability. Then the user should insert the data concerning the critical events, selecting the dangerous phenomena of interest from a menu (see Figure 16).



Scale 1: 135,746

Critical Event

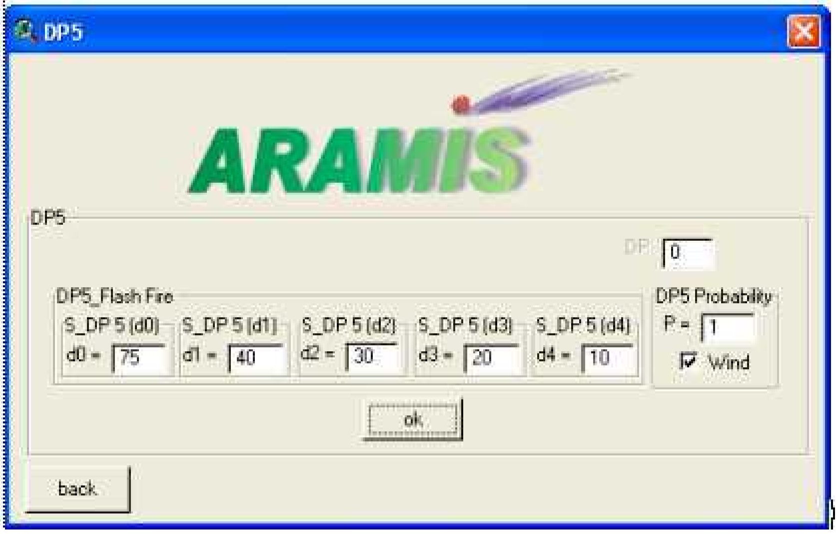
0

DP6_Toxic Cloud

Critical Event Frequency = 666 *10^-6

Figure 16 : Selection of the dangerous phenomenon for a critical event.

The distances relevant to each severity value should be inserted into the mask of each dangerous phenomenon, indicating also its probability and whether it is influenced by wind direction (as the flash fire shown in Figure 17) or not.



DP: 0

S_DP 5 (d0)	S_DP 5 (d1)	S_DP 5 (d2)	S_DP 5 (d3)	S_DP 5 (d4)
d0 = 75	d1 = 40	d2 = 30	d3 = 20	d4 = 10

P = 1

☑ Wind

Figure 17 : Data input for a dangerous phenomenon.

When all the input concerning the dangerous phenomena associated to a critical event are completed, the severity map of that critical event is calculated. Then, the input data of the following critical event are inserted, and the procedure is repeated. When all the data concerning the critical events have been inserted, the overall severity maps are calculated.

6.3.2 Results: Severity Maps

By inserting all the data of the application into the Severity GIS Tool, a number of maps were obtained. For example, Figure 18 shows the map of Risk Severity Index of the whole installation, calculated according to Eq. 2. It can be observed that the value of the risk severity index for this installation is *very low* for distances higher than approximately 750 m and *low* for distances below 750 m. The influence of wind direction can be noticed in the detail of the inner grid. As a matter of fact, some critical events were associated to dangerous phenomena, such as a pool fire, not influenced by wind direction (for example C.E. 6, shown in Figure 19) while others were associated to dangerous phenomena, such as a flash fire (for example, C.E. 7, shown in Figure **20**) sensible to this parameter.

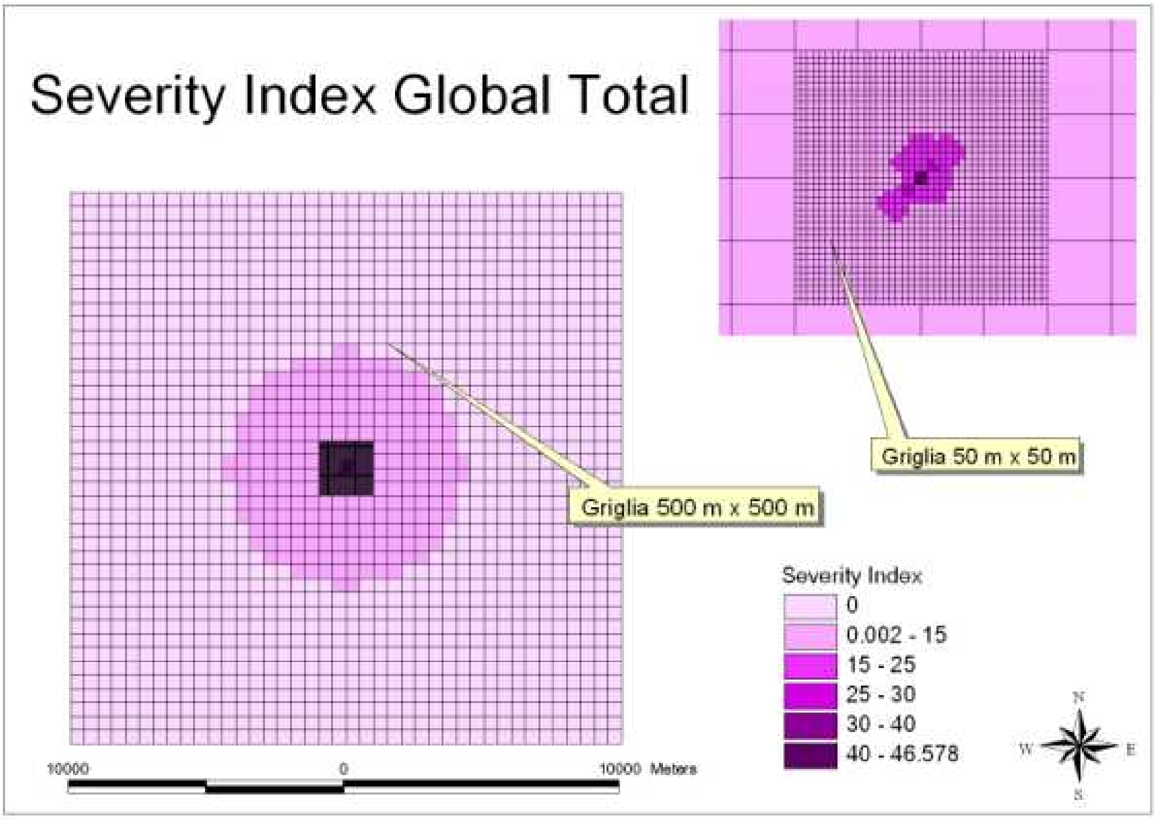


Figure 18 : Map of global Risk Severity index for the whole installation.

The application refers to an installation where only thermal and overpressure effects are associated to the critical events: Figure 21 and Figure **22** show the detail of the risk severity index for the whole installation corresponding to these effects. It can be noticed that overpressure effects are not sensible to wind direction, and that they contribute to the severity index less significantly than thermal ones.

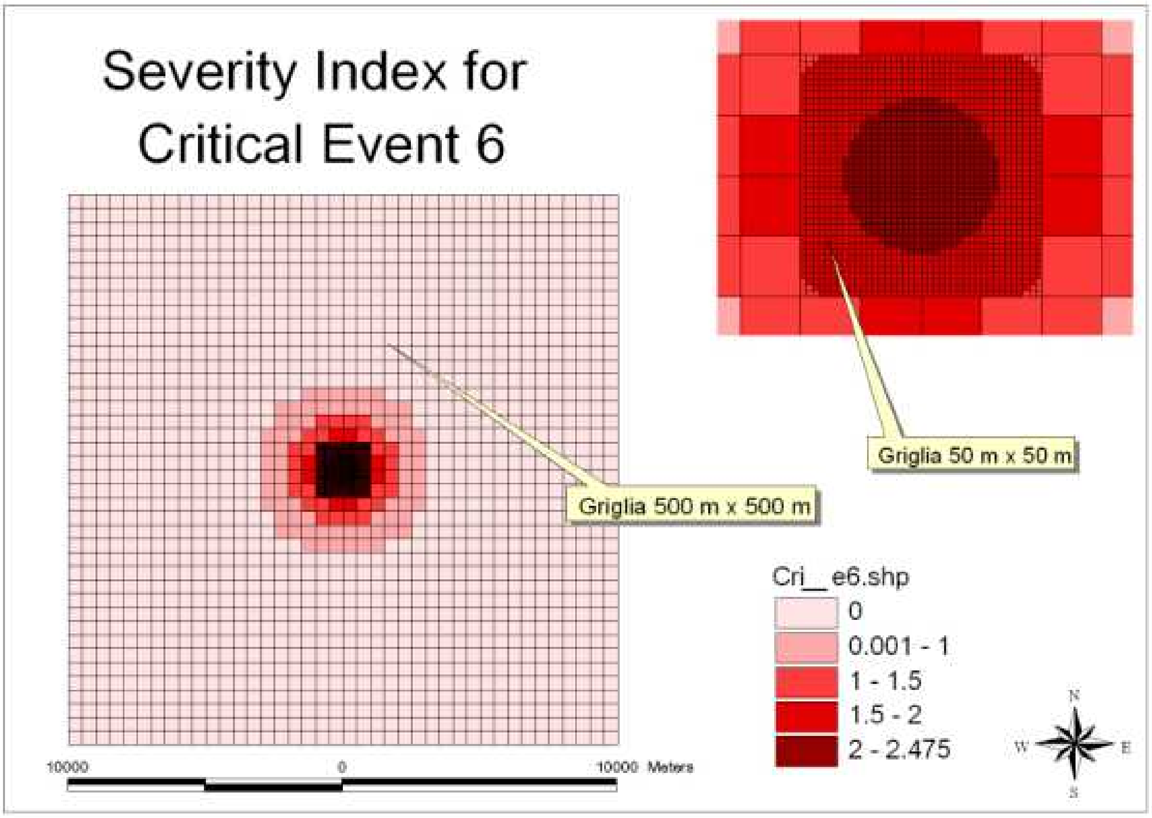


Figure 19: Map of Risk Severity index for C.E. 6 (dangerous phenomenon: pool fire).

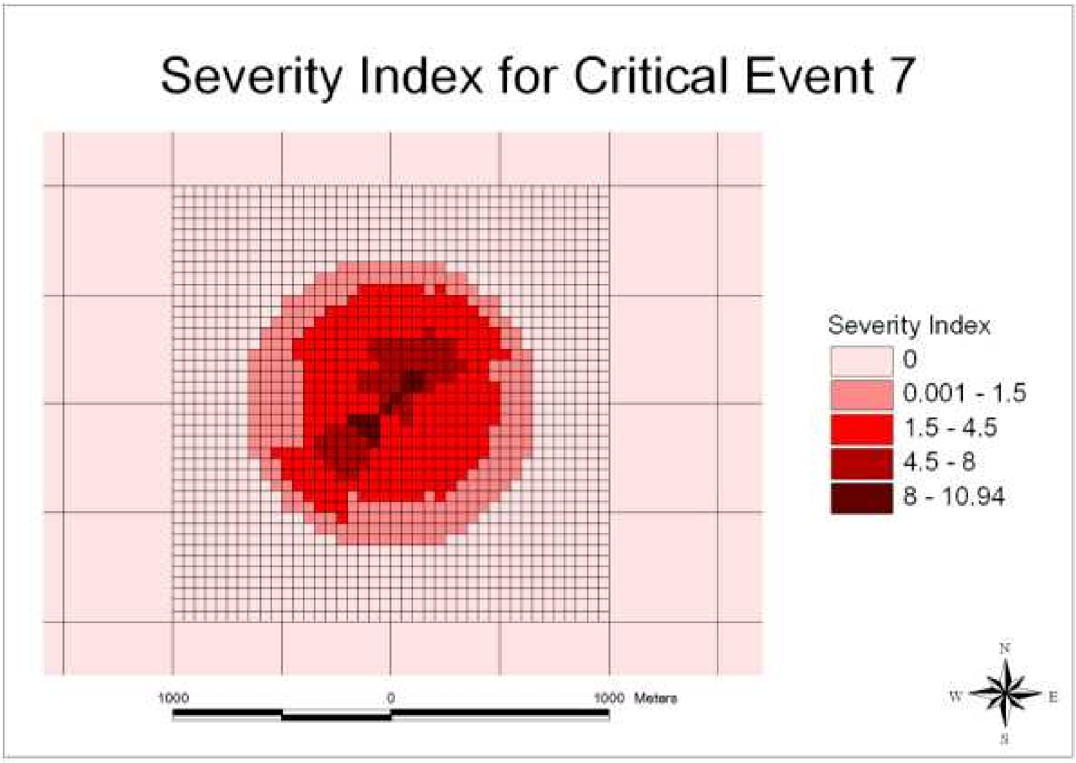


Figure 20: Map of Risk Severity index for C.E. 7 (dangerous phenomenon: flash fire).

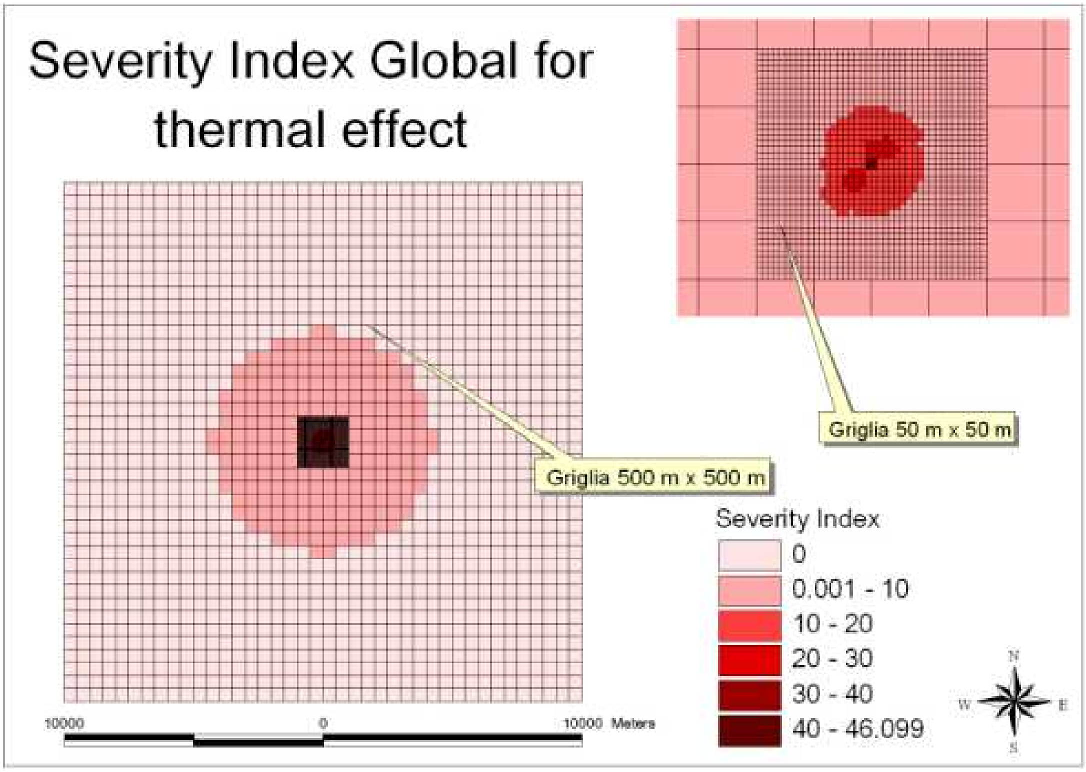


Figure 21: Map of Risk Severity index for the whole installation for thermal effect.

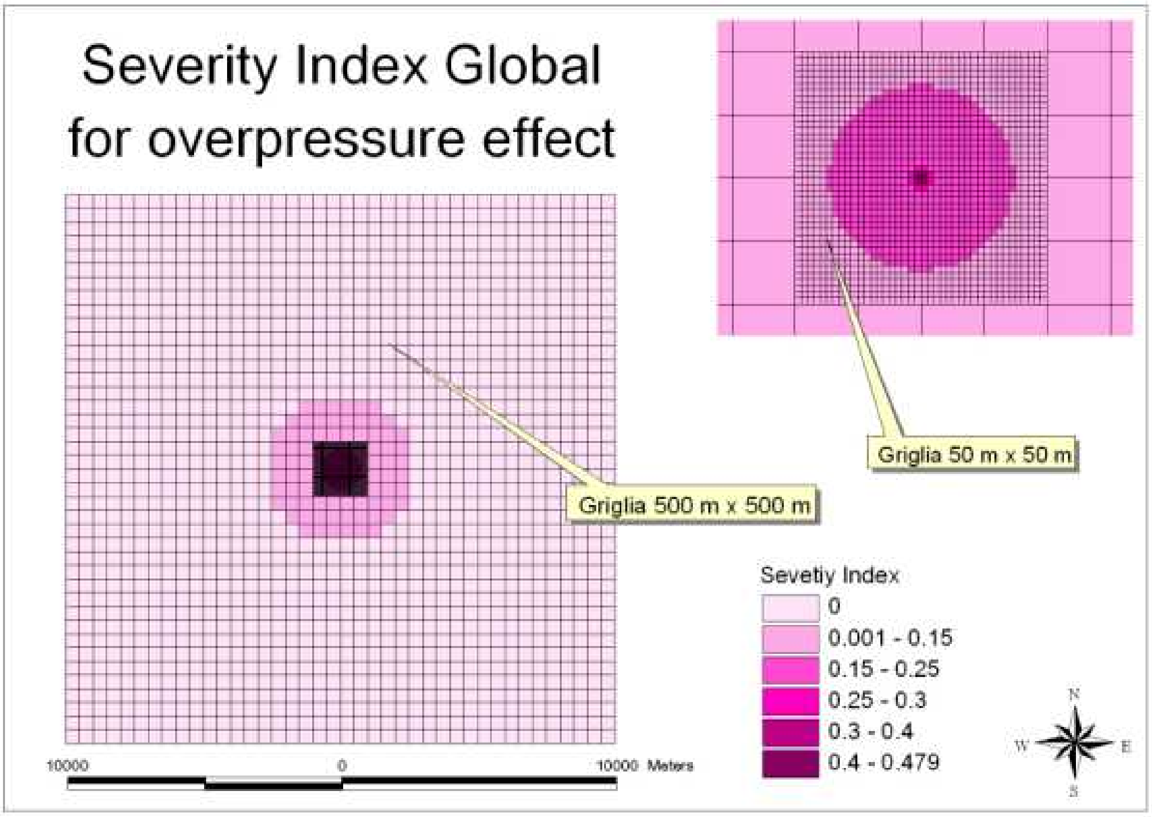


Figure 22. Map of Risk Severity index for the whole installation for overpressure effect.

6.3.3 Discussion

The Risk Severity Index allows a practical quantification of the risk associated to industrial installations. The possibility of plotting it –by using a GIS– on the map of the affected zone gives a very interesting information, which can be used both for territory planning and for emergency management. This information has to be compared with that obtained from vulnerability mapping to give a detailed overview of the impact of the installation on the surrounding territory. Moreover, the maps allow to identify the influence of single critical events, and or single effects (toxic, thermal, etc.).

6.4 Selection of models to be used in calculations

There is a wide diversity of mathematical models for the prediction of the effects derived from accidents. A selection of the most adequate ones to be used in the ARAMIS methodology has been carried out. The criteria used to make the selection were the following[5]:

Complexity of the model and of the resolution of its equations.

For example, in the case of pool-fires, the point source model is extremely simple and easy to use; nevertheless the results obtained are not very reliable. On the other hand, the solid flame model is a little bit more complex but it gives better results. Thus, in this case, the solid flame model has been selected.

Information required for using the model.

The multienergy model for overpressure calculations of vapour cloud explosions requires much more information than the TNT equivalent model. For those cases in which little information is available, the TNT model has been selected. Otherwise, if all the information required is available, the model selected is the multienergy model.

Model availability, as a set of equations or as a free software.

For atmospheric dispersion calculation, the models selected are those usually used, as Gaussian or integral models. Some of these models are freely available.

Degree of acceptance and use from the scientific community.

There are some publications or books with a huge acceptance and which are very spread and used. This is why, in some kind of accidents, models there proposed are suggested. For example, for the prediction of the thermal radiation from a jet-fire, the model selected is that proposed in the "Yellow Book"[10].

Nevertheless, it should be emphasized the fact that the models used to calculate the major events are really completely independent from the methodology designed to obtain the severity index, S. Therefore, the user can apply any mathematical models for the estimation of the accident effects.

6.5 Example: storage installation for flammable materials

The MIRAS methodology has given the following critical events to be studied:

---

[5] The models proposed are those considered to be the most adequate ones for the ARAMIS system (according to the criteria exposed). The methodology proposed for the evaluation of the S index can be used with any kind of model; i.e. the user can assess the major events by using the models he decides.

Table 28: Critical events considered for the studied storage of flammable materials

Loading/unloading area (tank wagons)	**CE_01**	-	Breach on the shell in liquid phase (connection)
	CE_02	-	Breach on the shell in liquid phase(10mm)
	CE_03	-	Breach on the shell in liquid phase (100mm)
	CE_04	-	Leak from the liquid pipe (full bore)
	CE_05	-	Leak from the liquid pipe (10% equiv.diameter)

Atmospheric storage tanks	**CE_06**	-	Breach on the shell in liquid phase (10mm)
	CE_07	-	Breach on the shell in liquid phase (100mm)
	CE_08	-	Catastrophic rupture (internal explosion)

Table 29: **Wind rose probabilities**

N	***NE***	***E***	***SE***	***S***	***SW***	***W***	***NW***
8.43	20.48	7.23	10.84	14.46	19.28	9.64	9.64

Critical events:

Table 30 to Table 37 show the results obtained, for all the critical events considered and their corresponding dangerous phenomena, after the application of the models. In each table all the necessary data for the GIS tool are included: the frequency of the critical event, the distances d_0 to d_4 for each dangerous phenomenon together with their probability of occurrence and the type of effect (thermal, overpressure, toxic or pollution).

Table 30. Data for the critical event 1

Critical Event	CE_01	**Frequency**	$9.6\cdot10^{-5}$

Dangerous Phenomena		**d0**	**d1**	**d2**	**d3**	**d4**	**Probability**	**Type**
Pool Fire	DP1	2413	60.6	43.9	29.1	17.9	0.698	therm
VCE	DP2	2623	95	57	1	0	0.0896	overp
Flash Fire	DP3	1200	57	38	29	18	0.0896	therm

Table 31. Data for the critical event 2

Critical Event	CE_02	Frequency	$1.0\cdot10^{-4}$

Dangerous Phenomena		d0	d1	d2	d3	d4	Probability	Type
Pool Fire	DP1	1981	48.5	35.9	25.2	16.7	0.005	therm
Flash Fire	DP2	495	26	17	11	10	0.027	therm

Table 32. Data for the critical event 3

Critical Event	CE_03	Frequency	$1.2\cdot10^{-5}$

Dangerous Phenomena		d0	d1	d2	d3	d4	Probability	Type
Pool Fire	DP1	4290	91	62.2	38.2	20.8	0.8	therm
VCE	DP2	2630	95.4	57.7	1	0	0.0117	overp
Flash Fire	DP3	1500	73	48	37	22	0.108	therm

Table 33. Data for the critical event 4

Critical Event	CE_04	Frequency	$2.0\cdot10^{-4}$

Dangerous Phenomena		d0	d1	d2	d3	d4	Probability	Type
Pool Fire	DP1	3080	74	53.1	35.2	20.3	0.7	therm
Flash Fire	DP2	1100	52	33	25	16	0.16	therm
Pool Fire	DP3	4290	91	62.2	38.2	20.8	0.0145	therm
VCE	DP4	2630	95.4	57.7	1	0	0.00038	overp
Flash Fire	DP5	1500	73	48	36	22	0.0034	therm

Table 34. Data for the critical event 5

Critical Event	CE_05	**Frequency**	$2.0\cdot10^{-3}$

Dangerous Phenomena		**d0**	**d1**	**d2**	**d3**	**d4**	**Probability**	**Type**
Pool Fire	DP1	1555	39.8	29.7	20.9	13.9	0.1	therm
Flash Fire	DP2	566	37	20	11	10	0.5	therm
Pool Fire	DP3	2930	72.1	51.5	33.9	19.3	0.0145	therm
Flash Fire	DP4	1000	51	32	23	14	0.0034	therm
VCE	DP5	2630	95.4	57.7	1	0	0.0004	overp

Table 35. Data for the critical event 6

Critical Event	CE_06	**Frequency**	$1.0\cdot10^{-4}$

Dangerous Phenomena		**d0**	**d1**	**d2**	**d3**	**d4**	**Probability**	**Type**
Pool Fire	DP1	3212	35	25.7	18.9	14.2	0.099	therm

Table 36. Data for the critical event 7

Critical Event	CE_07	**Frequency**	$5.0\cdot10^{-6}$

Dangerous Phenomena		**d0**	**d1**	**d2**	**d3**	**d4**	**Probability**	**Type**
Flash Fire	DP1	672	32	21	16	10	0.088	therm

Table 37. Data for the critical event 8

Critical Event	CE_08	**Frequency**	$1.0\cdot10^{-8}$

Dangerous Phenomena		**d0**	**d1**	**d2**	**d3**	**d4**	**Probability**	**Type**

Overpressure generation	DP1	5740	212.2	129.3	47.7	29.2		1	overp

Results: Severity Maps

After the introduction of all the data into the Severity GIS Tool, several maps can be drawn. The following two figures are shown as examples. Figure 23 shows the Risk Severity Index of the whole installation according to Eq. 2. It can be observed that the value of the risk severity index for this installation is *very low* for distances higher than approximately 750 m and *low* for distances below 750 m. Figure 24 shows the risk severity index for the whole installation corresponding to thermal effects.

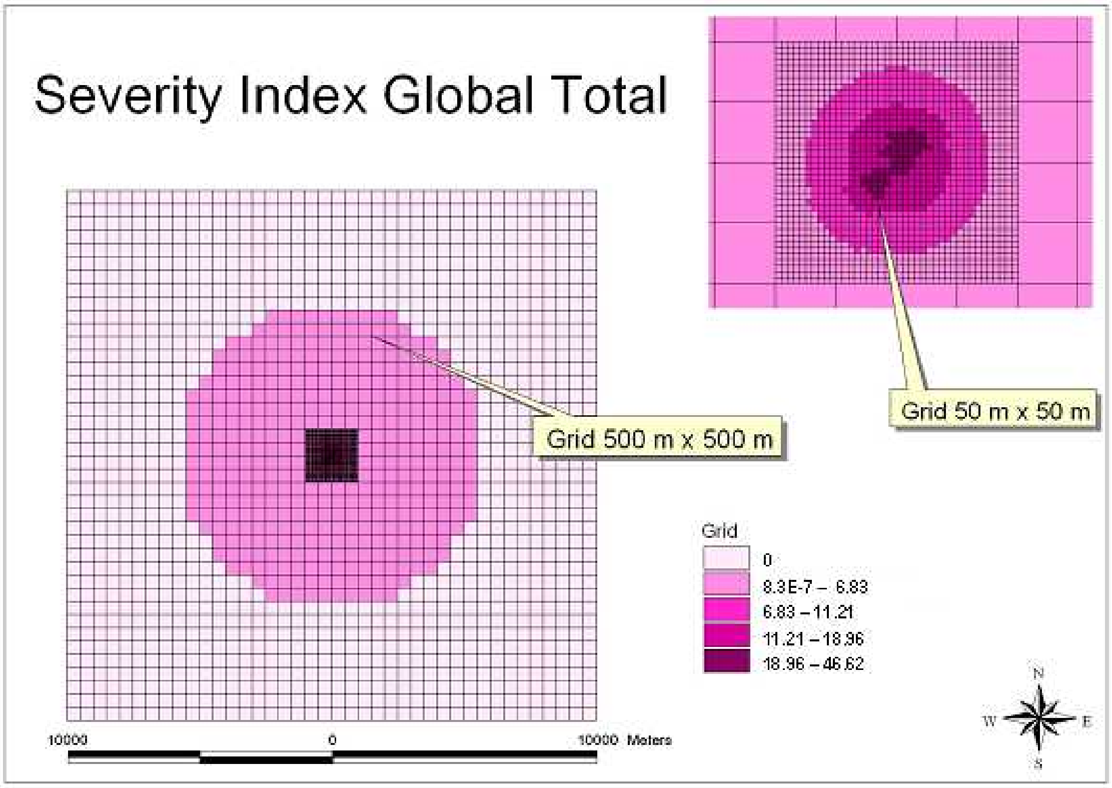


Figure 23. Total Risk Severity index for the whole installation.

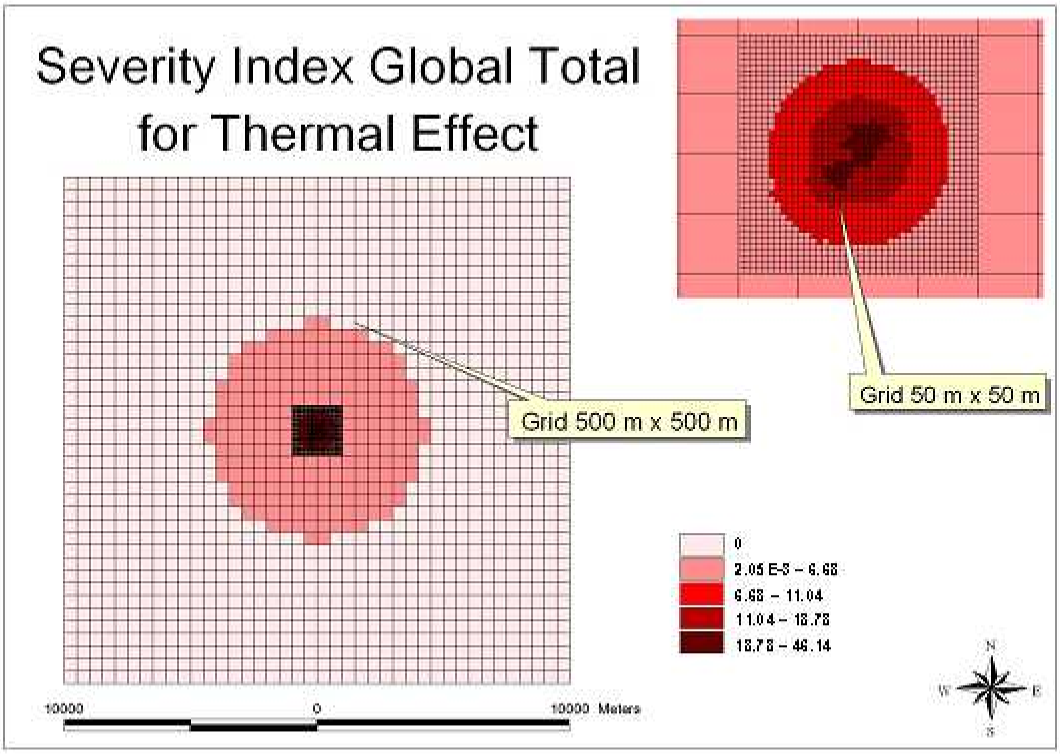


Figure 24. Risk Severity index for the whole installation corresponding to thermal effect.

6.6 Discussion

The Risk Severity Index allows a practical quantification of the risk associated to industrial installations. The possibility of plotting it –by using a GIS– on the map of the affected zone gives a very interesting information, which can be used both for territory planning and for emergency management.

7. Mapping the vulnerability of a plant’s surroundings

7.1 Purpose

ARAMIS project aims at developing an integrated risk index based on, among others, the vulnerability of the environment surrounding an industrial site. Indeed, environmental vulnerability is scarcely taken into account in risk assessment, and its integration in ARAMIS project represents therefore an innovative aspect of great interest. Figure 25 better explains the problematic addressed when defining the environmental vulnerability, which may be summarized as follows: is area 1, which is composed of human, environmental and material targets, more or less vulnerable than area 2 also composed of human, environmental and material targets, but in different quantity and of different nature?

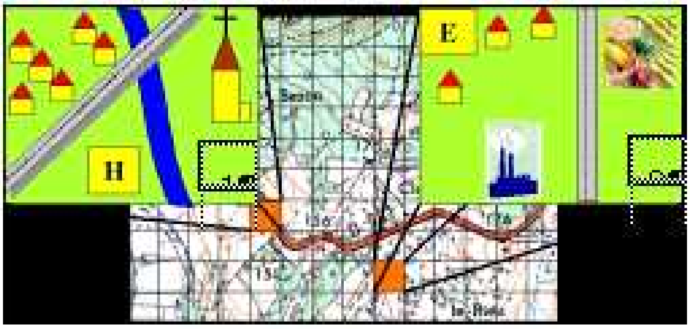


Figure 25: Problematic of environmental vulnerability definition

The idea here developed is to define a vulnerability index to identify and characterize the vulnerability of all possible targets located in the surroundings of a Seveso industrial site (vulnerability mapping). This would require first to establish the study area and define the targets of interest, then to identify and quantify the targets in the study area and, finally, to assess their vulnerability: this last step needs a specific methodology. In this work a semi-quantitative approach to vulnerability is adopted, which is a multicriteria decision method (Saaty’s method) based on expert judgements. This method allows to take into account both the “status” of a specific target (qualitative approach) and the “census” of that target (quantitative approach).

7.2 Typology of vulnerabilities

The aim of this paragraph is to define the environment of an industrial site that can be affected in case of an accident generated by an industrial installation. It is therefore necessary to propose a set of target types to characterise with accuracy the environment, while keeping in mind the importance of the transferability of the method and its flexibility. Indeed, it is necessary to find a proper balance between the number of targets to be taken into account and the limitations due to the multicriteria decision method.

First of all, targets were divided into three categories and each of these categories is then detailed in a list of target types:

- ✓ Human (H)
  - ➢ Staff of the site (H_1)
  - ➢ Local population (H_2)
  - ➢ Population in an establishment receiving public (H_3)
  - ➢ Users of communications ways (H_4)
- ✓ Environmental (E)
  - ➢ Agricultural areas (E_1)
  - ➢ Natural areas (E_2)
  - ➢ Specific natural areas (E_3)
  - ➢ Wetlands and water bodies (E_4)
- ✓ Material (M)
  - ➢ Industrial sites (M_1)
  - ➢ Public utilities and infrastructures (M_2)
  - ➢ Private structures (M_3)
  - ➢ Public structures (M_4)

Two databases have been used to get most information concerning these targets.

The Corine Land Cover (IFEN, 2002) database provides homogeneous geographical information about land use in each country of Europe. The main information included in this database corresponds to topographical map, vegetation and type of forest map and finally soil and network description.

There are five main types of territory description:

- ✓ artificial territory
- ✓ land for agricultural use
- ✓ forest and natural areas
- ✓ humid areas
- ✓ water areas

The five previous types are described by forty four classes in order to characterise the natural environment.

The TeleAtlas database is made of local data collection activities in all European countries and in the USA (TeleAtlas, 1996).

The included themes are:

- ✓ road and street centre-lines
- ✓ address areas
- ✓ administrative areas
- ✓ postal districts
- ✓ land use and cover
- ✓ railways
- ✓ ferry connections
- ✓ points of interest: built-up areas
- ✓ settlement centres
- ✓ water

These two databases fill most of our objectives to describe the natural environment and man made targets. Concerning the human targets, specific data provided by each country must be used. The information concerning the population will be obtained with the data provided by the INSEE for France which gives a status of the French population in 1999 by district (INSEE, 1999). In Italy, ISTAT (the National Institute for Statistics) also gives this type of information based on the 1991 (ISTAT, 1992) and, soon, on 2001 census of Italian population by district or census unit.

To use these population data, some rules must be assumed to allocate a number of people to each mesh included in a district, as discussed in the paragraph concerning the quantification of environmental targets. If more precise results are required, information at the cadastral level should be taken into account. This second approach is more time consuming than the first one.

It has to be pointed out that other more specific information concerning some important environmental features, such as parks or protected zones are available from national environmental organisations, such as APAT in Italy, or Natural zone of faunistic and floristic interest in France (ZNIEFF).

Finally, some other information, such as that concerning the industrial site, has to be provided directly from the user, since it is not available to the general public. A specific procedure is proposed to fill these data, which can be used also to add information concerning special targets, such as sites concentrating high number of people, vital infrastructures, monuments, etc.

7.3 Vulnerability method and prioritisation of target vulnerabilities

The objective is to quantitatively assess the environmental vulnerability. With that aim, the Saaty multicriteria decision method (Saaty, 1984)*[11]* is applied, which is a ranking method using expert judgements and binary comparisons, based on four main steps:

- definition of the objective;
- description of the environment;
- organization of information in order to answer the problem;
- quantitative assessment of vulnerability factors based on the expert judgment.

To this end, the environment is described by means of three typologies:

- definition of targets categories: human, environmental and material. Each target category is subdivided in four types of targets. For human targets: staff of the site, local population, population in establishments visited by the public and users of communication ways. For environmental targets: agricultural areas, natural areas, specific natural areas, wetlands and water bodies. For material targets: industrial site, public utilities and infrastructures, private structures and public structures.
- definition of physical effects: overpressure, thermal radiation, gas toxicity and liquid pollution;
- definition of the impacts: integrity, economical and psychological impacts.

The information is structured to address the objectives of the study, adopting the following definitions of the vulnerability:

- for a class of targets and a given physical effect, the vulnerability of each type of target with respect to the others is evaluated from binary comparisons, obtaining the vulnerability of each class of target to each physical effect;
- for a class of targets, the importance of each physical effect with respect to the others is evaluated from binary comparisons, obtaining the overall vulnerability of each class of targets;
- finally, the vulnerability of each class of targets is compared to the others, obtaining the global vulnerability.

From this approach, the matrixes and the functions are derived combining the quantification factors of the targets and their vulnerability factors (52 functions are defined) to give the vulnerability index. These matrixes and functions allow to collect the expert judgement for determining the vulnerability factors of each vulnerability function. To this end, 38 experts, coming from various Countries and with different backgrounds (risk analysts, competent authorities, industrialists) were individually consulted (Tixier et al, 2003)*[12]*. After treatment of the questionnaires collected from the expert judgement, the vulnerability factors of the 52 functions were calculated from the eigenvectors of the matrixes. For example, the global vulnerability, V_{global}, of a study area results from the following combination of human, natural environment and material vulnerabilities (V_H, V_E and V_M):

$$V_{global} = 0.752 \text{ x } V_H + 0.197 \text{ x } V_E + 0.051 \text{ x } V_M \qquad (1)$$

Where the vulnerability of each class of targets depend on its vulnerability to the physical effects (overpressure = op, thermal radiation = tr, toxicity = tox, pollution = poll)

$$V_H = 0.242 \text{ x } V_H^{op} + 0.225 \text{ x } V_H^{tr} + 0.466 \text{ x } V_H^{tox} + 0.067 \text{ x } V_H^{poll} \qquad (2)$$

$$V_E = 0.071 \text{ x } V_E^{op} + 0.148 \text{ x } V_E^{tr}\ 0.277 \text{ x } V_E^{tox} + 0.503 \text{ x } V_E^{poll} \qquad (3)$$

$$V_M = 0.446 \text{ x } V_M^{op} + 0.410 \text{ x } V_M^{tr} + 0.069 \text{ x } V_M^{tox} + 0.075 \text{ x } V_M^{poll} \qquad (4)$$

In order to apply this methodology and assess the area vulnerability, the first step consists in the definition of the features of the study area: its size should be large enough to cover the effects of the expected accidental scenarios for the industrial site, and, for the purpose of vulnerability mapping, it should be divided into meshes. A 20 km x 20 km size for the study area, with 500 m x 500 m mesh size or less is suggested, where the mesh size may be reduced close to the industrial site, for a better visualisation of the vulnerability in that zone. Then, information about the various targets in the area has to be obtained from suitable commercial databases, and, possibly, completed with user data, to determine the quantification factors of each type of target to be inserted in the vulnerability functions. This requires to make a census of each target category and type in each mesh of the study area. In particular, the quantification factor is a dimensionless variable assuming values in the range 0-1, where 0 indicates the absence of the target in the area under exam and 1 indicates that the quantity of that target in the area reaches its expected maximum. Details about this procedure are reported in (Tixier et al., 2003)*[12]*.

The whole vulnerability functions are described in the deliverable D.4.A.*[13]*

7.4 Vulnerability mapping

The approach described above has been conveniently developed in the form of a GIS tool. In order to assess the vulnerability in the zone of interest, the following steps have to be performed (see Figure 26):

- select the study area and divide it into meshes;
- assess the vulnerability for each mesh, by identifying and quantifying the detailed target types of the categories human, environment and material included into the mesh;
- calculate the vulnerability indexes of the meshes;
- map the results.

These actions should be repeated for all the meshes of the studied area.

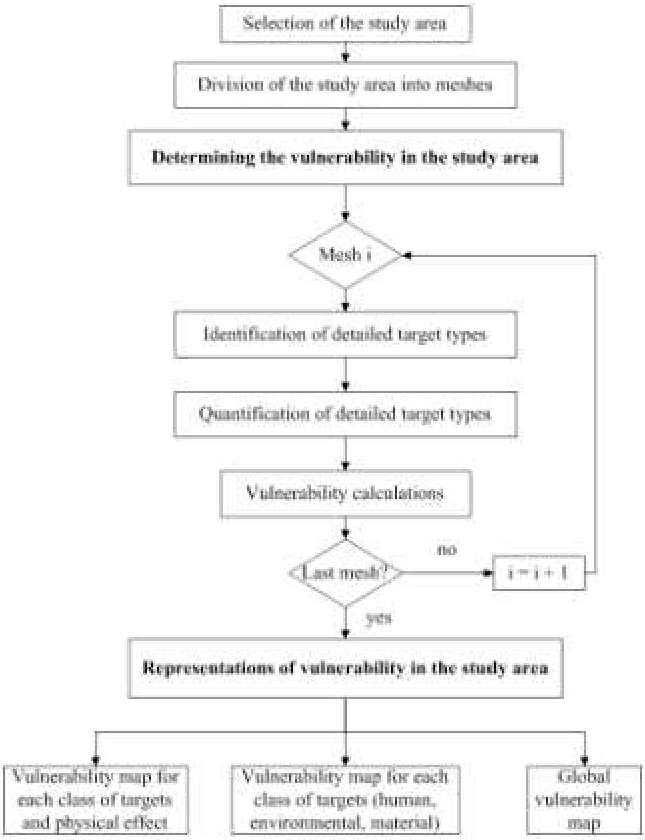


Figure 26: Structure of the GIS tool for vulnerability mapping

The study area will be a square centred on the industrial site (Figure 27 and Figure 28). Most required information concerning location and type of the various targets are rather easily available from commercial databases (such as Corine Land Cover, 2002, TeleAtlas, 1996, etc.) including data about land use, transportation networks and points of interest, and from census data of the resident population (in France available from INSEE, 1999); other useful information concerning the natural environment can be obtained from environmental organisations. Additional information, not included into commercial databases and concerning the industrial site, such as its boundaries or the exact location of special targets (for example, office buildings within the industrial site) can be easily introduced by the user.

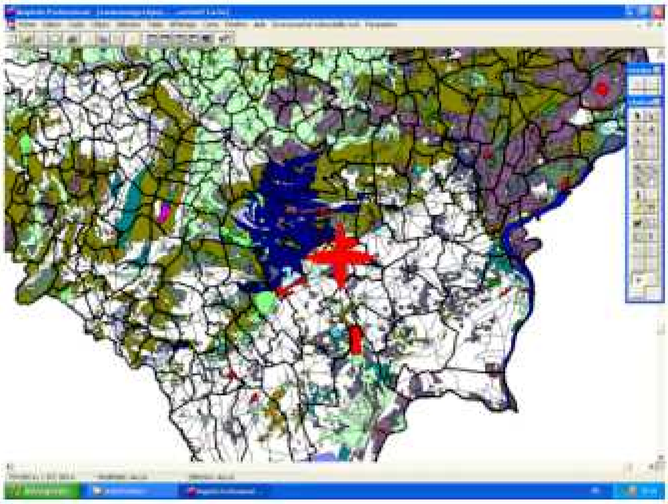


Figure 27: Localization of an industrial site on the map

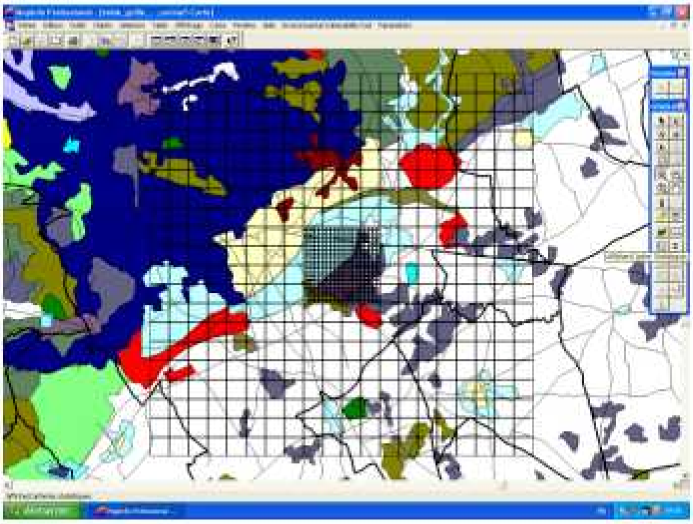


Figure 28: Study area 10 km x 10 km (mesh 500 m); inner grid 2 km x 2 km (mesh 100 m)

The GIS tool can be developed with any commercial GIS software (MapInfo, 2002; ArcView, 2000, etc.): the examples shown here were obtained with MapInfo, but an ArcView tool is available as well. In any case, the tool provides the user with procedures for selecting the study area, dividing it into meshes, and identifying and quantifying the different types of targets into each mesh. The quantification step is fully automated for the targets belonging to natural and built-up environment, based on the ratio of the area covered by each target of this type to the area under exam. The same procedure cannot be adopted for human targets, where the quantification factors have to be determined based on the maximum number of persons expected in the area (for details see Tixier et al., 2003)*[12]*: suitable default values are suggested to obtain the quantification factors, which, however, can be modified by the user.

7.5 Example

In order to validate and to underline the contribution of the vulnerability assessment, the methodology was applied on several test cases.

In the next part of this paragraph, both the environment of the French test case of the ARAMIS project and the deduced maps of vulnerability are presented.

The French test-site is located in the Haute -Normandie region in France.

7.5.1 Description of the environment of the French test-site

The study area (Figure 29) is composed of two grids:

- the main grid is a square of 20 km per 20 km with meshes of 500 m per 500 m
- the inner grid is a square of 2 km per 2 km with meshes of 50 m per 50 m

The inner grid allows to obtain a more precise representation of the vulnerability close to the industrial site.

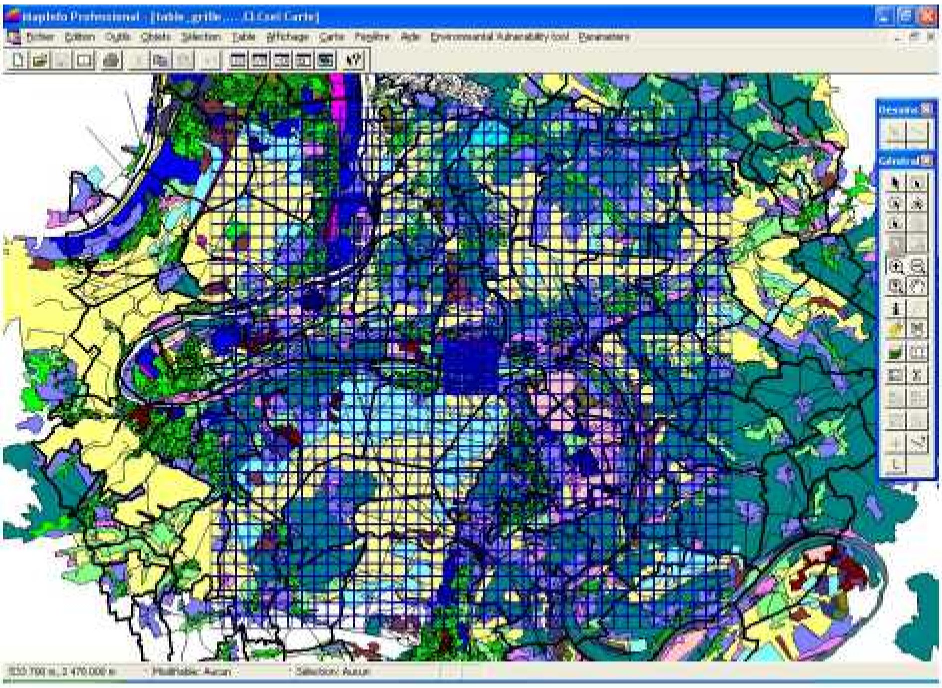


Figure 29 : Study area of the French test-site

This environment contains various stakes which are detailed in Figure 30 and Figure 31.

Human stakes (Figure 30), are mainly composed of districts with a very low and low density (ranging from 0 to 1000 people per square kilometre). Only about 20% of the study area presents districts with a medium value of density (between 1000 to 2000 people per kilometre square).

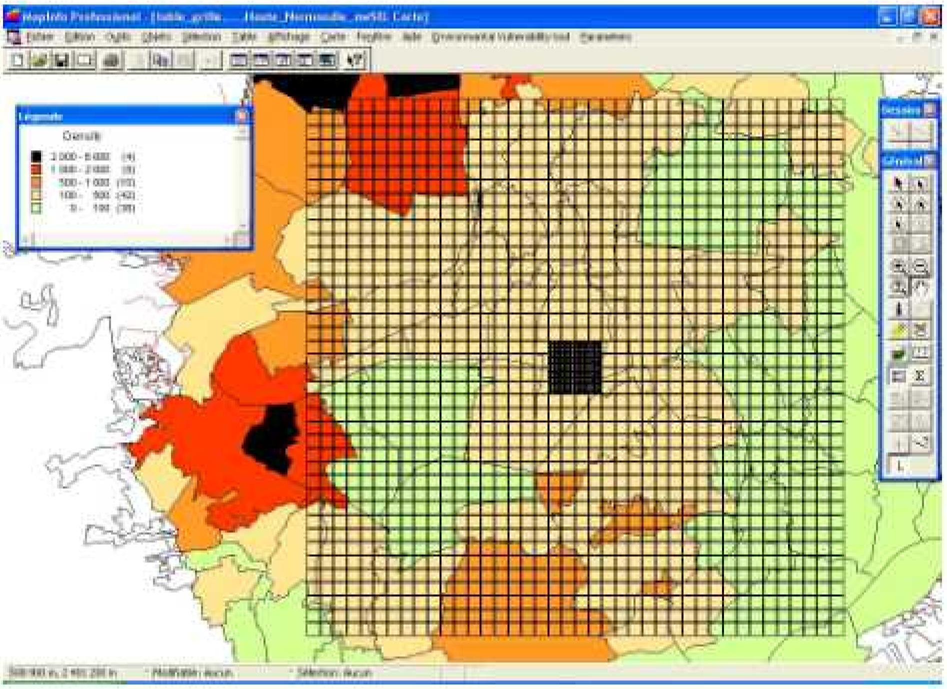


Figure 30: Human stake of the study area

Natural and material zones are mainly composed of agricultural areas and of forests and semi natural areas (Figure 31). The other part of the study area is characterised by artificial areas, wetlands and water bodies.

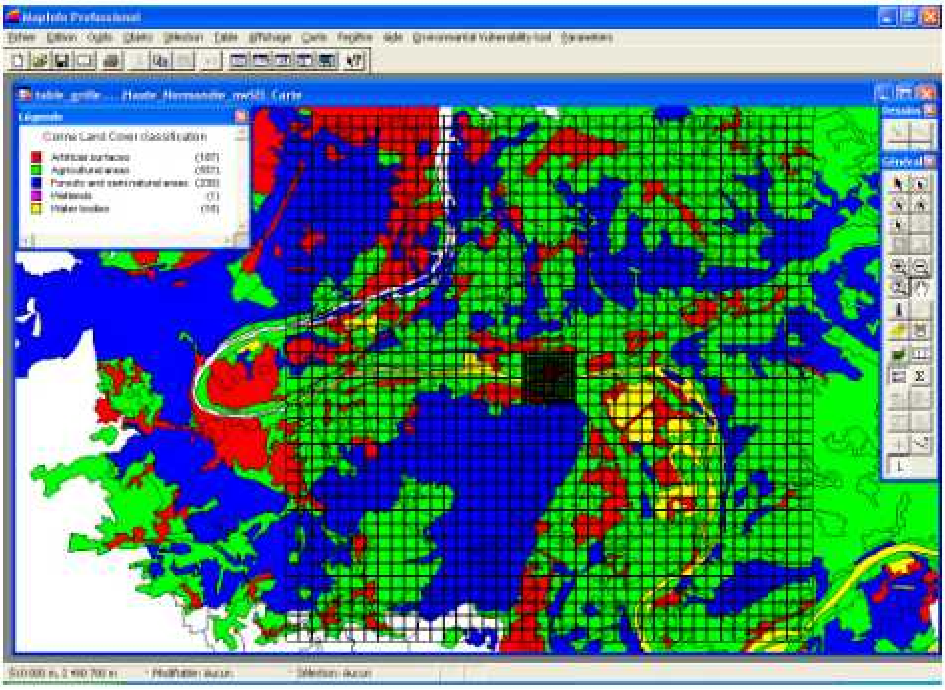


Figure 31: Natural and material stakes of the study area

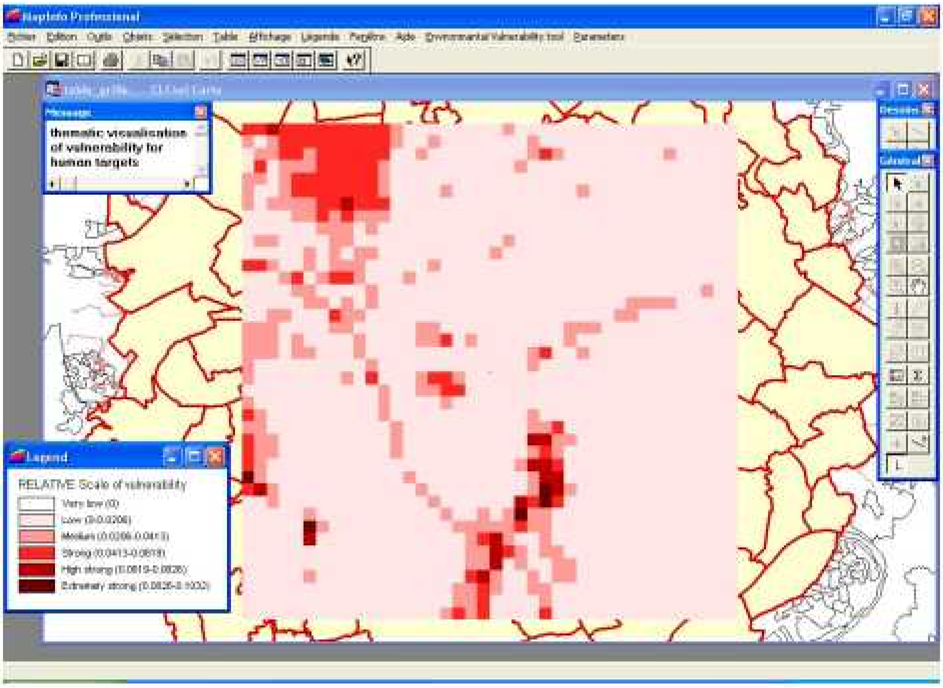
In a general way, from this first analysis, one can say that the vulnerability for the whole area might be low or medium.

Nevertheless, the following maps of vulnerability give an exact value of the vulnerability and also the location of sensitive spots.

7.5.2 Presentation and analysis of vulnerability results

In this part, two different sets of vulnerability maps are presented and commented, which are:

- a set of vulnerability maps for each type of targets (human, environmental and material) and a map of global vulnerability
- a set of vulnerability maps for each physical effect (overpressure, thermal radiation, toxicity and pollution)



thematic visualisation of vulnerability for human targets

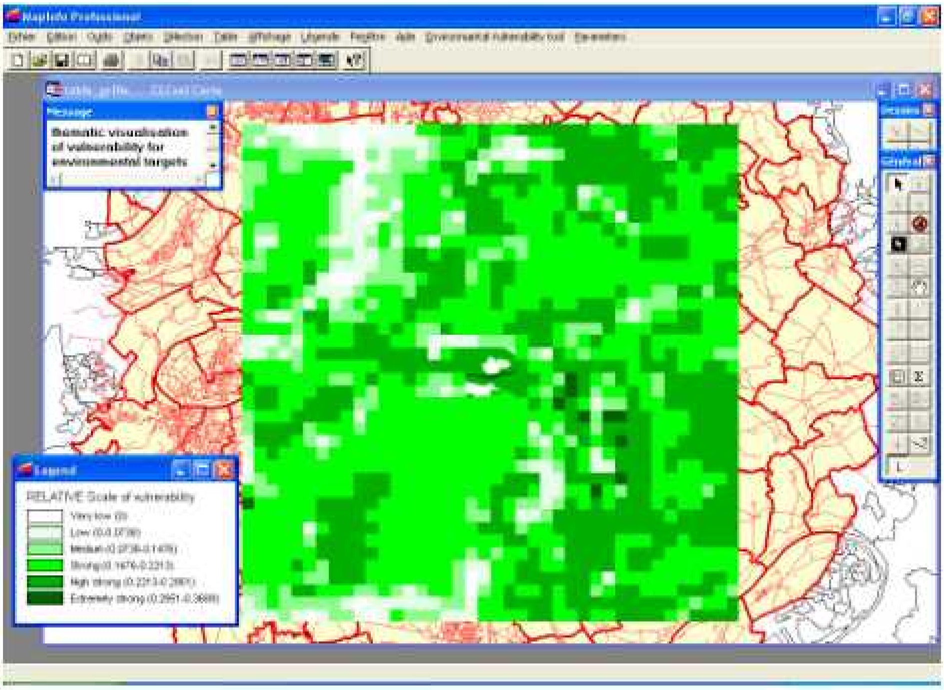
RELATIVE Scale of vulnerability

☐	Very low (0)
☐	Low (0-0.0206)
☐	Medium (0.0206-0.0413)
■	Strong (0.0413-0.0619)
■	High strong (0.0619-0.0826)
■	Extremely strong (0.0826-0.1032)

Figure 32: Map of the human vulnerability

The human vulnerability (Figure 32) is very low in great part of the study area. Indeed, the human vulnerability is strongly correlated to the population density and to urban or semi urban areas (artificial areas). So only, the artificial areas present some spots of vulnerability with a low value of vulnerability due to the low value of population density in our study area.

The inner grid is characterized by a very low vulnerability for the industrial site where there are about 600 workers.



thematic visualisation of vulnerability for environmental targets

Figure 33: Map of environmental vulnerability

A great part of the study area is characterized by a medium vulnerability value (Figure 33).

Only the part which corresponds to the artificial areas has a low value of vulnerability. In the inner grid, the presence of water bodies increases the value of environmental vulnerability.

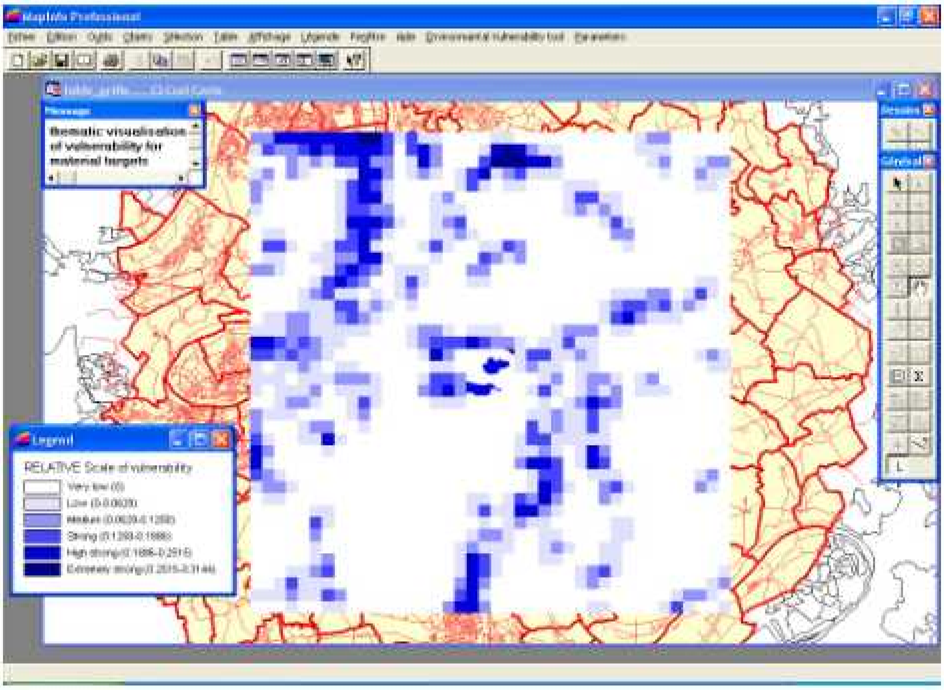
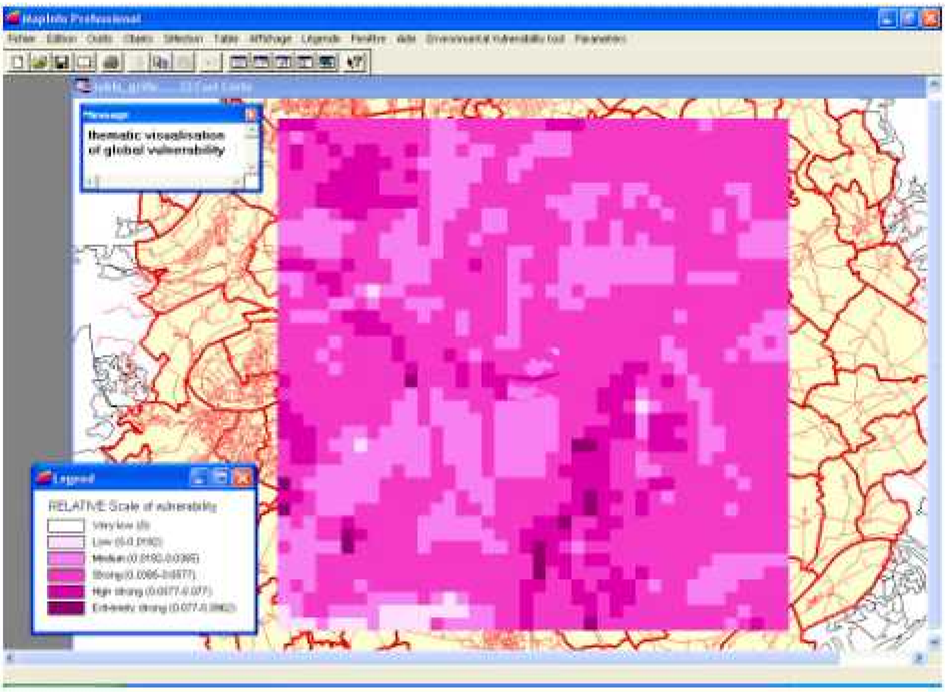


Figure 34: Map of material vulnerability

The material vulnerability map (Figure 34) underlines some specific spots of medium vulnerability mostly due to the location of artificial areas in the study area. In the inner grid, close to the industrial site two spots of high vulnerability are present.

From the comparison of the three maps (human, environmental and material) we can deduce that the spatial location of the most vulnerable zones is really similar for the human and the material targets. We can also point out that the spatial location of most vulnerable areas on the map of environmental vulnerability are opposite from those for human or material vulnerability maps.

From the three previous maps of vulnerability (human, environmental and material), the map of global vulnerability (Figure 35) can be deduced.

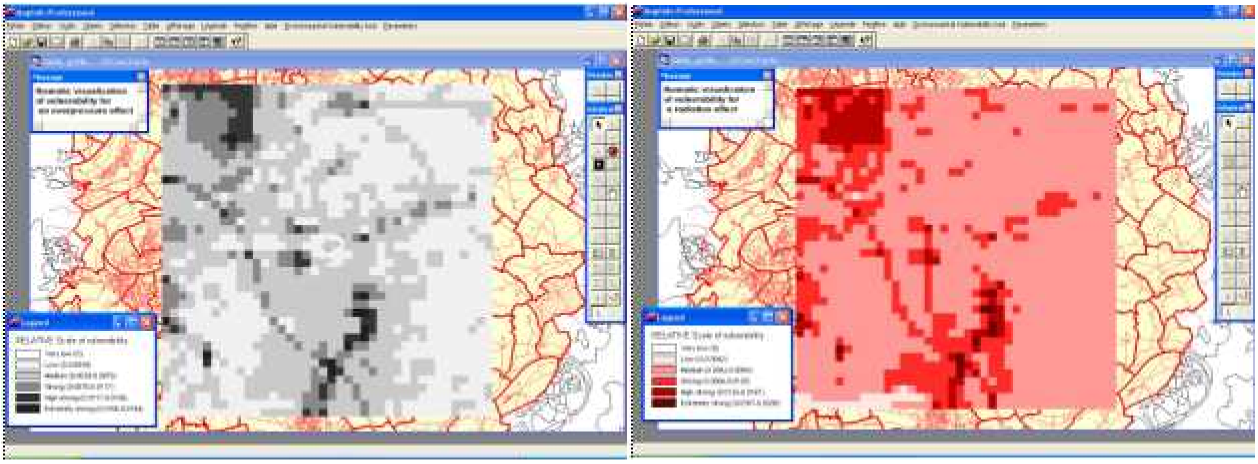


thematic visualisation of global vulnerability

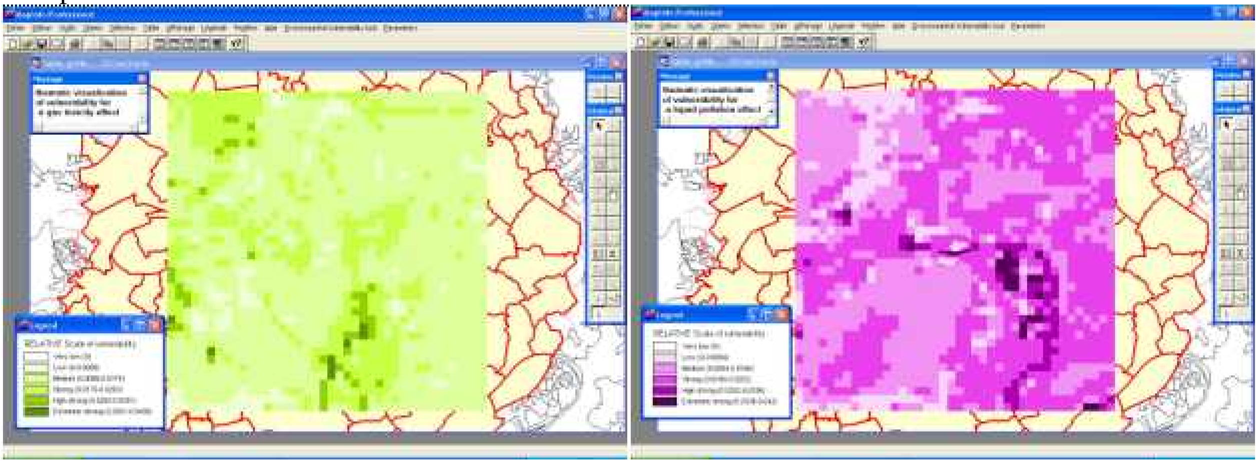
Figure 35: Map of global vulnerability

The global vulnerability is low for this study area. This map is clearly linked, even for the spots of higher vulnerability, to the map of human vulnerability which represents 75% of global vulnerability.

The values of vulnerability to physical effects (Figure 36) are low for overpressure and thermal radiation, and medium for toxicity and pollution effects. Concerning the maps of vulnerability for overpressure, thermal radiation and toxicity, the location of the most vulnerable areas are linked to the human vulnerability. For pollution effect, the spots of vulnerability are linked to natural environment.



Overpressure Thermal radiation



Toxicity Pollution

Figure 36: Maps of vulnerability for each physical effect

7.6 Discussion

The vulnerability values obtained in the previous phases can be mapped, for each mesh, by associating to the calculated values of vulnerability a class of vulnerability represented with a characteristic color.
Three cartographic representations of vulnerability can be obtained:

- a global vulnerability in the study area;
- a vulnerability of a class of target (human, environmental or material) for all physical effects;
- a vulnerability of all the targets for a given physical effect (overpressure, thermal radiation, toxicity and pollution).

The maps of the vulnerability layers relevant to each physical effect (V_{op}, V_{tr}, V_{tox} and V_{poll}) should be then compared with the corresponding severity maps. These two representations (severity and vulnerability) provide the end users, (plant operator, risk analysts and/or the competent authorities), with a complete picture of the situation in the area surrounding the industrial site.

This information not only allows to draw considerations on the risk of a specific industrial site in order to validate the level of safety, but also highlights dangerous situations, from a vulnerability or a severity point of view. Therefore, specific efforts can be made, in order to improve the level of safety of the industrial site.

In the future, the representation can be improved with a normalised scale and corresponding colours, to enable comparison of the vulnerability between several zones.

8. Using ARAMIS for further applications and fields of research

8.1 Developing bow-ties and scenarios

Besides providing tools such as generic fault and event trees and associated lists of safety functions and barriers, MIMAH and MIRAS provide also a conceptual and methodological framework for risk analysis. The elements presented briefly in this document, generic bow-ties and safety functions and barriers, gave precise definitions which are now shared by all the project partners and the Review Team. They are also used for the development of other fundamental parts of the methodology such as severity computation or management efficiency assessment.

In parallel, probabilities (frequencies/probabilities of initiating events, frequencies of critical events, transmission probabilities) have been studied all along the branches of fault and event trees. Even if some results were obtained, this part of ARAMIS shows that, on one hand, there is a lack of reliable data and, on the other hand, coupling between the available data and the generic trees is a major difficulty. A European data collection program should be really of interest and would result into an improvement of ARAMIS.

Moreover, ARAMIS has also shown the need to harmonise the risk acceptation criteria in the different countries of the European Union. Some scientific criteria have to be determined in order to harmonise the different approaches for the acceptability of risk.

Improvements will be possible thanks to the work carried out in the European Working Group on Land Use Planning co-ordinated by the JRC-MAHB.

The "bow-tie" approach with the concept of "safety functions and safety barriers" can have promising applications in other fields, like the occupational safety or the hazardous substances transportation safety.

8.2 Evaluating barrier performance

In the industries, the identification of 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. One of the strengths of ARAMIS is to focus on the influence of safety systems and safety management in the definition of accident scenarios. This approach intends to give an acute estimation of the risk level.

In taking into account the safety systems and the safety management actually existing on site in order to define Reference Accident Scenarios, the efforts made by industry are recognised and this allows promoting investments in safety systems.

This approach is mainly based on the evaluation of the performance of the safety systems. However, even if the IEC 61508 and 61511 standards give the criteria to assess the level of confidence of safety instrumented systems, it is difficult to determine the parameters, like "Safe

Failure Fraction (SFF)" and "Fault Tolerance (FT)", for a subsystem. Concrete data on equipment or methods in order to determine these parameters have to be established and made available.

Moreover, some active safety barriers are not purely automated and require an human intervention or an human diagnosis. There is a need for clear criteria in order to take into account this human factor in the evaluation of performances of these barriers.

8.3 Evaluating Safety Management Structure and Culture

8.3.1 General

The experience from the case studies and the feed back from the review panel makes clear that the benefit of the ARAMIS methodology of evaluating safety management structure and culture lies to a high degree in the qualitative feed back from the audit process and the safety culture investigation to the company on specific weak points and possible improvements in management. The quantification process still contains many uncertainties, though the process is transparent and can provide help to prioritising safety management issues in relation to certain safety barriers in site-specific conditions.

Understanding safety management in terms of recognising and structuring its essential, important and “orthogonal” factors and functions is still not well-established, and as such ARAMIS is just one achievement along the way of a long-term research effort. We may expect that the ARAMIS set of recognised safety-management structural factors and safety-culture dimensions will alter and be adjusted as our scientific insights improve. Though, the ARAMIS methodology points at a promising way of assessing safety management effectiveness:

- It has been shown that the assessment can be performed with an affordable amount of effort, also by assessors that have not been involved directly in the development of the method;
- The focus on the relation between safety management activities and concrete safety barriers turns the evaluation into an assessment of tangible activities and processes, that are easy to understand by the companies and useful for their improvement process.

8.3.2 The Safety Management Audit

The general conclusion of the ARAMIS audit project is that the tool has great potential. The idea of focusing the assessment of management influences on specific scenarios and barriers got general support from the companies as a helpful addition to their assessment tools. However, there is still considerable work to do in crystallizing this tool out and making it auditor-friendly. There is much work still to be done to arrive at a practicable tool which will incorporate all of the development work done in the series of EU and national projects stretching from Manager, through PRIMA and I-Risk (Oh, J. I. H. and others, 1998) to ARAMIS.

8.3.3 The Safety Culture Questionnaire

The questionnaire has been developed from earlier work in similar safety-critical domains, which has given evidence, that a number of outcomes have definite diagnostic value with respect to the safety level of a site or company. Until now, these tools have been used as qualitative tools, often in a comparative way. In the ARAMIS context, an absolute reference should be provided, and more research is required to provide a sound basis for such a reference. To that end, it is intended to extend the data collection and to develop a repository of data that can shed light on the ranges of possible outcomes in relation to both actual safety performance (accidents and incidents) and outcomes of the Safety Management Audit.

8.3.4 Quantification of efficiencies

There is a lack of objective empirical information on the relative importance of safety management factors in relation to the reliability of barriers or the occurrence of initiating events. So far, this type of information is collected from expert opinion elicitations. Notwithstanding the importance of the knowledge of experts in industrial safety, these elicitations have a tendency to become self-confirming when not supported by some independent other source of data.

In principle, it is possible to collect useful empirical information from (statistical) incident and accident analysis, but it needs to be complemented by surveys of actual safety management performance (using audits and the questionnaire) in the plants that contribute to these incident data. This can give us, using Bayes' theorem on conditional probability, the ratio between failure rate under condition of deficiencies in a certain management factors and failure rate without this deficiency, which is the influence factor that we are looking for.

Such combined statistical incident/accident analyses and safety management surveys require (apart from substantial effort) that a consistent taxonomy of management factors be used for both the incident/accident analyses and the safety management surveys.

8.4 Mapping the Risk Severity of a plant and Mapping the Vulnerability of its surroundings

Many improvements are still possible for the risk severity and the vulnerability assessment. These have already been discussed in the corresponding chapters of this user guide. However, what is probably the most important is to be able to use these results in a land use planning decision making process. The crossing of severity and vulnerability maps should enable to take decisions to either reducing the severity by modifying the plant or its organisation or to reduce the vulnerability by moving the targets (expropriation) or by reinforcing the structure. The building of these rules is not only a scientific matter. It has to do with the land use planning policy. Yet, once they are decided, their implementation may require some adaptation of the ARAMIS tools, for example in terms of threshold definition for the severity or refinement of the vulnerability assessment. These will be made easier by the existence of precise needs of end users, which themselves will rise from the availability of a method like ARAMIS. The long term result should be a global improvement of the land use planning methods.

9. References

[1] "Deliverable D.1.C. - Report presenting the final version of the Methodology for the Identification of Reference Accident Scenarios", ARAMIS Project - 5th Framework Program of the European Community, 59 pages + 15 appendices, July 2004, Mons (Belgium), (Delvosalle C., Fiévez C., Pipart A.)

List of the appendices cited in the text :

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

[2] DGRNE (Direction Générale des Ressources Naturelles et de l'Environnement), Walloon Region Ministry, Belgium, 2000, *Vade Mecum: Spécifications techniques relatives au contenu et à la présentation des études de sécurité*, Cellule Risque d'Accidents Majeurs

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

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

[5] Deliverable D.3.B "Methodology to determine a Safety Management Efficiency Index ", Nijs Jan Duijm, Henning Boje Andersen, Andrew Hale, Louis Goossens, Frank Guldenmund

[6] W.G. Johnson, "MORT - the Management Oversight & Risk Tree", SAN 821-2, February 1973

[7] "Purple book", Guidelines for quantitative risk assessment, CPR 18E, Committee for the Prevention of Disasters, Den Haag, 1999.

[8] Deliverable D.2.C "THE RISK SEVERITY INDEX" WP 2: Severity evaluation Casal, J.; Planas, E.; Delvosalle, C.; Fiévez, C.; Pipart, A.; Lebecki, K.; Rosmus, P.; Vallee, A

[9] USDE (U.S. Department of Energy), 2000. *ERPGs and TEELs for chemicals of concern*. Rev. 16. Report WSMS-SAE-00-0001. http://tis-hq.eh.doe.gov/web/Chem_Safety/teel.html.

[10] "Yellow book", Methods for the Calculation of Physical Effects, CPR 14^E, Committee for the Prevention of Disasters, Den Haag, 1997.

[11] Saaty T.L. 1984. Décider face à la complexité. *Les éditions ESF*.

[12] Tixier J. et al.. Assessment of the environment vulnerability in the surroundings of an industrial site, ESREL 2003, Maastricht, Pays-Bas, 16-18 juin 2003

[13] Deliverable D.4.A "Guide describing the methodology to calculate the spatial vulnerability index V" WP 4: Environment vulnerability Tixier J., Dandrieux A., Dusserre G., Mazzarotta B., Di Cave S., Bubbico R., Londiche H., Debray B., Hubert E., Rodrigues N.