Chapter IV: RISK ASSESSMENT

Version 2.0 – January 2007

Table of content

1. RISK ASSESSMENT

Contributing author	Main contributions	Organisation	e.mail
Angunn Engebø	Chapter coordinator	DNV	*Angunn.Engebo@dnv.com*
Sandra Nilsen	RA principles	Hydro	*Sandra.Nilsen@hydro.com*
Christian Kirchsteiger	Modelling risk	JRC	*christian.kirchsteiger@jrc.nl*
Lionel Perrette	Safety plan	INERIS	*Lionel.Perrette@ineris.fr*
Myriam Merad	Risk perception	INERIS	
Henning B. Andersen	Methodology	Risoe	*henning.b.andersen@risoe.dk*
Henning B. Andersen	Human factors	Risoe	*henning.b.andersen@risoe.dk*

Contributing reviewer	Information reviewed	Organisation	e.mail

1.2 DEFINITIONS AND RISK ASSESSMENT PRINCIPLES

The objective of risk assessment is to evaluate the risk related to a specific activity for the purpose of managing this risk in an effective way.

1.2.1 Definitions

Acceptable risk, Tolerable risk	Risk which is accepted in a given context based on the current values of society
Consequence	Harm related to accidental event
Deterministic risk analysis	Analysis to determine the greatest level of harm possible
Frequency	The number of times a repeted event occurs over a period of time
Harm	Physical injury or damage to the health of people, or damage to property or the environment
Hazard	Potential source of harm
Probabilistic risk analysis	Analysis estimating the probability of occurrence of harm and the severity of that harm
Probability	The likelihood that a certain event will occur. The probabilityis always between 1 and 0. If the probability is 1, the event is certain to take place, if the probability is 0 the event will never take place.
QRA	Quantitative Risk Assessment.
Risk	Combination of the probability of occurrence of harm and the severity of that harm
Risk analysis	Systematic use of available information to identify hazards and to estimate the risk
Risk assessment	A risk analysis followed by a risk evaluation

Risk control	Controlling the residual risk by means of risk reduction measures
Risk evaluation	Procedure based on the risk analysis to determine whether the tolerable risk has been achieved
Safety	Freedom from unacceptable risk
Systematic risk management	An iterative process of risk assessment and risk reduction

1.2.2 Safety management principles

Two different safety management principles are possible: Consequence Based Safety Management will claim that the worst conceivable events at an installation processing hazardous materials should not have consequences outside certain boundaries, and will thus design safety systems to assure this. Risk Based Safety Management maintains that the residual risk should be analysed both with respect to the probabilities and the nature of hazard, and hence give information for further risk mitigation. This implies that very unlikely events might, but not necessarily will, be tolerated.

1.2.2.1Risk Based Safety Management

Risk based safety management is the philosophy in line with central regulations and legislation in Western countries increasingly requiring risk assessment and documentation.

The Risk Based Safety Management (often called risk management) principle is that some risks, specified through risk acceptance criteria, should be removed or reduced to meet safety requirements (residual risk level objectives). However, both prescriptive requirements (detailed standards) and goal-oriented requirements (risk based decisions) have a role to play in design of processes and installations.

The Risk Based Safety Management is a systematic approach which measures risk through risk analysis methods and relates it to established risk acceptance criteria for the identification of design specifications or need for risk reduction measures. Beyond implementing risk reducing measures in order to meet tolerable risk level, such measures should also be implemented if further risk reduction can be obtained at costs lower than the benefits obtained. This is often referred to as the ALARP principle. They can either be consequence reducing measures or accident probability reducing measures. Probability reducing measures should be preferred.

The principle is illustrated in the figure below

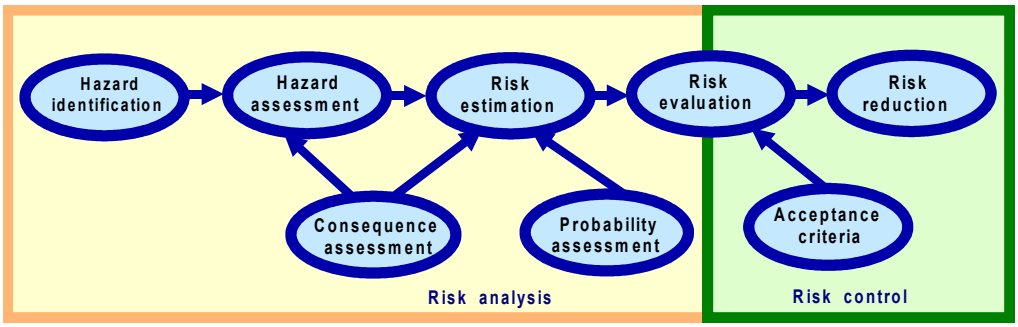


Figure: Risk Based Safety Management

1.2.2.2The ALARP principle - As Low As Reasonable Practicable

Below a certain risk level where where the hazard is in the unacceptable area and risk cannot be tolerated whatsoever; normally defined by risk acceptance criteria, the ALARP principle (As

Low As Reasonable Practicable) should be applied in order to optimise risk reduction. In such cases cost benefit analyses should be used in order to evaluate different risk reducing options. Risk reducing measures should be implemented if the cost is not disproportoinate relative to the benefits of risk reduction.

The ALARP principle is illustrated in the figure below

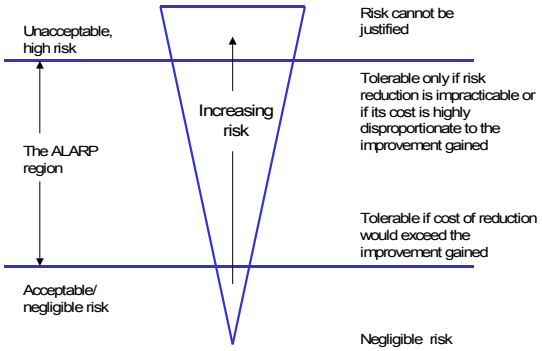


Figure: The ALARP principle

1.3 RISK ASSESSMENT METHODOLOGIES

Status: Risk assessment methodologies are in principle applicable to any object or activity. Risk assessment methodologies are frequently applied for risk assessment of flammable gas applications, though there are not many examples of specific hydrogen studies so far.

Risk Assessment studies should preferably be undertaken by multidisciplinary teams, all though the effort should be in proportion to the risk being assessed. There are several risk assessment methods available, and one should select the method most applicable to the object analysed and the purpose of the assessment.

1.3.1 Risk assessment process:

The risk assessment process is an iterative process, as shown in the figure below: The risk is assessed, as well as the effect of risk reduction measures, until the risk inflicted by the system assessed (with implemented risk reduction measures) is evaluated as tolerable.

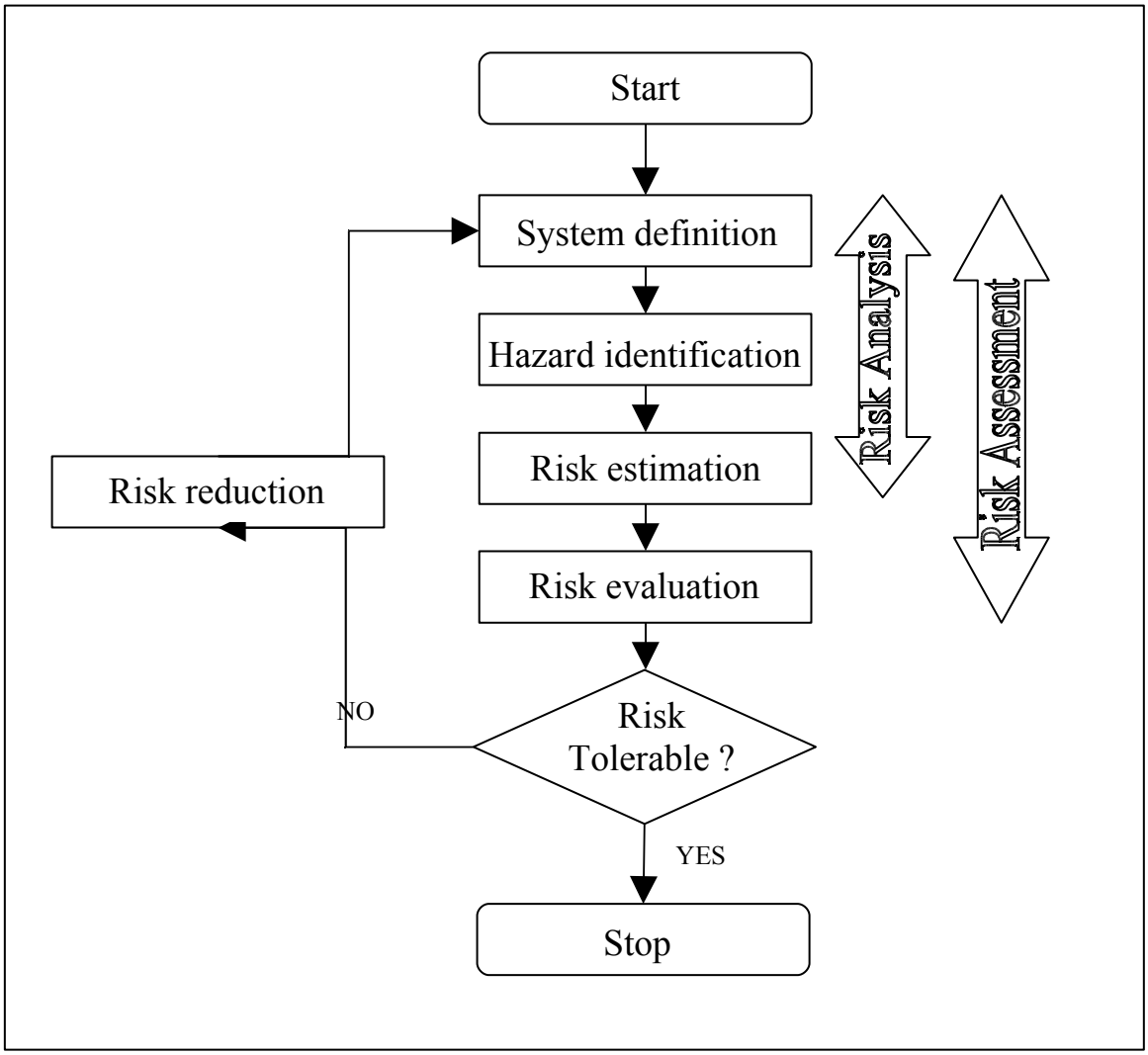


Fig 1-1: Risk assessment process

But even when the assessed risk is evaluated as tolerable, the risk assessment process is not finished. The society's safety objectives and even an enterprise's safety objectives are more ambitious than maintaining the risk at a fixed level : risk assessment and risk reduction is also an iterative process through time. Indeed, change in state of the art enabling further risk reduction will eventually lower the level of tolerable risk. Besides, new knowledge about the hazards evaluated may also render risk assessments obsolete.

1.3.2 Hazard identification methodologies

The hazard identification is the initial step in risk assessment, and thorough hazard identification is of indisputable importance to the worth of the risk assessment. The purpose of the hazard identification is to identify all hazards of relevance. Each hazard should be described in terms of accident(s) it may lead to. In order to identify the hazards which may arise, a systematic review should be made of technical as well as operational conditions which may influence the risk. Historical records and experience from previous risk analysis do provide a useful input to the hazard identification process. Examples of this type of methodology are checklists, hazard indices and review of historical occurrences.

The hazard identification should not only consider the initial events, but also include the chain of events causing local and remote impairment, loss or damage.

Hazard identification of a particular system, facility or activity may yield a very large number of potential accidental events and it may not always be feasible to subject each one to detailed quantitative analysis. In practice, hazard identification is a screening process where events with low or trivial risks are dropped from further consideration. However, the justification for the events not studied in detail should be given. Quantification is then concentrated on the events which will give rise to higher levels of risk.

Fundamental methods such as Hazard and Operability (HAZOP) studies, Fault trees, Event tree logic diagrams and Failure Mode and Effect Analysis (FMEA) are tools which can be used to identify the hazards and assess the criticality of possible outcomes. These methods also have the advantage of being sufficiently general for use on hydrogen facilities without specific adaptation.

The HAZOP technique consists of the application of a formal systematic detailed examination of the process and engineering intention of new or existing facilities to assess the hazard potential of operation outside the design intention or malfunction of individual items of equipment and their consequential effects on the facility as a whole. The technique is to divide the process into natural sub-section and use a set of guidewords to identify possible deviations with hazardous potential. The technique is well suitable for hydrogen applications, especially for the more complex systems.

The Failure Mode and Effects Analysis (FMEA) is a qualitative technique for systematically analysing each possible failure mode within a system, and identifying the resulting effect on that system, the mission and people. FMEA is highly suitable for reliability assessment and can e.g. be used for in depth study of a critical part of a system. The FMEA may be extended with a criticality analysis (CA); a quantitative procedure which ranks failure modes according to their probability and consequences (i.e. the resulting effect of the failure mode on system, mission or personnel) and is then named a Failure Mode and Effects Criticality Analysis (FMECA).

The FMEA and FMECA, were originally developed by the NASA as a means of assuring that hardware built for space applications had the desired reliability characteristics. In the offshore industry FMEA and FMECA have been increasingly utilised during the last years. FMECA was also used in the European Integrated Hydrogen Project (EIHP2) for development of guidelines for inspection and maintenance of hydrogen applications.

The initial step of an FMEA is a functional description of the system and the division of the system into subsystems and items. Each item is given an identification code. For each item the purpose/function of the item is then described, and possible failure modes are listed and analysed with respect to causes and possible consequences. Means for detection of failure modes and mitigation/repair are also analysed.

1.3.3 Risk analysis methodologies

The risk assessment tasks will depend on the purpose of the risk assessment. The risk assessment will normally involve a comparison of a calculated risk level with criteria for acceptable risk level. The acceptable or tolerable risk level would be based on the enterprise's own safety standards and/or risk criteria established by the authorities. The risk assessment may also include comparison of alternative designs or activity plans.

If the risk is not controlled (acceptance criteria are not met) or the objective is to reduce the risk further to a level as low as reasonably practicable (ALARP), options of risk reducing measures should be addressed and their desirable effect should be estimated. This should indeed be a multidisciplinary exercise, preferably involving people responsible for (future) operation of the object evaluated. The process of the risk assessment includes thus a re-evaluation of the risks and of risk reduction measures based on cost-benefit analysis.

If the risk is controlled and the acceptance criteria are met, the chosen concept including the assumptions might be acceptable, but not the optimum from a cost-benefit point of view. In order to optimise the design, sensitivity calculations may be carried out.

Risk analysis methodologies are often grouped into three categories: qualitative, deterministic and probabilistic. A qualitative analysis will normally characterise hazards with respect to likelihood and severity of consequences without quantification. A deterministic analysis will quantify the consequences of the most severe event possible, while the probabilistic analysis will quantify the probability and consequences of different scenarios developing from the possible initial events. The probabilistic analysis, also called quantitative risk analysis, is further described in Ch 4.4.

The qualitative analysis will normally include an element of rough quantification though, and the deterministic analysis will also have an element of probability evaluation involved in determination of which events are possible. The detailing level of the analysis will primarily depend on the anticipated risk, the knowledge of the system analysed and of the quality of data and models available. Indeed, a comprehensive and detailed analysis based on limited information, poor data or inadequate models would be a waste of resources.

Rapid Risk Ranking [5] is a semi-quantitative risk analysis methodology adapted for hydrogen applications in the European Integrated Hydrogen Project (EIHP2). The method involves elements of quantification for both likelihood and consequences, but the effort is focused on the most severe consequences, as well as the most likely outcomes of the initial events analysed. The risk is then presented visually in a way that facilitates risk evaluation and comparison of different applications/plants/installations analysed.

GAPS: Though risk assessment methodologies are frequently applied to flammable gas applications, there are only a few examples on risk assessments made for hydrogen applications.

Recent progress: The Rapid Risk Ranking methodology has been adapted to an applied on several hydrogen applications.

1.4 ACCIDENT DATA-BASE, FAILURE RATE DATABASE

It is acknowledged in most industries that it is of utmost importance to learn from accidents, incidents and failures of the past to prevent them to happen in the future and to mitigate their consequences. I.e. an important part of the work towards achieving effective risk control one should learn from events, failures and errors committed in the past, and not only within their own industry or company, but also look beyond and draw lessons from elsewhere.

The use of incident and failure rate databases as a management tool has shown that it provides an opportunity for an organisation or company to check its performance, learn from its mistakes, and improve its management systems and risk control. Comprehensive knowledge of events having the potential for inducing hazardous situations or loss of production, will also contribute to the corporate learning and memory. On company or plant level, the lessons to be learned from consulting such databases are both qualitative as well as quantitative. They can range from the identification of component/system failures, accident scenarios or initiating events not being predicted in advance to quantitative statistical calculations and estimations to be used in reliability, maintainability or risk studies. They also increase the culture of personnel working in risky technology industries by making them aware of the factors (technical, organisational, human, etc.) and the dynamics that led to accidents or failures. On a national or international level, Safety Authorities are utilising accident databases as an operative and a management tool in several ways, such as following up of the overall safety level within the area of the authority's interest, resource allocation concentrated and prioritised on the most accident-prone areas and in accident prevention. Accident information taken from a database may also support surveillance visits, in conducting accident investigations and in the work of developing of rules and regulations.

1.4.1 Recent progress

1.4.1.1 Hydrogen Accident Databases

Hydrogen Incident and Accident Database (HIAD)

Under the EU's 6th framework programme, a Network of Excellence project "HySafe – Safety of Hydrogen as an Energy Carrier" was established and defined. In this project, a specific Work Package (WP) was devoted to database development, namely the WP5 – Hydrogen Incident and Accident Database (HIAD).

HIAD is planned to be one of the tools for communication of risks associated with hydrogen to all partners in the HySafe Consortium and probably beyond at a later stage. In addition, HIAD will serve as a common methodology and format for data collection and storage. HIAD is aiming to hold high quality information of historical accidents and incidents related to hydrogen production, transport (road/rail/pipeline), supply and commercial use. The database will be maintained such that it is updated with the latest information concerning each event for example in order to take advantage of results from accident investigations. Hence, HIAD will, when fully

operable be an important source for most tasks constituting a risk analysis process, such as hazard identification, estimation of probabilities and consequences and to propose risk reduction measures.

During the work with developing HIAD, the challenge was to develop a tool that should serve various purposes such as being a data source for doing risk assessments and reveal trends and being a source for experience transfer and risk communication. In addition it should be easy to use, so the user friendliness encompassing the tasks of recording and extraction of information/data by having a professional and modern user interface, was hence given high priority.

The building blocks of HIAD are illustrated in the figure below.

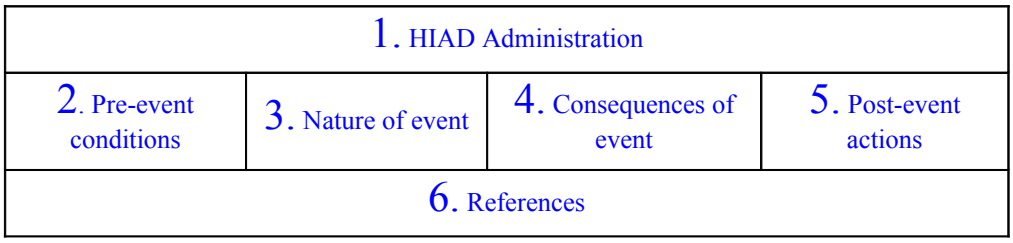


Figure 2. HIAD building blocks

Information held by HIAD and being relevant for risk assessment exercises and related modelling development work could be such as environment/location and application, release size and volume, ignition sources and ignition time ('ignition modelling'), fire characteristics, description of consequences (input to work with safety distances), damage cost, and causal relations (input to fault tree construction). All information recorded for each event will in general be important for the corporate learning about risks related to hydrogen applications and serve as ballast for the risk analysts in their hazard identification phase of any risk analysis. This work is by experience considered as the most crucial one in the sense that hazards and risk elements not captured here will not be included in the further risk assessment process.

It has been decided that HIAD should not be limited to real accidents and incidents, but should also include hazardous situations and near-misses. An example of this is that HIAD should contain all hydrogen releases irrespective of size/volume and not only those that ignited. One benefit of this is enabling the estimation of ignition probabilities from the HIAD data.

H_2Incidents

US Department of Energy has published a tool for reporting of hydrogen incidents and a database called H_2Incidents at http://www.h2incidents.org/. This database is designed as a simplified version of HIAD, described above.

This database has focus on initiating events and pre-event conditions and could be a useful tool for improving check lists and hazard identification tools. The lack of scenario orientation (nature of event) makes it less useful for evaluating likely progress of an initial event.

1.5 MODELLING AS A TOOL FOR QUANTITATIVE RISK ASSESSMENT

The objective of this subchapter is to describe the basic principles of Quantitiative Risk Assessment (QRA) as applicable to estimate the safety performance of hydrogen systems. Each QRA step, ending in the development of overall Event Trees estimating the risk of an installation/activity, will briefly be introduced and a link to the corresponding tools e.g.: How can the information from incident/accident databases, accident progression models and consequence modelling be utilised in order to model event trees. Corresponding knowledge gaps are identified as well.

1.5.1 Quantitative Risk Analysis Procedure:

Risks from technical systems to human health and the environment come from external forces acting on a system, resisting its objective and trying to move the system away from it ("challenges"). It is difficult to find a generally accepted definition of the term "risk", but basically this involves responses to the following three basic questions:

- What can go wrong? - resulting in events
- How likely is it that this will happen? - resulting in probabilities of these events
- If it does, what are the consequences? - resulting in consequence values of these events

Risk analysis means responding to these three questions and trying to combine the individual responses to one statement on the system's performance for the purpose of decision-making. It deals with the occurrence of individual failure events and their possible adverse consequences on system, functional or overall plant level. Certain combinations of such events can produce an incident or accident with adverse consequences relevant for human health, for the environment or for infrastructure.

In a QRA a total risk is calculated as the sum of several products of frequency and consequence for each identified initial event. To illustrate the different potential outcomes of an initial event and to calculate the total risk one would often carry out an Event Tree Analysis (ETA). ETA can moreover be used for estimating accidental risk for physical and decision-making/ management systems, with or without human operators. ETA systematically explores system responses to initiating "challenges" and enables probabilistic assessment of success/failure, resulting in overall accident scenarios. The starting point (referred to as the initiating event) disrupts normal system operation. The event tree displays the sequences of events involving success and/or failure of the system components, and results in overall accident scenario consequences and probabilities, due to a certain initiating event. Probability and consequences establish overall risk.

Shortcomings of ETA are that operating pathways must be anticipated and that partial successes / failures are not distinguishable. Advantages are:

- End events need not to be foreseen.
- Multiple failures can be analyzed.
- Potential single-point failures can be identified.
- System weaknesses can be identified.
- Zero-payoff system elements/options can be discarded.

1.5.2 Information requirements for QRA

Frequency Information:

In many cases, the incident frequency information required in a full or partial QRA can be obtained directly from historical records, as the ones to be collected under HySafe's Hydrogen Incident and Accident Database. The number of recorded incidents can be divided by the exposure period to estimate a failure estimate of the frequency. This is a straightforward technique that provides directly the top event frequency without the need for detailed frequency modelling, e.g. on the basis of fault tree analysis. Event probabilities can similarly be estimated for inclusion in ETA. Example of the use of historical information is the conditional probability of a vapour cloud explosion following a release. The use of databases in QRA is further described in Chapter 4.3.

"Likelihood" stands for the numerical output of this technique; frequencies or probabilities may be derived using this approach. The units of frequency are the number of events expected per unit time. Probabilities are dimensionless and can be used to describe the likelihood of an event during a specified time interval, e.g. 1 year, or the conditional probability that an event will occur, given that some precursor event has happened.

Frequency modelling using causal analysis:

The objective of the cause analysis is to establish the methods for frequency (probability) estimations of initial events, e.g. hydrogen releases. The basic data used such as HC release frequencies, pipeline frequencies etc. are based partly on accident and failure statistics, and partly on detailed cause analysis (Fault-tree or similar).

The accident statistics reflect average environment, technologies and operational standards of the past, thus, the specific features of the system considered and its environment should be considered whenever this is judged necessary. The discussions should compare these specific features to "average conditions" in the relevant area in order to assess whether the system is expected to be exposed to the initiating event more often or less frequently than the average. If there are good reasons to expect such differences, the statistical figures could be adjusted accordingly.

The causes of each initial event should be identified to a level of detail suitable for the intended use of the risk analysis. Risk mitigation measures which reduce the probabilities of the initial events should always be emphasised where appropriate.

Adverse Consequences Information:

The consequence evaluation should result in a description of the initiating event as well as the development of the initial events into different accident scenarios, and include both consequence calculations and impact assessments. The consequence calculations should be carried out to accuracy suitable to the level of the analysis, in order to assess impacts of relevance from the accident scenarios.

The consequence calculations should predict the physical circumstances relating specifically to the accident, i.e. explosion overpressure, radiation levels etc. The impact assessments should predict the effects of the accident scenarios on the subjects (people, system/installation and the environment) for which risk is to be estimated.

Many sophisticated models and correlations have been developed for consequence analysis and a presentation or even overview of them is far beyond the scope of this chapter. The results from the consequence analysis step are estimates of the statistically expected exposure of the target population to the hazard of interest and the safety/health effects related to that level of exposure. Consequences are usually stated in expected number of injuries or casualties or, in some cases, exposure to certain levels of energy or concentrations of substances. In some cases simply assessing the quantity of material or energy released will provide an adequate basis for decision making. In general, the results from the consequence analysis and this the adverse consequences information to be used for decision making is a direct function of the objectives and scope of a specific risk assessment study.

The consequence analysis involves the following activities and related information requirements:

- Characterising the source of the release of material or energy associated with the hazard being analysed;
- Measuring (through experiments) or estimating (using models and correlations) the transport of the material and/or the propagation of the energy in the environment to a target of interest;
- Identifying the effects of the propagation of the energy or material on the target of interest;
- Quantifying the health, safety, environmental, or economic impacts on the target of interest.

Events & Sequences of Events Information:

Information requirements on events and sequences of events are related to the hazard identification phase of QRA with the techniques described above. To perform such a qualitative study one should first define the (adverse) consequences of interest, identify the initiating events and accident scenarios that could lead to the consequences of interest, and identify the equipment failure modes and human errors that could contribute to the accident scenarios (barriers).

1.6 HUMAN FACTORS

1.6.1 Human factors and safety

In the context of technology and safety, the term 'human factors' refers to factors that involve humans and that have an impact on safety. The involvement of humans in a technological setting comprises humans as planners and operators (that is, professional engagement with technology) and as users (typically non-professional users, clients or customers).

In any technological application, the contribution of humans is to some degree paradoxical: humans contribute essentially to maintaining safety not only in the design phase but also in the operational phase by controlling processes; but, at the same time, humans also make errors and thereby create dangerous situations and sometimes accidents. The various estimates of how often human error is the primary causal factor in industrial and transport vary somewhat, but typically range between 50% and 90%. Organizational factors may be involved in active human errors and will typically be categorized as poor/lacking procedures, training, man-power planning etc. or sometimes more global shortcomings such as poor safety culture.

1.6.2 Human errors and organisational failures

The modern view of human error among safety specialists is that while human error is unavoidable the circumstances that prompt human errors or allow us to capture them before they lead to negative outcome are to a large extent controllable. This view of human error has in large part been shaped by Rasmussen[1] and Reason[2] each of whom has promoted the "systems view" of human error. Rasmussen advocated on a general level the idea that human error is human-system mismatch. His so-called SRK-framework (skill, rule, knowledge) has been used widely in for analysing human error and was subsequently further developed by Reason.

Rasmussen's three levels of performance essentially correspond to decreasing levels of familiarity or experience with the environment or task.

- Skill-based performance: at this level people carry out routine, highly-practiced tasks in what can be characterized as a largely automatic fashion. Except for occasional checking, very little conscious effort is required (e.g., writing on a keyboard, changing gears, or doing any of the countless daily well-rehearsed tasks at home or at work)
- Rule-based performance: at this level we execute a well-known routine procedure, but have to take into account some change in a situation and modify our pre-programmed behaviour, typically a situation with which we are familiar or have been trained to deal with, we engage in rule-based behaviour (e.g., filling up petrol in one's car at the usual petrol station)
- Knowledge-based performance: this level of performance is required and used when we face a novel situation and have no applicable rules. It may be a form of problem solving

[1] Rasmussen, J. Information Processing and Human-Machine Interaction. Amsterdam: North Holland, 1986. Rasmussen, J. (1983). Skills, rules, knowledge: Signals, signs, and symbols and other distinctions in human performance models. IEEE Transactions on Systems, Man, and Cybernetics, 13, 257-267. For more accessible description of Rasmussen's theories see Vicente, K.J. 1999. Cognitive Work Analysis: Toward safe, productive, and healthy computer-based work. Mahwah, NJ. Lawrence Erlbaum.
[2] Reason, J. Human Error, Cambridge: CUP, 1990; Reason J. Managing the risks of organizational accidents. Aldershot: Ashgate, 1997.

employing analytical reasoning and stored knowledge. In a technological setting this is the type of behaviour

Rasmussen's skill-rule-knowledge framework for classifying performance relates essentially to a cognitive classification of how familiar we are with tasks and, hence, at which level of conscious effort and attention we are devoting to our tasks. These distinctions between different levels of performance are important and useful, because they allow us

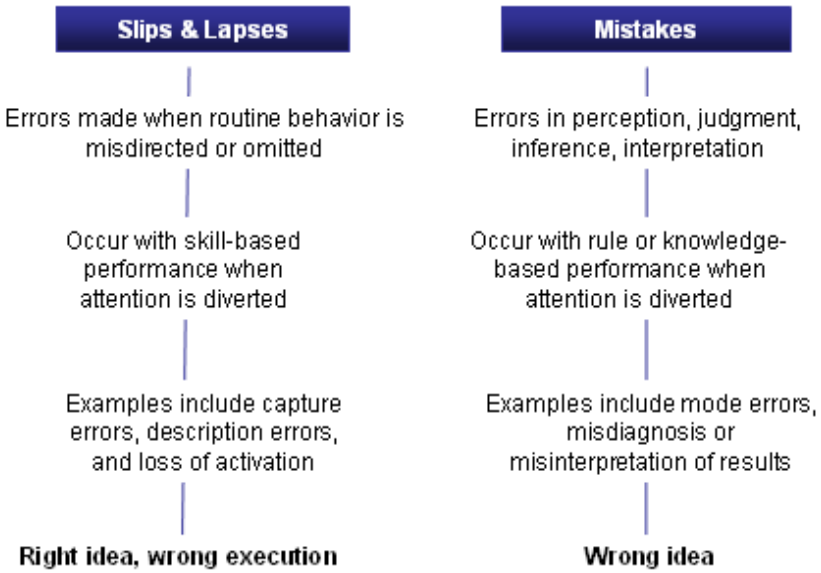
- to model complex performance (typical in technological work settings) by reference to the short-cuts that people have learned to use to save time and effort, and
- to analyze errors according to different levels of performance.

Reason adapted Rasmussen performance based model, tying the classification of errors to cognitive processing. An often used definition of human error is the following taken from the domain of medicine but based on Reason's work focusing originally on industrial safety:

> *An error is defined as the failure of a planned action to be completed as intended or the use of a wrong plan to achieve an aim*[3].

An error is thus either a failure for form a suitable plan (wrong intention) or a failure to carry out one's plan. The latter Reason classified as lapses and slips, depending on whether it is memory failure (lapse) or a response failure (a slip).

The diagram below shows Reason's categories and how they expand upon the SRK-framework.



1.6.3 Human Reliability Assessment (HRA)

[3] Institute of Medicine. To Err is Human: Building a Safer Health System. Washington, DC: National Academy Press, 1999

In his well-known textbook on HRA methods, Kirwan emphasizes that one of the primary goals of human reliability analysis is to provide a means of properly assessing the risks attributable to human error. [4] To achieve this aim three overall phases must be carried out: (A) Identifying what errors can occur. (B) Deciding how likely the errors are to occur (C) Enhancing human reliability by reducing this error likelihood (Human Error Reduction)

Thus, HRA is used to identify, model, predict, and when possible, to reduce human errors in operations and will typically include normal production operations, maintenance, testing and emergency conditions. It is well-known that maintenance and testing are phases are especially vulnerable to human error that can seriously influence system safety[5]. For instance through insertion of an incorrect component, miscalibration, failure to align the system back to its operational configuration.

A number of methods and techniques are available with which to perform a structured analysis of human reliability of a specific industrial setting in which an HRA is undertaken. A common preliminary phase for conducting an HRA is, when the scope of the problem and the exercise to be undertaken has been defined, to perform a risk assessment. This may be carried out with techniques described in the section above on hazard identification methodologies, e.g., fault and event trees. Next, it is customary to define the interaction between humans and the system in terms of a task analysis - e.g., hierarchical or time-line task analysis. The next step involves the identification of possible errors, possibly by using group-based techniques such as HAZOP, as described above. Following the identification of errors, it is necessary to estimate the likelihood of their occurrence. To arrive at a quantification of human error probabilities either human error databases can be used or expert judgment or a mixture of both.[6] In the table overleaf we show an illustration of human error quantification from a commonly used HRA method. Finally, risk reduction options must be reviewed and possibly a prioritization, selection and a plan for implementation of risk reduction.

➢ Scope
➢ Task analysis
➢ Risk/hazard identification
➢ Modelling
➢ Human error identification
➢ Human error quantification
➢ Impact assessment
➢ Risk control options
➢ Risk reduction plan
➢ Safety assessment reporting

[4] Kirwan, B. A Guide to Practical Human Reliability Assessment. London: Taylor and Francis, 1994. See also J.R. Wilson & E.N. Corlett, Evaluation of Human Work. London: Taylor and Francis, 1995.
[5] See Kirwan, B. & Ainsworth, L. K. (Eds.) A guide to task analysis. London, Taylor & Francis, 1992
[6] David I. Gertman, Harold S. Blackman. Human Reliability and Safety Analysis Data Handbook. John Wiley 1993; Williams

Generic classifications (HEART, after Williams, 1986)

Generic task	Proposed nominal human unreliability (5th-9th percentile bounds)
(A) Totally unfamiliar, performed at speed with no real idea of likely Consequences	0.55 (0.35-0.97)
(B) Shift or restore system to a new or original state on a single attempt without supervision or procedures	0.26 (0.14-0.42)
(C) Complex task requiring high level of comprehension and skill	0.16 (0.12-0.28)
(D) Fairly simple task performed rapidly or given scant attention	0.09 (0.06-0.13)
(E) Routine, highly-practised, rapid task involving relatively low level of skill	0.02 (0.007-0.045)
(F) Restore or shift a system to original or new state following procedures, with Some checking	0.003 (0.0008-0.007)
(G) Completely familiar, well designed, highly-practised, routine task occurring several times per hour, performed to highest possible standards by highly-motivated, highly-trained and experienced person, totally aware of implications of failure, with time to correct potential error, but without the benefit of significant job aids	0.0004 (0.00008-0.009)
(H) Respond correctly to system command even when there is an augmented or automated system providing accurate interpretation of system stage	0.00002 0.000006-0.0009)

1.6.4 Safety culture

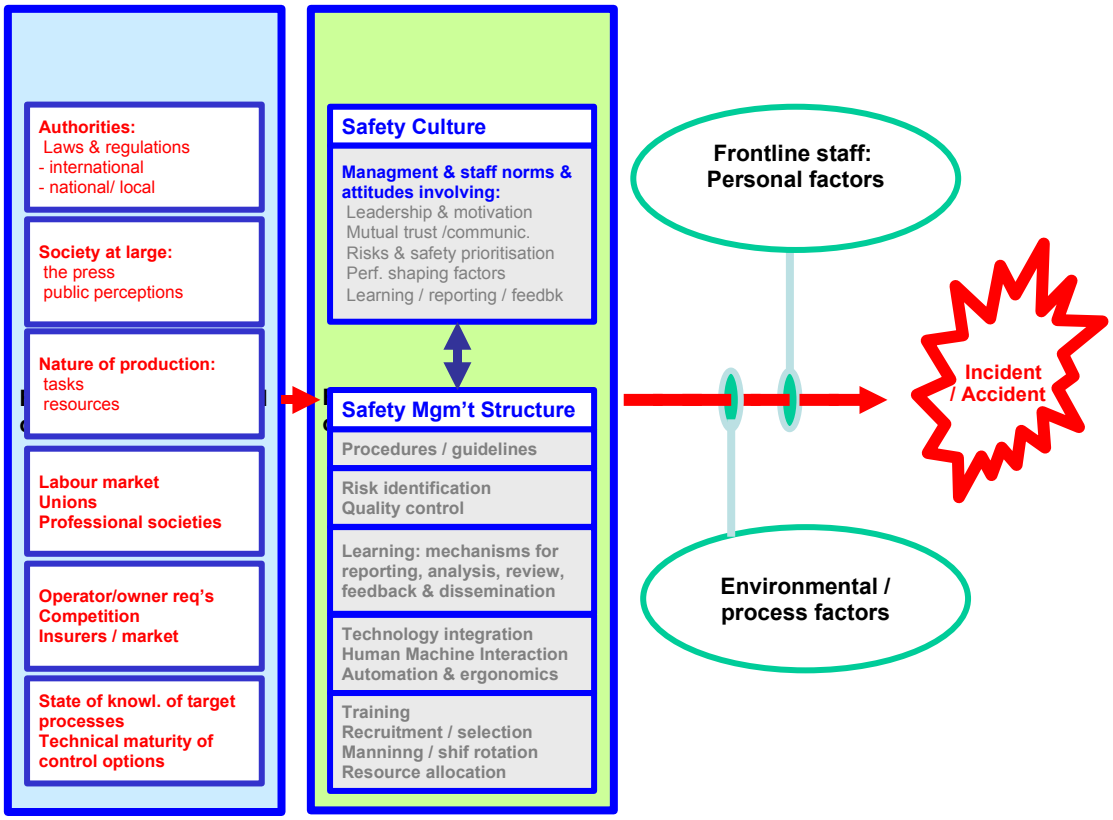
It has become widely accepted that an organisation's safety culture can have an impact on safety performance. Two installations may be entirely alike in terms of production, ownership, workforce, procedures and yet differ in terms of safety performance and measurable safety climate[7].When seeking to assess and control the impact of human factors on the level of risk of a plant or other installation the area it is therefore essential to include organizational factors as well.

The diagram overleaf seeks to depict how safety cultural factors along with traditional work condition factors (here called safety management factors) are within the control of the organization at hand. In this section we review briefly how safety culture is conceptualised in the safety analysis literature and how it may be measured.

The concept of safety culture was introduced in the aftermath after the nuclear power plant accident in Chernobyl in 1986, when the concept was invoked to explain a corporate attitude

[7] Andersen, H.B.; Nielsen, K.J.; Carstensen, O.; et al. Identifying safety culture factors in the process industry. In: Loss prevention 2004. 11th International symposium on loss prevention and safety promotion in the process industries, Czech Society of Chemical Engineering, Prague, 2004). 5225-5233

and approach that tolerated gross violations and risk taking behaviour. A large number of



studies have since developed models and measures of safety culture. One of the most widely cited definition of safety culture was offered by the Advisory Committee on the Safety of Nuclear Installations in the UK[8] (ACSNI, 1993), who defined safety culture as follows:

> *The safety culture of an organisation is the product of individual and group values, attitudes, perceptions, competencies and patterns of behaviour that determine the commitment to, and the style and proficiency of, an organisation's health and safety management. Organisations with a positive safety culture are characterised by communications founded on mutual trust, by shared perceptions of the importance of safety and by confidence in the efficacy of preventive measures (ACSNI, 1993).*

The first-generation models characterised positive safety culture for a given organisation as founded on mutual trust, shared belief in the importance of safety and shared belief that preventive measures make a difference. In subsequent models (from mid-90s and later) there is additionally an emphasis on organisational learning: i.e., willingness and ability to learn from experience (errors, incidents and accidents).

There is no "standard model" of safety culture, but there is widespread agreement that safety culture includes factors relating to

[8] ACSNI Human Factors Study Group: Third report - Organising for safety. HSE Books 1993

- Visible top management and shop floor management commitment to safety
- Work force ownership and participation in safety solutions
- Open communication
- Mutual trust between management and employees
- Willingness and ability to learn from experience ("an organisation with a memory")
- Work force involvement in company and motivation

Measuring safety culture / climate

A distinction is often made between culture and climate: culture is slow to change and involves mostly tacit (unspoken, hard or impossible to articulate) beliefs and norms, whereas climate is shaped by context and more explicit. Therefore, empirical studies, and especially surveys and interviews, are usually said to uncover, at best, safety climate, whereas safety culture is only characterised indirectly.

When considering empirical approaches to safety climate, decisions must be made about the following three dimensions:

(a) what should be measured (what are the factors to be measured?)
(b) how should measures be made (what are the methods and techniques to perform the measurement?)
(c) where should measures be made (in which part of the organisation should sampling and appraisal be made?)

As described above, the issue of what should be measured is addressed in somewhat different but not necessarily incompatible ways by different analysts. There is general but not precise agreement about the factors that are involved in safety climate [culture].

Similarly, different methods and techniques are available for assessing safety climate – interviews, field observations, participation, surveys. But within this range of methods, surveys (written or web-based questionnaires, oral interview surveys) yield a uniform output that may be quantified more or less directly.

Finally, assessment of safety climate in an organisation may be targeted at both the management level (top and middle management including supervisors) and the shop floor level, and at different operational units and even office staff and planners.

Taking the range of choices into account, the most typical kind of safety climate [culture] assessment method is that of questionnaire-based surveys of staff perceptions and attitudes. A questionnaire-based survey will typically be targeted at the operational staff, including possibly group leaders, and, of course, will use some form of safety climate questionnaire – a safety climate assessment tool.

There are a large number of such tools (questionnaires) available, some of these being domain specific (maritime, oil production platforms, aviation, process industry etc). Questionnaires require the respondent to answer specific questions in terms of the selection of one among a fixed set reply options – typically a selection from a Likert-type ranking scale: "Strongly Agree, Agree, Neither Agree Nor Disagree, Disagree, or Strongly Disagree". Question items will form groups that correspond to underlying factors (say, perception of top management commitment to safety). For validated survey tools, factors will have been established through possibly pilot surveys and subsequent statistical analysis (for instance, factor analysis). Finally, analysts will be able to establish a benchmark when survey tools that have been applied to a range of installations or workplaces within comparable parameters. For instance, the EU-project ARAMIS, adapting a construction and production plant questionnaire, has used this to collect

data from five European Seveso-type plants. On the ARAMIS approach (Duijm et al. 2004)[9] , a single global safety climate index has been established for use in integrated assessment of safety management – instead of a range of different indices, each corresponding to a single safety climate factor.

1.6.5 supplier and delivery organisations

1.6.6 GAPS &Recent progress:

1.7 RESIDUAL RISK AND SOCIAL PERCEPTION OF HYDROGEN (RISØ, INERIS)

For a long time, risk assessment process was considered as of the relevance of the technicians or experts. However, with the recent changes in both international and European juridical context the public and other entities of the civil society became and are recognised as being concerned by the decision aiming at reducing the risks; and are then involved in the risk assessment and risk management process.

The Aarhus convention on "Access to Information, Public Participation in Decision-making and Access to Justice in Environmental Matters" (1998) have influenced a lot of current national approaches to risk assessment. In France for example, this convention was introduced through the law n° 2002-276 of February 27th 2002 on "the democracy of proximity" and more recently the law n° 2003-699 of July 30th 2003 on "industrial and natural risks prevention and damages amends", and its 1st February 2005 decrees of application including that "Local Committee of Information and Dialogue" must be created for all industrial Seveso High threshold site.

Let notice that even if the juridical and technical wills are present, the involvement of different people (stakeholders) raised practical problems: how to go toward a common understanding and a co-elaboration of common decisions.

1.7.1 Risk perception research paradigm(s)

There are two major frameworks for studying the views on risk by the public involved, respectively, a largely anthropological approach that seeks to characterise risk perception by reference to social structures ("ways of life"). The other and rather more dominant approach, sometimes called the psychometric paradigm, attempts to characterise the underlying factors behind the perception of risk by the public (and various sub-populations defined by, e.g., age, education, gender, profession, ethnicity etc.) by methods refined by psychologists who identify such factors as types of personality or heuristics and biases behind judgments about probability estimates.

[9] Duijm, NJ, Andersen HB, Goossens L, Hale AR, Guldenmund FW, & Hourtolou F (2004). ARAMIS project: Effect of safety management's structural and cultural factors on barrier performance, 2004, 11th International Symposium on Loss Prevention and Safety Promotion in the Process Industries, Prague, 31 May-3 June

However, both approaches demonstrate the fact that the risk management process (identificationtion, assessment, control) aims at reducing the uncertainty a stakeholder has concerning a done situation. One can think that the only competent person to do that is the "expert". The objective would then be to reduce the gap between the expert and the non-expert person and create a common way of looking to "risk" and its causes and consequences.

1.7.2 Risk perception research approaches

It has been known for long that lay people tend to overestimate low-frequency events and underestimate high-frequency events. But it was not till the late 70's that it was discovered that that there is, one the one hand, a low correlation between lay estimates of risk and direct measures of subjective seriousness of a large and widely delimited set of activities, but on the other hand, a strong correlation between the perception of risk and two main dimensions: the level of dread or perceived disastrousness (imaginability of the hazard) and the perceived controllability of the hazard (familiarity and predictability).

Four approaches to risk perception exist: two approaches that insist on the "decisional dimension" of risk perception and two other approaches on the "contextual dimension of perception".

The first approach to risk perception is based on economics paradigm. This approach status that, in a risky situation, each rational actor knows the possible results of a decision (losses and gains) and are able to define the chance (probability or possibility) of a given result. Each rational actor aims at maximising the utility. This first approach consider that: (i) stakeholders (actors) are all similar in their perception and (ii) each risk perception depends on "probability" and "consequences".

The second approach based on a psychometric paradigm focus on perception biases. This approach recognise, in addition to the quantitative criteria that make risk perception "probability" and "gravity of the consequences" the existence of some other "qualitative aspects" like: novelty, familiarity, controllability, acceptability, redoubt ability, etc.). Two biases of perception are here listed: "the availability bias" and "the catastrophe potential". The first bias makes a direct correlation between "information availability" and "stakeholder correct perception" of a done situation. The second bias states that perception do not only depend on "observable facts" but also on "potential consequences".

These two first approaches have omitted the heterogeneity of "stakeholders" and the heterogeneity of the context where they live.

The third approach is a sociologic one. This one study how do people perceives risk in their diversity using both quantitative and qualitative approaches. By insisting on the importance of the socio-demographic profiles of the stakeholders and their individual's history, the sociological approach tends to consider each risk as equivalent.

The fourth approach, to risk perception, takes into account the diversity of both people and risks. This approach is based on the cultural dimension of perception. This approach reveal that risk percpetion depend on stakeholders' values and on the way their conceive knowledge.

1.7.3 Empirical studies of risk perception of hydrogen technologies

There have been a small number of published studies of public perceptions of the risk of hydrogen technology. There is, of course, an old history of hydrogen applications (the Hindenburg airship; H-bomb; but it is not known how important such associations are)[10]

The following studies of risk perception of hydrogen technology for transport applications have been identified:

The EU-funded CUTE [11] project which has tested the introduction and operation of H2 buses in London, has collected public perception of hydrogen technology for buses. Method: telephone survey, N=414. Results: 45% heard about H2 vehicles, 35% support the introduction of H2 vehicles, 60% need more information, 4% gave "danger" as the first words that come to mind when hearing the word *hydrogen*, 22% "positive",13% "explosive/flammable", 13% fuel/energy.
LBST project[12] (Ludwig-BOolkow-Systemtechnik) in in co-operation with Ludwig-Maximilians University of Munich: Method: surveys of respondent attitudes Sub-study 1: The attitudes towards hydrogen of secondary students in three schools Sub-study 2: In 1997 the first hydrogen bus was introduced in Munich, and the passengers of this bus were surveyed. Sub-study 3: Students who were among the bus passengers (Sub-study 2) and compared their answers to those of the students questioned during Sub-study 1. This gave an indication of how the experience of using hydrogen transportation affects the attitude towards this new fuel. Results: the often-expected spontaneous association of hydrogen with danger or past accidents like the Hindenburg airship was not confirmed. Generally the attitude of the interviewee towards hydrogen was positive. Contact with hydrogen technologies was shown to have a further positive effect on attitude towards the fuel.
Title: Greening London's black cabs: a study of driver's preferences for fuel cell taxis[13] Method: the study investigates the preferences of London taxi drivers for driving emissions-free hydrogen fuel cell taxis, both in the short term as part of a pilot project, and in the longer term if production line fuel cell taxis become available. Results: driving hydrogen-fuelled vehicles does not seem to raise safety concerns amongst taxi drivers.

[10] Midden, C. & Montijn-Dorgelo, F. Developing and introducing hydrogen technology, an analysis of social psychological factors. Eindhoven Univ. Technology. 2004.

[11] T. O'Garra, S. Mourato and P. Pearson: Analysing awareness and acceptability of hydrogen vehicles: A London case study, *International Journal of Hydrogen Energy, Volume 30, Issue 6, May 2005, Pages 649-659* .

[12] LBST. The acceptance of hydrogen technologies—A study carried out by Ludwig-BOolkow-Systemtechnik GmbH (LBST) in co-operation with Ludwig-Maximilians University of Munich, 1997. Available at: http://www.hydrogen.org/accepth2/execsumm.html. [Accessed on 08.09.2006]

[13] Mourato, S., Saynor, B. and Hart, D. Greening London's black cabs: a study of driver's preferences for fuel cell taxis. *Energy policy*, 2004, vol. 32, no5, pp. 685-695

1.7.4 Risk criteria: other domains, comparable applications, harmonisation efforts.

It is usual to consider "risk perception" at the end of a "technical process" based on identification, evaluation, assessment and hierarchization of risks. However, risk perception do not depend on purely facts measures (gravity of the consequences) or prediction (probability). Values and contextual aspects like socio- economics ones, organizational ones, etc. determine the stakeholders perception.

These statements show us that "risk assessment" process must be enriched at its early steps by both qualitative and quantitative studies of stakeholders' visions and perceptions.