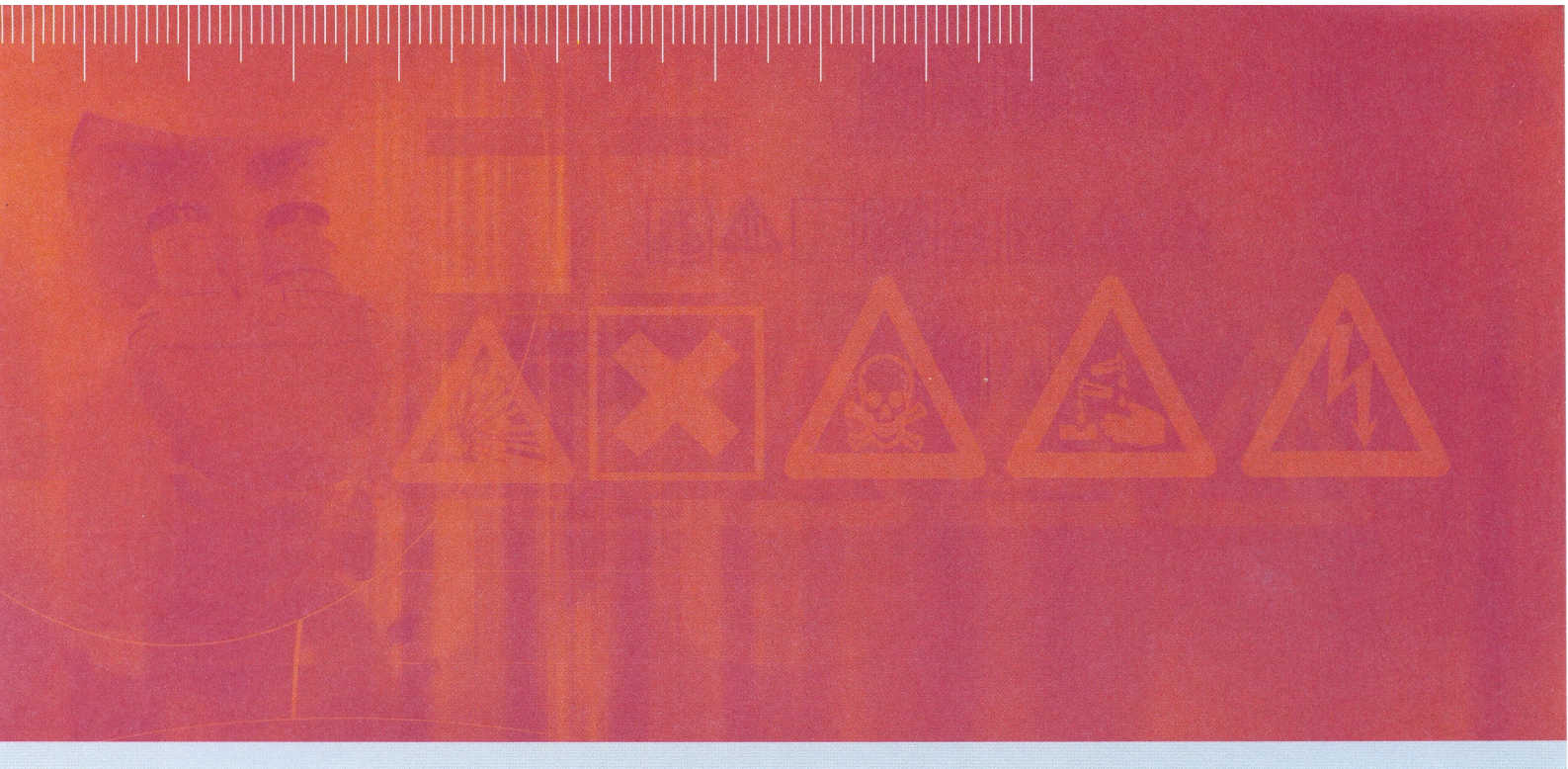


STUDY REPORT 09/11/2009

N° DRA-09-103041-13797A

Program 181 - DRA 77 : Control of accidental risks by technological and organizational arrangements (DRA-77)

Approach for evaluating human safety barriers

- Ω 20

INERIS

maîtriser le risque
pour un développement durable

Program 181 - DRA 77 Control of accidental risks by technological and organizational arrangements

Approach for evaluating human safety barriers - Ω 20

Accidental Risk Division

List of persons involved in the study: E. Miché, R. Périnet

PREAMBLE

The present document was drawn up:

- with view to the available scientific and technical data having been the subject of a recognized publication or of consensus among experts,
- with view to the applicable legal regulatory or prescriptive framework.

These are data and information in effect at the date of edition of the document, March 2009.

The present document comprises proposals or recommendations. It has by no means the purpose of substituting itself for the decisional power of the risk manager(s) or of an interested party.

The present study report written in English is for information only. The French version shall prevail over any translation that may be made.

LIST OF CHANGES

Review	Proofreading	Application	Modifications
PROJECT	August 2006		Creation of the document
Version 1	December 2006		Version 1 of the document
Version 2	March 2009		Various modifications for improving appropriation of the method by the users Clarification of the model used by the method and of its limits Minor specifications or modifications on certain steps of the method and on its modes of application

Foreword to the reader: the modifications which are the subject of the present version of the document are only very partially directed to the tables shown in paragraph 4.3 which allow evaluation of the performance of the barriers. If these tables have slightly changed since version 1 of the method, the relevant modifications should further be considered as formal rather than basic modifications. However, this document is intended to change within the scope of a continuous improvement process based on return of experience and on advances in the investigation on human factors.

For more details on the process for developing the method, see paragraph 1.5.

TABLE OF CONTENTS

1. INTRODUCTION

1.1 GENERAL BACKGROUND OF THE PRESENT DOCUMENT

Since 2000, the French Ministry in charge of Ecology and Sustainable Development has been financing a program of studies and research entitled « Formalization of the knowledge and tools in the field of major risk ».

The subject of the first part of this program is to produce a global inventory formalizing the expertise of INERIS in the field of accidental risks. This updatable inventory will consist of different reports dedicated to the following themes:

- physical phenomena involved in an accidental situation (fire, explosion, BLEVE…),
- analysis and control of the risks,
- methodological aspects for carrying out statutory services (safety studies).

Each of these documents receives a specific identifier of the « Ω-X » type in order to facilitate the follow-up of the different possible versions of the document.

In fine, these documents describing methods for evaluating and preventing accidental risks, will form an inventory of the working methods of INERIS in the field of accidental risks.

In this background, INERIS has developed an approach for evaluating technical safety barriers, available in the Ω10 report [1]. The goal of the present document is to propose an approach which is inspired from that developed in the Ω10 report allowing characterization of the human safety barriers and evaluation of their performance. Both approaches thus have useful similarities pedagogically and their joint application provides an evaluation of the whole of the architecture dedicated to safety on industrial installations.

The present report is the second version of the document and was drawn up on the basis of the first Ω20 report dated December 2006 [1].

1.2 GOALS OF THE Ω20 METHOD

A major goal of the SEVESO II Directive is the control of the risks at the source; to do this, it is the responsibility of the industrialists to set up measures for controlling the risks – called safety barriers in this document – the purpose of which is to ensure an efficient prevention of risks of accidents and if necessary to limit the effects of these accidents outside its site.

The risks generated by the plant – represented by accidental scenarios – are demonstrated upon performing risk assessment. For each of the scenarios, the safety functions are determined. These functions are fulfilled by safety barriers. The probability of an accident in a hazardous installation depends, i.e. on the performances of the safety barriers, i.e. their capability of efficiently fulfilling the safety function which is allotted to them.

Safety barriers may exclusively consist of technical elements: they are called technical safety barriers. They may also have a human component, i.e. totally or partly consisting of operations performed by humans with the aim of opposing the chain of events likely to result in an accident: they are called human safety barriers.

The development of the approach presented in this document was guided by the requirement of having tools with which the performance of human safety barriers may be evaluated and demonstrated. In present practices evaluation and management of risks are performed by « technicians » (notably engineers). The latter do not generally have all the knowledge required for taking into account the dimension of the human factor which is however essential in controlling risks.

The goal of the approach described in this report is especially to provide to non-specialist "risk technicians" of human factors, an evaluation method in order to characterize and evaluate the performance of human safety barriers.

1.3 ISSUES OF THE EVALUATION AND DEMONSTRATION OF THE PERFORMANCE OF HUMAN SAFETY BARRIERS

First this is a safety issue. Industries with risks assign to the agents operating them as close as possible to the site, an essential role in managing these risks (monitoring of the parameters, detection of abnormalities,…). These arrangements have to be set up by industrialists in order to allow these agents to effectively fulfil their safety mission (e.g.: elaboration of procedures, making available equipment, training the agents…). These arrangements have to be evaluated in order to make sure that they are suitable with regard to safety performances aimed and to the accepted risk level. Omega 20 was designed for meeting this issue.

This is also a statutory issue. In France, the policy for preventing technological risks is mainly based on the regulations of hazardous installations supported by the French Code of the Environment, changed by the law dated July 30th 2003 relating to preventing technological and natural risks and to repairing the damages (JO (Official Gazette) as of July 31st 2003)).

This new law introduces at a regulatory level[1] the principle of a safety study based on a risk analysis which should characterize not only the potential severity, but also the probability of occurrence of accidents by taking into account the performance of technical and human safety barriers, designated by the generic term of « measures for controlling risks » in the regulatory text. Complementarily, article 4 of the decree as of September 29th 2005 specifies that « in order to be taken into account in the evaluation of the probability, measures for controlling risks should be efficient, have application kinetics appropriate with that of the events to be controlled, be tested, maintained in order to guarantee continuity of the aforementioned positioning ».

[1] Ministerial decree as of September 29th 2005 relating to the evaluation and to the taking into account of the probability, kinetics, intensity of the effects and of the seriousness of the consequences of potential accidents in the installations subject to approval.

It is in this background that we wished to develop a method for evaluating the performance of human safety barriers (HSB), the results of which will be compatible with a semi-quantified approach (in a probability class) for evaluating the risks.

1.4 SCOPE FOR USING THE Ω20 METHOD

The main scope of use is that of **evaluating the risks with as a goal the demonstration of the control of risks** as mentioned hereinbefore. The characteristics of the Ω20 method – its purpose, its methodological choices, its ambition of deep analysis, its modes of application and the associated means – were developed in order to meet this goal and are therefore specific to this specific scope of use.

Thus, **the main user of this method is the analyst or the risk (or safety) evaluator**, whether he/she is an industrialist or an external counsel for the industrialist.

Other possible scopes of use:

We consider that the method – in its entirety or at least in its principles – may be used with benefit in other scopes and in the perspective of other purposes such as for example:

- Within the scope of an approach for improving safety arrangements (safety architecture) which have been set up: for example, during periodic reviews of these arrangements or of redesigning steps for these installations. With this goal, the method will be applied with the concern of showing points of improvement (for example: improvement in the ergonomics of the work station or of the interfaces or action means, improvement or simplification of the procedures, setting up additional verifications or additional barriers,…)

- Within the scope of the critical review of a safety study presented by the operator: the method proposes elements for appreciating the evaluation of the performance of human safety barriers, complementary to those of « Sheet No. 7: Measures for controlling risks, based on human intervention »[2] available to the inspectors of Classified Installations by the French Ministry in charge of Ecology and Sustainable Development (a sheet appended to the guide for elaborating and reading studies of hazards for AS Establishments as of 28.12.2006).

[2]This sheet provides elements for appreciating the taking of human safety barriers into account within the scope of critical review of a safety study. The Omega 20 method is notably distinguished from this sheet, as regards the confidence levels which may be assigned to them.

Indeed, this sheet notably indicates that except for a particular justification, measures for controlling risks based on human intervention from the responsible operator for the process further have a maximum confidence level of 1, and that the measures for controlling risks based on human intervention from a third party relatively to the operator responsible for the process (in the case of a redundant verification) has a maximum confidence level of 2.

- Within the scope of incident analysis: the method proposes a model of the barrier and descriptive criteria of the working situations which may be used as an analysis grid for identifying the causes of incidents or accidents.

The user of the method may then also be an internal auditor, an inspector, an actor responsible for analyzing events or further any person responsible for safety.

1.5 PROCESS FOR DEVELOPING THE METHOD

The Omega 20 method was the subject of an initial development and of application tests on actual industrial cases. On this account, we would like to thank RHODIA who have contributed to improving the method through exploitation of application tests of the method on several chemical installations and via exchanges as to the advantages and drawbacks of the method.

Within the scope of a continuous improvement process, Omega 20 continues to be the subject of methodological developments and will thus be led to change over time in order to:

- improve the relevance of the method for evaluating human safety barriers on the one hand,
- at best meet the needs of the main users who are the analysts or risk evaluators on the other hand.

We call on the users of the method to contact us (see the Internet site www.ineris.fr) in order to share with us their feedback experience in a dually beneficial approach in accompanying users of the method and integrating their needs and comments in the future version of the method.

1.6 OUTLINE OF THE REPORT

In addition to this introduction (chapter 1), this document is organized in 4 main chapters.

In a first phase (chapter 2), the present document provides the reader with the main theoretical and methodological foundations which should allow him to become familiar with the terms relating to the performance of human safety barrier. With this chapter it is also possible to address the difficulties opposed by the goal of evaluating human reliability. Finally, it will be possible to mention methodological choices made within the scope of the approach developed in the present report and to present the limits associated with such an approach.

The method presented here, as for it, provides elements of justification by which it is possible to assign under certain conditions, a confidence level of 2, including for safety barriers not involving any third party.

Next, (chapter 3), INERIS briefly presents the developed approach for allowing evaluation of the human barriers which may be retained for controlling technological risks. The reader may thus acquire a global view of the methodology before being interested in the details at the different steps required for evaluating human safety barriers (chapter 4). The short chapter (chapter 5) which follows shows how the performances evaluated from a set of human safety barriers acting on a scenario may be aggregated in a goal for demonstrating risk control.

Finally, the reader will find as an annex, four examples for evaluating human safety barriers mostly from the field of chemical industrywhere the whole of the approach proposed in this document was applied.

2. THEORETICAL AND METHODOLOGICAL FOUNDATIONS OF THE OMEGA 20 METHOD

The goal of this chapter is to introduce the definition of the human safety barrier which is used for applying the method developed in this document and its role in controlling risks. On the other hand, we shall mention as didactically as possible certain theoretical and methodological foundations required for explaining the principles on which the method was built. We have in particular retained the development of two important notions: that of the human safety task and that of the working environment. We also hope that this will awaken the interest of the reader on the ambition and difficulty of the goal which is given here, i.e., the evaluation with a purpose of quantification, of the performance of the complex activity which may be a human safety task. Finally, we shall attract attention on the limits which result from the models used on the evaluation achieved through the method developed in this document.

2.1 WHAT IS A HUMAN SAFETY BARRIER ?

The barrier concept appeared with that of extensive defense[3]. This concept aims at securing a system by setting up a set of successive measures, independent of each other – or further defense levels[4] – for preventing or controlling possible incidents and limiting the consequences thereof. The designation “safety barrier” used in the Omega 10 and Omega 20 methods is restricted to active or passive, technical or human systems, providing a safety function.

2.1.1 HUMAN SAFETY BARRIERS: DEFINITION

Human safety barriers consist of human activity (one or several operations) which is opposed to the chain of events likely to result in an accident.

Like the technical safety barriers, the human safety barriers are defined by the safety function[5] which they provide against a major accident scenario.

They are also defined by the elements which make them up: human safety barriers have a human component, most often associated with a **technical component (the operator is at least interacting with the technical element** of the system which he/she supervises or on which he/she acts). When the barrier consists of technical safety elements entering a safety chain, the term used is **Manual Action Safety System (MASS).**

[3] This concept was used in the United States by the IAEA (International Agency for Atomic Energy) in the 1960s in order to design the safety of the first nuclear reactors.

[4] Arrangements are found among these defense levels which are adopted as regards design, construction and modes of exploitation including maintenance and internal and external emergency measures.

[5] Function having the purpose of preventing and protecting against dreaded events

Fig. 1 shows a typology of safety barriers which illustrate the different types of barriers.

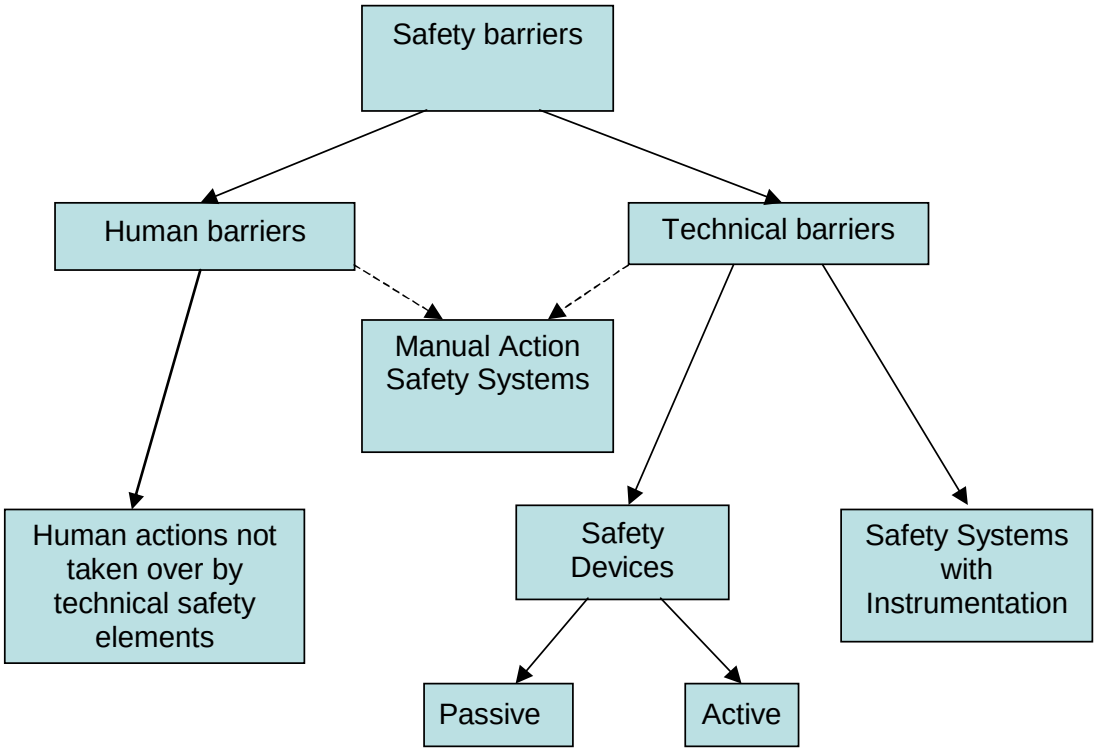


Fig. 1: Typology of safety barriers
(complement to the typology presented in the Ω 10 report [1].

Examples of human safety barriers:

- An operation for checking the seal of a pipe before the use of it.
- An action of manually closing a valve subsequent to visual detection of an abnormal increase in the pressure of a reactor.

Example of a MASS:

- An action for securing the installation by actuating an emergency shut down button subsequent to detection of a gas leak during a surveillance round.

Important note:

The aim of this document is to propose an approach providing assistance for evaluating both types of safety barriers. **For manual action safety systems, the evaluation approach presented in this document is exclusively applied to the human component of the safety chain. In order to have full evaluation, the reader may associate this with the approach presented in the Ω 10 report [1].**

2.1.2 CATEGORIES OF HUMAN SAFETY BARRIERS RETAINED FOR CONTROLLING RISKS

The option for identifying human barriers is to consider the human in an industrial system in his/her function of preventing or compensating the degradations of a process or an activity with risks. Human activities which work towards normal operation for exploiting the system are therefore not considered. For example, the loading of a reagent in a reactor is not considered as a safety barrier.

The application of this principles leads to the identification of two types of actions capable of being considered as independent:

- Those which intervene upstream from an activity or from the starting of the process likely to have risks of major accidents and which consist in preparing this activity, under the angle of safety: the safety function will be to verify that the conditions for occurrence of an accident scenario are controlled prior to an activity with risks. **These barriers will be called "verification barriers".**
- Those which take place during the dangerous activity/process (or downstream from the activity/process) and for which the safety function will be to detect a predicted degradation and to act in order to limit its consequences. The action of these barriers fits into the kinetics of the incidental or accidental sequence**. These barriers will be called "compensation barriers".**

  The detection of the degradation may be carried out at different stages of the dangerous activity: for example highly upstream from the dreaded event (or deviation) such as certain surveillance rounds and inspection campaigns of equipment or further downstream from the dreaded event such as compensations of process degradations (intervention on the abnormal temperature rise in the reactor) or even downstream from the dangerous phenomenon (intervention in the case of a fire).

2.2 WHAT ARE THE PROBLEMS IN EVALUATING A HUMAN SAFETY BARRIER?

The evaluation of human safety barriers cannot amount to simple evaluation of human skills. Their reliability does not only depend on the humans responsible for their application, it also results from designed, planned or organized situations, allowing them to fulfill their mission. Unlike what may be understood by the expression of « human reliability », human reliability is not reducible to the sole reliability of the single human component. Human reliability in reality is that of the human taken in his/her naturally complex environment (of a material, procedural, organizational, cultural nature…). Human reliability depends on these different human and environmental factors, on their complementarity and on their influences on the different processes involved in the work of humans (cognitive, affective, sociological, physical processes,…).

For a given situation, the question is to identify **the most determining factors regarding the success of the relevant human safety task** and to characterize them depending on the assistance which they provide to humans for fulfilling their missions (**aid factors**), or on the threats which hang over the success of the latter (**perturbing factors**).

The evaluation of human safety barriers can neither amount to simple evaluation of safety rules such as those shown in the procedure. Indeed, work of humans is differentiated from the simple application of prescribed rules: it consists in permanent adjustments, more or less significant and more or less conscious, relatively to these rules which may lead depending on the case, to unsuitable actions or else to actions promoting safety. Mechanical application by humans of safety rules is not possible: indeed, these rules are irremediably the subject of interpretation from humans, notably depending on their experience and on the context of the situation. Further, work situations are naturally singular, considering their variability notably in terms of exploitation requirements, organizational constraints or technical resources. This variability, by excluding the possibility of exhaustively predicting all the work situations, confirms the impossibility of mechanical application of safety rules by humans.

Evaluation of human safety barriers therefore implies a qualitative analysis of the real work , notably considering the knowledge of the relevant operators and their working conditions. Therefore, this approach is firstly in line with an ergonomic approach to work situations.

2.3 METHODOLOGICAL ORIENTATIONS RETAINED FOR EVALUATING HUMAN SAFETY BARRIERS

We shall develop in the following paragraph the principles with which we have used the ergonomical approach to work situations in order to elaborate our methods for evaluating human safety barriers.

2.3.1 PRINCIPLES FOR EVALUATING HUMAN SAFETY TASKS

The Omega 20 method was designed for the largest number of barriers. For pedagogical reasons, it was elaborated from a view of human work close to the operation of safety systems with instrumentation. Indeed, Omega 20 considers that humans consist of three systems: a sensorial system, a cognitive system, and a motor system. Like systems with instrumentation, we assume that these systems successively intervene in the acquisition and processing of information, in the decision-making and in producing a safe behavior.

This highly simplifying task model is close to the general models developed in ergonomic psychology to account for human activities in a first analysis. One of the most used grids for analyzing human tasks, inspired from Rasmussen [3], considers three main sub-tasks: detection, information processing and action.

The Omega 20 method therefore proposes breaking down human safety barriers into three main sub-tasks: detection, diagnostic and action..

- **Detection (or obtaining information)**: the aim is to obtain one or more pieces of information allowing identification or detection of a failure or degradation which may lead to a major accident or to the on going phenomenon. The operator may have a more or less active role in obtaining this information.
- **A diagnostic allowing selection of the safety action:** the aim is to produce a diagnostic from the information obtained upon completion of the previous phase and to select the adequate safety action which will be carried out.
- **Action**: this is a manual action (or a chain of actions) or an action conveyed by a technical system which, if efficient, opposes the predicted major accident scenario (actions on a safety element or on an aggressive element of the installation).

The Omega 20 method proposes evaluation of the influence of the environment on the performances of each of these sub-tasks.

2.3.2 PRINCIPLES FOR EVALUATING THE WORK ENVIRONMENT

The Omega 20 method considers humans as users of resources and of means (time, skills, information…) made available to them for allowing them to fulfil their missions. It proposes an approach aiming at evaluating the suitability or the sufficiency of these means towards the goals to be achieved. Omega 20 proposes proceeding with this evaluation from a set of general factors determining human reliability, characteristics or descriptions of the conditions and of the work environment of the operators, and selected for their relevance towards the largest number of interventions or safety tasks.

These « determining factors » essentially concern the relationships between a signal or a piece of information, humans and safety actions to be carried out:

- presentation and access to the information,
- availability of the operator,
- quality of the information useful to the diagnostic,
- guiding level for selecting the correct action,
- level of stress within the context of the action,
- requirement and complexity level of the action.

There exist several classifications of factors determining human reliability. One of the most used is the classification proposed by Hollnagel [4], illustrated by Fig. 2. According to this model, the performance of human action may be considered as the result of interactions between three main categories of factors: Humans, Technology and Organization

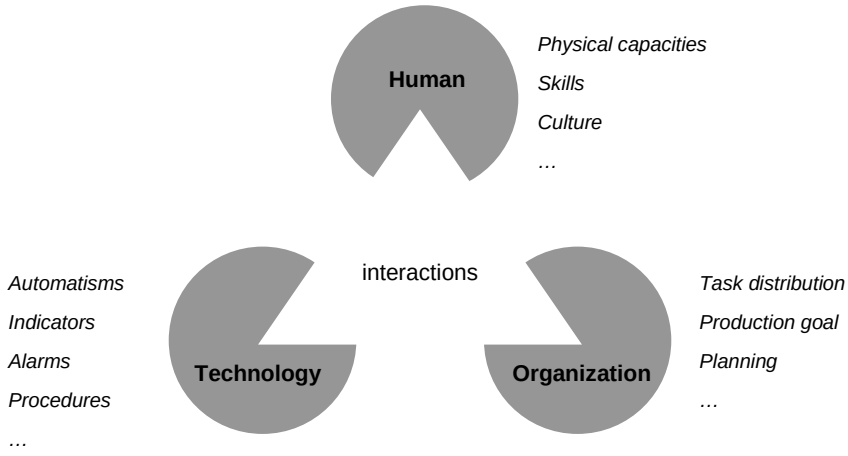


Fig. 2: Model of the causes and expressions of human error (from Hollnagel, 1998)

We consider that this type of classification may help in identifying determining factors. However, we also consider that a full inventory of these factors would only have any sense if it was possible to claim this exhaustiveness, which is not the case. For the Omega 20 method, we chose to encourage users in searching for more relevant factors as regards these situations. Further, experience has shown that the challenge of this identification is less related to the exhaustiveness of the completed inventory than to the relevance of the identified factors regarding the specificities of the situations.

Identification of these factors (or determining factors) is an exercise which requires being well aware of the relevant work situations, both from the required point of view in terms of safety (e.g.: closing a valve) and from the point of view of the work of the involved operators, as they perform it usually, including in certain degraded situations. **It is by comparing the work situations as they are expected and the work situations as they are actually carried out, that it is possible to show the factors which facilitate or perturb the achievement of safety missions entrusted to humans.**

The identification of these determining factors is important as regards the quality of the evaluation of the barrier. It is carried out by comparison between:

- Theoretical, formal and prescriptive data on the task and the predicted conditions for accomplishing it, as defined by the designers and managers of the installations. These data are most often formalized in operating procedures, procedures or organization notes.
- More informal and more subjective data on the context and on actual work practices. These data for example correspond to certain perturbed situations or not predicted by the organization within which humans have developed different strategies or adaptative forms, either consciously or not, with which they may achieve the set goals with certain compromises (e.g.: considering the emergency of a situation, an operator entrusts one of his/her tasks to another operator).

The analysis of the facilitating or perturbing character of the thereby identified factors will be the first step which should allow in a first phase, qualitative appreciation of the risk of failure of each of the sub-tasks within the scope of the Omega 20 method. The question will then be to meet the goal of quantifying the performance of the barrier, of « expressing », by means of the tools proposed by the method, the risk of failure of each of the sub-tasks forming the safety barrier as a global failure rate of the mission entrusted to the operator, expressed quantitatively.

2.3.3 PRINCIPLES OF QUANTIFICATION OF HUMAN SAFETY BARRIERS

The fault or failure rate of a mission entrusted to an operator may be compared with an equivalent notion usually used for a technical device: the Probability of Failure on Demand (PFD). This notion may be extended to human action in order to evaluate the probability of failure on demand of the operator responsible for a safety action.

Orders of magnitude of the failure rate of human actions may be found in the bibliography [5]. For example, here are values which are found in annex F of the NF-EN 61511-3 standard [6] for estimating the probability of failure on demand (PFD).

Action of a trained and unstressed human : 1.0×10^{-2} to 1.0×10^{-4},

Response of an operator to an alarm : 1.0×10^{-1},

Action of a stressed human : 0.5 to 1.

These values are quantities which do not account for various influence parameters such as the nature of the task which was requested or further the background surrounding the operator. Nevertheless there are several methods for evaluating reliability (THERP, SHERPA, …) which use this type of quantified data, by correcting them with influence factors.

The THERP method for example takes several tens of influence factors into account on human actions such as the number of working hours, the temperature, the complexity, the time pressure… etc.

In 1985, a study was conducted by the JRC[6] in order to proceed with a cross-evaluation of the probability of human failure on an « incidental » sequence identified on a nuclear site [7]. Fifteen teams of experts from 11 different countries proceeded with this evaluation. The results bring to light problems of application – increasing difficulty of application and sensitivity to expert assessment – and insufficient consideration of the interactions of humans with the organization and the organizational culture.

[6] The JRC (Joint Research Center) or Common Research Center is the scientific body of the European Commission.

Although other methods which have been developed more recently provide an answer to some of the criticisms usually aimed at the HRA methods (Human Reliability Assessment), problems remain: uncertainties attached to evaluations, sensitivity to expert judgement… etc. Experts on human factors agree with the statement that knowledge on the processes of human error is today sufficiently broad for better designing the interfaces, but these knowledge remains simplified models of mental activity and of complex realities.

Also, considering these limits, we choose to adopt a quantification per probability class and an *a priori* conservative approach, by considering a nominal human failure probability of 10^{-2}; this failure probability should be revised upwards in the case of identification of factors perturbing human reliability during the analysis of the work situation but it cannot ever be less than this value.

The Omega 20 method from this point of view is distinguished from fixed methods based on the single use of a database, most often referring to too general data which do not integrate the specificities of the environment of the evaluated safety barriers.

2.4 LIMITS OF THE Ω20 METHOD

The aforementioned orientations as well as the methodological choices presented in the previous paragraphs are justified by the intended goal and scope of use of the method. Indeed, let us recall that the approach developed in this document is dictated by a pragmatic transfer purpose for non-experts about subjects relating to human factors, but experts in the field of industrial risks. These choices imply two major limits about which the reader should be warned. They are mentioned in the following paragraphs.

2.4.1 A SIMPLIFIED VIEW OF HUMANS AND THEIR WORK

The simplified vision of the human task (detection, diagnostic and action) has the advantage of being easy to take over for the largest number of users. On the other hand, it does not take into account a certain number of other characteristics of humans and of their behavior: their capabilities of anticipating hazards and of recovering from their own errors, the influence of the company safety culture, their perception of risk, their confidence in procedures, their personality, their rigorousness, their values, their beliefs, their relationships with colleagues, their resistance to stress …

Depending on the cases, the affective, social and cultural dimensions may have an influence on the performance of HSBs sometimes more important than the cognitive and physiological dimensions taken into account in Omega 20. For example, these dimensions are predominant in the performance of symbolic barriers based on observance of certain prohibitions (no smoking, no entry into room, …etc.). taking into account these dimensions needs complementary analysis approaches which requires being knowledgeable in work psychology, in ergonomics, or in sociology, and deeper analysis. These subjects also provide better consideration of the collective aspects and those relative to cooperation between actors for applying human safety barriers.

Accordingly, with this method, it is not possible to apprehend the whole of the failure modes as proper operating modes of these barriers, which is inherent to any analytical approach of this type. In other words, we consider that the view of human work on which the method and the associated evaluation criteria are based allows an essential part to be apprehended - and within the reach of non-specialists – of the operating dimensions of human barriers.

2.4.2 LIMITED CONSIDERATION OF THE ORGANIZATION

We consider that human safety barriers are socio-technical systems designed, maintained and controlled by a set of processes which accompany their development or life cycle: updating set values, maintaining supervision systems, education and maintaining skills, hierarchical control and audit,…etc. These processes contribute to guaranteeing humans means of action or resources which they need for acting and confronting possible perturbations so as to thereby maintain over time a reliability level which meets the safety tasks. **Thus, we consider that the performance of each of the human safety barriers is dependent of that of a set of organizational processes.**

In other words, we may consider that **maintaining performances of human barriers should be ensured by organizational means set up by the corporation**. These means normally handled by safety management processes (described by the Safety Management System or SMS), are the following:

- means for maintaining competence over time: education, training, exercises,
- means for managing degradations and migrations of the practices and for maintaining resources over time: managing modifications and controlling exploitation,
- means for controlling performance of the barriers: exercises, inspections,
- means for monitoring the system, detecting degradations and improving practices: audits and an experience feedback system.

However, the Omega 20 method is not aimed at these organizational processes and does not allow their evaluation. The evaluation of these organizational processes requires other types of approaches (audit, organizational diagnostic) which will then be complementary to the approach proposed in Omega 20.

Note:

Within the scope of the methodology developed in this document, it is not possible to evaluate *a priori* the performance of a procedure, of a set of organizational means (Permit to work, Internal Emergency Plan) or of a management process (such as maintenance and training). Only the operational arrangements which are provided within the scope of applying these procedures, organizational means or management processes, may be evaluated with the Omega 20 method.

2.4.3 LIMITS BUT POSSIBILITIES OF LINKING WITH OTHER APPROACHES

As already indicated at the end of paragraph 2.2, the Omega 20 method is included in an ergonomic approach of the evaluation of work situations. However, if the issues of the Omega 20 method converge with those from the methodology of ergonomic analysis, the Omega 20 method is distinguished therefrom by at least two points of view, among which that of voluntarily simplifying assumptions on which Omega 20 is based and that of the complexity and of the voluntarily limited cost of its application.

This method, necessarily a simplifying method, proposes a first approach which depending on the context and issues, may be completed by application of « human and organizational factors » by specialists of analytical methods more representative of the complexity of work systems.

2.5 SHORT SUMMARY OF THE FOUNDATION PRINCIPLES OF THE OMEGA 20 METHOD

The Omega 20 method is a method which proposes a first approach of human factors accessible to risk managers for evaluating the performance of human safety barriers.

It is based on a qualitative analysis of the work situation corresponding to the application of the human safety barrier. The work situation is analyzed in order to detect factors which contribute to or perturb the achievement of safety missions entrusted to humans. This analysis requires the assessment and expertise of a work group, with the purpose of comparing work situations as provided and work situations as they are actually managed.

In order to meet the need for quantitative evaluation of the performances of safety barriers, the method proposes a scoring system with which from the qualitative analysis, it is possible to determine a failure probability class of the safety barrier.

3. SUCCINCT PRESENTATION OF THE OMEGA 20 METHOD

It is recalled that prior to applying our approach, the whole of the dangerous situations as well as the safety functions with which the consequences of these dangerous situations may be prevented or limited, will have been identified during an analysis of risks.

3.1 STEPS OF THE OMEGA 20 EVALUATION

The approach first comprises a **qualitative analysis** conducted in a work group requiring an effort for collecting data on the investigated work situation.

The collected data in a first phase allow « selection » of the barrier while ensuring that it meets the three following minimal criteria:

- **Independence,**
- **Efficiency (or feasibility),**
- **Response time,**

Once it is « selected », the barrier is evaluated for its contribution to reducing risks of accident. This **evaluation** is made through the **confidence level** criteria.

3.1.1 PRIOR ANALYSIS: FUNCTIONAL BREAKDOWN AND COLLECTING USEFUL DATA FOR THE EVALUATION

In order to meet the selection and performance criteria of human safety barriers, a prior step is required: it aims at allowing the human safety barrier to be broken down functionally depending on the splitting (detection, diagnostic, action), which also involves identification of the elements which describe each of these sub-actions. The question is also to collect a sufficient set of relevant pieces of information for informing the different evaluation criteria proposed by the method. These criteria essentially relate to the level of requirements of the task and its feasibility by humans involved, taking into account the suitability of the provided technical devices.

3.1.2 SELECTION STEP BY MINIMUM CRITERIA

1 – Verification of the independence principle:

The human safety barrier should be **independent** of the initiating event which may lead to its actuation so that it may be retained as a barrier acting on the scenario induced by the initiating event. **Its performances should not degraded by the occurrence of the initiating event.**

2- Evaluation of the efficiency:

The efficiency is the capability of the safety barrier of fulfilling the safety function for which it was selected, in its **context of use** and **during a given operating time.**

Evaluation of the efficiency is based on the principles of **adapted dimensioning** and of **resistance to specific constraints**.

3- Evaluation of the response time:

The response time corresponds to the time interval between the moment when a safety barrier, in a context of use, is actuated and the moment when the safety function provided by the safety barrier is carried out in its integrality.

Let us recall that, **in order to retain a barrier according to this criterion, the response time of the barrier should be in adequacy with the kinetics of the phenomenon which it should control, i .e. it should significantly less than that of the kinetics.**

3.1.3 STEP FOR EVALUATING PERFORMANCE : CONFIDENCE LEVEL (CL)

The CL allows determination of a risk reduction factor induced by the barriers according to the following correspondence: for a barrier of confidence level CL, the **risk reduction is conservatively 10^{CL}**: the following Table shows the equivalences between confidence level, probability of failure on demand and risk reduction factor.

PFD	CL	Risk reduction factor
$10^{-3} \leq PFD < 10^{-2}$	2	100
$10^{-2} \leq PFD < 10^{-1}$	1	10
$PFD \geq 10^{-1}$	0	1

Table 1: correspondence between confidence level, probability of failure and risk reduction factor

The evaluation of CL is carried out in 3 steps, corresponding to the three sub-functions by which the human safety barrier is broken down (detection, diagnostic and action). For each of the sub-functions, with a table it is possible to associate a downrating depending on the characteristics of the work situation to be analyzed.

In the case of a safety barrier involving several actors, qualitative criteria associated with the collective dimension of the barrier will have to be verified. Taking this dimension into account requires a thought process adapted to the context, like the remainder of the approach.

The method proposed in the present document postulates that the maximum confidence level of a human safety barrier is 2 ($10^{-2} \geq PFD \geq 10^{-3}$). **Depending on the downrating level associated with the analyzed barrier, the final confidence level may be 2, 1 or 0.**

3.2 METHODS FOR APPLYING THE APPROACH : RECOMMENDATIONS

The quality of the evaluation will depend on the comprehension level of the actual dimension of the work situation and on the capability of the users of integrating these knowledge items in their appreciation of the generic criteria of the method.

Two complementary points of view should be taken into account:

- The points of view of the technical expert of the method or of the operational activity in play, of the « designer » of the safety barrier and of the persons responsible for controlling its application: what are the efficient and prescribed actions, what is their purpose, and what are the expected results as regards the method or the activity to be controlled, what context and what associated conditions have been designed, … ?
- The point of view of the operator(s) responsible for the constitutive actions of the safety barrier: how does the operator usually react to the instructions and prescriptions (is this in adequacy with the pursued goal within the scope of the safety barrier ?), what are the limits and difficulties for accomplishing the action which are known or considered by him/her by experience, … ?

For these reasons, the evaluation should imperatively be made within the scope of a work group, led by a guarantor of the method, result from collective work and from interactions between the different members of the work group, so as to obtain elements of appreciation of the different criteria of the method on the basis of a vision as close as possible to the actual work situation.

Certain precautions should therefore be taken and the guarantor of the method will take particular care in promoting expression from the operator(s) of items of knowledge on the work situation from their own feedback experience and from that of their colleagues responsible for the same safety barrier.

Prior to forming the working group, it is absolutely necessary to visit on the site the relevant installations and work stations in order to realize for example:

- the physical environment - distances, luminosity, accessibility, etc -
- the clarity of the information to be processed by the operator,
- the accessibility of the operating procedures, the assistance or action means,
- etc.

A visit of the site and the forming of a work group, led by a guarantor of the method and comprising representatives of the different job functions concerned by the safety task and its issues, are required.

4. DETAILED PRESENTATION OF THE STEPS OF THE OMEGA 20 METHOD

In this chapter, the term of « human safety barrier » is also used for designating the human component of a safety barrier, in the sense given in the definition of the MASS.

4.1 PRIOR ANALYSIS: FUNCTIONAL BREAKDOWN AND COLLECTING USEFUL DATA FOR EVALUATING HUMAN SAFETY BARRIERS

We shall designate by « work situation », the system formed by the safety task of the whole of the means designed for allowing the operators to meet the requirements of the task and of other factors capable of perturbing its performance. As a corollary, we consider that the performance of the safety tasks depend on the sufficiency and adequacy of the designed means considering the requirements of the task but also predictable effects of a certain number of perturbing or threatening factors.

Therefore the aim is:

- to analyze the requirements of the task from a functional breakdown of the safety barrier into three sub-functions,
- to collect the data relative to the work situation in order to highlight the factors which facilitate or perturb the achievement of the safety missions entrusted to humans.

The first result of this step corresponds to the breakdown of the safety barrier according to the three sub-functions which make it up.

The following Table gives an exemplary functional breakdown of the human safety barrier « Operation for checking the seal of a circuit conditioning activation of the circuit ».

Obtaining the information	Diagnostic / selection of the safety action	Performing the safety action
Information obtained by applying a foaming product and a pressurized air flow inside a pipe	Interpretation of the bubbling at the surface of the pipe as leakage	Closed the pipe

Table 2: Functional breakdown example of the human safety barrier

Note: Caution with the definition of the safety action:

The safety action included in the HSB is reduced to the tasks which may be opposed to the predicted accident scenario. That is to say that it notably does not encompass the activities for repairing installations subsequent to detection of an abnormality.

For example, subsequent to the possibility of occurrence of a leak scenario by corrosion, a human safety barrier has been set up: it consists of performing a periodic inspection of the thickness of the pipe. When this inspection results in the identification of a fault (detection and diagnostic phases), provision is made for replacing the concerned tube. The safety action of the barrier is not the replacement of the tube but the stopping of the installation (or bypassing the conduit portion) before occurrence of the scenario.

The second result of this step for analyzing and collecting data consists of identifying the elements relative:

- **to the means provided for accomplishing the safety task:** persons responsible for the actions, available delay, resources used (procedures, tools, documentation, …, etc), signaling devices used and actuated control elements,
- **to the background elements** related to the environment, to the working conditions, to the general activity in progress, …

As explained in the previous chapter, **the methods for collecting these data are those of the work group.** The latter may rely on analysis and questioning methods of the WWWWWHH [7] or 5M[8] type. It may also be useful to exploit the data from observations *in situ*, of exercises, of feedback experience on the application of the barriers, and on the encountered incidental/accidental situations.

Let us note that it is of interest to track these elements for various purposes: justification of the demonstration of the evaluation, consideration of fine context elements, valuation of the experience of the work group, …etc.

[7] WWWWWHH : What – Who – Where – When – Why – How – How much ?

[8] 5M: EnvironMent, work Method, Material (products), EquipMent, Man power (Fishbone / Ishikawa diagram)

4.2 EXAMINING SELECTIVE PERFORMANCE CRITERIA OF HUMAN SAFETY BARRIERS

4.2.1 PRINCIPLE OF INDEPENDENCE

In order to be able to select a human safety barrier as regards an accident scenario, it is required that it **should be independent of the cause of the scenario** or of the actual scenario. The HSB should be **independent** of the initiating event which may lead to its actuation so that it may be retained as a barrier acting on the scenario induced by the initiating event, i.e. the operator responsible for the barrier and the technical elements which he/she uses should be independent of the cause of the scenario or of the actual scenario.

This first principle of independence is a selection criterion within the scope of the barrier approach. **If this criterion is not met, the approach will stop at this stage: the barrier cannot be retained.**

Expressed in another way, checking the independence of the barrier amounts to « checking the independence between the safety task and the exploitation task ». This verification consists of pondering on the dependencies between the causes of failure of the barrier on the scenario and the actual cause of the scenario (for example a technical failure or an operating error).

For the case of compensation barriers, the possible dependency mode is often easy to identify. For example, if an overflow is caused by uneasiness of an operator, the action of this same operator cannot be considered for compensating the overflow: the barrier is under the dependency of the cause of the scenario.

For verification barriers, this may be more delicate, as the safety and exploitation functions are structurally less separated than in the technical field (for example, good industrial practices are frequently expressed by redundancy of an exploitation valve with a safety valve).

As regards verification operations, the independence of the safety barrier may be provided in two ways:

- The safety task is performed by a person different from the one who performed the first action: this corresponds to an « organizational » independence form.
- The safety task is included in a work sequence different from the exploitation action[9]: this corresponds to a “time” independence form.

[9] It should be noted that the self-control capability of the operator during performance of the action and the capability of compensating the situation in the case of detection of an error is a process inherent to humans and therefore cannot be considered as an independent action.

4.2.2 EFFICIENCY (OR FEASABILITY)

This is the capacity of a safety barrier of fulfilling the safety function for which it was selected, in its context of use, for a given operating time.

Efficiency should be considered with respect to all the elements making up the HSB.

By analogy with Technical Safety Barriers, evaluation of the efficiency is based on adapting the principles of:

- adapted dimensioning,
- resistance to specific constraints.

4.2.2.1 PRINCIPLE OF ADAPTED DIMENSIONING

The human component of HSBs meets the principle of adapted dimensioning:

- if the safety task, as provided, allows the safety goal indicated in the context of the scenario to be achieved,

- if the knowledge needs of the operator related to performing the safety task have been identified and provided (awareness of the safety issues related to the task to be carried out and to the conditions of its performance, training, guilds, …),

- if the material needs of the operator related to performing the safety task have been identified and provided (help tools, documentation, procedures, … etc.).

By collecting information from answers to the following questions (non-exhaustive list) it is possible to justify the provided means and evaluate the adapted dimensioning of the barrier towards the safety function to be provided:

- Is the operator sufficiently aware of the safety issues related to the task to be performed? Is he/she aware of dangerous phenomena which may be generated and of the risks incurred by him/her?
- Have the required skills for performing the task been identified? What are the applied training means for meeting these needs: initial training, guilds, training sessions, etc.
  Depending on the nature of the task to be carried out as well as on their frequency of performance, it may be necessary to have regular training sessions or re-training sessions. The training should be carried out under conditions as close as possible to actual conditions.
- Is a documentation (procedure, check-list, logic diagram, abacus, …etc) required for assisting the operator in his/her task ? If yes, is this anticipated? Is it updated sufficiently regularly? Is it available to the operator?
- Are the required tools for performing the task provided? Are they available to the operator?
- Is there any feedback experience from applying the barrier, in an actual

situation or under conditions close to the actual conditions?
By exploiting feedback experience (confrontation of experiences from different operators, exercises, audits, …), it is possible to justify to a certain extent the proper design and proper dimensioning of the task.

4.2.2.2 PRINCIPLE OF RESISTANCE TO SPECIFIC CONSTRAINTS

The human component of the HSBs meets the **principle of resistance to specific constraints if the constraints related to the context of use of the barrier (constraints related to the environment, to exploitation, to the applied products, ...) do not bring up the issue of the operation of the constitutive elements of the barrier.**

The goal is to verify that the constraints related to the context of use of the barrier do not question the operator's capacity of accomplishing his/her safety task. In particular the question is to make sure that the actors who have to perform safety actions will be protected from the accidental context of the scenario.

(Non-exhaustive) list of questions for meeting the principle of resistance to specific constraints:

- Are the individual pieces of protective equipment suitable for protecting the operator who has to intervene?
- Are the intervention means designed and positioned so as not to expose the operator who will have to actuate them?

4.2.3 RESPONSE TIME

This is the time interval between the moment when a safety barrier, in a context of use, is actuated or activated and the moment when the safety function ensured by the safety barrier is carried out in its integrality.

This definition implies that the response time integrates:

- the time required for detecting the incident or the sought information (if necessary comprising the time required for this search),

- the time required for the diagnostic providing the selection of the safety action ensuring the safety function,

- the time required for performing the safety action.

In order that the human safety barrier should be retained, its response time should be in adequacy with the kinetics of the phenomenon which it should control.

This criterion may also be inapplicable in the case of certain types of barriers: notably the task consisting of making sure that the intended conditions are met in order to safely operate the installation. In this case, the only time requirement on the verification action is that it actually takes place before operating the installation**.**

The response time is obtained by considering the whole of the elementary steps required for performing the safety task.

For example, response time integrates:

- In the case of watchman rounds: the maximum lapse of time between the potential starting of the fire and the moment when the watchman may actually detect this fire. If the round takes place every two hours, the maximum detection time will therefore be two hours, a time to be added to the time required for example to walk up to the control station and to set off the alarm and start up the fire means, as well as the time for the fire protection means to become fully operational.
- In the case when the operator has to be protected for intervening: the time required for putting on individual protective pieces of equipment (suits, individual respiratory units, …).

It should be noted that the response time as defined earlier does not integrate the time required for the danger flow (for example a fire) to reach the (technical or human) detection means. For example, if the detection is olfactory, the time between the beginning of the leak and the time when the odor reaches the operator is not included.

It will be noted that the evaluation of the response time should be conservative so as to take into account a certain number of aggravating factors such as stress, non-optimum availability or the resources, etc. It should also be conservative in order to take into account the autonomy of the the operators in order to face these hazards and stress sources.

Carrying out exercises (for example a fire intervention case) and exploiting feedback experience on these accident simulations (observation, timing, hazard analysis, …) are thus greatly recommended.

4.3 EVALUATION OF THE PERFORMANCE OF HUMAN SAFETY BARRIERS: CONFIDENCE LEVEL (CL)

The proposed method postulates that the optimum confidence level of a barrier is 2 ($10^{-2} \geq PFD \geq 10^{-3}$) and that this level decreases from the moment when the requirements related to the three sub-functions (obtaining information, processing allowing selection of the action and performance of the action) making up the safety function provided by the barrier are partly or not satisfied.

The method requires **examination of three tables** (one table per sub-function) **and then examination of minimum conditions for taking into account the HSB when it involves several actors**.

The confidence level retained for the human safety barrier corresponds to the difference between the optimum confidence level (2) and the sum of the downratings over the three tables corresponding to each of the sub-functions. It will be zero if the minimum conditions to be taken into account are not observed.

The following paragraphs show indicative tables for evaluating the adequate downrating level. For each sub-function, the tables indicate two types of requirements to be fulfilled in order to provide an optimum performance level. Practically, application of these tables is accomplished in the following way:

- Zero downrating is obtained when each of the two requirements for the success of the task is satisfied.
- An intermediate downrating (-1) is obtained when at least one of the two requirements for the success of the task is only fairly satisfied.
- Maximum downrating (-2) is obtained as soon as one of the two requirements for the success of the task is not satisfied.

Let us recall that the selection of a downrating is made on the basis of a **qualitative assessment built by the persons from the work group** involved in evaluating the performance of the barrier**.** The selection of the downrating in particular relies on the **identification which will have been made of the aid factors or perturbing factors which are determining towards the success of the evaluated safety task.**

4.3.1 FIRST SUB-FUNCTION: OBTAINING THE INFORMATION

Within the scope of this first sub-function, the activity of the operator may be of different nature. Two cases are possible:

- The operator has a « passive » role: the operator is alerted or approached by the arrival of a fortuitous information (expected alarm, physical phenomenon, …); arrival of the information may interrupt the current activity.
- The operator has an « active » role: he/she should be engaged in a programmed activity (for example a surveillance phase, a round, …) for preventing the risks, the purpose of which is to obtain one or more pieces of information allowing abnormalities or process deviation to be detected. The term of “information” has a sufficiently wide connotation, it notably encompasses the value of an operating parameter, a physical measurement, the characterization of a condition (sealed or non-sealed, closed valve or not, resistance to pressure or not …), …etc.

4.3.1.1 "PASSIVE DETECTION"

Downrating	Characteristics of the work situation
0	Information clearly perceivable and identifiable: Information available in a hierarchical way (for example: a dedicated visual and sound alarm clearly distinct from the other types of alarms) giving the condition of the system, regardless of the environmental conditions (night, fog, …) and which would be capable of preventing or hindering perception of this information. AND Total availability of the operator: The operator is present in the location where the information is available and he/she may interrupt any other current activity. The working conditions are favorable to maintaining a good vigilance level.
- 1	Information perceivable and identifiable with moderate difficulty: Information available in a non-hierarchical way in the midst of a limited number of other pieces of information. AND/OR Availability of the operator: The operator is present in the location where the information is available and he/she may be led to managing an acceptable number of other tasks at the same time without questioning his/her perception capabilities.
- 2	Information difficult to perceive and identify: The information embedded in other pieces of information or information which is difficult to detect (localization of the information is not adapted to the activity of the operator, perception which may prove to be difficult, notably under certain environmental conditions or within the scope of the progression of the scenario). OR Low availability of the operator: The operator is seldom present in the location where the information is available or else he/she is present randomly, in an unpredictable way, or he/she may be led to managing a significant number of tasks at the same time.

Table 3: Estimation of the confidence level on the sub-function for obtaining information ("passive detection" case)

4.3.1.2 "ACTIVE DETECTION"

Downrating	Characteristics of the work situation
0	Easiness for obtaining the sought information: Identifying or obtaining simple information (clearly identifiable information, no possible confusion, …) relatively to the expected competence level of the operator and working conditions which are estimated as non-restricting (favorable environmental conditions, good accessibility to information …). AND Total availability and commitment of the operator: This task is a programmed activity, well dimensioned in the work load program of the operator, and perceived as being a priority[10] by the operator. The latter has sufficient autonomy in order to face possible hazards without compromising the performance of the task under the required conditions.
- 1	Fairly easy conditions for obtaining the sought information: Identifying or obtaining the information is achieved with an acceptable (intellectual and/or physical) effort with regard to the expected competence level of the operator and to the conditions for accessing the information. AND/OR Availability and commitment of the operator: This task is a programmed and dimensioned activity in the work load program of the operator, and perceived as being important by the operator. The latter has a more reduced autonomy in order to face possible hazards.
- 2	Impossibility of or difficulty in obtaining the sought information: Identifying or obtaining information is difficult to achieve or is achieved with a substantial (intellectual and/or physical) effort or the working conditions are estimated as being restrictive (very difficult access to information, tiresome activity, …). OR Low availability and commitment of the operator: This task is not provided or is not properly dimensioned in the work load program of the operator or this task may be perceived as being of lesser priority with respect to other operational constraints.

Table 4: Estimation of the confidence level on the sub-function for obtaining information ("active detection" case)

[10] The priority which the operator may assign to the safety task should be evaluated in the more general background of the global activity of the operator. As the available resources are not infinite and the safety task is only part of the work of the operator, the latter may depending on the hazards or unexpected events, be led to punctually or more durably revise the planning of the priority of certain of his/her tasks. Consequently, non-accomplishment of the safety task as expected may have multiple explanations. Attention may be made in particular:

- To the conditions of the operator (routine tasks, poor environmental conditions, isolation, very physical labor or difficulties in accessing the work station,…etc.: by integrating ergonomics upon designing and modifying work stations or conditions, it is possible for the operator to optimize the use of his/her resources and to limit the risk of successive postponements of certain tasks or even their progressive negligence.
- To the sense which may be given by the operator to the safety task: for example, if the rounds up to now have not shown any fault or if the safety culture is low, the operator may gradually acquire the feeling or even the conviction of the « pointlessness » of the task. The practice of inspections regarding performance of this task (surprise visit, inspection by sampling, recording of the actions, instrumented surveillance, …) may contribute to maintaining attention on the importance of the task as regards safety.

4.3.2 SECOND SUB-FUNCTION: DIAGNOSTIC ALLOWING SELECTION OF THE ACTION TO BE PERFORMED

Downrating	Characteristics of the work situation
0	Good quality and accessibility of the information useful for the diagnostic: Explicit presentation and sufficient level of information: direct information not subject to interpretation on the condition of the system (and localization of the accident), on the incident or on the failure(observance of conventions for displaying information, the case of faulty indicators being signaled,…). The operator if necessary has a comfortable time period in order to stand back from the useful quality and level of information, and to go deeper into the diagnostic. AND Guiding level adapted to the situation: The use of procedures is not necessary or in the opposite case, decision is guided by explicit procedures (clear instructions and explanation of the consequences of the action on the system) or contextual help provided by the system (on the driving system, signaling in proximity to signaling devices or control units…) which allow easy determination of the action to be performed.
- 1	Acceptable quality of the information useful for the diagnostic: Presentation of not directly usable information for making the diagnostic but processing modes are provided in order to obtain the information useful for the diagnostic but which may sometimes be a source of error (certain types of calculations, unit conversion,…) Or a level of information which is not always sufficient but it is possible to go deeper into the diagnostic by seeking complementary information (the operator then has a reasonable time limit for standing back and collecting the required information) AND/OR Provided but sometimes insufficient guidance: A certain level of guidance is required: the general rules to be applied are known or formalized but a certain level of interpretation of the rules is required in order to decide on the course of action to be taken (for example the procedures deal with many known cases but a thinking process remains necessary for making a decision).
-2	Insufficient quality of the information useful for the diagnostic: Insufficiently explicit information (ambiguous or requiring complex calculations, cross- referencing of data or a thinking process mobilizing unfamiliar knowledge). Or an insufficient information level for identifying the problem or the conditions of the system, deepening of the diagnostic is conceivable with difficulty considering the context or the organization of the work (insufficient available time, geographic isolation,…). OR Insufficient guidance: Application of the rules is conceivable with difficulty, taking the situation into account: a too general or too specific rule which requires quasi-systematic adaptations, or a too large number of selections of possible actions, standing back or asking for external advice being difficult (insufficient required time resources relatively to the progression of the scenario or resorting to a third party not provided in the work organization).

Table 5: Estimation of the confidence level on the sub-function for processing information allowing selection of the action to be performed

4.3.3 THIRD SUB-FUNCTION: SAFETY ACTION TO BE PERFORMED

Downrating	Characteristics to the work situation
0	Acceptable stress level: Resources required for performing the action are estimated to be sufficient: absence of time pressure or an intervention time much less than the kinetics of the accident, no exposure to danger, significant experience of the situation, sufficient feedback on the engaged action;… AND Simple and not very demanding task: Limited number of actions, without any complex sequence (for example: closing several valves without any notion of order), an error-robust system (foolproof device, timer, color codes or symbols avoiding the risk of confusion,…) or allowing the operator to be alerted in order to give him/her the possibility of going back. The action means being easily accessible and easily maneuverable.
- 1	Possible but tolerable stress level: Resources required for performing the action, estimated that they may be insufficient, notably under certain difficult conditions (no time margin, exposure to danger,…) AND/OR Fairly demanding or difficult task: A limited number of actions but a higher requirement level: significant memorization or concentration efforts, sequences which should be strictly observed (for example: stopping pump P1 and then only after this, closing valve V1 and then V2. Modifying the order of these actions would cause an accident) but the system allows the operator to go back. Or the action means may be fairly accessible and maneuverable.
- 2	Significant stress level: Strong feeling of pressure: resources required for performing the action are estimated to be unsuitable with respect to the goals to be achieved (time estimated to be insufficient, exposure to danger, panic effect,…). OR Very demanding, difficult or impossible task: Too high requirement level (a large number of actions with strict sequences, impossibility of interrupting the effects of an action engaged erroneously,…) and/or difficult or impossible accessibility or maneuverability of the action means.

Table 6: Estimation of the confidence level on the sub-function for performing the safety action

4.3.4 CONDITION FOR COMPLETE DOWNRATING OF THE BARRIER: CASE OF THE HUMAN SAFETY BARRIER INVOLVING SEVERAL ACTORS

In this case it is necessary to make sure that the roles and the responsibilities of the different actors are clearly established and known to them, that the transmitted information is without any ambiguity (designation of the equipment, the devices, the safety action…) and that the communication tools are clearly identified and performing.

In the opposite case, the human safety barrier will not be retained (NC=0).

4.4 APPLICATION TO THE CASE OF MIXED BARRIERS WITH TECHNICAL AND HUMAN COMPONENTS: THE MASSES

As indicated in paragraph 2.1.1, a human safety barrier may include a technical safety device.

In this case, each of the components[11] should be evaluated separately according to the principle of independence and the criteria of feasibility, response time and confidence level.

Next, the evaluation of the safety barrier encompassing the human and technical components follows the following principles:

- Independence of the barrier is ensured if each of the components is independent
- The global efficiency of the barrier will be evaluated with reference to the safety function provided by the whole of the technical and human components forming the barrier.
- The overall response time will be the sum of the response times of each of the components.
- The retained confidence level for the barrier will be the minimum of the confidence levels of each component.

11For the technical component, the reader may usefully rely on the Ω10 report "Evaluation of preventive and protective devices used for reducing the risks of major accidents".

5. AGGREGATING HUMAN SAFETY BARRIERS

Within the scope of demonstrating the control of the risks on a scenario, one may be led to evaluating the performances of each of the barriers acting on the scenario in order to evaluate the reduction level of the risks brought about by the whole of the risk-controlling measures on this scenario. In this specific case, one may be led to wanting to aggregate several human safety barriers together by adding the confidence levels of each of the barriers.

5.1 EXAMINING THE EXISTENCE OF A COMMON FAILURE MODE BETWEEN THE HSBS TO BE AGGREGATED

In order to aggregate on a same scenario several human safety barriers, it should be ensured that the barriers are actually **independent of each other**.

Therefore the existence of a common failure mode between the HSBs which one wishes to aggregate should be examined: for example, when two HSBs have a **same technical element** (same valve to be actuated in both barriers or same communication means) or a same **human element** (same operator in charge of both barriers). If this is the case and if both of these barriers ensure the same safety function, it will be possible to retain the confidence level of only one of these barriers (the one for which the confidence level is the smallest).

In the absence of a failure common mode among the HSBs which one wishes to aggregate, it will be possible to sum the confidence levels of the barriers together. This is equivalent to considering the performances of the barriers as being independent of each other. However, **it will be necessary to ensure that the overall response time is properly evaluated by taking into account the whole of the safety barriers acting on the scenario and that the latter is in adequacy with the kinetics of the scenario.**

Notably in the case when two barriers would intervene during the accidental sequence, the second barrier will be actuated in the case of failure of the first, the response times of both barriers should therefore be added together; the second barrier will only be performing if this total time is compatible with the kinetics of the accident.

Note: An exception to this principle may be made in the case when the common element would be an operator in charge of both:

- a barrier which intervenes upstream from the accidental sequence prior to the risky activity (case of the verification barrier),
- and a barrier which intervenes by compensating an already initiated accidental sequence (case of the compensation barrier).

In this case, the activities concerned by both barriers are quite distinct because of their position in the accidental sequence: adding the confidence levels of both barriers is possible provided that there is no other common failure mode.

5.2 PARTICULAR CASE OF AGGREGATION ON AN ACCIDENT SCENARIO OF HUMAN SAFETY BARRIERS PROVIDING THE SAME SAFETY FUNCTION

For barriers acting prior to the risky activity, it being understood that there is no time pressure relatively to the kinetics of a scenario, it is possible to consider a capability of compensation by applying an additional verification step.

Example: The starting a chemical reaction is conditioned by the pH of a reaction medium; this pH is checked once by the production operator and then by the laboratory of the company.

The application of an additional test or checking operation is considered as able to increase the confidence level of the activity from one level to the maximum, the maximum confidence level associated with the ensured safety function is then 3. In this case, and with caution, the confidence levels are not summed in order to take into account the possibility of a common failure mode (for example: informal arrangements between operators resulting from mutual trust).

6. GLOSSARY & DEFINITIONS

HSB : Human Safety Barrier

TSB : Technical Safety Barrier

JRC : Joint Research Center- European Commission

MEDDE : Ministère de l'Ecologie, , du Développement Durable et de l'Energie (French Ministry in charge of Ecology, Sustainable Development and Energy)

CL : Confidence Level

PFD : Probability of Failure on Demand

MASS : Manual Action Safety System

SMS : Safety Management System

DEFINITIONS:

INERIS proposes here definitions of the main technical terms used in this document. It will be noted that some of the following definitions are derived from the technical glossary of technological risks published by MEDDE.

Accident: An undesired event such as an emission of a toxic substance, a fire or an explosion, resulting from uncontrolled developments having occurred during the operation of an establishment which causes consequences/damages to persons, property or the environment and to the company broadly speaking. This is the occurrence of a dangerous phenomenon, combined with the presence of vulnerable targets exposed to these effects to this phenomenon.

Major accident: « An event such as an emission, a fire or an explosion of major importance resulting from uncontrolled developments having occurred during operation of an establishment, causing for the interests indicated in article L.511-1(humans, environment, patrimony) of the Environment Code, serious, immediate

or differed consequences and involving one or more substances or dangerous preparations.» (Modified decree as of May 10th 2000).

Activity: The activity corresponds to actual work: this is what the operator actually accomplishes when he/she is confronted with a practical situation. Two components are in play in the activity of an individual (i.e. the effective completion of the task): a physical component which comprises the gestures and postures and a mental component which relates to processing information and to thought processes.

Human Safety Barrier (HSB): Human safety barriers consist of human activity (one or more operations) which opposes the sequence of events likely to result in an accident.

Technical Safety Barrier (TSB): A barrier which provides a safety function. It consists of a safety device or a safety device with instrumentation which opposes the sequence of events likely to result in an accident.

Efficiency: The efficiency of a safety barrier is evaluated as regards its capacity of fulfilling the safety function for which it has been selected, in its context of use and for a given operating time. This capacity is expressed in an accomplishment percentage of the defined function, by considering normal (non-degraded) operation. This percentage may vary during the actuation time of the safety barrier.

Ergonomics: Ergonomics is the scientific specialty which aims at fundamentally understanding the interaction between humans and other components of a system, and the application of methods, theories and data for improving well-being of persons and global performances of the system. Ergonomists contribute to the design and to the evaluation of tasks, of jobs, of products, of environments and of systems, in order to make them compatible with the needs, the capabilities and limits of persons. (International Ergonomic Association, 2000)

Ergonomics uses knowledge from i.a., cognitive psychology (memory, attention, perception, learning…) and from psycho-physiology (vigilance, postures, working conditions…).

Initiating event: A current or abnormal event, internal or external to this system, located upstream from the central dreaded event in the causal sequence and which is a direct cause in simple cases or a combination of events at the origin of this direct cause. In the « bow-tie » (or causal tree) illustration, this event is located at the left end.

Central dreaded event: A conventionally defined event, within the scope of risk analysis, at the centre of the accidental sequence. Generally, this is a loss of confinement for fluids and a loss of physical integrity for solids. The events located upstream are conventionally called « pre-accidental phase » and the events located downstream « post-accidental phase ».

Safety function: A function having the purpose of preventing dreaded events and affording protection against them. The identified safety functions may be provided from technical safety barriers, human barriers, or more generally by a combination of both.

A same safety function may be achieved by different safety barriers.

A safety function may be broken down into related safety sub-functions.

Measure for controlling risks (or safety measure or safety barrier): The whole of the technical and/or organisational elements required and sufficient for providing a safety function.

Confidence level: This is an adaptation by INERIS of the requirements of the NF-EN 61508 [8] and NF-EN 61511[6] standards, notably as to the architectures of systems for all safety equipment, regardless of their technology. The term of confidence level is retained for the measures for controlling risks activated or provided by humans.

Performance of the barriers: The evaluation of the performance is made through their efficiency, their response time and their confidence level with regards to their architecture.

Scenario of a (major) accident: Sequence of events leading from an initiating event to a (major) accident, for which the sequence and the logical links result from risk analysis. Generally, several scenarios may lead to a same dangerous phenomenon which may lead to a (major) accident; as many scenarios are listed as there are possible combinations of events resulting in them. The obtained accident scenarios depend on the choice of the risk analysis method used and on the available elements.

Manual Action Safety Systems: These are a combination of a technical safety barrier and of a human activity in order to successfully complete a safety function (pressing on an emergency stop button, low flow rate alarm followed by manual closing of a safety valve…).

Task: The task is the result which is more or less explicitly expected from the individual under conditions imposed for performing it (to be distinguished from activity). The task corresponds to the prescribed work.

Response time: It corresponds to the time interval between the moment when a safety barrier in a context of use is actuated and the moment when the safety function provided by the safety barrier is carried out in its integrality.

7. REFERENCES

[1] N. Le, V. De Dianous, "Evaluation des dispositifs de prévention et de protection utilisés pour réduire les risques d'accidents majeurs" Ω10, Study Report No. DRA-08-95403-01561B, 01/09/2008: INERIS for the French Ministry in charge of Ecology and Sustainable Development, a report available on www.ineris.fr

[2] E. Miché, F. Prats, S. Chaumette, Démarche d'évaluation des Barrières Humaines de Sécurité. Ω 20, Study Report No. 46055, 21/12/2006

[3] Rasmussen J., Information Processing and Human-Machine Interaction, Amsterdam, North-Holland, 1986

[4] Hollnagel E., Cognitive reliability and error analysis method: CREAM. Elsevier, 1998

[5] Swain A.D., Guttmann, H.E., Handbook of Human Reliabiliaty Analysis with emphasis on Nuclear Power Plant Applications. NUREG/CR-1278, Washington, D.C.: US Nuclear Regulatory Commission, 1983

[6] NF-EN 61511, parts 1 to 3: Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur de l'industrie de process, March 2005

[7] Human Factors Reliability Benchmark Exercise, Reactor Safety Programme 1985-1987, Nuclear Science and Technology, Commission of the European Communities, August 1989 – EUR 12222 EN.

[8] NF-EN 61508, parts 1 to 7: Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité, March 2002

8. LIST OF ANNEXES

Mark	Designation	Number of pages
Annex A	Examples of application of the whole approach	12

ANNEXE A:

EXEMPLARY APPLICATIONS OF THE WHOLE APPROACH

EXEMPLARY SHEET NO.1: TASK FOR CHECKING CLOSURE OF BOTTOM VALVE PRIOR TO FILLING A REACTOR

In a workshop for making paint, mixtures are produced by an operator in a reactor. The bottom valve of the reactor (quarter turn valve) is located on the ground floor and loading is carried out on the first floor. This task is performed about 1,000 times a year by the same operator. Once the mixture is considered as satisfactory, the reactor is emptied via the bottom valve. Next the reactor is cleaned. At the end of the cleaning operation, the operator closes the bottom valve of the reactor.

The safety action consists in that the operator checks whether the bottom valve is closed before pouring the products into the reactor.

Independence	*This task may be considered as independent of the moment when checking of the closure of the valve is:* - *accomplished by a different person, this person giving the go-ahead to the loading operator ("organizational redundancy"),* - *accomplished by the same operator, from the moment that this check is carried out in a different working sequence ("time redundancy"):* a) *If the check is directly coupled to the cleaning operation, this task cannot be considered as independent.* b) *If another operation is performed before this check (for example: establishing connections required for producing the next mixture, checking the quality of the raw materials for the next mixing…) this task may be considered as independent.* *In this example, the latter case will only be considered (b).*
Efficiency	*Trained personnel, identified task in an operating procedure.* *The task is essentially physical, turning the valve does not require any particular strength or tool*
Response time	*irrelevant*
CL	*<u>"Active" detection:the operator has to go and check the position of the valve:</u>* 1. *The information is easy to obtain (the bottom valve is located in a covered and illuminated workshop) all the more as this is a quarter turn valve (when the valve is in the closed position, the actuator is perpendicular to the pipe). However, there may be a slight confusion with the bottom valve of another reactor (in particular taking into account round trips between both floors).* 2. *The task is well anticipated and dimensioned in the loading plan of the operator, and the whole of the task of the operator is programmed (specific operating procedure). However, the nature of the task (a rather repetitive task and having some hardship due to performing round trips (first floor – ground floor) may be perceived as constraining by the operator and affect commitment of the operator confronted with this task.* *Partial conclusion: the factor 1, like the factor 2, justifies **<u>downrating by one</u>***

	level *<u>Diagnostic and selection of the action:</u>* *1. The operator is directly informed on the condition of the valve (quarter turn valve)* *2. The action selection rule is known (no procedure required on the action selection)* *Partial conclusion: no downrating* *<u>Safety action:</u>* *1. There is no particular pressure related to the dreaded accident* *2. The task is simple: if the valve is open, then close it* *Partial conclusion: no downrating* *<u>Activity involving several actors: inapplicable</u>* ***Estimated confidence level: 1***

EXEMPLARY SHEET NO.2: TASK FOR MEASURING PH PRIOR TO STARTING THE REACTION

The reaction is catalyzed in an acid medium and the pH should be comprised in a safety range in order to minimize thermal runaway risks. The pH meter is calibrated every day.

This check is carried out on a sample taken from the synthesis reactor before heating the reactor. The operators are posted. An operator carries out between 150 to 200 syntheses of this type a year. The workshop includes five synthesis reactors which may be operated at the same time.

The safety action consists of measuring the pH of the reaction medium and of only starting the reaction (heating the reactor) when the pH is in the safety range. The work instruction specifies that if the pH is out of the safety range, the instructions are to evacuate the contents of the reactor after approval by the foreman.

Independence	*Yes: this check is the condition for starting the synthesis, the task is performed in a work sequence distinct from the starting (« time redundancy »)*
Efficiency	*Trained personnel, task identified in the process sheet.* *The measurement is conducted on a sample taken from the reaction medium.* *The pHmeter is calibrated once per station (recorded in the calibration log book)*
Response time	*irrelevant*
CL	*<u>"Active" detection: the operator has to go and take a sample and carry out a pH measurement</u>* *1. The information is easy to obtain (the workshop is covered, sampling the reagent does not pose any problem, the pH measurement is conducted in a dedicated laboratory in the workshop and located on the floor of the reactors, the operator is competent for conducting the pH measurement).* *2. The task is well anticipated and dimensioned in the loading plan of the operator, and the whole of the tasks of the operator is programmed (specific operating procedure) while the operator may be lacking in availability: he/she has several reactors to handle and he/she may be under pressure by the other tasks to be performed* *Partial conclusion: the factor 2 justifies the* ***downrating by one level*** *<u>Diagnostic and selection of the action:</u>* *1. Once the pH is measured, the operator only has to compare the pH with the tolerance range written down on the process sheet.* *2. The action selection is clearly determined in the instruction: the contents of the reactor have to be evacuated after validation by the foreman.* *Partial conclusion: no downrating*

	<u>Safety action:</u> 1. *The pressure related to the dreaded action scenario is under control as long as the reactor has not been started up again: similar situations may have been experienced by the operator.* 2. *The task is simple: the action consists of not starting the reaction (and warning the foreman). He is alone in handling the reactions, therefore there is no possibility that anybody else starts the reaction.* *Partial conclusion: no downrating* *<u>Activity involving several actors:</u>* *For each station, there is only one person to which this task is assigned. However, because of the changing of job posts and because the pH verification can only occur at the end of a post, it is possible that the following operator is not aware of the result of the pH measurement and thus a reaction will be started under bad conditions. To remedy this, an overlapping period is provided and information is transmitted on the basis of an instruction manual.* ***Estimated confidence level: 1***

EXEMPLARY SHEET NO.3: EXTINCTION OF A FIRE BY A WATCHMAN

An installation for storing liquid hydrocarbons consists of:

- a holding tank,
- a manually actuated installation for diffusing an emulsifier, installed at the periphery of the holdup tank,
- a firewall of degree 2h which protects a liquefied gas reservoir implanted nearby.

It is sought to estimate the confidence level of the task consisting of having a hydrocarbon fire extinguished by a watchman knowing that a round occurs every 1h30min. The goal is to prevent BLEVE of the liquefied gas reservoirs.

Independence	*The surveillance task is independent of any leak scenario*
Efficiency	*The itinerary of the round may be defined, a pool fire in the holding tank will be well visible provided that the itinerary of the round is observed, the extinguishing system is dimensioned in order to respond to the fire scenario.* *Educated and trained watchman.* *The extinction button remains well accessible and protected in the case of fire.*
Expected response time *Estimated response time*	*The maximum intervention delay is 2 hours (after this time the firewall is assumed to be inoperative).* *The response time integrates the time required for performing the round and starting up the extinction system. The watchman passes every 1h30min at the same place and starting the extinction means only takes a few minutes.* *The response time is of the same order as the kinetics of the accident*
CL	*<u>"Active" detection: the watchman has to go and seek the information by going to the edge of the tank</u>* *1. Detection of the fire during the surveillance round is clear (visual detection of flames and fumes).* *2. The round is the main task of the watchman and the periodicity of the round is defined as imperative (1h30min i.e. about 5 rounds per post). However the watchman is also assigned to other tasks: considering these general conditions and the work organization, it is considered that there exits a "moderate" risk of shifting or delaying the round (also having an impact on the regularity of the rounds)* *Partial conclusion: downrating by one level* *<u>Diagnostic and selection of the action:</u>* *1. The demonstration of the information to be processed is sufficiently explicit (the actual dangerous phenomenon) and is sufficient for diagnosing the problem.* 2. *The operator is aware of the significance of the event and masters the*

	instructions (starting the extinguishing system: this is for which he/she is trained). *Partial conclusion: no downrating.* *<u>Safety action:</u>* 1. *The response time is slightly below (about 1h35min) the expected maximum response time (2hrs) which induces strong pressure (over time and related to the dangerous phenomenon which may be very developed)..* 2. *The task of applying the extinguishing operation does not have any complexity, the watchman is educated and regularly trained for this type of intervention.* *Partial conclusion:* ***The stress level produced by the lack of time notably justifies complete downrating of this barrier (-2).*** *<u>Activity involving several actors: inapplicable</u>* ***Estimated confidence level: 2 – 2 = 0***
Comments	*The industrialist has integrated into the round a mandatory point of passage as regards the intervention obligation with indication of the time of passage on a register. On the other hand, the work organization of the watchman was changed in order to reduce the other tasks which are assigned to him/her. Arrangements are made so that the watchman may have sufficient autonomy for making his/her round in priority in any situation. He/she is regularly reminded of the importance of observing the periodicity of the round. The work group estimates that considering the whole of these arrangements, the availability and commitment of watchman is sufficient. CL may then be raised to 2.*

EXEMPLARY SHEET NO.4: FLOODING A REACTOR IN THE CASE OF A RUNAWAY REACTION

Description of the installations

A workshop of chemical syntheses on two floors is assumed:

The second floor is dedicated to preparing reagents before introducing them into the synthesis reactors. The tanks for preparing the reagents are used for the different synthesis reactors of the shop. Selecting the destination reactor is carried out by a set of valves. The device for flooding the reaction is located at this floor.

The first floor receives the synthesis reactors (4 in number).

The ground floor is assigned to storing the reaction products in drums.

The whole of the transfers between the floors are carried out by gravity.

A typical synthesis reactor is equipped for operation:

- with a stirrer driven by an electric motor,
- with a separate heating device,
- with a separate cooling device,
- with measurement of temperature,
- with measurement of pressure.

A typical synthesis reactor is equipped for safety:

- with measurement of temperature,
- with measurement of pressure,
- with a device for flooding the reactor (a tank filled with a sufficient amount of water for stopping thermal runaway). This tank is equipped at the bottom with the valve for opening the circuit towards the reactor,
- with a rupture disc allowing reaction gases to be sent into the chimney

Note: This relatively succinct description, corresponds to a pedagogical case and as such does not discuss the whole of the devices capable of being encountered on an industrial reactor.

Description of the synthesis operations

After having loaded and started heating of the reactor, the assignment of the operator is:

- to conduct and monitor progression of the synthesis according to conditions defined in the process sheet,
- to stop the synthesis and pour the reaction products towards the filling of drums.

Conducting the synthesis operations is provided by a posted operator. The shop operates 24hrs a day. An operator performs between 150 and 200 syntheses a year. The shop includes four synthesis reactors which may be operated at the same time.

Human safety barrier towards the scenario of reaction runaway:

The operator should proceed with flooding the reaction upon reaching:

- a temperature rise rate threshold of 1°C/min,
- a high temperature threshold,
- a high pressure threshold.

For the purposes of this example, two cases of conducting synthesis will be investigated:

- Conducting and monitoring the synthesis by reading temperature and pressure sensors on the reactor. For reading the temperature, the operator has a screen with which he may view the temperature curve versus time,
- Conducting and monitoring the synthesis by means of a supervision system transferred to the control room. The different representation modes required for tracking the reactions are transferred onto a specific screen.

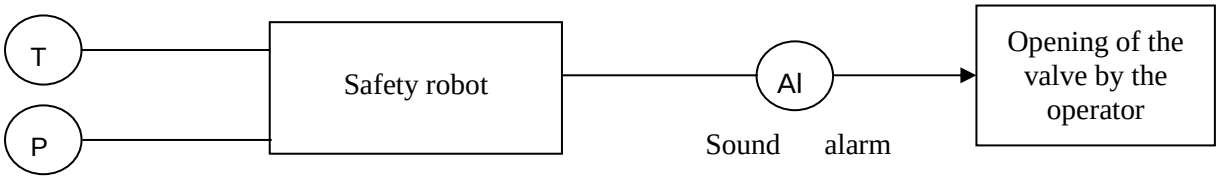
<u>Investigation of case 1: Conducting and monitoring by the operator</u>

Independence	*OK – Monitoring the progression of the synthesis is identified as a specific task independent of the accident scenario.*
Efficiency	*The system for flooding the reaction may be considered as a system with a well-proven concept (widely distributed in the chemical industry). The valve with which it may be actuated is accessible to the operator and maneuverable.* *The volume of water was determined for the reaction medium (calculation note).* *The personnel is educated and trained. Exercises are performed by telling them that the reactor is in a runaway condition and asking them to react to the problem. The completed training is not optimum and was not able to show the difficulty in diagnosing the accidental situation. This training does not allow the reality of the accidental situation to be taken into account such at as it would occur. Conservatively, it may be considered that this is sufficient for canceling the confidence level of the barrier.*
Expected response time	*The maximum intervention delay is supposed to be equal to 10 minutes (depends on the runaway kinetics).*

Estimated response time	*The response time integrates the time required for detecting the accidental situation (calculation of the temperature rise rate and possibly confirmation) + the time required for opening the circuit for emptying the water into the reactor knowing that the valve is located upstairs. As the second floor is dedicated to the preparation of the reagents, access to the valve risks being difficult because of the presence of drums or bags or raw materials. Further, it should be noted that the operator may be led to moving temporarily away (a time which may be estimated with difficulty). The response time does not seem to be optimum, of the order to 6 minutes with optimistic assumptions.*
CL	*"Active detection": the operator has to consult available indicators giving the parameters of the process* 1. *The information is provided either by the indicators, or by a temperature rise curve. Reading the information is easy (legible indicators and curve).* 2. *The operator is supposed to be close to the reactor during the risky phase but may be led to moving temporarily away from it. In this case, there is no anticipated alarm. The availability of the operator is not optimum.* *Partial conclusion: the work group estimated a downrating by one level (**-1**) relatively to the unavailability of the operator (possibility of other risky phases on several reactors at the same time).* *Diagnostic and selection of the action:* 1. *Early detection of reaction runway requires determination of a temperature rise rate. This information is not directly available and results from a calculation or an extrapolation on a curve for which the scale does not necessarily show the sensitivity adapted to the detection threshold (for example: time division: 1 minute, temperature division: 5°C). The task of determining by a calculation the temperature rise rate may lead to errors and therefore requires at least one confirmation.* 2. *Easy selection of an action – The operator is aware of the significance of such a rise in temperature and masters the instructions (opening the flooding system). He/she is perfectly aware that any cooling attempt other than flooding would not be sufficiently fast.* *Partial conclusion: The difficulty in processing the information justifies complete downrating of this barrier (**-2**).* *Safety action:* 1. *The response time is at least 6 min (provided that the operator is present) while the maximum intervention delay is 10 min: there is a non-negligible time pressure and stress level.* 2. *The task for opening the valve of the flooding system does not have any complexity and the valve is easy to maneuver (quarter turn valve)* *Partial conclusion: the optimistic response time of the order of 6 minutes (provided that the operator is present) is to be compared with the expected response time of 10 minutes. This response time alone also justifies complete downrating of this barrier all the more so since this is an optimistic response time (**-2**).* *Activity involving several actors: inapplicable* ***Estimated confidence level : 0***

Investigation of case 2: Conducting an monitoring the synthesis via a supervision system

In this case, the safety barrier may be described by the following diagram.



Upon reaching a safety threshold (temperature or pressure) a sound alarm is set off in the shop and information on the accidental situation is indicated on the monitoring screen (see hereafter).

In a first phase, the human component of this barrier is investigated in detail. Next the technical components are described in order to estimate the overall confidence level of the barrier.

Human component:

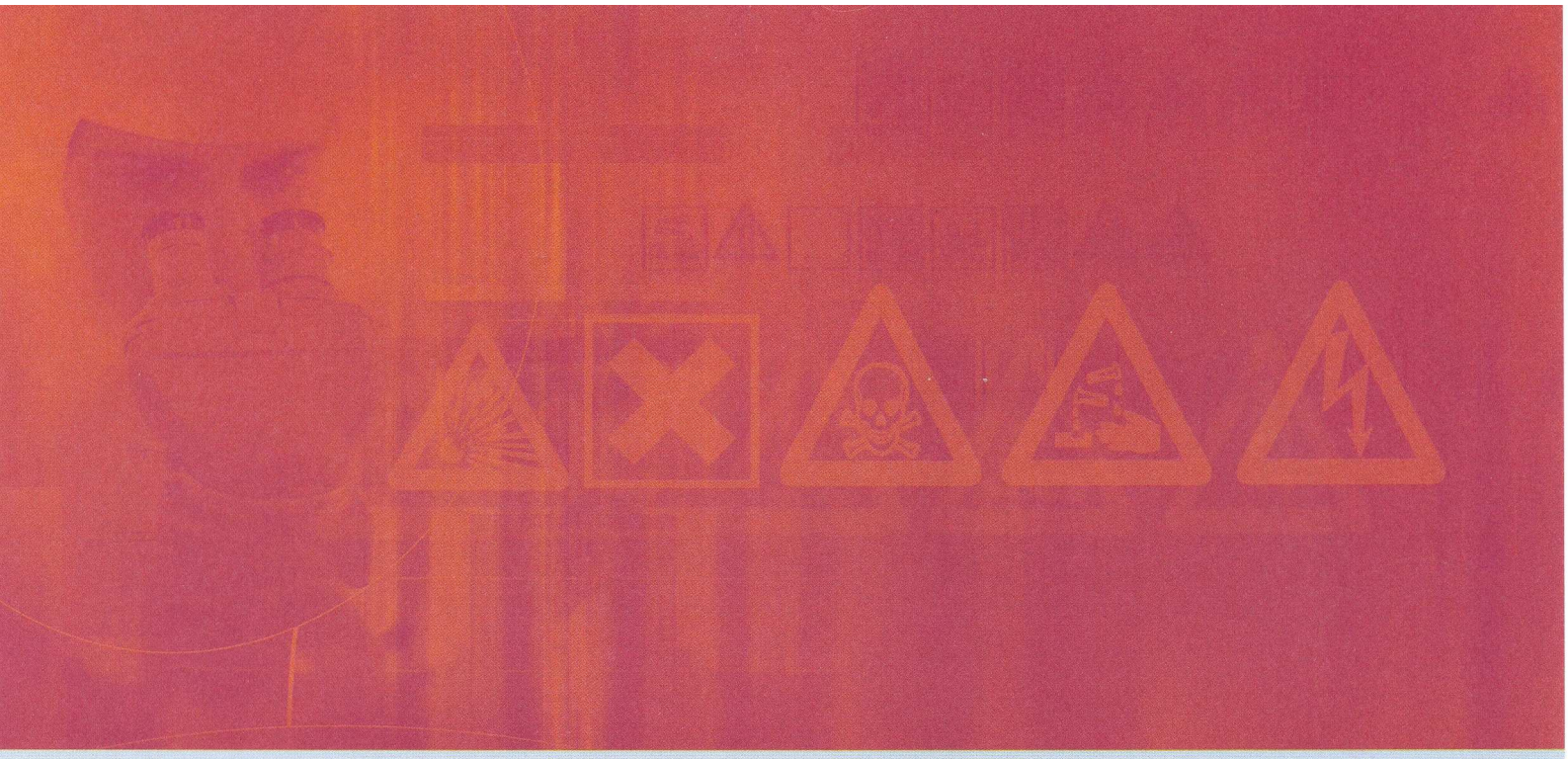
Independence	*OK – Monitoring the progression of the synthesis is identified as a specific task independent of the accident scenario. This monitoring is carried out in a control room.*
Efficiency	*The system for flooding the reaction may be considered as a system with a well-proven concept (widely distributed in the chemical industry). The volume of water was determined for the reaction medium (calculation note). The valve with which it may be actuated is accessible to the operator and maneuverable.* *The sound alarm is clearly audible in the whole shop.* *The personnel is educated and trained. Exercises are carried out by informing them of the actuated alarm and asking them to diagnose and react to the problem. With this training, it is possible a priori to take into account the reality of the accidental situation as it would occur.*
Expected response time *Estimated response time*	*The maximum intervention delay is supposed to be equal to 10 minutes (depends on the runaway kinetics).* *The response time corresponds to the time required for identifying the alarm and opening the circuit for emptying the water into the reactor, being aware that the valve is located upstairs. In the case when the operator has moved away from the monitoring station, given that the alarm is a sound alarm, the reaction time of the operator is limited to the time for returning to the station (about 2 minutes): the operator may easily interrupt the activities for which he/she is responsible. As the second floor is dedicated to preparing the reagents, access to the valve risks being difficult because of the presence of drums or bags of raw materials (about 3 minutes). The maximum response time may be estimated to be 5 minutes.*

CL	*<u>"Passive" detection (alarm):</u>* *1. The information is clearly identifiable: The monitoring screen reports the crossing of the thresholds (indication of the relevant reactor and the reached safety threshold – use of display code with which this information may be highlighted), and a sound alarm is retransmitted in the shop, therefore detection is obvious.* *2. The operator is normally in the control room during the risky phase but he may be led to move away temporarily from there. In this case, a sound alarm (broadcasted in the whole shop) is provided and he/she abandons any other current activity.* *Partial conclusion: no downrating* *<u>Diagnostic and selection of the action:</u>* *1. The information is sufficient and explicit: the task for determining the temperature rise rate by a calculation is automated.* *2. Easy selection of action –The operator is aware of the significance of the alarm and masters the instructions (opening the flooding system). He/she is perfectly aware that any cooling attempt other than flooding will not be quick enough.* *Partial conclusion: no downrating.* *<u>Safety action:</u>* *1. The response time is at least 5 min (at most) while the maximum intervention delay is 10 min: the situation may prove to be quite stressing considering the response time and the distance to the valve to be actuated.* *2. The task of opening the valve of the flooding system does not have any complexity and the valve is easily maneuverable (quarter turn valve).* *Partial conclusion: The situation may prove to be stressing which justifies partial downrating of this barrier (**-1**).* *<u>Activity involving several actors:</u> inapplicable* ***Estimated confidence level: 1***

<u>Technical component</u>:

In this study case, it is supposed that the overall confidence level of the barrier will only be equal to 1 if the confidence level of each of the constitutive technical elements of the barrier (temperature and pressure sensor, safety robots, alarm, valve) is at least equal to 1.

In order to finally estimate the confidence level of the technical components (on a detailed case), the reader may usefully rely on the Ω 10 report [1].



INERIS

maîtriser le risque
pour un développement durable

Institut national de l'environnement industriel et des risques

Parc Technologique Alata
BP 2 - 60550 Verneuil-en-Halatte

Tél. : +33 (0)3 44 55 66 77 - Fax : +33 (0)3 44 55 66 99

E-mail : ineris@ineris.fr - **Internet :** http://www.ineris.fr