International Institute for
Applied Systems Analysis
Schlossplatz 1
A-2361 Laxenburg, Austria

Tel: +43 2236 807 342
Fax: +43 2236 71313
E-mail: publications@iiasa.ac.at
Web: www.iiasa.ac.at

Interim Report **IR-05-003**

Human Errors Analysis and Safety Management Systems in Hazardous Activities

Leva Maria Chiara, chiara.leva@polimi.it

Approved by

Aniello Amendola
Research Scholar, Risk, Modeling and Society

January, 2005

[**Click:** Type additional cover information or delete this text]

Contents

Abstract

The present report describes human error analysis as emerged from the Three Mile Island accident, that was a milestone in the development of studies on human factors; it then presents some methods to quantify and analyse the risks related to human error. A further case of analysis is examined, focusing on the importance of organizational-related factors, as the Root causes of operator-error at the sharp end of the accidents chain of events. Some of the most relevant managerial/organizational factors are discussed, following the classification that G.Drogaris (G.Drogaris 1993) derived from his analysis of the MARS database. The classification is then confronted with the aspects required by the Seveso II Directive for a Safety Management System. Finally the sixth chapter considers the way in which human factors are analyzed in the Safety Management System of an Italian Oil Refinery, and possible ways of placement and improvements of this process through a particular use of the Success Likelihood Index Methodology.

Acknowledgments

The Present Report has been written under the supervision of Aniello Amendola, whose teaching and guidance has been, and continues to be, very precious for the overall direction of my studies.

I would like to thank the Librarians in IIASA and Miss Helene Pankl for their technical support.

A special Thank to Cesare Marchetti for introducing me in some of his interesting points of view on science.

Thanks to the Risk, Modeling and Society Group for giving me hospitality during my staying in IIASA...I really felt like Alice in Wonderland.

Leva Maria.Chiara

About the Author

Maria Chiara Leva is currently enrolled in the PhD program in the Polytechnic University of Milan. She graduated with first class honours with distinction in Industrial Engineering at the University of Bologna, Italy. She also studied in the department of Industrial Engineering in the University of Limerick, Ireland during the fourth year of her program.

She worked on her final thesis in the International Institute for Applied System Analysis (IIASA) in Laxenburg, Austria studying Human Error Analysis in Industrial Accidents and Safety Management Systems, in relation to the EU Seveso II directive.

From February to October 2003, she worked in the department of Safety Engineering in the API Oil Refinery in Ancona, Italy, where she developed an Accident-Non Compliance database and related Performance indicators for the Safety Management System.

From June 2004, she spent four months at Westinghouse Electric Corp, Windsor, Connecticut, USA, where she conducted Human Reliability Analysis for the Probabilistic Risk Assessment at the design stage of a new Nuclear Power Plant. During this period she developed the preliminary HRA study in conjunction with the 2004 IRIS PRA Multidisciplinary Team.

The main research area of her PhD regards "Planning and management of human factors for transport systems safety" in collaboration with D'Appolonia spa.

Human Errors Analysis and Safety Management Systems in Hazardous Activities

Maria Chiara Leva*

Introduction

"Western civilization places a high value upon rationality, and this civilization is sustained, if not dominated, by clusters of organizations, large and small, which profess an intention to display this value by pursuing rational courses of action.

In such a society the occurrence of a disaster indicates that there has been a failure of the rational mode of thought and action which is being relied upon to control the world."
(Barry A. Turner 1978)

Examples of man-made disasters are the accident that occurred in the nuclear facility of Chernobyl in 1986, or the leakage of methyl isocianate that occurred in Bhopal in 1984 resulting in the death of more that 2500 people; or, more recently, the explosion in the chemical plant of Toulouse in September 2001.

The potential destructive capacity of some industrial activities can be compared to that of natural cataclysms, but cannot be "regarded as resulting from some external and unfathomable force which could not be directly controlled but only accepted"(B.Turner 1978) .

The responsibility of controlling the potential hazards of a production-related activity is shared by the company that performs the activity and the regulatory authority under whose jurisdiction the activity is being performed. The consequences of a major accident can affect a wide area. It is often necessary to have a cooperative approach both in the industrial sector (the Bhopal accident was followed by a period of crisis in the chemical industry) and in the regulatory field. This has been the subject of the European Directive EEC/501/82A) which defines a 'Major accident', as:

"An occurrence such as a major emission, fire or explosion resulting from uncontrolled developments in the course of an industrial activity, leading to a serious danger to man, immediate or delayed, inside or outside the establishment, and/or to environment, and involving one or more dangerous substances".

The approval of the Major Accident Hazard Directive took place some years after the Seveso Accident and 8 years after the Flixborough accident "which was the spark starting discussion about a European common approach to industrial major accidents" (K. Rasmussen 1996).

The Directive was amended twice in 1987 and 1988 to incorporate lessons from two accidents: Bhopal (1984) and Basle (1986). Eventually in 1996 a new Directive (96/82/EC the so called Seveso II) was introduced, demanding in addition to previous requirements for

* Polytechnic University of Milan, Piazza Leonardo da Vinci 32, 20133 Milano, Italy, chiara.leva@polimi.it

- land use planning and control to decrease vulnerability of target environment
- and, safety management systems (SMS) in the industry to decrease hazard from the source.

The need for SMS derived from the analysis carried out through the use of accident data which highlight that the root causes of most accidents are due to human and organizational factors. The data base MARS (Major accident Reporting System) has been established at the Joint Research Center of the European Union in Ispra (Italy), and it contains all the Major Accidents notified by the EU Member Countries.

According to the analysis carried out on the accidents in MARS, management inadequacies are a significant causative factor in over 90% of the accident in the European Union since 1982. In the accident reports for which the root cause was attributed to management factors, a human/operator error was stated to be the actual immediate cause.

This finding confirms results anticipated by B Turner and from subsequent empirical studies like those of Trevor Kletz (T.Kletz 2001).

A safety management system is, according to the definition of the OHSAS 18001 (1999):

" part of the overall management system that facilitates the management of the Occupational Health and Safety risks associated with the business of the organization.

This includes the organizational structure, planning activities, responsibilities, practices, procedures, processes and resources for developing, implementing, achieving, reviewing and maintaining the organization's Occupational Health and Safety policy".(OHSAS 18001 1999)

In the context of the Seveso II Directive the definition of a Safety management system is strictly connected with that of safety policy in fact a SMS is the organizational structure, responsibilities, procedures and resources for implementing the safety policy (C.Kirchsteiger et al 1998) and its are defined as:

"(a) the major accident prevention policy should be established in writing and should include the operator's overall aims and principles of action with respect to the control of major-accident-hazards;

(b) the safety management system should include the part of the general management system which includes the organizational structure, responsibilities, practices, procedures, processes and resources for determining and implementing the major-accident prevention policy;

(c) the following issues shall be addressed by the safety management system:

(i) organization and personnel - the roles and responsibilities of personnel involved in the management of major hazards at all levels in the organization. The identification of training needs of such personnel and the provision of the training so identified. The involvement of employees and, where appropriate, subcontractors;

(ii) identification and evaluation of major hazards - adoption and implementation of procedures for systematically identifying major hazards arising from normal and abnormal operation and the assessment of their likelihood and severity;

(iii) operational control - adoption and implementation of procedures and instructions for safe operation, including maintenance, of plant, processes, equipment and temporary stoppages;

(iv) management of change - adoption and implementation of procedures for planning modifications to, or the design of new installations, processes or storage facilities;

(v) planning for emergencies - adoption and implementation of procedures to identify foreseeable emergencies by systematic analysis and to prepare, test and review emergency plans to respond to such emergencies;

(vi) monitoring performance - adoption and implementation of procedures for the ongoing assessment of compliance with the objectives set by the operator's major-accident prevention policy and safety management system, and the mechanisms for investigation and taking corrective action in case of non-compliance. The procedures should cover the operator's system for reporting major accidents of near misses, particularly those involving failure of protective measures, and their investigation and follow-up on the basis of lessons learnt;

(vii) audit and review - adoption and implementation of procedures for periodic systematic assessment of the major-accident prevention policy and the effectiveness and suitability of the safety management system; the documented review of performance of the policy and safety management system and its updating by senior management."

The present report describes human error analysis as emerged from the Three Mile Island accident, that was a milestone in the development of studies on human factors; it then presents some methods to quantify and analyse the risks related to human error. A further case of analysis is examined, focusing on the importance of organizational-related factors, as the Root causes of operator-error at the sharp end of the accidents chain of events. Some of the most relevant managerial/organizational factors are discussed, following the classification that G.Drogaris (G.Drogaris 1993) derived from his analysis of the MARS database. The classification is then confronted with the aspects required by the Seveso II Directive for a Safety Management System. Finally the sixth chapter considers the way in which human factors are analyzed in the Safety Management System of an Italian Oil Refinery, and possible ways of placement and improvements of this process through the use of the Success Likelihood Index Methodology.

1. THREE MILE ISLAND ACCIDENT AND HUMAN FACTORS.

> *"Since the accident in 1979 at the Three Mile Island Unit 2 plant, the nuclear industry and the NCR (Nuclear Regulatory Commission) have become acutely aware of the fact already established in many industries, that human error in some form is responsible for a large proportion of accidents and is a challenge to system safety and productivity" (The national Academy of Sciences 1988).*

The analysis of human factors and their connection with safety management in this paper will begin with a practical example: The Three Mile Island Accident. The analysis of this case brought great changes in dealing with human performance problems especially in the nuclear field. The Institute for Nuclear Power Operations and the National Academy for Nuclear Training were established in the years following the accident. The chain of events that lead to the occurrence, the improvements and the actions suggested in the investigation of the accident on behalf of the President of the United States (Kemeny 1979) covered several aspects. However the most crucial were the human related ones.

.

1.1 ACCIDENT DESCRIPTION.

On the 28 of March 1979, at about 4:00 am, a choke occurred in a resin polisher unit used to filter the secondary water. In order to clean the choke the operators used instrument air. The instrument air turned out to be at a lower pressure, and hence water got into the instrument air lines. The amount of water supplied to the steam generator drastically diminished and the main feed water pumps stopped running. Within seconds the turbine tripped and the reactor automatically shut down; the control rods, which absorb neutrons, dropped down into the core and stopped the fission chain. The production of heat still continued due to radioactive decay. The reactor coolant pumps continued feeding the primary circuit, but no heat could be removed by the secondary system. In fact, no addition water could be supplied to the secondary system, since the emergency feedwater system had been tested 2 hours before the accident and several valves were mistakenly left closed. Only 8 minutes after the beginning of the accident, they were discovered closed and reopened

The primary water then started boiling and a power operated relief valve (PORV) opened, allowing the steam to be discharged to the quench tank, while the make-up pumps started automatically to replace the water that had evaporated in the primary circuit. After the water pressure dropped below the set point for closure, the valve did not act as expected and stuck open. The light indicator on the operator panel was activated by the signal given to the valve and not by its actual position, so that the operator thought the valve was shut.

The stuck-open valve caused the pressure to continue to decrease in the system, and some voids began to form in the circuit. This resulted in the system water being redistributed in such a way that the pressurizer (a tank that controls the pressure) became full of water. This in turn allowed the level indicator to point to the operators that the circuit was full of water. They therefore shut down the make-up water pumps, preoccupied with avoiding damages due to potential excessive vibration.

Within two or three hours the damage to the reactor occurred: a significant amount of fuel melt, and the radioactivity in the reactor coolant increased. After the accident the water in the

primary circuit began to carry fuel debris that escaped from the reactor coolant system and flowed to the floor beneath the containment. Eventually, the cause of the incident was understood and water was added to the reactor cooling system and the reactor was allowed to cool down.

The environmental and radiological consequences of the accident were minor, thanks also to the swift emergency response, and no deaths or injuries, or significant levels of contamination outside the plant occurred.

1.1.1 HUMAN AND MANAGEMENT FACTORS ANALYSIS

Going through the accident description it is clear that if the operators had kept the emergency cooling system on in the early phase of the accident, the melt down in the core wouldn't have occurred. So the accident could be labeled as due to 'operator/human error'.

But there are other factors that need to be taken into account:

1) The operators lack of proper training:
   At TMI only two hours per year were dedicated to training for operators on operational problems and from experiences at other reactor plants (lessons learned form other accidents).
   The training, nevertheless, might have been adequate for the normal operation of the plant but it did not provide an understanding of the plant phenomena, which could have enabled them to deal with problematic circumstances. In fact, for instance, they were not able to recognize the relationship between the temperature and pressure of the water in the primary circuit, and to understand it was boiling. The training should prepare operators of hazardous activities as problem solvers, since it is not possible to "foresee everything that will go wrong and write instructions accordingly" (T. Kletz 2001).

   In order to convey more experience and well informed diagnosis skills, training should have included real simulated emergency situations and up-to date preparation.
2) The emergency feedwater system, at the start of the chain of events, was unable to function. As part of maintenance procedures the feedwater system has to be tested and the valves that connects it to the main system has to be closed and then reopened. But in this case either because of operator slips of attention and for an administrative lack of supervision, the valves were not reopened. The human performance problems related to maintenance and work-permit procedures will be discussed in chapter 3.
3) The emergency response and the safety procedures at the TMI plant, and in many other nuclear facilities, were developed mainly with the intention of meeting the requirement of the legislation. So as the emergency procedures and design were concentrated on major occurrences such as a LOCA (Loss of Coolant Accident) because of a large break in the primary system or a LOECC (Loss of Emergency Core Cooling), which do not allow time for significant operator intervention, they ignored the possibility of a slowly developing small-break accident. The same type of accident has been even pointed out in a memorandum written 13 months before the occurrence of TMI, by a senior engineer of the Babcock & Wilcox Company (suppliers of the nuclear steam system): warning ignored!.
4) As pointed out by the Report of the President' Commission (Kemeny 1979), the control room, in which the supervision of the operations of the TMI unit 2 plant was performed, lacked an ergonomics human-machine interface:

- The light indicators of the PORV valve were not connected to the actual position of the valve, and this provided false information to the operators, leading them to think that the valve was closed while it was stuck open.
- The control panel was huge, with hundreds of alarms. During the first minutes of the accident, more than 100 alarms were sounding, and it was not possible to suppress the less important ones in order to let the operators focus on the main issues.
- Some key indicators were placed in unsuitable locations. The operator could not even see them, in normal conditions.
- The information was not presented in a clear and, as much as possible, plain form. For instance, even if the pressure and temperature of the reactor coolant were shown, there was no indication that the combination of the two meant that the water was turning into steam.

Few and relatively inexpensive improvements in the control room could have significantly facilitated the management of the accident. Human factors design is a vital aspect of safety operation of a Nuclear Power Plant, Since the TMI accident existing operational and near-operational power plant control rooms has been revised from the human factors standpoint.

5) Another factor that was found to have some implication was the way the shifts of the operators were organized. Long-duty periods or sleep losses reduce the mental and physical capacity of even the best-trained operator. The HSE (5) has recently developed a tool for assessing short-term daily fatigue or cumulative fatigue over a shift cycle. The tool consists of an index based on five factors (shift start time, shift duration, rest periods, breaks and the number of consecutive shifts). In order to avoid the effect of fatigue the shifts and the turns should be carefully planned, the use of an index to assess their implications is advisable. Furthermore there are strategies, or ergonomic devices, that can be used for incrementing operator alertness. These include physical activity, light therapy with a high-intensity light box, planned naps etc. The safest means is however a wise schedule for the shifts.

This analysis demonstrates that root causes of the accident were to find in a complex of factors that were linked to faulty management factors in design, licensing and operation of the plant.

1.2 HUMAN FACTORS TAXONOMY

1.2.1 THE BASE

"The health and safety Executive's Accident prevention advisory unit and others have shown that human error is a major contributory cause to 90% of accidents, 70% of which could have been prevented by management actions" ("Improving compliance with safety procedures" Human Factor Reliability Group)

If 90% of the causes of accidents are under the same umbrella of "human error" that means that under this voice are grouped different aspects and different items.
The use of a sound classification can be useful to better specify our object of study and to direct towards methods of prevention.
Unfortunately in the field we are approaching there is no universally agreed classification system, hence the taxonomy we would like to adopt must be made for our

specific purpose: studying how human errors contribute to the industrial framework, as part of the organizational failures that lead to major accidents.

Unsafe acts in an accident cause-chain that are mainly responsible for the final outcome are rooted in the organizational environment; on this we focus our attention.

A useful starting point is the description of cognitive control mechanism errors made by Jens Rasmussen.
Rasmussen's model was primarily directed at analysing errors made by those in supervisory control of industrial installations, particularly during emergencies in hazardous process plants.
The Skill-rule-knowledge structure is derived from a study conducted on operators working on localizing breakdowns throughout electronic devices (Rasmussen &Jensen 1974).

•Human performance at the skill-based level is characterized by models of well-known instructions and those that could be seen as "analogical structures in a space-time domain".
•The rule-based level is characteristic of performance related to familiar problems, whose solutions are rules with an if-then structure. It is part of the training and preparation baggage of the operator, formalized usually in procedures.
•The knowledge-based level is related to new situations, in which a complex interaction between the human "bounded rationality"(H.Simon 1956) and the new reality is required, without the help of structured and available models or rules.
In the study developed by Rasmussen there are eight steps in the heuristic proceeding of problem solution:
- activation
- observation
- identification
- interpretation
- evaluation
- goal selection
- procedure selection
- activation

These steps, in real decision processes, are not sequential. There are several patterns that can be built up with the elements of this list. The general frame for a Knowledge-based pattern, for instance, is a rule-based model (whenever it's possible human tends to recur to known rules).

The three main kinds of errors related to these performance levels can be (Reason 1998):

Performance level	**Error type**
Skill-based level	slips and lapses
Rule-based level	RB mistakes
Knowledge-based level	KB mistakes

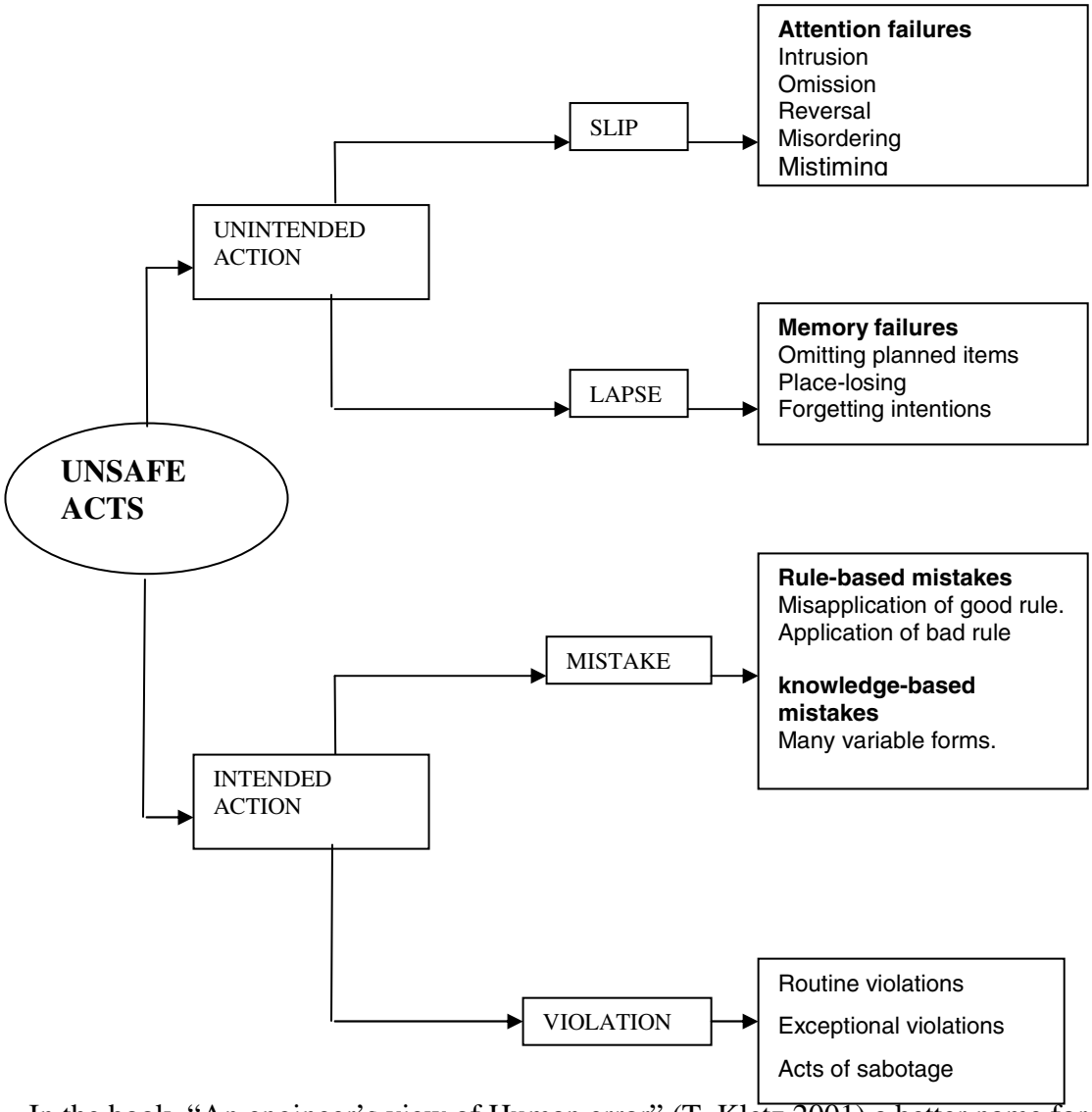
- **Slips and Lapses** are considered a momentary lack of attention. The operator knows what to do and how to do it but the task is in any event not carried out. Routine tasks are monitored by the lower levels of the brain and are not continually controlled by the conscious mind. (Reason and Mycielska 1982).

- **Rule-based mistakes (RB mistakes)** can be defined in relation to the if-then structure. It can happen that the diagnosis of the situation is wrong (if clause), even if the situation had been foreseen by the procedures or by the human/machine interface. So the rule applied is not appropriate or it can happen that even if the diagnosis of the situation is right the wrong rule is applied (then clause).

- **Knowledge-based mistakes (KB mistakes)** are typical of those situations in which the person involved in a problem solving condition has no stored problem-solving routines to apply. Hence s/he is obliged to try to build up a model for the reality s/he has to cope with, referring to his personal knowledge background and his ability to analyse problems.

Furthermore slips and lapses generally precede the problem detection while RB and KB mistakes occur in the trials that follow the detection of a problem.
The human mind-control that can be used for each kind of error also differs: As pointed out by Rasmussen at the skill-based level "performance is based on feed-forward control and depends upon a very flexible and efficient dynamic internal world model"; at the Rule-based level "performance is goal-oriented, but structured by the feed-forward control through a stored rule. Very often the goal is not even explicitly formulated, but is found implicitly in the situation releasing the stored rules….The control evolves by the survival of the fittest rule".
The only level at which a feedback control exists is the Knowledge-based level. The action in this case is lead by a local goal, every local achievement must be verified and the action must be corrected if not appropriate (error-driven methodology).

A further development adopted in our classification is the step highlighted by Reason in his book "Human error":
"Errors involve two distinct kinds of "straying": the unwitting deviation of action from intention (slips and lapses) and the departure of planned actions from some satisfactory path towards a desired goal (mistakes). But this error classification, restricted as it is to individual information processing, offers only a partial account of the possible varieties of aberrant behaviour. What is missing is a further level of analysis acknowledging that for the most part, humans do not plan and execute their actions in isolation, but within a regulated social milieu. While errors may be defined in relation to the cognitive processes of the individual, violations can only be described with regard to a social context in which behaviour is governed by operating procedures, codes of practice, rules and the like. For our purposes, **violations** can be defined as deliberate-but not necessary reprehensible- deviations from those practices deemed necessary (by designers, managers and regulatory agencies), to maintain the safe operation of a potentially hazardous system…
…An unsafe act is more than just an error or a violation- it is an error or a violation committed in the presence of a potential hazard: some mass (Tokaimura), energy (Chernobyl),or toxicity (Bhopal) that, if not properly controlled, could cause injury or damage."
The scheme number 1 reproduces Reason's classification (Reason 1990):
Scheme 1: Reason classification



In the book "An engineer's view of Human error" (T. Kletz 2001) a better name for violations that is to say non-compliance, is proposed, because violations can be seen as errors that occur when "someone knows what to do but decides not to do it" and most of the time "the person concerned genuinely believes that a departure from the rules, or the usual practice is justified"(see the case study of the Tokaimura accident).

There is a fifth kind of error that Kletz proposes in his classification: **mismatches**, that is to say "errors that occur because the task is beyond the physical or the mental ability of the person asked to do it, often beyond anyone's ability".

Among the knowledge based mistakes it is worth noting a particular category highlighted by J. Reason: the so called "**fixation**". This kind of attitude is the obstinacy to continue to act according to a familiar pattern or a first diagnosis chosen, without considering new aspects of the problem or new signs coming from the evolution of the problem under analysis. This is a normal human attitude, and the only way to make it less likely to determine bed outcomes is to warned the operators of this possible "trick" and to provide a very good training using simulators.

2 METHODS FOR HUMAN RELIABILITY ASSESSMENT

2.1 STARTING IN "MEDIAS RES".

Human Reliability is defined as "the probability that a human correctly performs an assigned task at the specified time, within the specified time duration, and in the specified environment".(LaSala 1998))

This definition is very similar to the most widely accepted definition of reliability that is mainly used for technical equipment:

"Reliability is the probability that a system will perform satisfactorily in a specified interval of time(t, t+ Δt) when used under stated conditions and supposing it was not broken in t "(Von Alven 1965). Reliability is used for not repairable components and it is characterized by the failure rate η, $\eta(t)*\Delta t$ expresses the probability that the components will have a failure in [t, t+ Δt] , if it was in perfect conditions in t.

In the paper "Mathematical Characterization of Human Reliability for Multi-task system operations" by R.E. Giuntini(Giuntini 2000), in fact, the method applied to quantify human reliability is analogous to that used for esteeming hardware reliability.

A Reliability function is a curve that relates the frequency with failures that occur in a time period R(t). It can be derived from the probability density function f(t) for errors:

$$F(t) = \int_{t=t0}^{t=tm} f(t)dt \quad \text{and} \quad R(t) = 1 - F(t) \rightarrow R(t) = 1 - \int_{t=t0}^{t=tm} f(t)dt$$

The probability density function for the error rate of hardware equipment, is normally expressed by the Weibull probability distribution:

$$f(t) = (\beta/\eta)(t/\eta)^{\beta-1} e^{-(t/\eta)}$$

where η is the characteristic life and β is the shape or slope parameter.(Abernethy 1983)

The Weibull probability distribution is used for describing the pattern of the error rate illustrated by the 'bathtub' curve for hardware reliability analysis. In the paper mentioned above the same curve is applied for describing a human error rate.

The three phases of the curve are:

1) the learning phase: during this phase the rate at which human errors occur decrease with time: "as the operator learns the task, there is less likelihood that errors will occur "(Giuntini 2000)
2) the stabilized error phase: the operator has learned the task and human error rate will be constant(same likelihood of occurrence during the phase).
3) fatigue phase: the error rate increased with time due to operator fatigue, lack of motivation, etc.

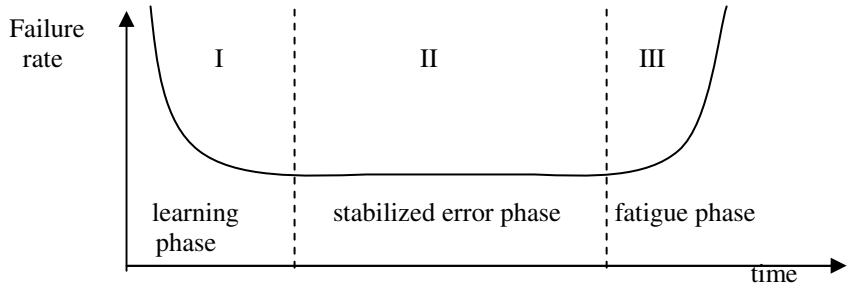


Figure 2.1 Combined error rate curve

This is just one example, it is worth noting that the central part of the assumed bath-tube curve is obtained from $\beta=1$ which leads to $f(t)= (1/\eta)\, e^{-(t/\eta)}$, consequently the human reliability assumes the value of $R(t)= e^{-(t/\eta)}$, that is the typical form of the R-function of a component in the stabilized error phase. This model can be mainly applied for modeling the skill-based performance level, on the base of this correspondence.

This is just one example of the several models that have been proposed in more than 50 years for evaluating human performance reliability.

There is no unique way of approaching and for evaluating human error, in this report the attention will be focused only on two methods:

- THERP (Technique for Human Error Rate Prediction)
- SLIM (Success Likelihood Index Methodology)

Before going further in presenting human reliability assessment methods it is important to point out a common problem in the field: the data.

There are three aspects, in my opinion, that need to be taken into account:

1) Human errors, that have been presented as slips of action and lapses of memory in the previous chapter, are valuable for probability and statistical methods, because they are mainly beyond intention; while mistakes and violations are more difficult to evaluate because they are due to a certain degree of intention and "People intuitive inferences, probability assessment and prediction do not conform to the law of probability theory and statistics" as emerged in the study conducted by D. Kahneman, (D. Kahneman et al. 1982).
2) Much of the data available are 'highly application-specific' and not transferable tout-court to other applications, "it is not sufficient to say that the probability of error in reading an instrument is 5x10-3; it is necessary to specify the environmental conditions, the characteristics of the instruments, the personnel training etc.."(P.Vestrucci 1990).
3) The data collection presents, at the moment, some other difficulties regarding the establishment and the maintenance of a database. "Data repertories have been established several times, but some have not been maintained" (K.LaSala 1998).

In general, human reliability data can be divided into three main categories:

- data obtained from historical statistics
- data obtained from laboratory simulations

- data obtained from the judgment of experts.

The data used in the two human reliability assessment methods we are going to analyse are: data from historical statistics and laboratory simulations for THERP, and data obtained from the judgment of experts for SLIM.

2.2 THERP

Therp (Technique for Human Error Rate Prediction) is the most widely used and recognised model for human reliability assessment.

It was developed in 1964 by Swain (A.D. Swain 1964), Its object is ”to predict human error probabilities and to evaluate the degradation of a man-machine system likely to be caused by human errors, alone or in connection with equipment functioning, operational procedures, and practices, or other system and human characteristics that influence system behaviour” (Swain and Guttman)(A.D. Swain H.E. Guttman 1983).

In this technique the operator error can be considered as an equipment failure, and the main analytical tool is the event tree.

The event tree is a logic structure that is used for identifying the possible events that can be originated from an initial situation. Every limb represents a point of a binary decision (the decision can only result to be correct otherwise incorrect, no other possibilities are available.).

The steps to follow in implementing a human reliability analysis using THERP are (J.Reason 1990):

a) identify the system functions that may be influenced by human error
b) list and analyse the related human operation (dividing the operations in simple tasks).
c) estimate the relevant error probabilities using a combination of expert judgment and available data for each task
d) estimate the effects of human error on the system failure events (integrating Human Reliability analysis with the wider Probability Risk Assessment).

At each limb of the tree (that is to say a task) is associated a specific value of HEP (Human Error Probability). There are some databases and tables from which it is possible to take the value for a nominal HEP (like in the table reported below that is taken from the “Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications”(Reason 1990).

In order to take into account the specific features of each case of analysis, it is necessary to modify the value of the nominal HEP by the use of Performance Shaping Factors (PSF). According to the judgment of the expert it is possible to choose a value of HEP in a range fixed by the upper and lower limits, that are respectively:

(nominal)HEP x EF

(nominal)HEP / EF

Where EF is Error Factor that is a value associated for each given HEP in the tables. The HEP is considered to be an average value in an interval where HEP x EF and HEP/ EF are the extremes.The HEP is incremented if the conditions are worse than the nominal conditions, and it is decremented otherwise.

ITEM	POTENTIAL ERRORS	HEP	EF
Making an error of selection in changing or restoring a locally operated valve when the valve to be manipulated is			
(1)	Clearly and unambiguously labelled, set apart from valves that are similar in all of the following: size and shape, state, and presence of tags	.001	3
(2)	Clearly and unambiguously labelled, part of a group of two or more valves that are similar in one of the following: size and shape, state, or presence of tags	.003	3
(3)	Unclearly or ambiguously labelled, set apart from valves that are similar in all of the following: size and shape, state, or presence of tags	.005	3
(4)	Unclearly or ambiguously labelled, part of a group of two or more valves that are similar in one of the following: size and shape, state, or presence of tags	.008	3
(5)	Unclearly or ambiguously labelled, part of a group of two or more valves that are similar in all of the following: size and shape, state, or presence of tags	.01	3

Table 2.2 Example of a THERP error data table (Swain and Guttman 1983)

When at each limb is the associated an HEP value and when the final event of the tree has been identified as a success event (S) or a failure event (F), the probability of each sequence of events is calculable by multiplying the values of the branches that are part of the sequence.

In the example below there is an event tree, branches labeled with lower case letters represent successful performance of an action. Branches labeled with capital letters represent failure of the same action.

Ps= a· b· c· d

Pe= A +a· B + a· b·C+ a· b· c·D

Pe+Ps+1

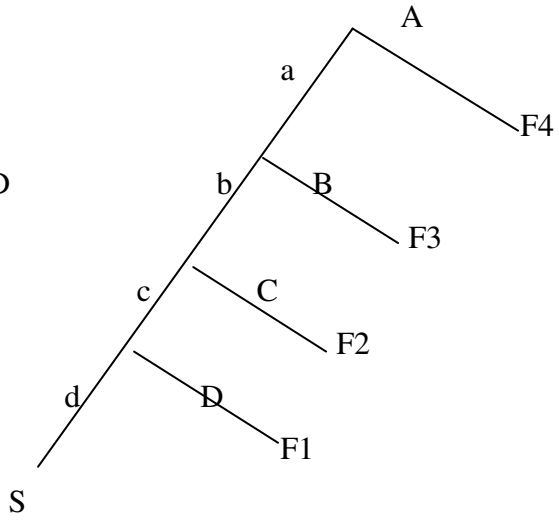


Fig 2.4: example of an event tree used in THERP

where Ps is the probability of success,

while Pe is the probability of error.

It is then possible to complete the analysis considering the possible recovery actions. It may be also done only for major sequences of events.

An example taken from P.Vestrucci (Vestrucci 1990) is reported in the figure below:

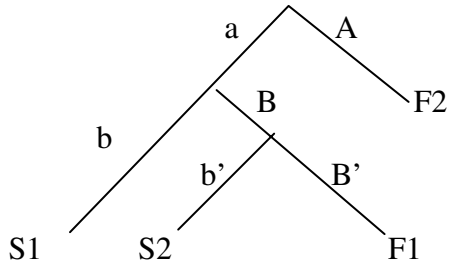


Fig 2.5 example of an event tree with multiple success paths

$$Ps = S1 \dashv S2 = ab \dashv aBb'$$

$$Pe = F1 \dashv F2 = A \dashv aBB'$$

Where
+aBb' is the effect of the recovery action on Ps
– aBb' is the effect of the recovery action on the Pe.

In the calculation the actions are considered independent from each other, this can lead to underestimation of the error probability.
In THERP the dependence is considered only for consequent actions. The dependence can be
- negative:
The error in A increases the probability of success in B, in other words

$b \mid A > b$,

$B \mid a > B$

then

$B \mid A < B$

$b \mid a < b$

- positive:
The success in A increases the probability of success in B.

$b \mid a > b$,

$B \mid A > B$

then

$B \mid a < B$

$b \mid A < b$

The degree of dependence can be chosen among five values:
ZD= Zero dependence
LD= low dependence
MD= medium dependence
HD= high dependence
CD= complete dependence

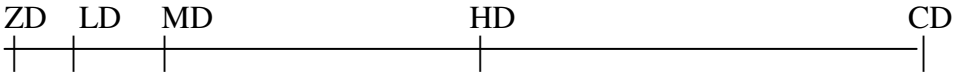


Fig 2.6: Dependency level scale.

For establishing the nature of possible dependencies, the suggestions by Swain and Guttman (9) may be useful:

- It is better to examine the influence of the error or of the success of the precedent action on the one that is under examination, without establishing a unique dependence level for all the actions of one task;
- In case of uncertainty is better to use the higher dependence degree;
- It is important to evaluate the time and space relationship between actions (the dependency increases for actions that are close in time and space);
- Evaluate the functional link between actions, if they are functionally linked the dependency is stronger;
- Stress increases dependency especially in operators with lack of experience or self confidence;
- Consider similarity in the personnel (operators with similar characteristics are more keen to interact with each others);
- In case the situation of analysis is the supervision of one operator by another operator it is important to consider the compound probability of error in case it is HEP is around 10^{-6}, because it is very unlikely for two operator's actions, to have an HEP < 10^{-5};

The following table (table 2.3) illustrates equations for calculating the probability of success Ps("N" |"M") for the action "N", considering the success in the previous action "M", where n is the basic probability of success for the action "N". The second table (table 2.4) refers to the probability of error Pe("N" |"M") for the action "N", considering the failure of the previous action "M", where N is the basic human error probability (BHEP) for the action "N".

Table 2.3: Dependency levels for success probability evaluation (P. Vestrucci 1990)

Dependency level	*equation*
ZD	Ps("N" |"M") = n
LD	Ps("N" |"M") = (1 +19n) / 20
MD	Ps("N" |"M") = (1+6n) / 7
HD	Ps("N" |"M") = (1+n) / 2
CD	Ps("N" |"M") = 1.0

Table 2.4: Dependency level for error probability (P.Vestrucci 1990)

Dependency level	*equation*
ZD	Pe("N" |"M") = N
LD	Pe("N" ("M") = (1 +19N) / 20
MD	Pe("N" ("M") = (1+6N) / 7
HD	Pe("N" ("M") = (1+N) / 2
CD	Pe("N" ("M") = 1.0

2.3 SLIM.

SLIM (Success Likelihood Index Methodology) is a method based on the structured expert judgment (Embrey et al. in 1984). This methodology "allows experts to generate models that connect error probabilities in a specific situation with the factors that influence the probability"(J. Reason 1990). These factors are the Performance Shaping Factors (PSF); while in THERP the PSF are used to adapt the situation to the general frames the data are referred to, in this case, they are the starting point of the method itself.

Following a description of the method (Vestrucci 1990), the steps into which this method can be divided are:

1) Constitution of the group of experts and first approach to the case of analysis.
2) Definition and selection of the Performance shaping factors for the case of analysis. (see table 2.5)
3) Assignment of weighting factors for each PSF
4) Scoring of each PSF
5) Calculation of the success likelihood index
6) Conversion of the SLI in HEP.

<table>
<tr><th colspan="2">External PSF</th><th>Internal PSF</th></tr>
<tr><td>Situation
• structure
• environment
• work period
• work shift
……</td><td>Task and tools
• perception
• motion
• compatibility
• prediction
……</td><td rowspan="3">• training
• experience
• skill
• personality
• intelligence
• motivation
• mentality
……</td></tr>
<tr><td colspan="2">Stressor</td></tr>
<tr><td>Mental
• abruptness
• duration
• work speed
• workload
……</td><td>Physiological
• duration
• fatigue
• discomfort
• hunger, thirst
……</td></tr>
</table>

Table 2.5: Examples of performance shaping factors

The PSFS have to be ordered in a list that starts with the most important one.
Once that the weight wi of the most important PSF is established, the others are fixed according to the first (if for instance the first is training and its weight is 100 and the second PSF is stress and its weight is 50, that means that the influence of the training is two times more important than the one of the stress in performing the task).
The weights are then normalized (every value is divided by the sum of all of them).
For each PSF a value ri, is then fixed that represents the specific condition of the case of analysis in relation to that feature (if for instance we are evaluating the PSF "knowledge of the system" and the case of the analysis present the operator at his first month of employment, with very little training and no precedence experience in the field, the ri,

would be probably be 0 or in any case very low, depending on the scale ($0 \leqq r_i \geqq 100$ etc..).
An example of the data that can be produced with these two steps is reported in the two tables below (table 2.6 and table 2.7).
Tables 2.6/2.7

PSF	Importance	Weight
Quality of information	100	0.50
Training	50	0.25
Available time	30	0.15
Procedure	20	0.10
Total	200	1.00

PSF	Weight	PSF score	weight×score
Quality of information	0.50	70	35.0
Training	0.25	20	5.0
Available time	0.15	10	1.5
Procedure	0.10	50	5.0
Total			46.5

The success Likelihood index is then calculated with the simple expression:

$$SLI = \sum_{i=1}^{N} w_i r_i$$

Where N is the number of PSFs considered (in the example above, they are 4).
The index SLI is already a valid instrument for supporting quantitatively a human reliability analysis, in connection with the managerial and organizational factors:
It is in fact, possible to evaluate the effects of modifying the r_i values, that mirror also organizational aspects, or to analyse the influence of every single PSF.
The SLI can be also used as a Performance Indicator, in order to monitor aspects of a safety management system (as proposed later on in the present report).
The last step of the method concerns the way by which is possible to obtain the value of Ps or Pe from the value of SLI.
The author of the method proposed two possible ways:

$$\ln(Ps) = a_1 \, SLI + b_1$$

$$\ln(Pe) = a_2 \, SLI + b_2$$

Where the constant have to be specified, calibrating the equation using some empirical data points (like in the example below, figure 2.7).

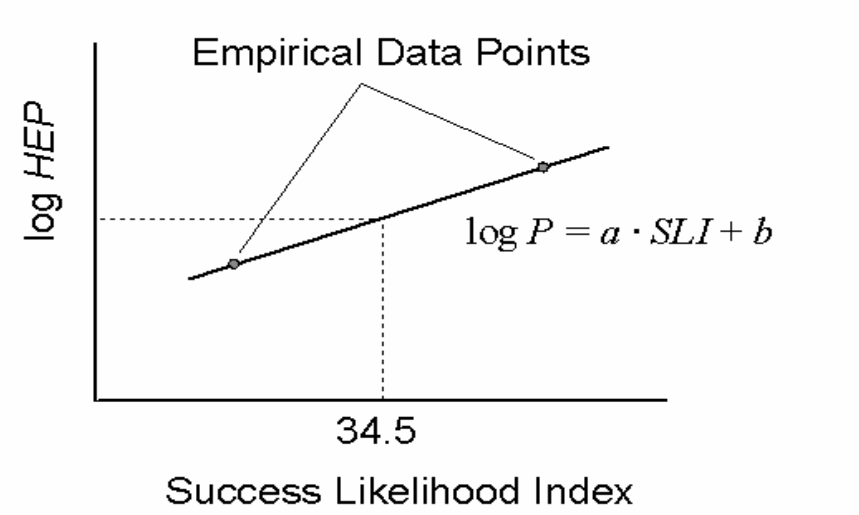


Fig 2.7: Success Likelihood Index and Human Error Probability

The method proposed for the conversion presents various problems, mainly due to its arbitrariness. For a further detailed analysis of the problems it is advisable to consult the (Vestrucci 1990), which illustrates another possible way of performing the conversion. However, within the scope of this report it is not interesting to examine the issue further because it will be only used the SLI Index, in order to perform a Human Reliability Analysis in our application to a practical case.

3. ANALYSIS OF THE TOKAIMURA ACCIDENT

The Tokaimura nuclear fuel processing plant is operated by JCO Company. In this facility uranium is re-processed, and supplied to fuel producers. The facility is one of medium-to-small-sized chemical plants, emplying 120 people.

The plant is located 120 KM northeast of Tokyo. Tokaimura is a large village in Ibaraki Prefecture, which is also close to the town of Nakamachi.
There are about 310,000 inhabitants within a 10 Km radius from the plant.

There are three conversion facilities at this site:

- one for low enriched uranium (enrichment of less than 5%),annual capacity 220 tonnes/year;
- one for low enriched uranium (less than 5%) with an annual capacity of 495 tonnes/year;
- one, in which the accident took place, in a conversion building at the western side of the site, for enriched uranium. The enriched uranium was processed either for the production of uranium oxide (U_3O_8) powder from uranium hexafluoride (UF_6), or for the production of uranium oxide powder from the scrap.

On the 30th of September 1999 a nuclear flash at the JCO Company's Tokaimura nuclear plant resulted in the deaths of two inexperienced workers.

The main function of the plant is to convert isotopically enriched Uranium hexafluoride into uranium dioxide fuel. This is one step in the process of making reactor fuel rods.

The uranium used in this process has been enriched to contain up to 5% of the fissile isotope ^{235}U (the ^{238}U is relatively inert).

The JCO plant occasionally purifies uranium to be made into fuel for an experimental fast-breeder reactor known as Joyo, which requires fuel enriched to 18,8% ^{235}U.
The enrichment of the fuel to the 18,8% of ^{235}U implied a higher probability of accumulating a critical mass that can lead to the triggering a chain reaction.
The Japan's Science and Technology Agency (STA) in licensing this nuclear facility in 1980 established regulations by which a mass limit of 2,4 kg was fixed on the amount of 18,8% enriched uranium that could be processed at one time at the JCO plant.
The procedure needed for purifying the uranium fuel for the Joyo facility licensed by STA was:

- small batches of uranium oxide U_3O_8 , in powder form, are put into a dissolving tank ,where it is mixed with nitritic acid to produce uranyl nitrate, $UO_2(NO_3)_2$.
- the uranyl nitrate solution is then transferred to a buffer tank (geometrically shaped in order to avoid criticality). The buffer tank attends a mixing function.
- from the buffer tank the solution is sent into a precipitation tank where is ammonium salt solution is added, to form a solid product ammonium diurinate $(NH_4)UO_7$.

Uranium oxide is extracted from the solid precipitate, and reprocessed in the dissolving tanks until the uranium oxide is sufficiently pure.

Then it is converted to uranyl nitrate, transferred to a storage container, and shipped to another facility where it is prepared and made into Joyo fuel.

JCO therefore needed to mix some high-purified enriched uranium oxide with nitric acid to form uranyl nitrate for shipping.

When the accident occurred, three technicians, had put about 2,4 Kg of uranium powder into a 10 litre stainless steel bucket with water and a specialized acid, for the last steps of the conversion process.

The procedure of homogenization to a uniform consistency was supposed to be controlled using a specially shaped narrow storage column tank on a one-batch basis.

In order to speed up the process, they mixed the oxide and nitric acid in stainless steel bucket rather than in the dissolving tank. This new way of operating followed instructions in the JCO operating manual which had not received STA approval. After the Licensing process in fact, no inspection or periodical audit was performed by the competent authority.

The chemical in the bucket was moved to a five-liter beaker through a filter and tipped into the precipitation tank with a funnel.

In doing so they skipped the solvent extraction column, the extraction-stripping column and the buffer column.

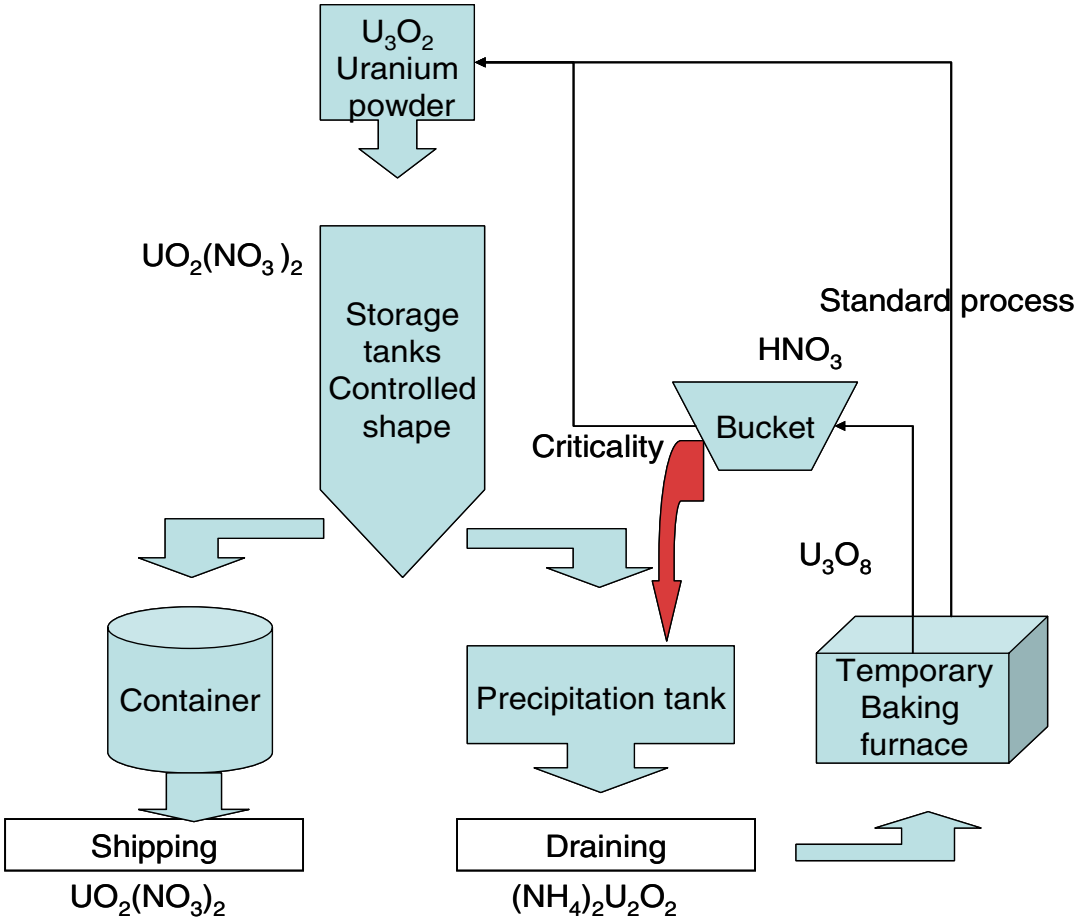


Fig 3.1: Simplified scheme of the process as it should have been and as it was actually followed (critical passage from the bucket to the precipitation tank : red arrow)

The total amount of enriched Uranium poured from the bucket directly into the precipitation tank was about 16,6 Kg (the precipitation tank was designed for 2,4 Kg of uranium per batch).

This caused the criticality:
At 10:30 a.m. the addition of the seventh bucket caused a self-sustaining chain reaction, the technicians saw a blue flash. The two technicians near the vessel began to experience pain, waves of nausea, difficulty in breathing, and problems with mobility and coherence.
The gamma radiation alarms activated immediately.
The blue flash was a result of the Cherenkov radiation that is emitted when nuclear fission ionizes air.

OPERATORS FACTORS AND ORGANIZATIONAL MEASURES.

1. The JCO had modified the procedure approved by the Japan's Science and Technology Agency (STA) for processing highly enriched Uranium, in order to speed up the production and the workers were following this "unlicensed procedure". In Japan, periodic inspection during operation seems not to be a legal requirement for facilities of this type.
2. On the other hand the competent authority never performed any periodic inspection on the facility.
3. The procedures used were completely different from the one specified for the equipment and methods used, and were not approved by the regulatory authorities.
4. The operation that the workers were performing was not one in the normal manufacturing process of uranium fuel for light water reactors but was during the process for manufacturing uranium fuels for Joyo. The accident occurred during a process in which a special product was manufactured in small quantities.

The worker involved described the reasons for these methods in an interview as reported by the Asian Labour Update (Occupational Safety and Health Resource Centre Newsletter August 2000):

a. The accumulation tower was only 10cm above the floor, making it inconvenient to put the liquid into the container. Therefore, the remaining liquid in the tower was removed using a dipper. The worker thought it was improper to handle the material in this way, but the equipment had not been improved. Furthermore they were obliged to handle the material in this way because of the unauthorized change in the process made by the JCO .
b. It was common practice to put 16Kg of uranium into the tower, and he thought that it would be acceptable to put an equivalent quantity of uranium into the precipitation tank, because the tower and the tank had a similar capacity.
c. He was obliged to work in a remote and strange workplace
d. Although his supervisor gave him no instructions to accelerate the operation including sampling after homogenization, he wanted to complete these operations earlier to allow new staff, which were scheduled to join the crew in October 1999, to handle the liquid waste process from the outset.
e. The workers were involved not only in the highly enriched uranium handling operation, but also in the low level radioactive waste handling operations, which was a quite confusing situation for them.

THE ACCIDENT COULD HAVE BEEN PREVENTED BY:

The fact that the procedure followed in the company was not the one licensed by the Japanese Science and Technology Agency, meant that it was possibly unsafe in itself. This violation demonstrates that it is not possible to rely on self responsibility of a company in severe safety matter: this could have been prevented if regular inspections in the nuclear facility by the authority that had licensed the plant were foreseen. Also regulation was lacking since the only inspection foreseen was at the time of commissioning, to ascertain that it was constructed according to the licensed design.

The violation would have been less likely If the facility would have been inspected periodically by the competent authority.

The facility in which the accident occurred was not operating continuously, its cumulative use was about 2 months per year. For tasks that are not routine ones particular attention has to be

focused, because the ability required for performing these tasks are not skill-based, hence a higher probability of errors is likely to be present.

The performance should be seen as a rule-based one, therefore good training and an established written procedure must be followed, and supervised.

The operators found the equipment unsuitable for the task they were asked to perform. It probably required a not very difficult change in the design in order to meet their suggestion. It's possible to improve processes and equipment if the relationship of the management with the front line is not the one-way communication type.

The fact that there was a possible source of confusion in the way the equipment of the process was designed (the tower and the tank had a similar capacity), is a sign that it's possible to avoid criticalities adopting a Poka Yoka approach in designing which is normally something easy and relatively un-expensive to do. As reported in this example (T. Kletz 2001): In the early days of anesthetics an apparatus was used to mix chloroform vapor with air and deliver it to the patient. If the apparatus was connected up in the other way round liquid chloroform was blown into the patient with results that were usually fatal. The apparatus was redesigned with different types of connection or different pipes sizes so that they were no longer interchangable.

The three workers were working in a remote area of the plant; this in turn, could have affected the way they perceived themselves and their role in the company.

The fact that they felt the area as a remote one could be due to a lack of supervision from the plant manager, and could have conveyed the sensation that the process they were performing was a not very important one (it was not part of the normal manufacturing process); lowering the level of attention, which is strictly connected with the motivation.

This effect could be avoided directly supervising the area, even only during the everyday patrol of the plant manager (particularly when the process at which the area was assigned, was being performed).

The operators were under time pressure because they were waiting for new staff to join the crew, and they wanted to enable them to start from the beginning of the process. Being under time pressure is one of the environmental conditions that raises error probability; In the process industry production should be scheduled considering all the possibilities to avoid time tight conditions that could lead to criticality.

The safety management system that the company had was mainly focused on meeting the legal requirements; a safety culture in a high hazard process plant is part of the integrated management. It could be built up over time, if the SMS is tailored upon the reality which is actually applied and if the management of the company is directly involved and consider the problem of the technician that is handling the hazardous substance as part of its own job.

The daily safety report, that the plant manager was expected to compile, was just seen as a bureaucratic-routine in the organization culture, that meant that the form and the attention paid to that tool could be changed in order to use it as a proper method of prevention.

An Audit could be performed monthly, partially based on the result of the daily reports, by the manager of the manufacturing department.

And a weekly safety report meeting, as the one presented in the SMS suggested by the Seveso II directive, should be introduced, as a common practice to discuss daily reports and accidents that occurred in companies of the same field. Also this directive institutes a regular inspection process, also aimed to assess the SMS adequacy.

4. CRITICAL FEATURES OF SAFETY MANAGEMENT

"Human factors dominate the risks to complex installations. Even what appear at first sight to be a simple equipment breakdown can usually be traced to some prior human failure.

The casual sequence of an accident move from fallible decisions, through the intervening planes to an accident, that is, the unplanned and uncontrolled release of some destructive force, usually in the presence of victims" (J. Reason 1990)

Human error can be more widely intended as the direct human responsibility in the occurrence of one of the elements in the chain of events that lead to an accident.

This is then not only related to the sharp end (operator's error) but it can be related to errors of the managers at every level of the company, this type of 'human performance problems' are usually known as organizational/managerial factors.

In the already mentioned book "An engineer's view of human error" by Trevor Kletz, it is quoted "Try to change situations, not people" as the main theme of the book itself.

It is important from an engineering point of view to focus the efforts on the aspects of the problem on which it is possible to intervene in order to optimize the general situation.

The organizational factors are easier to be modified than human nature. Another aspect of the problem is the specificity of the hazard that the organization has to cope with.

The attitude that is generally adopted towards industrial activities is a cost-benefit approach: The activity is undertaken if it provides economic benefits that justify and reward the effort of undertaking it.
Risk management is part of these efforts, and has to be carried out in order to avoid losses that will overwhelm every reached, promised or foreseeable benefit.
Risk characterized most human activities, especially those regarding knowledge, as it is suggested by the title of one of the *Gerling Akademie*[†] publications, *"Risiko und Wagnis" (Risk and Adventure).* Risk is an object by definition, very difficult to handle, thus the related organizational activity is called 'Safety Management'. The process of safety management consists of well-defined steps aimed at avoiding losses and identifying opportunities to improve security, quality and, as a consequence, performance in an organization.
Management is a technique, a method, hence its rules have to be adequate to the object that has to be managed; the main starting point is the observation of the object itself.
The circumstances in which the object (Risk) expresses itself in a more striking way are accidents. The discussion on some of the most critical features of safety management, as emerged in the cases reported in Major Accident Reporting System (MARS), can start from the classification derived from G. Drogaris about Root causes of Accident scenarios.
From this experience he derived the following classification that examines the main managerial/organizational critical features of safety management, and underlying or root causes of 'human/operator' errors in most of the accidents presented before.

Root causes:

1) Managerial/organizational omissions
   1.1 Lack of a safety culture

[†] Die Gerling Akademie für Risikoforschung hat sich die Aufgabe gestellt, die verschärfte Risikosituation in der industriellen Welt zu erforschen und bewußt zu machen. Sie greift dabei auf interdisziplinäre und ganzheitliche Ansätze zurück. Das hieraus gewonne Wissen wird in Form von Publikationen, Beratungen und Seminaren Unternehmen zugänglich gemacht. **From the web site of Gerling Akademie für Risikoforschung AG, Zürich.**

1.2 Inadequate safety organization
1.3 Pre-determined safety procedures not observed (E.g.: to keep up or to speed up the production, etc)
1.4 Insufficient or unclear procedures
    1.4.1 Operational procedures
    1.4.2 Maintenance procedure
    1.4.3 Testing, commissioning, inspection or calibration related procedures
    1.4.4 Construction procedures
    1.4.5 Internal communication procedures
    1.4.6 Work permit procedures
    1.4.7 Laboratory analysis procedures
    1.4.8 Material storage procedures
1.5 Insufficient supervision
1.6 Failure to clarify causes of previous accidents
1.7 Insufficient operatory training
1.8 Understaffing
1.9 Other related to design inadequacies (to be attributed whenever causative factors 2.1/2/3/4 as defined here below are identified among the causes of accident)
1.10 Insufficient installation of safeguarding

2) Design inadequacy
    2.1 Application of codes/practices not suitable for the process
    2.2 Process inadequately analysed from the safety point of view so that the hazards had not been identified
    2.3 Design error (omission, no proper application of codes practices)
    2.4 Failure to apply ergonomic principles to the design of man-machine interface
    2.5 Codes/practices applied provided only for limited protection
3) Appropriate procedures not followed (short-cuts)
    3.1 Operational procedures
    3.2 Maintenance procedures
    3.3 Testing, commissioning, inspection or calibration procedures
    3.4 Construction procedures
    3.5 Internal communication procedures
    3.6 Work permits
    3.7 Laboratory analysis procedures
    3.8 Material storage procedures

All the above issues could be discussed in more detail, for the scope of the present work we will focus the attention on the organizational failure to clarify causes of previous accidents.

“Accident investigation is like peeling an onion or dismantling a Russian doll. The outer layers deal with the immediate technical causes and triggering events, while the inner layers deal with ways of avoiding the hazard and with the underlying weaknesses in the management system.” (T.Kletz 1993)

The purpose of reporting and evaluating/investigating accidents has to do whit the core of safety management is to prevent further occurrence identifying weak points in a safety management system. “The function of safety is to locate and define the operational errors that allow accidents to occur. This function can be carried out in two ways: (1) by asking why-searching for the root causes of accidents, and (2) by asking whether or not certain known effective controls are being utilized” (Dan Petersen 1989). Organizations should therefore establish effective procedure(s) for dealing with this task, and because the main aim of identifying causes and root-causes of accidents is similar to that of detecting causes of near

misses and non-conformities. The procedure(s) should be able to handle all of them. Minor failures or malfunctions could be indicative of earlier stage of major accident occurrences, which is why it is useful to analyse them.

In the OHSAS 18002 2000 it's possible to find some guidelines for implementing a process of accident, incidents and non-conformances investigation:

"The procedure should:

- define the responsibilities of the persons involved in implementing, reporting, investigating, follow-up and monitoring that corrective and preventive actions;
- require that all non-conformances, accidents, incidents and hazards be reported;
- apply to all personnel (contractors, temporary workers and visitors as well)
- take into account property damage;
- ensure that no employee suffers any hardship as a result of reporting a non-conformance, accident or incident;
- clearly define the course of action to be taken following non-conformances identified in the safety management system".

There are two features related to human attitude, that needs to be underlined as influencing factors in accident investigation.

First of all, as already indicated in the OHSAS 18002 2000 suggestions, it is important to avoid a blame attitude in the company.

A study conducted by D.A. Hoffmann and A.Stetzer (Hoffmann, Stetzer 1998) has pointed out that "a necessary prerequisite for accident investigation, might be a context that encourages open, positive and free-flowing communication about negative events". They conducted an experiment using two different samples of respondents that were workers of a large utility company. The sample 1 in one experimental condition "received clear information indicating that a worker was the cause of the accident, they were workers in team where open and upward communication regarding safety were not encouraged, and they were less willing to make internal attributions. With respect to the second sample, whose members received information indicating both internal and external causes, the results indicated that workers on teams with a positive safety climate and where communication about safety issues was open made more internal attributions."

The second feature regards the tendency to draw only superficial conclusion from the accident scenario under analysis, and to stick to the first hypothesis that come to our mind, this tendency is called mind-set or, with the German term, 'Einstellung'.

A reason for this behaviour is the one quoted by Dörner (D. Dörner 1987):

"Reductive hypotheses are very attractive for the simple reason that they reduce insecurity with one stroke and encourage the feeling that things are understood (they can even be right- why not, that can be proved. The probability is rather low, however, that organic structures are monocausal and radially organized)"

The only way to avoid the 'Einstellung' is to be aware of this natural tendency, and to encourage the investigation to go beyond premature conclusions.

The training of the personnel in charge for the accident investigation can provide sufficient awareness.

There is a last suggestion in the OHSAS 18002 2000 worth noting:

- "Identified causes of non conformances, accidents and incidents should be classified and analysed on a regular basis…. The associated documentation should be appropriate to the level of corrective action."

A computerised database is the modern tool for obtaining a useful record-keeping instrument. Furthermore it permits to implement a methodical data analysis, which in turn can provide Key Performance indicators for this peculiar “managerial activity”. Quoting again Dan Petersen we might say that “Safety should be managed like any other company function. Management should direct the safety effect by setting achievable goals and by planning, organizing, and controlling to achieve them. The key to effective line safety performance is management procedures that fixed accountability.”

5 SAFETY MANAGEMENT SYSTEMS AND ROOT CAUSES OF ACCIDENTS.

A safety management system is, according to the definition given by the OHSAS 18001 (1999):

> " part of the overall management system that facilitates the management of the Occupational Health and Safety risks associated with the business of the organization.
>
> This includes the organizational structure, planning activities, responsibilities, practices, procedures, processes and resources for developing, implementing, achieving, reviewing and maintaining the organization's Occupational Health and Safety policy".

In the present chapter, with the aim of confirming adequate regulatory coverage, the root causes according to the classification derived from accident analysis (see chapter 4) are confronted with the main seven points constitutive of a major accident prevention policy according the Seveso II Directive, that is to say:

> "(a) the major accident prevention policy should be established in writing and should include the operator's overall aims and principles of action with respect to the control of major-accident-hazards;
> (b) the safety management system should include the part of the general management system which includes the organizational structure, responsibilities, practices, procedures, processes and resources for determining and implementing the major-accident prevention policy;
> (c) the following issues shall be addressed by the safety management system:
> **(i) organization and personnel** - the roles and responsibilities of personnel involved in the management of major hazards at all levels in the organization. The identification of training needs of such personnel and the provision of the training so identified. The involvement of employees and, where appropriate, subcontractors;
> **(ii) identification and evaluation of major hazards** - adoption and implementation of procedures for systematically identifying major hazards arising from normal and abnormal operation and the assessment of their likelihood and severity;
> **(iii) operational control** - adoption and implementation of procedures and instructions for safe operation, including maintenance, of plant, processes, equipment and temporary stoppages;
> **(iv) management of change** - adoption and implementation of procedures for planning modifications to, or the design of new installations, processes or storage facilities;
> **(v) planning for emergencies** - adoption and implementation of procedures to identify foreseeable emergencies by systematic analysis and to prepare, test and review emergency plans to respond to such emergencies;
> **(vi) monitoring performance** - adoption and implementation of procedures for the ongoing assessment of compliance with the objectives set by the operator's major-accident prevention policy and safety management system, and the mechanisms for investigation and taking corrective action in case of non-compliance. The procedures should cover the operator's system for reporting major accidents of near misses, particularly those involving failure of protective measures, and their investigation and follow-up on the basis of lessons learnt;

(vii) audit and review - adoption and implementation of procedures for periodic systematic assessment of the major-accident prevention policy and the effectiveness and suitability of the safety management system; the documented review of performance of the policy and safety management system and its updating by senior management."

The confront can be easily made by the use of a matrix, where each line is one of the seven points in above and each column is one of the root causes highlighted in the Drogaris's analysis in the previous chapter:

(SEVESO II)	**Critical features in safety management according to Drogaris' classification**	1.1	1.2	1.3	1.4.1	1.4.2	1.4.3	1.4.4	1.4.5	1.4.6	1.4.7	1.4.8	1.5	1.6	1.7	1.8	1.9	2	3
C.1	Organisation and personnel	■	■						■	■					■	■			
C.2	Identification and evaluation of major hazard									■				■				▒	
C.3	Operational control			■	■	■					■	■							■
C.4	Management of change							▒										▒	
C.5	Planning for emergencies																▒	▒	
C.6	Monitoring performance						■						■						
C.7	Audit and review						■			■									

Tab 5.1 Cross Sectional Analysis between the seven points of the Seveso II and Drogaris classification

Where the numbers in column correspond to:

Root causes:

1) Managerial/organizational omissions
   1.1 Lack of a safety culture

   1.2 Inadequate safety organization

   1.3 Pre-determined safety procedures not observed (E.g.: to keep up or to speed up the production, etc)

   1.4 Insufficient or unclear procedures

      1.4.1 Operational procedures

      1.4.2 Maintenance procedure

      1.4.3 Testing, commissioning, inspection or calibration related procedures

      1.4.4 Construction procedures

      1.4.5 Internal communication procedures

      1.4.6 Work permit procedures

      1.4.7 Laboratory analysis procedures

      1.4.8 Material storage procedures

1.5 Insufficient supervision

1.6 Failure to clarify causes of previous accidents

1.7 Insufficient operator training

1.8 Understaffing

1.9 Insufficient installation of safeguarding

2) Design inadequacy

3) Appropriate procedures not followed (short-cuts)

The boxes filled with a clearer colour need some clarifications:

- the problems regarding construction procedures (column 1.4.4) can be considered partly in the field of "management of change" partly in "operational control". Indeed the former concerns change for parts that are to be built brand new or to be modified while the second covered all the operations, also the construction ones, that are " for safe operation, including maintenance, of plant, processes, equipment and temporary stoppages";
- "Design inadequacies"(column 4.2) can be managed partly in the field of management of change (they regards both old and new plants, or parts of the plant), and partly in the field of "identification and evaluation of major hazards", since one of the best ways to increment safety is "an inherently safe design";
- The column 1.9 " Insufficient installation of safeguarding" belongs to the field of Planning for emergencies because the installation of safeguarding requires a systematic analysis of the possible way by which an emergency can be detected and the first steps in order to resolve it or to mitigate the consequences.
- It is important to notice that in the analysis of the critical features of safety management according to Drogaris' classification there was not a specific voice dedicated to management of change (which is a cause connected with the one of the Flixborough Accident as well). The accident , in fact, was mainly due to a change applied without a proper plan for its design and its consequences: the temporary substitution of a reactor with a pipe was at the origin of a relevant explosion.

After this analysis, it appears that the regulatory requirements cover control of all root causes identified for major accidents, in addition they make more explicit reference to important issues such as management of change.

As the Tokaimura accident demonstrated, it is not enough to rely on self control of management systems: it appeared very appropriate to establish routine inspections from authority to control the main critical features of safety management. Check lists may be useful instruments both for external inspections and self-evaluation as well. Examples of possible questions in such check lists are reported below[‡]:

- Is safety management supported by the higher levels of the organization?
- Who is responsible of its implementation?
- Are the performances or the activities of the company monitored through the use of some specific mechanisms for qualitative and quantitative evaluation?

[‡] Other guidelines are available in the documentation of the Major Accident Hazard Bureau of the European Union, MAHB or in the OHSAS 1800/1999 and 1800/2000 of the BSI.

- Is Risk analysis and risk assessment carried out by the use of an appropriate methodology, such as Hazop or similar methods, that enable to design or to modify equipment and procedures with a systematic criterion.
- Is risk analysis carried out in relation of all the most critical parts and the most critical operation of the plant?
- Is the population around the establishment adequately informed of possible hazards and of the consequent emergency plan that regard them?
- Is the management system documented with the appropriate standards?
- Does the organization assign clearly, roles and responsibilities at every level, in relation to the required competencies?
- Does the organization have internal committees for safety? If yes, what are their functions?
- Is the organization able to manage changes so that every change is adequately evaluated and integrated with the rest of the operational assess?
- Does the organization have an internal audit system? Is the audit frequency planned in relation to the particular features of the object that has to be checked?
- Does the organization have a procedure for reporting and investigate past accidents or non-conformities?
- Does the organization have a procedure for the follow up actions in relation to past accidents and non conformities?

The analysis of cause of accidents, SMS regulation requirements and inspection possibilities constitutes a valid background for approaching analysis and improvement of existing procedures in an industrial environment, as discussed in the following chapter.

6 HUMAN FACTORS ANALYSIS AND SAFETY MANAGEMENT SYSTEMS: A CASE STUDY FROM THE PROCESS INDUSTRY

Reporting and investigating accidents, incidents and near misses aim at preventing further recurrences by identifying weak points and failures in technical equipment and in the management system, and by taking appropriate corrective actions. The adoption of a sound procedure is one of the main channel by which is possible to implement the "continue meliorating cycle" for the management system.

- Furthermore the OHSA 18002 (2000) suggests "Identified causes of non conformances, accidents and incidents should be classified and analysed on a regular basis…. The associated documentation should be appropriate to the level of corrective action."

A computerised database is the modern tool for useful record-keeping. During the stage of the author at the Falconara (I) oil refinery, because of the construction of a new database, the company organised a review of the procedures for dealing with non conformance and incident analysis, and reporting on human and organizational factors. The author participated in this revision by proposing the adoption of a procedure based on the SLIM methodology for ameliorating the procedures for remedying to non conformances emerging from the analysis. The proposed procedure has been now considered for adoption by the operator of the facility.

6.1 NON CONFORMITIES AND ACCIDENTS ANALYSIS IN AN ITALIAN OIL REFINERY

The Oil Refinery is characterized by:

- a work capacity of 3,9 tons per year
- electric energy production with IGCC unit of 2.000.000 MW/h per year
- work force of 400 operators and 1500 contractors
- oil products store capacity of 1.500.000 m^3

The Refinery is endowed with an integrated safety quality and environment management system that responds to the regulation requirements as shown in the following matrix

D. Lgs. 334/99 (SEVESO II)																							
	Feature of the internal safety management system	I.1	II.1	III.1	IV.1	V.1	VI.1	VI.2	VII.1	VIII.1	IX.1	IX.2	IX.3	IX.4	IX.5	IX.6	IX.7	IX.8	X.1	XI.1	XI.2	X.
C.1	Organization and personnel			■	■	■	■		■					■								
C.2	Identification and evaluation of major hazards					■		■		■	■	■	■									
C.3	Operational control					■					■			■	■	■	■	■				
C.4	Management of change					■						■	■									
C.5	Planning of emergencies					■	■												■			
C.6	Monitoring performance					■														■	■	
C.7	Audit and review					■														■	■	

Tab 6.1 Correspondence between the Safety Management System of the Refinery and the seven points of the Seveso Directive

Where the value in column are:

I.1 Policy document	VII.1 Communication	IX.6 Inspections
II.1Objective and programs	VIII.1 Planning/ Risk management	IX.7 Audit and surveillance
III.1 Organization	IX.1 Operative control/Safety and Environment	IX.8 Security
IV.1 Management of the documentation	IX.2 Changes control	X.1 Emergency plan
V.1 Legal prescriptions	IX.3 Work permit procedure	XI.1Non conformances management and Review
VI.1 Information and training	IX.4 Supply/ contractors	XI.2 Internal Audit
VI.2 Personal protective equipment	IX.5 Maintenance	

In particular:

The procedure used to analyse and report accident and non-conformances is structured as a part of the IX.1 point of the safety management system and it is structured in the following steps:

1) Identification of all the relevant information about the accident or the non conformance

2) Event description

3) Evaluation of the events in terms of real or potential risk (using the matrix in the module A1 section B reported in the following)

4) Analysis of the immediate and root causes

5) Re-examination of the events, evaluating the problems identified

6) Definition of the follow up actions in order to prevent or to control the root causes that have been underlined

7) Control of the time schedule established for the follow up actions.

To report a non conformance is responsibility of all the personnel in the refinery, contractors included. The non conformance has to be reported to the foremen of the area where it occurred. These collect then the information and order the first actions needed for bringing the situation back to a safe condition. The internal report and the analysis is implemented using the modules presented in the following (module A.1 section A, A.1 section B, A.1 section C).

6.2 PERFORMANCE INDICATORS FOR NON CONFORMANCES ANALYSIS AND PRIORITIZATION OF CORRECTIVE ACTIONS

The "Non conformances Procedure" is a critical element for the ameliorating cycle of the safety management system. At the moment, as key performance indicator for this particular aspect, the system assumes the percentage of corrective actions completed according to the time scheduled after identifying the non conformances.

In the present chapter a strategy is proposed, in order to measure the vulnerability of the system to human errors.

This is possible by introducing a further key performance indicator, that in turn can be used also for implementing trend analysis and for establishing a priority scale among the different corrective actions. This aspect could be also further developed in order to use this indicator as a quantitative term for a Cost-Benefit analysis (this aspect however, will not be discussed in the present report).

The accident reporting system in the refinery is structured in such a way that for each event the analyst should report immediate causes (two macro categories: Operative Practices below the standards, Operative conditions below the standards) and root causes. The root cause are subdivided into two macro categories as well:

- **Human Factors:**
  - Operator's Physical or Psychical conditions unsuitable for the task
  - Physical or Psychical Fatigue
  - Lack of general knowledge
  - Lack of specific technical knowledge required for the task
  - Insufficient motivation
  - Slip/lapsus
  - Routine violation
- **Job related factors:**
  - Incorrect environmental/safety/ health evaluation
  - Design /construction inadequacies
  - Erroneous task planning
  - Inadequacy of materials or components quality
  - Incorrect maintenance by contractors
  - I&T equipment inadequacy
  - Lack of inspections /fatigue of the components/ incorrect use
  - Criticality related to the procedure/Operation as assigned

For the root causes, it has been proposed to modify the analysis format according to a different safety management strategy. The latter is based on SLIM, the method of analysis for human errors that has been already described at chapter of the present report. The method is based on the proceduralized judgment of a group of experts in relation to the event under scrutiny. For each event they assign the appropriate Performance Shaping Factors, that is to say those factors, or aspects, characterising the environment in which the event has occurred and the particular operative context (e.g.: the human machine interface in a control room, the level of training required for the task in a complex system, and so on).

For each one of these factors it is required an estimation of two values:

w_i that expresses the importance of each factor and

r_i that expresses the actual condition in relation to that aspect at the moment in which the event occurred.

The first value is a weight (usually chosen between 0 and 100) for taking into account how important is the factor i in relation to the event or the task under analysis (it is normally better to start from the most important in order to assess the others in relation to the first). The value r_i aims, instead, at giving an indication about the actual condition of the factor i at the specific moment of occurrence of the event (e.g.: to give a numerical example for the non conformance for the operation is referred to, the training of the operator is very important ($w_i = 80$), but at the moment the non conformance occurred the operator in charge was a new employee with very little experience and very little specific knowledge about his task ($r_i = 20$) .

Then is possible to calculate

$$SLI = \sum_{i=1}^{N} \overline{w}_i r_i$$

Where $\overline{w}_i$ is the weighted value $\overline{w}_i = w_i / \sum_i w_i$

If SLI<50 corrective actions and a follow up plan are needed in short time.

In order to implement the method for the root causes related to human errors some performance shaping factors have been introduced (some of which were previously considered among job related factors). For each one of those, every time a human error has to be reported the analyst (or the team of analyst) should assess the w_i (importance) and r_i (real condition in relation to that aspect at the moment in which the event has occurred). Using those values the SLI index in relation to each event can be evaluated.

It is then possible, through the use of this index, to assign a priority to each possible corrective action by considering:

1) Risk index (real or potential according to which one is the highest) referred to the non conformance, identified through the use of the risk matrix reported in the accident reporting system modules of the refinery.
2) SLI index, the lowest the value is, the more attention is required: the non conformance analysis find out some critical pint and corrective actions are needed.
3) In relation to each event among all the possible corrective actions is better to assign resources first to the one presenting the highest w_i and lowest r_i and following this criteria the resources are assign step by step to the others as well.

In order to evaluate how effective a corrective action can be, is possible to recalculate the SLI index considering how the corrective action would meliorate the w_i and r_i parameters in relation to the factor it would affect. On the base of this proceeding, it could be even possible to introduce a cost benefit analysis for the more expensive actions.

Following the prioritization is then necessary to ensure the control of the scheduled time for the execution of the follow up plan, with all the corrective actions. We now report the modules for reporting and analysing non conformances, as they should be changed in relation to the proposed procedure; the modules are in Italian, but the parts that are relevant for illustrating the application of the SLI index have been translated into English. In particular the following table refer to the SLI implementation as part of the modules of the accident reporting system. It is worth noting that the root causes classification, as far as the human related factors are concerned, are following the Reason's classification scheme, and this enables the analyst to highlight more easily the most appropriate corrective actions.

Tab 6.2: Root causes related to human factors: Table for SLI evaluation in modules of the refinery accident reporting system

	HUMAN FACTORS	*PERFORMANCE SHAPING FACTORS*	*IMPORTANCE wi*	*REAL CONDITION ri*
	Operator's Physical or Psychical conditions unsuitable for the task		*(from 0 to 100)*	*(from 0 to 100)*
	Physical or Psychical Fatigue	Training		
	Lack of general knowledge	Communication		
	Lack of specific technical knowledge required for the task	Adequacy of Planning/Supervision		
	Insufficient motivation	Adequacy of Procedure /documentation		
	Slips/lapsus	Time available for task execution		
	Routine violations	Adequacy of Human Machine interface		

A1 SECTION A

Da:	**Date of the report**
A: CSA (Sicurezza Ambiente e Qualità, Sistemi Sicurezza, Antincendio e Prevenzione, Sistemi ambientali, Off site, Manutenzione e affidabilità, Affidabilità, STF, Produzione, Operazioni IGCC, Ingegneria e Costruzioni. Ingegneria di Sicurezza, Tec. Prog. contr. ottim. lavor.)	
C.C. : Direttore, Segreteria	**Altre Funzioni**

ACCIDENT OR INJURY	**NEAR ACCIDENT**	**ENVIRONMENTAL INCONVENIENCE**	**OPERATIVE INCONVENIENCE**
Infortunio Esplosione Incendio Crollo o implosione Danno a proprietà aziendali Danno a proprietà esterne Spandimento grave Fuga di gas Emissione non controllata dai camini …..……	Potenziale I.I. Potenziali danni a salute Potenziali danni all'ambiente Spandimento lieve Limitata fuga di gas Perdita di chemicals Potenziali danni ai processi Fuori servizio temporaneo effluenti. gassosi Fuori servizio temp. effluenti liquidi ……	Emissioni Atmosferiche Diffuse Emissioni Atmosferiche Convogliate Scarichi idrici Rifiuti Suolo / Sottosuolo Rumore anomalo Odori sgradevoli anomali Reclami esterni Picchi emissione / fumate Scarichi anomali torcia e/o effluenti ……..	Perdita di produzione Ritardi preparazione Ritardi nelle spedizioni Fuori specifica prodotti Incremento consumi Fermata impianti Ritardo delle forniture di servizi / lavori Prodotti / servizi non conformi ……. …….
Luogo dell'evento		Data	Ora

Real risk low: C = P = R =	**Real risk medium: C = P = R =**	**Real risk high: C = P = R =**
Ptential consequences C =	**Potential risk R =**	

EVENT DESCRIPTION

IMMEDIATE CAUSE -

Numeri	

FUNDAMENTAL CAUSES

Lettere	

CORRECTIVE ACTION PROPOSED

A	
B	
C	
D	
E	

EVENT	More analysis required	Does not Require more analysis	Has to be riexamined by CSA

Function to be involved -

Leader

Firma (leggibile) di chi ha steso il Rapporto

TO BE COMPILED BY THE CSA SECRETARY

Classification	**S**	**A**	**Q**

Leader

The CSA President

CONSEQUENCES						OCCURRENCE PROBABILITY				
C	Parola chiave	Economiche	Immagine	Ambientali	Salute e Sicurezza	A MOLTO RARA Probabilità quasi nulla	B RARA Improbabile	C OCCASIONALE Può accadere alcune volte (1)	D PROBABILE Può accadere più volte	E FREQUENTE Può accadere ripetutamente
1	*MINIMA*	No / o leggera influenza sulle lavorazioni < 10 K€	Entro i confini	Effetti ambientali entro i confini	Disagio Medicazioni / Inf. da 1 a 3 g	1	2	3	4	10 (x2)
2	*MODERATA*	Slow down > 10 < 100 K€	Aree limitrofe	Picchi di emissione / Segnalazioni singole	Malessere Da 3 a 10 g	2	4	6	16	30 (x3)
3	SERIA	Shut down breve >100 K€ <1M€	Territorio Comunale	Emissioni prolungate / Segnalazioni Ripetute	Malattia Profes. Reversibile Da 10 a 30 g	3	6	18	36	60 (x4)
4	MOLTO SERIA	Shut down prolungato > 1 < 10 M€	Provinciale / Regionale	Perdite o rilasci / Contaminazione reversibile	Danni alla salute permanente >30g / Infortun. a + persone	4	16	36	64	80 (x4)
5	ESTREMA	Sostanziale o totale perdita di operatività > 10 M€	Nazionale	Perdite o rilasci / Contaminazione permanente	Esposizioni letali Infortunio mortale	10	30	60	80	100 (x5)

IMMEDIATE CAUSES

OPERATIVE PRACTICE BELOW THE STANDARD		WORK CONDITIONS BELOW THE STANDARD	
1	Eseguita un'operazione che non si voleva / doveva fare / senza autorizzazione	19	Sistemi di sicurezza / prevenzione / protezione non adeguati
2	Dimenticata un' operazione che si doveva / voleva fare	20	Apparecchiature / Attrezzature / Materiali non idoneo all'utilizzo
3	Mancanza di comunicazione / Segnalazioni errata / insufficiente / non alle persone appropriate (es. di un'azione, un pericolo, allarme)	21	Apparecchiature / Attrezzature non in sicurezza
4	Mancanza di condizioni di sicurezza errate / insufficienti	22	Rottura e/od usura che poteva essere prevista / imprevista
5	Mancata Valutazione / Pianificazione errata / insufficiente	23	Sistema di segnalazione / allarme inadeguato / malfunzionanti
6	Mancanza di precisione / velocità di esecuzione impropria / fretta	24	Pericoli di incendi / esplosioni
7	Uso non corretto / improprio di attrezzature / apparecchiature	25	Congestione dell'area / Possibilità di azione limitata
8	Uso di attrezzature / apparecchiature malfunzionanti	26	Pulizia e ordine carente / Presenza di ostacoli
9	DPI non utilizzati / usati male / difettosi	27	Presenza di polveri, fumi, nebbie, gas o vapori
10	Conoscenza inadeguata di regole e procedure	28	Ventilazione inadeguata
11	Procedura non seguita / Disposizione impropria	29	Esposizione ad alte o basse temperature
12	Resi non operativi i sistemi di sicurezza / controllo	30	Illuminazione inadeguata o eccessiva
13	Appar./ strutture/ macchine posizionate/ caricate in modo inadeguato	31	Rumore eccessivo / esposizione eccessiva
14	Impropria operazione di carico / sollevamento / ripristino / sostituzione di apparecchiature / strutture/ macchine	32	Transito pericoloso / Mezzi di trasporto
15	Posizione o postura impropria per l'attività svolta	33	Segnaletica carente
16	Manutenzione / Intervento su apparecchiatura in funzione	34	Procedura mancante od inadeguata
17	Disattenzione / Comportamento non adeguato	35	Esposizione a radiazioni
18	Altro:	36	Altro:

ROOT CAUSES

HUMAN FACTORS

A	Operator's Physical or Psychical conditions unsuitable for the task	*PERFORMANCE SHAPING FACTORS*	**IMPORTANCE wi**	**REAL CONDITION ri**
B	Physical or Psychical Fatigue	*Training*	**(from 0 to 100)**	**(from 0 to 100)**
C	Lack of general knowledge	*Communication*		
D	Lack of specific technical knowledge required for the task	*Adequacy of Planning/Supervision*		
E	Insufficient motivation	*Adequacy of Procedure /documentation*		
F	Slips/lapsus	*Time available for task execution*		
G	Routine violations	*Adequacy of Human Machine interface*		

	JOB RELATED FACTORS	IMPORTANCE wi	REAL CONDITION ri
H	**(from 0 to 100)**	**(from 0 to 100)**	(da 0 a 100)
I	Design /construction inadequacies		
L	Erroneous task planning		
M	Inadequacy of materials or components quality		
N	Incorrect maintenance executed by contractors		
O	I&T equipment inadequacy		
P	Lack of inspections /fatigue of the components/ incorrect use		
Q	Criticality related to the procedure/Operation as assigned		

A1 SECTION C

RIEXAM OF THE EVENT FROM THE EXPERT TEAM

Area of the Event	**Department**	**Date of the event**
Leader of the accident investigation	**Classification**	**Date of the report**
Rischio Reale Basso : C = P = R =	**Rischio Reale Medio: C = P = R =**	**Rischio Reale Alto: C = P = R =**
Potential Consequence of the event C =	**Potential Risk R =**	
EVENT DESCRIPTION: FURTHER FINDINGS		
IMMEDIATE CAUSES: FURTHER FOUNDINGS		
Numeri		
FUNDAMENTAL CAUSES: FURTHER FOUNDINGS		
Lettere		
SLI INDEX OF THE EVENT SLI=		
LESSON LEARNT –		

	CORRECTIVE ACTIONS	**priority Index**	Collaborator	**EXECUTOR**	**DEAD LINE**
A					
B					
C					
D					
E					
F					

6.3 IMPLEMENTATION OF A DATABASE FOR NON CONFORMANCES ANALYSIS

In order to analyse the events and to keep an historical records of all the events in the refinery, a Database has been implemented. The three functions of the database are:

- Reporting the Non Conformances (data entry), using as a model the format A1.C illustrated above.
- Searching among the Non Conformances using as a criterion Risk index, place of the event, fundamental or immediate causes, functions involved, corrective actions etc..
- Reporting Statistics regarding risk index, causes(among which human and organizational related causes), type of events (Incident, Near messed, Operative or Environmental Inconvenient), Corrective actions

Fig 6.1 First dialog box of the user interface of the database menu:

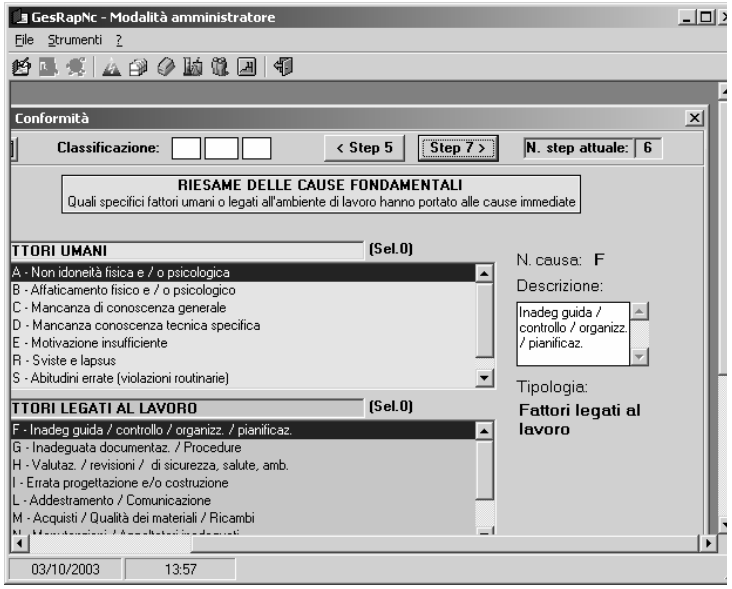


Fig 6.2 dialog box of the database: the menu of the possible causes human factors and factors related to job conditions

The database represents a valid aid for the identification of critical areas, recurrent type of events, recurrent causes in the refinery. It enables the analyst to develop a trend analysis for evaluating the effectiveness of follow up plans on risk index. In the same way it is possible to evaluate the performance of the organization in respects of the human factors using the index proposed and recording the data in the database. Thus in turn it can lead to implement a cross sectional analysis in order to identify possible concurrent causes of human factors problems.

In the following pages are reported some of the possible results of the data analysis implemented using the database; the real values are not showed in the figures for protection of the industrial secret of the company they refer to.

The following figure (Fig 6.3) shows the number of Non Conformances reported during the years in the refinery. The Non Conformances have been distinguished in NA (Near Accident), II (Incident or Injury), IO (Operative inconvenience), IA (environmental Inconvenience). The last classification category has been introduced only in 1998 this is

the reason why it does not appear before then(yellow curve). The velvet curve on top of the other represent the total amount of Non Conformances reported. The curve has a positive trend during the last part, this can be due to two different causes, the most immediate to underline is the fact that more accident happen in the refinery, which is a negative sign, on the other hand it is possible to say that the safety culture of the company has been improved, and as a result more Non Conformances are reported considering that during the previous years some of the events were not reported at all. In favor of this hypothesis is the number of events collected under the category IO (Operative Inconvenience) and IA (Environment Inconvenience) which did not exist before and therefore were possibly not taken into account in the previous years.

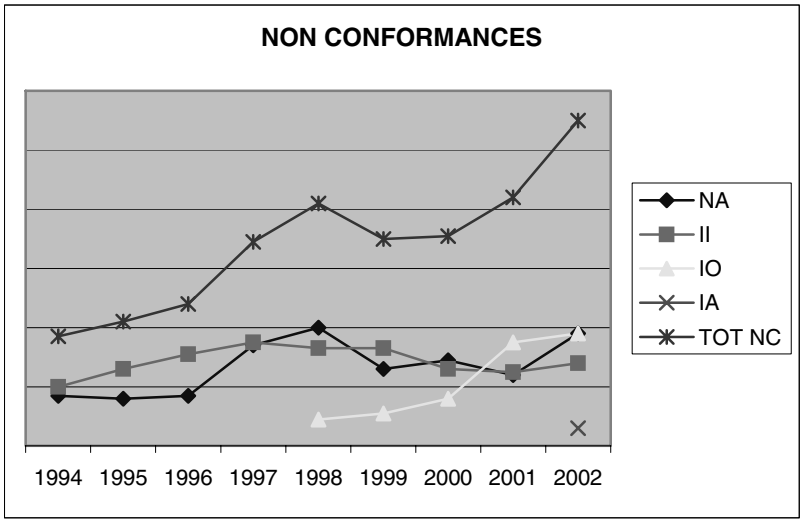


Fig 6.3 Number of the various categories of non conformances reported during the years in the refinery. The higher velvet curve is the cumulative

The following figures illustrates the fundamental causes identified for the event reported during the years. The blue curve represents the event for which the main fundamental causes are human related factors, the pink curve are the ones for which the causes were mainly job related factors; while the yellow curve represents the amount of events for which the causes have not been clearly identified (e.g.incomplete reports).

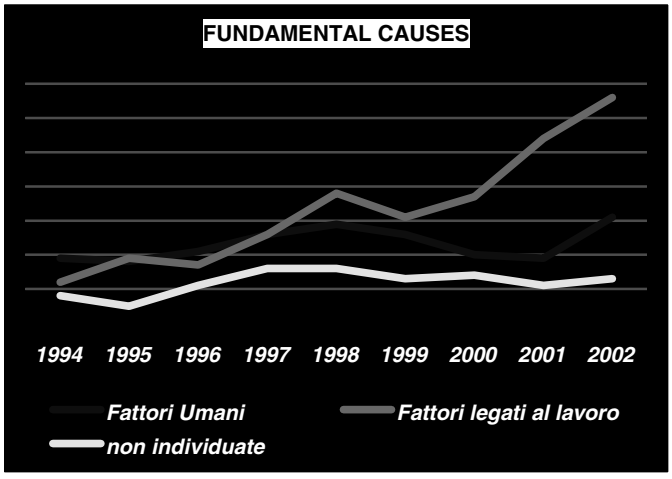


Fig 6.4 Fundamental causes reported during the years: Human related Factors(blue curve) , Job related factors (pink curve), Not identified(yellow curve)

Using the database it is possible to built diagrams able to show for each human related factors the percentage contribution to the event occurred during each year. An example is showed in the following figure (Fig 6.5). This in turn enables to highlight possible critical area of intervention in order to prevent human errors. Furthermore for each human related factors identified as critical (in the example reported for year 2002 the most recurrent errors were slips/lapsus), it is possible to find out which performance shaping factors are more strictly connected, and therefore direct towards them a medium/long term preventive/ mitigation plan.

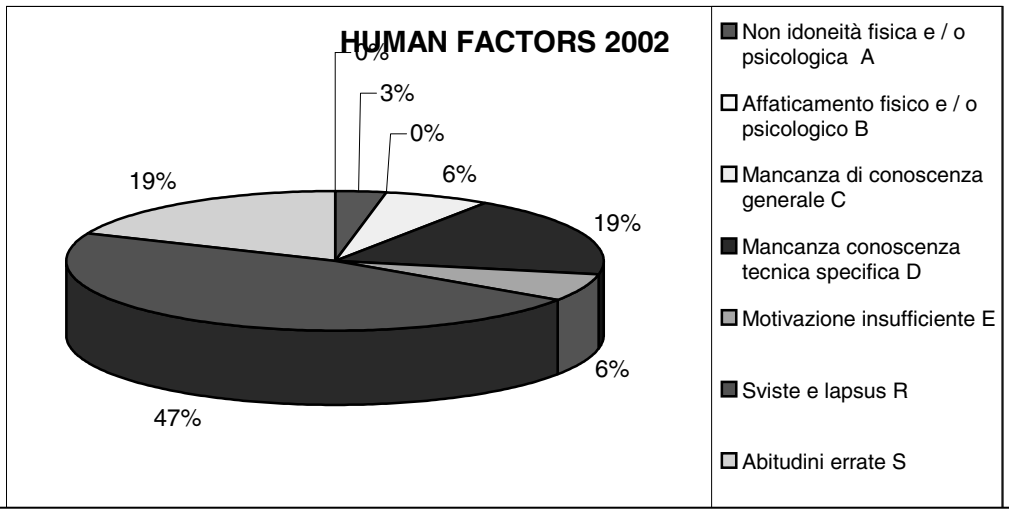


Fig 6.5 Human factors identified as major contribution for the accident occurred during the year 2002 in the refinery

CONCLUSION

The method proposed will not change completely the current procedure in the oil refinery. It can be introduced as a possible addition to the present one. It is important to demonstrate the usefulness of the new method of analysis to all the foremen and the operation directors that are going to be members of the group of analysis of reportable event in the refinery.

This can be done by examining 100 cases of previous accidents due to human factors, and performing a trend analysis using the values of SLI calculated in this way.

The proposal is aimed at reaching a better understanding of the various forms of danger that can be present in a complex system as an oil refinery, and therefore at constructing a base of evaluation for the operative methods used to keep safety.

A very important step to improve the meliorating cycle of a safety management system, is a cultural orientation of the members in the organization, aimed at finding remedies for preventing major accident, and not culprits to accuse. Being conscious of the defects that every human system, even the most “perfect”, can present.

REFERENCES:

1. Api Raffineria da Ancona s.p.a "Rapporto Ambientale 2001".
2. Occupational Health and Safety management systems- specification OHSAS 18001:1999 British Standar Institution 02-2000
3. Turner Barry A. "Man made disasters" Wykeham Pubblications London 1978
4. Vestrucci P. "Modelli per la Valutazione dell'Affidabilità umana" Franco Angeli editore 1990
5. Abernethy Robert B. et al "Weibull Analysis Handbook" Aero Propulsion Laboratory, Wright-Patterson AFB Ohio 1983.
6. Api Raffineria di Ancona S.P.A. "Manuale del Sistema di Gestione Integrato, Sicurezza Ambiente e Qualità" 2002
7. Donald K. Lorenzo JBF Associates Inc. "Practical Applications of Human Reliability Analysis" CH2682-3/89/0000-0778 1989 IEEE
8. Dörner Dietrich "On the difficulties People have in Dealing with Complexity" *New Technology and human error Edited by J.Rasmussen, K.Duncan and J.Leplat 1987 John Wiley and Sons Ltd.*
9. Drogaris G. "Major Accidents Reporting System. Lesson learned from accidents notified". Joint Research Center, Commission of the European Communities Elsevier 1993.
10. Embrey D.E., Humphreys P.C., Rosa E. A.,Kirwan B., e Rea K., "SLIM-MAUD: An Approach to Assessing Human Error Probabilities Using Structured Expert Judgment" U.S. Nuclear Regulatory commission NUREG / CR3518 1984.
11. Frank E. Bird Jr "Management Guide to Loss Control" International Loss Control Institute Georgia USA
12. Giuntini R.E. Wyle Laboratories "Mathematical Characterization of Human Reliability for Multi-task system operations" 2000 IEEE.
13. Hofmann David, Stetzer Adam "The role of safety climate and communication in accident interpretation: implications for learning from negative events" Academy of Management Journal 1998 Vol 41 No 6, 644-657
14. Human Factors Research and Nuclear Safety' The national Academy of Sciences 1988
15. IAEA "Report on the preliminary fact finding mission following the accident at the nuclear fuel processing facility in Tokaimura, Japan" Austria November 1999
16. International Loss Control Institute Atlanta "International Safety Rating System Guidelines" 1978 Atlanta USA
17. Kahneman D., Pslovic, A.Tversky "JUDGEMENT UNDER UNCERTAINITY: HEURISTICS AND BIASES" Cambridge University Press 1982
18. Kansai Occupational Safety and Health Centre "Tokaimura Nuclear Accident from an occupational safety and Health viewpoint"; Japan Occupational Safety and Health Resource Centre Newsletter No 21 August 2000
19. Kemeny J.G. (1979) "Report of the President Commission on the accident at Three Mile Island, Washington DC: US Government Printing Office.
20. Kirchsteiger C., Christou M., Papadakis G. "Risk Assessment and Management in the context of the SevesoII Directive" Elsevier 1998.

21. Kletz T. “Lessons from disaster” 1993 IChem.
22. Kletz Trevor “An Engineer’s view of Human Error” 3-rd edition 2001 Taylor & Francis
23. LaSala K.P. “Human Performance Reliability : A Historical Perspective” vol 47 no 3-sp September 1998 IEEE.
24. Petersen Dan “Technique for Safety Management” 1989 Alostray Inc.
25. Rasmussen J & Vincente K.J. “Cognitive control of Human Activities: Implication for Ecological Interface Design” RISO-M-2660 Roskilde Denmark; Riso National Laboratory 1987.
26. Rasmussen J. ”Human Errors: a Taxonomy for describing Human Malfunction in Industrial Installations” RIS- M-2304 Roskilde, 1981.
27. Rasmussen Jens “On the structure of knowledge- A Morphology of Mental Models in a Man-Machine Context” RIS-M-2192, 1979
28. Rasmussen K. ‘The experience with the Major Accident Reporting system from 1984 to 1993’ Report EUR 16341 JRC European Commission 1996.
29. Reason and Mycielska “Absent minded? The psychology of mental lapses and everyday errors”, Prentice-Hall, Englewood Cliffs, New Jersey 1982.
30. Reason J. “Human error” Cambridge University press 1990.
31. Reason J. “managing the risk of organizational accident” Ashgate Publishing company 1998
32. Simon H. A. Models of Man: Social and Rational New York: John Wiley and Sons, Inc., 1956
33. Swain A.D. THERP SCR-64-1338 1964 Aug Sandia National Laboratories.
34. Swain A.D., Guttman H.E., “Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications” NUREG/ CR –2986 1983.
35. University at Buffalo “The Tokaimura Accident: Nuclear energy and reactor safety” Michael E. Ryan Department of Chemical Engineering University at Buffalo, New York. Web site of the University at Buffalo 25/6/01
36. Von Alven, William H. (ed) “Reliability Engineering” Prentice-Hall, Inc. 1965