4

Trends, problems and outlook in process industry risk assessment and aspects of personal and process safety management

Bruno Fabiano[1] and Hans Pasman[2]
[1]*DIChePUniversity of Genoa, via Opera Pia 15 – 16145 Genoa - Italy*
E-mail: brown@unige.it
[2]*Mary Kay O'Connor Process Safety Center, Texas A&M University, College Station, TX 77843-3122, USA*

1. Introduction

Process industry brings economic activity and provides us with unique materials. While mankind grows in numbers, needs are at the increase and while natural resources become more scarce, process industry is even more needed to provide for energy and energy carriers, fertilizers, plastics, fibres, coatings, pharmaceuticals to name a few, and even clean water. At the down side there is an always looming risk of accident, loss of containment of hazardous substances and the ensuing hazards of explosions, fires and toxic spread. This creates a background threat to workers and when risks have effect outside plants to the general population. Since for several reasons industry favours locations near crossways of trade and traffic and thus vicinity to population is inevitable, risk assessment has in many places become a routine based on legislation. Risk assessment as an instrument to describe and delimit the risk of chemical process operations was introduced to the community of Loss Prevention in the process industry in the mid-seventies. Much has been written about it since that time and considerable investments made in developing methodology, release and dispersion models, as well as ways to predict damage. Many data have been collected and much has been said about interpretation of results. The latter has been an infinite source of quarrels. Meanwhile, the use of risk assessment has become rather widespread and more decision making depends on it. Not only installations bound to a certain location, but also transportation routes have been object of risk analysis and assessment. Yet, the methodology produces results which in a number of aspects are still unsatisfactory. To mention an aspect the variance of outcomes of an analysis for example is high and can cover in some cases two orders of magnitude in risk defined as the product of expected event frequency and likely damage (Pasman et al., 2008, 2009).
Apart from having doubts about the magnitude of remaining risk, there is the question why despite the large body of experience still major accidents happen. In process industry progress in maintaining safety has been impressive. Statistic figures on personal safety of

workers have fallen over 40 years in a steady rate. Yet, from time to time, high loss process incidents keep on occurring. This paper will start off presenting a statistical study on petrochemical accidents over a long period of evidence underpinning the need of developing and sufficiently strengthening control barriers to prevent catastrophic consequences to people or environment resulting from accidental releases of hydrocarbons. It will present some results extracted from a data base on the main categories of causes. It will then pay attention to human performance with respect to safety. Human decisions and acts in management, design, construction, and operation of plant have a large influence on safety. Qualitative and quantitative assessments should cover the human/machine interface, operating and emergency procedures, and training. Unfortunately, human performance factors do not always find systematically its way as input into facility design, development of operating procedures, or operator training. Also underlying economic and organizational processes have large influence as recently described by Knegtering and Pasman (2009). Cost pressure, aging, work force turnover and failing safety management play an important role and have an adverse effect on culture. This weakens the resilience of an organization.
The paper will continue describing what is meant with risk assessment, where it is used for and why and what trends can be seen. It will briefly summarise experiences in various countries. It will then try to analyse the underlying problems as there are the subjectivity in hazard identification, oversimplification in release models, assumptions in environmental conditions (weather, terrain), the large uncertainties in technical failure mechanisms and failure rates, and the deficiencies in consequence modelling and in view of the above about organization and Human Factor the effects of failures of safety management system. It will try to formulate how to go ahead.

2. Accidents in the oil industry

Investigating and analyzing the origins and consequences of accidents over a long period in a given industrial sector, in connection with proper statistical evaluation, can provide lessons on how to improve assessment and management of risk. In fact, historical analysis leads to the identification of the most probable scenarios (e.g. release, fire, explosion etc.) including consequences, as well as to the identification of the most frequent immediate or direct and underlying or root causes. Where safety improvement based on accident analysis is mainly addressed via quantification of lagging indicators as lost time injury frequency, the statistical approach can also be useful in identifying key indicators which on an industry wide basis better resolve the nature of incidents. Accidents that are considered in this section are taken from the TNO FACTS Database (TNO), which includes accident data from a number of countries starting from the beginning of the twentieth century. We focused our attention on the downstream oil industry sector for which accidents, connected to both personal and process safety, represent an area of significant concerns. By the way to put things in perspective, some measures evidence that in 2004 oil and gas workers were six times more likely to die from a fall than from an explosion/burn (OGP, 2005). We analyzed a time period starting from the early 1930s to 2008, during which 1209 events are identified. Distribution of accidents according to time, by natural decades, is depicted in Figure 1, showing a jump followed by a slower increasing trend in the last four decades after much power and chemical industry became oil based.

The distribution is to be attributed both to the improvement of accident information availability and to the increase of oil product consumption and corresponding development of the downstream oil industry.
Considering in detail the last three decades, (see Fig. 2) accident trend from statistical viewpoint is not a monotonic one, but evidences upswing and drop, which contrarily to other industrial sectors cannot be correlated to production rate (expressed as million barrel per day). Traditional lagging indicators (i.e. measures of outcomes and occurrences) are determined for a work unit. They include lost time accident frequency (e.g. eq. 1), total accident frequency index (e.g. eq. 2), fatal accident frequency index (e.g. eq. 3); high potential incident frequency; worker compensation expressed as percentage of payroll; property damage costs; loss of hydrocarbon containment; etc. They can provide historical trends in safety performance for a certain location or work unit useful for highlighting appropriate opportunities and priorities for safety improvement.

$$LTI = \frac{Number\ of\ hours\ absent\ from\ work}{Number\ of\ worked\ hours} 10^6 \tag{1}$$

$$FI = \frac{Number\ of\ total\ accidents}{Number\ of\ worked\ hours} 10^6 \tag{2}$$

$$FAFR = \frac{Number\ of\ fatalities}{Number\ of\ worked\ hours} 10^8 \tag{3}$$

Leading indicators on the other hand try to detect trends in potential 'precursors' and in safety culture. For a further overview and definitions, see CCPS, 2008. These indicators on the basis of hours worked will not be pursued here; instead we shall develop a picture for the oil downstream industrial sector as a whole. It is interesting to analyze statistics on the severity of recorded accidents, again going decades back to the middle of the twentieth century, based on total number of fatalities and total number of injured people in the sector.

From Fig. 3, it can be observed that in the last three decades, the number of fatality evidences shows a decreasing trend, while the number of injured people increases continuously from the fifties onward reaching a maximum by the end of the 20th century. It seems that in this sector the most effective actions in preventing casualties result in less fatal accidents, while the general improvement in process industrial practice and automation has lower effect on injuries.
The classification of each accident was done elaborating a structured scheme based on the approach of EU MARS (Major Accident Reporting System) reports and considering three macro-categories, namely Organization, Plant/process and Environment. Under the headline Plant/process are grouped the possible causative factors directly connected to hardware and inherent characteristics of the process (see Fig. 4). The area Organization collects causative factors related to human factors at different levels and to the safety management system and safety culture (see Fig. 5). Under the headline Environment were included natural events, domino effects, items related to work place lay-out, machine safety,

ergonomics and other environmental conditions. According to this framework, starting from the direct cause of the accident, it is possible to analyze the accident histories deeper (provided that adequate data are available) in order to identify two/three underlying causes in a sort of causal logic chain that, for example links a direct cause under Plant/process to more distant causes within the heading Organization.

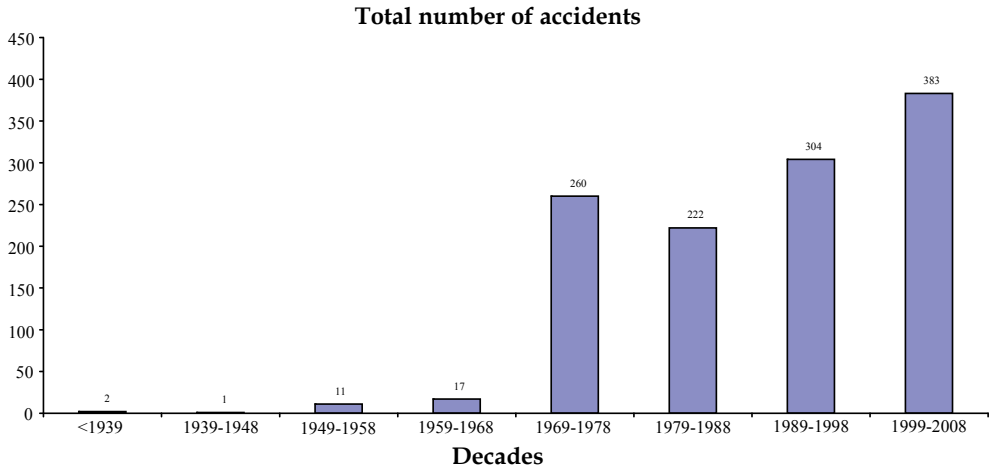


Fig. 1. Global total number of accidents in the downstream oil industry per decade recorded in the TNO FACTS data base.

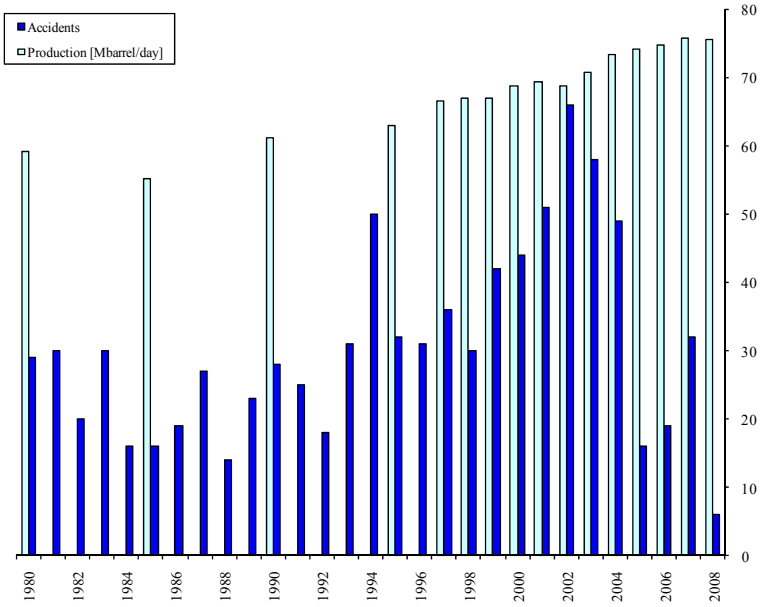
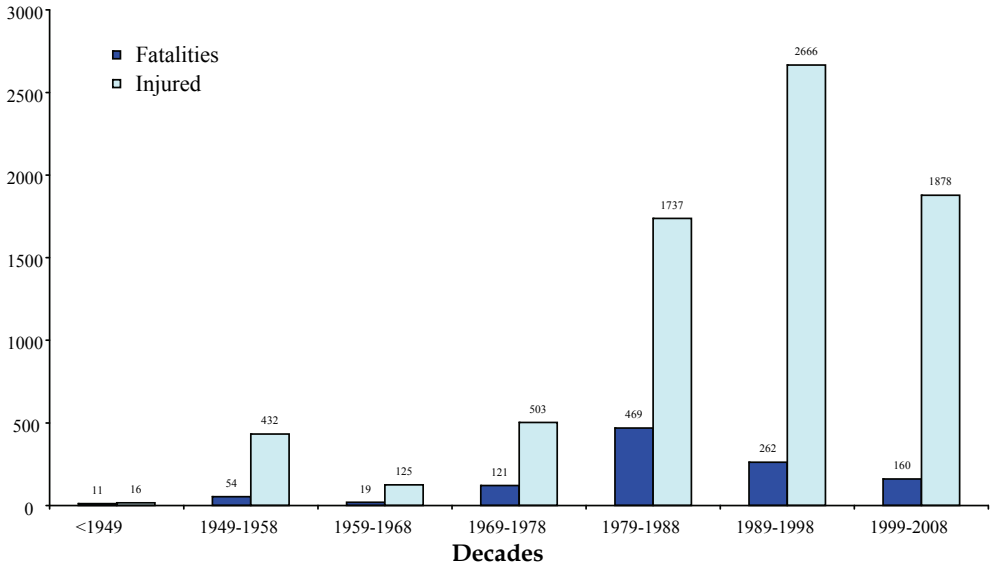


Fig. 2. Oil production over the last few decades and number of accidents.



Number of fatalities and injured people

Fig. 3. Casualties (fatalities and injured persons) per decade found in Database FACTS recorded industrial accidents.

The distribution of the entries among the three main categories evidences that in the downstream oil industry Plant/process cause accounts for 64.8 % of total accidents, Organization for 28.8% and, at last, Environment for the remaining 6.4 %.

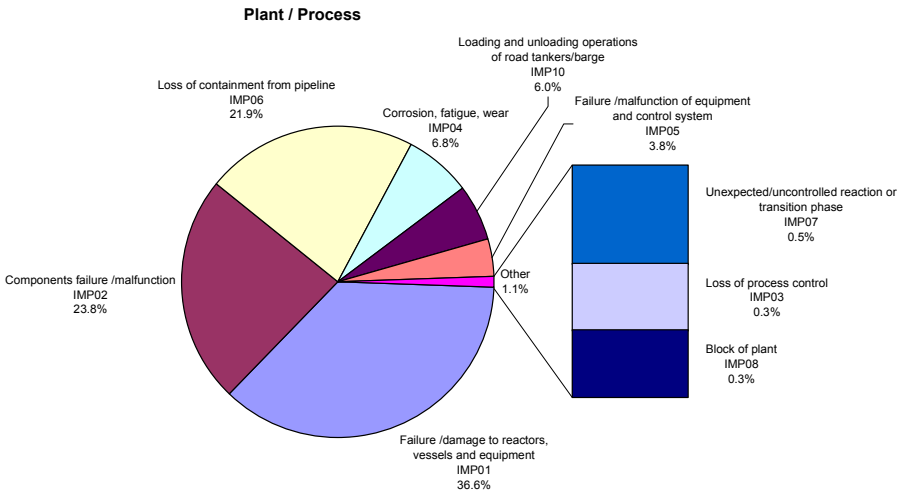


Fig. 4. Distribution of accident causes within the category Plant/process

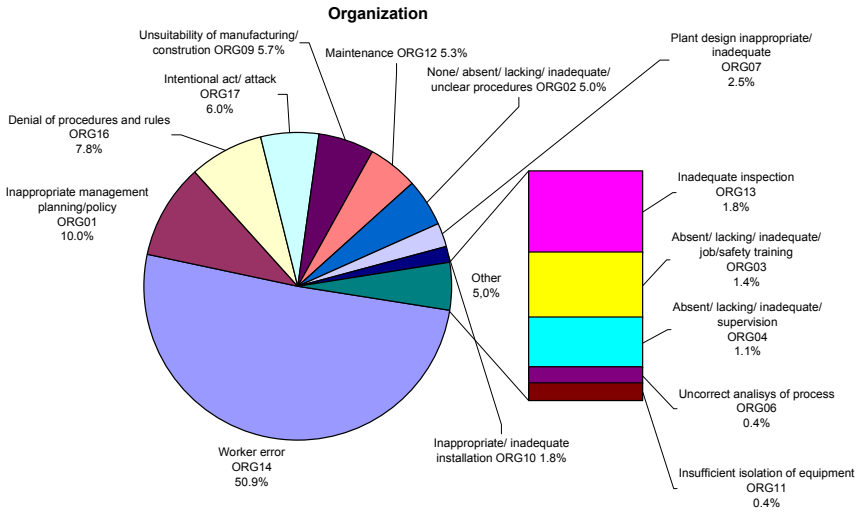


Fig. 5. Distribution of accident causes within the category Organization.

The distribution of the main direct causes is depicted in Figures 4 and 5, respectively for Plant/process and Organization, corresponding to the two items that globally cover more 93.6 % of the accidents. Under each heading three sub-steps were identified as possible underlying cause (recalling the complete classification scheme), allowing evidence to possible deficiencies in the safety management system or in the safety culture of the company.

Dealing with the category Organization (see Fig. 5), it appears that more than 50 % of the accidents can be connected to a form of human error: the analysis shows worker error (unsafe act) to be a significant direct cause as well as a root cause during design stage, operation, and management of the plants, the so-called latent failures. Remarkably, accident analysis as mentioned before revealed that both immediate and root causes are often interacting in parallel and/or in series among multiple, interdependent elements in the complex, high hazard context of a refinery. This has already been concluded in general by Professor James Reason in his many publications, e.g. Reason, 1997 and embodied in his so-called Swiss Cheese concept. It does not help to make risk assessment an easy job!

Accidents can be divided into classes according to the number of fatalities per accident. Although information is not available for all accidents that occurred, it can be assumed that the sample taken here is statistically significant. Data on accidents with fatalities can then be elaborated as suggested by Oggero et al., 2007 obtaining curves in a way similar to societal risk f/N. Calculated is the (relative) probability of occurrence of an accident class exceeding a given number of fatalities, normalized by the total number of accidents involving at least one fatality observed in the sector over a certain period. The cumulative probability data are plotted as a function of the given number of deaths of each class:

$$P_{(x \geq N)} = F_j = \frac{\sum_{i=j}^{n} \nu_i}{\sum_{i=1}^{n} \nu_i} \tag{4}$$

where: N is the lower limit number of deaths in a class (x -axis);
i is class number;
$P_{(x \geq N)} = F_j$ is the probability of an accident class j in which the number of deaths will be ≥ N (y-axis);
n is the total number of classes;
ν_i is the number of accident entries for a given class i.

Figure 6 shows the cumulative probability of accidents with N or more fatalities as a function of N, in the downstream oil industry, obtained on the basis of all selected worldwide accidents and plotted on a log-log axis diagram.

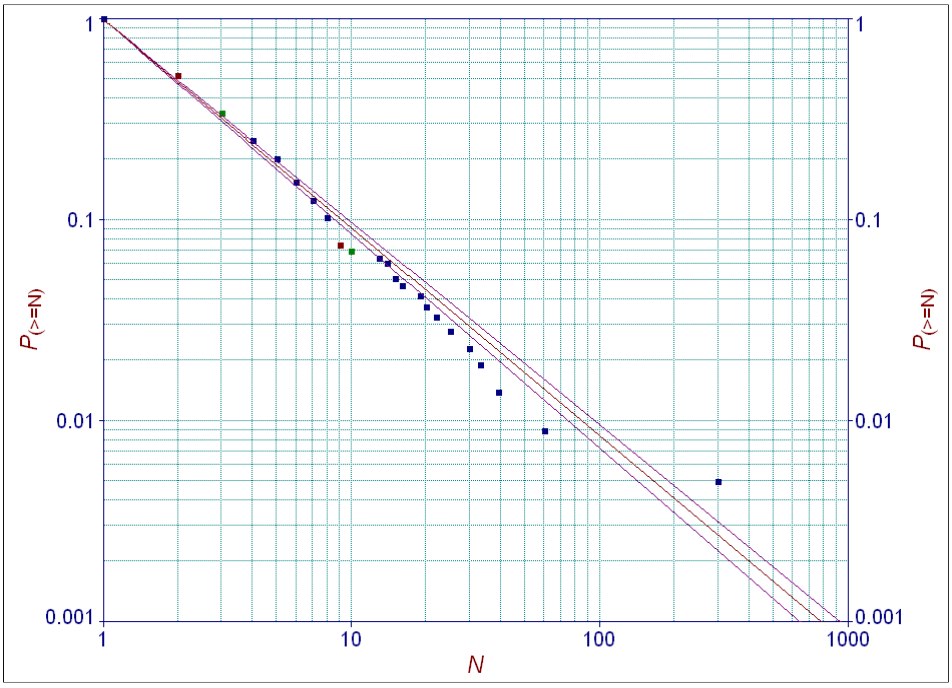


Fig. 6. Cumulative probability of an accident with N or more fatalities as a function of N for all accidents with fatalities in the downstream oil industry (TNO database FACTS entries over the time period 1938-2008).

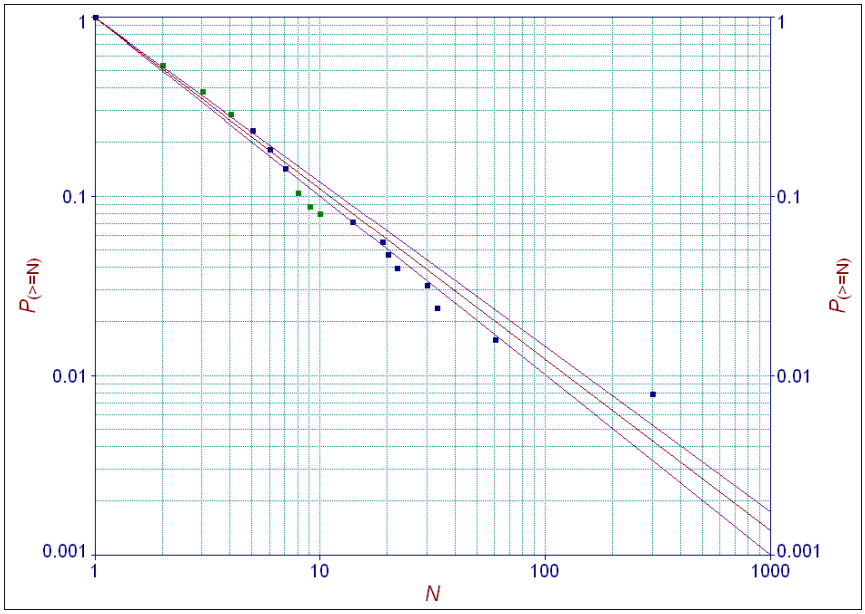


Fig. 7. Cumulative probability of an accident with N or more fatalities as a function of N for all accidents with fatalities in the downstream oil industry, within the category Plant/process (TNO Database FACTS entries over the time period 1938-2008).

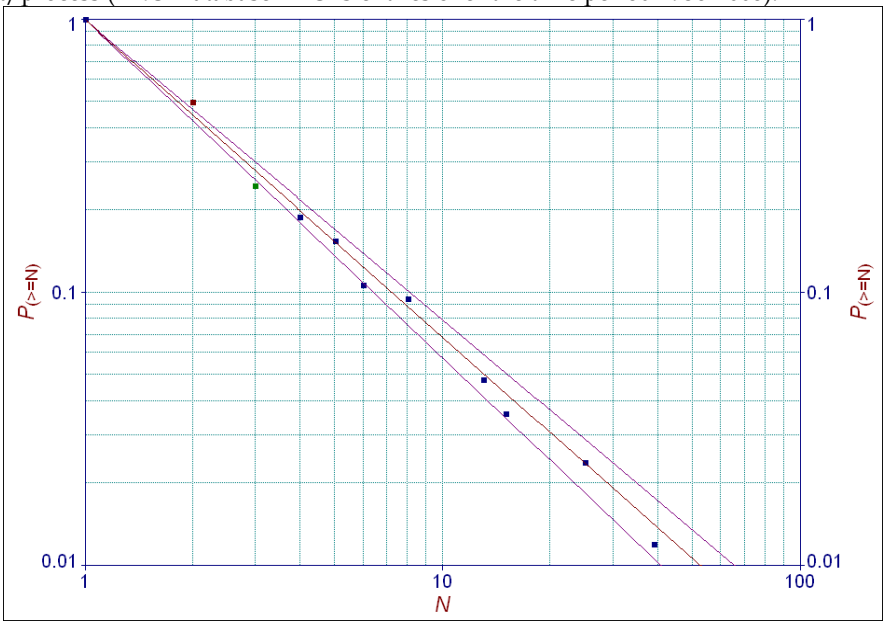


Fig. 8. Cumulative probability of an accident with N or more fatalities as a function of N for all accidents with fatalities in the downstream oil industry, within the category Organization (TNO Database FACTS entries over the time period 1938-2008).

As shown in the same figure, the best-fit provides a $P=N^b$ curve type, with 95% confidence limits, ($r^2 = 0.995$) yielding $b = -1.037$. This finding means that the probability of an accident involving ten or more deaths is about 11 times higher than the one of an accident involving 100 or more deaths. By selecting entries in the two items accounting for nearly all fatalities (Plant/process and Organization), we obtained the trends respectively shown in Figure 7 and 8.

According to this elaboration, based on the concept of cumulative probability of fatal accidents, it can be argued that the consequences in terms of human harm of an oil refinery accident are likely to be more severe, when the accident is primarily connected to a cause in the category Plant/process, rather than in the category Organization.

It is interesting applying the same approach to a specific major hazard activity within the oil industry, namely storage. The statistical elaboration over the same time period allowed obtaining the graph depicted in Fig. 9. The best-fit yields a value b=-0.835, indicating that the consequence of an accidents connected to storage activity is significantly higher than the average for all downstream oil activities. This may have to do with the relative large quantities of hazardous material involved in storage accidents.

It is amply recognized that the ultimate goal of industrial accident analysis is the generation of lessons learned in order to avoid accident recurrence; however, events having the potential of inducing hazardous situations though not materializing after all – the so-called near misses-, can also contribute to the corporate learning and memory (ESReDA, 2001). The challenge of improving the organizational memory and the need for a new look at the sort of injury and accident data that are collected, was already highlighted by Kletz (1993). Problems in actually analyzing case histories have been described by Pasman (2009). In this context shall be mentioned that examination of statistics and causes of minor injuries, hazardous situations and in particular of near-misses can prove even more challenging but also more fruitful with respect to extraction of experience because it is based on an higher frequency of occurrence (see also Körvers et al., 2010). In fact, injury and fatality statistics tend to reflect the quality of the organization in managing personal safety hazards, while near misses point more effectively to process safety hazards.

For the purpose of learning lessons we developed a *Near-miss reporting system (NMRS),* suitable to trace back near-misses to possible deficiencies within the company under examination, including both human and organizational factors. As case-study, this framework was applied to categorize events directly collected in-the-field, over eight years observation, in a major downstream oil company.

According to this approach, the immediate cause classification of near-misses was identified as schematically shown in Fig. 10. The distribution over the categories is roughly similar to the distribution observed earlier in accident causes.

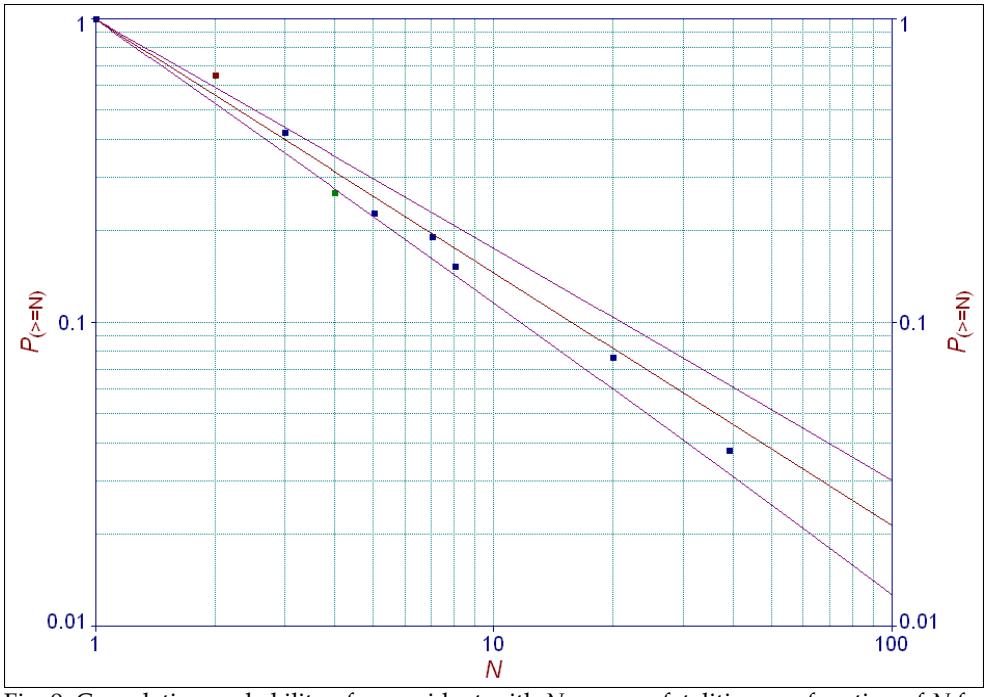


Fig. 9. Cumulative probability of an accident with N or more fatalities as a function of N for all accidents with fatalities, related to storage activity in the downstream oil industry (TNO Database FACTS entries over the time period 1938-2008).

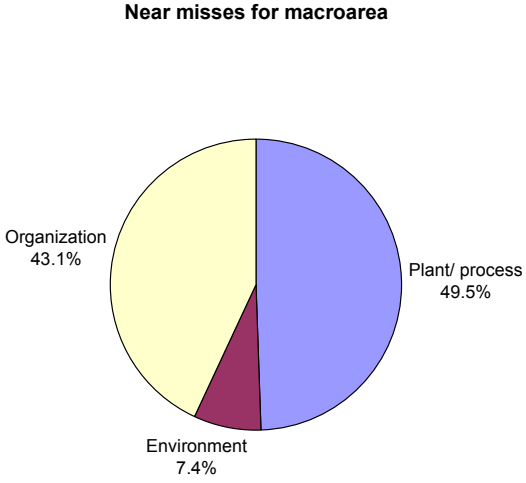


Fig. 10. Near miss classification within the NMRS framework, recorded over an 8-year period in a downstream oil company.

Further analysis can maximize the benefits of a near miss reporting system. Among them, we can mention (CCPS, 2008):

- the utilization of process safety near misses in connection with process safety lagging indicators to build up a process safety performance Heinrich pyramid;
- the evaluation of process safety near misses considering the potential as well as the actual consequences of the event;
- the establishment of ties between the near miss data and the deficient management system, so as to drive system improvement from near miss as well as from actual incidents.

As shown in Fig. 11, an effort was made to identify top ranking direct causes of near-misses over a prolonged period: the knowledge of how frequently these categories are involved in potential accidents can help in improving safety performance. In addition, for every near-miss it is important to conduct a complete root cause analysis while keeping in mind the question why that cause could be present. Component failure or malfunction appeared to be the top cause. However, it must be underlined that the near-miss reporting system evidenced again in several events a combination of root causes.

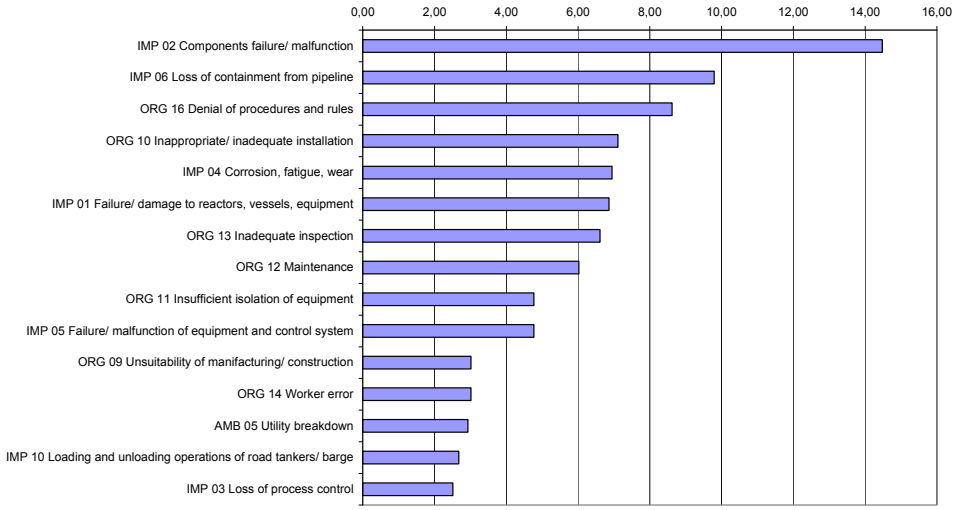


Fig. 11. Top fifteen immediate causes of near-misses (percentage of the entire number of entries) recorded in a downstream oil company over an eight-year period.

3. Some considerations on the human factor

The investigation on many high profile accidents across the process industry, confirmed by the statistical analysis previously outlined, concludes that different human failures can be identified as prominent amongst the root causes. Many of these can be ascribed to poor safety culture, or an inadequate safety management system. Safety culture is hard to precisely define although its absence can be sensed easily observing details in the execution

of work. In the Culture Ladder training programme developed by Van der Graaf, Hudson et al. for Shell E&P, available at the website of the Energy Institute in London, the various stages of culture development are each characterized by a few pithy words (see Van der Graaf et al., 2002 and Hudson et al., 2004). In case leadership is serious about safety the organization will follow. The boss' seriousness about safety is in fact what determines the safety attitude of the worker (Zohar,1980 and 2000).

Human failures were categorised by HSE in the UK as either unintentional (error) or intentional by breaking of the rules (violation): the importance of its definition is connected to possible risk reduction by proper intervention. Generally speaking, the factors influencing accident frequency can be divided into following categories:

- technical factors: low automation, multi-product industries, discontinuous operating cycles, and non-standardized production affect safety negatively, since they require a higher interaction between man and devices. On the other hand, a reduction in individual exposure to severe hazards was reported in case of the introduction of mechanized machinery and equipment in the mining (Asogwa, 1988) and the logging industry (Laflamme, 1988).
- economical factors, e.g., the general economic climate (Saari, 1982), the unemployment rate, labour and social-insurance legislation, (Blank, 1996);
- organization of the work, e.g., management system and performance monitoring, work practice, oversight, communication structure, etc.;
- environmental conditions: about half of the general industrial accidents in Italy are related to conditions at the work place and they could be prevented by rather simple lay-out and protection measures, but in small companies their realization becomes extremely difficult, or even unfeasible because of operating, economic and/or space constraints (Fabiano et al., 2004);
- human factors, both individual and inter-individual, e.g., workload, experience and training, competencies, fatigue, etc.

Petrochemical and process industries experienced in the last two decades a substantial level of change in both terms of production globalization and in the way the business is structured. Current market conditions often make it necessary to apply outsourcing to remain competitive, particularly utilizing external and precarious human resources. In fact, in the last 20 years there has been a significant growth of workers in casual, part-time, subcontract or franchised arrangements, virtually in all OECD countries. Investigation of a possible relationship between personal and process accidents/near miss and temporary work was recently performed, adopting a questionnaire survey, for the definition of peculiar risk factors and for setting priorities to improve safety standards in this context. Data from the structured questionnaire were coded and entered into a database for subsequent multivariate analysis of variance (ANOVA).

The independent variables, whose effects on the number of injuries and their severity were evaluated, included: worker age, job position, training period, on-site experience, temporary contract life, perceived accident cause. Significant results can be usefully analysed by

adopting response surface methodology (RSM). An applicative example related to personal safety is depicted in graphical form in Figs. 12 and 13.

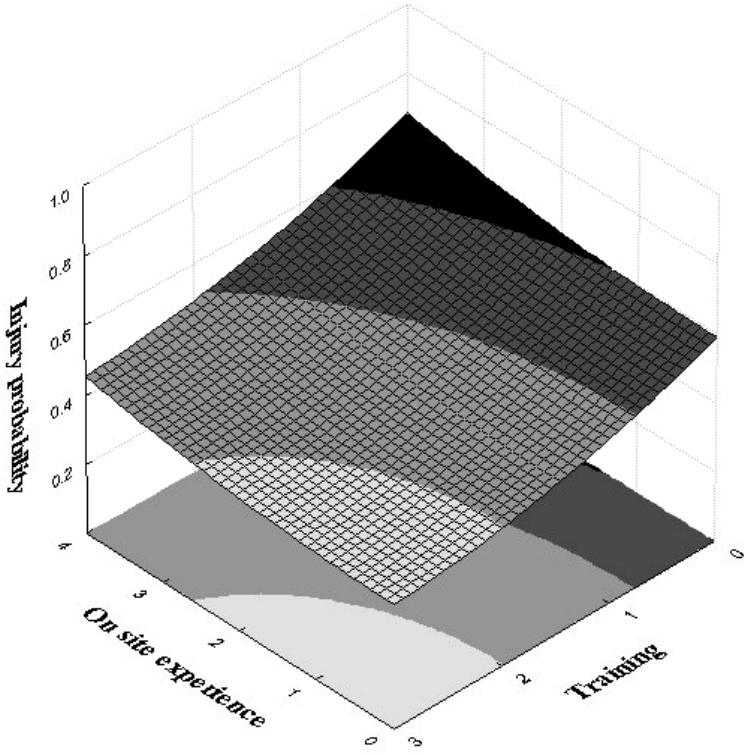


Fig. 12. Response surface for injury probability, as a function of training and on-site experience (Legend: a=less than 7 days; b=7-30 days; c=31-60 days; d=61-90 days; e=more than 90 days; r=less than 3 hours; s=3-5 hours; t=6-7 hours; u=more than 7 hours). (Fabiano et al., 2008).

The significant interaction of the independent variables indicates that an increase of the training period (professional training and job tutoring) greatly reduces injury probability. Notwithstanding efforts by many consultants to train personnel, there is no substitute for a period spent within a process company to gain experience. It must be noted that safety programs include training as a part of the risk management process. However, implementation of rules followed-up by training may often not sufficiently reduce unsafe practices, as safety rules are often seen to apply only in certain situations and as being impossible to follow in the many exceptional situations which are seen to be the reality of the shop floor situation (Hale, 1990). Complacency, not seeing a risk or masculine pride not to fear a hazard plays also a role.

Equally, it seems that staying of the worker on the same job site involves an increase of experience and knowledge of one's duties, reducing the probability of an accident. In other words, even if employees are unaware initially of occupational risk, they can often acquire on-the-job experience. A key aspect is that, as reported by Asogwa (1988), an adaptation period is required for workers to perform adequately in new work assignments and a changed environment, while under conditions of pressure and intensified production (like those that usually correspond to the utilization of temporary workers) this training period is being reduced or eliminated. It must be underlined that the type of human failure influences the choice of the most effective intervention for their reduction. In fact, for violations or mistakes further training of operators may be most appropriate whereas for errors by skilled operators, improvement of the work environment or design of the man-machine interface is more likely to be effective (Ellis and Holt, 2009).

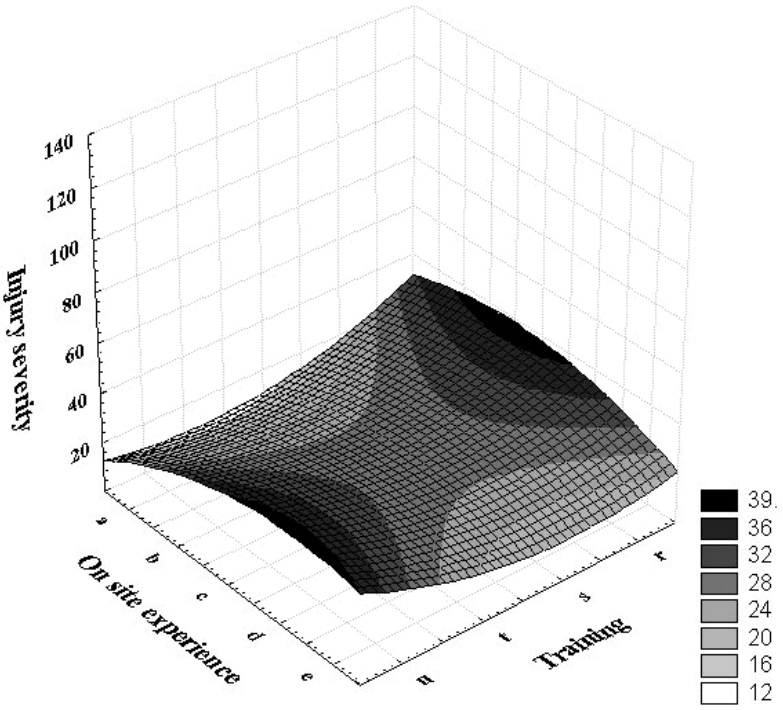


Fig. 13. Response surface plot of injury severity, as a function of training and on-site experience (Legend: a=less than 7 days; b=7-30 days; c=31-60 days; d=61-90 days; e=more than 90 days; r=less than 3 hours; s=3-5 hours; t=6-7 hours; u=more than 7 hours) (Fabiano et al., 2008).

In conclusion, remembering that "to err is human", human error must always be part of an effective training to shape a safety habit and must be considered in writing policy/procedures, so as to achieve maximum understanding and acceptance. It therefore also seems crucial to take human error into account when assessing risk.

4. The advance of risk analysis application

With the development of amongst others crude-oil based petrochemical industry in the late '60-ties of last century, large-scale chemical plants were built in areas with easy access to sea and inland waterways, mostly harbours, to enable transportation of feed stock and products and to find people to run the plants. After several catastrophic accidents, mostly explosions, but also fires and spread of toxic clouds safety concerns arose, which with rising prosperity and consciousness of people over time grew. Risk analysis as a methodology to describe and delimit the risk of chemical process operations was introduced in the mid-seventies to the then newly founded community of Loss Prevention in the process industry. The methodology borrowed from the nuclear industry, was seen by some as a panacea but initially stirred up endless discussions and controversy based on misunderstandings on contents of concepts and differences in definitions. Also, from the start there was an apparent dichotomy qualitative versus quantitative. In 1980 'human factor' became an issue and with good reason many did not believe this could ever be quantified. Moreover a qualitative search for the hazards in a hazard identification step is indeed half the work. The HAZOP method to that end became immensely popular. Quantification is afflicted with uncertainties and where failure of components is stochastic, the determination of risk as a product of damage and likelihood requires a probabilistic approach. Some argued that in safety, where human life may be at stake, once a possibility of mishap was identified, an improvement to the process should be made or an additional safety measure installed. This however adds to the complexity and has its limits. On the other hand a large quantity of stored chemical as existed on quite some places after the scale-up of the industry in the '60-ties, forms an undeniable hazard potential. The protection of the public at large requires therefore safety distances to such risk source, which can extend to far outside the plant's premises despite all safety measures taken. So, quantification of possible effects is a minimum requirement.
However, over the years economic activity and habitation development needed more space, everywhere. As long as space is not a scarce item, safety distances work. Risk quantification can take into account preferential directional effects and weigh the chances of occurrence. This enables assessment of the risk versus the benefit of use of land. No wonder that in densely populated industrial areas as in The Netherlands risk analysis as a tool for land use planning and licensing of plant became so widespread.

Quantification of effects had to be done anyhow, so in the second half of the'80-ties quite some countries initiated research projects to experimentally investigate and model so-called source terms: one- and two-phase outflow of pressurised or cryogenic liquid substances, evaporation of jets and pools formed on different substrates (water, soil), rain-out, dispersion of cold, dense clouds in time and space under different atmospheric conditions. Also radiation intensity of different kinds of fires (jet fire, pool fire, flashing flame, flame ball) was measured and modelled, vapour cloud explosions simulated and boiling liquid expanding vapour explosions (BLEVE) from a bursting tank with pressurised liquid heated by e.g. external fire investigated. The Research Directorate of the European Union got involved and the Europeans could do some cooperative work on gas dispersion and vapour cloud explosion that had body compared also with the field tests sponsored by the Department of Energy in the United States. In the early '80-ties TNO assigned by the Dutch government, composed the series of 'Coloured Books', latest edition 2005, and developed

the software package EFFECTS (TNO, 2007). Damage expressed as fraction of exposed people killed or extent of damage to structures given a threat intensity level was collected in probit relations.

Meanwhile at various places computerised risk analysis had been developed making use of the physical data and models. Known became the commercial PHAST tool (Process Hazard Analysis Software Tool) (DNV SAFETI) but there are others such as TNO's Riskcurves (TNO, 2007). Risk outcome is first of all the probability per year of an (unprotected) person being killed when permanently exposed on a certain location relative to the risk source - individual risk, or as a measure of societal disruption the number of people living locally which will be instantaneously killed – group risk.

As regards safety zones, in Europe the Seveso II directive (EU, 1996) and its Amendment of 2003 is in force implemented in national regulations, which in their application may still show considerable differences. It means that in different European countries safety zone areas for the same risk source can come out differently. Basically, two approaches can be sorted. The former is based on the consequences of credible accidents without detailing quantitatively the likelihood of the accidents. The consequence based approach therefore yields the distance at which the physical and human health impacts reach a threshold limit (i.e. non-reversible health effect or fatality). The risk-based approach adopts the conventional risk definition as a triplet combination of event, probability and consequences. It makes an inventory of possible scenario's with Loss of Containment events, analyzes the subsequent consequences of fire, explosion and toxic dispersion and calculates fatalities in exposed people and materiel damage of structures and the environment. The results are presented in the form of individual risk and societal risk, respectively calculated as probability of becoming a fatality over a period of e.g. a year when exposed at a certain location with respect to the risk source and the probability over a period (e.g. year) of exceedance of the number of fatalities due to an incident at an industrial activity as a function of that number. The individual risk data can be combined to iso-risk contours on a map; the cumulative probability F versus number of fatalities N as F/N- or societal risk curve for that activity. In general, a probabilistic approach results in use of less land for safety zoning than fixed effect distances and hence is more economic if probabilities are sufficiently low. The last few years there has been a trend towards the risk-based approach as was already the case in the Netherlands since the mid-80s. In such case beside the severity of consequences the probability of occurrence of an incident, and the density and extent of vulnerability of exposed people, structures and environment is considered. Given the activity complies with safety standards, the result of such risk assessment are decisive for land use planning and licensing. In 2003 the European Working Group on Land Use Planning EWGLUP, was founded which obtained the mission to map the differences in land use policies in Europe with respect to process industry risks, to suggest improvements in methodology and to guide steps to obtain a higher level of uniformity, see EWGLUP, 2003.

After the tragic Bhopal disaster in 1984 and later the Piper-Alpha oil rig calamity in the North Sea in 1988 process safety got a boost all over the world and risk analysis got applied more generally. Beside the communities sticking to a qualitative approach by conviction, people using QRA discovering drawbacks and weaknesses uttered criticism. Analysis

reports to convince competent authority to issue a licence were often actually drafted by consultants and after obtaining the license not used anymore in the company to improve safety, although continuing improvement is a cornerstone of the safety management system. Uncertainty in the methods, spread in outcomes and controversy between analysts undermined trust. In people's perception low probability is overshadowed by potential large effects. We shall now first consider some recent developments in the methodology before we shall analyse weaknesses and failures of QRA closer.

5. Recent improvements of the state of the art

Hazard & Operability study, HazOp (Crawley, 2000) and related methods such as 'What, if' had proven their merit since the early '70-ties. Going through a plant's Piping and Instrumentation Diagram by section and answering in a multidisciplinary team continually the same guide word questions is time consuming and tiring and may miss the overall top down view. However it identifies hazardous situations and initiating events, and hence provides triggers for improvement, but not a conceptual structure.
In the middle of the '90-ties in the United States Layer of Protection Analysis, LOPA, (CCPS, 2001) was introduced to the process safety community as a simplified risk assessment tool. It became in a short time very popular in industry. This was also because it fitted perfectly together with the then new standard IEC 61511, the first on a probabilistic basis, specifying levels of reliability of Safety Instrumented Systems (SIS) by applying the SIL (Safety Integrity Levels) analysis for reducing various categories of risk for the process sector to a tolerable value. By the way this norm states that any safety instrumented function design shall take into account the human factor. We can trace back to the norm EN61508 to define as "human error those human action or inaction that can produce an unintended result". So, according to this the following items are to be considered:

- the design of a safety integrity function and the assessment of process hazard and risk shall include a detailed evaluation of human factor and any credit taken from human intervention;
- the availability and reliability of the operator action are to be detailed in the Safety Requirement Specification (SRS) and quantified in the performance evaluation for the SIS;
- SRS must detail any action needed to ensure a safe state should a fault be detected in the SIS, considering all relevant human factors;
- SIS design should include all human factor requirements for safe operability, maintainability and testability.

LOPA is examining the functioning of safety measures in a process section given an initiating event which progressively would upset the system. A layer is defined as a subsystem (sensor, processor, actuator) counteracting the process deviation and trying to get the process back in a safe state. Once a layer fails the next will come in to action. Given an installation the team performing the HazOp and identifying the most probable and serious initiating events can carry out subsequently one or more LOPAs also involving the operating crew, to check the adequacy of present safety measures or ones additionally to be