Journal of Hazardous Materials 71 (2000) 375–394

Journal of Hazardous Materials

www.elsevier.nl/locate/jhazmat

Risk informed resource allocation policy: safety can save costs

Hans J. Pasman [*]

TNO, P.O. Box 6006, 2600 JA Delft, Netherlands

Abstract

During economic doldrums, decision making on investments for safety is even more difficult than it already is when funds are abundant. This paper attempts to offer some guidance. After stating the present challenge to prevention of losses in the process industries, the systematic approach of quantified risk assessment is briefly reviewed and improvements in the methodology are mentioned. In addition, attention is given to the use of a risk matrix to survey a plant and to derive a plan of action. Subsequently, the reduction of risk is reviewed. Measures for prevention, protection, and mitigation are discussed. The organization of safety has become at least as important as technical safety of equipment and standards. It is reflected in the introduction of a safety management system. Furthermore, the design process in a pro-active approach is described and the concept of inherent safety is briefly addressed. The concept of Layer of Protection Analysis is explained and also the reason why it is relevant to provide a cost–benefit analysis. Finally, after comments regarding the cost of accidents, the basics of costing and profitability are summarized and a way is suggested to apply this approach to risk-reducing measures. An example is provided on how a selection can be made from a number of alternatives. © 2000 Elsevier Science B.V. All rights reserved.

Keywords: Investment; Profitability; Risk matrix

1. The safety challenge

In pioneering new approaches, new concepts, and new materials, the community of engineers has been faced with catastrophic mishaps including over-estimation of the strength of structures. In fact, for the engineer to have become mature, it means to be able to design and build a technical installation that will be able to produce for what it

[*] Tel.: +31-15-269-48-25; fax: +31-15-262-73-19; e-mail: veldhoen@do.tno.nl

0304-3894/00/$ - see front matter © 2000 Elsevier Science B.V. All rights reserved.
PII: S0304-3894(99)00088-6

has been designed for with sufficient quality against an economical price. For the chemical engineering community, it also implies that the substances and materials produced and packaged are to be of benefit to the user and society and not detrimental. Hazards shall be curbed and hazardous materials shall remain contained.

The paradox is that in the 70s and 80s, with the increase of knowledge of the science of safety and engineering and the decrease on the frequency of accidents, the requirements of the general public to suppress accidents went up. It led to more stringent legislation as, e.g. by OSHA and EPA in the US and the Seveso-II directive in Europe. It also led to industry initiatives as Responsible Care™. In the US in 1985, the American Institute of Chemical Engineers founded in 1985 the Center for Process Safety in New York with about 100 corporate members. In Europe, this was followed in 1992 by the creation of the European Process Safety Centre based in the UK; EPSC has currently 35 member companies. Slowly, awareness has become apparent regarding Safety, Health and Environmental protection, i.e. the SHE-measures have become important and shall be initiated by the highest level of management of the company. These shall not be left to staff experts, but must be felt and appreciated by the company as a whole. To achieve this is as much a technical as an organizational task and it requires good communication. The human factor is a major element in safety.

In the present era of pronounced market mechanisms and efficiency, the drive is to make production as cheap as possible, to save investment money where possible, and to avoid overdoing measures that just serve to safeguard. History, however, learns that in the end, safety pays well, but it requires the wisdom of a longer-term view to make this truth operational. The major companies of the chemical process industry have learned their lessons, therefore, the requirement for safety experts is to maximize inherent safety and to quantify remaining risks. The downward trends in accident indicators such as the

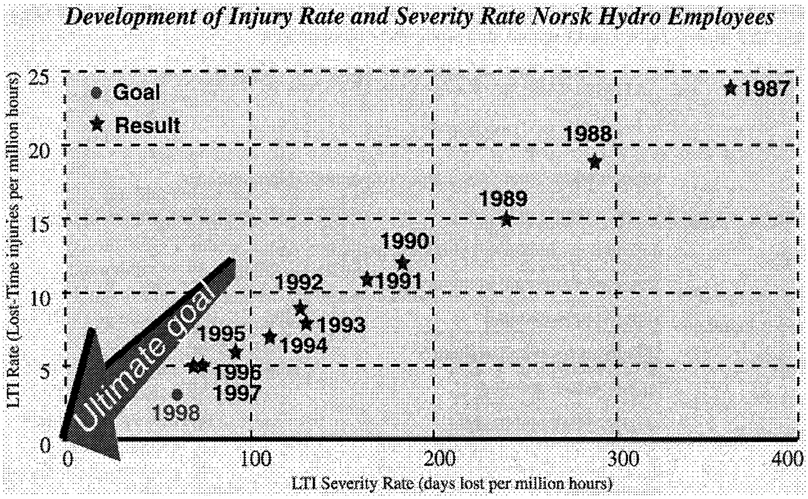


Fig. 1. Safety performance benchmark of the multinational company Norsk Hydro based in Oslo, Norway, showing zero accidents as an ultimate goal.

Lost Time Incident Frequency (LTIF) and the Lost Time Incident Severity Rate have been apparent for many years (Lost time being a worker not able to resume working the following day). In Fig. 1, an example is given from the Norsk Hydro safety annual report 1997 [1].

The goal of zero accidents is coming in sight. The challenge to the engineering community is to further improve safety under severe economic pressure. In the process of renewal and innovation, there is also the challenge to be able to predict the hazards; to determine beforehand both the maximum effect and the probability of occurrence. With the aid of statistical methods, we learn to deal with uncertainty; however, we shall be beaten by ignorance. To protect against phenomena which are fully unknown is almost impossible. Hence, there is a challenge to safety research to further improve methods and gain knowledge.

This paper will address the methodology to consider the costs involved in improving safety and how to make the best judgement given investment limitations.

2. Systematic hazard identification and risk assessment

2.1. Hazards in the process industries

Knowledge of material properties and hazard mechanisms is elementary for safety. In addition, thoughtful design of components like pumps, flanges, etc. is crucial to improve technical safety. Engineering codes and standards contributed much to improvement. For larger installations, the whole system shall be examined; systems analysis is required. Potential accident scenarios shall be conceived, to determine the likelihood and possible consequences. The most complete textbook in this field is: Loss Prevention in the Process Industries [2].

In the 70s, analytical methodology of risk assessment came in use for process installations. In its ultimate form, it became quantified and was called Quantified Risk Assessment (QRA). It was originally derived for nuclear safety studies and is known in that field as Probabilistic Safety Assessment (PSA). QRA developed rapidly in the 80s, specifically the consequence analysis segment. In Fig. 2, the various steps in risk assessment are shown.

Initially, it was seen as a means for governments to more strictly regulate safety. Fierce politically motivated discussions followed. An EFCE Study Group on RA published a report in 1985 [3] of which a second edition came out in 1996 [4]. Today, the methodology is widely used and remains under development. As was shown at a recent CCPS conference in Atlanta [5], it is finally becoming applied to support decision making within a company to assist safety investment policy and to meet the self-set safety goals.

2.2. Identification of an unwanted event

The imaginative capability of a human being for something that he has never experienced before, is rather limited. We, therefore, need techniques to stimulate the

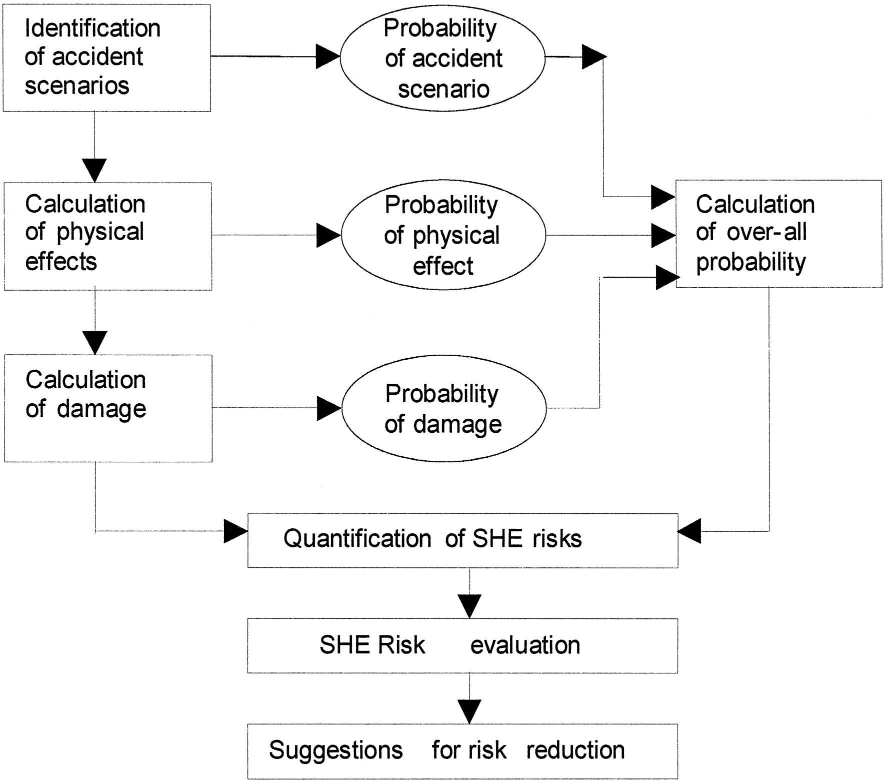

Identification of accident scenarios
Probability of accident scenario
Calculation of physical effects
Probability of physical effect
Calculation of over-all probability
Calculation of damage
Probability of damage
Quantification of SHE risks
SHE Risk evaluation
Suggestions for risk reduction

Fig. 2. Flow diagram of risk assessment: tasked by the Netherlands government, TNO prepared manuals on calculation of physical effects, Yellow Book (1), of damages and their probability, Green Book (2) and the probabilities of accident scenarios, Red Book (3).

human mind and to structure the collection of information. The most widely spread technique is 'HAZOP' (Hazard and Operability Study). The method originated in ICI [6]. On the basis of an engineering line diagram, a team of engineers, preferably with different backgrounds and led by an experienced chairman, would systematically check the effect of deviation from the design conditions. This is done by use of guide words like 'No', 'More', 'Less', 'Reverse', etc. and consideration of possible effects. A drawback is the time needed to perform HAZOP. A recent estimate for a team to do one piping and instrument diagram is a week of roughly 80 man hours [7]. To enhance the productivity of the exercise, there have already been several attempts to support the HAZOP by knowledge-based computer systems tapping from *incident data banks*, as e.g. FACTS [8], or applying a neural network to obtain a learning effect. Alternative identification techniques are the What-If method [9], Index methods [10,11], Cause–Consequence Analysis [12], Failure Mode and Effect Analysis [13]. Helpful in the identification and scenario development is the logic diagram approach of the Event Tree [2], to identify possible hazard effects branching out from an 'Initiating Event' and to show the various possibilities of fire, explosion, and toxic dispersion given loss of containment.

2.3. Quantification of consequences

The calculation of physical effects and the damages due to those effects is also called consequence analysis. For certain critical design features, a quantitative consequence analysis can be required. It consists of two stages: effect and damage analyses. The physical source terms, i.e. the outflow of hazardous material due to a leak, spray release if it was stored as a liquid under pressure, jet flow, pool formation and evaporation, neutral or heavy gas dispersion, heat radiation from pool and jet fire, flame balls, the blast from vapour cloud explosions and BLEVEs, and the fragments of ruptured vessels are calculated [14]. In this field, the concepts are relatively well developed. In The Netherlands recently, the third much improved edition of the Yellow Book [15] has been published (in English) and TNO is about to launch EFFECTS software under Windows which will make consequence analysis easier. The EFFECTS give input to the estimation of damage in the environment, e.g. on the basis of probit functions [16,17]. These are compiled in the Green Book, which has been put into the DAMAGE software.

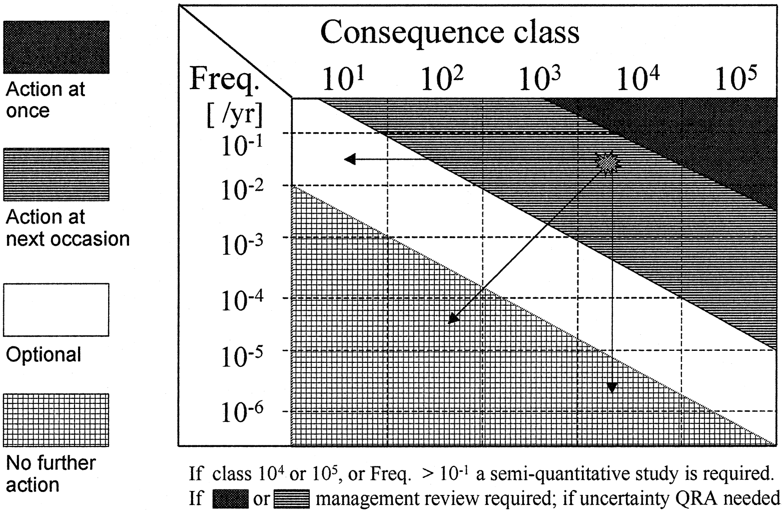
A consequence not considered in great detail is the ecological effect. Attempts to include this in quantitative risk analysis are increasing. Consequences are expressed as the ratio of predicted environmental concentration divided by the no-effect concentration (PEC/PNEC).

2.4. Quantification of expected frequency

To determine event probability, it is necessary to obtain reliable information regarding accident statistics and failure probabilities of piping and other equipment such as vessels and tanks. Fault Tree Analysis (FTA), as developed for Reliability Engineering [18], helps to estimate the frequency of an unwanted ‘Top Event’ from a logic model of failure mechanisms of a system; it does not resolve all uncertainties. In chemical processes, often delays occur as in a runaway reaction. This is not simple to handle in FTA. Likewise, there are dependent and common cause failures also due to chemical problems associated with contamination, fouling, etc. The Human Factor in design, operation, and maintenance provides another element of uncertainty.

2.5. Rapid ranking and the risk matrix

Consider a chemical plant. Because of the complexities of reality, a full analysis of all possible incidents and scenarios is, given limited resources, impractical. Therefore, an order of magnitude ranking of events is desired before any detailed work is to be carried out. A risk matrix approach is often the solution (see Fig. 3). The plant is sectioned and for the various parts, estimates of the order of magnitude of the damage due to an unwanted event and the expected corresponding frequency are estimated. Frequencies range from once in a year until once in 10 million years, while the event damage has been grouped in five classes. These classes have been specified in Table 1



If class 10^4 or 10^5, or Freq. > 10^{-1} a semi-quantitative study is required.
If ■ or ▤ management review required; if uncertainty QRA needed.

Fig. 3. Risk matrix approach of consequence class vs. expected frequency with the areas indicated in which a certain action level is required.

(see, e.g. Refs. [5,19]), with some modification by this author. The financial part of the damage can range from US$10,000 to over US$100 million.

The serious cases, either due to their high frequency or due to their effect, are collected along the first rows and the columns most to the right, while in the upper right corner those appear, which must be addressed without delay in more detail and need to be quantified (QRA).

The company itself will set the risk criteria. The application of QRA for high risk parts of an installation is now starting to produce results for industry and to improve safety. In the off-shore industry, this trend was already visible some time ago (see, e.g. Vinnem [20] who put, e.g. probability values to the strength of semi-confined gas explosions).

Table 1
Consequence class characteristics

Consequence class	Plant personnel	Community	Environment	Financial loss, k$ ($ is US dollar)
10	No lost time	No hazard	No notification	< 100
10^2	Single injury	Odor/noise	Permit violation	> 100
10^3	> 1 Injury	Injuries; local news	Serious impact	> 1000
10^4	Fatality	Injuries; regional news	Severe short term effects	> 10,000
10^5	Multiple fatalities	Fatality; international news	Disastrous effects, long term	> 100,000

After hazards are identified and consequences estimated, risks can be evaluated. This shall be followed by suggestions for risk reduction: prevention–protection–mitigation. Economic pressure, however, will lead companies to perform risk management in such a manner that process safety will be linked to business objectives. In this context, quantified risk analysis is increasingly becoming applied in cost–benefit considerations. Below, we shall see how this can be achieved.

3. Risk reduction measures

3.1. Safety management system (SMS)

The organization of safety has become at least as important as technical safety of equipment. Attention of management to safety matters has proved to be of utmost importance and it is a major improvement in the past 10 years that this has been understood in many large companies. SHE (Safety, Health and Environment) shall be no less important than production, quality, cost, and personnel [21]. It should reflect in installing a safety management system in both production, as in trans-shipment or storage facilities.

The critical ingredient is leadership directed towards the desired level of safety performance. Management systems are comprehensive sets of policies, procedures, and practices designed to ensure that barriers to major incidents are in place, in use, and effective. The functions to be distinguished are planning, organizing, implementing, and controlling. An SMS is therefore a true management system. According to an early CCPS publication on this topic [22], an SMS contains 12 elements:

1. Accountability, i.e. clarity in objectives (who is responsible for what, which lines of communication, how to report and audit)
2. Process knowledge and documentation, records of design criteria and management decisions
3. Critical project review and design procedures for new or existing plants, expansion, and acquisition
4. Process risk management including encouragement of clients and suppliers to conform
5. Management of change of technology, facility or organization, both temporary and permanent
6. Process and equipment integrity (reliability, materials, installation, inspection, maintenance, alarms)
7. Human factors (error assessment, task design, man–machine interface, ergonomics)
8. Training and performance (development of programs, design of procedures, manuals)
9. Incident investigation (near-miss reporting, accidents, follow-up)
10. Standards, codes and laws (in- and external)
11. Audits and corrective actions
12. Enhancement of process safety knowledge by research and improvement of predictive techniques.

Table 2
Principles of inherent safety [23–25]

1. Intensification
2. Substitution
3. Attenuation
4. Limitation of effects
5. Simplification (change early-on)
6. Avoiding knock-on effects
7. Making incorrect assembly impossible
8. Make status clear
9. Tolerance
10. Ease of control
11. Administrative controls/procedures

3.2. Inherent safety

The concept, strongly promoted by Kletz [23–25] starting 15 years ago, is creating great furore. Recently, a CCPS committee published a concept book on the topic [26]. The 11 principles inherent safety is based on are given in Table 2.

A practical checklist is given by Lutz [27].

The EU sponsored project INSIDE [28], in which TNO participated, has brought together a variety of inherent SHE expertise for process development and plant design, since August 1994. The concepts have been developed to produce the Inherent SHE Evaluation Tool INSET [29].

Embracing the inherent safety concept in a company implies breaking down communication barriers between the various subcommunities such as management, engineers, designers, and maintenance personnel. Ashford and Zwetsloot [30] advocate a technology options analysis in an inherent safety opportunity audit. The experience with such an audit is highly encouraging.

3.3. Layer of protection analysis (LOPA)

To evaluate safety of existing installations or plans for a new plant — after developing a risk matrix and focusing on the major issues — severity of consequences and likelihood of undesired events are quantified where necessary and thus mapping risk. The next step is to perform layer of protection analysis (LOPA), i.e. defining which independent protection layers (IPLs) are in place (see Dowell [31]). The concept of LOPA can be depicted as in Fig. 4. It can also be considered as series of independent layers of defense against undesired events and their effects. The first layer can be process design and the mechanical safety system including pipe specifications, relief valves, etc. On top of that, an organizational safety system is put in place with procedures, an SMS, quality designers, quality operators, and maintainers, etc. Then a basic control system follows with process alarms and operator supervision. The next layer of defense will be that of critical alarms and manual intervention. The probability of human error leading to hazardous situations can be lowered by a layer consisting of

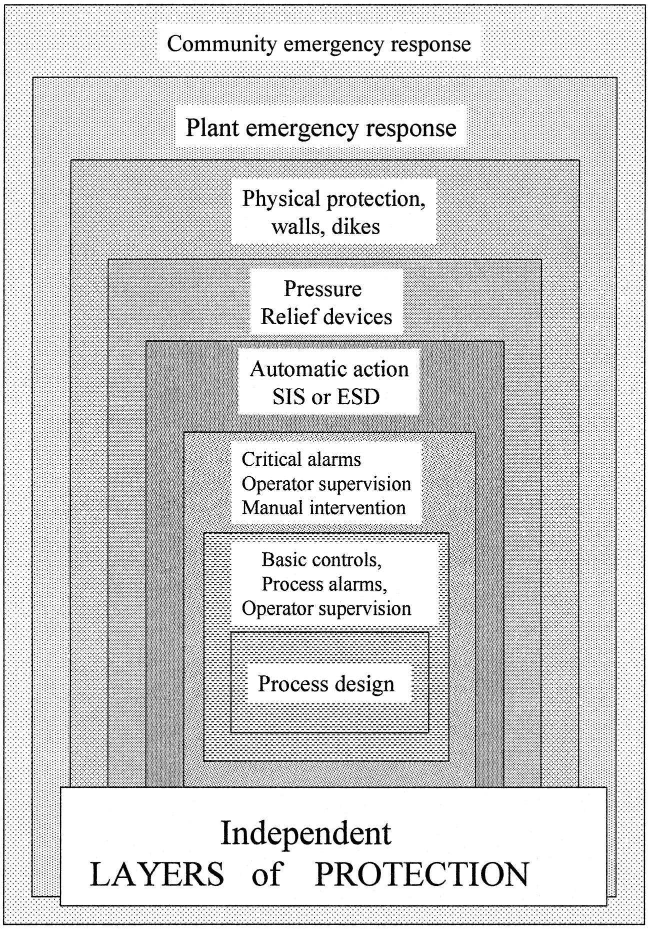


Fig. 4. Independent layers of protection around a process installation (see, for example, Ref. [26]).

an automated system: the safety interlock system or emergency shutdown. A further protection layer can be obtained by an emergency pressure relief. Subsequently, a structural safety system can be installed with concrete cubicles, safe haven (off-shore), fire and blast walls, dikes, passive fire protection, etc. As final layers, emergency response planning can be prepared both for the plant and the community outside.

Risk reduction needs to be quantified per identified layer. In the event that layers fail, the impact on the environment shall be considered. As with HAZOP, LOPA is performed by a multidisciplinary team. For each IPL, the Probability of Failure on Demand (PFD) is to be determined. This includes not only equipment reliability, but also human error. A Safety Instrumented System (SIS) or interlock based on a Programmable Electronic System (PES) can also be used as an IPL.

According to standard IEC 61508 (and ANSI/ISA S84.01), it shall fulfil a specified target Safety Integrity Level (SIL) [32]. These run from 1 to 4 corresponding to PFD value ranges from $< 10^{-1}$ to $\geq 10^{-2}$ at SIL 1, to $< 10^{-4}$ to $\geq 10^{-5}$ at SIL 4. At the same time, false alarm rate shall be extremely low.

Establishing the adequacy of protection layers can be combined by studying opportunities for automation, manpower reduction, and other cost reduction at the same time.

The trend will give new stimulus to improving consequence and other models and collecting reliability data. Consequence model predictions on close-in effects should become more reliable and reflect the probabilistic distribution of effect intensity better. Because of automation, this will include the reliability of programmable electronic systems (PES) or what is generally known as computers and software. Certification of emergency shutdown systems and other safety critical systems are interesting topics.

3.4. Maintenance

Maintenance statistics are to be used in the analysis of the effectiveness of the protection layer over the life cycle, thereby maintaining a balance between availability/quality and safety.

Chemical plants are complicated; there are many components sometimes functioning under adverse conditions. A number of companies have created their own information gathering system with the aim to improve inspection and maintenance schemes. Certainly with instalment of process computers and high integrity protective control systems, including redundancy and diversity to avoid common cause failures, reliability considerations are essential. As large investments are at stake and well-chosen maintenance schedules can reduce cost significantly, research will continue to improve methods and obtain better data. An example is Reliability Centered Maintenance (RCM) with which maintenance of pressure equipment can become optimized with respect to availability by applying Failure Mode and Effect Analysis and by subsequent prioritization. A variant based on Bayesian statistic is Structural Reliability Analysis (SRA, developed by DNV). Optimizing for lowest risk is Risk-Based Inspection (RBI). For the process industry the method is still under development [33].

3.5. Design reviews

The design of a new plant will be a focus for further cost savings, both in effort, and in time of realization. By use of computerized tools, the design process itself is producing better results and making more efficient trade-offs. At different stages in the development of a process, several companies have introduced formal reviews on the basis of safety studies in increasing detail as the design progresses (see James and Wells [34]). At the *exploration stage* (conceptual engineering), a process safety study — supported by experiments if required — can help to avoid risky process routes or hazardous chemical intermediates and by-products. Event data banks on accidents may be consulted. At the *process and project specification stage* (basic engineering), significant hazards and their causes shall be identified in order to make necessary design changes timely as soon as a process flow-sheet is available. Management decision on further investment in licensing detailed design and cost estimates is opportune (for an example, see the procedure depicted by Falke and Kuschnerus [35]).

When a detailed line diagram and full operating instructions are available (i.e. at the *detailed design stage* and the development of specification), HAZOPs and where necessary more detailed studies shall be performed like FTA and consequence analysis. This shall result in a process safety management audit. At actual *plant construction*, an operability review, and after *commissioning* an operating review (or pre-start-up safety review) shall take place to confirm whether plant operation is consistent with the design basis. An additional design aspect is the consideration of ergonomics such as the location of valves, the accessibility of equipment for maintenance and repair, etc.

The advent of modern computational techniques promises further progress in plant siting and structural design, and the provision of temporary refuge and escape routes for personnel on off-shore platforms.

Mitigation of the effects takes many forms. In Fire Hazard analysis, the obvious goal is to minimize damage; fire protection, therefore, is an established expertise. It can be attempted to dissolve toxic or flammable clouds in water sprays or to lift them by steam curtains.

Also *emergency planning* aims to minimize the consequences of an accident. In an industrial project, it shall be considered at a stage in the design process before plant layout is decided. It follows the same pattern as risk analysis of the plant itself. In addition, the planner shall address two important aspects:

- the emergency organization in acute operation must be able to cope with nonsteady activity with rapid and unforeseen changes: crisis management;
- cooperation with (the surrounding) society is vital during major accidents including the demanding task of provision of adequate information.

Efficient crisis management takes the interaction with the media into account. Powerful information technology tools become available to assist in quick, effective decision making.

TNO prepared a project for the Rotterdam–Rijnmond public regional emergency service. It is linked to fire-brigade, police, medical service and companies. It makes use of new concepts of military command and control information technology. It is based on a geographic information system, displaying maps of the threatened area including actual information on, e.g. toxic release, estimated cloud contours, messages on traffic jams, etc. all in real time. It is controlled from the coordination centre of operations; the latest updates are available to all involved via intranet, enhancing ‘situational awareness’. The infrastructure provides access to data banks and models like TNO EFFECTS, which can be consulted during the incident.

4. The costs of accidents

In 1974, the first International Symposium on Loss Prevention and Safety Promotion in the Process Industries, took place in Delft, Netherlands. Webster [36] pointed out that ‘Safety is Good Business’. At that time, his paper drew little attention and it even had to be renamed as the original title ‘Safety is a Money Spinner’ was not acceptable because of the ethical aspect of safety. However, Webster’s message was clear: in analogy of the

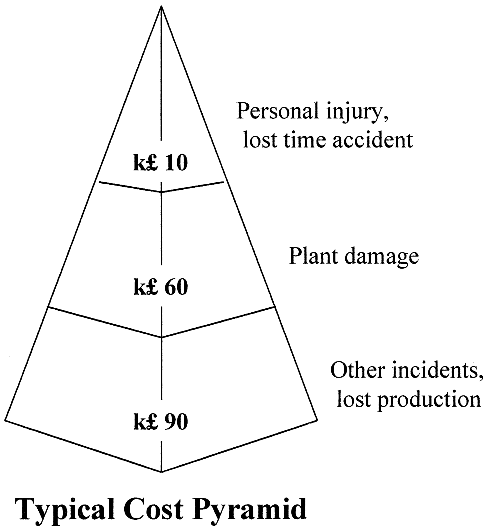


Fig. 5. Accident pyramids show the spectacular serious accidents at the top, but serve to remind us that overall seen total losses at the base are much larger.

well-known accident pyramid, at which one can perceive against one serious accident at the top one to two orders of magnitude larger number of minor accidents and again a larger number of near misses on a lower plane. So when considering cost, the pyramid is applicable as well. Accidents are costly due to lost working days, but also due to lost production, damage to equipment and plant, investigation time and liability claims. The pyramid may be steep: the serious event will be costly, but due to their sheer number minor accidents, which will go past more or less unnoticed, will in total cost more. The pyramid is reproduced as Fig. 5.

Explosions followed by fire can have a notoriously high damage effect on plant. The vapour cloud explosion accident following a massive gas release at the Phillips polyethylene plant in Pasadena, Texas in 1989, is known as the most costly accident so far. The financial losses were at least US$1400 million due to equipment damage and interruption of business. They exceeded those of the disaster of the Piper Alpha, the off-shore platform in the North Sea that was wrecked too by explosion and fire. (For more data on financial losses, see also Ref. [37].)

5. The costs of safety

5.1. Investment and profitability

Standard concepts of process economics are summarized below, while reference is made to Perry's Chemical Engineers' Handbook [38].

Annual sales income minus various types of annual expense minus annual tax and minus expenditures of investment capital (in particular, the first year) produces an annual cash flow A_{CF}. In calculating profitability from cash flow figures, depreciation of assets is taken care of by including in the calculation capital recovery. Profitability can be expressed in different ways. A simple measure is the payback period (PBP) in years. This is the number of years required to accumulate a cash flow equal to the amount of fixed capital cost C_{FC} assuming the scrap value is zero.

A current, more adequate method for determining profitability is calculation through the Net Present Value (NPV) of the project. This takes into account the so-called time value of money. The present worth of money P is related to the value F of that money j years in future through the discount factor, being the reciprocal of the annually compounded interest i over j years:

$$P = F * f_d(j);\ f_d = (j) = \text{discount factor(over } j \text{ years)} = 1/(1+i)^j.$$

When considering the profitability of an investment over a life cycle of n years, the NPV (at the moment of the investment) is built up from the discounted cash flow annual values at years 0, 1 ... n:

$$(A_{DCF})_j = (A_{CF})_j * f_d(j);\ (\text{NPV}) = \sum_{j=0}^{n} (A_{DCF})_j.$$

A measure of profitability is the Discounted Cash Flow Rate of Return (DCFRR), which is the interest r producing up until and including year n a value of (NPV) = 0. It means that the return on investment is such, that at year n, the project generated sufficient money to pay all expenses and taxes and to raise the money to repay the original investment.

Unlike the usual investment that generates income, an investment in safety measures may only prevent a negative cash flow to occur when an accident would happen. The cost terms are the fixed capital cost at the start of operation and cost of maintenance. These have to be placed against the cost an accident would cause in case the safety measures are not taken. However, we do not know whether and, if so, when the accident will happen. In the original state an accident frequency or event likelihood p_0 [year^{-1}] and expected loss D_0 can be estimated producing a risk $p_0 * D_0$. After risk reduction measures are installed, the residual risk is $p_1 * D_1$. The difference:

$$p_0 * D_0 - p_1 * D_1 = \Delta(p * D)$$

expresses the risk reduction. It is usually almost equal to the original risk, since the residual risk is relatively small. The investment results in a reduced expected annual loss cost $A_{LC} = \Delta(p * D)$. (The maintenance cost for the safety devices can be included in the latter.) In analogy with the above formula for the NPV, a discounted loss cost at j years from now can be calculated as:

$$(A_{DLC})_j = (A_{LC})_j * f_d(j).$$

Suppose the life cycle of the project is n years. The safety device investment shall be such that the reduced accumulated discounted loss costs over that period are larger than the investment required, or the loss NPV shall be larger than or equal to the fixed capital cost, C_{FC}, invested in the risk reduction. Hence:

$$(\mathrm{NPV})_{\Delta\,\mathrm{loss}} = \sum_{j=0}^{n} (A_{\mathrm{DLC}})_j \geq C_{\mathrm{FC}}.$$

(Note that in case of cash flow, the negative capital expenditure is included in the terms. This is not the case in the terms of loss cost.) Since A_{LC} has a constant value $\Delta(p*D)$ in all years, the terms of the discounted loss cost at 0, 1,... n years in this equation can further be evaluated to:

$$\Delta(p*D)\left[\{(1+i)^n-1\}/\{i(1+i)^n\}\right] \geq C_{\mathrm{FC}} \text{ or } \Delta(p*D)/f_{\mathrm{AP}} \geq C_{\mathrm{FC}},$$

in which f_{AP} is called the annuity present-worth factor.

As an example, consider a plant built for 20 years. The interest value on investment capital is 10%. The fixed capital cost in safety equipment is 250 k$. The value of $\Delta(p*D)/0.117$ shall then exceed 250 k$ or the risk reduction $\Delta(p*D) \geq 29.3$ k$. Assume p equals one event in 100 years or 10^{-2} [year^{-1}], then on average, the investment is adequate if the possible damage reduction does not exceed 2940 k$. In case the life cycle foreseen would be only 5 years, an investment of 250 k$ would be justified if at the same event frequency, the loss reduction could become at least as high as 6600 k$.

Since safety devices may need to be installed on the basis of government regulations and licensing and not on the basis of economics or because the loss may include elements which cannot be expressed in money value, the above reasoning will often be of no value.

5.2. Cost optimization

When a larger project is studied and safety features are considered, for economic reasons, the costs of the installation shall be minimized over the life cycle of the asset. Total cost C_t can be written as the sum of initial investment costs C_{FC}, maintenance costs C_m, other running costs including insurance C_{ins} and decommissioning costs. In fact, for the life cycle costs as a whole to be calculated, it is required to develop a lifetime scenario the installation could be exposed to in terms of availability, and the capacity profile it will operate on. Other factors will be derived from that.

In case risk reduction is considered, for given investments, residual risk has to be estimated in terms of probability and damage. As above, damage is formulated as the economic loss D as a consequence of an event occurring and the expected event frequency p [year^{-1}]. The expected overall life cycle cost of safety will then be:

$$C_t = C_{\Sigma\,\mathrm{FC}}(p,D) + C_m(p)/f_{\mathrm{AP}} + C_{\mathrm{ins}}(p,D)/f_{\mathrm{AP}} + p*D/f_{\mathrm{AP}}.$$

Both investment costs, maintenance, and insurance costs are a function of the event probability tolerated, the first two increasing with risk reduced, the latter decreasing. Total cost can be plotted as a function of risk, in which the first two terms are taken together on the curve increasing when the risk decreases, while at the same time, the

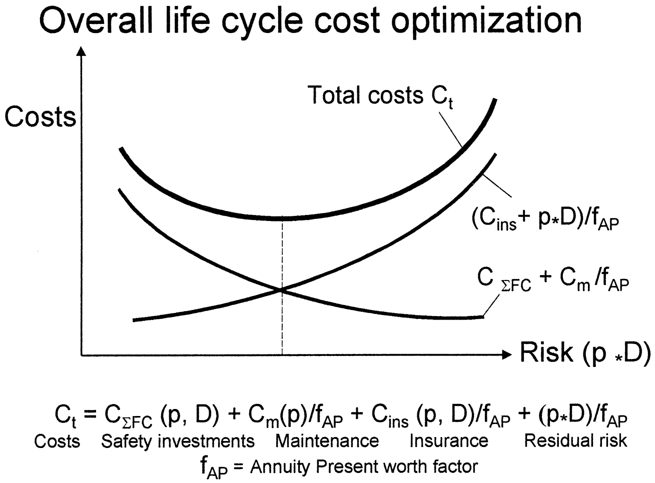


Fig. 6. An optimum can be found in the total costs of safety, when risk reductions are applied.

loss curve increases (see Fig. 6). So at a certain value of the residual risk, the total cost is at minimum.

5.3. Loss of life

A problem is how to take into account loss of life and other grief caused by the accident. When claims are expressed in money value, it is relatively simple. On loss of life, much has already been written (see, e.g. Ref. [38]). It can be expressed as the value of a person's future economic output of earnings, together with a notional sum for 'pain, grief, and suffering' felt by those affected by the death. Along this line, one arrives at an order of magnitude (US\$3.5 × 10^5, 1989) per fatality averted. However, there is more to it. The challenge is to avoid any fatality, even injury as mentioned at the introduction. Therefore, depending on economic strength, the investments to save a life go up to several millions, till, e.g. \$5 × 10^6 (Ref. [39] specified the amounts in Pound Sterling as £2 × 10^5 and £3 × 10^6, respectively).

5.4. The law of large numbers

Probability is a statistical quantity expressing the likelihood of occurrence of the event over a given time. It involves uncertainty. The event likelihood is distributed. For this type of event, the 'memory-less' exponential or Poisson distribution is usually applied. Besides a mean value, there is a dispersion connected to it. The expected mean is the frequency p [per year]. It will show itself when a sufficient number of cases can be considered. So either the statistic concerns a component that repeats itself often enough in the plant or it concerns the plant as a whole, but in that case, the company should own a number of these plants in the world to make the statistics feasible. Depending on the number of cases considered, confidence limits can be specified.

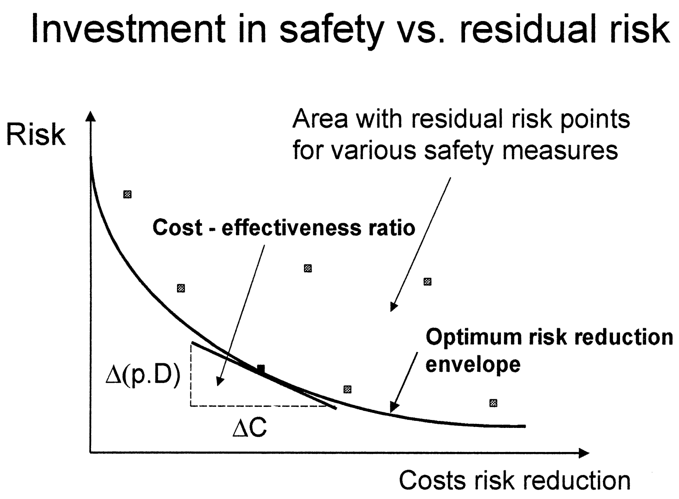

Investment in safety vs. residual risk
Risk
Area with residual risk points
for various safety measures
Cost - effectiveness ratio
Optimum risk reduction
envelope
Δ(p.D)
ΔC
Costs risk reduction

Fig. 7. Graphical means to obtain an overview of the relative costs of various safety measures to curb a risk, and the cost-effectiveness of these measures as derived from the tangent slope of the optimum risk reduction envelope [40].

5.5. Limited scope: selection of alternatives

If a certain case is considered in which risk shall be reduced and a number of options are available, a graphical procedure can be followed. This can be done in a graph of risk as a function of costs of alternative risk-reducing measures (see e.g. Fig. 7 as shown in Ref. [39]).

It is more effective to design a decision matrix. As an example, we can consider a petrochemical plant in which, if no further risk-reducing measures would be taken, a scenario of a minor incident of a leak in piping and a major accident caused by fracture of a tank or vessel could occur. The first could lead to a small explosion followed by a small fire, the other to a strong blast, followed by a catastrophic blaze. Then, risk reduction measures are studied. A relative small investment would reduce the risk of the small explosion; a large investment would be needed to reduce the risk of the heavy

Table 3
Decision matrix for risk reduction measures, minor leak

Options of risk reduction	C_{FC} [k\$]	p_0 resp. p_1 [year^{-1}]	D_0 [k\$] D_1 [k\$]	NPV$_0$ loss (20 years, 10%) [k\$]	$\Delta(p*D)$ [k\$/year]	NPV Δloss (20 years, 10%) [k\$]	C_{FC} + NPV$_0$ loss [k\$]
No measure	0	10^{-1}		$\sim 10^5$	0	0	$\sim 10^5$
Small	100	10^{-2}	10^5	$\sim 10^4$	9000	$\sim 10^5$	$\sim 10^4$
Medium	1000	10^{-3}	10^4	$\sim 10^2$	990	$\sim 10^4$	$\sim 10^3$
Large	10,000	10^{-4}	10^3	~ 1	10	$\sim 10^2$	$\sim 10^4$

Table 4
Decision matrix for risk reduction measures, major leak
~ is approximated value.

Options of risk reduction	C_{FC} [k$]	p_0 resp. p_1 [year^{-1}]	D_0 [k$] D_1 [k$]	NPV$_0$ loss (20 years, 10%) [k$]	$\Delta(p*D)$ [k$/year]	NPV Δloss (20 years, 10%) [k$]	C_{FC} + NPV$_0$ loss [k$]
No measure	0	10^{-3}	10^8	$\sim 10^6$	0	0	$\sim 10^6$
Small	1000	10^{-4}	10^8	$\sim 10^5$	90,000	$\sim 10^6$	$\sim 10^5$
Medium	10,000	10^{-5}	10^7	$\sim 10^3$	9900	$\sim 10^5$	$\sim 10^4$
Large	100,000	10^{-6}	10^6	~ 10	99	$\sim 10^3$	$\sim 10^5$

explosion followed by fire. Calculated are the NPV − values of the original risk and the reduced risks for the situations of a minor and a major leak. The difference loss (Δloss) is always taken incremental, i.e. relative to the previous less stringent option (the line above). The last columns of Tables 3 and 4 contain the sum of the capital investment cost in the risk-reducing measures and the NPV − value of the original risk.

It can be concluded that with the parameter values selected, the risk reduction measures for the medium reduction produce the largest benefit. The large reductions prove to be too costly in both cases. Then also the criterion of NPV Δloss to be larger or equal to the capital cost is not met. The law of the diminishing returns has clearly its effects here as well.

6. Conclusion

Despite the ever decreasing trend in accident frequencies, there is a strong challenge to improve safety. This is not only because expectations have gone up and regulations have become more preventive of nature. Although of course every life lost is one too much, the reason for the challenge is also an increasing financial incentive to improve processes and to produce less hazardous substances. Due to worldwide competition, cost reduction obtains priority and this is a driving factor for down-sizing the work force as well as investment in automation and inherent safe production. In this paper, it is shown that by the technique of, e.g. decision matrices, optimization of cost vs. safety can be achieved. Since this results in a larger demand for models and data, there is also a challenge to improve scientific risk assessment methods.

Notation

AIChE	American Institute of Chemical Engineers
BLEVE	Boiling Liquid Expanding Vapour Explosion
CCPS	Center for Chemical Process Safety (AIChE, New York, USA)
DNV	Det Norske Veritas
EFCE	European Federation of Chemical Engineering
EPA	Environmental Protection Agency, USA
EPSC	European Process Safety Centre (EFCE, Rugby, UK)

EU	European Union
FTA	Fault Tree Analysis
HAZOP	Hazard and Operability Study
HF	Human Factors
HSE	UK Health & Safety Executive
IChemE	Institution of Chemical Engineers
IPL	Independent Protection Layer
ISO	International Organization for Standardization
LOPA	Layer of Protection Analysis
LTIF	Lost Time Incident Frequency
NPV	Net Present Value
OSHA	Occupational Safety and Health Administration, of the US Department of Labor
PES	Programmable Electronic System
PSA	Probabilistic Safety Assessment (nuclear energy)
QRA	Quantified Risk Analysis
RA	Risk Analysis
SHE	Safety, Health and Environment
SMS	Safety Management System
TNO	Toegepast Natuurwetenschappelijk Onderzoek (Applied Scientific Research)
UN	United Nations
US(A)	United States (of America)

Acknowledgements

The critical remarks of my colleagues at TNO, Jitse Schaafsma, Gerard Opschoor, Rolf Perié and Nettie Veldhoen for the improvement of this paper are acknowledged.

References

[1] Hydro's safety report for 1997, Norsk Hydro Corporate HES, Oslo, Norway, February 1998.

[2] F.P. Lees, Loss prevention in the process industries, hazard identification, assessment and control, 3 Vols., 2nd rev. edn., Butterworth/Heinemann Oxford, ISBN 0-7506-1547-8, 1996.

[3] Cox, A.P., Risk analysis in the process industries, secr., EFCE Publ. Series No. 45, IChemE, Rugby, UK, 1985.

[4] R. Turney, R. Pitblado, Risk assessment in the process industries, 2nd edn., IChemE, Geo Davis Building, Railway Terrace, Rugby CV21 3HQ, UK, ISBN 0-85295-323-2, 1995, pp. 165–171.

[5] W.G. Bridges, T.R. Williams, Risk acceptance criteria and risk judgment tools applied worldwide within a chemical, Int. Conf. and Workshop on Risk Analysis in Process Safety, CCPS (AIChE), Oct. 21–24, Atlanta, USA, ISBN 0-8169-0737-4, 1997, pp. 545–557.

[6] C.D. Swann, M.L. Preston, Twenty-five years of HAZOP's, J. Loss. Prev. Process Ind. 8 (6) (1995) 349–353.

[7] F.I. Khan, S.A. Abbasi, Mathematical model for HAZOP study time estimation, J. Loss Prev. Process Ind. 10 (4) (1997) 249–257.

[8] L.J.B. Koehorst, An analysis of accidents with casualties in the chemical industry based on historical facts, Sixth EuReData Conf. on Reliability Data Collection and Use in Risk and Availability Assessment, Siena, Italy, TNO-ref.no.88-340; also 8–12 Oct. 1990, FACTS, a database for industrial safety, Eurocourse, ISPRA, Italy, 15–17 March 1989.

[9] R. Schumacher, R. Pitblado, S. Selmer-Olsen, Next generation risk management, Process Safety Progress 16 (2) (1997) 69–71.

[10] Fire and explosion index, Corporate Safety and Loss Prevention, Dow Chemical, 1976.

[11] D.J. Lewis, The mond fire, explosion and toxicity index, AIChE Loss Prevention Symposium, Houston, 1979.

[12] D.S. Nielsen, The cause/consequence diagram method as a basis for quantitative accident analysis, Danish AEC Report RISO-M-1374, 1971.

[13] Procedures for performing a failure mode and effect analysis, Dept. of Navy, Washington, DC 20362, MIL-STD-1629A, 1977.

[14] Methods for the calculation of the physical effects of the escape of dangerous materials (liquids and gases), 1st edn., Parts I and II, Report of the Committee for the Prevention of Disasters, Dir. Gen. of Labour, Min. Social Affairs, Balen van Andelplein 2, 2273 KH Voorburg NL, 1979.

[15] Methods for the calculation of the physical effects Yellow Book, CPR 14E 3rd edn., Parts I and II, Report of the Committee for the Prevention of Disasters, ISSN: 0921-9633/2.10.014/9110, Sdu, available at MEP-TNO, P.O. Box 342, 7300AH Apeldoorn, Netherlands, Fax: +31-55-541-98-37, 1997.

[16] Methoden voor het bepalen van mogelijke schade (Methods for the determination of possible damage) Green Book, Ministry of Housing, Physical Planning and Environment, CPR 16, le druk 1990, ISSN 0921-9633; available at MEP-TNO, P.O. Box 342, 7300AH Apeldoorn, Netherlands, Fax: +31-55-541-98-37.

[17] R.F. Griffiths, The use of probit expressions in the assessment of acute population impact of toxic releases, J. Loss Prev. Process Ind. 4 (1991) 49–57.

[18] D.F. Haasl et al., Fault Tree Handbook, USNRC NUREG-0492; see also Guidelines for Chemical Process Quantitative Risk Analysis, 1989, Center for Chemical Process Safety (AIChE), 345 East 47th Street, New York, NY 10017, ISBN 0-8169-0402-2, Jan. 1981.

[19] J. Gillett, Rapid ranking of hazards, Process Energy, Feb. 19, 1985.

[20] J.E. Vinnem, On the sensitivity of offshore QRA studies, in: C. Guedes Soares (Ed.), Advances in Safety and Reliability, Proc. ESREL '97, 17–20 June, Lisbon, Portugal, Vol. 2, 1997, pp. 745–762.

[21] B.C.S. Fröhlich, Safety management systems, IChemE, Davis Building, Railway Terrace, Rugby, Warwickshire CV21 3HQ, UK, ISBN 0-85295-356-9, 1994, pp. 165–189.

[22] Guidelines for technical management of chemical process safety, Center for Chemical Process Safety (AIChE), 345 East 47th Street, New York, NY 10017, ISBN 0-8169-0423-5, 1989.

[23] T. Kletz, Friendly plants, Chem. Engrg. Progr., July, 18–26, 1989.

[24] T. Kletz, Inherently safer plants, an update, Plant Operations Progress 10 (2) (1991) 18–26.

[25] T. Kletz, Plant design for safety, Hemisphere Publ., NY, 1991.

[26] R.E. Bollinger et al., Inherently safer chemical processes, a life cycle approach, in: D.A. Crowl (Ed.), CCPS/AIChE, New York, ISBN 0-1869-0703-X, 1996.

[27] W.K. Lutz, Take chemistry and physics into consideration in all phases of chemical plant design, J. Process Safety Progress 14 (3) (1995) 153–160.

[28] R.D. Turney, et al., The INSIDE project on inherent SHE in process development and design — the toolkit and its application, Hazards XIII: Process Safety: The Future, IChemE Symposium, series no. 141, Manchester, 22–24 April, ISBN 0-85295-388-7, 1997.

[29] The INSET toolkit (Inherent SHE evaluation tool): AEA technology, Eutech Engineering Solutions, INBUREX, Kemira Agro, TNO, VTT Manufacturing Technology.

[30] N.A. Ashford, G. Zwetsloot, An inherent safety opportunity audit/technology options analysis, in: C. Guedes Soares (Ed.), Advances in Safety and Reliability, Proc. ESREL '97, 17–20 June, Lisbon, Portugal, Vol. 1, 1997, pp. 613–627.

[31] A.M. Dowell III, Layer of protection analysis: a new PHA tool after HAZOP, before fault tree analysis, Int. Conf. and Workshop on Risk Analysis in Process Safety, CCPS (AIChE), Oct. 21–24, Atlanta, USA, 13–28, ISBN 0-8169-0737-4, 1997.

[32] M.J.M. Houtermans, D.M. Karydas, A.C. Brombacher, Overview of programmable electronic systems, 9th Int'l. Symposium on Loss Prevention and Safety Promotion in the Process Industries, Barcelona, Spain, 4–7 May 1998, ISBN 84-88167-46-6, Vol. 2, 1998, pp. 905–914.

[33] J.T. Reynolds, The API methodology for risk-based inspection (RBI) analysis for the petroleum and petrochemical industry, Int. Conf. and Workshop on Reliability and Risk Management, CCPS (AIChE), Sept. 15–18, San Antonio, TX, US, ISBN 0-8169-0768-4, 1998, pp. 399–417.

[34] R. James, G. Wells, Safety reviews and their timing, J. Loss Prev. Process Ind. 7 (1) (1994) 11–21.

[35] K.-O. Falke, N. Kuschnerus, Bayer's procedure for the design and operation of safe chemical plants, in: M. Arai, R. Dobashi, (Eds.), Proceeding for the International Forum for safety Engineering and Science (IFSES), April 25–28, Tokyo, 1994, pp. 142–156.

[36] T.J. Webster, Safety is good business, 1st Int'l. Symp. Loss Prevention and Safety Promotion, Buschmann, Elsevier, Delft, Netherlands, June 1974, pp. 41–44.

[37] P. Fewtrell, I.L. Hirst, A review of high-cost chemical/petrochemical accidents since Flixborough 1974, Loss Prevention Bulletin 140, IChemE, Davis bldg, 165–171 Railway Terrace, Rugby, Warwickshire CV21 3 HQ, UK, 1998, pp. 3–9.

[38] R.H. Perry et al., Perry's Chemical Engineers' Handbook, 7th edn., in: D.W. Green, J.O. Maloney (Eds.), McGraw Hill, New York, ISBN 0-07-115448-5, 1997.

[39] A.B. Fleischman, M.S. Hogh, The use of cost benefit analysis in evaluating the acceptability of industrial risks: an illustrative case study, 6th Int'l. Symp. Loss Prevention and Safety Promotion, Oslo, Norway, June 19–22, 1989, 60-1/60-16.

[40] H.A. Merz, H. Bohnenblust, Cost/effectiveness analyses and evaluation of risk reduction measures, 2nd World Congress on Safety Science, Meeting Budapest Organizer, Budapest, 21–24.11.1993, pp. 371–397.