Journal of Hazardous Materials, 4 (1981) 225—234
Elsevier Scientific Publishing Company, Amsterdam — Printed in The Netherlands

PURPOSE AND FRAMEWORK OF A SAFETY STUDY IN THE PROCESS INDUSTRY

T. VAN DE PUTTE

Directorate General of Labour, Voorburg (The Netherlands)

(Received January 30, 1980; accepted March 27, 1980)

Summary

The difference between a remedial and a preventive approach towards safety in general and industrial safety in particular is indicated. After this, a description is given of how a safety study of an industrial object (in the widest sense) can be systematically made. It is emphasized that only a selective approach can be realized in practice. Regarding the methods that can be used in a safety study, special attention is given to techniques for identifying unwanted events. The probability—effect/damage relationship and the consequence of emphasizing low probability-large damage events are also touched upon. Finally, it is argued that the usefulness of safety studies lies especially in optimizing the safety of a given activity, whilst, with respect to decision-making on the permissibility of an activity, the result of a safety study can only serve as *one* of the elements on the basis of which decision-making takes place.

1. Introduction

For centuries it has been man's custom to try, while learning from his mistakes, to prevent the recurrence of such mistakes. Via this trial-and-error method man has succeeded, at the expense of an unknown number of victims, in making a distinction between elements friendly and inimical to him in his environment. This form of action may be labelled curative or repressive.

As technology developed further and the consequences of unwanted events* (incidents, accidents) grew, there gradually developed alongside the above form of action a way of thinking in which an attempt is made to predict everything that can go wrong with a certain system.

In this context, a system means a man-machine system; such as a technical plant including operation, inspection, maintenance, repair, etc.

Once the unwanted events, which often have not occurred before, have

*An unwanted event is interpreted here as a happening in which, through a certain cause, dangerous substances or energy escape from an installation, and may present a serious threat to the health of a person in the vicinity of that installation or may cause damage to a building, installation, etc., situated in that vicinity.

0304-3894/81/0000—0000/$02.50

been identified, efforts are then made to eliminate the possibility of their occurrence or, if this is not possible, to limit the consequences and/or reduce the probability of occurrence. The latter preventive approach is, for instance, quite clearly recognizable in the safeguarding of pressure vessels that came into being in the previous century at the urging of the Dutch "Dienst voor het Stoomwezen" (Boiler and Pressure Vessel Inspectorate), founded in 1855.

Notably in the military field, aviation and space travel, and nuclear technology, various predictive methods have been developed, on the one hand, to optimize the reliability, availability and safety of technological systems, and, on the other hand, to support policy decisions.

More recently this trend has also spread to the process industry.

2. The system to be studied

Before a preventive safety study is initiated, a distinction should first be made between systems to be studied that are unequivocally described and defined, such as storage of a dangerous substance at a given place, and systems that are less well defined and demarcated, such as a tank car, containing a dangerous substance, moving through a changing environment.

This distinction is of great importance to the safety study to be performed, since the lack of demarcation of a system entails that no detailed study can be made of all causes of possible undesirable events, while, in addition, in view of the undefined environment, the damage resulting from unwanted events can be represented only very much as a model. Moreover, in the case of a travelling tank car, all unwanted events, in terms of both probability and consequences, are dominated by the unwanted event in which the tank of the moving car is penetrated as the result of a collision with another object.

When setting up a safety study it is advisable to bear these aspects in mind so as to prevent the study from concentrating on what are, in fact, marginal matters for the safety of the system.

3. The depth of a safety study

The desired depth of a preventive safety study of a system is determined by a large number of factors. Among these, the following may be mentioned.

3.1 The purpose of a safety study

A safety study can be performed on behalf of the choice of process, the optimization of a plant design, or the continuity of the company. In general, the results of the study will be utilized within the company in these cases.

In addition, it is increasingly common that a safety study is — or has to be — performed on behalf of the safety of the workers or the people living nearby, or on behalf of an insurance company. In that case, the results of the study will also be assessed outside the company.

3.2 The development stage of a system

In the development of a system a large number of stages may be identified that vary from the laboratory development and the pilot plant phase to the plans to implement the system at a certain place, and the detailed design of the final system. In a number of these stages it may be necessary to perform a safety study, for instance as a basis for decisions to be taken by the management or licensing authorities. The depth of the study is then determined above all by the information available at that time on the design of the system.

3.3 The experience with the system

As more experience is gained with a given system, there will be more information available on any unwanted events that may occur within that system. This case history has been incorporated in codes, standards, and guidelines, in a number of instances.

The extent to which this is the case for a system to be considered will affect the depth of the preventive safety study to be performed. It should, however, be certain that the system to be studied is identical to the system with which the experience has been gained.

3.4 The potential hazard of the system

The potential hazard of the system is determined by the hazards associated with the substances present in the system, by the inherent hazards of the process to be conducted in the system, and by the process conditions.

With regard to the physical or chemical process to be conducted, it should be investigated by means of a process safety analysis* what hazards may be associated with the process [1]. Some examples are:

— electrostatic charging,
— exothermic reactions,
— formation of toxic or explosive by-products.

The potential hazard of the system under consideration can be expressed by a hazard index. Among others, the following methods for hazard indexing may be mentioned:

— Dow's Hazard Classification Guide for assessing material damage [2];
— the designation system and the hazard indexing system in the Dutch Safety Report Regulation [3, 4];
— sheet G 0701 of the "Dienst voor het Stoomwezen" for the classification of systems in hazard categories [5].

The depth of the safety study to be performed will be closely connected with the recognized potential hazard of the system to be considered.

---

*A report on process (un)safety is at present being compiled by a working party instituted by the Directorate-General of Labour.

4. The safety study

A preventive safety study of a technological system (substance(s), process(es), plant, operation) consists, in principle, of three elements, viz:

(a) The fullest possible identification of events which, from the viewpoint of safety, are unwanted. The causes of these events should be stated at the same time.

(b) The quantification of the physical effects and the possible resultant material and immaterial damage, and also of the probability of the occurrence of these events.

(c) The evaluation of the results of the investigation stated under (a) and (b).

4.1 The identification of unwanted events

The most essential element of a preventive study aimed at a safety level of a system that is as optimal as possible consists in the identification of unwanted events that may threaten or impair the safety of people or property.

Depending on the required depth of the safety study to be performed (see section 3), an identification method which varies from broad to detailed may be chosen, while with regard to the causes of unwanted events a distinction may be made between inductive and deductive methods.

In the case of an inductive method, unwanted events are detected by postulating possible causes that are (in part) derived from events that have taken place (case history).

In a deductive method, deviations that may in principle occur in the system are identified, and only then is it investigated whether causes exist that may lead to these deviations. Once they have been identified, events can be analysed further with the aid of event trees and failure trees.

4.1.1 Inductive identification methods

An inductive identification method investigates, largely by means of a check list [6—10], the causes which may give rise to unwanted events. In this a distinction is made between:

(a) causes having their origin in the system to be considered (internal causes);

(b) causes having their origin outside the system to be considered (external causes).

Examples of internal causes are:

— failures in the supply, discharge and circulation of process materials;
— failures in the fuel supply;
— failures in the electricity supply;
— failures in the cooling water supply;
— failures in the instrument air supply;
— design, construction, fabrication or assembly errors;
— gaskets, stuffing boxes, etc., blowing;

— corrosion (internal and external), erosion, fatigue phenomena;
— mechanical stresses;
— overfilling;
— thermal expansion;
— overheating, undercooling;
— overpressure, occurrence of a vacuum;
— internal explosion;
— exceeding of safe limits by the process;
— operating errors such as incorrect starting up or shutting down, incorrect blocking-in, errors in connecting, incorrect bypassing of safety devices, incorrect valve settings, incorrect draining, incorrect sampling, etc.;
— incorrect inspection, maintenance or repair;
— departure from established procedures;
— fire in the part of the plant under consideration (lagging fire, flange fire, etc.);
— blockage (sublimation, caking), fouling.

Examples of external causes are:
— weather influences (low or high temperature, precipitation, wind, lightning striking, high or low humidity, etc.);
— flooding;
— subsidence (scouring, liquefaction of the soil, etc.);
— explosion and/or fire in the vicinity (pressure waves, fragments, heat radiation);
— unintended mechanical load (collision, falling crane, etc.).

In the case of external causes it must always be investigated whether the external cause is not, in turn, the result of an event in the vicinity which is already of such an extent that any unwanted events in the system under consideration are insignificant in comparison to it.

4.1.2 Deductive identification methods

In a deductive identification method, attention is focused on the system to be studied and by means of a certain technique, an effort is made to detect causes that may result in a disturbance of the system. For the process industry the technique of hazard and operability study has been developed for this purpose [11, 12]. Unlike a P and I review, in which it is investigated whether the designed system can perform its task, in a hazard and operability study an investigation is carried out with the help of detailed information to determine whether the system can function in a different way from that for which it was designed.

To achieve this, guidewords are used to systematically investigate what deviations from the envisaged function may occur, whether causes can be indicated for these deviations, and what the consequences of these deviations may be in a qualitative sense.

Performance of the hazard and operability study defined here is a labour-intensive activity. The technique, which yields a fairly exhaustive survey of

internal causes (see section 4.1.1) of unwanted events, must therefore be applied selectively.

Complex, potentially dangerous plants with which there is as yet relatively little experience, and procedures that are of infrequent occurrence, such as the commissioning of a plant, are particularly suitable subjects of study in this respect.

4.1.3 Event and fault trees

The identification methods described in Sections 4.1.1 and 4.1.2 yield unwanted events which, in a number of cases, have to be further analysed.

Event trees [1] can be used for the more detailed analysis of subsequent events that may follow from an identified unwanted event. Fault trees [1] can be used to gain more insight into the failure mechanism forming the basis of an identified unwanted event. Event and fault trees can likewise be useful aids in the determination of the probability of events occurring (see Section 4.2). The above can be summarized schematically as shown in Fig. 1.

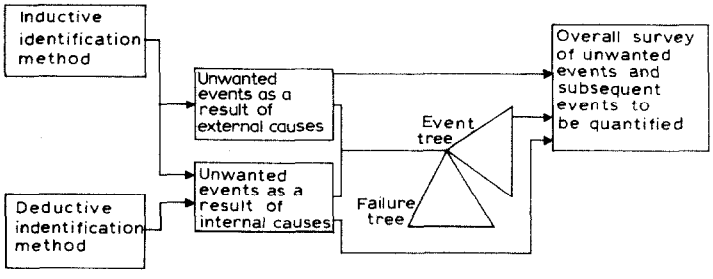

Fig. 1.

4.2 The quantification of consequences and probabilities

As regards the identified unwanted events and subsequent events, it should be investigated as part of a safety study what physical effects and consequent material and immaterial damage may occur and, insofar as this is relevant, what the probability is of these events occurring.

4.2.1 The quantification of consequences

In this context, consequences of unwanted events are divided into two elements, viz. the physical effect and the possible consequent damage from this.

If a combustible gas/air cloud is ignited and in the subsequent deflagration a pressure wave occurs, the peak overpressure and positive phase duration of this pressure wave, which in this case together form the physical effect of the explosion, will have a certain value at a certain distance from the epicentre of the explosion. Depending on the nature of the surroundings, this effect can be translated into terms of damage. With the aid of the report of the 'Committee for the Prevention of Disasters by Dangerous Substances' on methods for the calculation of the physical effects of the incidental release

of dangerous materials [13], it is possible to make an estimate of these physical effects. It must be borne in mind when so doing that the extent of these effects is dependent not only on identified unwanted events but also on, for instance, the prevailing meteorological conditions and the ground conditions (roughness, obstacles). The influence of the latter factor is still difficult to estimate.

If the physical effect is known and the environment in which the unwanted event takes place has been accurately defined, an attempt can be made to arrive at a damage estimate. For the time being, a deterministic approach will suffice, in which the damage is established by means of the limits exceeded [1].

A probabilistic approach, which indicates the probability of certain damage, given a certain effect, would yield a more exact picture. The beginnings of such an approach may be found in the Vulnerability Model of the U.S. Coast Guard [14].

By means of effect and damage estimates it is possible, depending on the purpose of a given safety study, to apply a further selection to the identified, and now thus partly quantified, unwanted events.

4.2.2 The quantification of probabilities

For those events which are worthy of further study, on account of their potential for damage, an effort must be made to estimate the probability of occurrence of calculated damage. This probability is determined from, sometimes, a large number of subprobabilities. This may be clarified by means of an example.

Suppose that following an incorrect action a valve is opened and, as a result, the combustible contents of a plant can disperse into the atmosphere. The probability (p) of, for instance, a worker suffering severe injuries may be determined as follows, assuming that the subprobabilities are independent of one another:

$$p = p_1 \times p_2 \times p_3 \times p_4 \times p_5 \times p_6,$$

where p_1 = the probability of the incorrect action being performed; p_2 = the probability of a certain part of the contents of the plant dispersing into the atmosphere; p_3 = the probability of certain meteorological conditions; p_4 = the probability of ignition at a certain place; p_5 = the probability of a certain pressure build-up as a result of the deflagration; and p_6 = the probability of the presence of the worker under consideration at a certain place.

p_1 and p_2 relate to the identified unwanted event; p_3—p_6 relate to the development of that event in terms of physical effect and damage.

In many cases reliable data for estimating the subprobabilities are not yet available. In view of the relatively great uncertainty in each subprobability, little significance may be attached to the final result in such a case.

Without going more deeply into the problems of estimating probabilities here, attention will be drawn to one other aspect.

In a number of safety studies, extremely small probabilities of certain events or damage are sometimes given. As far as is known, the record is held by a probability of 10^{-53}/year in an LNG study [15]. Particularly with regard to probabilities smaller than 10^{-5}—10^{-6}/year extreme caution is called for. In many cases, a dependence of subprobabilities on each other or a common mode has been overlooked.

A value of 10^{-10}/year for the probability of chlorine escaping through rupture of an above-ground chlorine line must be viewed with suspicion, because the probability of the line being struck by a crashing aircraft is, in itself, of the order of 10^{-7}—10^{-8}/year.

In addition, the assigning of probabilities must always be governed by a law of nature, which we learn by experience, that the greater the consequences of events, the smaller the probability of t .t occurrence [16, 17].

4.3 The evaluation

The evaluation of the results of a safety study will depend on the purpose for which the study was performed. In view of the uncertainty inherent both in the identification (exhaustiveness) of unwanted events and in the quantification of consequences and probabilities (inaccuracy), there is generally little point in testing the result of a safety study in the absolute sense numerically against a safety standard, even assuming that the latter were available.

The "evidence" in the American report Wash-1400 [18] on reactor safety, in which it was demonstrated that nuclear reactors are safer by several orders of magnitude than other technological systems, was impaired while the report was still in the draft stage by an incident in which an inspector set fire to a reactor with a candle, severely threatening the reactor safety [19]. Needless to say, the compilers of the report had overlooked the inventiveness of this inspector. This is not to say that consequently the whole reactor safety study was of no value. On the contrary, precisely through such systematic studies it is possible to eliminate a large number of potential unwanted events, or to limit their consequences, or to reduce the probability of their occurrence. Such a story teaches us, however, that the results of a preventive safety study should be presented with the necessary caution and modesty.

The comparative use of results to detect weak (unsafe) spots in a given system and to spend funds allocated to safety as rationally as possible must be a primary consideration. Considerable time can be devoted to the evaluation of the results of safety studies in the light of risk perception in particular.

Here, only one further aspect will be elucidated. This concerns unwanted events with great potential consequences and a low probability of occurrence. A hundred deaths in traffic, spread out over a year, evoke other emotions and, consequently, other reactions than an event in traffic with a hundred deaths once a year. That this observation may have certain consequences may be demonstrated as follows.

Suppose that someone digging in his back garden comes across an unex-

ploded aerial bomb from the Second World War. Usually this identification leads to a violent reaction in which the house and the neighbourhood are evacuated and the bomb is dismantled by experts. And yet this bomb, together with probably many thousands of others in total, has lain in the ground for more than 30 years without exploding spontaneously. We therefore have here a situation in which an unwanted event may occur with serious consequences but which has a low probability of occurrence. However, the potential consequence fully determines the action to be taken. It will be of little influence, therefore, whether two or three other bombs are encountered besides the first specimen as long as the potential danger does not increase as a result (exclusion of sympathetic detonation).

If this example is translated into, for instance, storage of a dangerous substance into still "virgin" territory — though without taking the comparison so far that storage of a dangerous substance is equated to the presence of a bomb — this implies that installing the first tank determines the emotional assessment of the danger and it matters much less how many (identical) tanks will ultimately be standing there.

From the viewpoint of safety the following rule should therefore apply in the localization of potentially dangerous activities: if in the introduction of several potentially dangerous activities it can be ensured that in not a single case will the consequences of an unwanted event be greater than for each of the activities separately, on grounds of risk, concentration of these activities is to be preferred to their dispersion (concentration of similar risks).

5. Concluding remarks

Summarizing, it may be stated that by means of a systematic preventive safety study it can be illustrated what potential dangers may be associated with a certain system, as a result of which the safety of a system can be rationally optimized.

The depth of the study must take into account the purpose of the study and the nature of the system.

Within a safety study, calculation of the consequences of unwanted events plays an important role. In the first place, it is possible to make a selection among identified unwanted events by means of calculated consequences. In addition, it is true to say that, as the consequences increase in significance, the perception of an unwanted event comes to be determined more by the consequences than by the probability of occurrence and, in the case of very great consequences, almost exclusively by the size of the possible consequence.

The greatest problem in safety studies is the lack of data on the strength of which reliable probabilities can be estimated. Therefore, efforts must be directed towards the compilation of representative data collections, both nationally/internationally (for instance in an EC context) and by the user of a system.

Finally, it should be mentioned that in the decision-making regarding the implementation of a technological system, safety is not the only element forming a basis for that decision-making. In general, economic, social, legal and psychological aspects will play an important part in this. Since these aspects possess, for each individual, different values which cannot be compared in themselves and also vary in time, it will be clear that decision-making is by definition a subjective business. Representatives appointed for this purpose by a firm or by the community should attend to this task; before taking a decision as much objective information as possible must be available on the various aspects mentioned. If this is the case, then the most that can be achieved is a fair decision which all concerned should accept.

References

1 T. v.d. Putte, PT-P 33 (1978) No. 9-531.
2 Dow Chemical : Fire and Explosion Index/Hazard Classification Guide, May 1976.
3 Leidraad betreffende het aanwijzingssysteem voor het arbeidsveiligheidsrapport, November 1979.
4 Leidraad voor het samenstellen van het arbeidsveiligheidsrapport, October 1979.
5 Draft G 0701/79-08 of the Rules for Pressure Vessels.
6 Checklist. A publication of the Directorate-General of Labour, P.O. Box 69, Voorburg, Netherlands.
7 J. Parker, Hydrocarbon Processing, 46 (1) (1967) 197.
8 V.J. Whitehorn and H.W. Brown, Hydrocarbon Processing, April/May 46 (4) (1967) 125, 227.
9 Guidelines for Risk Evaluation and Loss Prevention in Chemical Plants, Manufacturing Chemists Association, Washington, U.S.A.
10 Safety Audits. A Guide for the Chemical Industry, Chemical Industries Association Limited, Alembic House, London, 1973.
11 Hazard and Operability Study. Why? When? How? 1st edn., 1979. A publication of the Directorate-General of Labour, P.O. Box 69, Voorburg, Netherlands.
12 A Guide to Hazard and Operability Studies, 1977, 1st edn. Issued by the Chemical industry Safety and Health Council of the British Chemical Industries Association.
13 Methods for the estimation of the physical effects of the release of dangerous materials. A report by the Committee for the Prevention of Disasters by Dangerous Substances, published by the Directorate-General of Labour, P.O. Box 69, Voorburg, Netherlands.
14 Vulnerability Model : A simulation system for assessing damage resulting from marine spills. NTIS AD-AO 15245, US Coast Guard.
15 LNG Terminal Risk Assessment Study for Los Angeles, California. SAI-75-614-LJ, Western LNG Terminal Company.
16 T.J. Webster, 1st Int. Loss Prevention Symp., Delft, 1974.
17 J.J. de Jong, Summer Conference, Systeemgroep Nederland, Noordwijkerhout, 1979.
18 Reactor Safety Study. An assessment of accident risks in U.S. commercial nuclear power plants. USA EC, WASH-1400, 1975.
19 R.G. Sawyer and J.A. Elsner, Fire Journal, 5 (1976).