Zeitschrift: IABSE congress report = Rapport du congrès AIPC = IVBH Kongressbericht

Band: 11 (1980)

Artikel: Risk management: the realization of safety

Autor: Bøe, Carsten

DOI: https://doi.org/10.5169/seals-11213

Xb

Risk Management — The Realization of Safety

Gestion des risques — réalisation de la sécurité

Risikobehandlung — die Verwirklichung von Sicherheit

CARSTEN BØE
Dr. Eng.
The Royal Norwegian Council for Scientific and Industrial Research
Oslo, Norway

SUMMARY
This report reviews major problem areas in safety concepts related to management of risks and realization of safety targets in practice. In particular the lack of overall safety assessment and attention to human error is pointed out.

RESUME
Ce rapport examine les aspects problématiques des concepts de sécurité relatifs à la gestion des risques et les moyens mis en oeuvre pour atteindre ces objectifs de sécurité. L'absence d'une conception globale de la sécurité est soulignée ainsi que l'attention à porter aux erreurs humaines.

ZUSAMMENFASSUNG
Dieser Bericht überblickt die grösseren Problemgebiete der Sicherheitsbegriffe, die mit der Risikobehandlung und Verwirklichung von Sicherheitszielen zu tun haben. Insbesondere wird auf den Mangel sowohl vom gesamten Sicherheitskonzept wie auch auf menschliches Versagen hingewiesen.

1. INTRODUCTION

Risks have emerged as real constraints to the introduction and development of new technology. This has happened in many fields of engineering. It will happen again in the future.

For several years now engineers have been asked - and sometimes forced - to consider risks related to design in a wider perspective than before. In this respect the engineering profession is changing. There is a mounting pressure from public authorities, and sometimes the general public itself, that risks be taken into account whenever a new installation is conceived and put into operation. In some instances the pressure becomes a demand for all conceivable risks to be controlled. People also anticipate the standards of risk control to be immaculate.

This awakening of our surroundings to risks from technology means that every engineer may eventually find himself responsible for analysing or managing risks in some way. The engineer who has not prepared himself for that moment is going to have problems.

At the root of these problems is the lack of broad experience with risk management in traditional design engineering. Of course such experience will be different in different fields of engineering. Those who are used to reliability engineering and quality assurance work will find it easier to cope with safety problems in a systematic way. The time has now come to exchange experience in how to handle safety problems. A discussion is needed and may in time create a broad basis for knowledge and understanding of risk problems related to design.

The purpose of this report is to focus on this issue, to indicate current major problems and to raise questions which may eventually be answered.

2. THE LACK OF OVERALL SAFETY ASSESSMENT

One of the biggest problems an engineer may run into is the question *'Is this installation safe ?'* Such questions are very difficult to answer for two specific reasons. Firstly, because the question in itself is imprecise and put forward in a language that the engineer does not normally speak. Secondly, because the question comprises the installation as a whole and not only the part for which there are design codes or where some detailed risk assessments have been made. The question, however, deserves a good answer and it deserves a precise answer. It is impossible to address this question, however, without considering some kind of overall safety assessment of the design as a whole.

The lack of overall safety assessment for any installation is a basic problem in engineering. It should really be interesting to know why. Perhaps the main reason is the fragmentary way professional responsibilities are taken care of in the design process? However, in this context the following two statements are important:

- Once a design solution or operational procedure has been decided on and is implemented, the composite installation and its operation represent a level of risk to people, investments and environment which depend on the decisions made from conceptual design to the commissioning of the installation.

- This level of risk is present whether it is analysed or not, whether it is ignored or not, and it is an attribute similar to structural strength or production capacity which can be appraised, changed and controlled.

So the starting point for any discussion on overall safety assessment will be the basic, superior safety requirements which are present at the outset of the design process. The starting point must also include the practical limitations in terms of people, nature and money which exist as boundaries to the actual solution of the design problem. These limitations and overriding requirements have clear and direct consequences for the risk control actions which are to be realized. Furthermore, every decision taken during the design and construction phases limit the scope and contents of the risk control actions.

Figure 1 is an attempt to illustrate how risk control depends on selection, choices and basic requirements. It really describes a risk management process.

In figure 1 there is an unbroken connection between the elements at the top and at the bottom of the figure. The important thing to remember is that every decision taken add to the boundaries on eventual risk control actions which have to be put into force to make the installation meet safety requirements. This is very easily forgotten.

One example of a crucial decision is the selection of a design alternative to be realized. Very often the selection is made according to economic criteria only. Later on one may discover that "*if you want economy, you've got to pay for it*". This happens when practical realities of risk control actions suffuse the design problem and it is discovered that another design alternative was really the better choice. One wonders whether or not for instance the North Sea offshore oil activities are filled with such discoveries. Perhaps the same wondering ought to apply to dam construction or bridge design sometimes?

There is another reason for why the selection of a design alternative is so important. Inherent to every design alternative is the range of risks which have to be controlled and those which one cannot control or does not wish to control. The latter risks are called residual risks. Once a particular design alternative has been chosen, one has also selected a specific range of risks which are to be controlled and a range of residual risks which are impossible or too costly to control. The residual risks one has to live with, and at least they have to comply with the superior safety requirements given at the outset. This is also easily forgotten and sometimes calls for grand mistakes.

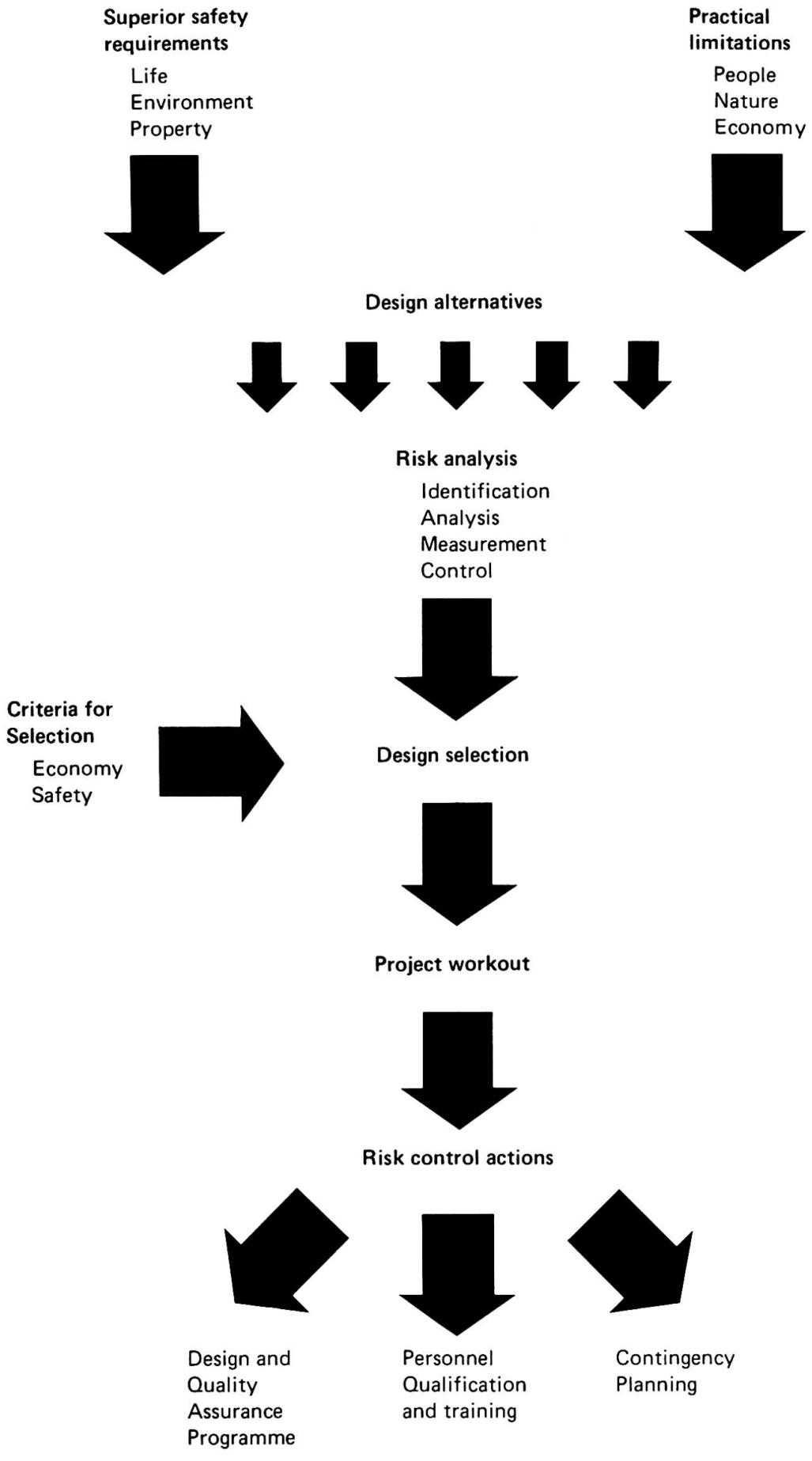

Fig. 1. Risk management process

3. THE IMPORTANCE OF THE CONCEPTUAL STAGE RISK ANALYSIS

To obtain some initial idea of what the overall safety of the different design alternatives may look like, a risk analysis at the very conceptual stage of a design is necessary. Such a conceptual stage risk analysis consists of a broad hazard identification at system level with corresponding analysis and assessment of the major risks to be found for each of the particular design alternatives. The result of this preliminary risk analysis will assist in deciding which risks are to be considered controllable risks and which are to be considered residual risks.

Very little statistical data are required in the conceptual stage risk analysis. The important thing to remember at this stage is that qualitative evaluation of the hazard spectrum is a necessary data base for deciding between residual and controllable risks for each particular design alternative.

It is of course important that the conceptual stage risk analysis is performed when the design is still at the conceptual stage. Then the alternative solutions may be assessed on an overall basis without serious economic consequences to the design project. The first stage risk analysis covers items such as preliminary main layout of the installation, simplified process diagrams, the initial planning of the various construction phases and preliminary outline of operational procedures and their limitations. One should be especially aware of basic design attributes where safety and economy may come into conflict. This allows for trade-offs to be performed at the earliest possible stages of the design.

One should also be aware that such a conceptual stage risk analysis cannot be performed without having a proper risk management organization. However, the experience with overall safety assessment is very small indeed and is found in very limited fields of engineering. A broader base of experience should be found and discussed. One will probably discover that both theoretical work as well as careful analysis of practical applications are required.

4. QUESTIONS RELATED TO RISK CONTROL

Anyone who is tempted to answer 'yes' to the question whether a design is safe, should be prepared to answer further questions related to risk control. Risk control actions are the necessary instruments actually put into force to ensure a certain level of safety. In practice risk control actions easily become ineffective and empty rituals because they are founded on wishful thinking or antediluvian codes - instead of realistic appreciations of actual risks from a design alternative. Realistic appreciations mean systematic risk control actions covering the full range of controllable risks based on causative patterns found in the results of risk analyses for a particular design.

Looking at the practice today, one is tempted to raise several questions. Firstly: *Why is the engineering design of a complex installation so totally independent of the design of the organization which is to run and maintain it ?* In practice there is a big gap between design engineers and those with experience in operating the installations being designed. In some areas this gap is more prominent than others. Perhaps those who

feel this gap to be very real and a hindrance to arrive at a proper design may learn something from those who have bridged this gap.

Another question: *Do codes in general lock design details to specific solutions which preferably instead should be tailored to meet the risks inherent to this particular design alternative ?* A new way to write codes might be to ask for risk assessments of a design. This has been attempted in some fields of engineering, but the experiences seem to be both good and bad.

Thirdly, the last question so far: *Why is the human being almost totally absent from the considerations on design and construction details ?* Too often one finds that the design has become so complex to maintain and operate that human errors seem to be built into the design. One should also give thought to the fact that the actual construction of a design is left to human beings for the most part. No matter how safe a design may look on the drawingboard, the finished product may end up as a quite different thing because the possibility of human error was forgotten. As a general statement it seems that design engineers have a poor understanding of human beings. After all the latter are responsible for operation and maintenance of the installation as well as all vital details in the construction phase.

5. THE HUMAN ERROR SYNDROME

In many areas of technology the basic element in the safety problem is found to be the confrontation between a very complicated technical and social system. After one or more accidents, public opinion creates a pressure on those responsible for something to be done. In such situations it is easy to take one specific problem, eliminate that particular risk and then believe that the causative pattern leading to the accident is broken. One also believes that overall safety has been increased.

In almost all cases one concentrates on concrete technical design problems. These are very easy to recognise: defect structure members, broken down machinery foundations, welding or material failures in piping, defect automation systems etc. By developing reliable technical components based on rigid codes, the risk that a technical failure can develop into a technical breakdown or catastrophy is diminished.

Of course this way of approaching things has a kind of logic of its own. By always increasing and developing technology the risks from technical design failures and defects will always diminish. However, the technical reliability sometimes can be so good that personal vigilance and the use of personal judgement of those operating and maintaining the installation can be deteriorated. It is possible to rely so much on the design of technical systems that one does not maintain the personal qualities of knowledge which are necessary to detect and control an unforeseen situation where the technical system has broken down, or more important, where it is about to break down.

Statistics and reports from the more serious accidents in industry tell us that human failure or lack of knowledge or experience are the main causes of accidents. This is of course only one part of the problem, but it illustrates that at the bottom of it all safety problems are based on human problems. It is difficult to give general recommendations of the human

aspects of safety because people are so different when it comes to abilities, precision, reactions, responsibility and many other qualities.

These difficulties make the study of human errors less exact and complete than studies of technical design failures. Something has nevertheless been learned through systematic studies of human behaviour in different situations. The most important is perhaps that human error is not subject to simple cause-effect relationships. In a hazardous situation many complicated and interactive events can be the consequences of a similar random pattern of events, which are called causes. Then to take one simple cause-effect relationship out of this complicated pattern may just as well serve to hide what actually happened in an accident as to tell the truth. In such undefined situations it is not easy to know what to do.

The thing one usually recommends to do is to emphasize development of safety routines and safety drills to promote selection and education, and of course to tighten responsibilities. This normally describes the extent of any risk control actions in practice today related to personnel. This approach may increase the vigilance and some of the personnel qualifications which are needed to cope with an abnormal situation. However, at the same time it may lead the attention and the actual safety work away from the technical conditions which were created on the drawingboard, and which may change by degree until they reach a point where there is no longer a balance between technology utilized and the human resources involved.

For instance, an installation may have reached such huge dimensions and the technical and physical chain reactions in a process may have become so fast that life saving equipment and contingency plans no longer are in balance with the rest of the technology creating the risks. This problem is well known in industry, offshore petroleum activities, shipping, and air transport.

6. THE ROLE OF EDUCATION AND TRAINING

When attacking the human error problem one may start at two different levels. The first level is the organisation. One may speak of an organisation with a safety conscious climate. An organisation with a safety conscious climate is an organisation which has the ability of internal self-regulation instead of relying on coordination and control from outside. This has the ultimate consequence that those who are concerned with safety, for instance those in the design department and those in the construction team, must work with safety themselves and also have influence and responsibilities in relation to their work.

The second level is the safe operator. He is easier to define than the organisation with a safety conscious climate. It can be done in a systematic way by stating the problem as two tasks:

- to minimize the probability of failure,

- to maximize the probability of correction when an error has occurred.

These two possiblities should be considered by every design engineer. However, there are two approaches to solve this problem. One is the philosophical approach where it is reasoned that no human being is perfect. This results in the belief that all human actions will be imperfect and it is human to fail. One anticipates that there will always be a component of failure in people, and that it sooner or later will show up.

The second approach is that of the ergonomist who tells that human error is caused by lack of adaptation between the abilities of the operator and the demands of the work situation. A human failure will occur when the relation between ability and demand is out of balance. The built-in potential for failure in all human beings is not released until a predisposing condition which creates unbalance acts as a catalyst to realise a potential failure.

This type of thinking has the advantage that - at least in theory - human errors can be completely eliminated simply by eliminating the predisposing condition. This is a challenging task for any design engineer, and current work on human failures and human engineering is performed at this level. The goal is to create the safe operator or the safe man-technology interface where human error can be tolerated. Over the years a lot has been learned in this field. Some of the problems with the safe operator are that too little of that knowledge is used in practice. Now is the time to share experience in this field.

The really difficult safety problem, however, is found at the organisational level. It is very important to solve the safety problem at the organisational level because the safety conscious climate in an organisation determines the possibilities for achieving the safe operator. This means that the simultaneous design of an installation and its operational organisation becomes very important.

Education and training are always necessary risk control actions in relation to human error. Especially important is to evaluate clearly the gap between the level of ability which can be achieved by selection and what is really needed to perform the work. It is also of vital importance to differentiate between training and education based on a complete understanding of the situation, and training based on fixed routines activated by external signals. One finds that in education it is difficult to differentiate between safety and professional matters. Very often a professionally first class work is also the best with regard to safety. However, how one chooses to approach the problem of education and training of people is not a random decision to be left to a personnel department. The approach to training and education should be determined after thorough appreciation of the risks involved with an installation and what kind of risk control measures one wants to take.

The role of education and training in risk control actions seems to be grossly underestimated.

7. SAFE ENOUGH - WHEN DO WE STOP ?

In all safety work one has to stop at some stage for many reasons. One reason is that total and absolute safety cannot ever be achieved for any design. The second is that there are limited amounts of money to be spent on safety evaluation, safety assessment, and improvement of safety. 'Safe enough' becomes a trade-off between what one can afford and what one can accept in terms of risk.

There are no ground rules for assessing how safe is safe enough. In spite of this the question of whether an installation is safe enough turns up every time safety is discussed. For some design details the answer may be found in codes. Codes may define the use of materials, construction procedures, design loads etc. To follow the code in some ways means that the design is safe enough. The codes very seldom give safety criteria for the installation as a whole. Therefore it is usually assumed that if the details are correct, and these are added up, the sum will be correct as well. Unfortunately, this is not the case, and it would be interesting to know how this dilemma has been solved in the various fields of engineering and at different levels of detail in the design of an installation.

Perhaps the only field where an attempt to arrive at an overall safety requirement has been made is the design of nuclear reactors. For reactors design and risk assessment procedures include not only hardware details of the design, but total considerations to the environment and people in the vicinity of the installation. Attempts have been made to quantify safety criteria for nuclear reactors of which perhaps the best known are the Farmer Criterion for radio-active releases and the subsequent site comparisons illustrated in two-dimensional risk diagrams.

8. CONCLUDING REMARKS - MAJOR PROBLEM AREAS

Looking back to Figure 1, it is admittedly difficult to envision a connection between 'superior safety requirements' and the practical realities of design work. It is not easy to be aware of social and political goals when one is struggling to meet with deadlines and codes. The main point in this report is that it really is difficult because risk management is an unknown word to most designers and design managers. Sooner or later, however, a design engineer will find that risk management tasks are put in front of him. Then he needs to know something about overall safety assessment and risk control actions. What is more, he is going to need a systematic way of doing safety work to ensure that a theoretical level of safety is really achieved in practice.

Safety conscious companies, authorities and political bodies have started to ask whether designs are safe. At present very few members of the engineering community can handle such questions.

If only to preserve the credibility of the engineering profession one should start to prepare oneself to answer questions on overall safety. Listening to those who have made attempts at answering is a very good start. Therefore we need exchange of experience and perhaps better education in this field.

The use of risk analysis as a basis for concrete risk control actions is at present a rare thing to find. It has been done, however, and the experiences so far seem to be very promising. The reasons for the scarce use of risk analysis are certainly plentiful. Some of the main reasons may be that this powerful tool is generally very little known, and that there is a belief that risk analysis is a complicated theoretical technique suitable for other people only. Experience with risk analysis, however, shows it to be an extremely flexible technique ranging from simple risk assessment to complicated analyses. Some people who have used risk analysis call it a scientific approach to common sense. The important thing is that the results are used to design risk control actions which are effective and to the point. How this is done ought to be common knowledge.

Human errors are given as causes to all kinds of accidents. However, it seems that too many people resign when it comes to take practical steps to avoid or ameliorate effects of human errors. The role of education and training seems to be grossly underestimated as a concrete risk control measure. Furthermore, design engineers do know too little about ergonomics, behaviour in stress situations, physiological attributes, the time people need to react, reversible failures, converging decision situations etc. This applies to the design work itself as well as construction and operation. Some fields in engineering have gained more experience than others in this respect. They should share their experiences and point out the practical 'tricks of trade' being used.

As one hundred percent safety can never be achieved, the question of how safe is enough always enters safety discussions at some point. Today, one can find several, quite different views on how this question should be handled. It is a field in rapid development. The interesting thing is that at present most of the development seems to follow a kind of trial and error pattern. One should expect that codes will play an important part in this development.