Risk management in the industry

The basic features of an effective safety management system

Waldemar Witt, Hanover

Published in "Technische Sicherheit" 2/2014 Springer-VDI-Verlag.

The safety management of technological processes intends preventive organizational measures and means of emergency preparedness in the technological process itself, as well as in the protective measures and the means for prevention, restriction and elimination of hazardous consequences of industrial accidents.

The requirements of legal and regulatory documents intend to achieve the necessary level of industrial safety and aim to prohibit the dangerous decisions in all stages of the life cycle of the object with an increased level of risk. The phases in this sense include (among others) the planning, construction, equipment manufacturing and installation, its operation, reconstruction, demolition, decommissioning and recycling.

An accident is a result of the process of accumulation of errors.

This includes, among other things, the equipment and system failures, the failure of the protective equipment and emergency systems, process control mechanisms and human errors in all affected processes.

Of course, all preventive, protective equipment and measures should be designed and selected so that they can prevent the significant negative consequences of the accident safely through the coherent and concerted processes.
This requires, above all, a high quality hazard assessment, risk and reliability analysis of such a system taking into account the technological coherence and compatibility of the events, the participation of the people as elements of the system, the characteristic features of the cause and the development of the accidents of the regarded technology.
Here, in this context, the investigation of the dynamic properties of the process followed by the investigation of the extent and forms of accident impacts is emphasized.
In relation to the systems with an increased risk of danger, generally, physical threats such as explosions, fire and dispersions of toxic substances in the atmosphere, soil and water are to be observed. A special place is occupied by radiation hazards.
Of course, particularly the processes, which show a remarkable extent of consequences, carry a probability of human injury and represent significant property damage, pose as a big reason for interest in the analysis.
Due to the large scale of such processes, these should be analyzed by simulation, appropriate case studies or the examination of similar accidents.

Accidents with catastrophic consequences are rare events. Therefore a statistical processing of their parameters leads to a significant expansion of the confidence interval and thus to largely unreliable conclusions and decisions.
The modeling of processes to a better level and under consideration of a maximum number of important factors allows for a much more realistic picture of the potential consequences.

The choice of preventive measures and protective systems is supposed take the dynamic properties of the processes into account, while their skills reliably guarantee a decisive effect on the existing situation.
Moreover, the considerations of the impact of their use are of enormous importance.
Additionally, special attention should be paid not only to the concordance of such equipment and protective systems to comply with legislation and standards, but also their mutual compliance.
A particular problem is the typical mistake regarding the determination of the level of safety and reliability.

The safety level also indicates the possible consequences of failure (human injury, property and environmental damage, etc.) and the abilities through organizational measures and protection devices to prevent, isolate and eliminate said consequences.
The safety level also indicates the probability for these resources to reliably fulfill their function at the right time.

It should be noted that regardless of the high confidence in the effectiveness of the emergency measures and protection devices, an absolute 100% safety cannot be achieved!

The integral characteristics of safety and reliability are represented by so-called technogenic risks.

In the case that the risk is to be regarded as a quantitative measure of danger and danger consequences, the process of analysis and monitoring of risks is a necessary and sufficient condition for the reviews and the decisions in the field of technical plant safety.

Active management of the technogenic risk

Modern technology and advanced technologies become more complex and comprehensive.
The integrity of elements and technological processes increases enormously, which, in turn, leads to an exponentially growing need for safe operational management and technical reliability. As a result, the strengthening of the role of automatic controls makes the production processes in many cases more vulnerable.
The high level of integration and complexity of the system management, emergency preparedness and technical support systems also bring their share of failure probability along with the advantages of such systems. Due to the increasing complexity of the systems, this simultaneously increases the likelihood of human failure in their operation and maintenance.

In many cases, the technogenic risk increases, contrary to the expectations.

In this case, the unforeseeable processes hold special hazards, which aren't intuitively defined or estimated without a thorough analysis. In addition, the desire to reduce the costs of safety in times of economic crisis often leads to decisions that actually cause a fatal increase of risks.
In this context, the technogenic risk management issue regarding multiple parameters or new opinions became a currently discussed topic.

First:
Based on the accident statistics in recent years, it can be said that the reliability and safety will not change in the direction of improvement, due to the increasing complexity of the processing of objects with increased potential risk. It confronts the company with the problem systematically threatening, material, social and even political losses. This is particularly crucial if the local display of the result of such losses could be fatal for some companies or businesses.
This is particularly evident in economic terms. The material loss of a single medium-level accident at a petrochemical plant is a hundred times higher than the total cost of an integrated risk assessment, reliability monitoring and optimal decision making in the field of safe industrial process control.

Second:
In the context of the current economic situation (and beyond), it is quite reasonable to take advantage of technical and organizational solutions in order to achieve an acceptable level of risk for the production. Such solutions are in turn based and optimized on a range of possible losses and the costs necessary for their prevention. Possible losses due to an existing risk represent the extent of negative effects under consideration of their probability (frequency) of occurrence. The costs of avoiding these losses are based on the costs of organizational and technical resources that are necessary to achieve an acceptable safety level of technological process control.

Thirdly:
The business operations should be carried out under compliance with the national and international legislation. However, even the complete compliance with regulatory and normative requirements is not a guarantee against accidents with significant losses. The methodology of the control of technogenic risk is designed to strike a balance between an unacceptable (or acceptable) amount of expected losses and unnecessary (or insufficient) costs of protection- or emergency measures for its prevention.

This concerns the following method:

- Danger- and performance analysis of the properties with a potential hazard on a method basis in accordance with national and international standards and guidelines. Analysis of operational safety, reliability and effectiveness of the protective devices. Project-specific analysis, preparation of the safety report, the definition of fire prevention measures.

- Quantification of the probability (frequency) of the emergence of distinct and characteristic accidents of the scanned objects. It is extremely important that a specific degree of objectivity has to be reached through the consideration of the causal relationships and the development of an accident. In order to reach this, the use of such methods as fault tree analysis and event tree analysis is unavoidable. In rare exceptions, only statistical information may be used. Ranking methods in this application are classified as subjective and unreliable.

- Simulation of the formation of a hazardous environment, development of accidents and their negative effects. Thus, the number of people affected and the economic consequences of the accidents should be determined

- Calculation of such integrated risk indicators, such as the territorial risk, the expected number of casualties, the individual risk, the expected damages and other factors that pose as the basis for the decisions and insurances. Preparation of risk reports.

- Industrial property insurance and liability insurance. It is desirable to make the decisions in the insurance sector on the basis of a qualitative underwriting process, including a versatile integrated risk analysis.

- Risk monitoring as a basis for decision making during the operation and the reconstruction of the plant, changes in business strategy and the insurance. Development of internal corporate standards related to the management of technological risks.

- Independent investigation of accidents and conflicts.

It is obvious that the integrated risk management is based on an information technology and needs appropriate software tools for its realization. The complexity of such software solutions is extremely high. The advantages are obvious. A merging of science, technology and engineering, computer science and legal requirements through such a system provides a new way to bring the safety level of industrial facilities to a maximum attainable level.

Information technology for the safety analysis and risk management

The management of technogenic risks initially contains a classification of technogenic objects with their further assignment to danger groups. For this, usually such methods or processes are used like HAZID (Hazard Identification Study), or the rank identification- or classification on the content's amount of toxic or explosive substances.

This is followed by an investigation and thorough analysis of the object and its operating environment.
During the investigation, the characteristic dangers and performances of facilities (Hazard and Operability Study - HAZOP) were observed under critical failure situations and disorders including human failures. A special place in this case is taken by the analysis of cause-effect relationships of the hazardous processes.
The accident as a fact is nothing more than the completion of the accumulation of errors and faults.
The first requirement for an accident to happen is a change in the process parameters outside the limits of the permissible range but still without loss of control over the entire operation process.
At this stage, a flawless technical functionality of automatic protection devices and correct actions of the technical operations staff ensures successful safety.

Errors and failures at this stage and the previous stages (design, installation, determination of the remaining resources, etc.) can lead to the second stage of the accident development - invalid parameter changes with a complete loss of control. At this stage, correct actions from the staff and effective emergency equipment can avoid serious consequences.

The third stage begins with the damaging and destruction of facilities or technology elements. At this stage, possible manifestations of dangerous physical processes (explosions, fires, toxic-, biological- or radiological contamination,

etc.), injuries to people, property- and environmental damage are to be expected. The accidents may have a catastrophic nature and cause very large, long-term, negative consequences.
The identification of the potential consequences of incidents and accidents is one of the main objectives of risk management.

To assess the impacts of such negative events, the applications of models of negative processes, human injuries, property and equipment destructions with following economic and social impacts are the best practices.

The quality of the modeling, the limits of accepted assumptions in the modeling and the evaluation of their consequences should be within the acceptable confidence interval. Here, a conservative application (worst consequence) is preferred.
A very important aspect of modeling is the transparency and understanding (basis) of the definitions and applications of the models and their input data.

The next stage of risk management is the selection of all possible emergency situations that significantly affect the stable operation or can cause obviously unacceptable loss and damage.
At this stage, it is rational to make the decisions in cooperation with the management of the company and the local and state government.
The informed agreement of all members of such a decision circle is a basis of the acceptable risk. Here, the level of acceptable risk for the individual examined object or the entire operation could be defined.

The next step of the emergency selection is to determine the event probabilities (frequencies) of emergencies for an evaluation period. This requires preparations by experts. However, it is ultimately limited to a relatively simple formalization of causal relationships of the identified risk- and function capabilities of the object in the analysis phase.

The result is a quantification of the probability of an accident based on a developed formal model.

Mostly, the fault tree method (FTA) is used for the evaluation of operational risks, while the event tree method (ETA) is applied to assess the effectiveness and reliability of protective measures.

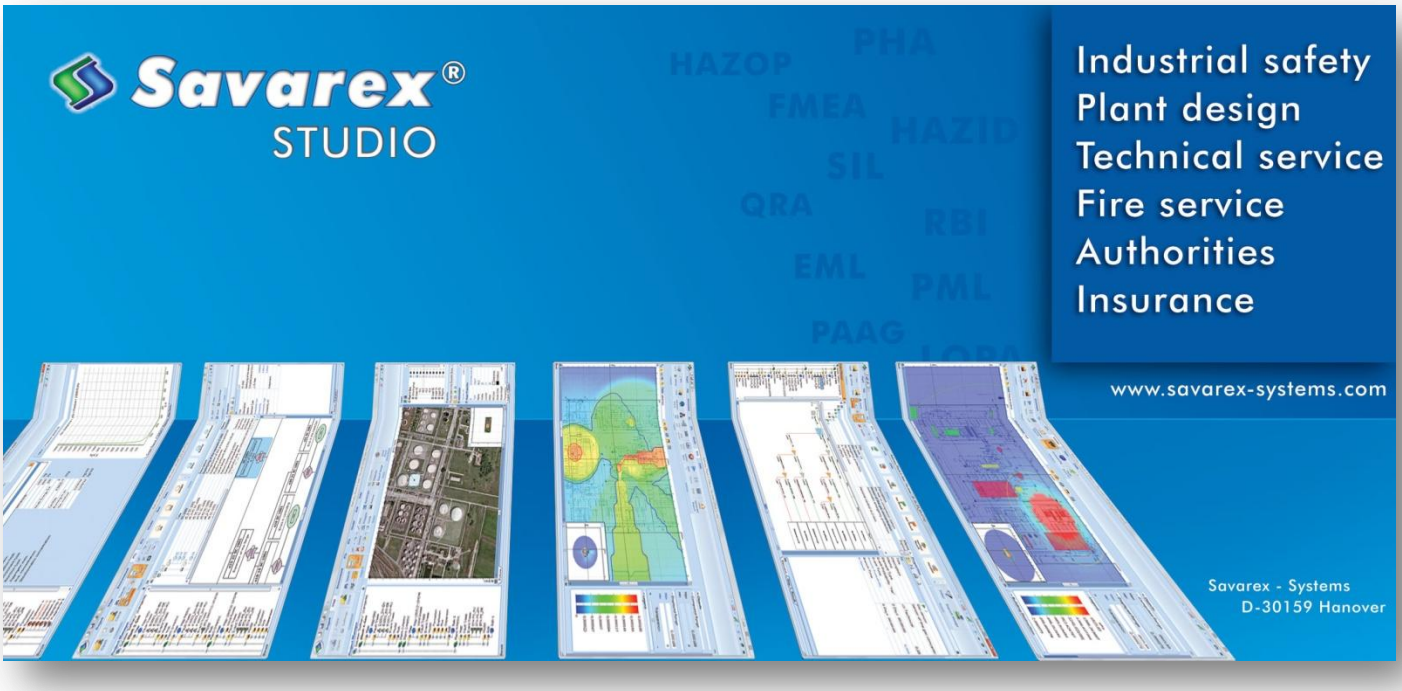
In some cases, the ranking methods are permitted or a quantitative determination of the probability based on the statistical data processing is applicable.
However, it is important to note that the statistics for severe accidents (which are clearly rare events) usually lead to a very large confidence interval and can reject all the efforts of risk management at the level of assumption.
In contrast, a use of statistical data and technical parameters according to the manufacturer and failure data for the individual elements of production (eg, armature, gauges, actuators, etc.) in the investigation of their behavior in the fault tree allow not only for a much more reliable approach to determining the risk, but also help to identify "bottlenecks and gaps" in safety technology and the operations of the object through special analysis methods.

In the final phase of the risk management, the selected emergency situations are evaluated and risk indicators determined. These include the territorial, personal and societal risks, the expected human injuries and the expected property damage. Finally, and based on the iterative methods, decisions are made only for such situations, elements and objects for which the risk has been found to be unacceptable.
Thus, a cost optimization of the safety measures was automatically achieved through such an approach and on the basis of the objectively verifiable material.

The scope of application for this technology stands out in the project analysis, construction, installation, operation and reconstruction of facilities and equipment with a hazard potential. Such findings are also the basis for decisions for industrial insurances or technical inspection institutions.

A special place is taken by this technology in the technical inspection and particularly in a so-called risk-based inspection (RBI). The innovation is shown through the fact that the maintenance and repair work on a large system can be scheduled according to its state of condition, which in most cases significantly reduces the cost of repairs and maintenance while simultaneously increasing the safety level.
The application of the system at Safety-Integrity-Level-examinations (SIL) in various stages of the life cycle of the automatic control is a reasonable and meaningful step to represent the reliability of these systems. In particular, the selection of various technical components, controls and safety devices for such investigations is the best opportunity to also reduce the costs in the project phase.

The Insurance is one of the most effective mechanisms for risk management.
The application of this technology in the determination of “possible maximum losses" (PML), the reporting of the expert or in a qualitative underwriting process allows for



the easy transfer of the insurance process from a financial transaction to an industrial safety technology. In this case, the joint work of the insurer and the insured generates a win-win-situation through a fusion of goals and transparent methods.

The difficulty in implementing this technology and its application are missing (complete or partial) appropriate and effective information systems (software, databases, evaluation methods and models of technogenic risks). As a consequence, there is also a shortage of highly qualified specialists in this field. It should also be noted that for a complete and detailed risk analysis of the company, a lot of information about the objects has to be collected and processed, which is not easy regarding the effort, confidentiality and information specificity.

Despite all the obstacles, all of the problems mentioned above can be overcome very quickly through proper use and proper organization, through which the value of the obtained information and the effects of using this technology will turn out to be several times higher than the costs of their implementation.

Summary

Unfortunately, there are only a handful of software solutions, but which deal only peripherally with the subject of risk assessment though and are missing the field of risk management entirely.
The enormous complexity, lack of know-how and organizational barriers in the preparation of such information technologies and their tools have kept the developers away for decades.
Nevertheless, and after several years of development, the company Savarex-Systems from Hanover has developed the information technology and program system "Savarex Studio" as part of an EU project and has now made it available to the international market. The multilingual and self-sufficient system structure presents the relationships of processes, events, scenarios and evaluations, and offers traceable, complete and rapid safety- and risk assessments among other features.

"Savarex Studio" offers the unprecedented possibility to link all necessary system modules to a closed and complete investigation process with continuous data transfers. All of the necessary modules and data for the assessment, classification and management of the safety level and existing risks of industrial plants and facilities are already implemented.
In addition to the solutions to optimize costs for maintenance and repair work, the program also supports and helps the company in the field of scientific and technical hazards expertise. Thus, among other things, safety reports and emergency plans for industrial facilities with increased potential risks can be created or even risks within a company over the entire life cycle can be estimated or evaluated.

Therefore, through the use of this information technology, a closed loop system with an informative and long-sought after feedback technology is realized, while the promising goal to reach the highest safety- and reliability level for potentially hazardous installations is made possible.

Author

Dipl.-Phys.Ing.-Inform.
Waldemar Witt,
Managing director,
Savarex-Systems
Hanover