David VALIS, Miroslav KOUCKY
University of Defence, Brno, Czech Republic
Technical University of Liberec, Liberec, Czech Republic

SELECTED OVERVIEW OF RISK ASSESSMENT TECHNIQUES

Key-words:

Risk, Safety, Standards, Risk management, Risk Assessment Methods-Techniques.

Summary

As we deal with risk in many aspects and in different phases of the technical object's life cycle, we should choose and apply proper methods for risk assessment. Some of the methods are common and typical, and some of them are rarely used.

The paper presents a general overview of the methods and techniques, which are to be of use in the risk assessment, namely, in the risk analysis. Obviously, we have to take into account such methods applicable for risk reconnaissance as well as the risk treatment. Nevertheless, the methods of risk analysis are the most frequently used and not very well known at the same time. Due to limited space, the paper offers only a general overview and not very deep and comprehensive information.

Introduction

Organisations of all types and sizes face a range of risks that may affect the achievement of their objectives. These objectives may relate to a range of the organisation's activities, from strategic initiatives to its operations, processes and projects, and are reflected in terms of societal, environmental, technological, safety and security outcomes, commercial, financial and economic measures, as well as social, cultural, political and reputation impacts. All activities of an organisation involve risks that should be managed. The risk management process aids decision making by taking account the uncertainty and the possibility of future events or circumstances (intended or unintended) and their effects on agreed objectives. Risk management includes the application of logical and systematic methods for the following:

- Communicating and consulting throughout this process;
- Establishing the context for identifying, analysing, evaluating, treating risk associated with any activity, process, function or product;
- Monitoring and reviewing risks; and,
- Reporting and recording the results appropriately.

Risk assessment is that part of risk management which provides a structured process that identifies how objectives may be affected and analyses the risk in term of consequences and their probabilities before deciding on whether further treatment is required.

Risk assessment attempts to answer the following fundamental questions:

- What can happen and why (by risk identification)?
- What are the consequences?
- What is the probability of their future occurrence?
- Are there any factors that mitigate the consequence of the risk or that reduce the probability of the risk?

Is the level of risk tolerable or acceptable and does it require further treatment? This paper is intended to reflect current good practices in the selection and utilisation of risk assessment techniques and does not refer to new or evolving concepts that have not reached a satisfactory level of professional consensus.

This paper is general in nature, so that it may give guidance across many industries and types of systems. There may be more specific information sources in existence within these industries that establish preferred methodologies and levels of assessment for particular applications. If these sources are in harmony with this paper, the specific approaches will generally be sufficient. Figure 1 well presents the all consequences to understand the position of risk assessment.

1. Principles for decisions about methods for risk assessment

Risk assessment is the overall process of risk identification, risk analysis, and risk evaluation. Risks can be assessed at an organisational level or a departmental level for projects, individual activities, or specific risks. Different tools and techniques may be appropriate in different contexts. Risk assessment provides an understanding of risks, their causes, consequences, and their probabilities.

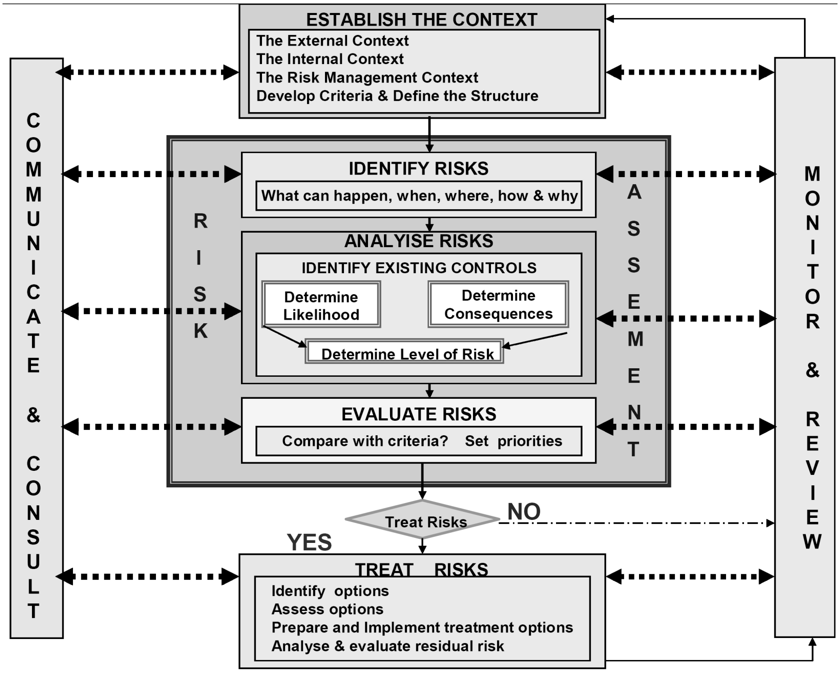

Fig. 1. Risk management process

Risk assessment provides decision-makers and responsible parties with an improved understanding of risks that could affect achievement of objectives and the adequacy and effectiveness of controls already in place. This provides a basis for decisions about the most appropriate approach to be used to treat the risks. The output of risk assessment is an input to the decision-making processes of the organisation.

Risk analysis is about developing an understanding of the risk. It provides an input to risk assessment and to decisions about whether risks need to be treated and about the most appropriate treatment strategies and methods.

Risk analysis consists of determining the consequences and their probabilities for identified risk events, taking into account the presence (or not) and the effectiveness of any existing controls. The consequences and their probabilities are then combined to determine the level of risk.

Risk analysis involves consideration of the causes and sources of risk, their consequences, and the probability that those consequences can occur. Factors that affect consequences and probability should be identified. An event can have multiple consequences and can affect multiple objectives. Existing risk controls and their effectiveness should be taken into account. More than one technique may be required for complex applications. Risk analysis normally includes an estimation of the range of potential consequences that might arise from an event, situation or circumstance, and their associated probabilities, in order to measure the level of risk. However, in some instances, such as where the consequences are likely to be insignificant, or the probability is expected to be extremely low, a single parameter estimate may be sufficient for a decision to be made. In some circumstances, a consequence can occur as a result of a range of different events or conditions, or where the specific event is not identified. In this case, the focus of risk assessment is on analysing the importance and vulnerability of components of the system with a view to defining treatments that relate to levels of protection or recovery strategies. Methods used in analysing risks can be qualitative, semi-quantitative, or quantitative. The degree of detail required will depend upon the particular application, the availability of reliable data, and the decision-making needs of the organisation. Some methods and the degree of detail of the analysis may be prescribed by legislation.

Qualitative assessment defines consequence, probability and level of risk by significance levels, such as "high," "medium" and "low," may combine consequence and probability and evaluates the resultant level of risk against qualitative criteria.

Semi-quantitative methods use numerical rating scales for consequence and probability and combine them to produce a level of risk using a formula. Scales may be linear or logarithmic or may have some other relationship, and the formulae used can also vary.

Quantitative analysis estimates practical values for consequences and their probabilities, and produces values of the level of risk in specific units defined when developing the context. Full quantitative analysis may not always be possible or desirable due to insufficient information about the system or activity being analysed, the lack of data, the influence of human factors, etc. or because the effort of quantitative analysis is not warranted or required. In such circumstances, a comparative semi-quantitative or qualitative ranking of risks by specialists, knowledgeable in their respective field, may still be effective.

There is desperate need to take into account other aspects of conducting risk assessment. These include risk analysis like the following:

- Controls assessment,
- Consequence analysis,
- Likelihood analysis and probability estimation,
- Preliminary analysis,
- Uncertainties and sensitivities,
- Risk evaluation,
- Documentation,
- Monitoring and reviewing risk assessment,
- Application of risk assessment during life cycle phases, and
- Selection of risk assessment techniques.

In general terms, suitable techniques should exhibit the following characteristics:

- It should be justifiable and appropriate to the situation or organisation under consideration;
- It should provide results in a form which enhances the understanding of the nature of the risk and how it can be treated;
- It should be capable of use in a manner that is traceable, repeatable and verifiable.

Types of technique

The first classification shows how the techniques apply to each step of the risk assessment process as follows:

- Risk identification;
- Risk analysis – consequence analysis;
- Risk analysis – qualitative, semi-quantitative or quantitative probability estimation;
- Risk analysis – assessing the effectiveness of any existing controls;
- Risk analysis – estimation the level of risk; and,
- Risk evaluation.

For each step in the risk assessment process, the application of the method is described as being either strongly applicable, applicable, or not applicable

Factors influencing selection of risk assessment techniques

Next, the attributes of the methods are described in terms as follows:

- The complexity of the problem and the methods needed to analyse it,
- The nature and degree of the uncertainty of the risk assessment based on the amount of information available and what is required to satisfy objectives,
- The extent of resources required in terms of time and the level of expertise, data needs, or cost, and
- Whether the method can provide a quantitative output.

2. Selected methods-techniques for risk assessment

2.1. Brainstorming

Brainstorming involves stimulating and encouraging free-flowing conversation amongst a group of knowledgeable people to identify potential failure modes and associated hazards, risks, criteria for decisions and/or options for treatment. The term “brainstorming” is often used very loosely to mean any type of group discussion. However, true brainstorming involves particular techniques to try to ensure that each member’s imagination is triggered by the thoughts and statements of others in the group. Brainstorming can be used in conjunction with other risk assessment methods described below or may stand alone as a technique to encourage imaginative thinking at any stage of the risk management process and any stage of the life cycle of a system. It may be used for high-level discussions where issues are identified, for more detailed review, or at a detailed level for particular problems.

2.2. Delphi technique

The Delphi technique is a procedure to obtain a reliable consensus of opinion from a group of experts. Although the term is often now broadly used to mean any form of brainstorming, an essential feature of the Delphi technique, as originally formulated, was that experts expressed their opinions individually and anonymously while having access to the other expert's views as the process progresses. The Delphi technique can be applied at any stage of the risk management process or at any phase of a system life cycle, wherever a consensus of views of experts is needed.

2.3. Checklists

Checklists are lists of hazards, risks or control failures that have been developed, usually from experience, either as a result of a previous risk assessment or as a result of past failures. A checklist can be used to identify hazards and risks or to assess the effectiveness of controls. They can be used at any stage of the life cycle of a product, process, or system. They may be used as part of other risk assessment techniques but are most useful when applied to check that everything has been covered after a more imaginative technique that identifies new problems has been applied.

2.4. Preliminary hazard analysis (PHA)

PHA is a simple, inductive method of analysis whose objective is to identify the hazards and hazardous situations and events that can cause harm for a given activity, facility, or system. It is most commonly carried out early in the development of a project when there is little information on design details or operating procedures and can often be a precursor to further studies or to provide information for specification of the design of a system. It can also be useful when analysing existing systems for prioritising hazards and risks for further analysis or where circumstances prevent a more extensive technique from being used.

2.5. HAZOP

HAZOP is the acronym for **HAZ**ard and **OP**erability study and is a structured and systematic examination of a planned or existing product, process, procedure, or system. It is a technique to identify risks to people, equipment, environment, and/or organisational objectives. The study team is also expected, where possible, to provide a solution for treating the risk. The HAZOP process is a qualitative technique based on use of guide words that question how the design intention or operating conditions might not be achieved at each step in the design, process, procedure, or system. It is generally carried out by a multidisciplinary team during a set of meetings. HAZOP is similar to FMEA in that it identifies failure modes of a process, system, or procedure, their causes and consequences. It differs in that the team considers unwanted outcomes and deviations from intended outcomes and conditions and works back to possible causes and failure modes; whereas, FMEA starts by identifying failure modes. The HAZOP technique was initially developed to analyse chemical process systems, but it has been extended to other types of systems and complex operations. These include mechanical and electronic systems, procedures, and software systems, and even to organisational changes and to legal contract design and review.

2.6. Toxicity assessment (TA)

Environmental risk assessment is used here to cover the process followed in assessing risks to plants, animals and humans as a result of exposure to a range of environmental hazards. Risk management refers to decision-making steps, including risk evaluation and risk treatment. The method involves analysing the hazard or source of harm and how it affects the target population, and the pathways by which the hazard can reach a susceptible target population. This information is then combined to give an estimate of the likely extent and nature of harm. The process is used to assess risks to plants, animals, and humans as a result of exposure to hazards such as chemicals, microorganisms, or other species. Aspects of the methodology, such as pathway analysis, which explore different routes by which a target might be exposed to a source of risk, can be adapted and used across a very wide range of different risk areas, outside human health and the environment, and is useful in identifying treatments to reduce risk.

2.7. Structured "What-if" Technique (SWIFT)

SWIFT was originally developed as a simpler alternative to HAZOP. It is a systematic, team based study, utilising a set of 'prompt' words or phrases that are used by the facilitator within a workshop to stimulate participants to identify risks. The facilitator and team use standard 'what-if' type phrases in combination with the prompts to investigate how a system, plant item, organisation, or procedure will be affected by deviations from normal operations and behaviour. SWIFT is normally applied at more of a system level with a lower level of detail than HAZOP. While SWIFT was originally designed for chemical and petrochemical plant hazard studies, the technique is now widely applied to systems, plant items, procedures, and organisations generally. In particular, it is used to examine the consequences of changes and the risks thereby altered or created.

2.8. Scenario analysis (SA)

Scenario analysis is a name given to the development of descriptive models of how the future might turn out. It can be used to identify risks by considering possible future developments and exploring their implications. Sets of scenarios reflecting (for example) "best case," "worst case," and "expected case" may be used to analyse potential consequences and their probabilities for each scenario as a form of sensitivity analysis when analysing risk. The power of scenario analysis is illustrated by considering major shifts over the past 50 years in technology, consumer preferences, social attitudes, etc. Scenario analysis cannot predict the probabilities of such changes but can consider consequences and help organisations develop strengths and the resilience needed to adapt to foreseeable changes. Scenario analysis can be used to assist in making policy decisions and planning future strategies as well as to consider existing activities. It can play a part in all three components of risk assessment. For identification and analysis, sets of scenarios reflecting (for example) "best case," "worst case" and "expected case" may be used to identify what might happen under particular circumstances and analyse potential consequences and their probabilities for each scenario.

2.9. Business impact analysis (BIA)

Business impact analysis, also known as business impact assessment, analyses how key disruption risks could affect an organisation's operations and identifies and quantifies the capabilities that would be needed to manage it. Specifically, a BIA provides an agreed understanding of the following:

- The identification and criticality of key business processes, functions and associated resources and the key interdependencies that exist for an organisation;
- How disruptive events will affect the capacity and capability of achieving critical business objectives; and,
- The capacity and capability needed to manage the impact of a disruption and recover the organisation to agreed levels of operation.

BIA is used to determine the criticality and recovery timeframes of processes and associated resources (people, equipment, and information technology) to ensure the continued achievement of objectives. Additionally, the BIA assists in determining interdependencies and interrelationships between processes, internal and external parties, and any supply chain linkages.

2.10. Root cause analysis (RCA)

The analysis of a major loss to prevent its reoccurrence is commonly referred to as Root Cause Analysis (RCA), Root Cause Failure Analysis (RCFA), or loss analysis. RCA is focused on asset losses due to various types of failures, while loss analysis is mainly concerned with financial or economic losses due to external factors or catastrophes. It attempts to identify the root or original causes instead of dealing only with the immediately obvious symptoms. It is recognised that corrective action may not always be entirely effective and that continuous improvement may be required. RCA is most often applied to the evaluation of a major loss but may also be used to analyse losses on a more global basis to determine where improvements can be made. RCA is applied in various contexts with the following broad areas of usage:

- Safety-based RCA is used for accident investigations and occupational health and safety;
- Failure analysis is used in technological systems related to reliability and maintenance;
- Production-based RCA is applied in the field of quality control for industrial manufacturing;
- Process-based RCA is focused on business processes; and,
- System-based RCA has developed as a combination of the previous areas to deal with complex systems with application in change management, risk management and systems analysis.

2.11. Failure modes and effects analysis (FMEA) and failure modes and effects and criticality analysis (FMECA)

Failure modes and effects analysis (FMEA) is a technique used to identify the ways in which components, systems, or processes can fail to fulfil their design intent. FMEA identifies the following:

- All potential failure modes of the various parts of a system (a failure mode is what is observed to fail or to perform incorrectly);
- The effects these failures may have on the system;
- The mechanisms of failure; and,
- How to avoid the failures, and/or mitigate the effects of the failures on the system.

FMECA extends an FMEA so that each fault mode identified is ranked according to its importance or criticality. This critical analysis is usually qualitative or semi-quantitative but may be quantified using actual failure rates.

2.12. Fault tree analysis (FTA)

FTA is a technique for identifying and analysing factors that can contribute to a specified undesired event (called the “top event”). Causal factors are deductively identified, organised in a logical manner, and represented pictorially in a tree diagram that depicts causal factors and their logical relationship to the top event. The factors identified in the tree can be events that are associated with component hardware failures, human errors, or any other pertinent events that lead to the undesired event. A fault tree may be used qualitatively to identify potential causes and pathways to a failure (the top event) or quantitatively to calculate the probability of the top event, given knowledge of the probabilities of causal events.

2.13. Event tree analysis (ETA)

ETA is a graphical technique for representing the mutually exclusive sequences of events following an initiating event according to the functioning/not functioning of the various systems designed to mitigate its consequences. It can be applied both qualitatively and quantitatively. ETA can be used for modelling, calculating, and ranking (from a risk point of view) different accident scenarios following the initiating event. ETA can be used at any stage in the life cycle of a product or process. It may be used qualitatively to help brainstorm potential scenarios and the sequences of events following an initiating event and how outcomes are affected by various treatments, barriers or controls intended to mitigate unwanted outcomes.

2.14. Cause-consequence analysis

Cause-consequence analysis is a combination of fault tree and event tree analysis. It starts from a critical event and analyses consequences by means of a combination of YES/NO logic gates, which represent conditions that may occur or failures of systems designed to mitigate the consequences of the initiating event. The causes of the conditions or failures are analysed by means of fault trees. Cause-consequence analysis was originally developed as a reliability tool for safety critical systems to give a more complete understanding of system failures. Like fault tree analysis, it is used to represent the failure logic leading to a critical event, but it adds to the functionality of a fault tree by allowing time sequential failures to be analysed. The method also allows time delays to be incorporated into the consequence analysis, which is not possible with event trees.

2.15. Cause-and-effect analysis

Cause-and-effect analysis is a structured method to identify possible causes of an undesirable event or problem. It organises the possible contributory factors into broad categories, so that all possible hypotheses can be considered. It does not, however, by itself point to the actual causes; since these can only be determined by real evidence and empirical testing of hypotheses. The information is organised in either a Fishbone (also called Ishikawa) or sometimes a tree diagram. Cause-and-effect analysis provides a structured pictorial display of a list of causes of a specific effect. The effect may be positive (an objective) or negative (a problem) depending on context. It is used to enable consideration of all possible scenarios and causes generated by a team of experts and allows consensus to be established as to the most likely causes that can then be tested empirically or by evaluation of available data. It is most valuable at the beginning of an analysis to broaden thinking about possible causes and then to establish potential hypotheses that can be considered more formally.

2.16. Layers of protection analysis (LOPA)

LOPA is a semi-quantitative method for estimating the risks associated with an undesired event or scenario. It analyses whether there are sufficient measures to control or mitigate the risk. A cause-consequence pair is selected and the layers of protection that prevent the cause leading to the undesired consequence are identified. An order of magnitude calculation is carried out to determine whether the protection is adequate to reduce risk to a tolerable level. LOPA may be used qualitatively, simply to review the layers of protection between a hazard or causal event and an outcome. Normally, a semi-quantitative approach would be applied to add more rigour to screening processes, for example, following HAZOP or PHA. LOPA provides a basis for the specification of independent protection layers (IPLs) and safety integrity levels (SIL levels) for instrumented systems, as described in the IEC 61508 series and in IEC 61511, in the determination of safety integrity level (SIL) requirements for safety instrumented systems. LOPA can be used to help allocate risk reduction resources effectively by analysing the risk reduction produced by each layer of protection.

2.17. Decision tree analysis

A decision tree represents decision alternatives and outcomes in a sequential manner that takes into account uncertain outcomes. It is similar to an event tree, in that it starts from an initiating event or an initial decision and models different pathways and outcomes as a result of events that may occur and different decisions that may be made. A decision tree is used in managing project risks and in other circumstances to help select the best course of action where there is uncertainty. The graphical display can also help communicate reasons for decisions.

2.18. Human reliability assessment (HRA)

Human reliability assessment (HRA) deals with the impact of humans on system performance and can be used to evaluate human error influences on the system. Many processes contain potential for human error, especially when the time available to the operator to make decisions is short. The probability that problems will develop sufficiently to become serious can be small. Sometimes, however, human action will be the only defence to prevent an initial failure progressing towards an accident. The importance of HRA has been illustrated by various accidents in which critical human errors contributed to a catastrophic sequence of events. Such accidents are warnings against risk assessments that focus solely on the hardware and software in a system. They illustrate the dangers of ignoring the possibility of human error contribution. Moreover, HRAs are useful in highlighting errors that can impede productivity and in revealing ways in which these errors and other failures (hardware and software) can be "recovered" by the human operators and maintenance personnel. HRA can be used qualitatively or quantitatively. Qualitatively, it is used to identify the potential for human error and its causes so the probability of error can be reduced. Quantitative HRA is used to provide data on human failures into FTA or other techniques.

2.19. Other possible and applicable techniques with no comments

These methods sometimes enable one to gain some – but not always all – parameters of a risk profile. Examples are as follows:

- Bow tie analysis,
- Reliability centred maintenance,
- Sneak analysis (SA) and sneak circuit analysis (SCI),
- Markov analysis,
- Monte Carlo simulation,
- Bayesian statistics and Bayes Nets,
- FN curves,
- Risk indices,
- Consequence/probability matrix,
- Cost/benefit analysis (CBA),
- Multi-criteria decision analysis (MCDA), and
- Learning curve – entropy (Duffey/Saul approach), etc.

Conclusions

Due to the limited space of this paper, it is not possible to present more information and techniques-methods available, although they exist. Nevertheless, most of these methods can stand alone or might be incorporated into complex process of higher management – quality management, for instance, or RAMS. Most of the method presented might also be supported by software applications. Among others the RS - “Risk Spectrum,” Item: QRAS –

“Quantitative Risk Assessment” or Relex are good choices for software dealing with risk. More information about support might be also found in 11

Acknowledgement

Preparation of this paper was supported by the GA Czech Republic project number 101/08/P020 “Contribution to Risk Analysis of Technical Sets and Equipment,” and by the Ministry of Education, Czech Republic project number 1M06047, “The Centre for Production Quality and Dependability.”

Bibliography

1. ISO 31 000:2009 Ed.1.0 - Risk management — Principles and guidelines on implementation.
2. ISO/IEC 31010:2009 Ed. 1.0: Risk Management - Risk Assessment Techniques.
3. ISO 13824:2009 Ed. 1.0- General principles on risk assessment of systems involving structures.
4. ISO/IEC Guide 73:2002 Ed. 1.0 Risk management — Vocabulary — Guidelines for use in standards.
5. ISO/IEC GUIDE 51:1999 Ed. 1.0 Safety aspects — Guidelines for their inclusion in standards.
6. IEC 61508-(1-7)/:2008 Ed. 2.0 Functional Safety of Electrical/Electronic/ Programmable Electronic Safety-Related Systems
7. JCSS (Joint Committee on Structural Safety) - Principles, System Representation & Risk Criteria.
8. The National Risk Register http://www.risksociety.org.nz/what_is_risk_management/
9. ECSS (European Cooperation for Space Standardisation)-Q-ST-40-02C Space product assurance - Hazard analysis.
10. MIL-STD-882D Standard Practice for System Safety.
11. Valis, D., Vintr, Z., Koucky, M. Information sources regarding dependability on the internet. In: Materialy Szkoly Niezawodnosci Polska Akademia Nauk (Niezawodnosz Systemow Antropotechnicnych, XXXVII Zimowa Szkola Niezawodnosci). Warszawa: Wydzial Transportu Polytechniky Warszawskiej 2009, pp. 364–374. ISBN 978-83-7204-737-3.

Reviewer:
Krzysztof KOŁOWROCKI

Przegląd wybranych technik oceny ryzyka

Słowa kluczowe

Ryzyko, bezpieczeństwo, standardy, zarządzanie ryzykiem, metody i techniki oceny ryzyka.

Streszczenie

Aby prawidłowo zarządzać ryzykiem w różnych aspektach i w różnych fazach życia obiektu technicznego, należy wybrać i zastosować właściwe metody oceny ryzyka. Niektóre z metod są powszechnie stosowane i typowe, innych używamy bardzo rzadko. Artykuł przedstawia ogólny przegląd metod i technik, które mogą być wykorzystane w ocenie ryzyka, a mianowicie – w analizie ryzyka. Oczywiście podczas takiej oceny należy wziąć pod uwagę zarówno metody wykorzystywane do identyfikacji, jak i minimalizowania ryzyka. Jednak to metody analizy ryzyka są najczęściej wykorzystywane, jednocześnie często będąc mało znanymi. Ze względu na ograniczoną ilość miejsca, artykuł prezentuje jedynie generalny przegląd informacji na temat istniejących metod i technik stosowanych podczas oceny ryzyka.