Risk Management and Risk Assessment Methods

Aleksandra KokićArsić[1*] and Milan Mišić[2]

* Corresponding Author
1 Higher Technical Professional School in Zvečan, e-mail: akokicster@gmail.com
2 Higher Technical Professional School in Zvečan, e-mail: m.misic@vts-zvecan.edu.rs

ABSTRACT **This paper outlines the basis and the meaning of risk, as well as the risk management system. The aim is to present facts, which allow the identification of potential risks, the anticipation of their occurrence, and the implementation of appropriate measures to mitigate or eliminate risks. As a part of the management, key activities of the risk management process, as well as their main phases, are given. Different visual, auxiliary, and statistical risk assessment methods and tools are reviewed and emphasised using examples of fire risks in the workplace. These same methods and tools are nonetheless applicable to various other risk assessment domains in the fields of architecture and engineering.**

KEYWORDS risk picture, risk management, risk assessment methods and tools, fire

1 Introduction

A key fact when it comes to risk is that a comprehensive definition is not known (Ball & Ball-King, 2011). Different perceptions and applications have resulted in a variety of interpretations of risk in literature. The concept of risk can be framed by (Arsovski, Kokić Arsić, Rajković, & Savović, 2013):

- probability of loss;
- uncertainty; or
- probability of any outcome that is not anticipated.

Uncertainty and loss are common to all definitions of risks. The uncertainty occurs when the outcome of a particular activity is not sure. When the risk exists, there must be at least two possible outcomes of which at least one must be undesirable.

In general, the risk of any activity can be defined as a function of probability and impact (Fig. 1.1).

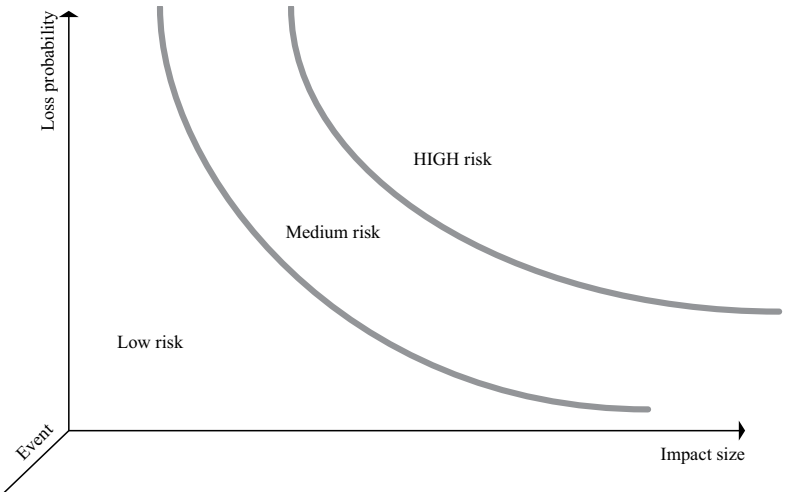

FIG. 1.1 Function of risk *(Arsovski et al., 2013)*

Risks represent a function of time, i.e. they change over time. This fact is relevant for monitoring the risk assessment dynamics in modern business-production systems exposed to constant changes. The research of risks, their consequences, and, in particular, the possibilities for their occurrence, are necessary for full understanding, raising, and strengthening of the level of knowledge and proper implementation of the risk management concept, and especially for its integral risk assessment process (Rausand, 2011).

Risks appear in many different forms and in various segments of industry. Professional risks, for instance, represent risks in the workplace. According to Bischoff (2008), these risks are within the limits of the norm, i.e. they are considered acceptable if they meet certain conditions:

- slight uncertainty regarding the likelihood of consequences;

- relatively low overall probability of injury;
- low or medium probability, low durability;
- inability to create the same, or repeated unwanted and unplanned activities;
- slight deviations between the assumed potential injuries and the likelihood of occurrence; and
- low level of risk related to social anxiety and potential dissatisfaction.

Risks are also very complex. Complexity is reflected in the assessment of a business-production system where the risks are identified, analysed, and evaluated systemically, not individually. Individual risk observation could have consequences for other activities, processes, or individuals within a system. In other words, individual risks that are considered acceptable, without taking into account their interdependence with other risks, may result in hazardous developments in another part of that system. To avoid this, a very good knowledge of hazards and harmfulness, that is, the nature of the risks that arise, is needed.

Organisations encounter a variety of risks that can influence the accomplishment of goals assigned to a range of activities. Actually, all activities of an organisation include risks. Expected results of an organisation's planned future activities are, by definition, unknown and uncertain, and thus vague. In the context of future activities, risk and uncertainty are therefore the most often mentioned. They may imply a possibility of failing to achieve the expected goals, of achieving poor results, or of losing the invested funds. Risk management is helpful in an organisation's decision-making process, taking into account uncertainty and impact on goal achievement. As such, risk management is the inherent part of organisation, overall management, management, process, policy, philosophy and culture (Đapan, 2014).

The most common interpretation and understanding of the objective of risk management concept is to reduce the risk by applying prescribed measures as a prerequisite for protection of people, environment, or property from the consequences of unwanted and unplanned activities. The essence of risk management is the willingness to accept a certain level of risk. Target is to create the balance between safety functioning of the system and avoiding losses and unplanned events and catastrophe. (Aven, 2008).

2 Risk Management Principles and Standards

Successful and sustainable risk management is embedded in a company and supported by its management. A risk management system aims to help a company to efficiently manage risks at different levels and in specific contexts, and to ensure that any risk information is used as a basis for decision-making at all relevant organisational levels.

Organisations should adhere to the principles of effective risk management. According to Arsovski et al. (2013), risk management

creates values; it represents an integral part of an organisation's decision-making processes, and takes into account the human factor. Furthermore, effective risk management explicitly addresses uncertainties, in a systematic and structured way. As such, it is based on the best available information and tailored to the specificities of an organisation. Finally, effective risk management is transparent, comprehensive, dynamic, iterative, and responsive to changes, all of which facilitate the continuous improvement and enhancement of an organisation (Arsovski et al., 2013).

Among numerous international standards on risk management, the following may be distinguished: Australian–New Zealand Risk Management Standard – AS/NZS 4360:2004; Canadian Risk Management Guide CAN/CSA-Q850-97(R2009); British Standard – BS 6079-3:2000; ISO 31000 – Risk Management – Principles and Guidelines; and ISO 31010:2009 – Risk Management – Risk Assessment Techniques. The Australian – New Zealand Risk Management Standard – AS/NZS 4360:2004 provided a general framework for establishing the risk management process and outlined procedures that can be applied to risk identification, assessment, analysis, and communication. The Canadian Risk Management Guide CAN/CSA-Q850-97(R2009) provides guidelines for decision-makers. The British Standard – BS 6079-3:2000, as a convention, includes past and present practices in risk management, but does not offer ways of managing risks in the future. The ISO 31000:2009 provides principles and guidelines for risk management implementation, and primarily focuses on company risk management. According to ISO 31010:2009, when carrying out the risk assessment procedure, it is necessary to consider:

- vision and goals of the organisation;
- type and level of risks that are acceptable, as well as how to deal with risks that are not acceptable;
- how the risk assessment process is integrated into the organisation's processes;
- methods and techniques used in the risk assessment process as an integral part of the risk management concept;
- responsibility for the implementation of risk assessment process;
- resources and needs for the implementation of risk assessment process; and
- how to report and review risk assessment processes.

3 Risk Picture

Risk assessment includes the most important phases in the risk management process (Fig 3.1): risk identification, risk analysis, and risk assessment.

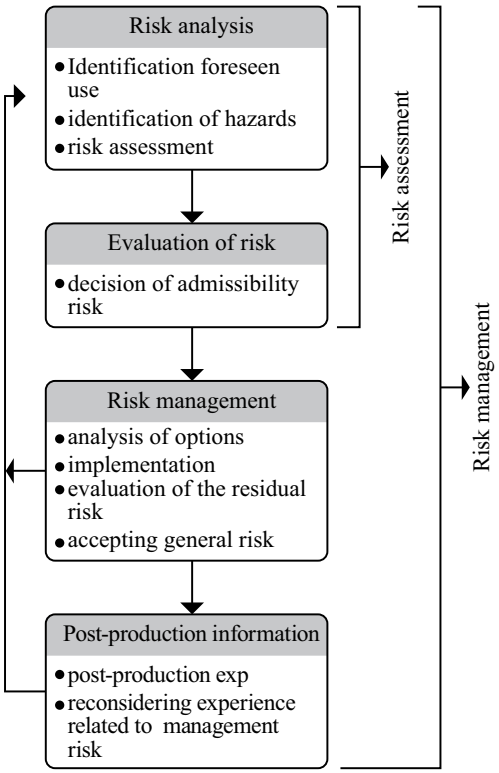

FIG. 3.1 Risk management processes *(Arsovski et al., 2013)*

According to Aven (2008), risk picture is a platform that contains certain constituent risk components. Protection system first considers implementation of risk analysis and risk assessment, then definition of barriers, all in sense to identify accident and implement continuos improvement. Aven and Vinnem (2007) identify two key risk management tasks that are to establish risk picture for different alternatives of decisions, and to use this risk picture in decision-making.

According to Ericson (2005), the hazard consists of the following components: element of the hazard, the initiating mechanism, and goal and threat. Hazards exist because they are inevitable (elements of hazards must be used in a system), and caused by inadequate safety considerations. Leveson (2011) defines a hazard as a condition that, together with the worst set of environmental conditions, will lead to an accident (loss).

The occurrence of unwanted activities can be caused by different internal and external factors, such as: problems in equipment and material, wrong procedures, human error, lack of adequate training, management problems, etc. Organisational mistakes are often at the

root of engineering system failures. However, when it comes to defining a risk management strategy, engineers often tend to focus on technical solutions, partly because of the ways in which risks and failures were traditionally analysed in the past.

Haimes (2015) identifies four sources of system failures: software, hardware, human, and organisational, and highlights the twofold importance of their consideration; they are comprehensive and include all aspects of the system life cycle (planning, design, construction, use, and management), and require full involvement of all persons at all levels of the organisational hierarchy in the risk assessment process.

The visually receptive concept developed by James Reason, subsequently called the "Swiss cheese model" (Fig. 3.2), illustrates how accidents arise from holes in multiple barriers caused by active failures and latent conditions (Reason, Carthey, & de Leval, 2001; Mannan, 2012).

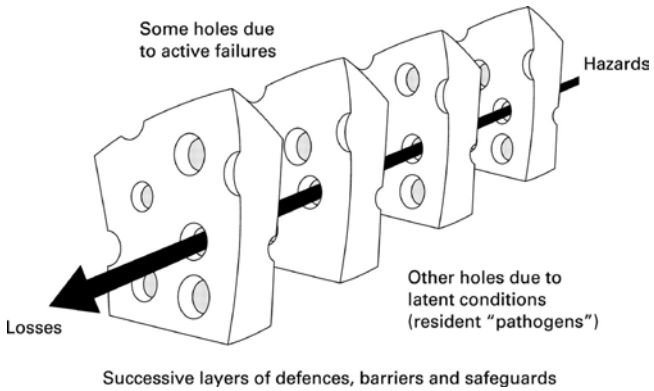

FIG. 3.2 "Swiss Cheese" model
(Reason, Carthey & de Leval, 2001)

3.1 Example: Fire Risk Picture

The assessment of the risk of fire is primarily an empirical decision-making process based on knowledge and experience, and is aimed at increasing fire safety. The specificity of the observed problem requires knowledge of the technological process of work, equipment, and the characteristics of the building. By looking at the "risk picture" (Aven, 2008), consideration is, after hazards and cause, directed to the barriers. In this context, barriers are elements located between initial and central elements of the "risk picture" on one side, and the final elements on the other. In general, barriers may be understood as tools used to protect certain values from some hazards.

Barriers are the key elements of protection system management. A fire protection system based on the barrier model comprises:

- danger analysis and fire threat assessment;
- defining and applying barriers;
- defining the barrier performance criteria;
- performance verification; and
- continuous enhancement.

According to Ware (2009), the following three groups of barriers can be defined: Buildings and Technologies; Processes; and Human Resources.

Building and Technologies
The group Building and Technologies relates to building, technologies, and technical protection systems and fire extinguishing equipment (stable detection systems, alarms, extinguishing and cooling systems, hydrant network with accessory equipment, and fire extinguishers). Threat analysis and risk assessment for buildings and technologies are carried out in the design, construction, and exploitation phases. An internal documentation audit during the design and construction phases aims to verify compliance with fire protection standards, whereas the external verification is done before exploitation in the form of a technical acceptance check.

Processes
Processes include: maintenance (keeping, inspection, and testing of all building elements, technologies, and systems relevant for fire protection); inspections and tests of equipment and assets belonging to the organisation's fire brigades; system of work permits for high-risk work activities and the management of contractors and third parties regarding industrial, ecological, and occupational safety and health, including fire protection; and fire and evacuation actions. In the event of a fire, every *trained* employee is obliged to participate in extinguishing it, and to assess the safe ways of doing so; otherwise, the employee is obliged to inform fire-fighting units immediately, to act in accordance with the appropriate instructions, if possible, and to evacuate. The fire-fighting units shall act in accordance with the operational fire extinguishing plans, fire protection plans, and recovery plans. The evacuation shall be carried out in accordance with the *evacuation plan*. The elimination of the consequences caused by the fire is done according to the *recovery plan*.

Human resources
Training and drills for human resources encompass trainings in fire protection as well as the fire-fighting drills, including evacuation.

4 Fire Risk Management

The management on the example of fire protection is a cyclical process applied in all phases of the life cycle of buildings and technologies (Fig. 4.1). It encompasses risk assessment and appropriate measures of preventive and repressive fire protection.

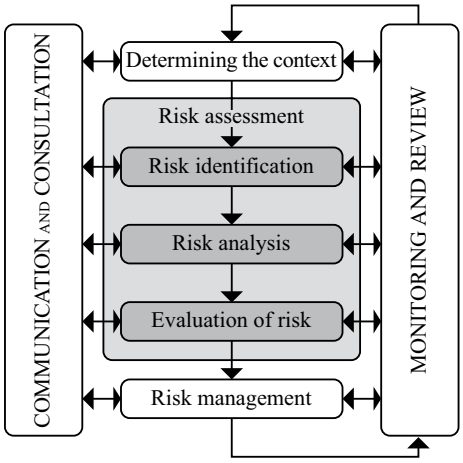

FIG. 4.1 Model of the fire protection management *(according to ISO 31000:2009)*

The risk of fire can be considered as a function of frequency and consequence. It is usually measured by the number of casualties, as well as the material and financial losses. Risk management represents identification, measurement, and risk control. Risk control depends on the priority of risk and implies the introduction of measures aimed at reducing the risk to an acceptable level.

In the context of responsibility for fire protection management, it is carried out on two levels. The first level consists of fire-fighting, and the second of preventive activities.

4.1 Fire Risk Assessment

Fire risk assessment includes identification, assessment, and management of risks arising from the occurrence of a fire. Simply put, fire risk assessment is a tool used to identify hazards and the risks arising from them, i.e. an organised methodological procedure for analysing workplace activities that can pose a risk of fire, likelihood of a fire, and an estimate of the damage caused by the fire. The objectives of the fire risk assessment in the workplace are to (Nikolić & Ružić-Dimitrijević, 2009):

- identify fire hazards;
- reduce the risk of noticed hazards by reducing the operational damage to the admissible; and
- apply technical and organisational preventive and repressive fire protection measures in order to protect the persons present.

There is no comprehensive risk assessment method. The procedure is to be conducted in a practical and systematic way, from design, construction, and finally to the exploitation of a building. Hazard analysis and threat assessment are used to obtain information on the types of hazards and the levels of threat, as a basis for defining the organisation of fire protection, barriers, performance standards, and the verification methods. In the design and construction phases, hazard analysis and

threat assessment are done through the documents arising from legal and other requirements. The results of threat analysis and assessment are incorporated in project documentation, and subsequently in *fire protection rules*, *fire protection plan*, *recovery plan*, *training program*, as well as in normative methodological documents referring to the protection against fire.

4.2 Assessment Procedure

The assessment of fire risks must include workplace, wider working environment (such as the parts of building that are rarely used), and outdoor space. Recognition and identification of fire hazards at the workplace are done on the basis of the data collected from available documentation, by monitoring the work process, obtaining the necessary information from employees and other sources, and by sorting the collected data and the possible hazards indicated by these data. Fig. 4.2 shows the course of the *Action Plan* for risk assessment.

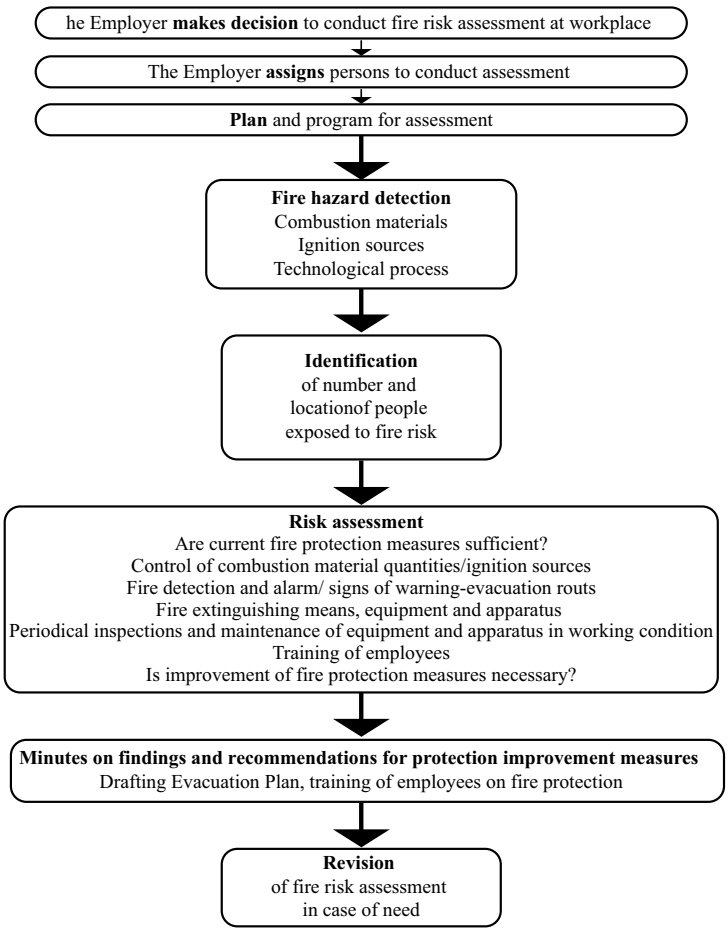

FIG. 4.2 Course of Action Plan for Risk Assessment

The first step in the assessment procedure foresees the identification of all fire hazards, including all sources of ignition (e.g. open flame, electrical energy, static electricity, sparks, etc.). It is also necessary to record the conditions that contribute to the rapid spread of fire,

such as inadequate division of the building into fire compartments, presence of stairs and elevators, low fire resistance of building construction elements, etc.

The second step foresees the identification of the number of persons who are exposed to the immediate risk in the event of a fire and those who are in close proximity. Identification should consider the permanent location of the workplaces, as well as occasional locations across the building. It is especially necessary to consider those persons who work independently and/or in isolated areas, persons with special needs who are not able to react quickly in the event of fire, as well as visitors who are not familiar with the evacuation routes.

After identifying the hazard and the individuals endangered by the fire, it is necessary to assess the fire risk. The analysis of existing measures of preventive fire protection represents the next assessment phase. Fire detection devices (e.g. manual detectors, fire detectors, sirens, telephone etc.) are assessed depending on the size and complexity of the workplace. The possibility of abandoning the workplace in the shortest possible time should be analysed. Evacuation routes and exits must be permanently passable, clearly marked, and illuminated. The assessment of the amount and conditions of existing devices, equipment, and the hazard analysis, as well as the existing measures, determine if the present level of protection is sufficient or if it should be upgraded.

Further assessment includes the categorisation into high, medium, or low risks. The fourth phase consists of making a record of detected fire hazards and taking measures to reduce or eliminate them. A plan to prevent fire occurrence and to carry out safe evacuation in the event of fire must be made. This phase also requires the adequate training of employees in the field of fire protection. Fire risk assessment documentation should be revised with the occurrence of new hazards and changes in the level of fire risk.

4.3 Key Indicators of Process Success

The *availability coefficient* is "equal to the probability of finding the system in the operational state at the needed moment of time" (Ushakov, 2016, 95). In relation to fire protection, it refers to technical protection systems and fire extinguishers, and their external and internal inspections. Internal and external checks of the availability of technical protection systems, fire extinguishers, and equipment, are determined by special instruction. At the organisational level, the additional indicators of the process success are collected, processed and analysed. The result of the verification represents the corrective and practical measures arising from inspection and audit, the investigation of events and consideration of performance indicators, all of which are defined in action plans (Kokić Arsić, Arsovski, Kanjevac Milovanović, Bojić, & Savović, 2013).

5 Methods and Tools for Risk Assessment

The concept of risk management implies that a balance should be found between providing secure functioning, and avoiding unexpected and unwanted events, so that it can be said that risk management is practically based on risk control. Since it is clear that risks cannot be eliminated, the primary objective of risk management is to provide a level of risk below the minimum allowable value.

Risk assessment is primarily the empirical process of making engineering decisions based on knowledge and experience in order to enhance safety and health at work by using selected, well-known and recognised methods. There are numerous recognised risk assessment methods established by various associations and associations worldwide. Nonetheless, none of these risk assessment methods prescribes a choice of preventive measures to reduce, eliminate, or prevent risks. Rarely is there only one "real" tool, method, or risk analysis model to provide a "correct" analysis to support decision-making. The proper choice of risk assessment methods will allow for the adequate application of measures to achieve a safer workplace and work environment, with less probability of work-related illnesses and injuries to employees.

The risk assessment methods presented in this study are based on the standard ISO 31010 and divided into visual, auxiliary, and statistical methods. For every method presented, a note of the benefits and limitations of their use is given. The methods are classified into logical units, and the work indicates in which part of the risk assessment process their utilisation is optimal. The utilisation of risk assessment methods (including tools), as presented here, is demonstrated primarily in the example of fire protection. These same methods and tools are nonetheless also applicable to various other risk assessment domains in the fields of architecture, construction, and engineering.

5.1 Visual Methods

Check list

A check list is a simple written form used to identify basic groups of risks for which the assessment is carried out (Table 5.1). After the basic hazards are defined, the identification of the minor, individual threats within the groups is done. Check lists are easy to use and, if precisely designed, they represent a significant tool for identifying risks. On the other hand, the weakness of this method is that the identification of certain hazards could be omitted due to their nature, origin, or interaction with other hazards.

1.	DOES YOUR ORGANISATION HAVE A FIRE PROTECTION POLICY?	YES	NO	NOTE
2.	Did your organisation establish and document action procedures in case of fire?			
3.	Are security fire protection procedures carried out regularly?			
4.	Are employees informed on fire protection procedures?			
5.	Are employees informed on current hazards that can occur in their workplace?			
6.	Is there a reaction plan in case of major fire?			
7.	Is there an authorised person dealing with fire protection in your organisation?			
8.	Has the authorised person for fire protection been appropriately trained and does he/she have the required certification?			
9.	Is contact with fire-fighting units possible both during and after working time?			

TABLE 5.1 Example of a check list for fire risk detection

Preliminary Hazard Analysis – PHA

Preliminary Hazard Analysis – PHA is a method for qualitative risk assessment used to identify possible accidents in a building. The goal is achieved by conducting tests in the following order: examining the sequence of events that can potentially turn into an accident; relating these unfortunate cases to the given hazard class; and, finally, considering measures to remove the hazard. PHA is most commonly used, at the earliest stage, for predicting potential problems in cases where only a small amount of information is available. However, this method provides only preliminary information, without detailed analysis or prevention measures. An example of the PHA method used for detection of the fire risk and hazard classes is given in Tables 5.2 and 5.3.

PART OF EQUIPMENT OR FUNCTION	HAZARDOUS ELEMENT	HAZARDOUS ACTION	HAZARDOUS STATE	DIRECT CAUSE	HAZARD CLASS	PREVENTION MEASURES
Gas container	Gas pressure	Leaking caused by container leaking	Free gas	Spark, flame, static electricity	I or II	Extinguishing system installed

TABLE 5.2 Example of PHA methods for fire risk identification

HAZARD CLASS I	CATASTROPHIC CONSEQUENCES - ONE OR MORE DEATHS AND COMPLETE BUILDING DAMAGE
Hazard class II	Critical consequences - serious injuries, building damage and complete cessation of production
Hazard class III	Marginal consequences - less damage and damage to the building, moderate production decrease
Hazard class IV	Negligible consequences - no injuries and no damage to the building

TABLE 5.3 Illustration of hazard classes and consequences

5.2 Auxiliary Methods

Interviews and brainstorming

Interviews and brainstorming are used for gathering the widest possible range of ideas that precede the risk assessment process. The benefits of these methods are that they help identify new risks and new situations arising from their identification. Furthermore, in terms of time, these methods are quick to organise and implement, and do not require significant prior preparation. They also enable good communication among all involved parties. The limitations are the lack of experience and of necessary knowledge, whereas the inclusion of

different types of personality in the implementation of these activities is highly unlikely to take into account all potential risks.

Delphi Technique

Delphi Technique is an independent analysis based on the opinions of experts. Its aim is to use knowledge, experience and intuition of processes and sub-processes in a rational and systematic way to secure realistic outlook (Arsovski, Vujović, Mišić, Nestić, & Gvozdenović, 2013). The Delphi technique belongs to the group of decision-making processes based on reaching a consensus among decision-makers. This technique can be applied at any stage of a risk management process in which an expert opinion is required. The advantages are that it gives a range of independent and anonymous opinions of the same rank and the same importance, and time efficiency. The limitations are that it requires constant participation of the employees, as well as the fact that the participants have to express their opinions correctly and completely in a written form (Kiral & Kural, 2014).

"What-if" Technique

A structured "What-if" Technique is applied in cases of emergency risk identification, with a very strong connection between the analysis and risk assessment (Golfareli & Rizzi, 2008.) This technique can be applied to different types of business-production systems. It takes very little time effort to prepare for its implementation. The "What-if" technique is relatively fast and the main risks are identified quickly. Here, the response of a system to the deviations is observed, while the consequences are not examined. Therefore, the technique can be used to identify improvements, and the results are used as input information for quantitative analysis. However, it should be noted that the identification of some risks and hazards requires expertise and preparations, and can be time-consuming. Regardless of the level of precision of this technique, there is a possibility to omit some more complex causes.

Human Reliability Analysis

Human Reliability Analysis evaluates the impact of a human being on a system and is used to evaluate human error. The results can be presented quantitatively or qualitatively. As shown in Fig. 5.1, human activity is introduced at all levels of the risk assessment, and individuals play a very important role here. Consideration of the human error as an influencing factor can reduce the probability of error occurrence. Human Reliability Analysis can include:

- task analysis;
- error identification (ways they in which can appear);
- presentation (determining cause-effect relationships between human-related events, software, hardware, environment, etc., in a logical and measurable manner);
- quantification (evaluation of error);
- reducing the error by preventive actions (probability of occurrence or its effect); and

– quality assurance and documentation (verification that evaluations are valid and can be used to inform future design or for another purpose).

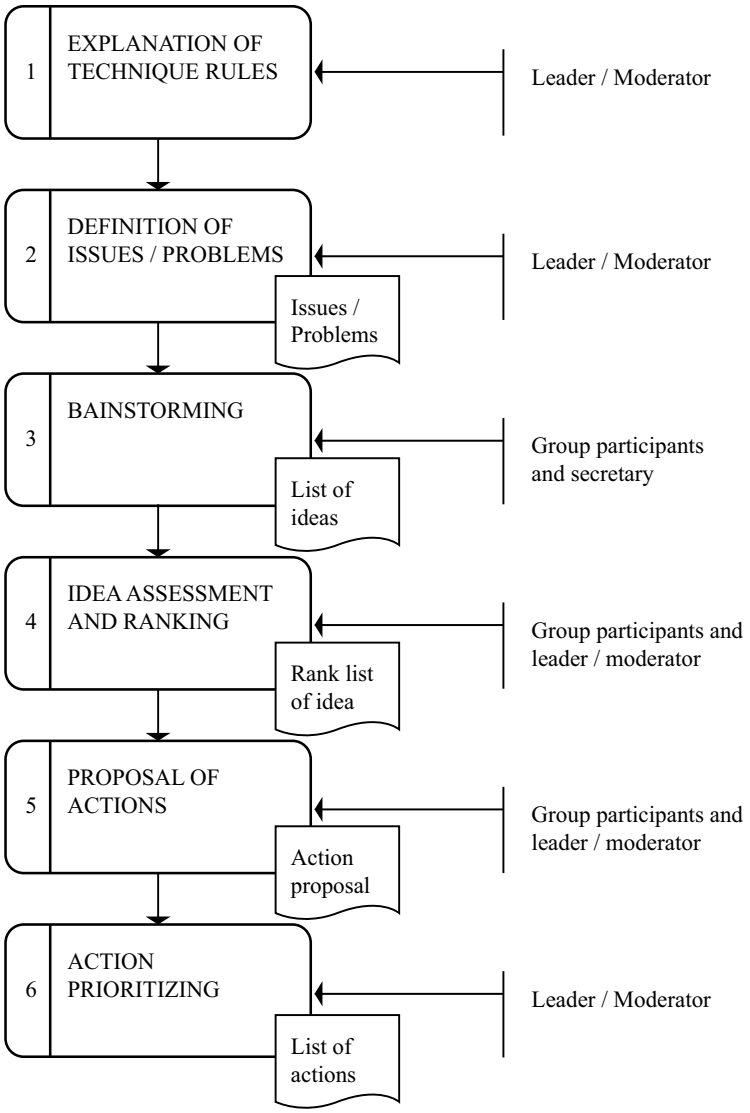

FIG. 5.1 Risk Assessment Action Plan flow *(Lazić, 2006)*

Root Cause Analysis

Root Cause Analysis deals with current errors and their fundamental causes (and not with obvious causes of errors) in order to improve the system and avoid similar future losses (Vorley, 2008). This analysis can be used in a large number of areas. The advantages are the participation of adequate and experienced experts in the team, structured analysis, consideration of all possible assumptions, documenting the results, and provision of recommendations for improvement. The limitations relate to difficulty in engaging experts at a given moment; potential inaccessibility or destruction of the main pieces of evidence during the occurrence of the error; inability to provide the team with sufficient resources for situation assessing; and inability to implement the recommendations.

Scenario Analysis

Scenario Analysis is a method of assuming future possible consequences based on present data and extrapolation tools. It is built mainly on descriptive models and used to identify the emergence of possible risks and their impacts. On the basis of the forecast, the future situation that may, though does not necessarily, have a trend similar to the one in the past, is assumed. This is very important for a system that contains very little knowledge on which a forecast can be based, or for systems where risk assessment is necessary over a longer period of time. Nonetheless, some of the scenarios offered may be unrealistic and are without adequate basis for the forecast, especially when there is a lack of data. The concept of the Scenario Analysis Method given in Fig. 5.2 indicates that a thorough understanding of the company situation requires the identification of internal and external factors, as well as their interactions, anticipated discontinuity, and transfer of the anticipated scenario outcomes into alternative business strategies.

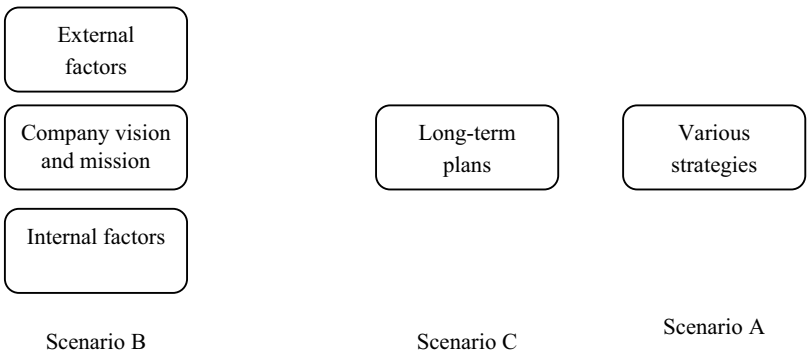

FIG. 5.2 The concept of the Scenario Analysis Method

Business Impact Analysis

Business Impact Analysis is also known as an impact assessment on business. It provides an analysis of how the key risks affect the systems functioning, as well as the possibilities of identification and quantification in the management of these systems. The advantages of this method are the facilitated understanding of critical systems and processes, and the possibility to redefine system processes, whereas the disadvantages relate to over-simplified or over-optimistic expectations, and the difficulties in the full and adequate understanding of systems processes and activities (Charters, 2011).

Fault Tree Analysis

Fault Tree Analysis is a technique for identifying and analysing factors that lead to an unwanted and unplanned event. It aims to determine, reduce, and eliminate potential causes / sources by using graphical representation of the logical diagram or tree. The advantages of this method are that it provides a very systematic approach to the problem, flexible analysis, a top-down approach, and usefulness of the analysis of more complex systems. The graphical representation, in many ways, facilitates system understanding and behaviour, as well as the factors that affect it. Its limitations relate to a possible high level of uncertainty during analysis, if the system is not sufficiently known. In some cases, the interaction of factors is not always possible, and the fault tree is a

statically time-independent model. As the fault tree manipulates only with two outputs - "with or without consequences", the human factor can neither be easily included in the analysis nor in the consequent cancellation and domino effect.

Cause-Consequence Analysis

Cause-Consequence Analysis represents a combination of the Fault Tree and the Event Tree. Here, the causes and consequences of the initial event are taken into account. The advantage of this method is that it combines two methods for improved results. As it is possible to overcome certain constraints by analysing events that develop after a certain period of time, this analysis gives a wider picture of the whole system. On the other hand, the level of analysis complexity is significantly higher than in separate Fault Tree or Event Tree analyses.

Cause-and-Effect Analysis

Cause-and-Effect Analysis is a structured method for identifying possible causes of an unwanted and unplanned event (Fig. 5.3). Influential factors are divided into categories where all possible assumptions are taken into consideration, but as such do not determine the real causes. This type of analysis is organised in the form of a so-called Ishikawa Diagram (Fishbone Diagram). The advantages of the method include participation of adequate and experienced experts in the team, consideration of all possible assumptions, structured analysis, and its graphic representation. Limitations refer to the possible lack of necessary knowledge and experience, and the exclusion of the ultimate concept of analysis from representation; for that reason, this method needs to be a part of some other more comprehensive analysis, such as Root Cause Analysis.

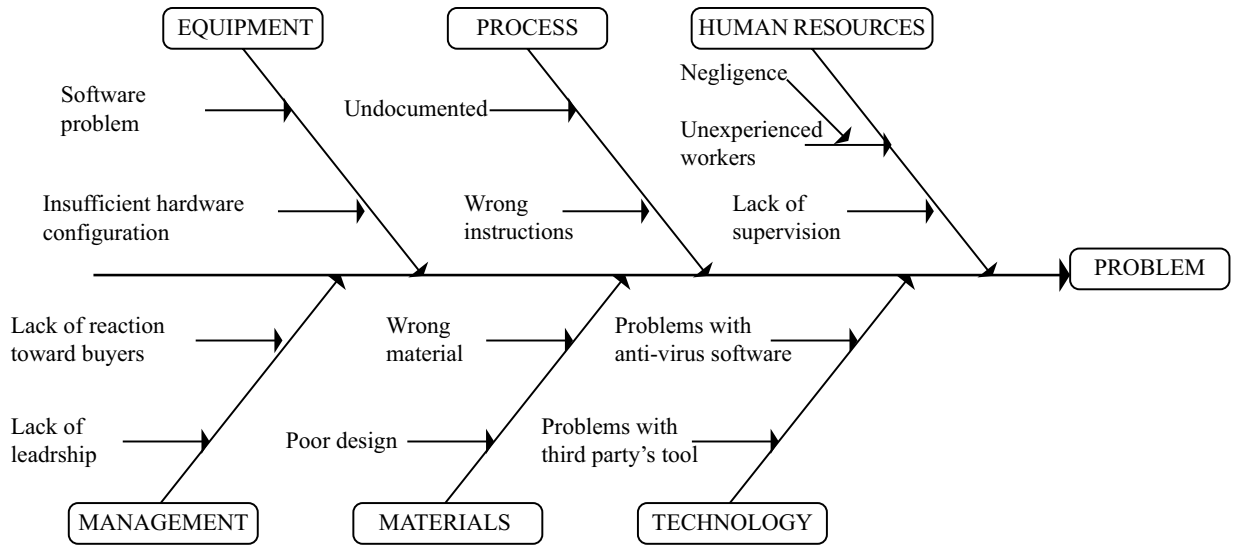

FIG. 5.3 Ishikawa Diagram *(Ishikawa, 1976)*

Failure Modes and Effects Analysis – FMEA

Failure Modes and Effects Analysis – FMEA identifies how components, elements, systems, and processes will fail to fulfil their projected function. In this case, all potential failures of each individual part of the entire system are identified. The goals of the FMEA method are to detect and localise potential errors in a timely manner; avoid or mitigate project risks; prevent costs of possible revocation due to the occurrence of an error; and prevent loss of reputation on the market.

The implementation of the FMEA goes through the following stages:

- making a decision on FMEA;
- appointment of the FMEA team;
- preparation for analysis;
- analysis;
- assessment of the current situation;
- control of FMEA; and
- implementation of corrective measures and assessment of the results of corrective measures.

Function	**Project design FMEA** ☐ New component or new use ☐ Improvement of current			Product	Sketch number
	Responsible person	Organizational unit/supplier	Plant / supplier	Type/system/function	Date of project design
				FMEA date	Page/s

Name of component / system	Class	Failure			Current state					Correction measures			Improved state			
		Type	Causes	Consequences	Control measures	R1	R2	R3	RPC	Recommend correction measures	Implementation responsibilities and dynamics	Undertaken correction measures	R1	R2	R3	RPC

Error /failure probability R1		Error / failure importance (severity) R2		Error /failure identification probability R2		Risk priority coefficient RPC		FMEA team	
Score	points	Score	points	Score	points	RPC = R1 R2 R3		Participants	Function
Negligible	1	Negligible	1	Negligible	1	Score	points		
Minor	2-3	Minor	2-3	Minor	2-3	Minor	1-50		
Medium	4-6	Medium	4-6	Medium	4-6	Medium	50-100		
High	7-8	High	7-8	High	7-8	High	100-200		
Critical	9-10	Critical	9-10	Critical	9-10	Critical	200-1000		

FIG. 5.4 FMEA form

In the first stage, the FMEA team answers the question: What possible mistakes (defects) can occur? Finding answers and determining the likelihood of defects is based on previous knowledge, testing, and experience. The second stage is the identification of potential errors (severity – weight of defects). The team analyses and identifies the possible consequences for each potential error. The third stage is to identify the cause of the fault (defects) and the possibilities of their detection. For each error, one or more causes are identified. The fourth stage involves an analysis of the system control and testing. The analysis determines to what extent the applied methods, control, and testing means ensure the timely detection of the cause of errors and prevent the occurrence of errors. The fifth stage is to determine the probability of occurrence of an error for any possible cause of error. A record of possible errors, causes, and consequences is achieved by using the

FMEA form (Fig. 5.4) which lists all activities of the FMEA team and represents the basis for conclusion-making.

Reliability Centred Maintenance
Reliability Centred Maintenance identifies guidelines that need to be implemented to better manage failures and thus to effectively achieve the required security, availability, and cost-effectiveness of the system.

Sneak Analysis and Sneak Circuit Analysis
Sneak Analysis and Sneak Circuit Analysis deal with the "sneak" or "hidden" conditions of the design phase. A "hidden" condition is any condition that can lead to an unwanted and unplanned event. It does not allow the desired event to proceed smoothly, but is not caused by the failure of some of the components.

DEVIATION	CAUSES	CONSEQUENCES	PRECAUTION MEASURES	COMMENTS, RECOMMENDATIONS
High flow	Failure of safety valve in open position	High level in reactor with potential overfilling	FI567 (local) LIT987 (remote indicator)	(R) FIT (remote) with alarm for high level alert
High level	Failure of either safety (open) valve or valve (closed)	Potential overfilling	LIT (remote indicator)	(C) Verify if an error in LIT triggers an error signal according to DCS, the last time the value was not maintained (R) Provide LAH, LAHH from the LIT signal (R) Secure LHHS from the independent level of the transmitter to the supply pump

TABLE 5.4 Illustration of HAZOP template

HAZOP – Hazard and Operability Study
HAZOP – Hazard and Operability Study deals with deviations from expected characteristics (Table 5.4). As a result, solutions for risk processing are expected. The benefits of this method are a systematic approach to testing systems, processes, or procedures, provision of results and activities for risk processing, applicability to a large number of systems, processes and procedures, and the provision of explicit access to consideration of causes and consequences of human error. Nonetheless, detailed analysis can be very demanding, both in terms of financial resources and time; it may require high-level criteria for documenting the methodology and is often aimed at finding a solution to complex problems rather than some fundamental assumptions.

Hazard Analysis and Critical Control Points – HACCP
Hazard Analysis and Critical Control Points – HACCP is a systematic and proactive approach to ensuring quality, reliability, and security of the process by monitoring and measuring selected parameters. The aim is to reduce the risk during the process and not to control the final product. HACCP requires detection of hazards, identification of risks and their importance, determination of critical control points, and undertaking the necessary measures when control parameters exceed limit values.

Layers of Protection Analysis – LOPA
Layers of Protection Analysis – LOPA is often referred to as a barrier analysis that enables the assessment of the control process effectiveness. It requires significantly less time and resources in comparison with, for example, the Analysis of the Failure Tree or Quantitative Risk Assessment. LOPA helps to identify and to direct resources to the most critical levels of protection, and identifies operations, systems, and processes that need the utmost protection (Dowell & Hendershot, 2002).

"Bow tie" Analysis
"Bow tie" Analysis represents a simple graphic solution for describing and analysing the risk spreading, ranging from hazard detection to control. It can be viewed as a combination of thinking, cause analyses, fault tree, and an analysis of the consequences with the event tree. The basic "bow tie" steps include: the timely detection and localisation of potential errors; avoiding or mitigating project risks; prevention of costs of possible revocation due to error occurrence; and prevention of the loss of reputation on the market.

5.3 Statistical Methods

Markov Analysis
Markov Analysis a probabilistic technique used when the state or behaviour of the system depends only on the current state and not on any state or behaviour in the past. It is most commonly used for systems that can come out of a state of failure and which can survive in multiple states.

Monte Carlo Analysis
Monte Carlo Analysis is applied in very complex systems when it is very difficult to understand certain situations and solve problems using analytical methods.

Bayesian Analysis
Bayesian Analysis is a statistical procedure that combines previously known information with the latter, in order to determine the overall probability.

Multi-Criterion Decision Analysis - MCDA
Multi-Criterion Decision Analysis - MCDA is an analysis that uses a set of criteria to objectively evaluate the value of a range of alternatives. Generally, this type of analysis allows the ranking of the offered or existing alternatives.

6 Conclusion

Numerous risk definitions refer to probability, opportunity, chance, or expected outcome, and may also relate to uncertainty, unwanted and unplanned activities, and hazards. In order to eliminate the occurrence of unwanted and unplanned events, it is necessary to understand these events and their consequences. Knowing the nature of the consequences represents the basis of their reduction and of the contined desire for their complete elimination.

In addition to the most common types of risk assessment used in the context of risk management, it is also necessary to define the framework of the risk assessment process, depending on the problem type and complexity, and to select appropriate:

- variables (parameters, factors); and
- techniques (methods, tools) for modelling.

The risk assessment process has been given a key role by the European Directive 89/391/EEC. In non-member states, for example in the Republic of Serbia, and in the fire protection context used in this work to concretise the topics of risk assessment and risk management, the basic binding guidelines that employers have to respect, apply, and implement are given through the Labour Law and the Occupational Health and Safety Act. Every organisation has the obligation to provide every worker with such work conditions that don't endanger life and health. When risk management activities are carried out in an appropriate and prescribed manner, it is a sure sign that workplace safety is enhanced.

There are many types of variables and methods that can serve as a stable basis for an adequate risk assessment. All methods and tools for risk assessment are conceived and adapted to reducing risks. The decision on selection is made on the basis of sufficient information on the type and characteristics of the workplace, the likelihood of occurrence of unwanted and unplanned events, possible consequences, etc. Therefore, it is necessary to choose the method that best suits and determines the real state for the observed workplace.

References

Arsovski, S., Kokić Arsić, A., Rajković, D. & Savović, I. (2013). Struktura standardizovanih sistema menadžmenta [Standardize Management System Structure]. In: S. Arsovski (Ed.). *Integrisani sistemi menadžmenta* [Integrated Management System] (2nd ed.) (pp. 169-317). Kragujevac: FIN Kragujevac, Centar za kvalitet.

Arsovski, S., Vujović, A., Mišić, M., Nestić, S. & Gvozdenović T. (2013). Merenje i praćenje [Monitoring and Measurement] performansi IMS-a. In: S. Arsovski (Ed.). *Integrisani sistemi menadžmenta* [Integrated Management System] (2nd ed.) (pp. 375-450). Kragujevac: FIN Kragujevac, Centar za kvalitet.

Aven, T. (2008). *Risk Analysis*. Chichester: John Wiley & Sons, Ltd.

Aven, T. & Vinnem J.-E. (2007). *Risk management* (2nd ed.). Netherlands: Springer.

Bischoff, H.J. (2008). Risk profiles in modern work life. In: H.J. Bischoff (Ed.). *Risks in modern society – Topics in safety, risk, reliability and quality* (pp. 11-16). Netherlands: Springer.

Ball, D. & Ball-King L. (2011). *Public safety and risk assessment: Improving decision making* (2nd ed.). London: Routledge.

Charters, I. (2011). *A practical approach to business impact analyses, Undestanding the organisation through continuity management*. BSI British Standards Institution.

Dowell, A. & Hendershot, D. (2002). *Simplified risk analysis layer of protection analysis*, AIChE, 281a, 16-20.

Đapan, M. (2014). *Unapređenje modela za procenu rizika na radnom mestu primenom teorije fazi skupova i prognostike* [Improvement of model for risk assessement on work place using theory of fuzzy sets] (Theses). Kragujevac: FIN Kragujevac.

Ericson, A. (2005). *Hazard analysis techniques for system safety*. Chichester: John Wiley & Sons, Inc.

Golfareli, M. & Rizzi S.(2008). UML-based modeling for what-if analysis. In: IY. Song, J. Eder & T.M. Nguyen (eds.). *Data Warehousing and Knowledge Discovery. DaWaK 2008. Lecture Notes in Computer Science*, vol. 5182. Berlin, Heidelberg: Springer. https://doi.org/10.1007/978-3-540-85836-2_1

Haimes, Y.Y. (2015). *Risk modeling assessment and management* (4th ed.). NJ: John Wiley & Sons.

International Organisation for Standardization, International Trade Centre & United Nations Organisation for Industrial Development. (2015). *ISO 31000: Risk management – A practical guide for SMEs*. Switzerland: ISO. Retrieved from: https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/iso_31000_for_smes.pdf

Ishikawa, K. (1976). *Guide to quality control*. Asian Productivity Organisation.

ISO – International Organisation for Standardization. (2009). *ISO 31000:2009 Risk Management – Principles and guidelines.*

ISO – International Organisation for Standardization. (2009). *ISO/IEC 31010:2009 Risk management – Risk assessment techniques.*

Kiral, I.A. & Kural, Z. (2014). Risk identification in construction projects: Using the Delphi method. *11th International Congress on Advances in Civil Engineering, 21-25 October 2014, Istanbul Technical University, Istanbul, Turkey.*

Kokić Arsić A., Arsovski S., Kanjevac Milovanović K., Bojić B. & Savović I. (2013). The management decision for competitiveness improvement. In: *Technics Technologies Education management*. Sarajevo: Society for development of teaching and business processes in new net environment in B&H.

Kosow, H. & Gaßner, R. (2008). *Methods of future and scenario analysis – Overview, assessment, and selection criteria*. Bonn: German Development Institute. Retrieved from: https://www.die-gdi.de/uploads/media/Studies_39.2008.pdf

Lazić, M. (2006). *Alati, metode i tehnike unapređenja kvaliteta [Tools, methods and techniques for quality improvement]*. Kragujevac: Mašinski fakultet u Kragujevcu.

Leveson, N. (2011). *Engineering a Safer World: Systems Thinking Applied to Safety.* MIT Press.

MS/2. (2000). *British Standard BS 6079-3:2000, Project management – Part 3: Guide to the management of bussines related project risk*. BSI.

Mannan, S. (2012). *Lees' loss prevention in the process industries: Hazard identification, assessment and control*. Volume 1. (4nd ed.). Amsterdam: Elsevier.

Nikolić, B. & Ružić-Dimitrijević, Lj. (2009). Risk assessment of information technology system. *Issues in Informing Science and Information Technology*, 6, 21-22.

Rausand, M. (2011). *Risk assessment theory, methods, and applications*. NY: Wiley.

Reason, T.J., Carthey, J. & de Leval, M.R. (2001). Diagnosing "vulnerable system syndrome": an essential prerequisite to effective risk management. *Quality in Health Care*, 10 (Suppl II), 21–25. Retrieved from: http://qualitysafety.bmj.com/content/qhc/10/suppl_2/ii21.full.pdf

Standards Australia. (2004). *AS/NZS 4360:2004 Risk Management.*

Standard Councils of Canada. (2009). *CAN/CSA-Q850-97(R2009) Risk Management: Guideline for Decision-Makers.*

The Council of the European Communities. (1989). Council Directive 89/391/EEC of 12 June 1989 on the introduction of measures to encourage improvements in the safety and health of workers at work. *Official Journal of the European Union,* L 183, 29/06/1989, 0001 – 0008.

Ushakov, I. (2016). Avaliability. In: S. Gass & M. Fu. (Eds.) *Encyclopaedia of Operations Research and Management Science*. Volume 1. (3rd ed.) (p. 95). Springer US. Retreived from: https://link.springer.com/referenceworkentry/10.1007%2F978-1-4419-1153-7_46

Vorley, G. (2008). *Mini guide to route causes analysis*. UK: Quality Management & Training (Publications) Ltd. Retrieved from: http://www.root-cause-analysis.co.uk/images/Green%20RCA%20mini%20guide%20v5%20small.pdf

Ware, J. (2009). *A systematic analysis to identify, mitigate, quantify, and measure risk factors contributing to falls in nasa ground support operations* (Doctoral Dissertation). Florida: University of Central Florida. Retrieved from: http://stars.library.ucf.edu/cgi/viewcontent.cgi?article=4909&context=etd