https://doi.org/10.26552/com.C.2008.1.20-23

Pavel Danihelka – Pavel Polednak *

RISK ANALYSIS – GENERAL APPROACH

Motto: Zero risk does not exist

The article deals with a general theory of risk analysis and corresponding risk management and provides the overview of the systematic method of risk analysis based on the MADS-MOSAR concept. Risk is represented as a flux of danger and typology of sources of danger, flux mechanism and potential targets are described. Quantification of risk is done as a combination of uncertainty and impact of an unwanted event and risk management is based on safety barriers introduction to overall process described by combination of FTA and ETA, so called "bow-tie diagram".

1. Introduction

Risks are inherent parts of our world and lives and we deal with them in our everyday live regularly, often intuitively without awareness that what we are doing is the risk analysis and management. Examples are the crossing of a street in traffic, antivirus software use, preventive health care or contraception and we can find thousands of others.

The expression "risk" is used in many domains and in many more or less different meanings. In the domain of natural and technological disasters, the definition of risk as a combination of uncertainty and effect is used the most frequently. To control and to communicate risks, we need common understanding of some expressions and relations and also the understanding of the process of risk analysis and related risk management. In the following paragraphs we will explain the basic terms and principles.

2. Theory of risk as a process

First important understanding is the fact that risk is the process and that it contains the flux of danger. Schematically is this situation drawn in Fig. 1, where the model of risk developed by a MADS-MOSAR expert group [1,2] is presented.

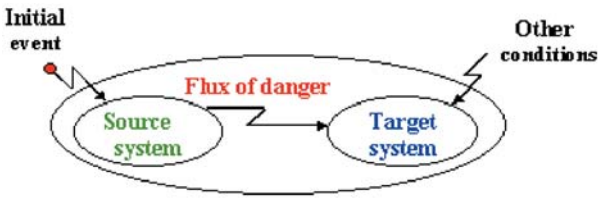

Fig. 1 Risk as a process involving the flux of danger [1, 2]

The expression "danger" is a little bit ambiguous and can reflect either "an exposure or vulnerability to harm or risk" (process) or "a source or an instance of risk or peril" (internal property). Important for the risk as a process is that we always have three key parts of it – source of danger, flux of danger and target system.

The *source of danger* [1] is composed of a system which contains internal energy or capacity to cause damage (impact). Generally, it is the system different from the target one, but in some cases, the source of danger and target systems can be identical; the energy sector is one of the examples, because the energy transmitted or generated can destroy the equipment of transmission or generation. Dangerousness is an internal property of the system and it usually cannot be separated or eliminated without a substantial change of the system. On the other hand, the dangerousness (danger) can be controlled and the risk managed in this way. An example is a sharply charged revolver. Its dangerousness as a capacity (energy involved) able to cause damage is the same in the case that we have it closed in a safety box as in the case that it is uncontrolled in a children's playroom. The risk is visibly different and what differs is the management of risk.

The *flux of danger* [2] is caused in one of the following ways:

- Flux of energy (heat, radiation, lightening, electric power, laser...)
- Movement of physical objects (means of transport, rotating parts of machines, fragments, water, falling structures...)
- Flux of information (data, signals, remote control...)

An important notice is that all risks are accompanied by some type of flux of danger, usually in chain. The break of this chain by safety barriers is the basic principle of safety.

The *target system* is what is influenced negatively by flux of danger and what suffers from the impact. Sometimes it is not easy to define properly the target system because of further indirect

* **Pavel Danihelka, Pavel Polednak**
Department of Fire Engineering, Faculty of Special Engineering, University of Zilina, E-mail: Pavel.Danihelka@fsi.uniza.sk

consequences. In the model case – energy transmission system (TSO – Transmission System Operation), the direct consequence is for the blackout, but the real impact is the break of operation of industry and infrastructures, societal discomfort and turbulence and for the TSO, the loss of image, commercial impact and even stricter regulations from the government side. Generally, the secondary impacts are much more serious than primary ones; in process industry the difference is estimated to be 3 to 100 times more.

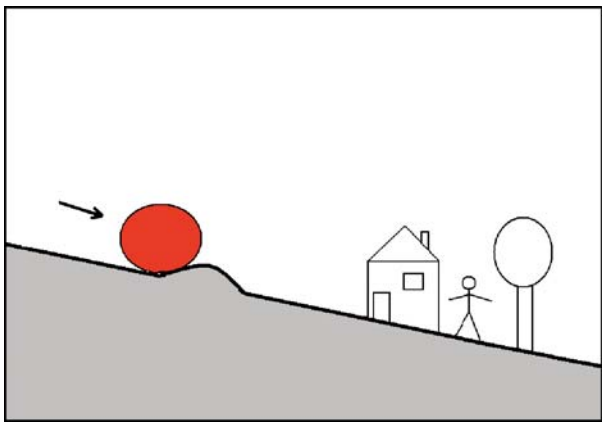

Fig. 2 Model of uncontrolled risk. Small initial event, e.g. the shock or pressure from left side, can move the shoulder to unstable position, trigger the flux of danger (potential energy of shoulder is changing to kinetic one and boulder moves) and the inertia of boulder destroys target systems (house, man and environment)

For the TSO, we generally have four types of target systems:

- Functioning of the TSO – transmission of energy according to demands. It is inherently linked to other systems
- Human lives, health and well-being
- Property and equipment
- Environment

In other systems, for example in chemical process industry, targets are similar [4].

The simplified example is in Fig. 2, describing the risk caused by fall of an unstable boulder.

3. Risk analysis principles

To efficiently face the risk, we need to identify and to understand the risk and its importance because we cannot successfully prevent unknown risk. From this reason, the risk analysis is crucial part of continuity business management and it is usually directly linked to risk management. The risk analysis and management process always contains certain steps which make the process of risk analysis systematic; nevertheless, we sometimes find only the part of this process which poses to be full risk analysis.

Systematic risk analysis consists of the following steps:

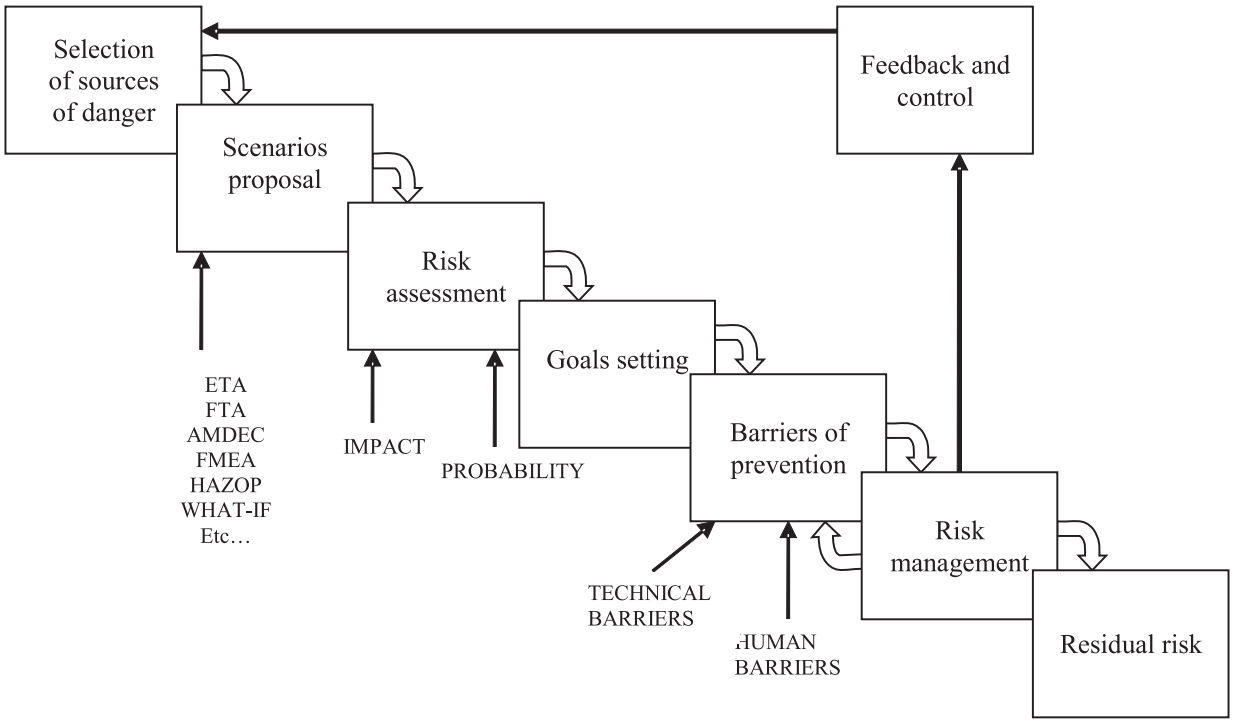

Fig. 3 Process of risk analysis and management

Before risk analysis, it is necessary to define the system which will be analyzed and to divide it into sub-systems. The reason for this step is that the analyzed system is usually too complex to be understood in one simple step. The division should be made either according to physical boundaries or according to the function of sub-systems. It is envisaged to always define as one subsystem environment and as another (but separated from technical equipment) operators. The reason is that environment phenomena and human errors are the most frequent causes of accidents.

Selection of sources of danger is a crucial part of risk analysis. When searching for them, the experience of personnel as well as imagination is important. What should not be neglected is the possibility of so called domino effect, where the series of events represented by flux of dangers happen and the original small initial event develops to disaster. The schematic view of domino effect is in Fig. 4:

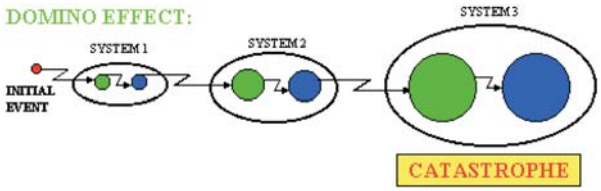

Fig. 4 Domino effect

Scenarios proposal is the second step of risk analysis and all important scenarios should be involved and evaluated. This step is imagination-demanding and what is important, is that all the phases of the life-cycle of installation must be considered. Frequent sources and periods of accident are start-up and shut-down procedures, maintenance, reparations and changes in concept or even dismantling of facility. In the preliminary step, all plausible scenarios should be studied, but only a reasonably low number of generalized ones (few tens at maximum) should rest to the end of the risk analysis process. The main obstacle of this step is the neglect of some important scenarios and often, the human factor reliability or environmental forces are underestimated. There are several tools to help find relevant scenarios and their detailed description is beyond the scope of this document. A general condition is that the scenario is a model of reality; we expect certain behavior of the system under study and evaluate them. Sometimes, we meet the opinion that a certain scenario cannot happen. This conclusion is wrong in all cases when the scenario is physically possible; in such a situation, this is only a question of higher or lower probability.

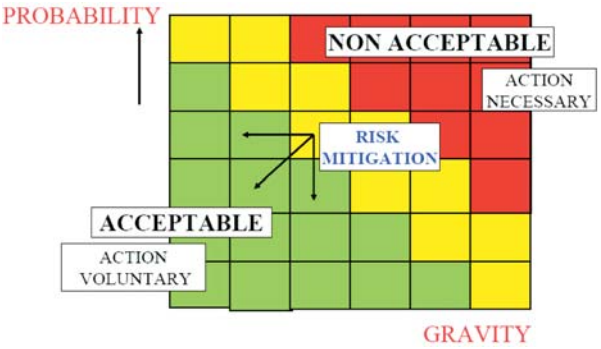

Fig. 5 Risk matrix

Risk assessment is based on the evaluation of two components, uncertainty and impact. As both of them may be quantified, the risk is quantifiable as well. A usual form of the expression of risks is the risk matrix:

Each scenario has certain probability or frequency and it creates a certain level of impact, so the corresponding risk can be located in the matrix. When the risk matrix is prepared, the following principles are recommended:

- Axis scales should be logarithmic or correspond to multiplication, not addition. The example is in frequency expressed as 10^{-2}, 10^{-3}, 10^{-4}/year. Axes can be semi- quantitative, it means that the levels like "frequent" or "extremely rare" can be used, but the consensus what it means is necessary.
- The number of levels is 3 – 6, we are rarely able really differ in a more detailed scale because of uncertainty of the datas available.
- Top management decision is necessary to set-up scales and acceptability of risk. When acceptability is discussed, keep in mind that large (even supposed) distance in time or space shift psychologically risks to an acceptable area and risk are underestimated by top management. Examples are frequent, the most significant being Challenger [5] or Chernobyl [6] disasters.
- All risks should be presented in one matrix, despite of the type of impact. Such "harmonization of scales" among others clearly declares the value scale of top management
- The scales of values and acceptability of the risk should be decided before the analyses are done, otherwise we risk that the scales will be distorted to fit an optimistic view.

4. Risk management

The risk matrix is a basic tool of risk analysis and management. Scenarios (risks), which are in a non-acceptable area, should be managed immediately but also risks in an acceptable area can be managed voluntary. The decrease of risk is done by decreasing the impact or decreasing probability of an event or both.

The moment where risk analysis comes to risk management is the *Goals Setting*. In the simplified form, the goal setting is the decision to decrease risks to an acceptable level in a decided timeframe. When managing risk, we attempt either to remove or to decrease the source of the risk or we attempt to put barriers to some steps of the scenario. Again, in a schematic simplified form, the setting of barriers is represented in Fig. 6

The principles described in Fig. 6 are general and can be applied in various ways, nevertheless it is not recommendable to rely on a single barrier because any of them may fail. As the result,

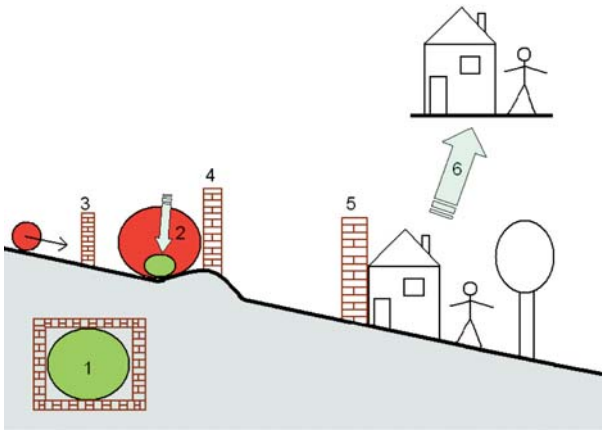

Fig. 6 Barriers of prevention: 1 – source of danger removal, 2 – source of danger minimization, 3 – prevention of initial event (triggering), 4 – prevention of flux of danger, 5 – protection of the target, 6 – protection of target by removal from the flux of danger

so called Ementhal cheese principle is applied. Safety barriers are like slices of Ementhal and protected with some gaps only. If throws are in the same positions at all slices, it means in alignment, Ementhal cheese barriers do not protect, the event will hit the target. So we need more than one barrier and to organize them so that no series of throws will lead directly to the target.

When considering the barriers, two main types are used, technical barriers and human (organizational) ones. Technical barriers, both well active and passive, are generally more reliable but always the use of some organizational barriers are envisaged from two principal reasons: Firstly, technical barriers have no imagination and creativity so they only function for the the situation they were designed for; human barriers are more flexible and creative. Secondly, the safety based on technical barriers creates the false feeling of perfect safety and people tend to sub-estimate risks and to neglect safety measures and behavior. An example can be found in the countries of Central and Eastern Europe in the early 90's, where after opening the market to new sophisticated cars the number of serious accidents increased because drivers believed that a technically perfect car would solve any situation.

After negotiation and setting-up the barriers, the process of risk analysis should be repeated with taking the barriers into account. They decrease either gravity or probability of an accident but they can bring other new risks which should be evaluated as well.

A very important fact is that we can never eliminate the risk totally; zero risk simply does not exist. The last step of risk analysis is thus the description and understanding of residual risks, which are not prevented and so they must be dealt with by crisis preparedness and management.

Acknowledgement: This publication is supported by EU Leonardo da Vinci Programme, Project UNDERSTAND, contract No. SE/06/B/F/PP-161031

References

[1] VERDEL, T.: *Methodologie d'evaluation globale des risques,* Presses de l'Ecole nationale des pontes et hausses, Paris, 2000, ISBN 2-85978-334-2
[2] *http://www.agora21.org/ari/*, acces 20. 10. 2007
[3] DANIHELKA, P.: *Analysis and Management of Industrial Risks*, VSB – TU Ostrava, 2002, ISBN 80-248-0084-5
[4] KIRCHSTEIGER, C., CHRISTOU, M. D., PAPADAKIS, G. A: *Risk assessment and Management in the Context of the Seveso II Directive,* ELSEVIER, Industrial Safety Series, Amsterdam, 1998, p. 537
[5] *Report on the Presidential Commission on the Space Shuttle Challenger Accident,* By Southgate Publishers, DIANE Publishing Company (1995), ISBN 0788119125
[6] *Japan Science and Technology Agency (JST) Failure Knowledge Database,* http://shippai.jst.go.jp/en/
[7] OECD: *Guiding principles for chemical accident prevention, preparedness and response Environment Monograph No 51,* OECD/GD 43, OECD Environment Directorate, Paris, 1992.