COMMUNICATIONS

Dear reader,

Safety, security, danger and risk are phenomena accompanying human communities during all their development. Related reactions involve the understanding of the mentioned subjects together with risk prevention and mitigation, preparedness and emergency response. Recent development of risks including new threats and emerging risks, together with lower societal acceptability of risk in modern society, have led to increasing demand of research and development in this area to the extent that the European Union declared security research as priority No 1. Communications, the scientific letters of Zilina University, follow the pathway of safety and security research by preparing this special issue dedicated to safety topics in the wide range from basis and principles of scientific discipline dealing with safety and security through basic research to applied science, development and practical issues of risk mitigation and emergency preparedness. The choice of topics reflects the spectrum of activities carried out on the field of security and safety and gives the reader an interesting insight to the development of this scientific orientation.

Pavel Polednak

https://doi.org/10.26552/com.C.2008.1.5-9

Karel Klouda – Stanislav Bradka *

ALSO THE 4TH DIMENSION OF THE TOWN – ITS UNDERGROUND STRUCTURES – HAS ITS RISKS

The article is devoted to risk assessment of underground structures from the point of view of their existence, operation and human failure (of users and/or operators). Two likely instances of their abuse for disseminating poisonous substances in an urban agglomeration are described. Both possibilities have been scrutinized using either physical simulation or an in-situ experiment. The distribution of agent depending on chosen parameters (agent's imitation, meteorological conditions, etc.) was verified on Prague's Old Town Square model in an aerodynamic tunnel. The in situ experiment with surrogates was performed at underground subway changing station. The parameters, results of the experiments and conclusions are discussed in detail.

1. Introduction

Apart from air pollution caused by exhalations and emissions from chemical, metallurgical and power generating industries, the biggest negative impact on the environment is the gradual occupation of land and free area by various construction development projects. The phenomenon has become extremely important particularly in connection with the fast development or expansion of urban agglomerations.

The space under the ground level (apart from extraction of raw materials) can be used for activities which are difficult to place and operate on the surface. The reasons may be e.g. technical, environmental or economic. Underground facilities are often situated in locations with adverse effects of the natural environment (aggressive underground water, distorted formations, pressures), and they are affected by operations in the underground facility and the time factor.

The processes require regular monitoring and diagnosing of defects of the underground structures, planning of maintenance and refurbishments and timely implementation of the planned measures (cement injections, waterproofing, anchoring, shot-concreting, safety elements etc.).

Poor maintenance increases risks associated with the operation of underground structures, such as traffic accident, fire, explosion etc.

Meanwhile, underground structures are very sensitive to technology failure as a result of sabotage or terrorist attack with the potential consequences – endangered lives and health of big numbers of people and disruption of municipal infrastructure. Underground structures, particularly line projects, may be for example abused for distribution (spreading) of dangerous chemical and biological substances on a large territory of the city. Also an explosion in a collector may have synergic effects, e.g. derailing of a subway train etc.

The above-mentioned facts have lead us to identification of risks and we also clearly recognized opportunities of potential abuse of some underground structures for spreading of poisonous agents in the urban agglomeration or direct application of such substances e.g. in an underground traffic structure.

For this reason we have performed some experiments using physical modeling and "in-situ" experiments with substitute chemical agents.

2. Determination of risks in underground structures

After the analysis we divided the risks based on association with:

a) the *existence of* underground structures,
b) the *operation of* underground structures,
c) the *human failure* of users or operators of underground structures.

a) Risks associated with the existence of underground structures
The risks are caving and sinking. The factors listed below increase the mentioned risks:
- effect of underground water (its chemical properties, temperature, flow rate, its effect on the rock, i.e. leaching, water bearing, swelling; its aggressiveness, i.e. acidity, content of mineral elements, sulphates, sulphanes, free carbonic acid etc.),
- the dead weight of lining,
- confining pressure (vertical, lateral, pressure on the stope bottom, lengthwise),

* **Karel Klouda[1], Stanislav Bradka[2]**
[1]State Office for Nuclear Safety, Praha, Czech Republic, E-mail: karel.klouda@sujb.cz,
[2]National Institute for Nuclear, Chemical and Biological Protection, Milin, Czech Republic, E-mail: sujchbo@sujchbo.cz

- loading with buildings and construction objects on the surface,
- long-term technological loading of underground structures,
- loading generated by operations on the surface,
- seismic effects,
- underground gases,
- underground temperature.

b) Risks associated with the operation of underground structures

b1) traffic line underground structures imply the following risks
- defect on one car or a railway set,
- traffic accidents with a property damage,
- traffic accident with an injury,
- traffic accident with a fatality,
- local fire,
- large fire,
- poisoning of persons with smoke and toxic products,
- explosion (explosive fire, detonation),
- destruction of building structures (structure collapse),
- burying and caving,
- suffocation of trapped persons,
- injury caused by electric power,
- scalding and burning,
- flooding,
- environment pollution,
- release of toxic substances.

b2) water management line underground structures imply the following risks
- pollution, contamination, poisoning of the medium,
- breakdown of the line and release of the medium in the environment, infection, epidemic,
- drowning.

b3) power engineering line underground structures imply the following risks
- fire,
- fire with explosion,
- loss of information and communication systems,
- leakage of media from the damaged distribution system,
- destruction of structures (collapse),
- burying and caving,
- injury caused by electric power,
- scalding and burning,
- flooding,
- contamination of air from ventilation shafts.

b4) hall-type underground structures imply the following risks
- fire,
- large scale fire,
- explosion,
- destruction of structures (collapse),
- burying and caving,
- suffocation of trapped persons,
- poisoning of persons with smoke and toxic products
- contamination of the environment.

c) Risks associated with human failure

Human failure, including accidental or deliberate actions, criminal acts or terrorist attacks imply the following risks
- violation of occupational safety rules, technical regulations, operating rules,
- violation of acts,
- civil unrest, occupation of portals, loss of access to the entries,
- theft, assault, murder,
- planting of an explosive, activation, explosion,
- application of an explosive with a contaminant,
- sabotage in the system,
- application of chemical and biological weapons.

Moreover, we used additional approaches available, i.e. selection of threats and their classification into those which endanger underground structures as a whole, those which have no effect on their safety and those which only affect a specific type of structure (e.g. an epidemic may endanger the subway operation).

Another potential approach was identification of the so-called TOP (main, key) events and initiations events (internal and external).

The analytic combination of the selected risks and threats and the identification and evaluation of initiation events allow to perform a very fast basic safety analysis for underground structures.

Subsequently, we provided examples of a potential abuse of underground structures and experiments we conducted to mitigate such threats and their impact.

3. Example of an Underground Structure abuse for Spreading of a Poisonous Substance in an Urban Agglomeration

As mentioned above, line underground structures may be abused for spreading of dangerous poisonous substances in urban agglomerations.

a) selection of the poisonous substance and location for the abuse

The selected substance for model abuse was sarin, i.e. nerve agent, classified as a chemical weapon. These agents are generally organic compounds of phosphorus featuring high toxicity for mammals, fast commencement of effects and penetration into organism through all portals of entry.

The reasons to select sarin included:
- its relatively simple preparation from available materials (CH_3Cl, $AlCl_3$, PCl_3, NaF, SbF_3, 2-propanol),
- its higher vapor pressure compared to other nerve agents (385.7 Pa, 25°),
- its slight odor,
- its latent effect.

We also considered the location for sarin abuse and when and which method to use to release sarin into the atmosphere. We

selected the Old Town square (Staroměstské náměstí) during the striking time of the Astronomical Clock and the method was spilling or by abuse of outlets of the underground structures under the square surface. For additional tests in an aerodynamic tunnel and for the "in-situ" method it was necessary to find an agent meeting at least partly the following criteria:

a) similar physical and chemical properties,
b) easy detection (including subjective response to smell or odor by the experimenting persons),
c) acceptable toxicity and labor safety while working with the agent,
d) availability (delivery, price).

Based on a comparison of basic physical properties (boiling point, vapor pressure) with sarin we opted for pentyl-acetate as a substituent. However, the published dependences of kinematic and dynamic viscosities and diffusion coefficient on temperature were not completely identical and therefore we had to use a graphical correlation comparison [1].

b) physical modeling of spreading of hazardous materials (sarin substituent, propane, aerosol) in the Old Town Square and its surroundings

Most human activities (including negative ones) are performed on the Earth surface surrounded with the so-called atmospheric boundary layer (ABL). Above ABL there is free atmosphere and bottom part of ABL is called the surface sublayer. The methods for description of flow patterns in ABL and thus also the spreading of hazardous agents are:

- mathematical modeling,
- physical modeling,
- direct measurement in the field ("in-situ").

Mathematical modeling consists in numerical solution of motion equations (non-lineal partial differential equations).

The method is still used particularly in cases with simple geometry – planar or slightly undulated ground.

The physical modeling is for more complex cases, e.g. for territories with a high density of structures (town centers). The method uses an analogy between flow patterns near the Earth surface and flow patterns near a wall in a special aerodynamic tunnel. The model requires development of a suitable geometrically similar model which forms a tunnel wall.

Our model of the Old Town Square was based on 45 first line core buildings and palaces. They were detailed replicas as shown in Fig. 1, of hardened polypropylene with a coat of façade paint. The used scale was 1:160. The total model was subsequently placed in an aerodynamic tunnel in the Institute of Thermomechanics of the Academy of Science of the Czech Republic in Nový Knín.

We modeled spreading of the sarin substituent – pentyl-acetate, "inert" propane and CO_2 aerosol + glycerin.

We selected the following four points in the Old Town Square as model source points from which the substituent (inert agent, aerosol) was released into do ABL:

- in front of the town hall tower (Town Hall),
- in Male namesti in front of the U Princů restaurant,
- at the end of Parizska street on the Old Town Square,
- next to the statue of J. Hus.

The point source – was an opening with the diameter of 0.4 cm at the surface level of the model for propane and aerosol, for pentyl-acetate we used an evaporation micro-bowl (1.5 x 1.5 cm).

Based on meteorological data about prevailing flow patterns in Prague 1 we selected the following wind directions:

Fig. 1: Model of the Old Town Square in the aerodynamic tunnel [Source: own]

- north-west,
- west-north-west,
- west,
- south-west.

An example of results of physical modeling of distribution of horizontal concentrations of pentyl-acetate and propane in the west wind from one of the selected points (sources) in the Old Town is shown in Figure 2.

A comparison of sizes of concentration fields for pentyl-acetate and propane shows a significant difference. One of the main reasons is that pentyl-acetate is the so-called active admixture, it is adsorbed on the model bottom surface and particularly on the walls of buildings (see the vertical profile or visualization of flow patterns [2]. Unlike pentyl-acetate, propane is the so-called passive admixture. Based on dimensionless concentrations the measurement results with propane have been identified as the worst potential variant of spreading of a hazardous material in the given location.

by abuse of poisonous war gases as a result of a criminal or terrorist act. For this reason the Ministry of Interior – General Directorate of Fire Rescue Service of the Czech Republic (GR HZS CR) strongly focused on this issue. The State Office for Nuclear Safety focused on one partial problem, i.e. on contamination of the subway premises and spreading of the contaminant in its premises.

For this purpose we used an "in-situ" experiment, i.e. we released substituent of the poisonous sarin (pentyl-acetate) in the area of the subway station "Muzeum", which is a junction of the C and A subway lines.

The agent was released on the platform of the "Muzeum" C station during the operation of subway trains and without operation of subway trains with winter ventilation (air intake into the space between stations, air extraction from the station via an exhaust shaft).

The speed and concentration gradient was determined in 7 measuring points (platform, escalator, corridors, lobby), and the

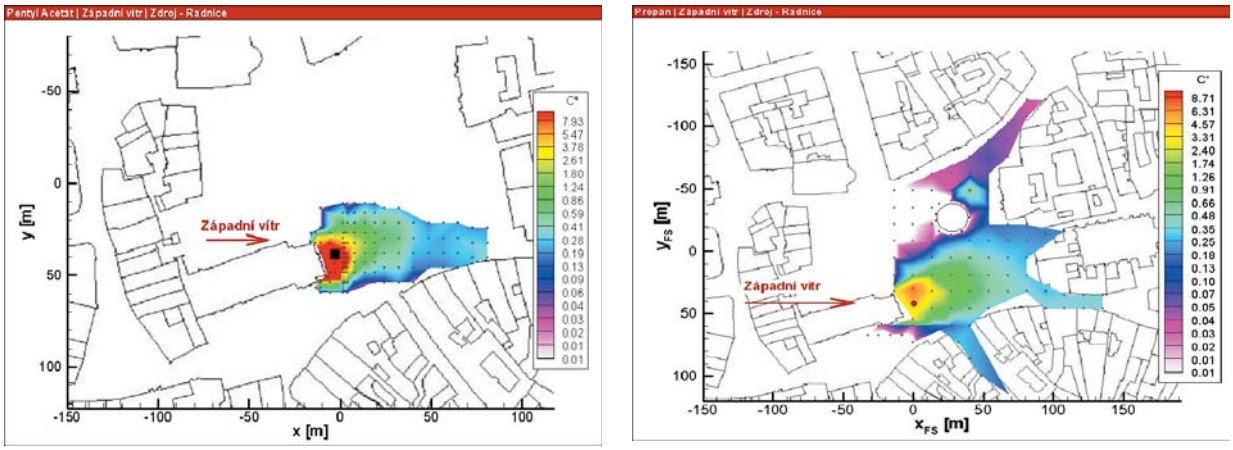


Fig. 2: Horizontal distribution of concentrations of pentyl-acetate and propane, with the source location in front of the town hall tower

We used modeling to select a place for the contaminant release within the square and the wind direction resulting in contamination of the entire Old Town Square.

Also capillary action of the agent was demonstrated at higher levels in the buildings compared to the square center (vertical concentration profile2). Experimental results from the aerodynamic tunnel were transformed into the MS Excel format compatible with geographic information systems (GIS) and they were provided to the Ministry of Interior of the Czech Republic and to the City Council of the Capital of Prague.

4. Example of abuse of Traffic line Underground Structures (Prague Subway) for spreading of Poisonous Agents

The Prague subway is a major traffic junction with a high concentration of persons and it may be a place potentially endangered

concentrations were also measured at the exhaust shaft and in the trains. The spreading results were processed but they are subject to special confidentiality regulations.

Apart from results of the experiments the report also contains a description of systems in the Prague subway (e.g. method of ventilation, station dimensions, types of trains, passenger turnover, time intervals of passenger movement etc.) and a list of factors affecting the real effects of the poisonous agent:

- spatial layout of the station,
- passability of exits from the stations,
- intensity and direction of flows in the station,
- intensity and direction of air intake from ventilation shafts,
- type of subway trains,
- operating schedule of subway trains,
- quantity of spread poisonous agent,
- toxicity of the poisonous agent,

- method of spreading (evaporation – aerosol, pressure – explosion),
- location from which the poisonous agent is spread,
- chemical and physical properties of the poisonous agent,
- adsorption and condensation of the poisonous agent on construction lining materials in the station (marble, eloxal coated aluminum),
- adsorption of the poisonous agent on clothes and hair of passengers and reverse desorption,
- chemical stability of the poisonous agent,
- temperature, pressure, air humidity inside and outside the station,
- concentration (density, turnover) of passengers in the station premises,
- demographic distribution of passengers in the station premises,
- physical parameters of passengers (body weight, height) in the station premises,
- psychological parameters of passengers – ability to respond to the event,
- mob frenzy – suggestion, panic,
- time of problem identification in the station,
- professional approach by the station dispatcher and Integrated Rescue System elements,
- response time to call help and hand over of qualified information (identification of the poisonous agent),
- relative delay of evacuation, decontamination, medical first aid for the afflicted passengers.

Each factor was analyzed and discussed. In some cases the analysis was supported with our own experiments, e.g. for adsorption and desorption of the poisonous agent on the subway station lining we measured the actual evaporation speed of sarin, depending on the air flow speed, we measured adsorption on different types of clothes etc.

5. Conclusion

Without the use of underground premises it is impossible to address some transport and infrastructural needs in many urban agglomerations.

However, the underground structures shall be resistant to negative effects of the natural environment, they are influenced by the operation, they represent a weak point for technology failure, sabotage or terrorist attack.

We determined risks to which the underground structures are exposed, selected threats and identified internal and external initiation events.

The purpose of the performed experiment on the Old Town Square model in the aerodynamic tunnel was to demonstrate the importance of physical modeling in urban agglomerations. The results obtained from this exposed location may contribute to better orientation of rescue service elements in case of an extraordinary event.

The "in-situ" experiments in the junction station of the Prague subway were very demanding in terms of organization. The spreading of the substituent of poisonous agent proved to be dramatically different with passing trains in the station and without the trains. One of the findings critical for safety was that if the trains are stopped from passing the deeper station premises will not be endangered by contamination (release of agent in the upper station).

References

[1] KLOUDA, K., DUDACEK, A., BEZPALCOVA, K.: *Reflection on "home-made" sarin*, Proc. of Pozarni ochrana 2006, Ostrava, p. 169, ISBN 80-86634-88-4

[2] KLOUDA, K., BEZPALCOVA, K., JANOUR, Z.: *Physical modeling of spreading of hazardous materials in the Old Town Square and its surroundings,* Proc. of Nebezpecne latky 2006, Ostrava, p. 61, ISBN 80-86634-91-4.

https://doi.org/10.26552/com.C.2008.1.10-15

Vaclav Nevrly – Petr Bitala – Petra Nevrla – Michal Strizik *

KNOWLEDGE-BASED EMERGENCY PLANNING FOR STORAGE TANK FARMS

Major accidents in storage tank farms can result in severe threats for emergency responders, neighbouring population and the environment as it was observed in the case of Buncefield (2005). The numerical modelling of dangerous phenomena is an important tool to support emergency planning for such complicated events. For this purpose, the case study in crude oil tank farm involving selection of reference accident scenario, CFD simulation of tank fire and prediction of delay to boilover was performed. The results were used to review the existing emergency plans and to enhance the tactical preparedness of emergency responders.

1. Introduction

Storage tanks are one of the most common types of technological units. They are often located in large industrial areas in the section with other storage equipment or in the close proximity of the different installations containing hazardous chemicals. It's not an exception that the large flammable liquid (especially crude oil) storage tanks with the volume capacity more than 100,000 cubic meters are constructed all over the world. Therefore the accidents in storage tank farms are associated with the strong potential to cause the domino effects and major loss. The historical experience with the accidents in Czechowice (1971), Litvínov (1996) described in [1] and more recently the lessons learned from Buncefield (2005) have confirmed that fires in storage tank farms can result in prolonged emergency situation and severe threats for emergency responders, neighbouring population and the environment. The industrial fires are generally coupled with the dangerous effects thermal radiation, the huge production of smoke (soot particles). In specific cases, the tank fire can be accompanied by boilover phenomenon.

2. Statistical review

Emergency response planning and preparedness for such complicated events requires reliable information concerning the accidental phenomena and their dangerous effects. The LASTFIRE project maps the fires of atmospheric open top floating roof tanks with large diameter (greater than 40 m). During the period of 1981–1995, 55 fires occurred on 2402 tanks observed for the sum of 33,909 tanks a year. 52 out of 55 fires represent the rim seal fires, full surface fire following the sinking of the roof was reported only in one case [2]. Chang and Lin [3] reviewed 207 flammable liquid tank fires in the period of 1960–2003 of which 66 represent the crude oil tank fires. The frequency of floating roof storage tank fires in Europe was statistically estimated to be about 1×10^{-3} per tank a year for rim seal fires. More severe tank fires are expected to occur in order of 3×10^{-5} per tank a year [3]. Tank fire study of Persson & Lonnermark [1] reported 20 cases of boilover (14 of these in the crude oil tanks) during the period of 1951–2003.

3. Modelling as a tool to support emergency preparedness

From the above stated data we can say that the industrial fires of large extent are relatively rare and the majority of fire fighters and emergency responders face up to this kind of situation once or a few times of their professional carrier. Scientific knowledge about this phenomenon is based mainly on the results of experimental observations and the mathematical modelling performed in different scales from the micro-scale laboratory studies to real-scale fire measurements and testing. Hence, the modelling and simulation of dangerous phenomena is an important tool to support decision making in the context of the emergency planning and to improve the tactical preparedness of emergency responders. As a first step needed to set up the efficient emergency plan the selection of relevant accidental scenario should be carried out before the model of given case of interest is employed. The plenty of risk analysis methods useful for this purpose exist, varying from fully qualitative and deterministic methods (e.g. expert judgement, preselected event checklist analysis) to quantitative and probabilistic approaches described extensively in [4, 5].

Recently available ARAMIS methodology [6] represents the alternative semi-quantitative approach to this step of risk analysis. Applicability of "Methodology for the Identification of Major Accident Hazards" (MIMAH) and "Methodology for the Identification of Reference Accident Scenarios" (MIRAS) published by Delvosalle et al. [6, 7] was examined by several case studies performed across Europe [8].

* **Vaclav Nevrly[1,2], Petr Bitala[1], Petra Nevrla[1], Michal Strizik[1,2]**
[1]VSB - Technical University of Ostrava, Faculty of Safety Engineering, Ostrava-Vyskovice, Czech Republic, E-mail: vaclav.nevrly@vsb.cz
[2]Institute of Thermomechanics, Academy of Science of the Czech Republic, Prague, Czech Republic

4. Reference Accident Scenario selection

Above mentioned methodologies (MIMAH and MIRAS), based on combined Fault Tree Analysis (FTA) and Event Tree Analysis (ETA) were employed to perform the initial phase of the case study in a real crude oil tank farm. This tank farm consists of 18 atmospheric open top floating roof crude oil storage tanks and related equipment and infrastructure. The whole tank farm was analysed in five individual sections:

- Storage tanks
- Input and output pipes to storage tanks
- Pipe corridor
- Pump stations
- Pipeline receiving and measuring unit

As the result of MIMAH and MIRAS methodology 25 most dangerous phenomena were selected based on matrixes for each section of the tank farm. These were summarized in 12 representative scenarios (RAS). The original criterion for selection of Reference Accidental Scenario (RAS) proposed by ARAMIS methodology was modified in order to reduce the number of considered scenario to a reasonable value. Although the wide variety of accidental events (e.g. spills or ruptures on pipes, flange fires, flash fires and vapour cloud explosions) could be considered for the above mentioned tank farm, only the selected scenarios are consequently used to estimate the risks (by detailed risk assessment methodology) as well as to give the preliminary list of emergency situations, which should be taken into account. But as the worst case scenario approach is commonly applied in the framework of emergency response planning, the full surface tank fire is often considered as the typical accidental scenario for tank farms.

5. Dangerous effects of storage tank fires

The tank fire is the specific case of pool fire and for the open floating roof tanks the tank fires are only associated with the collapsed or sunken floating roof and following ignition of flammable liquid (crude oil) pool formed within the tank shell. The turbulent diffusion flames characteristic for large hydrocarbon pool fires (tank fires respectively) represent very complex system involving tightly coupled phenomena of fluid dynamics, heat transfer and chemical reactions. The mechanisms such as air entrainment, combustion, and soot/smoke formation have a first-order effect on the local temperatures and radiative transport properties. Underlying these mechanisms is the turbulent fluid motion that creates, and responds to the large temporal and spatial fluctuations [9].

The hazards associated with such fires then occur on two separated length scales. Near the fire, over distances comparable to the flame length, the radiant energy flux can be sufficiently high to threaten both the structural integrity of neighbouring structures and equipment and physical safety of firefighters and plant personnel. At much greater distances, typically several times the plume stabilisation height in the atmosphere, the smoke and gaseous products generated by the fire can reach the ground in concentrations that may be unacceptable for environmental reasons [10]. The phenomenon of smoke plume was extensively studied in the context of in-situ burning of oil spills [11]. Remote-sensing (UV spectroscopic) measurements performed during Buncefield fire in December 2005 revealed elevated trace gas concentrations of SO_2 (70 ppbv), NO_2 (140 ppbv), HONO (20 ppbv), HCHO (160 ppbv) and CS_2 (40 ppbv) [12].

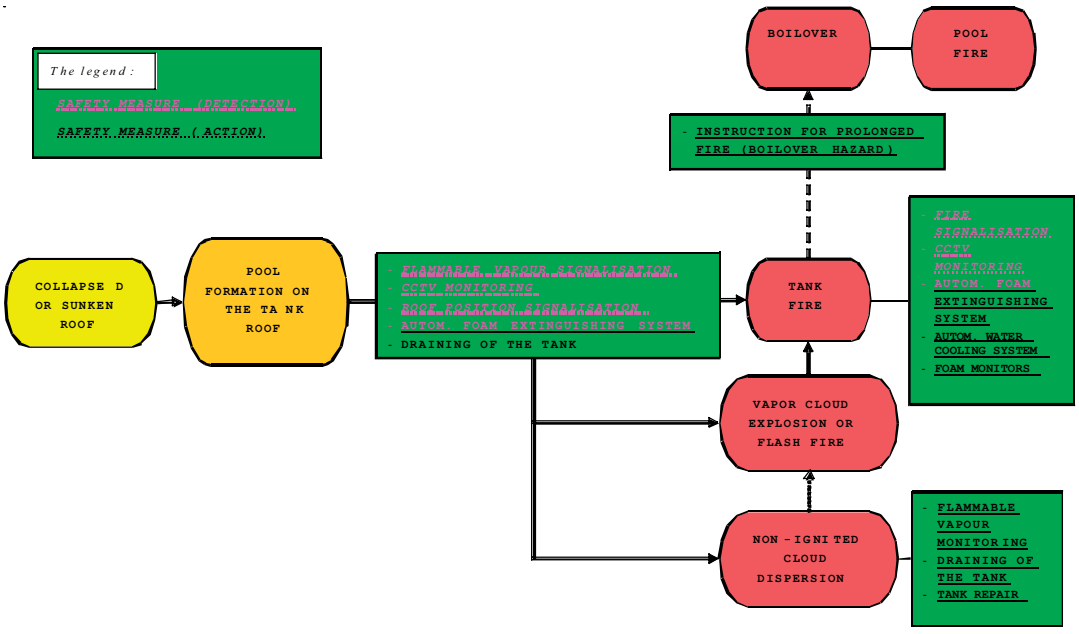


Fig. 1 Event tree for RAS - Collapse of the tank roof with the list of safety measures (barriers)

The special type of hazard associated with the crude oil tank fires is the formation of heat wave (hot zone) which propagates due to distillation process towards the tank bottom. In the case of prolonged tank fire consequent boilover phenomenon can occur. Boilover is a dangerous accidental phenomenon, which can lead to serious injuries to emergency responders. The boilover can occur several hours after the ignition of tank fire. The delay time is an unknown parameter of strong importance when managing the emergency response operations in oil tank farms. Hot zone formation and propagating process is the principal aspect of boilover phenomenon, which was experimentally studied in small and medium scales [13–15].

These experiments confirmed that several conditions and parameters of flammable liquid should be satisfied to enable occurrence of boilover after the prolonged tank fire. These parameters are mainly the range of boiling temperatures of the mixture components and viscosity. By the simplified way we can define that boilover can occur only in viscous flammable liquid mixtures with the mean boiling point above 120 °C and with wide distillation range. Three stages of boilover propagation are distinguished by Fan et al. [13] namely the:

- *Quasi-steady period* – the flame height is rather small and combustion is stable
- *Boilover premonitory period* – the flame height is fluctuating, caused by the water boiling on the fuel-water interface, emitting a 'crackling' sound
- *Boilover period* – the flame height increases quickly to the highest point and burning fuel is sprayed out of the tank

6. Approaches to large storage tank fire modelling

Mathematical modelling and simulation of dangerous phenomena allows us to determine desired characteristic features of assessed scenario and to prepare the corresponding safety measures. For emergency response planning and scenario-based training the threat zones (safe distances respectively) need to be estimated for selected scenario and different conditions (e.g. meteorological and technological) based on state-of-the-art modelling tools.

According to [16] the mathematical tools for predicting the radiative heat flux at the tank surroundings can be dividend broadly into three classes:

- Semi-empirical (point source and solid flame) models
- Field models
- Integral models

Point source semi-empirical models simplify the flame as a source term of radiative heat flux to be a single point usually located in the middle of the flame height. The fraction of heat of combustion, which is emitted from this point, is related on properties of fuel (sooting tendency) and diameter of the fire. These models over-estimate the heat radiation flux near the source, thus it should be used only for distances from the flame as far as approximately five pool (tank) diameters.

Solid flame models assume the flame as a surface emitter of heat radiation. This assumption can be enhanced by dividing the flame into two parts; first clear, strongly radiating lower part and second obscured by the layer of smoke soot particles which absorb the huge part of the incident heat radiation. Further refinement of this schema is possible to capture this characteristic feature of large scale hydrocarbons fires.

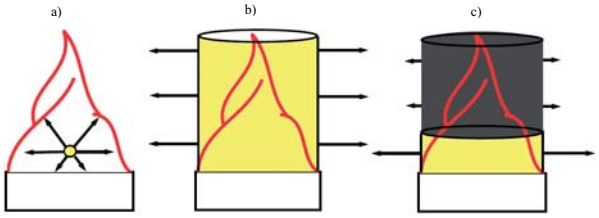


Fig. 2 The schematic typology of semi-empirical tank fire models (radiative source term assumptions modified after McGrattan at al. [19]); point source model a); solid flame (surface emitter) conventional model b); solid flame (surface emitter) modified model c)

As the semi-empirical models are relatively simple to understand and readily embodied in simple computer programs they are ideally suitable for routine risk assessment purposes. Moreover they provide relatively reliable (experimentally verified) prediction for low computational cost (available as on-line calculation tools).

Field models are based on numerical solution of balance equations for mass, momentum, species, energy and other desired variables in the computational domain divided into plenty of grid cells. Computational Fluid Dynamics (CFD) tools used to solve system of partial differential equations (PDE's) for turbulent flows represent mathematically complex tools with the pronounced requirements for computational time and hardware instrumentation. To carry out the phenomenon of tank fire, which can be described as buoyancy driven turbulent flow involving chemical reactions, several assumptions and sub-models need to be add to this system of equation.

Integral models were developed as the compromise between the field models and semi-empirical models. They are formulated in the similar way as the above-mentioned CFD models. Integral models are based on solution of conservation equations for mass, momentum and scalar variables in chemically inert or reactive flows. These equations are expressed in the integral form assuming the statistical similarity of variations of variables flow and combustion in the direction normal to flame axe. Thus the partial differential equations (PDE's) solved by the field models are integrated and reduced to form the ordinary differential equations (ODE's).

Unfortunately, the semi-empirical models implemented in standard computational tools for accidental scenario assessment are suitable for on-land or on-water pool fires rather than for large storage tank fires. These fires are specific by their exceptional

dimensions (diameter up to 100 meters) and disposition (base of the flames about 20 meters above ground). To involve the effect of tank height, the calculation algorithm had to be partly modified (in order to correct the view factor). Also there is considerable lack of experimental data for such a large scale of fires to set up and validate the empirical correlations. For these reasons the CFD (field) modelling of full surface tank fire was performed.

7. CFD simulation of crude oil tank fire

The Fire Dynamics Simulator (FDS, version 4.0 described in details in [17]) developed by NIST (National Institute of Standards and Technology) was used to determine the safe distances[1)] for fire fighters (based on heat flux levels in the tank surroundings) and to estimate the smoke plume movement in the different atmospheric conditions. The computational domain selected for simulation involves 4 crude oil storage tank (white objects) and fire fighting water reservoir (grey object) which represent the local geometry, see Fig. 3 a). As FDS 4.0 supports only the rectangular grid the entire volume of computational domain was divided into uniform grid consisting of 80 × 100 × 60 cubes with 4 meters side. All of the objects are specified as groups of rectangles fitted to this grid. The diameter of each tank is 84 m, the height 24 m.

The fire was defined on the roof of one crude oil tank. The grid resolution used for these simulations is consistent with the proposal given by Ma and Quintiere [18]. By their results FDS simulation data were found to fit well with empirical correlation for grid size equal to the characteristic length of the fire divided by twenty. The fire was assumed to burn with the heat release rate of 1900 $kW.m^{-2}$, which is equivalent to mass burning rate of 0.045 $kg.m^{-2}s^{-1}$ and heat of combustion of 42,600 $kJ.kg^{-1}$ (the data adopted from [19]).

The stoichiometric coefficients for the fuel, oxygen and burned gases were set to be that of propane and 13 % of the fuel was estimated to convert into the solid soot particles (in agreement with [20]). The local radiative fraction was determined as the default value, 35 %. Thus, approximately a third of released energy is emitted as thermal radiation. As the thermal radiation penetrates the thick layer of smoke and combustion products, the fraction of this energy is reabsorbed by the burned gas molecules and soot particles. Therefore the effective radiative fraction was found to give much lower values (by the conclusions of Baum [10] about 6 %). The above-described phenomenon is often called the smoke blockage effect, see Fig. 3b).

The results of simulation (both the instantaneous and temporally averaged data) confirmed that for the given accidental scenario relatively low radiative flux intensities can be expected for low speed wind conditions. As the wind speed augments, the flame is more and more tilted and heat flux in the downwind direction becomes dangerous for exposed personnel and equipment, see Fig. 4. Due to possible fluctuations of wind direction the both neighbouring tanks should be cooled by the installed water curtain system to avoid the fire escalation although this scenario is of very limited probability.

8. Boilover phenomenon modelling

As the boilover is the phenomenon, which can cause very serious consequences, the mathematical model was used to esti-

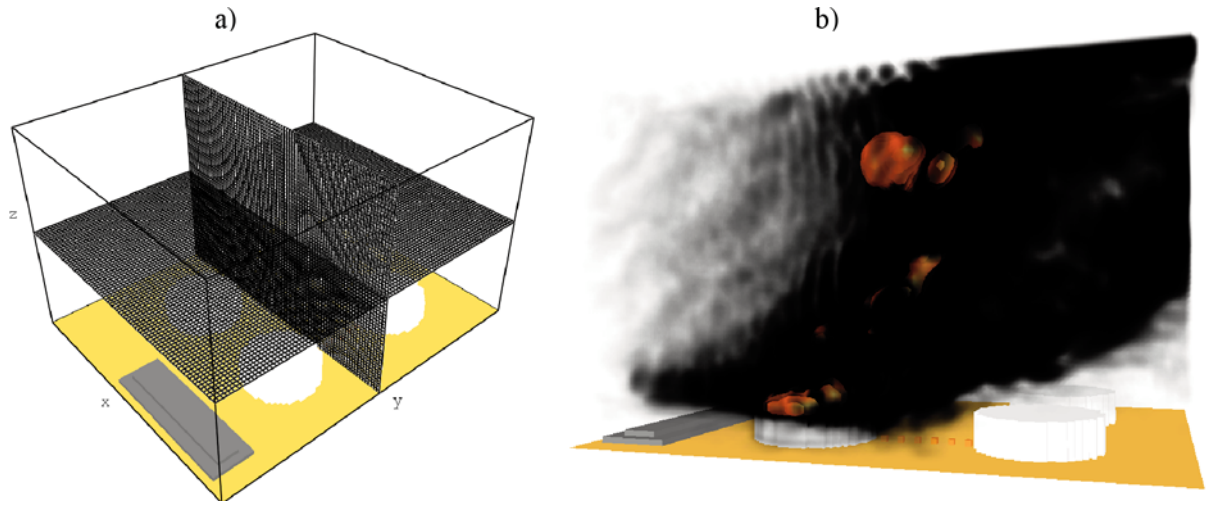


Fig. 3 Computational domain (x = 320 m, y = 400 m, z = 240 m) used for CFD large eddy simulation a); and the instantaneous screenshot from simulation of tank fire b)

[1)] The different data are available for human vulnerability to heat radiation. Commonly the heat flux values in range between 1.5 $kW.m^{-2}$ and 2.0 $kW.m^{-2}$ are recognised as threshold limit for long-term exposition without irreversible effects.

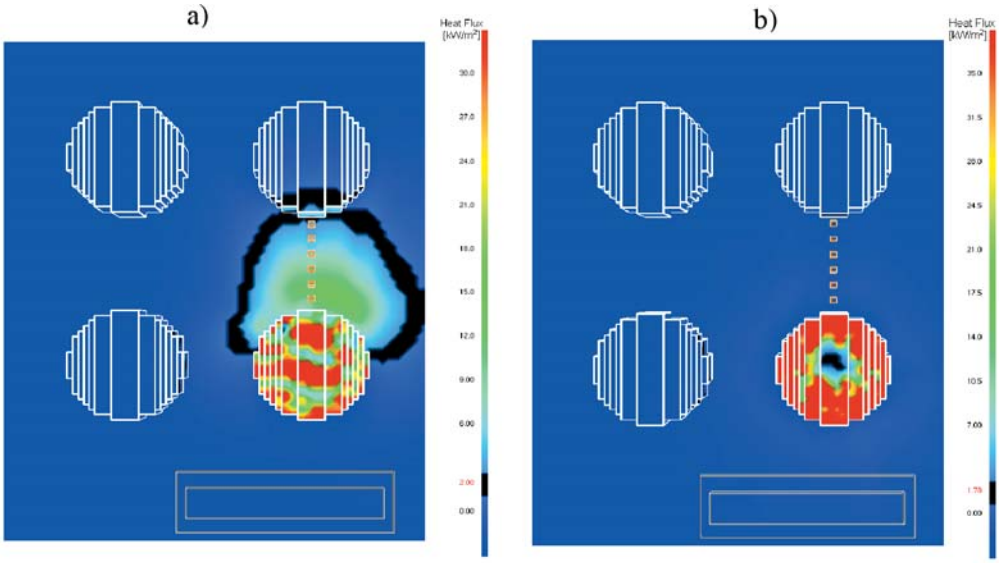


Fig. 4 Instantaneous heat flux profiles at ground level under different atmospheric conditions; plot of 2 kW.m^{-2} isocontours (black coloured) for a wind speed of 5 m/s in the height 3 m above the ground a); and plot of 1.78 kW.m^{-2} isocontours (black coloured) for a wind speed of 1 m/s in the height of 3 m above the ground b)

mate the time delay to boilover which should be understood as the time available for emergency response on site. The model is based on model previously published by Broeckmann [14]. Due to lack of available data for different crude oils the model was simplified to obtain the value of hot zone expansion rate, v_{HZ}, only from distillation curves, densities and basic thermodynamic properties known for a given crude oil, see equation (1).

$$v_{HZ} = \frac{\Phi_R}{\rho_{T_0} \cdot \left(X_{THZ} \cdot \left[\Delta H_{v,T_b} + \int_{T_0}^{\overline{T_b}} c_p dT \right] + (1 - X_{THZ}) \cdot \int_{T_0}^{T_{HZ}} c_p dT \right)} \quad \mathrm{m \cdot s^{-1}} \tag{1}$$

Here Φ_R is the radiation feedback (W.m^{-2}), ρ is the density of crude oil (kg.m^{-3}) and c_p is heat capacity of the crude oil (J.kg^{-1}.K^{-1}) and $\Delta H_{v,Tb}$ the heat of vaporisation at the boiling point (J.kg^{-1}). Temperatures needed for calculation are as follows; T_0 is the storage temperature of crude oil (K), T_{HZ} is the estimated hot zone temperature (K) and $\overline{T_b}$ is mean boiling point of crude oil (K). Vaporized fractions X_{THZ} are determined from the known distillation curve for estimated range of temperatures T_{HZ}. The present model describes the heat wave propagation (hot zone expansion rate), which is the principal aspect of the boilover phenomenon, in a very simplified manner. The following set of hot zone expansion rates, see Tab. 1, was calculated for three representative types of crude oil. The data in the third column are the conservative values recommended for emergency planning purposes.

These values are in agreement with the previously published sets of data but it should be pointed out that this model is not approved by practical experiments or more detail computational analysis. As this model gives only the approximate results, it is necessary to pay attention to the effects which occur during the preliminary phase of boilover. Mainly the sounds coming from the micro-explosions in the tank should serve as the last warning for the present emergency responders. Nevertheless, it should be pointed out that in several boilover experiments no sounds appeared before boilover period.

Calculated and recommended values of hot zone expansion rate for three crude oils. Table 1

Crude oil	Calculated values v_{HZ}	Recommended values v_{HZ},
Light crude oil Saharan Blend (Algiers)	10 – 17 mm/min	20 mm/min
Medium crude oil Flotta Blend (North Sea)	8 – 13 mm/min	15 mm/min
Heavy crude oil Basrah Heavy (Iraq)	6 – 8.5 mm/min	10 mm/min

9. Conclusion

The case study involving CFD simulation of tank fire was performed to support the emergency planning and tactical preparedness for major accidents in crude oil storage tank farm. Methodological approach employed in the framework of this study consists of:

- selection of relevant accidental scenario
- modelling and simulation of selected dangerous phenomena
- scenario-based emergency response training

Although the results of numerical simulation and modelling of accidental events are inherently coupled with different uncertainties there are many important qualitative features of dangerous effects which can be demonstrated by these tools. This theoretical knowledge needs to be understood as the supplement to practical training and fire fighting simulations. The periodically repeated sequence of all above-mentioned steps creates the main pillar of efficient emergency preparedness for industrial accidents.

Acknowledgement

This work was supported by the Ministry of Education, Youth and Sports of the Czech Republic (project OC 111 and OC 186 in the frame of the COST 729 Action) and Ministry of Environment of the Czech Republic (project no. SPII 1a10 45/70). The author V. N. also gratefully acknowledges toVSB-TUO. Faculty of Safety Engineering for financial support of the specific research granted by the Internal Grant System (project no. 023/2101/B10236011).

References

[1] PERSSON, H. LONNERMARK, A.: *Tank Fires - Review of fire incidents 1951-2003,* BRANDFORSK Project 513-021, SP Fire Technology, 2004.

[2] Ministerie van de Vlaamse Gemeenschap. Afdeling Algemeen Milieu- en Natuurbeleid.: *Handboek kanscijfers - Gecoördineerde versie 2.0.* Brussel, 2004.

[3] CHANG, J.; LIN, C.: *A study of storage tank accidents, Journal of Loss Prevention in the Process Industries, 2006,* 19, pp. 51–59.

[4] MANNAN, S.: *Lee's Loss Prevention in the Process Industries* (3rd Edition), Oxford: Elsevier Butterworth-Heinemann, 2005.

[5] AIChE. Center for Chemical Process Safety: *Guidelines for Chemical Process Quantitative Risk Analysis,* 2nd Edition, 2000, 740 p. ISBN 0-8169-0720-X.

[6] SALVI, O., DEBRAY, B.: *A global view on ARAMIS, a risk assessment methodology for industries in the framework of the SEVESO II directive, Journal of Hazardous Materials,* 2006, 130 (3), pp. 187–199.

[7] DELVOSALLE, C., FIEVEZ, C., PIPART, A., CASAL, J., PLANAS, E.; CHRISTOU, M.; MUSHTAQ, F.: *Identification of reference accident scenarios in SEVESO establishments,* Reliability Engineering and System Safety, 2005, 90, pp. 238–246.

[8] DELVOSALLE, C., FIEVEZ, C., PIPART, A., DEBRAY, B. ARAMIS project: *A comprehensive methodology for the identification of reference accident scenarios in process industries. Journal of Hazardous Materials,* 2006, 130 (3), pp. 200–219.

[9] TIESZEN, S., NICOLETTE, V., GRITZO, L., HOLENT, J., MURRAY,D., MOYAAND, J.: *Vortical Structures in Pool Fires: Observation, Speculation, and Simulation.* SANDIA REPORT SAND96-2607 UC-722. Albaqerque, 1996.

[10] BAUM, H.; Large eddy simulation of fires. *Fire Protection Engineering,* 2000, 6, 36 – 42.

[11] EVANS, D. D.; MULHOLLAND, G. W.; BAUM, H. R.; WALTON, W. D.; MCGRATTAN, K. B.: In Situ Burning of Oil Spills. *Journal of Research of the National Institute of Standards and Technology.* 2001, 106 (1), pp. 231–278.

[12] MATHER, T. A., HARRISON, R. G., TSANEV, V. I., PYLE, D. M., KARUMUDI, M. L., BENNETT, A. J., SAWYER, G. M., HIGHWOOD, E. J.: Observation of the plume generated by December 2005 oil depot explosion and prolonged fire at Buncefield (Hertfordshire, UK) and associated atmospheric changes. *Proceedings of the Royal Society A-Mathematical, Physical and Engineering Sciences.* 2007, 463 (2081), pp. 1153–1177.

[13] FAN, W., HUA, J., LIAO, G.: Experimental study on the premonitory phenomena of boilover in liquid pool fires supported on water. *Journal of Loss Prevention in the Process Industries,* 1995, 8 (4), pp. 221–227.

[14] BROECKMANN, B., SCHECKER, H.: Heat transfer mechanisms and boilover in burning oil-water systems. *Journal of Loss Prevention in the Process Industries,* 1995, 8 (3), 137–147.

[15] KOSEKI, H.: Boilover and crude oil fire. *Journal of Applied Fire Science,* 1993–94, 3 (3), pp. 243–272.

[16] Committee for the Prevention of Disasters. CPR 14E („Yellow Book") *Methods for the calculation of physical effects.* Third edition Second revised print, The Hague, 2005.

[17] BAUM, H., MCGRATTAN, K., REHM, R., HAMINS, A., FORNEY, G.: *Fire Dynamics Simulator - Technical Reference Guide,* National Institute of Standards and Technology, NISTIR 6467, Gaithersburg, 2000.

[18] MA, T. G., QUINTIERE, J. G.: Numerical simulation of axi-symmetric fire plumes: accuracy and limitations. *Fire Safety Journal,* 38, pp. 467–492.

[19] MCGRATTAN, K.; BAUM, H. HAMINS, A.: *Thermal Radiation from Large Pool Fires.* National Institute of Standards and Technology, NISTIR 6546, Gaithersburg, 2000.

[20] MULHOLLAND, G. W., LIGGET, W., KOSEKI, H.: The effect of pool diameter on the properties of smoke produced by crude oil fires. In *Proceeding of 26th Symposium on Combustion.* The Combustion Institute, 1996, pp. 1445–1452.

https://doi.org/10.26552/com.C.2008.1.16-19

Milan Majernik – Jana Chovancova – Imrich Fekete *

LIFE CYCLE ASSESSMENT AS A TOOL OF ENVIRONMENTAL SAFETY IN CAR RECYCLING

Numerous and wide-ranging initiatives are being pursued all over the world today to help pass on a sound natural environment to future generations. Automotive production is one of Slovakian leading industries. Because of urgent priority on protecting the environment, it is inevitable for manufacturers to be engaged in ongoing efforts to develop more environmentally friendly automobiles and a more viable infrastructure for them – one in which provisions for environmental protection, including recycling, constitute an essential part. The Life Cycle Assessment (LCA) is a tool for the systematic evaluation of the environmental aspects of a product or service system through all stages of its life cycle. The article is focused on some possibilities of improving the environmental safety of motor vehicles especially by application of the LCA in automobile production.

Keywords: End-of-Life Vehicles (ELV), Life Cycle Assessment, Recycling, Environmental Performance

1. The Reality of Recycling End-of-Life vehicles (ELV)

After years of debate between the car manufacturers and government officials, the End-of-Life Directive 2000/53/EC from the European commission was published in October 2000, combining requirements for the European Member States (e.g. recycling limits to be met as from 1st January 2006, collection of ELV´s), requirements for vehicle manufacturers (e.g. reduction of heavy metals as from 1st July 2003, availability of relevant information) as well as obliging the European Commission itself to amend existing European legislation (Whole Vehicle Type Approval: recyclability calculation). The End-of-Life Directive was implemented in Slovakian legislation by adoption of directive no. 125/2004. In order to meet all these requirements, close cooperation of all involved stakeholders is a must considering the "cradle to grave" philosophy. [1]

European member states had the obligation to implement the requirements of the ELV Directive into their national laws by 21st April 2002, however, some countries took up to Spring 2005. The EU ELV Directive also left the possibility to each of these member states how to arrange their national procedures for collection and treatment of ELV´s; moreover, the member states were allowed to apply stricter measures (e.g. The Netherlands – which requires a 95% recycling target for 2007 instead of 2015). Harmonization throughout Europe is also not supported by the fact that enforcement mechanisms vary between countries, states (e.g. Germany) and sometimes even regions (e.g. Belgium).

Meeting the recycling and recovery target as set by the EU ELV Directive is an issue for the European member state authorities; however they will have to rely on data gathered via various economic operators and according to the procedures from each member states. Here again an example that not the same data will be collected/required and thus could result in not the correct results when following the UE Commission Decision 2005/293/EC which sets out the rules on monitoring the reuse/recycling and reuse/recovery targets.

2. ELVs: A Valuable Source of Raw Materials

End-of–life vehicles present a valuable source or raw materials (table 1, figure 1) with a wealth of potential, which can be after appropriate selection and further processing used as input for further production. [4]

The changing automotive material mix over the past fifteen years and evolutionary technology trends for the future relative to automobile architecture for improved safety and environmental performance have and will continue to increase the recycling technical challenge.

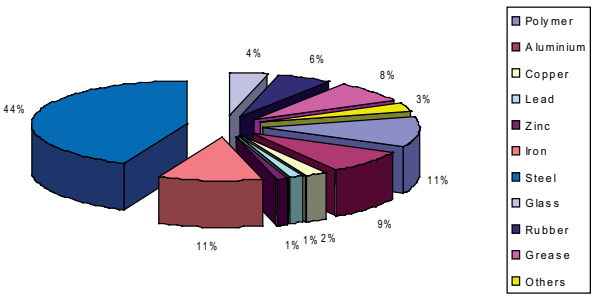


Fig. 1 Percentage of car materials

* **Milan Majernik, Jana Chovancova, Imrich Fekete**
Department of Environmental Studies and Process Management, Faculty of Mechanical Engineering, Technical University of Kosice,
E-mail: milan.majernik@tuke.sk

Car materials Tab. 1

Materials	Percentage	Weight [kg/car]
Polymer	11.4	116
Aluminium	8.9	91
Copper	2.2	22
Lead	1.5	15
Zinc	1	110
Iron	11	113
Steel	43. 3	442
Glass	3.7	38
Rubber	6	61
Grease	7.9	81
Others	3.1	32
Total	100 %	1021 kg

3. Improvement of Environmental Safety of Motor Vehicles

In order to provide society with products that help promote the protection of the environment and the conservation of resources, manufacturers have to adopt some basic guidelines in the conduct of their activities. These activities can be summarised in following four points:

1. Manufacturers will make comprehensive assessments of the environmental impact of the vehicles they produce, beginning at the vehicle development stage, in their effort to provide automobiles that are more environmentally friendly. In the manufacturing process, too, they will strive to develop cleaner production technologies.
2. Manufacturers will seek to establish a recycling-based infrastructure for automobiles to help promote environmental protection.
3. On a global scale and through international cooperation, manufacturers will strive for increased environmental protection through the application of appropriate technologies and their own expertise.
4. Manufacturers will, in addition, promote internal organizational systems that allow for appropriate and timely action in response to all environmental issues related to motor vehicles.

The objective is to use life cycle analysis to assess the environmental impacts of various mechanical separation technologies and alternative end-of-life recycling technologies. This information will then be used to create a flexible, computerized life-cycle inventory model, which is process-specific and yet can be modified to include additional recycling technologies and various material inputs.

4. Vehicle design and Development using LCA Methods

During the past two decades, a process called the life cycle assessment was developed that tried to make consistent and objective environmental assessments. Recently the LCA is a potentially powerful tool which can assist regulators to formulate environmental legislation, help manufacturers analyse their processes and improve their products, and perhaps enable consumers to make more informed choices. Like most tools, it must be correctly used, however.

Focusing on every stage of the life cycle of their products, manufacturers aim to reduce the environmental impact of motor vehicles. By application of the life cycle analysis (LCA) methods, manufacturers are making increased efforts to develop new, advanced technologies that will also satisfy important criteria in the areas of safety reliability, convenience and comfort.

The LCA methods are drawing more and more attention around the world as a means of quantitatively assessing the environmental impact of a product throughout its life cycle – from the development of raw materials and parts production through assembly, delivery, and use of the product in the market throughout the service stage, to the recycling of used components. Moreover, the International Organization for Standardization has established standards for the LCA (ISO 14 04X). [2]

However, numerous problems remain in the application of the LCA methods to the production, use and recycling of automobiles, owing to the fact that most vehicles are composed of at least twenty to thirty thousand parts. Stages of the Life cycle of motor vehicles is demonstrated in figure 2.

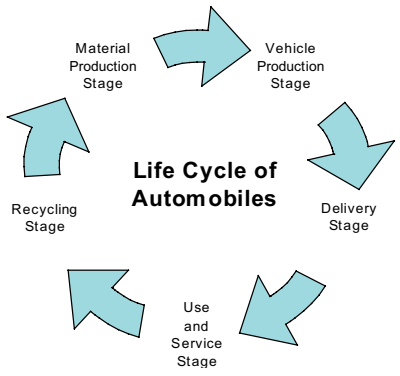


Fig. 2 Stages of Life Cycle of motor vehicles

In cases where contrary environmental goals exist the Life Cycle Assessment recommends the alternative that ensures the better overall environmental improvements. Therefore several studies were carried out on the dismantling and recycling process. These studies suggest certain life cycle aspects of different materials, constructions and drive systems.

All these studies showed that in comparison to production and use phase, recycling and disposal have only little impact on the overall environmental performance. [6] The main environmental aspects for recycling and recovery are the avoidance of landfill and the replacement of primary resources.

Both are common practice for all metals used. For plastics and other organic materials we've learned from external studies [7], that every option which leads to a replacement of primary (fossil) resources is nearly equal from an environmental point of view. The studies pointed out that mechanical recycling, energy recovery and feedstock recycling provides equal environmental performance. In short terms: there is no environmental waste hierarchy detectable for automotive wastes. On the other hand studies show that the economic burdens for dismantling and mechanical recycling, depending on the type of component, is at least twice up to 14 times higher than the expenses for post shredder recovery options. The main reasons for this are found in time consuming dismantling, high processing costs and additional logistics.

The conclusion from a life cycle perspective is not to focus on a very specific recycling methodology that might have slight advantages but to widen the scope of technologies applied for end-of-life vehicle recycling in general. Consequently, end-of-life vehicle recycling should not be focused on material recycling but must include feedstock recycling as well as other technologies able to replace primary resources. [5] These technologies can treat the entire waste stream or a major part of it and thus will provide a wider benefit to end-of-life vehicle recycling than a material recycling focussing on pure polymers only. In short term:

- the Life Cycle Assessment is a valuable tool for a holistic assessment of the environmental performance of components.
- A number of the Life Cycle Assessment case studies demonstrated that the environmental differences of the different options to treat non metal waste streams (e.g. material recycling, feedstock recycling, energy recovery) is little or negligible for end-of-life vehicles. Consequently no justification for an artificial waste hierarchy was found.
- In particular for complex and long life products like automobiles the results of the Life Cycle Assessment suggest a holistic approach taking into account all environmentally relevant life cycle stages rather than focussing on a specific life stages only.
- The use of the Life Cycle Assessment during product design in particular for conceptual decisions is a useful instrument to ensure that the environmental impact over the entire life cycle is taken into account. This will prevent different life cycle aspects being overrated wile others may be impaired.

5. Conclusions

The LCAs might be conducted by an automobile production to enable it to identify areas where improvements can be made, in environmental terms. Alternatively the LCA may be intended to provide environmental data for the public or for government. In recent years, a number of major companies have cited the LCAs in their marketing and advertising, to support claims that their products are 'environmentally friendly' or even 'environmentally superior' to those of their rivals. Many of these claims have been successfully challenged by environmental groups.

All products have some impact on the environment. Since some products use more resources, cause more pollution or generate more waste than others, the aim is to identify those, which are most harmful.

Even for those products whose environmental burdens are relatively low, the LCA should help to identify those stages in production processes and in use which cause or have the potential to cause pollution, and those which have a heavy material or energy demand.

Breaking down the manufacturing process into such a fine detail can also be an aid to identifying the use of scarce resources, showing where a more sustainable product could be substituted.

Since the disclosure of the EU directive on end-of-life vehicles a number of relevant developments can be recognised. In the past the recycling hierarchy was seen as the ecological guideline. [3] Based on this perception manual dismantling of plastic components was seen as a prerequisite. However, the latest results of Life Cycle Assessment case studies suggest a more holistic approach on environmental targets.

This should trigger a reconsideration of the basic demands and strategies for end-of-life vehicle recycling in the future as well as a discussion on the implementation of these requirements in product design and recycling processes in the member states.

The presented results are part of solution of the project KEGA no. 3/3155/05, solved at the Department of Environmental Studies and Process Management, Faculty of Mechanical Engineering at the Technical University of Košice.

References

[1] BADIDA, M., BOSAK, M., CHOVANCOVA, J.: *End-of-life vehicle recycling (in Slovak)*, KEGA 3/2155/04. Kosice: SjF-TU, p. 49, 2006.

[2] BADIDA, M., VARGOVA, J., HRICOVA, B.: *The possibilities of the improvement of environmental performance of industrial products,* MMA 2006: Zbornik radova: 9. mezdunarodna naucno-strucna konferencija fleksibilne technologije, Novi Sad, 2006. Novi Sad: Institut za proizvodno masinstvo, 2006, p. 139–140, ISBN 86-85211-96-4.

[3] MAJERNIK, M., BADIDA, M., BOSAK, M., CHOVANCOVA, J.: *Approaches to ELV recycling in Slovakia (in Slovak)*, Vplyv automobiloveho priemyslu na rozvoj regionov v SR, Kosice, TU, 2005, p. 7.
[4] MAJERNIK, M., BOSAK, M., CHOVANCOVA, J.: *Possibilities of component usage from ELV recycling (in Slovak),* Odpady 2006, zbornik prednasok z medzinarodnej konferencie, Spisska Nova Ves, Geologia PaB, 2006, p. 310–316, ISBN 80-968214-6-6.
[5] RUSKO, M., VARGOVA, J., CHOVANCOVA, J.: *Life cycle assessment and its potential in decision-making process,* Industrial Toxicology 2007, Bratislava, 2007, Proceedings, p. 369–373, ISBN 978-80-227-2654-2.
[6] SCHMIDT, HAHLQVIST, FINKBEINER at. al.: *Life-cycle Assessment of Lightweight and End-of-life Scenarios for Generic Compact Class Passenger Vehicles;* International Journal of Life Cycle Assessment; Vol. 9, 6/2004
[7] Verwertung von Kunststoffbauteilen aus Altautos – Analyse der Umwelteffekte nach dem LCA-Prinzip und ökologische Analyse; Abschlussbericht für Forschungsvereinigung Automobiltechnik e.V.; 2005

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.

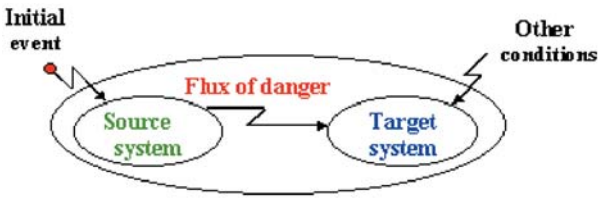


Fig. 1 Risk as a process involving the flux of danger [1, 2]

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.

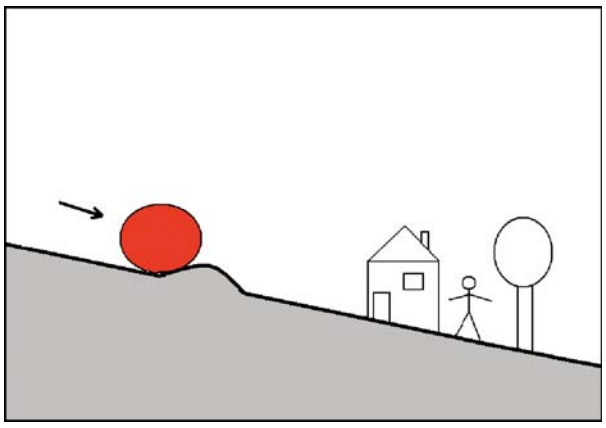


Fig. 2 Model of uncontrolled risk. Small initial event, e.g. the shock or pressure from left side, can move the shoulder to unstable position, trigger the flux of danger (potential energy of shoulder is changing to kinetic one and boulder moves) and the inertia of boulder destroys target systems (house,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

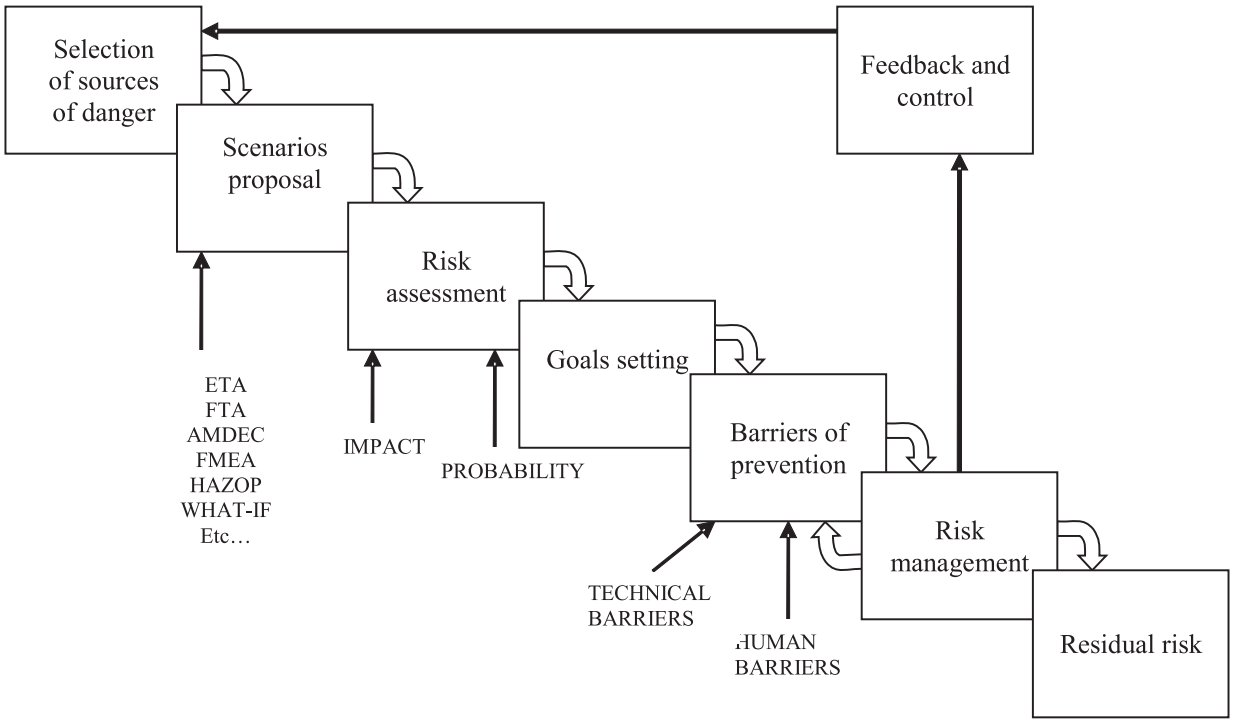


Fig. 3 Process of risk analysis and management

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:

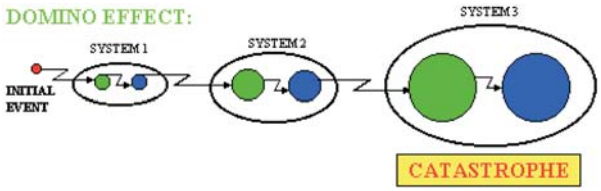


Fig. 4 Domino effect

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.

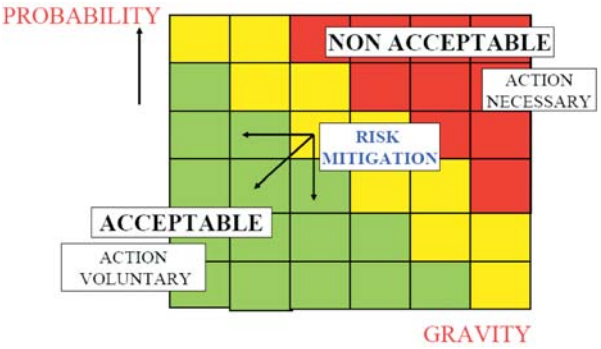


Fig. 5 Risk matrix

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,

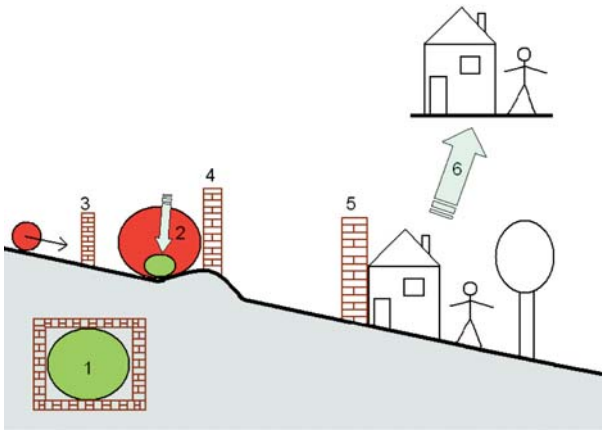


Fig. 6 Barriers of prevention: 1 – source of danger removal, 2 – source of danger minimization, 3 – prevention of initial event (triggering), 4 – prevention of flux of danger, 5 – protection of the target, 6 – protection of target by removal from the flux of danger

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.

https://doi.org/10.26552/com.C.2008.1.24-30

Karol Rastocny – Maria Franekova *

MODELLING IN DEVELOPMENT OF SAFETY-RELATED COMMUNICATION SYSTEMS

The aim of the paper is the use of modelling within development of safety-related communication systems presented in the areas where guaranty of a safety integrity level is required. The basic principles and standards used in the process of safety evaluation in closed transmission systems are summarised in the paper. Dangerous states of the system are mainly caused by systematic failures within a specification of the system, electromagnetic disturbance and random failures the HW effects. The main part of the paper describes the safety analysis process on the example of the end to end closed transmission system with the use of the fault tree and Markov's chain.

Key words: Integrity, safety, SIL, code, communication system.

1. Introduction

A variety of characteristics within manufacturing processes in different industry sectors evoke remaining requirements to flexible approach in the solution of safety of control systems including communication systems.

In many cases the communication system is a component part of the system which participates in control of safety-critical processes. Undetected corruption of data transmission (e.g. control commands) can cause considerable substantial damage within equipment, environment and demands on human health. This is the reason why the system has to be designed to guarantee the required safety integrity level (SIL).

COTS (Commercial Off-The-Shelf) communication technologies are not essentially available (without supplementary technical measures) for transmission of safety-related data, although their transmission systems involve detection and correction methods for transmission assurance or other protective mechanisms. Concerning the safety of the transmission, such systems are denoted as non-trusted. To decide which types of additional technical measures are necessary to apply depends on the risk analysis results (analysis of attacks and their effects) related to the controlled process and the acceptable risk.

Nowadays the number of vendors of the safety-related communication technologies who guarantee besides standard communication, communication among safety-related equipment according to [1] is increasing. In the present time the standard proposal [2] is prepared, which deals with a definition of functional safety for industry networks within digital communications used in the measuring area and the control systems in industry. Among the first manufacturers who have begun to use safety principles in development of their products there are the vendors of CAN technologies and products developed within the international organisation ODVA (Open Device Net's Vendor Association). The new network standard CIP Safety [3], published by ODVA, makes it possible to join standard and safety-related equipment across the same communication link. The vendors of Profibus and Profinet technology belong to the next important leaders in the area of industry Fieldbus. They develop a concept based on the integration standard and safety-related techniques that have been using the same communication tools for several years. This solution is signed as ProfiSafe and together with ProfiDrive profile it was approved and prepared for using in both types of industry networks Profibus and ProfiNet. In the present time the buses with communication profiles CIP Safety and ProfiSafe are recommended for using in safety-related systems with the safety integrity level 3 according to EN 61508 or the category 3 according to EN 954-1. The area of analysis and synthesis of safety-related communication systems assigned for control of the railway transport is presented in the norms [5] (for closed transmission systems) and [6] (for open transmission systems).

Modelling fulfils a very important task when specifying the requirements, in the process of structure design and the production of the communication system and also in the process of its verification and validation. In some cases modelling may help to optimize options, in other words, the setting of parameters within the existing communication system so that the requirements to safety integrity level and availability, which are defined by a customer or they are the result of the risk analysis, are accepted. In order to achieve these tasks it is generally required to combine suitable modelling methods and tools. Generally, in these cases an abstract model which graphically or mathematically describes features of transmission system is created.

* **Karol Rastocny, Maria Franekova**
Department of Control and Information Systems, Faculty of Electrical Engineering, University of Zilina, Slovakia,
E-mail: karol.rastocny@fel.uniza.sk

2. Modelling of safety characteristics of the communication system

Think of the communication system on the level of the end to end (Fig. 1). The communication system consists of the safety-related equipment SE 1, SE 2 and trusted transmission system, which realises safety-related functions within transmission in compliance with [5]. The base of the trusted transmission system includes a non-trusted transmission system (COTS system), which insures transmission messages by the transmission code (TC). To achieve the required safety level of transmission, transmission messages have to be ensured by the safety code (SC). It is necessary to realise the encoder and decoder of the safety code on the fail-safe principle. The component part of the transmission system is the communication channel, which is influenced by electromagnetic interference (EMI) only. The authors assume the closed transmission system and the independence of encoders/decoders of safety and transmission codes only.

It is an advantage when the development of safety–related communication system is based on modelling methods usage (for the define phases of the system development it is necessary). In fact the safety-related features of communication system modelling can be divided into the following parts:

- *Modelling of functional characteristics of the communication protocol.* In this case the model is based on the semi-formal and formal methods (they are usually supported by SW tools), which helps to produce explicit and logical descriptions of the functional possibilities of the system. In this area the object oriented modelling (OOM) can be used. One of the most suitable techniques for a production of such model is the unified modelling language (UML), which supports different modelling and visualisation elements [8].
- *Modelling of disturbing effects within the communication channel.* In this case the model describes the effects of EMI and the failures occurred in the communication channel. The result of solution is choosing the criteria for transmission selection and safety codes according to required SIL and calculation of residual error rate of decoders [7].
- *Modelling of failure effects in the transmission system.* In this case the model reflects the analysis of the failure subsequence on the communication system, which can be realised on the base of quantitative and qualitative methods.

Next part of this paper is devoted to the tasks of failure effects modelling.

3. Modelling of failure effects within the closed transmission system

Safety-related systems are typically resistent against hazardous faults. The failure effects on the system can be directly determined by monitoring the original system installation, by a simulation of the system operation using its model, by computing and theoretical reasoning. It is necessary to remark that strictly safety requirements for the safety-related system are not possible to achieve only by tests or results from practice (the frequency of occurrence of a dangerous state is very low and the mean time among failures multiply exceeds the value of the useful lifetime of one safety-related system). It is important to provide the proof of the safety request performance and the resultant risk acceptability.

The aim of the failure effects analysis on the safety is to form a model which allows to identify the transition process of the system from a safety state (it may not be necessarily a failure – a free state) to a dangerous state and permits to calculate probability of the dangerous state occurrence of the system as a failure effect to the operating system.

The transmission system normally does not work isolated but it is a component part of another superior system for which it pro-

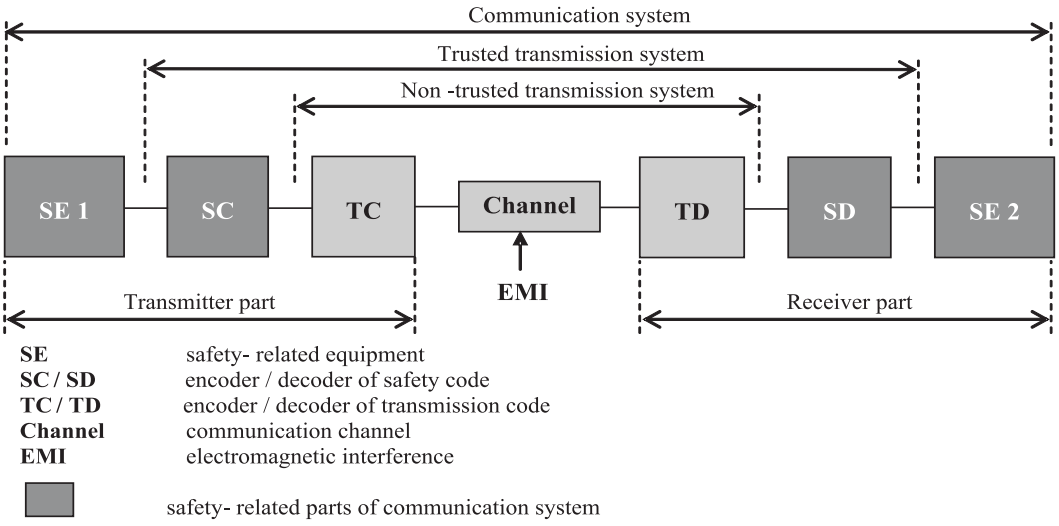


Fig. 1 The communication system on the level of the end to end

vides service. Therefore the starting moment of safety model generating is an exact definition of interface between the transmission system and the superior system with the aim to facilitate a total identity of treats with which it is necessary to consider in the process of analysis. Also it is necessary to define explicitly the event in the output of safety system which is considered as dangerous (undesirable) with regard to safety features of the transmission system. Generally, the undesirable event is considered to be such a violation of the transmission data which is not detected by the transmission system and further data are regarded as correct.

Except the safety procedures analysis (the source of a message identification, check of the type of a message, check of the current of data, the analysis of safety codes characteristics, the analysis of safety reaction mechanism, etc) it is necessary, according to the norm [5], to evaluate quantitatively the intensity of undetected failures of the transmission system.

The knowledge of failures and faults attributes of the transmission system forms the basic assumptions related to the measures realisation not only used to avoid failures but also for the fault detection and negation of the failure effects within their occurrence.

It is important to know where, when, and what types of failures occur in the system, what the reason of their occurrence and their effects to the system are. There are three ways in which a hazard may be created:

- random failures of the transmission system HW;
- failures caused by EMI;
- systematic failures of the transmission system.

The occurrence of a systematic failure is bonded to a concrete situation and a state of the transmission system. Mathematical modelling of this incidence is very problematic, because we have to know the type of a distribution and its parameters. Generally, we do not consider systematic faults in the process of a model realisation and we orientate to methods and techniques which are fixed to prevention of failures (e. g. formal specification, rigorous testing, etc). By a pursuant application of these methods we can assume that a systematic failure rates occurrence and consequently also their effects are negligible compared to random failure rates and failures involved in within a communication medium (it is caused mainly by influence effects in consequence of electromagnetic interference). Frequency of corrupted messages depends on a disturbance value. Because of the fact that the transmission system has to dispose with the required value of a safety level also in case of an unexpected reduction of the transmission line quality, in practical determination we generally issue from a very pessimistic assumption (each of the messages in the output of the transmission channel is corrupted).

The fault tree, which can cause undesirable event, is described in Fig. 2. Random failures can attack all parts of the transmission system. During the model realisation we accept the supposition that each of the messages in the input of the receiver is corrupted. This is the reason why we need not distinguish whether the corruption was caused by EMI or by a random failure of the receiver part of the transmission system or the communication channel. The random failures of a decoder of the transmission code create an important role in the failure effects analysis to safety of the transmission system. The failure of the transmission code's decoder can cause that all received messages are considered to be correct. It is also necessary to regard a situation in which a decoder of the transmission code checks the received message but consequently a message can be corrupted (during a transmission from a decoder of the transmission code to a decoder of the safety code). We do not consider a random failure of the decoder of the safety code

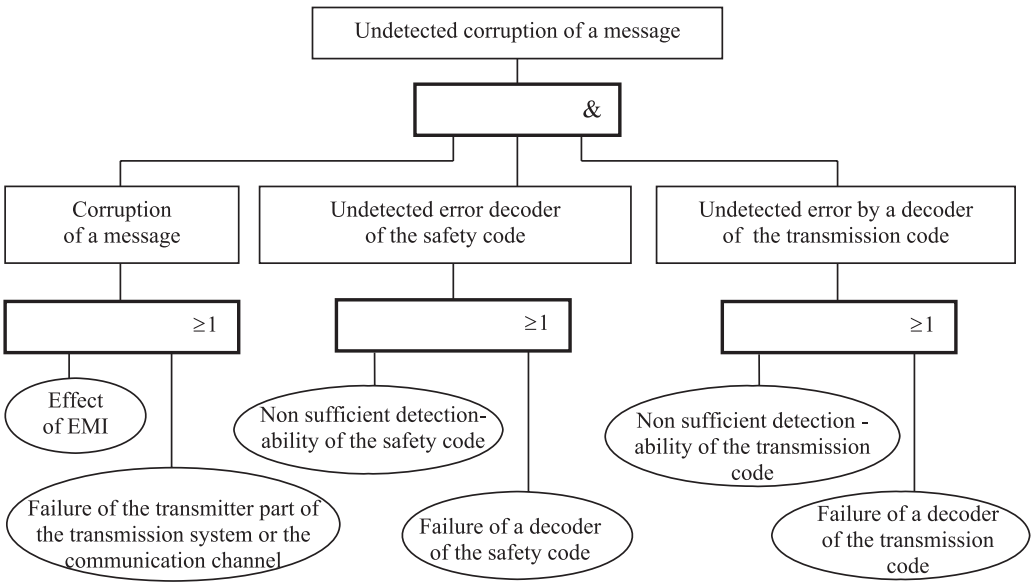


Fig. 2 Fault tree within the transmission system

because this type of a decoder is realised on the fail–safe principle (there are special technical measures applied for keeping required SIL). A safety code is not a component of the non-trusted transmission system.

The coincident effect of several factors to safety of the transmission system can be demonstrated by using Markov's chain. The system transition from a functional safety state 1 to dangerous state 6 is illustrated in Fig. 3.

The meaning of particular symbols in the diagram in Fig. 3 is illustrated in Tab. 1. The characteristics of the particular states in Fig. 5 are described in Tab. 2 and Tab. 3.

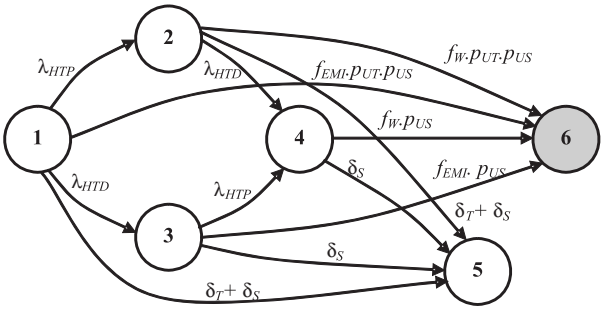


Fig. 3 Markov's chain of the transmission system

The meaning of symbols Table 1

Symbol	The meaning of a symbol
λ_{HTP}	HW failure rate of the transmitter part of the transmission system and the communication channel
λ_{HDT}	HW failure rate of a decoder of the transmission code
λ_{EMI}	The corruption rate of transmitted messages caused by EMI
p_{UT}	Probability of an undetected error of the transmission code
p_{US}	Probability of an undetected error of the safety code
f	Frequency of generating messages from a transmitter
f_{EMI}	Frequency of corrupted messages caused by EMI
f_{HTP}	Frequency of corrupted messages caused by HW failures of the transmitter part of the transmission system and the communication channel
f_W	Frequency of corrupted messages without the resolution of a corruption reason
T_T	Tolerance time of corrupted messages receiving in the non-trusted part of the transmission system
T_S	Tolerance time of corrupted messages receiving in the trusted part of the transmission system
δ_T	Intensity of the transition to permanent safety state caused by a failure of mechanisms operation for checking a number by a decoder of the transmission code
δ_S	Intensity of the transition to permanent safety state caused by a failure of the mechanisms operation for checking a number by a decoder of the safety code

Description of the diagram states Table 2

State	A description of the states
1	The transmission system is functional; transmission messages are corrupted by EMI
2	The transmission system state, when the transmitter part of the transmission system or some part of the communication channel are in failure
3	The transmission system state, when the decoder of transmission code is in failure
4	The transmission system state, when the transmitter part of the transmission system or some part of the communication channel and the decoder of the transmission code are in failure
5	Permanent interruption of transmission caused by a failure of mechanisms operation for checking of number of detected corrupted messages
6	The hazard state corrupted message was undetected

Transitions in the diagram

Table 3

Transition	A description of the transition	The meaning of transitions intensity
1 → 2	The transition is realised in consequence of the HW failure of the transmitter part of the transmission system or some part of the communication channel	λ_{HTP}
1 → 3	The transition is realised in consequence of the HW failure of a decoder of the transmission code	λ_{HDT}
1 → 5	The transition is realised in consequence of mechanisms operation for checking the number of detected corrupted messages by a decoder of the transmission code or the safety code	$\delta_T + \delta_S$
1 → 6	The transition is realised in consequence of the insufficient detection characteristic of the transmission and safety codes	$f_{EMI} \cdot p_{UT} \cdot p_{US}$
2 → 4	The transition is realised in consequence of the HW failure of a decoder of the transmission code	λ_{HDT}
2 → 5	The transition is realised in consequence of the mechanisms operation for checking the number of detected corrupted messages by decoder of transmission code or safety code	$\delta_T + \delta_S$
2 → 6	The transition is realised in consequence of the insufficient detection characteristic of the transmission and safe codes	$f_W \cdot p_{UT} \cdot p_{US}$
3 → 4	The transition is realised in consequence of the HW failure of the transmitter part of the transmission system or some part of the communication channel	λ_{HTS}
3 → 5	The transition is realised in consequence of the mechanisms operation for checking the number of detected corrupted messages by a decoder of the safety code	δ_S
3 → 6	The transition is realised in consequence of the insufficient detection characteristic of the safety code	$f_{EMI} \cdot p_{US}$
4 → 5	The transition is realised in consequence of the mechanisms operation for checking the number of detected corrupted messages by a decoder of the safety code	δ_S
4 → 6	The transition is realised in consequence of the insufficient detection characteristic of the safety code	$f_W \cdot p_{US}$

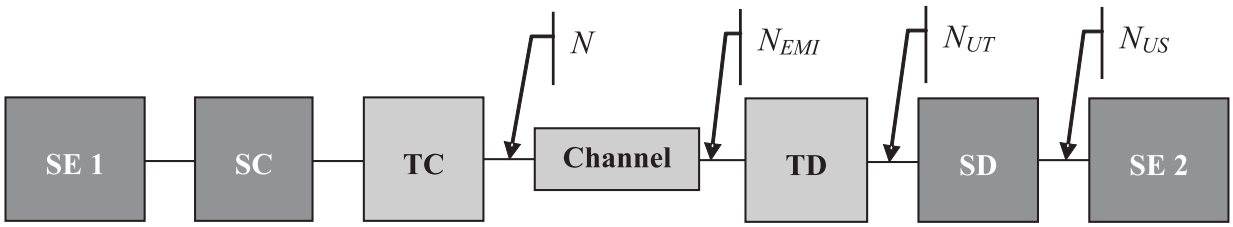


Fig. 4 Localities of number's determination of corrupted messages in the communication system

During the model designing it is necessary to know the number of corrupted messages (during a define time unit) in the parts of the communication system, which is important for the safety analysis (Fig. 4).

The meaning of the number of messages in Fig. 4 and their mathematical expression providing that the communication system is in a failure-free state:

- N is number of messages generated from a transmitter during time T, i. e. $N = f.T$.
- N_{EMI} is a number of corrupted messages in input TD during time T, i. e. $N_{EMI} = f_{EMI}.T$.
- N_{UT} is a number of corrupted messages in output of TD during time T, i. e. $N_{UT} = f_{EMI}.p_{UT}.T$.
- N_{US} is a number of corrupted messages in output of SD during time T, i. e. $N_{US} = f_{EMI}.p_{UT}.p_{US}.T$.

Similarly we can determine the number of corrupted messages which are detected by a decoder of the transmission code (N_{DT}) or by a decoder of the safety code (N_{DS}) during time T, i. e.:

$$N_{DT} = f_{EMI}.(1 - p_{UT}).T,$$

$$N_{DS} = f_{EMI}.p_{UT}.(1 - p_{US}).T. \quad (1)$$

The diagram in Fig. 3 can be simplified if we suppose that the failure of a decoder of the transmission code occurs so then there is no reason to consider some effects from other parts of the non-

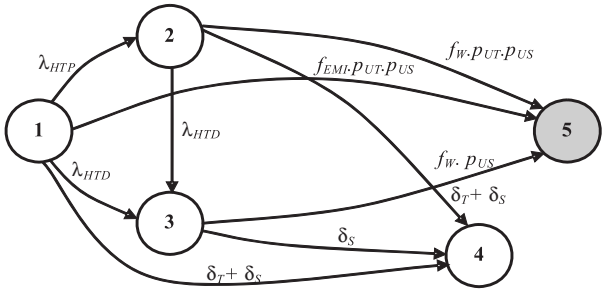


Fig. 5 Simplified Markov's chain

trusted transmission system on frequency of a corrupted data (Fig. 5).

Markov's chain can be mathematically described with the set of differential equations and by a vector of initial probabilities. The set of differential equations:

$$\frac{dP(t)}{dt} = P(t).A, \tag{2}$$

where $P(t) = \{p_1(t), p_2(t), \ldots p_n(t)\}$ is a vector of absolute probabilities and A is a matrix of intensity of transitions. The vector of initial probabilities is $P(t = 0) = \{1, 0, \ldots, 0\}$.

The matrix A for the diagram in Fig. 5 is

$$A = \begin{pmatrix} -(\lambda_{HPT} + \lambda_{HTD} + f_{EMI}.p_{UT}.p_{US}) & \lambda_{HPT} & \lambda_{HTD} & 0 & f_{EMI}.p_{UT}.p_{US} \\ 0 & -(\lambda_{HTD} + \delta_T + \delta_S + f_W.p_{UT}.p_{US}) & \lambda_{HTD} & \delta_T + \delta_S & f_W.p_{UT}.p_{US} \\ 0 & 0 & -(\delta_S + f_W.p_{US}) & \delta_S & f_W.p_{US} \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \tag{3}$$

The relation of probability of particular states occurrence in the diagram according to the parameters of a model can be exactly formulated by an analytical solution. The solution for more complex diagrams is very difficult; hence in praxis we are satisfied only with a numerical resolution. The calculation precision depends on a suitable selection of a calculation method and on a numerical precision of computing techniques. In the present time there are several SW products which support a solution with the use Markov's diagram (e. g. BQR reliability engineering [9], RELEX software [10], ITEM software [11], etc).

Such a model is based on a supposition that if the detection of a corrupted message occurs then the system will go to the previously defined safety state. Otherwise this solution contributes to the increase of the integrity level of the system but, on the other hand, significantly decreases availability of the system, which negatively affects the secondary safety. Generally, it is necessary to choose a suitable compromise between availability and on the level of safety integrity requirements. The system availability increased by using the channel correction techniques is problematic due to a masquerade of HW failures of the transmission system. For availability increase it is necessary to create such a mechanism which according to strictly defined criteria evaluates the number of received and corrupted messages and permits the communication system to remain in operation after receiving this message too. It is obvious that in this case a corrupted message must be discarded for next processing. The solution of this problem can be based on using a timer counter, which is activated in time of the corrupted message receiving. If during the specified time interval the defined number of corrupted messages is received, then the system will go to a safety state. An alternative method uses so-called ratio criteria, which is based on the evaluation of the positive and negative ratio results of the correctness control of a received message. In fact the base of this method uses a time counter, which counts in a defined range <I; M> and by start it sets an initial value I (e. g. 0). The actual value of the time counter changes according to the result of the correctness control of a received message. In case of a positive result the state of counter is decremented by P (as far of the initial value) and in case of a negative result the state of the counter is incremented by value N. The condition N>P must be fulfilled. When the counter achieves or overruns the boundary value M, the safety reaction and transition of the system to the safety state occurs.

In case this mechanism is applied it is necessary to respect this fact within the model creation and consecutive calculations.

4. Conclusion

The process of a dangerous failure rate determination, which is described in the informative part in the norm [5], is simplified and it can not be mechanically applicable within the analysis of the safety communication system. Every concrete solution of the communication system has its own specific characteristic which is to be respected within the analysis. In case of using the open transmission system the possibility of intentional corruptions or destruction of a message must be regarded.

This work has been supported by the scientific grant agency VEGA, grant No. VEGA 1/004/08 "Mathematic-graphical modelling of safety attributes of safety-critical control system.

References

[1] EN 61508: *Functional safety of electrical/electronic/programmable electronic safety-related systems,* 1998

[2] IEC 61784-3: *Digital data communications for measurement and control, Part 3: Profiles for functional safety communications in industrial networks,* CDV 2007

[3] NAIR, S., VASKO, D.: DeviceNet Safety: *Safety networking for the future*, 9th CAN conference, Munich, 2003

[4] ProfiSafe: *Test Specification for Safety-Related Profibus DP Slaves,* draft version 0.82, PNO Order No 2.242, 2003

[5] EN 50 159-1: Railway applications: Communication, signalling, and processing systems, Part 1: *Safety-related communication in closed transmission systems*, 2001

[6] EN 50159-2: Railway applications: Communication, signalling and processing systems, Part 2: *Safety-related communication in open transmission systems*, 2001

[7] FRANEKOVA, M.: *Mathematical Apparatus For Error Probability Determination of Block Code Decoders*, Scientific Journal Communications, 4/2001, pp. 59-63, ISSN 1335-4205

[8] Unified Modeling Language Version 2.1.1. http://www.uml.org

[9] BQR Reliability Engineering. http://www.bqr.com

[10] Relex Software Continental Europe. http://www.relexsoftware.de

[11] Item Software. http://www.itemuk.com.

https://doi.org/10.26552/com.C.2008.1.31-34

Vladimir Klaban *

SAFETY ENGINEERING, SECURITOLOGY AND INSOLVENCY

The basis of safety engineering is acceptance, introduction and maintenance of measures aimed at safety in various, mainly technical areas of human activities. Safety is a state during which there is an admissible probability of occurrence of damage to protected interests. Insolvency is a state of incapacity to pay. In the contribution, the specified definitions are developed, their mutual relations are shown and their connection with sustainable development theory and practice is emphasised.

1. Introduction

The aim of safety engineering as well as of securitology (i.e. a safety science) is elimination of threats. Insolvency is currently becoming a subject of contemplations and negotiations of not only politicians, economists and sociologists, insurance companies, entrepreneurs but also of ordinary people. It is so due to the fact that more and more entrepreneurial and non-entrepreneurial entities become insolvent. Municipalities and in a wider perspective even the whole states are not an exception.

2. Insolvency like a Threat

Insolvency, as a state of incapability to pay, is a threat not only for natural persons, legal entities entrepreneurs or non-entrepreneurs, but it also becomes a threat for entities of the state and public administration and whole countries, mainly the developing ones. Consequences of this insolvency, poverty and its overlooking, thus become a threat also for developed, rich societies.

Insolvency is a significant threat for implementation of sustainable development but not the only one. It is clear that development of society brings forward new sources of risks and increase of the intensity of risks already existing. The nature of these risks is based on undesirable effects of forces and phenomena with adverse consequences. In other words, it is damage to protected interests. [1]

The origin of the undesirable strengths and phenomena can be found either in nature or in human activities. Regardless of origin of these strengths and phenomena, their effects and consequences definitely deserve to be the subject of research. Also the problems of prevention of occurrence, mitigation of progress and elimination of impacts of these forces and phenomena deserve the same attention.

A huge increase of information and level of knowledge of human society significantly expanded possibilities of mankind, mainly in the technical area. The nature of human society has not changed too much. In last centuries we have seen an opinion that this development will get out of control of human power and due to its nature will lead to the end of mankind, or civilisation, if you want. One of the basic goals of the current developed society is the survival in a form of sustainable development.

Strictly speaking it is the protection of human society – or better said say (even though it is significantly narrowed) – of civilisation in our understanding, i.e. protection of the state security. We want to live in safe environment and thus we, as the mankind, deal with security aspects. Partial security issues in the whole number of areas are elaborated intensively – in other words, security research is being performed in the following areas, e.g.:

- Security of work;
- Security of transport;
- Personal security;
- Object security;
- Security of information;
- Safe filing of documents;
- Safe production technologies;
- Safe defence;
- Safe region;
- State security etc.

Most of the specified areas of safety research develops and examine adoption , implementation and maintenance of measures aimed at security in various, mainly technical areas of human activities. Security researches are theories for safety engineering the aim of which is practical implementation of measures leading to the ensuring of safety.

* **Vladimir Klaban**
Rasin University Brno, Czech Republic, E-mail: akademie@akademieops.cz

2. State security

An extraordinary position among the areas of security research belongs to the state security. The issues of the state security is not considered to be a kind of safety engineering but many areas of safety engineering deal with practical performance of measures connected with the issues of the state security. We have to be aware of the fact that it is the well-functioning state that is obliged to create conditions for harmony between the needs of the people and the society, economic prosperity, healthy environment, social justice and health and life protection of people with regard to not damaging future generations.

It is possible to assume that perspectives of further development of the Czech Republic in the following period will be strongly determined by external and internal factors that will be very difficult to influence actively. Globally, tendencies that will influence the overall development in the EU and thus also Central European countries will be dominating.

From the assessment of the threats it is clear that in the middle-term perspective no massive military attack against the EU is probable. Deterioration of security situation on a global level has impacts also in the Euro-Atlantic area. Despite the fact that the security situation on the global level deteriorated, it has impacts also on security situation in the Euro-Atlantic area. This is reflected in threats that are difficult to foresee. Their occurrence and fast spreading is facilitated by globalisation. More and more often their originators are non-state actors (traditional and new terrorist organisations, radical religious, sectarian and extremist movements and groups) that purposefully threaten our lives.

The practice shows how difficult it is to foresee the threats. The existence of various forces and elements trying to gain over the control, damage or eliminate various electronic, communication and information networks has been proved. There is a high risk of attacks of this kind. Extensive leaks of strategically important information or interference in the information systems of state institutions or businesses and companies ensuring the basic functions of the society and the state can threaten not only the strategic but also the vital interests of the EU states. [2]

The occurrence of threats is contributed by deepening imbalance between the North and the South. Economic and social slowdown of the South leads to dissatisfaction of its inhabitants. It creates breeding ground for radicalisation, extremism and terrorism. Dissatisfaction with living conditions leads to migration, often illegal one, to the countries in the North.

One of the thorniest problems the underdeveloped countries face is their astronomical indebtedness. Debts and the lack of capital arising from them restrict the access of the inhabitants to education and basic life needs and thus they also undermine the economic development.

Excessive indebtedness triggers and intensifies the economic, social and political problems of the debtor states. These problems can be seen in the pressure on export, elimination of social benefits, using of money from the development aid for settlement of debts, increasing unemployment, discouraging of investors, outflow of capital, destruction of the environment, growth of the poor class and increasing number of unsatisfied population of our planet.

The problem of insolvency and its consequences – growing poverty, lack of education, unavailable health care and suppression of the right for dignified life – does not only apply to poor countries, the consequences often have strong impacts also on more developed states of the North and they become threats for then. These consequences include:

- Increase of international polarisation and extremism – strengthening of the role of radical ideologies and violent tendencies, including international terrorism.
- Destroying of the environment- pressure on the growth of foreign exchange economy that would enable settlement of debts leads to massive destroying of the environment in many countries, which has global impacts.
- Increase of international crime – extending of sown areas for growing of drugs and increasing demand for them. Development of the international drug trade brings increase of grey and black economy and increase of international crime.
- Collapse of markets – collapse of the whole national economies in developing countries leads to decrease of markets also for companies from developed countries.
- Military conflicts – humanitarian crises drain the funds from the development cooperation and there is a growing need for expensive international military interventions.
- Influx of refugees – globally there is an increase in number of refugees trying to escape from the hopeless situation in their homes. It brings needs of further humanitarian interventions in the countries where the refugees move, there is growing xenophobia and violence.

The specified facts can be marked as threats that will not avoid even Central European states. We can assume that perspectives of further development in the following period will be strongly determined by the external and internal factors that will be very difficult to influence. In the period until the year 2015 (with an outlook until 2030) there will be dominating global tendencies which will also influence the overall development in the EU. They include mainly the following:

- Aging of the population and strengthening of migration from the countries of former Soviet Union, Near East and Middle East, Northern Africa, Asia with preconditions of creation of closed communities and subcultures outside the official control of the state.
- Outflow of investment means, mainly in favour of some countries in Asia with subsequent impacts on employment and social cohesiveness in the EU states.
- General and global deterioration of conditions of the access mainly to energy but also other raw materials. Continuous and unforeseeable growth of their prices and deterioration of their availability.
- Disturbing of traditional social connections and relations in the society with subsequent pressure on the change of social and political system.

- Deterioration of military and political situation in the world with the emphasis on the region of the Near East and Middle East.
- Increase of number of critical situations induced by natural disasters and intentional or unintentional activities of people, with subsequent important impacts on the general situation within the EU.
- Deepening of vulnerability of the developed civilisation and various forms of into dependency [3].

3. Safety Science as the Prevention

Despite the above mentioned development tendencies seem to be irreversible at the moment, it is possible to take preventive measures and actions that will enable minimisation of their subsequent impacts. One of the important elements within the scope of timely and mainly efficient solution of these impacts is also purposeful solution of the issues of the population protection system. Protection of lives, health and material values, together with ensuring sovereignty, territory integrity and protection of democratic foundations, is one of the basic obligations and thus also functions of the state. This problem must become a subject matter of research of safety science.

It is also worth noticing that safety is characterised (determined) by and connected with the space, time and human society. We cannot speak about security without relation to people and human society.

Safety is thus always seen in connection with people and human society. The aim is to reach such a state in the particular area and time so that human society is not threatened as regards its health, life and property. From this point of view it is possible to deduce that safety is kind of a subjective philosophical category which only exists in connection with people.

Without analysing or criticising other interpretations, in the following text we will follow the definitions defined in the Long-term intention of research directions in the CR (LIRT) and use also in other works, [4] i.e.: "*Security is a state during which there is admissible probability of occurrence of damage to protected interests*". We consider this definition to be sufficiently general and fitting.

As we have already specified above, security is always seen in relation to people (humankind) and thus we can also define the protected interests.

Protected interests are human lives, health and property. When analysing this definition we will come to a conclusion that it is necessary to protect everything connected with health, lives and property of people. Naturally, it will be mainly the environment and infrastructure of human society.

With regard to a wide range and complexity of possible threats and dangers, growth of human population, technical development and increasing extrapolation of nature it is absolutely necessary for security to become a subject matter of scientific research.

Other attributes supporting our conviction that nowadays the "security" issues deserve establishment of security science and development of special security research are the following:

- Stage of human society development;
- Wide extent of knowledge in the areas dealing with security;
- Lack of arrangement and fragmentation of approaches to the individual items (particularities);
- Inexistence of general approaches and solutions;
- Necessity to improve the current system ensuring security.

Being aware of the fact that the term of security science will not be to the liking of many people, we will now attempt to show justifiability of the statement that research in the area of security can be considered to be a security research and that we can rightfully talk about security science.

Most of books dealing with the issues of science and research state that the basic preconditions for existence of a science (a field of science) are

- Subject of examination
- Examination methods.

In our case, the subject matter of examinations of security science is "security" in its general conception, i.e. a state when there is an admissible probability of occurrence of damage to protected interests, and suitable examination methods are for example the following:

- Extrapolation of tendencies;
- Scenario creation method;
- Economic analysis;
- Decision-making matrix;
- Operational research;
- Decision-making theory;
- Diagram of goals;
- Network methods;
- Historic analogy;
- Comparative method;
- Creation of hypotheses;
- Exercises, training, experiment.

We have to point out that examination methods develop and extend in time and with development of knowledge. For the area of security it will be interesting to use the "comparative method" based on the hypothesis that rudiments of what is developing and growing already existed in the past and nothing was created newly – mainly in relation to terrorist threats.

In the classification of sciences by T. G. Masaryk, security science can be included among practical sciences [5]. In this classification (based on Aristotle's classification), T. G. M. differentiates the following:

- Theoretical sciences looking for the truth regardless its utilisation and having their organising principle in its subject matter (e.g. mathematics – quantity) and
- Practical sciences having their organising principle in the purpose outside the field of study and taking knowledge where and how it is offered to them by the theoretical sciences.

Practical sciences are built on theoretical sciences.

In the late 19th century and in the course of the 20th century a number of fields of science were established, which resulted from the intensive development of human society. As an example we can mention psychology, sociology, economy and political science.

Generalisation of knowledge in the area of security is possible and necessary. Thus also the requirement that a science must be sufficiently general will be fulfilled. However, there will be and must be mutual connections between other fields of science.

The current situation in the area of security is characterised by simplification of problems, the desire for creation of the lowest possible number of basic principles and forced unification and simplification of knowledge.

It is obvious that for the benefits of security science it will be necessary to conduct research and development work in a systematic way. In its document LIRT, the Research and Development Council of the CR specified seven thematic directions of the most important matter of the research: *Sustainable development*, Molecular biology, Energy sources, Material research, Competitive engineering, Information security and *Information research*. The term "research" is used to denominate systematic creative work extending knowledge, including knowledge of people, culture or society, by means of methods enabling confirmation, supplementing or disproval of gained knowledge performed as basic research, which consists of experimental or theoretical work performed with the aim to gain knowledge on the basis or nature of the examined phenomena, explanation of their causes and possible impacts of the use of the gained knowledge. This creative work is marked as the basic research, which includes experimental or theoretical work performed with the aim to gain new knowledge aimed at the future use in practice.

4. Conclusion

Security science dealing with research in favour of security is currently finding its place ?at both the specialist and lay public? and material, financial and institutional support. It is a correct way enabling implementation of sustainable development. We believe that the research programme "Security research" and solution of the partial programmes "Threats for critical infrastructure and Optimisation of relations of sustainable development and population protection", in the solution of which also the author of this contribution participates with the support from the Ministry of Interior, will contribute to the solution of the matter.

References

[1] KLABAN, V.: *Insolvency - today phenomenon (in Czech)*, Reorganizace podniku a priprava noveho upadkoveho zakona, Brno, Rasin College, 2006, ISBN 978-80-87001-04-4.

[2] KLABAN, V.: *Threats for critical infrastructure (in Czech)*, Proc. from 9th specialist conference with international participation „Presence and future of crisis proceedings 2006", Prague 2006, ISBN 80-239-7296-2.

[3] KLABAN, V.: Insolvency as a threat (in Czech), Proc. from conference Crisis management, UNI Pardubice, Lazne Bohdanec, 2007, ISBN 978-80-7194-951-0.

[4] KLABAN, V.: *Safety science, security research and defence research (in Czech)*, Specialist conference with international participation "Interoperability in population defence management", University of Defence, Brno 2006, ISBN: 80-239-3503-10.

[5] MASARYK, T. G.: *Selection from work (in Czech)*, published in 2001, translation Versuch einer concreten Logik, Klassification und Organisation der Wissenschaften (Vienna 1897).

https://doi.org/10.26552/com.C.2008.1.35-39

Tomas Lovecek *

PRESENT AND FUTURE WAYS OF PHYSICAL PROPERTY PROTECTION

Nowadays in the territory of Slovak republic, the property protection and security systems design lies in realization of requirements following from security requirements specifying details of tangible property protection (Law, Risk Analyze, Internal regulations of the company). In this article, three basic approaches to secure physical protection of property will be introduced. There is directive-oriented, variant-oriented and variable way of physical protection. For the most effective way of protection we can consider the variable way of protection, which allows due to its flexibility designing of the system in such a way, that it best suits requirements, conditions and possibilities of the subject.

1. Introduction

Nowadays in the territory of the Slovak republic, the property protection and security systems design lies in realization of requirements following from security requirements specifying details of tangible property protection. The security requirements come from the following three basic sources:

- legal aspects of property protection (e.g., law, ordinances, regulations, guides, business-law relations),
- independent evaluation of threats and their risks (security audit),
- set of principles, goals and requirements for property protection, which were developed by a given organization to support its operation.

Generally, binding legal directives define property protection only in certain areas (e.g., protection of classified information, critical/defending infrastructure, financial institutions). These are areas where the state has dominant interest in protection of its or private property against attack, misuse, damage or theft by other person or organized group. In case the state with the help of legal directives does not define a specific methodology of property protection (e.g., security standard of physical security and object security), there is a possibility to proceed according to requirements (e.g., insurance conditions, certification requirements according to ISO 27001) or proposals (e.g., designed or performed project of security system) of third subjects (e.g., insurance company, technical service for property protection). In case the state does not define a way of property protection against intentional threats, we can talk about so-called private security [6].

2. Property protection from confidential information point of view

The fact that the biggest attention in case of state property protection is dedicated to the classified information protection (under board of NBÚ SR), confirms that these problems are related to approximately 16% of organizations in the SR. Classified information (US) can be information (e.g., content of a document/drawing/map/photography, content of electrical/electromagnetic or other physical transport medium) or object (e.g., product, equipment, realty) [7]. From its beginning the classified information protection was subject to several changes from object and physical security point of view. The respective executing regulation specifies details about specifications of buildings and space where the classified information is located and details about the way of their protection. The main difference between the pilot regulation and later regulations (including the currently valid regulation) lies in the way how the creators of the regulation approached the classified information protection [8]. They used a *directive-oriented approach*, which caused problems for some subjects, related to holding the letter of the law, either from realization or financial position. For particular protection interests, specific precautions were defined. These were not allowed to be omitted or replaced by different ones. This approach was changed in the next execution directives [8] and for the evaluation of the US protection level the spot system has begun to be used, which allowed choice of various security variants. The spot system allows choosing such a combination of security precautions with respect to the specific conditions, which suits best the given circumstances. For objects and protected space the smallest spot values are defined, which are necessary to reach. The mathematical method is used which assigns spot evaluations to respective security precautions. Their sum is evaluated in a respective way. Precautions defined as optional do not have to be realized, but the prescribed total number of points must be reached. The philosophy of such *a variant-oriented way* of physical protection is built on the fact that the subject has to reach a necessary number of points with respect to local conditions. An example of possible variant of protection security corresponding to the US classification degree “confidential” or “reserved” is illustrated in Fig. 1. The spot system of security standard allows choosing, with respect to specific conditions, various combinations of protection

* **Tomas Lovecek**
Department of Security Management, Faculty of Special Engineering, University of Zilina, Slovakia, E-mail: Tomas.Lovecek@fsi.uniza.sk

precautions. It only depends on the given subject which combination will be chosen so that the summary point evaluation is equal or a higher than the minimum required value for respective amount of risk, which is a result of risks analysis.

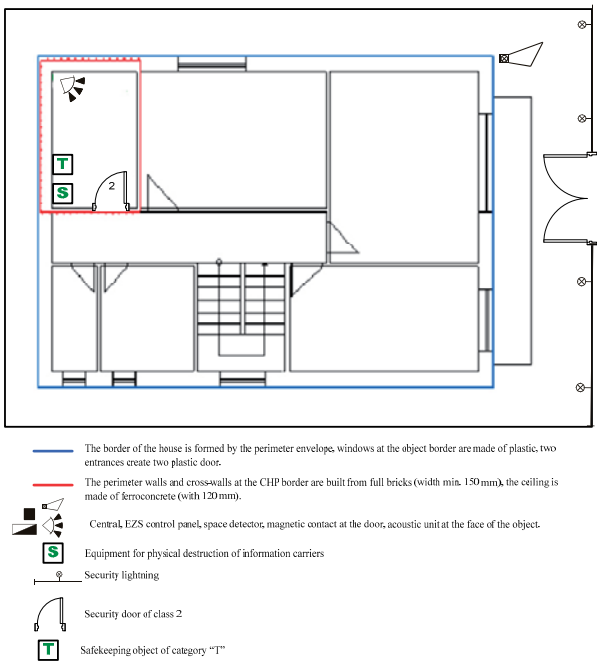


Fig. 1 Example of protected space of category classified

3. Property protection from financial institutions point of view

A combined method of directive and variant way of property protection security is used for example by financial institutions. The national bank of Slovakia (NBS) issued a precaution n. 12/2005 dealing with the analysis of risks related to the security of bank operation space where both the contact with clients and manipulation with financial cash (business office) is realized. This analysis of risks in connection with business office includes the technical-building fabrication of the object, passive and active security components of inner/outer environment, physical protection and organizational-regime precaution for employees, clients and other persons. A bank subject is, on the basis of the bank law, obligatory [9] to realize respective precautions and to discuss these precautions with a respective unit of police force. On the basis of this information, the office of judicial and criminal police of police force presidium has elaborated methodical directives for security of a unified procedure of the police force units at a risks analysis discussion which are related to the security of operational bank space. The directive part of a property protection way follows directly from the law [9] which obliges banks to secure the business office with a security and alarm system and to connect them to an alarm registration central. Furthermore, the law orders to secure the place with a camera monitoring security system in 24 hours recording time in a quality which allows distinguishing a specific person. The variant way of the bank and clients property protection security lies in the fact that the law orders to accept other security precautions which are results of risks analysis needs. A designated police officer at the risks analysis discussion uses the material presented by a bank and the methodological directive in which inner and outer environment of the bank subject is evaluated. In case the total level of risk is lower than the before set value presented in the methodological directive, the bank must accept only the directive protection precautions presented in the law. However, in case the total level of risk is higher, the bank must accept other protection precautions, which directly lower the risk level (e.g., optimization of financial cash according to operational needs of the business office, using safety caskets, transport containers and other technical means designated for financial cash protection, existence of means for financial cash devaluation, etc.).

4. Property protection from insurance companies point of view

A significant factor which influences security requirements for protection of both private and state property are conditions of insurance companies defining the security requirements for individual insurance events. Each insurance company has processed its own requirements for individual types of protection precautions with respect to the value of protected interest. Certain necessary conditions are set which the object must satisfy so that the insurance company can agree to the insurance contract. Unlike Czech insurance companies, Slovak insurance companies present only a type of necessary precautions (e.g., security door, IDS connected to the alarms registration central), but they do not present a level of protection for individual security precautions. The Czech association of insurance companies issued for insurance companies needs a so called security pyramid which declares both equality of protection elements with respective ČSN norms and respective degree of protection. On one hand, for each process of property protection and also design of security system is the owner (caretaker) of the property who has certain security requirements following either from generally binding legal directives or their internal needs. On the other hand, there is a designer/person realizing the project who comes with certain conceptual proposal how to satisfy requirements of the property owner. In practice, the fulfillment of criteria of binding legal directives and contracts (e.g., criteria following from law, executing regulations, insurance agreement, work contract) is a dominating security requirement. Let's assume that the goal of the purchaser is not only the fulfillment of the criteria of binding legal directives and contracts, but also the economic and functional effectiveness of the whole security system. We have used the word "assume" because in practice it is common that it is not possible to identify the given person from the recordings of security camera, while general conditions presented in the insurance agreement were satisfied. In the same way it is not a problem to meet the private security service, which wasn't successful at any of its "sharp" actions, while, again, general conditions presented in the insurance agreement were satisfied. From my own experi-

ence I can say, regardless the satisfaction of agreement requirements, not always the injured receives compensation. This fact is usually caused by inexact and generally formulated requirements of the respective insurance company, which are concretized by its legal and technical assistants only in case an insurance event occurs. From the presented examples follows that it should be in the personal interest of every subject which wants to insure his or her property, to include the whole effectiveness of the proposed or realized security system.

5. Property protection from critical infrastructure point of view

Also not all the state and private subjects can afford to secure their property only on the basis of requirements of insurance companies. It is about subjects which, on the basis of their activity, significantly influence the operating of the state, i.e., they influence lives of big amount of people. These subjects become on the basis of nature of their activity part of so called critical/defensive infrastructure. Under critical infrastructure we understand a set of physical or virtual systems, organizations, directives and other services, whose disruption, deficiency or destruction could cause disorganization of the society stability and state security, develop crisis or seriously influence functioning of the state administration and autonomy in crisis [5], [11]. On the basis of the given definition we can say that the following subjects come under critical infrastructure: subjects whose activity interfere in the area of providing basic goods and services with sectors, e.g., energetics, transportation, supplying with fuel and food, medical services, financial services, communication services, etc [4]. The question is how to secure property of these subjects, when insurance conditions aren't sufficient and no legal directive defines specifically the way and form of protection, as it is defined, for example, in the case of law of classified information protection. The existing legal directives define the way of property protection more or less in a proclaiming way and they do not present any concrete solution proposals. An example of such legal directive could be nuclear law [10]. It is set down in a proclaiming way in one of its executive regulations that the subject must secure by an appropriate combination of IDS effective enough and mechanical debarment means detection of violators and slowing down their progress and, in this way, enable the action unit to stop the violator's progress even before its manipulation with the subject of protection. Here, we have an interesting and important condition – even before its manipulation with the subject of protection. We can call this way of protection a *variable way* of physical protection, i.e., it is required to use enough passive and active elements of protection so that the violator is stopped by an action unit even before the individual manipulation with the subject of protection. The problem is the fact, in which a ratio the individual protection elements must be represented in the system. The law solved this problem by means of executive regulation where it sets down again, in a directive way, specific conditions of physical protection of the given subject.

In order to secure physical protection in a variable way, software tools were created, which use qualitative-quantitative methods, evaluating the existing or proposed security system, following from certain measurable values like Probability of Detection PDi, Response Force Time (RFT), Delay Time (DT) a Probability of Correct and Timely Guard Communication PC. On the basis of these data the Probability of Interruption P_I is estimated. In USA until the year 2004, 76 studies, methodologies, pieces of software or reports were developed, which engage in problems of attacks against a subject coming into contact with nuclear material [1]. Most of these studies were designated for development and implementation of computer models or decision trees, using mostly stochastic mathematical methods (e.g., Monte Carlo). The so called **EASI model** (*The Estimate of Adversary Sequence Interruption*) is used as basic methodology for judging the effectiveness of the security system which is integrated also in more complex methodologies, for example, in software tools **SAVI** (*Systematic Analysis of Vulnerability to Intrusion*) and **ASSESS** (*Analytic System and Software for Evaluation of Safeguards and Security*). The three given software tools come from the workshop of American laboratories Sandia National Laboratories [11]. These laboratories conduct research in the area of nuclear weapons, military technologies, energetics and critical infrastructure in the area of national security and protection.

The EASI Model is a stochastic method using mean values and standard deviations of above described times where in the mutual relation with Probability of Detection provides estimation Probability of Interruption P_I. Its disadvantage is the fact that it is

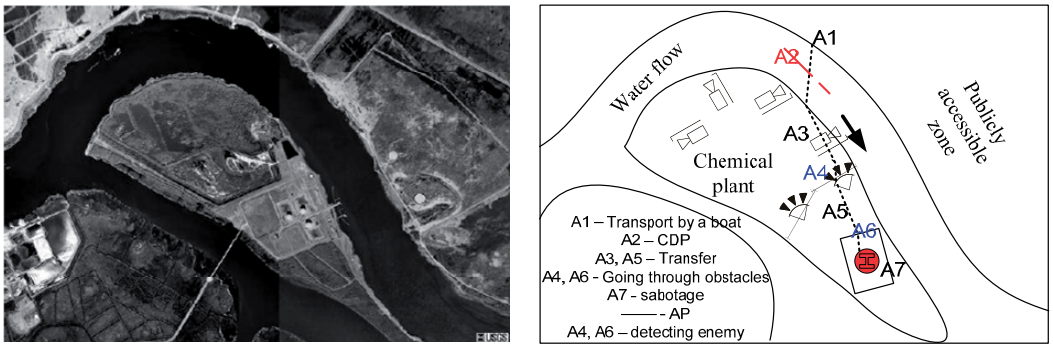


Fig. 2 a) Aerial photograph of a chemical plant b) Block diagram of eventual attack

able to estimate P_I only in one adversary path. The process of adversity is usually recorded into the so called *Adversary Sequence Diagram*. These deficiencies are removed in already mentioned SAVI and ASSESS methodologies [3]. Philosophy of the EASI module follows from the following equations:

$$PI = f\left[RFT, DT, P_{Di}, P_C, E(DT) > E(RFT)\right],$$

where *RTF* and $DT \in N(\mu, \sigma^2)$

$$P_I = \left[1 - \left(\prod_{i=1}^{j}(1 - P_{Di})\right)\right] * P_C$$

Fig. 2 a) presents an aerial photography of a chemical plant, while Fig. 2 b) shows a possible path of attackers and individual activities which they have to execute in order to reach their goal, which, in this case, is destroying the storage tank of detrimental chemical substance. Fig. 3 illustrates attackers' path with the help of a sequential diagram ASD.

SAVI software tool gives security system effectiveness estimation or vulnerability estimation, with respect to intentionally active outer or inner attackers, while it takes into account attacks type of damage or theft of given asset. Effectiveness or vulnerability of the security system is estimated on the basis of probabilities of attacker's elimination for individual possible paths of violation. The ASSESS methodology replaced the previous SAVI methodology, which didn't take into account some of the important factors (e.g., cooperation of an internal employee with an external violator). ASSESS is a software tool which evaluates the way of physical protection of nuclear material against theft and sabotage. The program consists of six modules *Facility* (the module enables analysis of elements of all system, e.g., protective elements and building constructions), *Insider* (the module enables definition of personal authorities and responsibilities of internal employees, furthermore it enables a definition of possibilities of internal employees to use slyness and falsehood to reach their goal), *Outsider* (the module enables to estimate probability of thwarting intentional security incident), *Neutralization* (the module enables to estimate probability that the action unit neutralizes attacker and stabilizes the situation) and *Hand-Off Collusion* (the module enables to assume cooperation of internal employee helping the outer attacker).

Nowadays the sections of the ministry of energetics in USA use the simulation software tools JCATS (*Joint Conflict And Tactical Simulation*), which started in 90's (JTS). JCATS is helping software tools, developed for training commanders and their action units in commands and directives during the action. Software tools take into account both actions from the ground and from the air, while it takes into account action of fire service unit. JCATS was developed on the basis of its predecessors JTS (*Joint Tactical Simulation*), UCCATS (*Urban Combat Computer-Assisted Training System*) or SEES (*Exercise and Evaluation System*). Other software tools which will be in the future used at simulations of action units look bit futuristic, but their time as the consequence of new technologies development will come (see Fig. 4). These tools are not directly used for judging the state of property physical protection, but they have to help architects in order to map the given object and to eventual simulation of already arisen security incident [2].

Apart from the already mentioned tools used for evaluation of security systems' effectiveness, it is appropriate to mention some other tools, methodologies and software dated earlier (70's and 80's of the 20th century), e.g., methodology BATLE (*Brief Adversary Threat Loss Estimator*), VISA (Vulnerability of Integrated Security Analysis), ISEM (*Insider Safeguards Effectiveness Model*) or FESEM (*Forcible Entry Safeguards Effectiveness Model*) [1].

6. Conclusion

In this article, three basic approaches to secure physical protection of property were introduced. There is a directive-oriented, variant-oriented and variable way of physical protection. For the most effective way of protection we can consider the variable way of protection, which allows, due to its flexibility, the designing of

a) b)

a)*Fig. 3 a) Block diagram of ASSESS b) screenshot taken from JCATS software*

a) b)

Fig. 4 a) CRIA ISMA STERTM b)A DEPT
(source: http://www.dtic.mil/ndia/security2/jaeger.pdf)

the system in such a way that it best suits requirements, conditions and possibilities of the subject. However, on the other hand, there doesn't exist any publicly accessible general methodology, handbook, manual or other tool which would define a detailed procedure at realization of physical protection of property. Certain possibilities and solutions are offered by system tools which were developed for needs of protection of nuclear material and equipment. Here, we point out some of its deficiencies or disadvantages. We can mention for example:

- tools were created for protection of specific materials and non-commercial pieces of equipment,
- they haven't been modified from the time of their creation (EASI – 1980, SAVI – 1987, ASSESS - 1989), which also indicates critics of individual authors and users,
- they don't enable evaluation of danger level in multi-level objects,
- the tools require a big amount of expert evaluation and the fact that resulting evaluation is based greatly on mathematical statistics and probability theory can lead to inexact or misleading conclusions (e.g., in case incorrect inputs' interpretation or absence of relevant data),
- the tools do not take into account the European technical norms and standards used in the area of physical protection of property.

In spite of the above mentioned deficiencies or better said disadvantages, it is necessary to prefer and further elaborate the variable way of physical protection, which is also affirmed by the fact that the new security conception of the NBU SR (National Security Agency of the Slovak Republic) declares a change of variant-oriented way of classified information protection to the variable one. The necessity of physical protection has to be derived from reaction times of passive or active elements of the security system.

References:

[1] BAGNALL, A. M., WILBY, J., GLANVILLE, J., SOWDEN, A: *Scoping Review of Sabotage and/or Tampering in the NHS,* [on line]. Centre for Reviews and Dissemination. Report25. [cit.10.10.2007], <http://www.york.ac.uk/inst/crd/pdf/report25.pdf >, 2004
[2] PHILLIPS, G., MAY, D., GOLDEN, M., MASTON, M.: *New Vulnerability Assessment Technologies vs the Old VA Tools,* [on line], NATIONAL SECURITY PROGRAM. [cit.10.10.2007], <http://www.projectenhancement.com/new.pdf>, 2004
[3] GRANT III, F. H., MINER, R. J., ENGI, D.: *A network modeling and analysis technique for the evaluation of nuclear safeguards systems effectiveness,* ACM Press, New York, NY, USA. ISSN 0163-6103, 1978
[4] HOFREITER, L.: *Safety, risks safety and threats (in Slovak)*, ZU, ZILINA, 2004, 146 S., ISBN 80-8070-181-4(23/23)
[5] MIKOLAJ, J., HOFREITER, L., MACH, V., MIHOK, J., SELINGER, P.: *Terminology of management safety (in Slovak)*, Vykladovy slovnik, Kosice, Multiprint s.r.o. 2004. ISBN 80-969148-1-2, 2004
[6] REITSPIS, J. et al.: *Managing of safety risks (in Slovak)*, EDIS, ZU, Zilina, ISBN 80-8070-328-0, 2004
[7] *Act NR SR Nr. 215/2004 Z.z. at security of classified materials (in Slovak)*
[8] *Public notice NBU Nr. 336/2004 Z.z. at physical safety and a objects safety (in Czech)*
[9] *Act NR SR 483/2001 Z.z. at banks (in Czech)*
[10] *Act NR SR Nr. 541/2004 Z.z. at peaceful exploitage nuclear energy (atomic act) – in Czech*
[11] *Sandia National Laboratories [online], SNL. [cit. 10.10.2007], www.sandia.gov.*

https://doi.org/10.26552/com.C.2008.1.40-44

Lubomir Ciganik – Iveta Balasicova *

PROTECTION AND DEFENCE OF RAILWAY TRANSPORT AGAINST INTERNATIONAL TERRORISM

The authors deal with the threat of international terrorism for the EU and global community and target the attention to infrastructure, critical infrastructure and rail transport. They analyse the EU approach towards the protection of critical infrastructure and point out the core criteria and principles of processing the protective system in separate countries. Moreover they concentrate on the protection of rail transport and possibilities of terrorist attacks. The last part presents danger of radiological terrorism and danger related to transport of radiological material on rails.

Key words: infrastructure, critical infrastructure, traffic infrastructure, rail transport, elements of rail transport, crisis, threat, crisis situation, international terrorism, protection and defence, police activities, police actions, intelligence, analysis and measures.

1. Introduction

European integration and world-wide globalisation have a significant impact on the countries in a way that they considerably change social requirements – social order for infrastructure protection, mainly protection and defence of critical infrastructure (CI), transport included – namely rail transport. Besides traditional threats such as disasters, accidents, catastrophes and crimes related to individuals and groups, terrorism represents a new threat. *It is an international terrorism, which might have a character of permanent threat for the European and global community* [4].

Ongoing terrorist attacks in Europe as well as growing violence in Iraq do confirm the saying that military operations in Muslim countries have only developed a risk of terrorism in the western world. Fails to fight against terrorism by means of wars have paved the way for the fight predominantly by more peaceful means. More and more the people address their governments and ask them to give up wars and instead, try to find the solutions of the reasons of terrorism.

2. Threat of international terrorism

Europe has been thinned by an international terrorism of Al-Quaeda [1] kind as is the case of train attacks driving the commuters to work and schools in Madrid. 192 people died and about 1600 were injured during the attack of 11th March 2004. As the first step the government accused ETA. Government's approach and socialists' shock were perhaps the most decisive factor that caused the victory of socialists in the election of 14th March 2004. The new Spanish government pulled its military units back from Iraq and thus fulfilled the election vow nevertheless Al-Quaeda's request as well. The Madrid attacks have intensified the European Union attempts to combat terrorism. On 15th March 2004 the European Commission issued an Action Paper [11] where contradictory issues and usable tools were drafted. This Paper presents five types of activities which, as proposed by the Commission, the EU shall react to: declaration of solidarity, improved implementation of existing legislative tools being relevant for combating terrorism and adoption of the proposals for measures discussed by the Council, strengthening the fight against terrorism financing, improvement of operational cooperation and coordination, external activity and other tools. On 25th March 2004 the EU leaders adopted Declaration on Combating Terrorism, which acts as a supplement to Action Paper of the EU for the fight against terrorism from the year 2001. One of the objectives of Declaration is to protect the security of international transport. Terrorist attacks aimed at transport systems in Madrid and London in 2005, which resulted in loads of victims and which were caused by Al-Quaeda cannot leave national and international terrorism in Europe unnoticed. Once those attacks for terrorist organizations such as IRA, ETA and FLNC (National Front for the Liberation of Corsica) were performed, a new period comes in the front, the period of searching a new identity because provided you would wish to present yourself as a militant willing to use violence as a tool of enforcing your own political goal, you would face the resistance of the European public poll.

Having witnessed the attacks on the U.S, Spain and Great Britain, the need to protect and defend CI on the national and international level has considerably grown up. That's why the countries and then international organizations themselves have changed their legislation and organizational measures in order to ensure the protection and defence of CI, which is from strategy viewpoint, inevitable for the operation of the state and if lost lives could be endangered that might reason immediate economic and social damage.

* **Lubomir Ciganik, Iveta Balasicova**
Academy of the Police Force, Bratislava, Slovakia, E-mail: ciganikl@minv.sk

Critical infrastructure [2] is a strategic element for the state and its failure would lead to a danger for the society as such. The European Union makes huge efforts to prepare Europe for an adequate response to terrorist attacks targeted at elements, buildings and objects of CI including the protection of rail transport. The current efficiency status of critical infrastructure protection within EU seems to be insufficient; the states are not able to adequately react to changing risk and threats conditions, nor they are able to effectively operate and solve the terrorism-related problems.

2. Sources of critical infrastructure protection

In the whole process one may find a quality enhancement in the understanding of security [5]. The principles that are placed in the front are: international or regional cooperation, complexity, comprehensiveness, planning, coordination, legality, subsidiarity and proportionality. Such principles have been even applied by the EU – draft of the Council regulation on identification the European critical infrastructure and assessment of the need to improve its protection.

The draft responds to the EU objectives and is in compliance with the objective stating "Keep and develop the Union as a space of freedom, security and justice, which guarantee free movement of persons and where appropriate measures related to protection of external borders, asylum, migration and prevention and fight against crime have their place" [7]. Moreover it responds to other relevant documents adopted by EU such as "Prevention, readiness and reaction to terrorist attacks" and "Green book on European program on the critical infrastructure protection" (EPCIP).

The Commission is of the opinion that CI does exist in member states and once being violated or damaged, two or more member states might be affected. It is also real that the failure of critical infrastructure in one state may affect the other member state. Thus the Commission states that such critical infrastructures should be identified and marked as European critical infrastructures (ECI) and protective measures should be adopted. Namely, we speak about an integrated approach on EU level that would act as a supplement to national programs for the critical infrastructure protection.

For all member states there must be a common framework, which would ensure coherent and united application of the principles and procedures in dealing with the European critical infrastructure. Common framework should deal first of all with the following issues:

- determine basic notions, – determine sectors where critical infrastructure will be identified, – elaborate methodology of risk and threats analysis, – identify the methods of protection and scope of security measures, – identify range and form of planning and other managing documents, – determine principles for the protection of classified data, – determine scope and method of material and financial provision.

A common framework defined this way should be applied in the national programs either, partly for the protection of European critical infrastructure, but predominantly for other critical infrastructures within a state.

The present requires an optimal, rational and effective system of the protection and defence of CI, transport one including – rail transport, whether we speak about separate areas, sectors, facilities, objects or elements. States and international organizations are expected to create institutional, legislative and organizational conditions for the effective protection and defence.

One of the main tasks within the Slovak security policy is to continuously analyse risks and threats on the national and international level. Risk analysis is a necessary tool how to understand threats in the world of globalisation, not excluding the analysis of security system and the protection of social values. It is obvious that building up isolated state units is not sufficient in this global world; on the contrary it is necessary to build up integrated systems where separate units are able to cooperate and get involved into crisis situations solutions, join one's own attempt according to the scope and character of endanger.

By applying the subsidiarity principle, the EU concentrates on the elements of world-wide significance and leaves other elements of CI system fall under the member states responsibility. Member states contribute to the system by providing information on threats and possible solutions; the system provides risk mapping. All information providers must be assured that information will be processed in an accurate and careful way. We must have at a disposal appropriate legal framework to ensure that classified information is processed properly and protected against unlawful use or publishing. All it falls under the EUROPEAN PROGRAM FOR CRITICAL INFRASTRUCTURE PROTECTION – EPCIP. Its objective is to ensure reasonable and steady security protection, as few failures as possible and fast examined measures.

The level of protection should not be the same for all critical infrastructures, but should be reasoned by the impact, which could cause its failure. Basic criteria for the protection of critical infrastructure are as follows:

- MS governments within their competence shall determine and create the list of critical infrastructures according the EPCIP priorities
- cooperation of industrial enterprises with government in order to provide information and diminish the possibility of incidents that would cause large or long-term breakage of critical infrastructure
- attempt of European Community to create a common approach how to deal with the security of critical infrastructures via the cooperation of all public and private subjects.

Core principles of EPCIP are:

- subsidiarity – protection of critical infrastructure falls under the responsibility of subjects mainly on the national level (MS and owners, providers)

- supplementary principle – a common framework of EPCIP would supplement already existing measures. Introduced communitaire mechanisms would ensure overall implementation of the program
- confidence – information of critical infrastructure protection would be kept in confidential environment and protected against misuse
- cooperation of subjects involved – all subjects involved, including MS are given a certain task in CI protection. MS bodies would be appointed the leading and coordinating status in the development and implementation of approaches for CI protection in a given territory. Owners, providers and users would be actively involved on the national and EU level
- proportionality – protective strategies and measures should be proportional to a certain danger. They should concentrate on the most risky areas
- indivisibility of security – strengthening of CI in the EU could be reached by the implementation of EPCIP, i.e. common objectives, methods etc. which would enable the exchange of the best practices and control mechanisms.

By its resolution no. 967 of 7th December 2005, the Slovak government adopted "Plan for the Security Council of SR for the year 2006" and put vice-chairman of the Slovak government and Economy Minister under an obligation to submit the "Conception of critical infrastructure in SR and the protection and defence methods", which was performed. By its resolution no. 120 of 14th February 2007 the government adopted the draft of submitted conception and at the same time requested to elaborate the National program for the protection and defence of CI in SR and submit the bill on critical infrastructure. Submitted conception creates a sufficient space for complex elaboration of CI in SR in connection to EU standard.

3. Subjects of protection and sources of critical infrastructure protection

Subjects [6] involved in the protection and defence of rail transport are:

- international organizations, international partners
  EU – common security policy, common security measures (recommendations), common legal protection of CI
  COLPOFER, RAILPOL – cooperation
- government, public administration
  legislative, executive and judicial power, adoption of legal framework for the protection and defence of rail transport, division of competences into public authorities, SIS (Slovak Intelligence Service), police, railway police and armed forces competences, etc.
- territorial units
  integrated rescue system, evacuative plan, civilian emergency planning
- state and private economic operators
  Railways of SR (Železničná spoločnosť, a.s.).

Subjects involved in the solution of rail threats concentrate on the following areas:

- risk and threats monitoring and analysis, development tendencies
- strengthening the protection of objects and facilities
- defence of separate objects and facilities against possible terrorist attacks
- civil protection tasks, alleviation of consequences, health service, vet service, consolidation of area of activities or state region
- emergency operation of rail transport, emergency transport of citizens and loads, emergency routes
- recovery of functional and effective status of rail transport.

Police competences result from the legal framework, which also determines the scope and contents of involvement. According to the valid legislation and international agreements binding for the Slovak Republic we may state that the police services (armed security forces and armed forces) concentrate on the competences and tasks resulting for each state in the area of protection and defence. Railway police have at their disposal power and tools to accomplish all the tasks related to prevention, lowering the risk of being endangered, warding off the attack, alleviation of consequences and substitute operation of rail transport.

In order to perform the job of the Railway police effectively, the risk analysis and assessment should give a response to the basic questions such as:

- Which elements of rail transport, facilities, premises and objects might be endangered?
- What are possible targets of terrorist attacks (destruction, contamination etc.)?
- Where are these targets situated?
- How might these targets be reached (taking hostages, kidnapping, etc.)?
- What are the weak points of rail transport protection?
- Who are potential terrorists?
- What is the level of training of persons in charge of the protection?
- How are technical tools applied?
- What is the cooperation with the police, rescue and emergency services (armed security forces, armed forces)?
- How is watch service applied for citizens (warning system) and public administration?

While drafting the plan of the protection and defence we follow the conclusions of the risk analysis and assessment as well as determine the terrorist goals. The attacks may be targeted at elements, facilities and objects of the rail transport such as:

a) trafo-stations and switch-control rooms, high tension nets, energy supervisor, compress stations
b) cars, stocks with chemical materials – burning, explosive, poisoning (ammonia) etc.
c) cars, stocks with radioactive material, etc.
d) rail crossings, bridges, tunnels, etc.
e) trains, railway stations
f) destruction, violation of the transport (e.g. violate the direction)
g) connecting systems including communication systems and technologies etc.

Nuclear (radiological) terrorism may be of the following forms: the use of stolen or otherwise obtained ready-to-use nuclear gun, the attack by the use of nuclear explosive device made from stolen cut material, the use of device in order to disperse explosives of highly radioactive (radiological) material (so-called dirty bomb) or the attack or sabotage against nuclear (radiological) device [3] or transport, where radioactive dispersion is possible.

Transport of radioactive materials is in the process of development due to their increasing usage. There are approximately 1.5 millions deliveries in the EU within one year. Such a transport joint with the production of electricity represents, in fact, a small percentage out of overall number of such deliveries.

At this point, regulations and procedures valid in individual states come to the front. Nowadays, the internal regulations of the states are more or less the same, since they are based on international requirements (ADR – The European Agreement concerning the International Carriage of Dangerous Goods by Road, RID – the International Carriage of Dangerous Goods by Rail, ICAO – International Civil Aviation Organization, IMDG – The International Maritime Dangerous Goods). It is more than important to carefully apply such requirements.

Transport of radioactive material in Slovakia is set by Act no.94/2007 Coll. from 7th February which is a supplement of Act no. 541/2004 Coll. on peaceful usage of nuclear energy (nuclear act) as amended and which changes the Act no. 238/2006 Coll. (act on nuclear fond). Besides others, the Act determines the competence of the Bureau of Nuclear Supervision in the Slovak Republic in the field of transport and loading of nuclear material, radioactive waste and burnt nuclear fuel, physical protection of the nuclear material transport and emergency planning. The act takes into account the requirements issued by International Agency for Nuclear Energy.

Besides administration documentation necessary for citizens' security, the Bureau approves, first of all, the means of transport usable for no longer than a five-year period. Valid are the regulations of the above mentioned act no. 94/2007Coll. as well as the provisions of the Bureau of Nuclear Supervision in the Slovak Republic which determines the details on requirements for the transport of radioactive materials (decree no.57/2006 Coll.). This decree regulates the procedures and methods of road, water, and air transport of radioactive materials.

When terrorist attack (using biological, chemical and radiological material) [5] is in question we must respect the fact that the society cannot be fully ready for any circumstances. Furthermore we must take into account the fact that a possible biological, chemical and radiological attack always brings its casualties. However, we must create, build and prepare a system, which would considerably reduce the number of these casualties. First persons who will respond to such attacks are members of Fire and Rescue Service, teams in charge of loading dangerous material, members of Railway Police and health rescue services and medical personnel since they will provide a first aid kit, maintain public order, search and prosecute offenders. Thus the requirements for training of such units are tough in order to improve their experience and skills.

Security authorities are empowered to eliminate the risk on maximum. One of the key players is the police and its coordination with other security services, mainly with Slovak Intelligence Service whose primary task is to obtain and analyse the information on organized terrorism. Railway police and the police itself are the core elements of the security system in the state and such a system must be comprised even in the protection of rail transport against terrorist threats. Nowadays, there is a need to improve the efficiency of the protective measures in the area of prevention, criminal intelligence, investigation and special task services, their use in our environment by relevant means, appropriate methodology of service activities within the cooperation and concurrence.

4. Conclusion

Plans in crisis situations must follow the principles and conditions of the fight against terrorism and respect the conditions and specifics of a certain area, territory and object. The plans are becoming practical measures and instructions in case the transport has been violated and basis for tactics of how to face them effectively and actively. The crisis plans may have different forms, however we may divide them into three categories, each of them has its own emergency measures. The categories are: measures against terrorist act, measures in the course of terrorist act and measures after the terrorist act is over.

To prevent and avoid the rail transport from being endangered it is necessary to have at a disposal certain measures, sufficient and effective forces and tools of the railway police. The goal of these preventive measures – actions is to discourage offenders and to pull them away from the attractive targets. If, nevertheless, the attack is performed, the measures enable to use those forces and tools in the territory in order to respond to the attack, search, isolate and apprehend the offenders.

One of the most effective measures is to perform security measures before the terrorist attack takes place [1] – in a certain territory. Such measures may be realized as a kind of the police preventive activities. Their scope, intensity and period will result from the level of danger (confirmed by intelligence activities, etc.) but, however still there is a space for political and economy decisions.

Protective and defensive police actions, which target at the protection and defence of the rail transport might get a global (international), regional (over-national) and local (national) character. Most frequently the preventive police actions will focus on the immediately endangered territory of rail routes, protection of objects – railway stations, stocks, cars and rail telecommunication.

References:

[1] CIGANIK, L., JASSOVA, E.: *Terrorism (in Slovak)*, Ustav politickych vied Slovenskej akademie vied, VEDA, Bratislava, 2006, ISBN 80-224-0892-1.
[2] HOFREITER, L.: *Protection of critical infrastructure (in Slovak)*, 9. vedecka konferencia s medzinarodnou ucastou, 1. a 2. cast, ZU Zilina, 2004, ISBN 80-8070-272-1.
[3] KIS, M., HRABOVSKA, D.: *Developmental models of crisis situation and application of measures related to economic mobilization in order to eliminate negative consequences of crisis situation (in Slovak)*, 9. vedecka konferencia s medzinarodnou ucastou, 1. a 2. cast, ZU Zilina, 2004, ISBN 80-8070-272-1.
[4] KULICH, M. et.al: *Terrorism (in Slovak)*, Terorizmus destabilizujuci fenomen sucasnosti a boj proti nemu, Bratislava: MO SR, 2002.
[5] PAWERA, R.: *New insight into European Union security (in Slovak)*, Policajna teoria a prax, Akademie PZ, Bratislava, 3/2004.
[6] PRUZINSKY, M.: *Protection of critical infrastructures (in Slovak)*, 9. vedecka konferencia s medzinarodnou ucastou, 1. a 2. cast, ZU Zilina, 2004, ISBN 80-8070-272-1.
[7] SIMAK, L.: *Security system of SR after EU entry (in Slovak)*, Ochrana osob a majetku, Kosice, 2004, ISBN 80-969148-7-1.
[8] *Conception of internal security of the Slovak Republic.*
[9] *National action plan of the fight against terrorism of the Slovak Republic.*
[10] *Constitutional law and other legislative regulations stated.*
[11] *European Commission action paper in response to the terrorist attacks on Madrid.*

https://doi.org/10.26552/com.C.2008.1.45-48

Josef Reitspis – Gabriela Kormancova *

IMPLEMENTATION PRINCIPLES OF THE PROJECT MANAGEMENT BY A SECURITY SYSTEMS DESIGN

The project management includes a complicated complex of activities. An important component of these activities is technical use of software for the support of project management and the management of the object, service (or their combination), which are outputs of the project. The important group of the activities creates the management of the cost with the accent on complex project efficiency. The next activities are connected with the management of the processes in the time, their coordination and their following communication among various participants of the project. There are many specialized activities in the life-cycle of the project, and for this reason the project manager must have a broad and complex area of special knowledge. He should improve not only in the area of his competences and skills but also in the area in which he works (in various economic areas or in the security area).

1. Introduction

Today, the project has become a standard part of our lives. The projects are realized for example in research, construction area and in services. People understand a design and project as some graphical forms which represent certain situations. Today we understand a design, project activities and project in a different way. The design includes many complex activities which are connected by the project preparation, realization, working and assessment.

2. Concept Definition of Project

Today people understand the project as a process of planning and management of big operations. We can see not only the result – project documentation – but also the creative process. There are many definitions of the "project". These definitions can be reduced to the following:

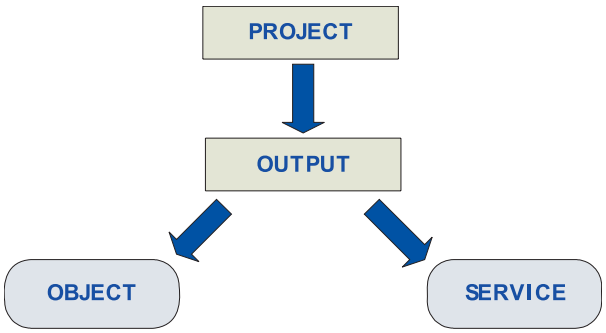


Fig. 1 Output of the project

The project is the systematic suggestion for the realization of definite innovation with the period of beginning and completion, the innovation with regards to time limit, realization of the output, costs and quality [1].

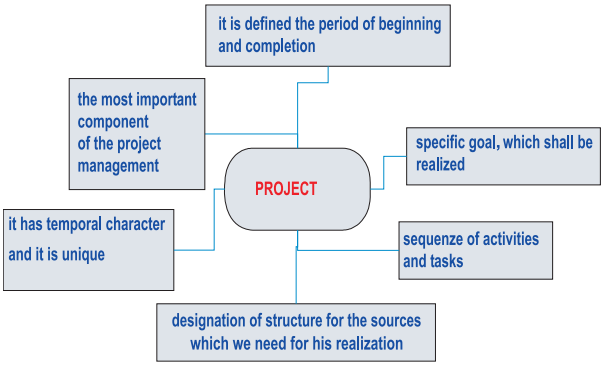


Fig. 2 Characteristics of the project

Every project is unique and this quality is managed with the monitoring of defined goals and with the concreteness of the conditions and environment in which is realized.

3. Categories and types of projects

The projects will be different due to the existence of all these presented characteristics not only in terms of extent, cost and time, but also in terms of its content. This is the reason for classification and categorization of projects according to their type.

* **Josef Reitspis, Gabriela Kormancova**
Department of Security Management, Faculty of Special Engineering, University of Žilina, Slovakia, E-mail: josef.reitspis@fsi.uniza.sk

3.1 Categories of projects

- *complex:* a long-time, unique project with a special organizational structure, this project includes many activities,
- *special:* an intermediate-time project, this project includes fewer activities requiring temporary additional staff,
- *simple:* a little project, which is realized in a short period, limited number of activities, and requires a limited number of staff.

3.2 Types of projects

- *building projects:* all types of projects, their goal is a new construction or reconstruction of an existing object,
- *research and development projects:* projects of strategic importance, which provide innovation in different economic areas,
- *technological projects:* projects which include new technologies to secure production effects (optimalization of technological and material flow, reserves detecting, etc.) and these projects bring the effects of time and space structure into production,
- *organization projects:* these projects include the change of existing structures [2].

4. Organization structure of project

The quality of project management depends mostly on people who are holders of the quality. It depends not only on their individual ambition but also on activities of the whole project team. The members of project team follow defined goals.

There are many interest groups involved in the realization of the project. Every group follows its own individual or group goals. The task of project manager's focus is the harmonization of individual and group goals with the project goals. These things are necessary for successful project achievement.

There are many subjects participating in the project (see Fig. 3).

4.1 Basic tasks project team members

Project sponsor – mostly managers of the company,
Project control – accredited member of the managers, responsible for the projects and is their coordinator at the same time,
Expert team – a group of experts, they co-operate with managers, who show interest in the project assignment and evaluate the process of steps, utilization of disposable sources, and effects of the project entry,
Contractors – they deliver products, work or services,
Managers of the project teams – they are responsible for the work of the project team (working on the subprojects),
Project manager – the key person creating the project planning, deciding about special positions in the project, coordinating various tasks from the beginning to completion and transfering outputs to the customer and its following administrative completion [4].

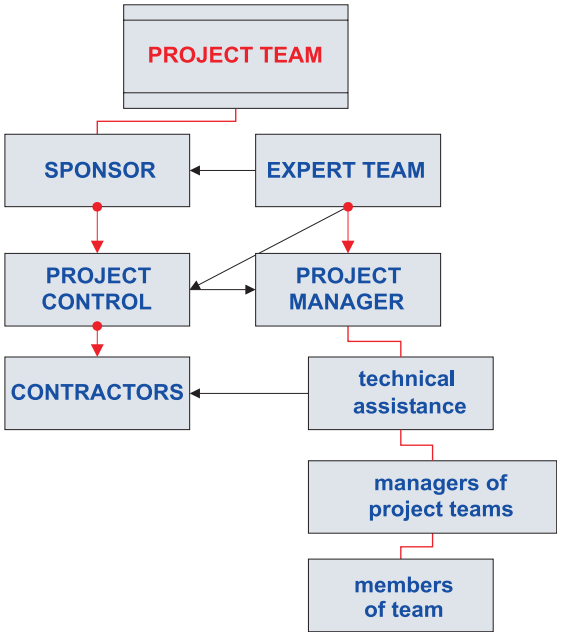


Fig. 3 Structure of the project team

5. Security systems design

The methodology of the design in the area of security systems is not defined as expressly as in the other areas (engineering, electrical engineering, building industry, etc.).

The design of security systems can consist of the following steps:
- *risk analysis:* includes analysis of the security environment, risk identification, their classification, assessment and priority,
- *simulation:* consists, for example, of simulation of functional behavior in selected parts of the security system,
- *construction (designing):* schematic design of components in security system with the use the location symbols,
- *optimization:* effective harmonization of various components in the security system,
- *verification of designed security system,*
- *project of security system,*
- *validation of security system.*

6. Software tools of design

The functioning of modern production, systems, and technological operations is not possible without consistent automation of preparation, production and monitor stages during the whole process. We use various software tools by the project management, which are very helpful during the project creation and they make work for the whole project team easier.

These tools are used mostly by projects of a great extent, where they have an irreplaceable task. The realization of the project

would not be possible without them or it would be realized with problems. The mostly used software tool in this area is *MS Project* (Fig. 4).

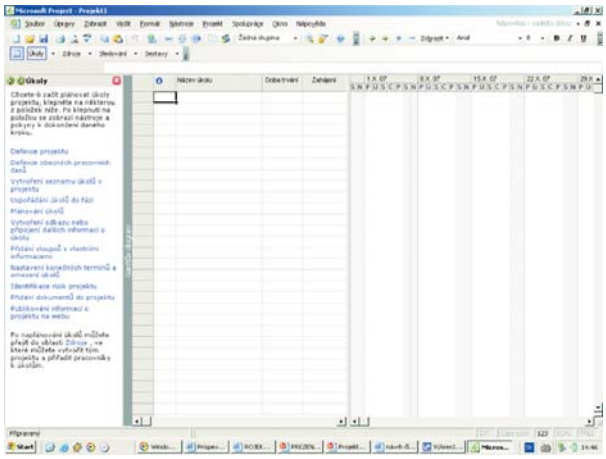


Fig. 4 Working environment of MS Project

Not only we can create completely new projects, but also it is possible to use "model projects" (templates). Advantages of this program are invaluable mainly for projects of a great extent.

When creating projects we can use the MS Visio software (Fig. 5). It creates simple drawings, schemata and also planning of simple tasks in the project.

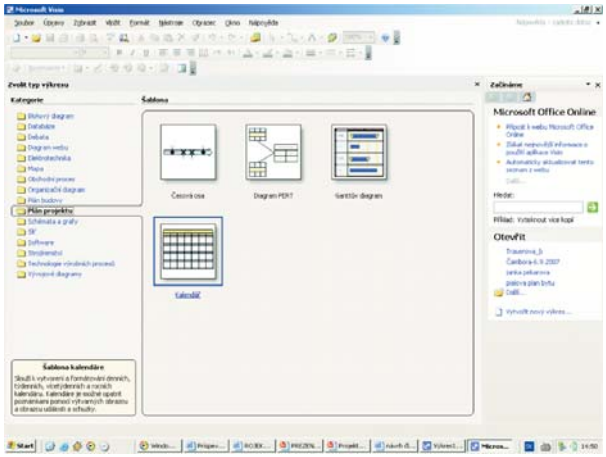


Fig. 5 Structuring of the categories in MS Visio

This program consists of various categories which include some relevant templates. It is comprehensible for a common user as well and sufficient for a projects of lesser extent.

The software tools named CAD (Computer Aided Design) is also used, for example the AutoCAD program. A big group of users apply this program when creating a project documentation including creation of space models. The advantage of this system is especially its exactness, saving of existing data, and the fact that we can create data bases for the using and creating various project documentation [3]. AutoCAD (Fig. 6) is the mostly used graphical system in the world. It offers a whole file of tools for 2D and 3D construction including the surface and dimensional simulation. It consists of various modules which make use of application program languages real. These application programs are adapted to the conditions of the local technical environment. It is important to use all professional tools for designing.

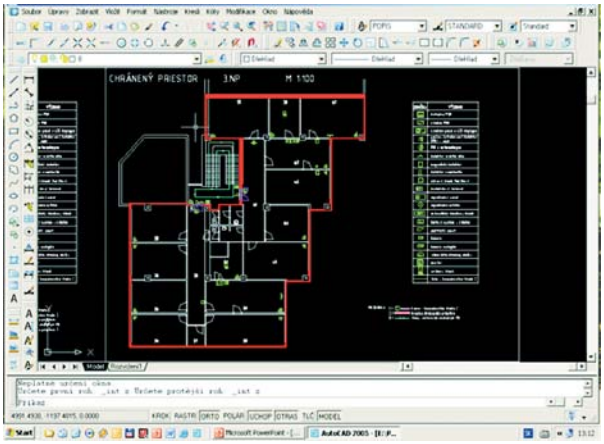


Fig. 6 Working environment of AutoCAD

There are also many others programs which can be used for the design of the security systems. One of the CAD programs which can be used in the security area is for example Video Cad (Fig. 7).

This software makes possible the design and correct location of security cameras in the space for their correct function and effective utilization, especially with reference to the requirements of customer.

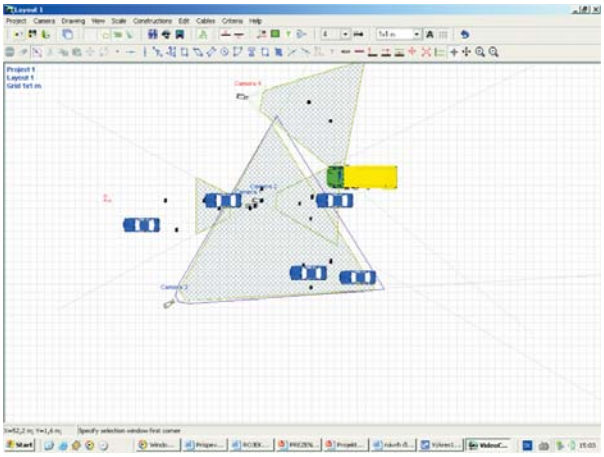


Fig. 7 Working environment of VideoCAD

7. Conclusion

The presented software tools are possible to use in the area of security systems design. In the future it is necessary to integrate all the project phases of the security systems design with the utilization of acquired experiences. At the same time it is important to define the methodical principles, basic process, management, control and responsibility for the realization of a security project.

References

[1] NEMEC, V.: *Project management (in Czech)*, GRADA Publishing, Praha 2000.
[2] ROSENAU, M.D.: *Operation of projects (in Czech)*, Computer Press, Praha 2000.
[3] FORT, P., KLETECKA, J.: *AutoCAD 14*, Computer Press, Praha 1998.
[4] LOVECEK, T., REITSPIS, J.: *Designing of security projects,* Proc.: 1. medzinarodna vedecko-praktickej konferencia Bezpecnost zivota ludí, ako podmienka staleho rozvoja sucasnej spolocnosti, Lvov, 2005, ISBN 966-699-131-4.

https://doi.org/10.26552/com.C.2008.1.49-53

Stanislav Bradka – Tibor Mikes *

CONTRIBUTION OF THE NATIONAL INSTITUTE FOR NUCLEAR, CHEMICAL AND BIOLOGICAL PROTECTION TO THE DEVELOPMENT OF METHODS AND PROCEDURES RELATED TO SAFETY ENGINEERING

The paper describes the National Institute for Nuclear, Chemical and Biological Protection involvements with regards to the development of methods and procedures related to Safety Engineering. It provides general information about the Institute's activities, history, presence and objectives for the near future to illustrate its role, tasks and responsibilities. The Institute's added values that consist in its share to the reduction of safety risks and incident consequences are presented and discussed in details.

1. Introduction

The main objective of the National Institute for Nuclear, Chemical and Biological Protection is to contribute to the protection of people and the environment against hazard under specific conditions, in which chemical, biological, radiological, nuclear (CBRN) substances and explosives are involved. Safety Engineering, according to various definitions in the literature, refers to any act of accident prevention with an obvious goal to increase the safety of operations, processes, systems, etc. Within this meaning, the Institute research activities concentrate on the methods and procedures closely related to this field of engineering.

It is evident that human activity will always unavoidably involve risks to safety. Improving the safety means reducing the risk. If all risks cannot be fully eliminated it should be interpreted that fewer fatalities, injuries and less damage occur to the property and the environment in case of an incident.

2. The background

It is a common routine of the authors dealing with the problem of the protection against CBRN substances to stress their potential abuse (terrorism) or to quote facts of their releases/spills in the past – either as a result of industrial or natural disasters. We do not consider it necessary to impress upon the readers the necessity of reasonable readiness of the society for such a potential incident. The following facts may probably have a more informative value about the attention paid to the protection against CBRN substances than any citations of the literature, normative acts, scientific authorities and historical events.

1. Starting in 2007, the EU will spend approximately €200 million per year for dual-use homeland security research projects. The EU money will be spent on technologies to support four broad missions:
   - border security;
   - protection of critical infrastructure;
   - crisis management;
   - anti-terrorism/counter-crime.

   A substantial part of this amount will be funding civil-military emergency response projects against biological, chemical and nuclear threats[1)].

2. There is an enormous quantity of publications in the literature and, if you put the key words (e.g. CBRN, weapons of mass destruction, NBC protection, terrorism, etc.) in the most common search engines on the world web, you may receive tens to hundreds of million references.

The issue of the protection against CBRN substances is very comprehensive and complex. On top of that, there exist lots of conventions, treaties, decisions, recommendations, etc. for each individual group of these substances, i.e. chemical, biological, radiological and nuclear ones, adopted at the international level and a corresponding number of various organisations controlling their observance. These organisations lay down different requirements for handling the individual groups of CBRN substances. Heterogeneousness of the requirements is due to the time of establishment and different historical development of the relevant organizations. The non-proliferation regimes according to the Australia Group – applied through the national export systems of the participating states – and the treaty based regimes in the case of the Chemical

* **Stanislav Bradka, Tibor Mikes**
National Institute for Nuclear, Chemical and Biological Protection, Milin, Czech Republic, E-mail: sujchbo@sujchbo.cz

[1)] See e.g. http://www.seceur.info/

Weapons Convention[2] (CWC) or the Biological and Toxin Weapons Convention[3] (BTWC) can serve as an example.

There are only a few countries in the world (and the Czech Republic is one of them) that are striving for the implementation of the internationally adopted principles from one centre. The supervision over the peaceful use of CBRN substances in the Czech Republic (CR) in compliance with international conventions stays within the competency of the State Office for Nuclear Safety (hereinafter the Office). The Office, apart from the supervision over the utilisation of nuclear power and nuclear materials, executes also the function of the National Authority of the Czech Republic for the implementation of the CWC and since 2002 it has also been fulfilling this task in relation to the implementation of the BTWC. The priorities of the Office are, from this point of view, strict controls of industrial facilities, import and export organisations, laboratories and other facilities where nuclear, chemical and biological substances are handled. Such controls should exclude any malpractice both from the respect of fulfilment of the objectives and the subject-matter both of the national legislation and the adopted international obligations.

Technical aspects of the supervision performed by the Office in the field of radiation protection and control of the observance of prohibition of chemical weapons and bacteriological (biological) and toxin weapons are guaranteed in a large extent by the National Institute for Nuclear, Chemical and Biological Protection (hereinafter the Institute or SUJCHBO, v.v.i[4].) established by the Office. The current organisational structure of the Institute (except for some elements like the Board and the Supervisory Board) was established only in 2000; nevertheless it has more than a fifty-year old history. The Institute's existence is closely linked to the boom of the uranium industry in the Czech Republic when the predecessor of SUJCHBO, v.v.i. provided mainly monitoring of miners under extreme climatic conditions. After the reduction of uranium ore mining at the beginning of the nineteen-nineties, the Institute transformed to providing expertises and responses to emergences. The transformation was successfully concluded during 2000 when the Institute's scope of activities was gradually getting narrower and specialised in the three fields: nuclear, chemical and biological protection. Concurrently, the Institute's instrumentation for the aforementioned activities got improved, its capabilities got extended and the Institute has become the main technical support body to the Office.

3. The contribution

SUJCHBO, v.v.i. as a public research institution (within the meaning of Act No. 341/2005 Sb[5]. on Public Research Institutions) has been designated to execute research and development activities focused basically on the identification and quantification of radioactive, chemical and biological substances for evaluation of their impact on persons and the environment since January 1, 2007. To perform the aforementioned *principal activity*, the Institute solves, either individually or in co-operation with other entities, comprehensive research tasks.

Main research and development activities that have been recently completed and/or are still on schedule at both the national as well as international level include:

- Research project "Study of material and personal factors for personal protection against chemical and biological agents including their detection and identification", which is divided into five sub-projects:
  - Methods for quantification of highly toxic chemical agents according to Schedule 1 of the CWC
  - Identification and quantification of compounds of biological origin by Liquid chromatography mass spectrometry (LC-MS) method
  - Elaboration of methods for rapid and effective detection of biological agents
  - Study of permeation velocity of toxic agents and surrogates through the protective materials in order to estimate the reliable time of personal protection
  - Physiological evaluation of effect of protective clothing inner layers' composition for the optimisation of their use
- Research project "Monitoring and evaluation of natural sources of ionizing radiation"
- Research project "Detection and identification of B agents by methods based on mass spectrometry" that is focused on detection and identification of B agents by MALDI-TOF mass spectrometry
- Research project "Protection against CBRN substances", which deals with specific requirements for the protection of First Responders
- The research project "Physiological aspects of personal protective equipment on their users"; its objective is to monitor the physiological behaviour of the user – the organism response to the workload, determination of usability or tolerance time to the protective means
- International research project "Innovative Measures for Protection Against CBRN Terrorism" (IMPACT) in the framework of Sixth Framework programme "Preparatory Action on the enhancement of the European industrial potential in the field of Security research" (PASR), where the main contribution of the Institute was in the area of CBRN decontamination.

It follows from the aforementioned that a decisive part of the Institute's activity is the research focused on evaluation and devel-

[2] The commonly used term for the "Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction"
[3] The commonly used term for the "Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction"
[4] Acronym "v.v.i" stands for public research institution
[5] Sb. stands for the Collection of Laws

opment of personal and collective protective equipment against CBRN substances, on their detection, identification and decontamination.

The secondary activity of the Institute is an activity performed in public interest, especially on the basis of demands of the competent organisational bodies of the state or territorial self-governing units with an objective to provide them professional support for their decision-making activities, assist in performing their tasks, including their education and training. Such activities are performed mainly by the Institute's involvement in the Integrated Rescue System of the Czech Republic (IRS CR).

As a part of *other activities*, SUJCHBO, v.v.i. also performs accredited and non-accredited tests and expertises, it organises professional courses, trainings and other educational events; performs consultancy, including research of partial problems related to its principal activity.

The Institute is a holder of relevant licences making it possible to handle and test otherwise prohibited chemical and biological agents or toxins. Meaningful research, development and testing of special protective equipment, investigation within the framework of the Institute's involvement in the IRS CR, as well as any other expertise in the given field, can be performed only under these conditions.

The Institute's laboratories have a Europe-widely recognized accreditation for the below listed activities. SUJCHBO, v.v.i. has also been authorized by the Office for Technical Standardisation, Metrology and State Quality Control as a metrological centre for calibration, verification and technical examination of the determined gauges of radon volume activity and radon equivalent volume activity.

Professional activities of the Institute are performed by the departments of nuclear, chemical and biological protection and an independent department of monitoring support.

- *Nuclear Protection Department* is focused on radon measurement and evaluation of its abundance, preparation, processing and evaluation of track detectors within the Radon Programme of the CR and beyond such programme. It also carries out personal dosimetry and monitoring of the environment in the vicinity of ionizing radiation sources, as well as both laboratory and field measurements of radioactivity.
- *Chemical Protection Department* and its laboratories are focused on detection, identification and quantification of highly toxic chemical agents in the working and natural environment. These activities are carried out both in laboratory and field conditions. It also evaluates quality of chemical and other special personal and collective protective equipment as well as quality of critical infrastructures protection. The department elaborates methods for their testing and participates in their development and standardization. Significant activity of the department is its support to the supervision exercised by the Office staff according to Act No. 19/1997 Sb. as amended.
- *Biological Protection Department* is focused especially on protection of persons under extreme conditions, including evaluation of personal protective equipment from the point of view of working and heat load. Besides, the department deals with detection and identification of biological agents and toxins. Such activity is utilised for the development of biological agents' detection methods and for supporting the supervision exercised by the inspectors of the Office according to Act No. 281/2002 Sb. as amended.
- *Independent department of monitoring support* conducts measurements in the vicinity of former and existing regions of uranium industry and mining works. It processes the results from the entire territory of the country, provides inspections, as well as support to the Radiation Monitoring Network of the Czech Republic in an air monitoring.

The Institute co-operates, within agreements concluded with other government departments, especially with the Ministry of Interior – General Directorate of the Fire Rescue Service of the Czech Republic, in solving all serious issues related to CBRN substances.

After the terrorist attacks in the USA on 11th September 2001 and after the subsequent wave of "anthrax consignments", such a "campaign" did not avoid the Czech Republic either. The first consignments appeared only about a month after the attack, and during the next three months, i.e. from October 15, 2001 to January 14, 2002, the Fire Rescue Service and/or the Police of the Czech Republic registered 2175 suspicious consignments. Due to its capabilities, instrumentation and its scope of activities, making it possible to analyse all possible components of the suspicious consignments in one site, the central Crisis Staff of the Czech Republic designated the Institute for collection and analyses of "suspicious consignments" and/or any other abandoned suspicious packages (potentially dangerous items) from the whole territory of the country.

More than 8000 consignments have been transported, mostly by the IRS CR, to the Institute for expertises and identification of unknown substances so far. These consignments and found items were processed according to the approved procedure based on the safety at work principles. The whole line for processing the examined items is designed to maximally ensure safety of operators as well as working environment. The coating compounds applied in the used areas are resistant to chemicals, possible toxic agents and decontaminants. Collection of decontamination waste products is solved in compliance with relevant regulations and standards.

To enhance safety during risky operations, the Institute developed various specialized equipment. One of them is a remotely operated drilling unit fitted in an air-tight container that can be filled with inert gasses. The container is equipped with cameras in such a way that the whole system is resistant to chemicals and pressure to specified extent. It can be connected to the filter-ventilation system and/or to any reservoir (see Fig. 1 bellow). It is successfully used for opening cylinders with unknown content as well as suspicious ammunition with an indeterminable content or

with a proved content of liquid. Though the examined ammunition found from World War II was smoke ammunition (filled with a mixture based on chlorsulphonic acid) in all the cases, it is generally known that the same artillery projectiles were also filled with bis(2-chloroethyl)sulphide (mustard gas).

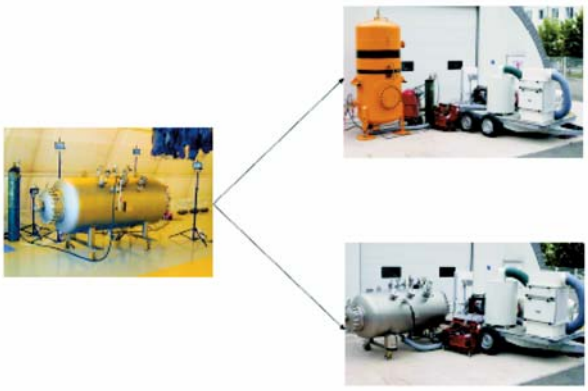


Fig. 1 Example of specialized equipment developed at the Institute

In the area of research and development the Institute closely co-operates with other research institutions of the Academy of Sciences and the Ministry of Defence of the Czech Republic, universities, especially the University of Defence, the South-Bohemian University in České Budějovice and the Faculty of Safety Engineering in Ostrava.

Among the Institute's basic achievements at the international level is its assistance to the Organisation for the Prohibition of Chemical Weapons (OPCW) and a bilateral co-operation with The Netherlands' Organisation for Applied Scientific Research (TNO). The Institute closely co-operated with well known European research institutes (EU Joint Research Centre JRC Ispra, the French Centre d'Etudes du Bouchet CEB, the Swedish Defence Research Agency FOI, Technical Research Centre of Finland VTT and others) within a multi-national consortium in PASR "IMPACT". In the last years, very significant was the co-operation of SUJCHBO, v.v.i. with Bruker Daltonics GmbH. The Institute developed a database of highly hazardous biological agents for MALDI-TOF mass spectrometry system on the basis of Bruker's requirements and in co-operation with the company.

For the coming years the tasks and requirements of the Office will remain the Institute's activities priority. Nevertheless, the Board and the Management link the scope of the Institute's future activities and further development also with the most demanding tasks of the protection against CBRN substances at the international level. Thereby the future activities will focus on the development of:

- Realistic scenarios to face CBRN threats,
- Testing methods
- Training and exercises

for complex systems being as close as possible to field conditions, with the following two main objectives:

1. Testing the quality of the protective materials and complex systems for CBRN protection
2. Contributing to the optimization of:
   - the use of the existing and newly designed protective systems and materials,
   - the methodologies for detection, identification and protection,
   - studies concerning behaviour (distribution, stability, etc.) of CBRN substances and/or surrogates in the environment under different conditions,
   - measurement/testing of the protective clothing and systems as well as cross-validation of the results,
   - bulk systems testing in real conditions.

The Institute wants to be more engaged in some of the OPCW's activities, especially in providing training to international inspectors and/or experts of the aforementioned organisation. The staff is ready and willing to be more closely involved in the Organisation's special projects.

The nearest objective in the field of testing is to complete the construction of a laboratory for large-scale tests to be conducted under real conditions. The laboratory could also be used for the simulation of industrial accidents and testing of large-scale objects within e.g. the "European Technology Platform for Industrial Safety" (ETPIS). SUJCHBO, v.v.i. closely follows the activities within the new European Community Regulation on chemicals and their safe use "Registration, Evaluation, Authorisation and Restriction of Chemical Substances" (REACH) that entered into force on 1 June 2007. Here, we can also see certain possibilities in providing expertises and engaging the Institute's capacities in some of the tests, especially the ones related to chemicals determined by the CWC (i.e. the Scheduled Chemicals).

Increased attention will be paid to the European Commission's numerous calls-for-proposals through its Seventh Framework Programme for research (FP 7 2007-2013). The objective is to actively participate in the fields of security research related to the protection against CBRN substances. The Board and the Management of SUJCHBO, v.v.i. consider it as a chance for the Institute to influence and participate in the debate on a new EU-wide health and safety standards, requirements and best practices.

4. Conclusions

The Institute, since its foundation, has significantly contributed to the improvement of protection of people and the environment in case of intentional or accidental release of CBRN substances. It has provided a wide range of expertise on security related sciences and research from general safety issues to security-oriented subjects. Its activities in the field of protection against hazardous substances are based on the following general principles:

- Anticipate, identify and evaluate hazardous conditions and practices,
- Develop hazard control designs, methods, procedures and programmes,
- Implement, administer and advise others on hazard control programmes,
- Measure, audit and evaluate the effectiveness of hazard control programmes.

Testing various equipment complexes and modelling a wide range of behaviour of surrogates and real CBRN substances in the near future with the aim to acquire data for reduction of their impact on persons and the environment, should increase the quality of protection against such hazard. The expected research results should be usable not only for further development of science and technology, but mainly for concrete technologically feasible measures in the given field.

References

A number of internal documents of the Institute have been used for drafting this paper but with regard to the nature of the presented information none of them are publicly available yet.

https://doi.org/10.26552/com.C.2008.1.54-59

Michail Senovsky – Pavel Senovsky *

CRITICAL INFRASTRUCTURE RISKS

Critical infrastructure can be taken as a phenomenon of recent time. Not only theory but also practice has shown that solving problems of the protection of critical infrastructure, especially ensuring its functionality, is a necessary precondition for the operation of public authorities, services, the viability of a region, area or country. The first step to protect the critical infrastructure must be the identification of risks endangering the security of single systems or elements. The contribution deals with the problems of searching for and denoting these risks and by looking for their interrelations.

Key words: Critical infrastructure, analysis, risk, assessment.

1. Introduction

The priority of critical infrastructure protection is given by efforts to preserve the functionality of public authorities. If the functionality of public authorities is preserved, then an assumption exists that also the population has a real chance of surviving a crisis state or situation without serious health damage. The complexity of ensuring the protection of critical infrastructure is given not only by the fact that it is a case of areas of decisive importance to the operation and functioning of the state, but also by the fact that many elements may significantly influence their surroundings, and cause thus a certain "domino" effect.

Then, the cardinal issue is a question of knowledge of individual limits of the system of critical infrastructure, and thus the determination of adequate protection.

What are the objectives of critical infrastructure protection?

As a simple answer we could use, e.g.: "When taking into account all threats and risks, the objective of critical infrastructure protection is to ensure the functioning of critical infrastructure objects, their interrelations and thus the creation of a basic precondition for the functioning of the state".

This general definition can be specified, for instance, as follows:
- A need to select critical infrastructure objects on individual management levels:
- The preservation of basic functions of a territory (municipality, region, state).
- The preservation of basic functions of the state.
- The preservation of functionality of objects necessary for dealing with incidents.
- The protection of potentially threatened objects.
- Establishing communication between the public authorities and entities of critical infrastructure.

The basic question of critical infrastructure protection is then the finding of interrelations between individual systems of critical infrastructure. By finding these interrelations we are able to assess or evaluate much better their vulnerabilities and consequences on the other systems of critical infrastructure. A result of critical infrastructure protection should be the minimization of consequences of infrastructure destruction so that damage to the functions of public authorities or services may be:
- short-term
- sparse
- controllable (also temporarily)
- limited in area.

To meet these preconditions, at first we must find risks, denote them, be aware of their interrelations across the systems of critical infrastructure, and accept adequate measures to eliminate the risks found. Countries can have various priorities and also different conceptions concerning which countries or elements of critical infrastructure should be included into the critical infrastructure.

The Security Council of the Czech Republic has determined the basic areas of critical infrastructure as follows: Table 1

ENERGY SECTOR	- Electricity - Gas - Thermal energy - Oil and oil products
WATER MANAGEMENT	- Water supply - Water security and management - Wastewater system
FOOD INDUSTRY AND AGRICULTURE	- Food production - Food safety - Agricultural production

* **Michail Senovsky, Pavel Senovsky**
Faculty of Safety Engineering, VSB – Technical University Ostrava, Czech Republic, E-mail: michail.senovsky@vsb.cz

HEALTH CARE	– Pre-hospital urgent care – Hospital care – Public health protection – Production, storage and distribution of pharmaceutics and medical means
TRANSPORTATION	– Road – Railway – Air – Inland water
PUBLIC AUTHORITIES	– State authorities and local authorities – Social protection and employment – Execution of justice and prison service
EMERGENCY SERVICES	– Fire and Rescue Service and Fire Brigades – Police of the Czech Republic – Army of the Czech Republic – Monitoring services of radiation, chemical and biological protection – Prognoses, alert, warning service
BANKING AND FINANCIAL SECTOR	– Finance – Banking – Insurance – Capital market
COMMUNICATION AND INFORMATION SYSTEMS	– Fixed net services – Mobile net services – Radio communication and navigation – Satellite communication – Radio and television broadcasting – Postal and courier services – Access to the Internet and data services

With regard to the fact that in the framework of EU any unambiguous method for the search for individual critical points of systems and their interrelations is not determined, the following part presents the opinion of authors about one of possible solutions for the analysis of critical infrastructure elements.

2. Network Analysis

For easy understanding, a network is necessary to be conceived as a large pattern with a large number of nodes and links. It is important to realise that we do not only search for individual elements that may endanger their surroundings, but that we search also for their interrelations by which a failure can spread. Some segments of critical infrastructure are of network character (road network, energy supply network); the other segments depend directly on these networks.

We are looking for a network model. We can say that individual objects can form network nodes. Pathways within the CI system then can be links between the nodes. However, we can see this problem also from the point of view of e.g. electricity distribution. Somewhere the transformer station will be located, from which electricity will be delivered to individual objects. Here, a system of distribution substations or switchboards will be implemented and electricity will be distributed to the last machine, to the last office. If we search further, it will be surely possible to map, describe and plot these networks.

2.1 Risk Concentration.

Risks endangering a network infrastructure are usually distributed non-uniformly in the network, concentrated into a relatively small number of "*critical*" nodes. These nodes are easy-to-identify by the number of links to other nodes and the capacity of them (according to the segment considered).

A difference between the uniform and the real distribution of nodes in the network is clear from Fig. 1.

Graphs in Fig. 1 were constructed by using the Scale-free Simulace program [1, 2].

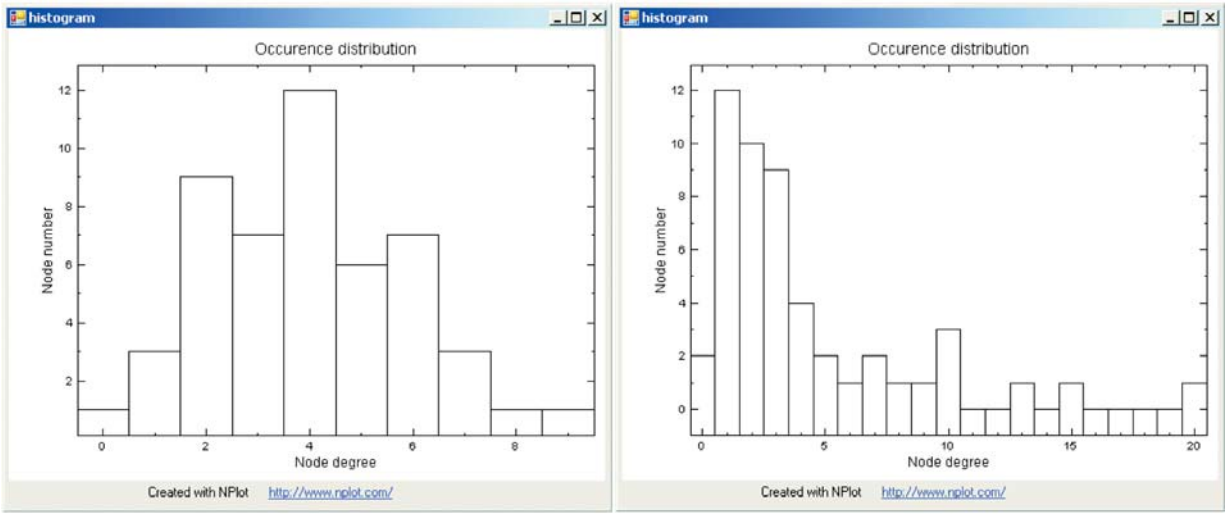


Fig. 1 Random frequency distribution in the network versus real node distribution in the network

The problem of network infrastructure protection often consists in the fact that we cannot afford to realise protection always on the same level for the whole network, and thus it is necessary to search for critical points – their putting out of action will bring the greatest damage. It is effective to protect just these points.

2.2 Networks, Cascades.

A sector failure is often caused by a cascade failure in the network. A relatively small fault in one node spreads through the network to other nodes, e.g. by a series of errors, the propagated error thus may lead to a collapse of the whole network. It is a velocity at which the fault spreads and the velocity at which individual nodes are repaired that will decide whether the damaged infrastructure will be finally restored or will collapse.

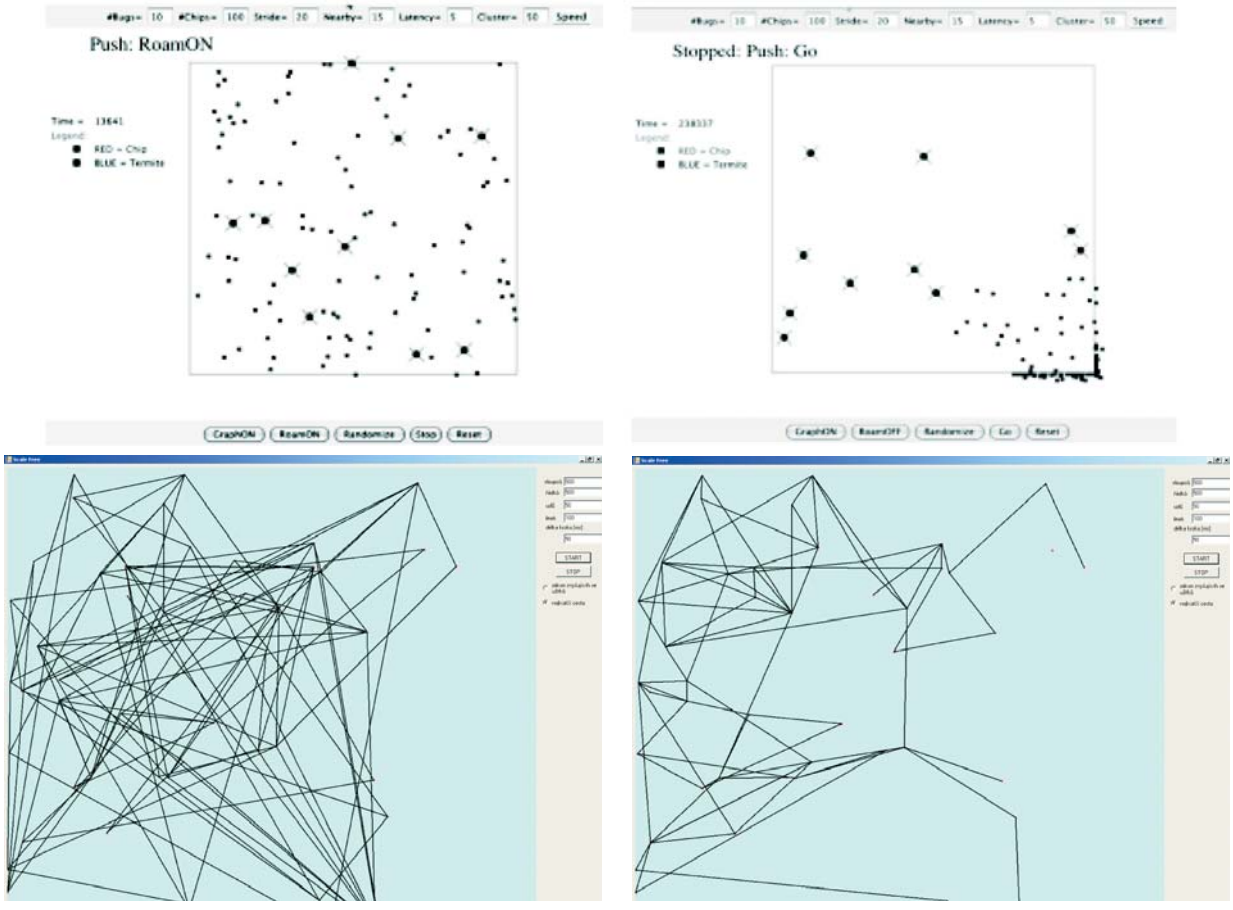
2.3 Simulation – an Approach to Searching for a Solution.

In studying networks, modelling as well as simulation is today implemented by special software. Simulations are usually based on the repeated application of simple principles in the universe of simulation, by which the gradual organisation of universum universe by an emergence effect will be achieved.

An example of result of such a simulation is presented in Fig. 2.

3. Vulnerability Analysis

To be able to assess quantitatively the vulnerability of a sector, we can use the vulnerability analysis that represents a model of vulnerability of critical nodes. The analysis consists of network analysis; for the determination of reliability of the whole system, engineering tools are used. These tools provide a complete system for the identification of system weaknesses and vulnerability estimation, and on the basis of this information we can determine steps leading to an increase in security. If we are able to find thus weak points of the system, in the following step it will be possible to madke the analysis of these critical points focused on searching for a possibility of synergetic effects of expected incident.



(start of the simulation) *(end of the simulation)*

Fig. 2 Application of shortest path principle to a randomly generated network

3.1 A Model Based on the Vulnerability Analysis.

The basic model of vulnerability analysis is a comprehensive analysis method that puts the network, faults (events) and reliability analysis together into one method for the quantitative sector analysis of a branched network. In the analysis, network branching is evident. We analyse the vulnerability of branching by using a fault tree; all possible actions are organised as an event tree.

Network analysis. The first step to make the vulnerability analysis is the mapping (identification) of a system being assessed. This step will also help us to search for individual nodal points and their interactions.

3.2 Fault Tree Analysis.

A fault tree contains vulnerabilities, and it is possible to model how single elements interact and create an error or fault. The root of the tree is there at the top of the tree and represents the whole zone or its main part, and the "leaves" of the tree represent partial threats endangering the zone. In the course of solving the fault tree we use logic and probability to estimate the occurrence (origin) of faults in the system. The outcome of fault tree analysis is a list of element vulnerabilities with the expression of probability of origin. In the following figure, an example of fault tree analysis is given.

3.3 Event Tree Analysis

We shall use the outcomes of fault tree analysis as input information for an event tree analysis. The tree of events is a list of all possible events and their combinations leading to faults. Event trees are binary trees, we consider yes/no. Each error may occur only once. The "root" of the event tree is there at the top of the tree and "leaves" are there in the lower part of the tree. The leaves represent all possible actions that may occur, including faults. The

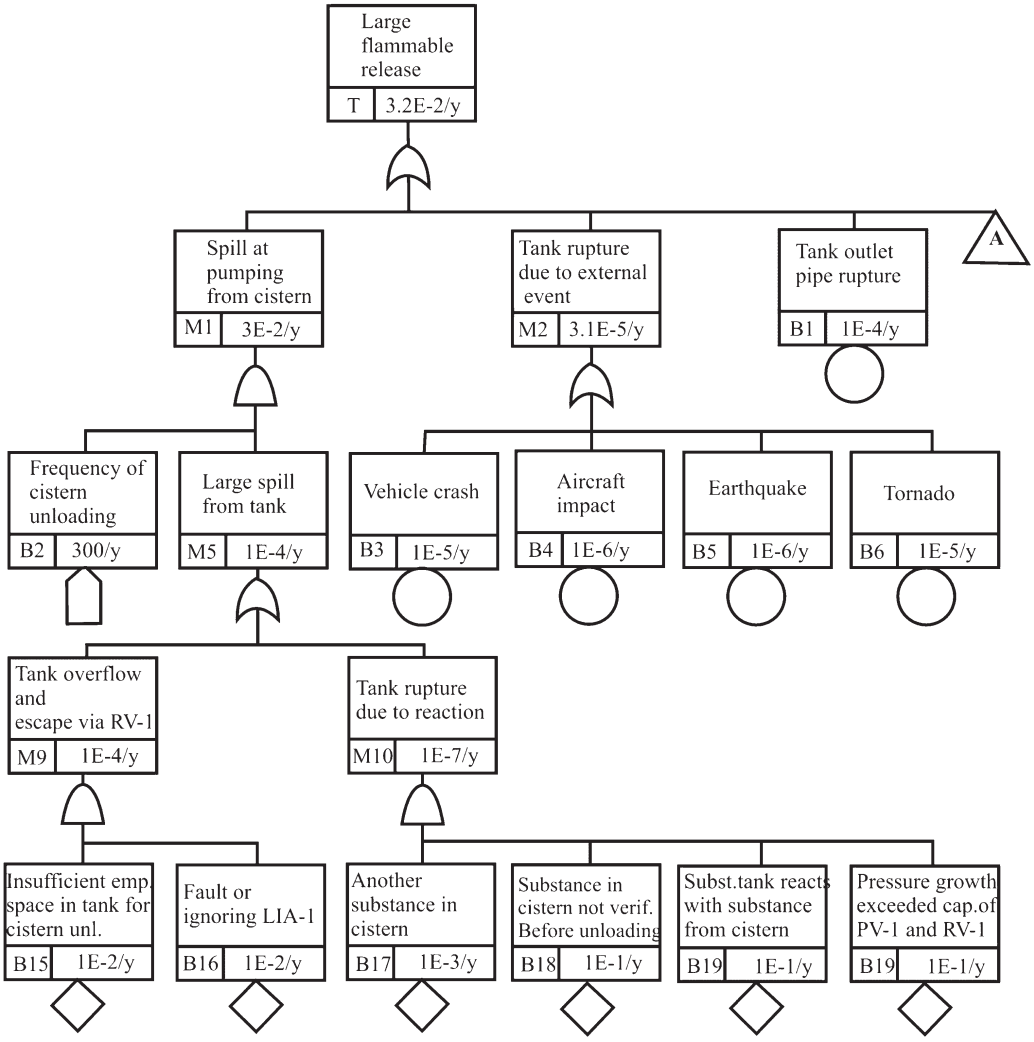


Fig. 3 An example of fault tree analysis

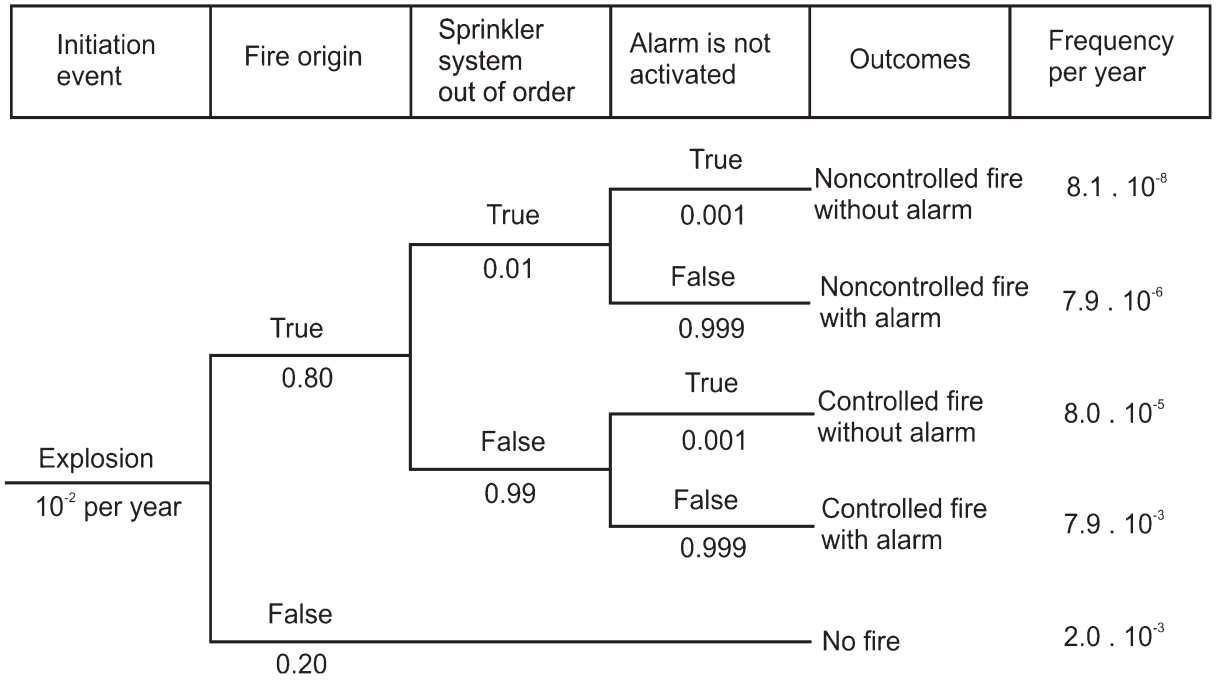


Fig. 4 An example of event tree analysis

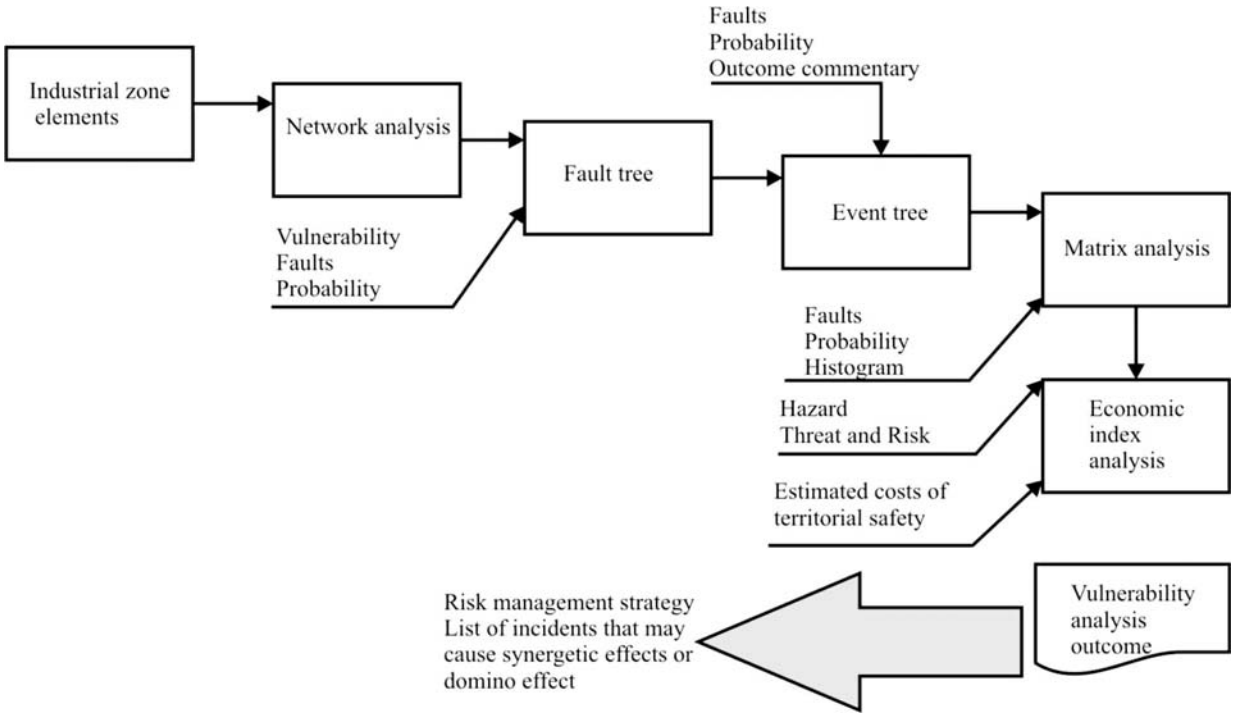


Fig. 5 Vulnerability analysis process

outcome of the event tree is a list of errors (vulnerability) and the probability of their occurrences expressed as the probability of error in a histogram. In the following figure an example of event tree is illustrated.

3.4 Matrix Analysis

The number of events listed in the event tree will become the number of potential errors. A matrix analysis can also work on the binary level or, in a more modern conception, each event can be described by more parameters, and thus we shall obtain a rather strong tool with which we are able, among other matters, to determine the severity of faults.

Diagrammatically the described system of analyses can be illustrated as shown e.g. in a figure given below.

4. Conclusion

Searching for an approach to the assessment of risks of critical infrastructure elements is at its very beginning. At present, we do not know any method being used by anybody with satisfactory results. The approach described in this contribution is a possible approach, but certainly not a single existing approach. We suppose that the final result of our research and search for a suitable model could be a knowledge-based system that would furnish the user with required information on critical infrastructure security requirements.

This article was written for the project no. VD20062008A04

References

[1] SENOVSKY, P.: *Scale-Free Simulace v1.1* [on-line], WWW <URL: http://homen.vsb.cz/~sen76/programy/cs/scalefree_v110_bin.7z > [cit. 2007-10-3].
[2] SENOVSKY, P.: *Usage of Emergence Effect for Simulation of Network Based Critical Infrastructure,* Proc. of conference Nebezpecni latky, SPBI: Ostrava 2006, 168 - 172, ISBN: 80-86634-91-4.
[3] SENOVSKY, M.; ADAMEC, V.: *Crisis Management Basics (in Czech)*, SPBI Ostrava, 2005, vol. 2, ISBN: 80-86111-95-4.
[4] URBANEK, J.F.: A *Prognosis for the Vulneranility of Cybernetic Items of Critical Infrastructure (in Czech)*, Proc. of 9. conference Soucasnost a budoucnost krizoveho rizeni, Praha, 2006, ISBN 80-239-7296-0, 06K-BE-12, pp. 5.
[5] VALASEK, J.: *Common Steps in the Risk Analysis (in Czech)*, Proc. of 11. conference Riesenie krizovych situacii v specifickom prostredi, Zilinska univerzita, Zilina, 2006, ISBN 80-8070-565-8.

https://doi.org/10.26552/com.C.2008.1.60-63

Libor Stroch *

EXPLOSION PREVENTION IN THE PRESENT CONDITIONS OF PRODUCTION

The article solves some questions of possible approaches to explosion prevention in production plants. In the introductory part it deals with thoughts about the safety of personnel in an industrial plant in areas with an explosion danger. Further, it defines individual views of industrial plants and suggests the means of solving the explosion prevention in industry. In the conclusion it recommends an approach to the described questions and the means of ensuring a systematic development in the field of explosion prevention.

1. Introduction

In each period of time and in different areas of human activities we ask ourselves a question how to further continue in technical, economic and cultural, or in other development of the society. With our own approach to this question we define our personality to the presented questions in the given sphere, and with our reaction to the question "how to continue" we join working groups that strengthen or weaken the development of human activity.

In a given moment the society always finds itself in a stage that corresponds to a certain degree of scientific knowledge and a level of technical support in the given field. By virtue of its legislative frame it forms larger or smaller possibilities for further development of this knowledge, and as such it forms and shifts itself among the technical elite or vice versa. This process, being permanent and unchangeable whether we like it or not, is also demanding, time consuming and tiring. The further development of industrial production is not possible without a continuously new, modern technical support which shifts the human activity onto a continuously higher level of performance, productivity, economics etc.

This trend sharply collides with human nature; person's feelings and needs mostly require satisfaction, security, peace and well-being. The new period of civilized development must bring the harmony between requirements of people and technical development. A systematic development is not possible without a scientific approach completed with manpower and its high qualification supported by a meaningful research activity.

This approach, ensured through an amount of current information on theoretical and practical basis, must be continuously kept and developed. This continuous development of knowledge and development of industrial production is even connected with such fields as occupational safety during the production process in every sphere of economics. Even in such fields as safety, namely industrial safety, the impacts of technical development can be seen. Just as the technologies are permanently being modernized, also the safety systems and equipment work on the principle of a still higher level of automation.

The safety level in the sphere of documentation, training and publication activities also depends on the entire scientific-research work in this sphere.

How to assess the safety level in industry, namely in the specialization of explosion protection, on a higher level from technical, organizational and economic points of view?

One of the views how to achieve this target is to define the ways of achieving the sub-targets and also the targets as a whole.

It is important to realize the successive way of achieving individual results with a precise definition of the final solution.

At the same time, accepting the individually achieved goals as a continuous and never ending creative activity.

This approach can get us to the front position in a certain field in the form of winning the needed information, an amount of credible details concerning the given questions, current state of knowledge, and individual approach of every person in the scientific or research work, increasing the level of technical solution of the questions. Subsequently, through an interconnection of these individual approaches with a group revision and discussion to form the final complete solution from all viewpoints, ensuring a continuous development of the given field.

This approach leads to an implicit viable solution which is essential to be immediately put in praxis for verification and to draw the feedback about its functionality.

* **Libor Stroch**
VVUU, Ostrava – Radvanice, Czech Republic, E-mail: vvuu@vvuu.cz

2. Assessment of industrial plant from the viewpoint of explosion protection

For the sphere of industrial safety with specialization in the explosion prevention the above mentioned can be made concrete into the following recommended working procedure enabling a complex solution.

On the basis of the present knowledge in the field of explosion prevention we can define the subsequent steps leading to ensuring the safety operation.

2.1. Define the industrial plant - technology, production and operational requirements [2]
2.2. Define the matters accompanying the technological process [3, 4]
2.3. Define the working procedures during a production process and risks assessment [9]
2.4. Perform the Explosion Protection Documentation [1]
2.5. Take over impulses from the practical solution for testing and development [5, 6, 7]
2.6. Examine the causes and reasons for new solutions [8]

2.1 Define the industrial plant – technology, production and operational requirements

Production lines and production plants reflect, during their formation, requirements of the manufacturer and they are solved by means of project documentation for the subsequent implementation of a particular plant on a production of the final product. Already in the stage of the project preparation it is necessary to deal with safety questions in the moment when manufactured material is a flammable substance which can form an explosive atmosphere. In such a case it is necessary to consider the explosion prevention. The project organizations must, in accordance with the valid legislation and in cooperation with professional workplaces, define conditions for a safety operation. These conditions refer even to such situations when it comes to changes in technology or its parts, or to changes in the used materials. This activity must be solved through a project change or project modification and the current state must be declared while commissioning.

After this solution we go out from the following initial basis:
- requirements of the technology operator
- technological scheme and production description
- current or created design and technical documentation,
- operational and safety regulation
- detailed data sheets of technology parts
- or data about selected technical parameters.

2.2 Define the matters accompanying the technological process

Materials entering the production process, going through the production process and forming final products including waste material must be subjected to a proper analysis and their fire-technical characteristics must be determined. These characteristics further serve as a basis for determining the outside influences according to ČSN inside and outside the technological devices [3] (being applied in the Czech Republic). For quality assessment of materials accompanying the production it is necessary to work with the safety sheets of the assessed matters. The selected parameters are essential for the performance of explosion measures in particular production conditions.

Among the main parameters belong mainly [2]:
- grain size composition of a substance,
- flash, ignition, or glow temperature,
- lower explosibility limit
- maximum explosion pressure,
- pressure increase rate,
- explosibility constant,
- oxygen content limit,
- minimum initiation energy,
- or other parameters according to a concrete assignment.

These characteristics and explosion parameters of substances are part of the created documentation and are documented by provable protocols about their determination. It is appropriate to determine these parameters on the basis of particular tests on a professional workplace so that the values which are further being worked with would have a credible value and would correspond to the current state in the particular plant.

2.3 Define working procedures during a production process and risks assessment

Definitions of working procedures in production technological sheets or production plans are necessary for the operator for a safe planning of activities of the production, maintenance, possibly repairs. A detailed analysis of individual steps during the starting of technology, the production process itself, technology shut down, maintenance procedure, check, revision or repairs of individual parts or of the whole technology must be properly assessed so that such organizational measures could be taken, or completed with technical solutions so that the enforced technology could be defined as safe. According to the legal regulation the employer is obliged to create conditions for a safe and healthy environment by means of a suitable organization of safety and operational health protection and by means of taking measures for risks prevention. Risks prevention means all measures resulting from legal and other regulations ensuring the safety and operational health protection and with measures taken by an employer aiming at prevention of risks, their removal or at minimizing the incidence of irremovable risks. In the production process, on the basis of the knowledge of concrete conditions, it is the duty of the employer to search for the risks, to investigate their causes and sources, and to take measures for their removal. When applying the principles of risks prevention or for ensuring the explosion protection, the employer takes the technical and organizational measures, in accordance with legal regulations, adequate to the

nature of the plant in accordance with the principles applied according to the type of particular activity, in the following order:
- preventing creation of explosive atmosphere,
- preventing initiation of explosive atmosphere,
- decreasing harmful explosion effects so that health and safety of employees would be ensured

Defining and evaluating particular activities in the production process must always be concrete and it is not possible to generalize them. After taking the technical and organizational measures, at minimum these three activities must follow:
- area classification to areas with explosion danger and to areas without explosion danger,
- indication of places with explosion danger with safety labels,
- creation of a written Explosion Protection Documentation and its administration corresponding to the current situation.

With this approach the operator is able to ensure a workable and safe production process with clearly defined requirements for performing operational activities of individual employees in all production parts.

2.4 Perform the Explosion Protection Documentation

With the knowledge of the previous points it is possible to come to creation of the complete explosion prevention proposal of a given plant and to create an up-to-date Explosion Protection Documentation according to Directive 1999/92/EC of the European Parliament and of the Council on minimum requirements for improving the safety and health protection of workers potentially at risk from explosive atmospheres. [1].

The Explosion Protection Documentation must contain, at minimum, the following parts of a complex assessment:
a) analysis of used substances occurring in the assessed plants,
b) risk analysis of individual assessed plants and devices – technology and device analysis in the period of starting, shut down, normal operation and expected failures,
c) environment proposal – resulting from the risk analysis,
d) defining the concrete initiation sources,
e) proposal on particular technical measures,
f) proposal of particular organizational measures,
g) coordination duties,
h) administration of documentation and indication of dangerous areas,
i) inspection, checks and trainings.

The operator or by the company authorized person must ensure the updating of this documentation in such a way that a continuous objectiveness should be ensured.

For ensuring the objectiveness it is necessary to perform an update always when:
- it comes to a change or modification of technology and to installation of new equipment and components,
- it comes to a change of used or elaborated substances,
- it comes to a change of operational procedures etc.

Each company or its manager as well as Occupational Safety and Health and Fire Prevention workers must process the outputs and conclusions of the Explosion Protection Documentation – technical and organizational measures into internal guidelines, directives, regulations, working procedures, and rules.

The staff of the given plants must be informed about the content of the Explosion Protection Documentation both in a written and oral form. Internal documents must be completed or edited in case of revision of the Explosion Protection Documentation.

2.5 Take over impulses from the practical solution for testing and development

Providing that we want to keep the time with the developing engineering in industrial production it is necessary to assess the setting of particular elements or to evaluate the current ways of explosion prevention. To solve possible shortcomings or requirements of the production process through verification of new parameters, through defining modified constructions or an entirely new conception. These solutions should be subjected to a development process ending in verification tests for the confirmation of hypotheses.

It is appropriate to confront the conclusions, achieved through fulfillment of the above mentioned, with similar activities in the field and to evaluate results of different technical solutions. Thus flexibly react to the market needs and in the given period to ensure a standard technical solution that conforms to all the required parameters.

2.6 Examine the causes and reasons for new solutions

The process running according to the previous points provokes many thoughts and questions. One of them can be the question of safety versus economics, or complication for technological production procedure and vice versa.

Here it is appropriate to subject such questions to a detailed analysis and in cooperation with research and scientific workplaces to search for correct answers. Thus an assignment for a research task of a concrete form can be created and can join together the power of production, construction, projection, development, and research in one unit. At the end of the effort of such group can be, and often is, a new solution or an entirely new product which shifts the safety further again if it ensures all the required conditions for production.

3. Conclusion

Everything already mentioned has been basically known and nothing extra new has been discovered here. This article provides

a simple, comprehensive suggestion how to proceed in a systematic way during a continuous ensuring of explosion prevention in industrial plants. It answers the question how to secure the safety in plants with explosion danger and how to maintain this safety during the whole operating life of production technology. It defines that the aim of a new striving in explosion prevention is not one solution, measure or protection element but a systematic approach to the questions under a continuous development and solution. Thus the goal of our action is a path guiding us through safe technologies while keeping the technical level of solution corresponding to the stage of knowledge in the given field.

Experience shows that my conclusion is not entirely normally used in praxis and in many cases it hardly gets into the common subconscious of the production workers. Though, responses from praxis prove that the topic of safety has become the topic of the day today and it is becoming priority number one. The witness of which is the modified legislative, constantly better approach of the technical public and the awareness of the companies of these questions. With quality control and enforceability of particular requirements from responsible workers and in companies it is possible, in a foreseeable period, to achieve satisfactory results to which conditions have already been created.

References:

[1] Directive 1999/92/EC of the European Parliament and of the Council on minimum requirements for improving the safety and health protection of workers potentially at risk from explosive atmospheres.
[2] European Standard EN 1127-1: *Explosive Atmospheres – Explosion Prevention and Protection – Part 1: Basic Concepts and Methodology.*
[3] ČSN 33 2000-3: *Electrical Regulations – Electrical Apparatus. Part 3: Determination of Basic Characteristics.* (Contains principles of IEC 364-3:1993)
[4] ČSN EN 61241-10: *Electrical apparatus for use in the presence of combustible dust. Part 10: Classification of areas where combustible dusts are or may be present.*
[5] EN 14373: *Explosion suppression systems.*
[6] EN 14491: *Dust explosion venting protective systems.*
[7] EN 13237: *Potentially explosive atmospheres – Terms and definitions for equipment and protective systems intended for use in potentially explosive atmospheres.*
[8] EN 12874: *Flame arresters – Performance requirement, test methods and limits for use.*
[9] EN 1050: *Safety of machinery – Principles for risk assessment.*

https://doi.org/10.26552/com.C.2008.1.64-68

Miroslav Janicek *

REPRESENTATION AND EMBASSY PROTECTION

In this article, on the basis of his theoretical and practical experience, the author tried to outline briefly the main principles and rules of protection of important objects nowadays, when there is higher hazard of possible terrorist attack. His conclusions may significantly stand interested people in these problems from both professional and laical public in good stead, as a basis or „point of bounce".

It can help significantly to specialists from this field.

Introduction

Nowadays, after well-known terrorist attack on New York "Twins" there is a grow of terrorist actions all over the world mainly in connection with joining of Czech republic Army troops in allied fights in Afghanistan and Iraq, technical security and protection of important objects, for example workplace of "Free Europe" in Wenceslas square or particular workplaces of our embassies, mainly in the countries of the "third world", grows with great importance. Therefore it's essential that specialists and professional public as well as firms and ordinary citizens in our country were familiar with the principles for necessary protection and defence of these objects.

1. General principles of object protection

Generally, technical protection can be mainly differentiated into spatial direction (peripheral, facial, spatial and subject protection), the way of handover the warning (the systems with local signalization, the autonomous systems, the systems with distant signalization) and the level of protection of protected object [6]:

1.1 Object hazard levels

- *Level 1 - low hazard* – households, recreational objects
- *Level 2 - low up to middle hazard* – shops with casual stuff (food, stationeries, ironmongeries, drug-stores,...), restaurants, libraries, production objects and halls
- *Level 3 - middle up to high hazard* – shops (electronics, needs for taking pictures, art subjects, antiques, chemicals...), museums, archives, chemists, important information
- *Level 4 - high hazard* – banking and deposit institutions, weapon and ammo shops, narcotic substances, state administration and self-government buildings (courts, police buildings, buildings of army – store rooms of weapons, ammunition, explosives...), government, senate, representation and embassy buildings.

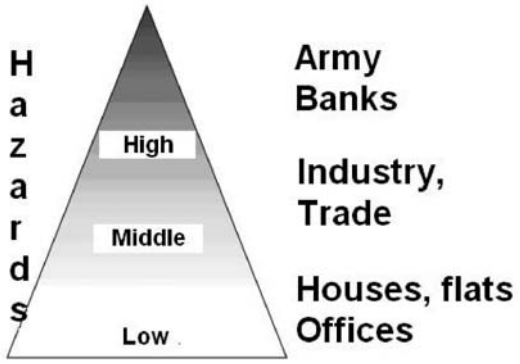


Fig. 1 Illustration of object hazard levels

1.2 Object protection categories

1.2.1 Peripheral protection is determined by the perimeter of the object which mostly makes its cadastral border (fence). Instruments of the peripheral protection signalize the disruption of the object perimeter.

1.2.2 Facial protection is determined by the cover of the object (building). Technical instruments of the facial protection signalize the disruption of the object cover.

1.2.3 Spatial protection is understood as the protection of rooms, hallways and places inside the object. Technical instruments signalize or embarrass the disturbing of this protected place.

1.2.4 Subject protection avoids "attacking" or manipulation with the protected subject. There belong for example strongboxes, strain-gauge or capacity sensors etc.

Systems with local signalization are used in case of low hazard. Attacking the object is signalized by the electronic equipment by

* **Miroslav Janicek**
RVC Institute, Uherske Hradiste, Faculty of Technology, Tomas Bata University, Zlin, Czech Republic, E-mail: janicek@ft.utb.cz

means of siren or light signalization which is placed directly inside the object or its imminent entourage. Autonomous systems have the signalization of electronic equipment loaded to the workplace with a non-stop service, for example to the security service. Then, the on duty worker reacts to the alarm signal either on his own or he calls the support (preferably The Police of the Czech Republic).

In respect of the systems with remote signalization, in principle it concerns telephonic or wireless transmission of alarm signal and alarm evaluation in the place with non-stop service with technical comfort (record of the event ancestry, graphic depiction of attacked object), with the sequence to hitting the group of security agency or to the action of The Police of the Czech Republic.

1.2.5 Physical protection – it concerns the object protection made by the security guards, members of the security service, police, army etc.

1.2.6 Regime protection – it involves administratively-organising disposals that have to focus on reservation of failure-free function of the whole safeguarding system (e. g. personal matters) [6].

1.2.7 Object protection organization ways:

Defence of the important objects is, under ideal conditions, usually organised in four areas. Border of *peripheral protection* is often delimited only with warning signs or another kind of letter of advice. The main sense of these disposals is to warn against the random entry to the protected zone. In some cases, the border of peripheral protection is made of the different mechanical barrier, mostly a fence, mechanical function of which is often supplemented by the technical devices that react to attempts to overcome or damage the fence. The area behind this border is monitored through the medium of different technical devices and sensors, eventually of secret or vice-versa demonstrative lookout. The aim of monitoring is detection of the disturbers and well-timed warning of the security guard. Territory is divided into several zones, where the physical protection operates according to the given system. Members of the guarding are equipped with the weapons and the tools which correspond to the conditions and necessities of their service. Means of *facial protection* are located on the outer walls of each building and in respect of the important buildings they are combined with the systems which monitor the entry. It concerns the components for the case mechanical becoming stronger, supplemented with the electronic components. The case is usually divided into several zones to precisely directed crackdown of the service against the disturber. *Spatial protection* protects individual places (rooms) inside the building. Means of the spatial protection are located only in the rooms where is the danger of attacking the low floors of buildings or in the rooms where the values are put. In this place means from all mentioned groups can be combined. *Subject protection* is concentrated on the only subject (strongbox, work of art). There exists a range of objects where the similar scheme of protection can't be simply used, e. g. in public buildings, banks, state administration buildings etc. In this case the protecting system has to be built according to the requirements (e. g. peripheral protection is cut out) to be fully functional and concurrently to secure the required level of protection. The ability to react effectively to the attack if no warning information preceded, is the important criterion of the object protection functionality. This ability (protection system functionality) can be verified by the model situations which demonstrate the real attack.

1.3 Example of possible security of objects [5]

1.3.1 Example

The security of the object at the fenced land that obviously has the set aside outer border. The object is owned by the Ministry of Foreign Affairs (it's the embassy). This object is the enclave in the foreign country. Under normal conditions it's the object where the public can't enter, on the contrary, the object succumbs to the special operating regime. The employees, who work in the object, have to count mainly on themselves. For those reasons the highest attention must be paid to the security of this object.

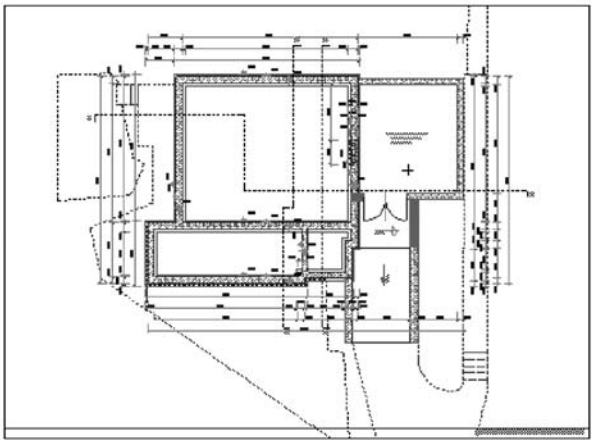


Fig. 2 The plan of object foundation (cellar)

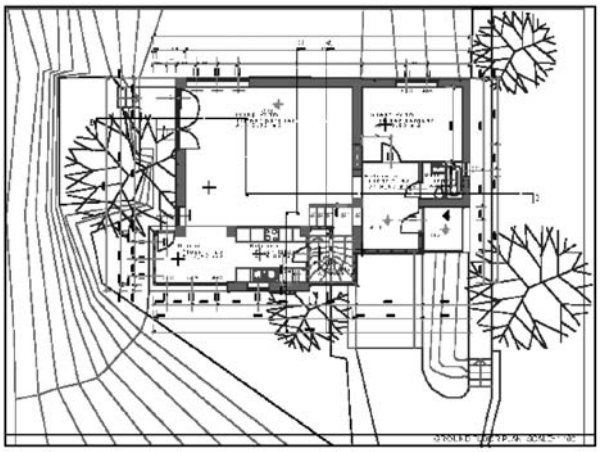


Fig. 3 The plan of object ground floor.

1st step lies in the thoroughgoing study of the real estate plans, with emphasis on land border, location of the building foundation, cellar places and the buried services. Then, all floors of the object must be perused. The same attention (which is paid to the study

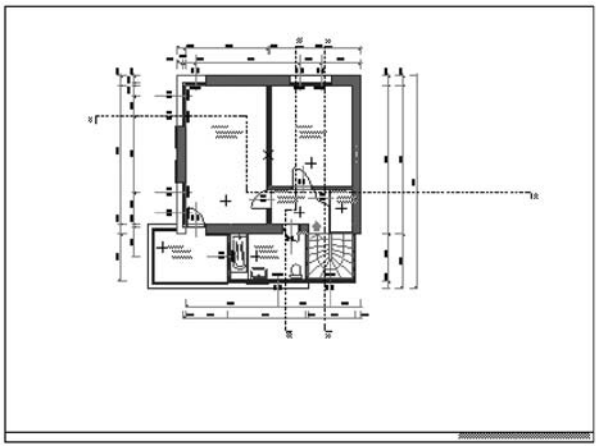


Fig. 4 The plan of object first floor

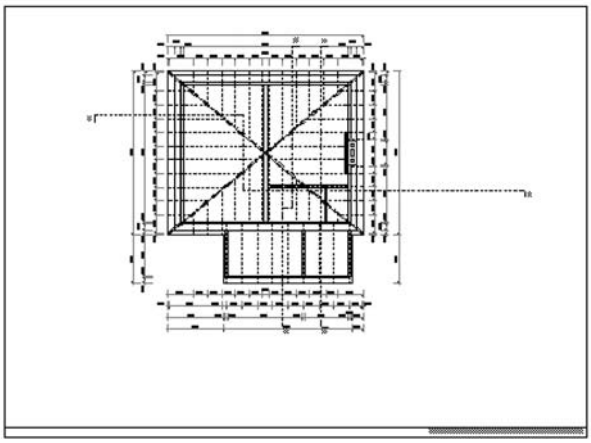


Fig. 5. The plan of object roof I.

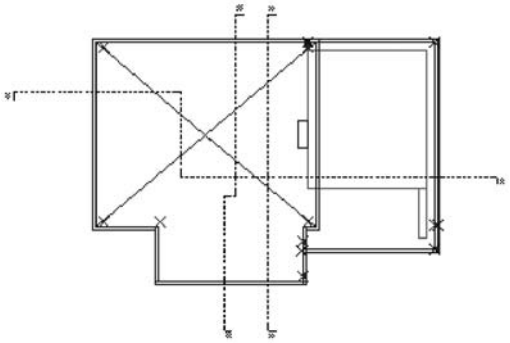


Fig. 6 The plan of object roof II

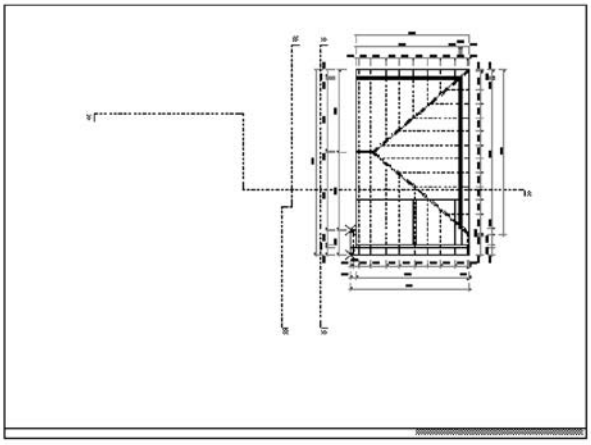


Fig. 7 The plan of object roof III

Fig. 8 View of the object from the north side

Fig. 9 View of the object from the south side

Fig. 10 View of the object from the east side

of the foundation and cellars) must be paid to the roof and attic places. On the basis of the plans it's important to interpret carefully the incorporation of the object into the terrain (unequal terrain, entrances, outdoor swimming pools, growth, neighbouring lands and objects, mainly the buildings overtopping the given object).

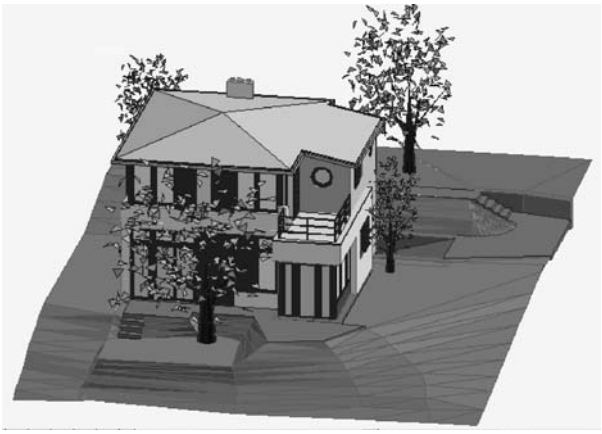


Fig. 11 View of the object from the west side

Fig. 12 View of the object roof

***2nd step** – after careful study of all real estate plans and thoroughgoing incorporation of the object into the terrain, we are able to determine exactly the peripheral, facial and spatial protection. In this step, it's decisive and principal to define mainly the peripheral and facial protection. It's obvious that in case of this object (with respect to its importance) we can't be satisfied only with caution lettering, possibly with the fencing as the mechanical barrier. It's important to gauge which special mechanical means to use for the protection of the object, e. g. special barriers, razor wire etc. Mechanical function of the fencing has to be strengthened by the technical means which will react to each attempt to overcome or damage the fencing. In respect to this object it's very important, within the peripheral and facial protection, to avail maximally the different classic and technical means, including the monitoring with the assistance of cameras, sensors, possibly to use the hidden or vice-versa the demonstrative observing. The aim of these steps has to be the well-timed revelation of disturbers and concurrently the instant warning the security guard. Facial protection will be divided into several zones where the physical guarding will operate according to the given system. All steps have to keep the attacker in certain zone so that the crackdown is efficient. Members of the guarding can be equipped with the weapons and the means which will correspond to the conditions and the necessities of their service.*

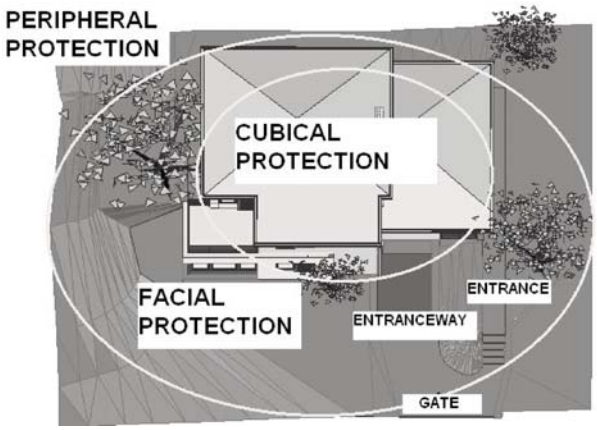


Fig. 13 Specification of the peripheral, facial and spatial protection

***3rd step** lies in the exact definition of spatial protection, it's necessary to determine which places will be protected and how. In this case the means of all mentioned groups, thus classic, technical, physical and regime protection, must be combined. Functionality criterion of protecting this object will be the ability to react effectively to attack of the object. It is therefore necessary to verify the operation of this protection on model situations which malinger the attack. In the case of the embassy or representation, there can be used completely atypical means of protection – sacks with sand, bullet-proof glass, armament store located usually in the object cellar, ciphering apparatus supplemented with self-destruction etc. To demarcate the circumference of spatial protection and determinate the most suitable way of securing, the plans and profile of the object will help us. All critical places come out well just on the profile: stairs, balconies, terraces, doors, windows, garages, cellars, roof, buried services etc.*

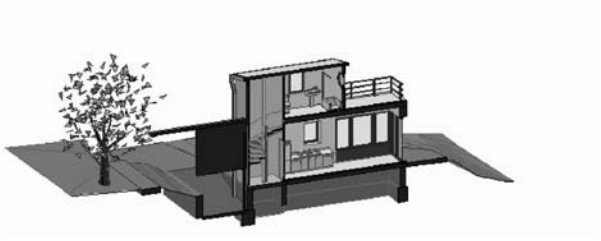


Fig. 14 Object profile

Conclusion:

In my brief article I tried to summarize and outline the most important parts and principles of protection of significant objects, such as "objects important for state protection – OISP" or "objects of possible attack – OPA", so that it could be a reliable guidepost for professional and laical public who prepare security of important objects. This article is neither exhausting nor detailed study, but it's only a survey of both theoretically and practically confirmed basic principles of protection of these objects.

References

[1] BREBERA, S.: *Special technology I. part (in Czech)*, FMVS Prague, Prague 1976
[2] BREBERA, S.: *Special technology II. part (in Czech)*, FMVS Prague, Prague 1976
[3] BRZYBOHATÝ, M.: *Terrorism I. a II. (in Czech)*, Police History, Prague 1999
[4] BRZYBOHATÝ, M.: *Introduction to the problems of terrorism and antiterrorism (in Czech)*, Police Academy Prague, Prague 1995
[5] JANICEK, M., DRAHOVZAL, P.: *Pyrotechnist in combat against terrorism*, DEUS Prague, Prague 2001
[6] KOCABEK, P., KONICEK, T., CERVENA, R.: *Key to Safeness (in Czech)*, MV CR Prague, Prague 2000
[7] KOKTEJL – *geographical magazine (in Czech)*, vol. X., special edition to issue 9, September 2001, Czech press, Usti nad Labem, ISSN 1210-4353
[8] PAVELKA, P.: *Teaching aid for the basic pyrotechnical course (in Czech)*, Protective service of the Czech Republic Police, Prague, 1998
[9] *Zen-2-6/c, Explosives and destructions (in Czech)*, MNO, Prague 1982

https://doi.org/10.26552/com.C.2008.1.69-70

Ales Bernatik – Katerna Sikorova *

CZECH TECHNOLOGY PLATFORM ON INDUSTRIAL SAFETY

At the beginning of June 2007 the Faculty of Safety Engineering founded the Czech Technology Platform on Industrial Safety o.s. (CZ-TPIS). The 1st meeting of the General Assembly launched the activity of this national platform in accordance with the already operating European Technology Platform on Industrial Safety (ETPIS).

Key words: technology platform, industrial safety

1. European Technology Platform on Industrial Safety

In the year 2004 the European Technology Platform on Industrial Safety (ETPIS – Safety for Sustainable European Industry Growth) was founded with a view to bring together professionals concerned with these problems and influence future researches into industrial safety. The Platform is divided into 5 Focus Groups and 4 HUBs (see Fig. 1). The Platform claims 270 professionals from 190 European organizations. The Platform has prepared the Strategic Research Agenda that contains short, medium and long-term objectives and priorities. More information is available at *www.industrialsafety-tp.org*.

At Platform meetings, a requirement for the establishment of industrial safety national platforms, which already operate, for example, in Spain, France, Italy, Poland and other countries, appears. The national platforms are of importance to close liaison with the European Platform in the specification of research topics to be addressed in the future. The Faculty of Safety Engineering of VŠB-Technical University of Ostrava has undertaken the role of

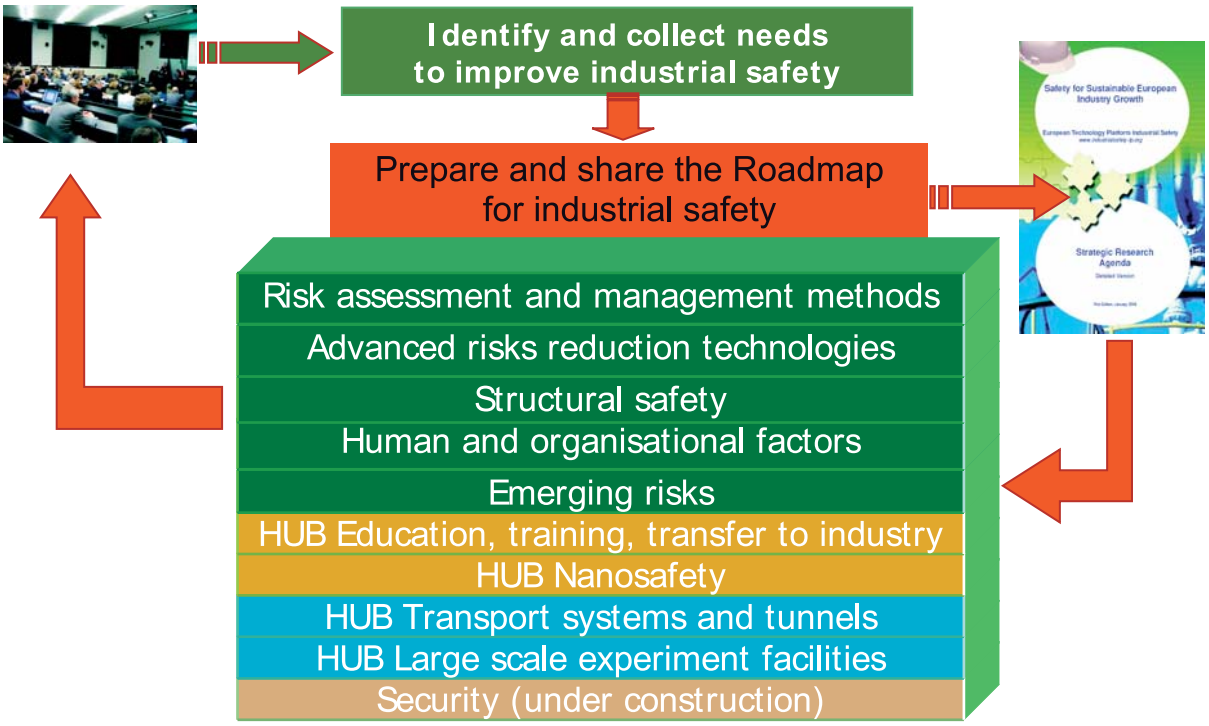


Fig. 1 Operating ETPIS to defragment R&D

* **Ales Bernatik, Katerna Sikorova**
VSB-Technical University of Ostrava, Faculty of Safety Engineering, Ostrava-Vyskovice, Czech Republic, E-mail: ales.bernatik@vsb.cz

co-ordinator for the establishment of the Technological Platform on Industrial Safety in the Czech Republic on the basis of its membership of the European Technology Platform.

2. Czech Technology Platform on Industrial Safety

The Czech Technology Platform on Industrial Safety is a voluntary, independent community bringing its members together on the basis of a common interest. Its mission is to provide support to the organizations that promote development in industrial safety in the Czech Republic, to identify jointly national interests in the area of industrial safety, and to enforce uniformly these interests at the European level. Any physical or legal entity wanting to support the Platform and agreeing with the Statutes of CZ-TPIS can become a member of the Platform.

The Platform is headed by the Executive Board composed of representatives of research and scientific institutions, state authorities and universities, industries and other significant organizations. The Focus Groups led by professionals in the areas concerned, and established to co-ordinate specific priorities, with links to relevant parties interested form the cornerstone. The Executive Board of the Platform, which is an executive board of CZ-TPIS, carries out the administrative control and organization of CZ-TPIS. Its members are elected by the General Assembly from a number of Platform members. The check and audit body of the Platform is the Check Commission. The supreme body of CZ-TPIS is then the General Assembly that is formed by all the members of the Platform (see Fig. 2).

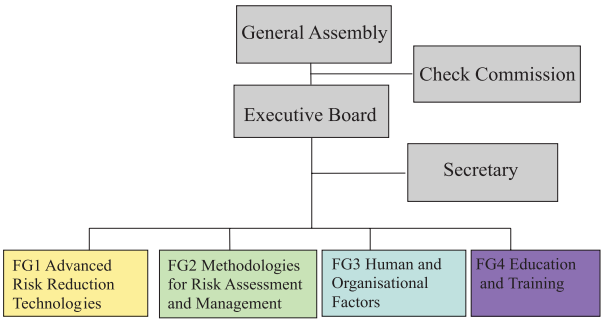


Fig. 2 Organizational structure of CZ-TPIS

3. Conclusion

The objectives of the Czech Technology Platform on Industrial Safety are to incorporate the Czech Republic into the ETPIS main activities, to disseminate acquired knowledge and experience in the Czech industries, and thus to achieve an increase in industrial safety and competitiveness in the Czech Republic. The establishment of CZ-TPIS will thus make it possible to interconnect the interests of industrial enterprises, research and scientific workplaces, universities and others with the interests of state authorities. Another objective of this community being founded is the more intensive participation of Czech partners in projects of the European Union's Seventh Framework Programme and other national and international projects, and in this way to contribute to the solving of issues of industrial safety in the Czech Republic. More information can be found at the web pages of the Platform at www.cztpis.cz.

https://doi.org/10.26552/com.C.2008.1.71-74

Stefan Hittmar *

THE MODEL OF SLOVAK RAILWAY STRATEGY

Rail transport plays a key role in transport services within a domestic and international scope. In the scope of social and economic changes and the dynamically developing transport sector, it is the task of railways to analyse and programmatically prepare its management.

In the context of European and national traffic policy the strategy of Railways of the Slovak Republic (ZSR – Zeleznice Slovenskej republiky) identifies the need for successful technological and company development in the coming decades.

This short paper of ZSR strategy contributes to better knowledge and a positive presentation of the direction of ZSR towards bodies of state administration and partner organizations within a domestic and international scope.

Keywords: Strategic Analysis, mission, vision, SWOT, priorities, main supporting process.

1. Introduction

ZSR were founded on January 1, 1993 by a decision of the Government of the Slovak Republic on establishment of a state company following the split-up of the Czechoslovak Federal Republic and thusthe split-up of the Czech and Slovak State Infrastructure into two independent entities.

As of January 1, 2002 ZSR was further divided into two independent entities according to the ZSR Transformation and Re-organisation Project – into ZSR and Železničná spoločnost, a.s.

ZSR is an infrastructure manager – it provides transport services as well as other related activities in the line with the state transport policy and market demands.

Since January 1, 2002 the main function of ZSR is as follows:
- management and operation of railway infrastructure,
- provision of operation-related services,
- founding and operating of railway, telecommunication and wireless networks,
- construction, regulation and maintenance of railway and funicular infrastructure,
- other business activities as recorded in the Commercial Register.

2. The starting points for strategy

The strategy of ZSR for the following decades is directed at the improvement of business activities, modernization of the traffic control system and infrastructure during the ongoing transformation so that the prescribed goals in the transformation and restructuring project of ZSR can be fulfilled. The objectives of traffic policy of the Slovak Republic for railway traffic have been established until the year 2015.

The traffic policy of the European Union (EU) presented in the White Book and subsequent legislative activities markedly support railway transport. The first aim incorporates the aggregate of targets and supporting measures for the increase of activities of railway companies in today's market conditions. The second labour-law-oriented objective is the relationship between the state and transport companies. Increase in railway traffic safety together with interoperability are the pillars of the integrated European railway system.

The external economic legal environment and internal conditions of ZSR influence the following SWOT analysis:

The SWOT analysis for strategy Tab. 1

Internal conditions	
Strengths:	**Weaknesses:**
The rail system of ZSR forms part of EU development plans and these activities are also included in the financing of EU; part of the network is included into European transport corridors. Railway transport contributes significantly to transport safety and represents the most environmentally friendly transportation.	High indebtedness; low flexibility; falling behind in railroad modernization and low interoperability mainly in railroad interconnection tracks with EU states.
External conditions	
Opportunities:	**Threats:**
The new structure of prices for individual segments; change of organization, management and marketing; expected increase of railway transport capacity influenced by the transport policy of the EU; the access of new foreign investors in the Slovak Republic are expected.	A decrease in the bulk transport of substrates, competition of road transport; competition of neighbouring railway lines and slow progression of ZSR railroad infrastructure.

* **Stefan Hittmar**
Faculty of Management Science and Informatics, University of Zilina, Slovakia, E-mail: hittmar@fria.utc.sk

Strategic vision for ZSR

To transform ZSR on the basis of its mission to be an effective market oriented company, under the conditions of regulated economic competition and European railroad integration with strong orientation to the customer in the given geopolitical area.

Mission of ZSR

To create an integrated offer of railroad infrastructure capacities and services for the transport of persons and goods based on the highest safety and effectiveness, reliability and environmental acceptability.

The main priorities of ZSR as the infrastructure manager include:

- trading activities focused on transport routes trading,
- process of transport organisation and management,
- modernisation of the infrastructure to support the ZSR's commercial orientation and efficiency,
- ongoing transformation of ZSR to a market-oriented entity in the conditions of regulated economic competition.

3. Model of strategy for ZSR

On the basis of being performed an analysis, defining a vision and mission of ZSR the strategy can follow. The basic model of strategy is an alternative which consists of priorities and main support processes, Fig. 1.

Fig.: 1. The basic model of strategy

Priority Nr. 1 – Business activity of ZSR

The offer and sale of ZSR train paths

The offer and sale of ZSR train paths increases the standard of offered services, both on a material and technological base. ZSR will provide high-quality delivery routes and prompt response to market needs. ZSR will build up customer loyalty and an individual attitude to different market segments. Today, total number of customers is 19.

Trade with energies

The reduction of total expenses in the purchase of power-producing media, increased rate of profits from trade with energies by the construction of a business-energy control station of ZSR and the provision of high-quality services for customers in the areas of energy supply.

Property management

An active approach to property handling and working-out of planning process for the prognostication of sale, demand and property leasing.

The offer of telecommunication services

Aimed at individual organisation units is to operate the sales of telecommunication services as an alternative telecommunication operator.

Priority Nr. 2 – Organization and traffic control

Management of transport operation of the ZSR railway system with the assistance of advanced railway technology will enable the application of a new system for dispatcher's control of ZSR transport. The modernisation of railway lines will enable centralisation of the operating staff of railway stations and the railway network, which will lead to the centralisation of dispatcher control at the corresponding corridor resulting in a reduction of mainly operating staff.

ZSR will create technical and organizational conditions for ensuring the customer's requirements in the activities of the infrastructure manager, mainly regarding accuracy and quality. The implementation of the compensative system for caused delays between carriers and the infrastructure management will mainly contribute hereto.

In co-operation with carriers, ZSR will accentuate *passenger transportation* the construction of train diagrams in order to achieve travelling without long latency periods. The publication of different forms of a railway guide will enable the travellers' easy access to information about the necessary train connections.

Within *freight transportation* ZSR will create conditions for a stable GVD (train traffic diagram). In collaboration with carriers and neighbouring countries, idle time at cross-border stations will be reduced.

Activities of train formation (a network of formation yards) will be adapted to the required capacity. ZSR will modernise these formation yards appropriately.

ZSR will monitor the business performances of railway private sidings and evaluate the efficiency of station yards during the modernisation and reconstruction of the railroads.

Priority Nr. 3 – Modernisation of infrastructure to support the business orientation and effectiveness of the company

ZSR must accelerate the modernisation of railways included in the Pan – European railways transport system IV; V; VI; these railroads form part of the TEN transport network. The important Bratislava railway junction within the framework of the Vienna – Bratislava interconnection makes increasing demands on the transport capacity of passenger and freight service.

The new infrastructure has to be utilised so that the provision of infrastructure services will also yield business growth for the company.

Modernisation of the railway transport system for the speed limit 160 km/h and the fulfilment of other parameters in AGC and AGTC agreements arise from the need of ZSR to be internationally accepted.

ZSR will implement:

ERTMS – European Railway Traffic Management System in accordance to the strategic EU/UIC technological projects,
ERTMS – European Railway Traffic Management System,
ETCS – European Train Control System,
GSM-R – Global System Mobil Railway,
GALILEO – ZSR will be connected to the railway satellite system applications after corresponding analyses.

The implementation strategies for these systems will be elaborated according to EU legislation.

Priority Nr. 4 - Continuation of transportation a market-oriented company under the conditions of regulated economic competition and European railway integration

The changeover process of the control system and organization belongs to one of the most important steps on the road to a more effective transport company in the long-term transformation process of ZSR. The definition of two regional directorates for the management of railway transport and the division of infrastructure for railway maintenance will enable a decrease in the number of workers and accurate economical breakdown of railway transport costs.

The legal form of ZSR as a state enterprise remains unchanged in the long-term strategy horizon.

The integration of ZSR into European structures, internationalisation of the railway transport market and creation of a European single railway system requires the membership of ZSR in strategic associations like UIC, CER, OSŽD, G4 – Regional Corporation, RailNetEurope and project ERIM TREND etc.

The implementation of EU legislation (Technical specifications for interoperability) into the system of internal technical norms of ZSR. This process is understood as harmonisation of the legislature of the Slovak Republic in the field of the legal status of ZSR as manager of the railway infrastructure on the level of EU legislature. This means a change in the relationship between the state and ZSR, provision of financial resources and the achievement of financial equilibrium and company stability.

Priority support process Nr.1: **Ensurance of human resources development**

The objective of human resources strategy is preparation for the competitive environment which requires system changes in the organisational processes with the accent on:

= changes in the behaviour of employees,
= changes on the level of work specialisation,
= increase in their professional level,
= increased level of identification with the
= company and with customer oriented policy.

The target groups of human resources strategy:

= managers;
= other employees.

The primary purpose of personnel strategy includes the following areas:

= optimisation of human resources,
= policy for workers who have been released from the company,
= increase in competence and performance of the employees,
= decrease in the average age of employees,
= complex incorporation of knowledge taken from railway psychology into railway development,
= implementation of the latest knowledge and experience taken from modern personnel management; improvement of work and social conditions of ZSR employees,
= establishment of career development system and system of personnel reserves,
= development of internal communication system,
= improvement of managerial skills,
= regulation of relations with trade union central offices,
= preventive health care for selected groups of employees.

Priority support process Nr.2: **Financial ensurance for the realisation of strategic objectives**

The provision of financial resources is the basic condition for the implementation of strategic objectives. The scope of possibilities for procuring financial resources is limited:

= legal status of ZSR and related legislation,
= financial situation of ZSR,
= political decisions of the government for financing ZSR.

Financial ensuring of long-term strategic objectives of ZSR:

= alternative financial model for the attainment of long-lasting economisation of ZSR,
= multi-source financing of long-term strategic projects,
= transformation of financial relations between the state and ZSR in accordance with the acquis communnautaire EU,

= sufficient financial resources needed for the modernisation of railway transport lines and technical equipment for other railway lines.

The financial model developed for strategy purposes analyses several scenarios for the development of ZSR according to different inputs and financial contribution from the state or the need to draw credit.

Priority support process Nr.3: **Rational fulfillment of the consolidating of ZSR**

The success of fulfillment of consolidating function is dependent on the reciprocal relationship between the state represented by Ministry of Finance of SR, Ministry of Transport, Posts and Telecommunications and ŽSR and fulfillment of costs purpose.

Solution of fulfillment the consolidation function of ZSR is based on decree of government. There are annually corrections of control mechanism on base of economic result for sections: economy, employment and social field.

The fulfillment of this objective is closely connected with the continuation of transformation of financial relations between the state and ZSR including the solution of the consolidating function.

The basic prerequisite is high-quality financial management of the company. Its basis was laid by the new organizational structure and within the gradual process of change founded on the basis of a procedure- oriented company.

This process include risks and unresolved problems:

Political risks
- the accomplishment of the ZSR mission and ensuring the fulfillment of strategic objectives is significantly subject to political decisions, concretized by the supportive measures of state administration and legislation.

Economic risks
- risks resulting from the transformational process,
- risks from indeterminateness of macro-economic development of the Slovak Republic,
- risks from liberalisation of the transport market and related branches,
- financial strategy risks (financial and investment risks).

Unresolved problems in the internal organisation of ZSR include
- restructuring of ZSR,
- the management of ZSR in full extent from implementation of strategy to the company, acceptation of strategy as the basis of the company plan, updates on the basis of feedback.

Connected risks of consolidation function of ZSR
- ensuring balanced management,
- establishment of economic qualified costs,
- regulation system of payment for transport path and its impact on ZSR economy results and state budget,
- completion of process capitalizing asset into ZSR basic capital,
- settlement of debts (principal + interest) from credits with state guarantee,
- justifying with property resulting from transformation process of ZSR.

References

[1] Internal sources of General Direction ZSR, Bratislava, 2006, 2007

COMMUNICATIONS – Scientific Letters of the University of Žilina
Writer's Guidelines

1. Submissions for publication must be unpublished and not be a multiple submission.
2. Manuscripts written **in English language** must include **abstract** also written in English. The submission should not exceed **10 pages** with figures and tables (format A4, Times Roman size 12). The **abstract** should not exceed 10 lines.
3. Submissions should be sent: **by e-mail** (as attachment in application MS WORD) to one of the following addresses: *holesa@nic.utc.sk* or *vrablova@nic.utc.sk* or *polednak@fsi.utc.sk* **with a hard copy** (to be assessed by the editorial board) **or on a CD** with a hard copy to the following address: Zilinska univerzita, OVaV, Univerzitná 1, SK-10 26 Zilina, Slovakia.
4. Abbreviations, which are not common, must be used in full when mentioned for the first time.
5. Figures, graphs and diagrams, if not processed by Microsoft WORD, must be sent in electronic form (as GIF, JPG, TIFF, BMP files) or drawn in contrast on white paper, one copy enclosed. Photographs for publication must be either contrastive or on a slide.
6. References are to be marked either in the text or as footnotes numbered respectively. Numbers must be in square brackets. The list of references should follow the paper (according to **ISO 690**).
7. The author's exact **mailing address of the organisation where the author works, full names, e-mail address or fax or telephone number,** must be enclosed.
8. The editorial board will assess the submission in its following session. In the case that the article is accepted for future volumes, the board submits the manuscript to the editors for review and language correction. After reviewing and incorporating the editor's remarks, the final draft (before printing) will be sent to authors for final review and adjustment.
9. The deadlines for submissions are as follows: September 30, December 31, March 31 and June 30.
10. Topics for issues: 3/2008 – Traffic engineering, 4/2008 – Networks for new generations.

COMMUNICATIONS

SCIENTIFIC LETTERS OF THE UNIVERSITY OF ŽILINA
VOLUME 10

Address of the editorial office:
Zilinská univerzita
Office for Science and Research
(OVaV)
Univerzitna 1,
SK 010 26 Zilina
Slovakia
E-mail: komunikacie@nic.utc.sk, polednak@fsi.utc.sk,

Each paper was reviewed by two reviewers.

Journal is excerpted in Compendex

It is published by the University of Zilina in
EDIS - Publishing Institution of Zilina University
Registered No: 1989/98
ISSN 1335-4205

Published quarterly

Single issues of the journal can be found on:
http://www.utc.sk/komunikacie