*Acta Polytechnica CTU Proceedings* **11**:53–62, 2017
doi:10.14311/APP.2017.11.0053

available online at http://ojs.cvut.cz/ojs/index.php/app

# DOMAINS OF RAILWAY TRAFFIC IN THE CZECH REPUBLIC, WHICH NEED THE SAFETY IMPROVEMENT

Dana Procházková*, Jan Procházka, Tomáš Kertis

*Czech Technical University in Prague, Faculty of Transportation Sciences, Praha, Czech Republic*

* corresponding author: prochdana7@seznam.cz

Abstract. The paper analyses the railway accidents sources in the Czech Republic on the basis of knowledge on complex system behaviour. It derives seven categories of sources of railway accidents. The individual categories include the accident sources from the same field domain. These domains are: technical related to rail traffic vehicles; technical related to rail infrastructure and railway station; railway operation control – organizational causes; railway operation control – cyber causes; control of rail traffic vehicles; attack on the train; domain legislative and other. The results show that for railway traffic safety improvement, it is necessary to pay attention to all categories, and especially to these that lead to organizational accidents origination.

Keywords: railway, railway accident, safety, security, criticality, railway accident causes.

## 1. Introduction

Humans need infrastructures for their life quality and development. Especially, at critical conditions the infrastructures' operations support the human survival. The traffic infrastructure in present dynamic age has three basic tasks at critical conditions caused by disasters occurrences, namely to ensure: the human evacuation from afflicted region; the transposition of response units to afflicted region; and interconnections between afflicted region and its vicinity. Therefore, its safety (the set of anthropogenic measures and activities that improve the system security) is the goal of human management and behaviour.

From the general view the railway system plays very important role in terms of transportation in the European area. The transportation mode is widely used not only for middle and long-distances, but it has also very important role in short distances between small agglomerations and for the public transport in cities. Therefore, the safety of railway system has long-term tradition as well as railway operating itself since twenties $19^{th}$ century. It is very followed in the Czech Republic that has very dense railway network with 9458 km of rail track, including 1329 km of rail track for the international transportation within the European railway system.

Although the railway safety has the long tradition, the number of requirements on safety and their depths are increasing because the increase of population density and vulnerability of environ, in which the railway system operates. Especially, in the European railway system the requirements on interoperability are very important [1]. Because the social phenomena based on human intent were found as the significant threat, the security requirements have been step by step introduced into practice.

From the system viewpoint there are other influencing aspects which affect the railway safety, e.g. the interconnection of cyber and physical systems, the human-machine interfaces and overall perceiving and handling with such complex systems, i.e. socio-technological (technical) systems [2]. The practice shows that their violation is often the cause of serious railway accidents, and therefore, we need to protect the railway system against them.

The monitoring of railway system and the critical assessment of previous railway accidents are necessary for understanding the complicated nature of railway system safety, for which reach there are necessary to implement the protective, mitigating, response and renovation measures.

Owing to complex structure of problem, it is also needed to understand the railway system in terms of integral safety that deals with systems of systems (SoS) safety, because we also need to reduce losses caused by the cascades effects or by phenomena that are the consequences of interfaces between systems of completely different nature, i.e. technological, cyber, social, environmental etc.

The results of research described in [3] show the causes of traffic accidents on railway and road that belong to the technical domain and the human factor domain, which is connected with drivers error. The present work is only directed to railway system. Its goal is to obtain the detail findings that can help to improve the safety in the railway traffic, which is the important part of critical infrastructure.

The next given results are based on the concept of integral safety of complex system with type "system of systems (SoS)" [2]. The main target is to reveal real causes of railway accidents. The authors' effort is especially focused on the recognition of risks that are connected with interdependences in the railway traffic system. They are mainly concentrated to those interdependences that are originators of organizing accidents, i.e. accidents caused due to bad human

decision or due to bad human management.

## 2. Risk and Safety

If we want to ensure the safety of any system, we need to determine the sources of losses and damages (generally denoted by term "disasters") and to determine the sizes of their destructive potentials. It means that incident, accident and other similar phenomena are the subcategories of category "disaster" [4]. In the risk engineering we work with three fundamental terms:

- **Danger** marks the conditions of human system at which the origin of harms on protected assets has the high probability; it is almost sure that the harm will origin [5], i.e. the term marks the rate of conditions. It means that it goes on mark of possibility of origin of harm, loss or damage of one or more assets. The danger is predetermined by substance properties that are in facility, object or territory and by properties of processes that are running in facility, object or territory. It is immediate, if the course uncontrollably goes to the disaster origin that causes the emergency situation; and it is creeping, if the course goes to disaster origin inconspicuously and without clear-cut precursors [5]. The danger for human means both, the big phenomena (e.g. natural disasters, industrial accidents, environmental or social disasters) and the seemingly small phenomena from daily life as slump of snow, icicle or roofing from roof, rough pavement etc. [5].
- **Hazard** marks the disaster potential to cause the harms, losses and damages on protected assets in a given site that is prescriptively determined. It goes on prescriptive measure of danger that is connected with the given disaster. For the strategic planning needs, the centennial disaster is often considered, i.e. the hazard is size of disaster that occurs once in hundred years, or professionally exactly, the disaster size that has return period 100 years; at special buildings and facilities it is considered from safety reasons the hazard determined by connected with thousand years' disaster or ten thousand years' disaster [5].
- **Risk** connected with a given disaster is the probable size of damages, harms or losses on protected assets that originate in given place at origin of disaster with size of normatively determined hazard, which is normalized to the certain territory unit or number of individuals and the time unit [5]. The difference between risk and danger is the following: the danger is specific (it denotes the topical conditions) and the risk is only expected opportunity. The humans ensure the protection of human society and populated territory against risks by the way that for each disaster they determine the certain size (so called design disaster). They only perform the preventive measures so the possible risk size may be acceptable. The problem arises if disasters with size greater than design disaster occur, because great damages, harms and losses origin as the consequence of failure of man-made technological systems [2, 5–7].

From the practical reasons it is necessary to consider that the entity risk connected with the given disaster does not represent only the direct losses on assets but also the indirect ones; the indirect losses are caused by: delays or errors in response, cascades of failures caused by synergic and cumulative effects, which are caused by linkages and couplings among the assets; and by domino effects.

Due to the entity structure its risk is the integral risk that is expressed by following formula

$$R(H) = \Big[ \sum_{i=1}^{n} A_i(H) Z_i(H) + \sum_{i=1}^{n} \int_0^T \int F(H, A_i, P_i, O, t) dS dt \Big] * \tau^{-1}$$

where: $H$ is the hazard connected with the considered disaster; $A_i$ are the values of assets, $i = 1, 2, ..., n$ that are considered in connection with complex technological facility safety, where $n$ is the number of monitored assets; $Z_i$ are the vulnerabilities of assets taken under account, $i = 1, 2, ..., n$; $F$ is the loss function; $P_i$ is the occurrence probability of $i$-th asset damage – conditional probability; $O$ is the vulnerability of safeguard measures; $S$ is the size of followed territory/facility; $t$ is the time that is measured from the origin of harmful phenomenon in facility; $T$ is the time for which losses arise; and $\tau$ is the return period for the given disaster [2].

Because the loss function $F$ form is not known, we use for determination of total risk (i.e. the integral risk) the scheme given in Figure 1 [2].

The problem is complicated by reality that the world is in dynamic development, i.e. both, the entity conditions and the risk sources are changing in time. Moreover, there is necessary to respect that the ***risk and safety are not complementary quantities*** – it holds that the risk reduction leads to safety increase but at the same risk value the safety can increase if humans perform special measures or at their behaviour use special manners following from correct safety culture [2].

Therefore, at solution of practical tasks connected with both, the entity safety and the entity risk, ***it is necessary to consider that risks are normal and for the entity safety it is necessary to apply*** not only the risk prevention measures and activities determined on the basis of correct intent and correct data and methods, but also: the safety culture by which the human behaviour in the entity and its vicinity is targeted to safety; and the tools that reduced losses and damages if some important disasters occur. Therefore, it is necessary to prepare the qualified response for important risks realizations, such as: the risk management plans for both, the entity and the entity vicinity for all relevant risks; the continuity

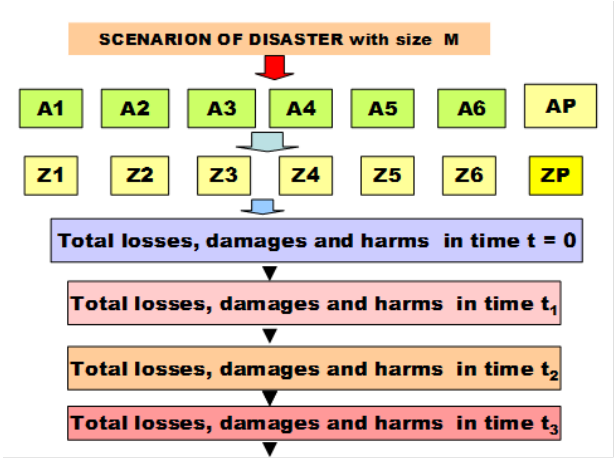


FIGURE 1. Flowchart for determining the risks for the strategic management of safety; $A$ – assets and $Z$ losses, damages and harms to the assets; Description: 1 – the human lives and health, 2 – human security, 3 – property, 4 – the public welfare, 5 – the environment, 6 – infrastructures and technologies, $P$ – private.

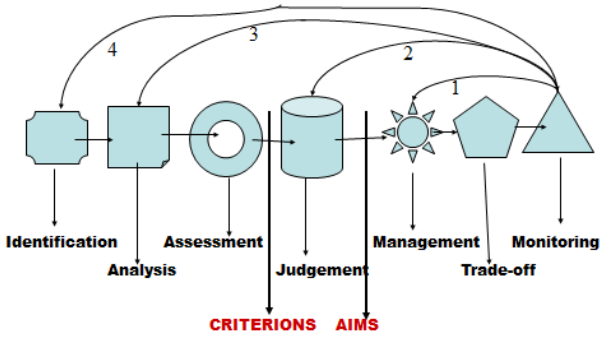


FIGURE 2. Process model of work with risks targeted to safe entity.

plans for survive of important complex technological objects and facilities; and the operational crisis plans for both, the complex technological objects and facilities and their vicinities.

According to knowledge concentrated in [2], the risk engineering uses the following principles:

- the risk is followed and considered during the given system whole life cycle, i.e. at sitting, designing, building, operation and putting out of operation, and eventually at territory bringing in original condition,
- the risk determination is directed to user's demands and to the level of provided services,
- the risk is determined according to the criticality of impacts on facility processes, provided services and on assets that are determined by public interest,
- the unacceptable risks are mitigated by tools according to technical and organisational proposals, by standardisation of operating procedures or by automatable check-up.

The advanced risk engineering directed to human system safety respects the co-existence of systems with different nature (SoS), and so fulfils present demands of humans [6]. To prepare groundwork it is necessary to combine analytical methods with expert judgement by which we remove vagueness in data. The problems that we need to solve in this consequence consist in acquisition of knowledge and in assignment "who is expert"; the last mentioned problem was broadly discussed in world conference ESREL2011 [8]. For the first problem solution we need systematically to monitor the human system and obtained data to process by qualified methods [9].

The process model for work with risks is shown in Figure 2 [5]. The criterions determine the conditions at which the risk is acceptable, conditionally acceptable or unacceptable. The aims in real case are selected from further given possibilities: to reduce risk to certain level; to secure the system, i.e. to ensure its security; to ensure safe system, i.e. to ensure security for system and its vicinity. The feedbacks are used in case if the monitoring shows that the risk is unacceptable; firstly, it is used the cheapest feedback 1; in case of its failure the feedback 2 etc.; at huge harms immediately it is used the feedback 4 that means the change of concept of work with risks.

## 3. Criticality and safety management

In followed context **the criticality** is directed to failures and hazards [10]. The infrastructure criticality needs to be determined on the basis of analysis of relevant and dangerous incidents and failures, losses and damages caused by functionality loss, outer disasters, mitigation measures, reactions and substances in a given facility, releases, leakages or discharges of substances (products' pipelines) etc. The criticality determines the condition at which the system does not ensure expected functions in a required time, a site and in a required quality. To criticality of each partial infrastructure we can approach from two viewpoints, teleological and systemic [8]. From the teleological viewpoint it follows that the criticality is a result of role and function of partial infrastructure in the society. This concept enables to work with non-network and non-technical objects and processes. Partial infrastructure criticality from the systemic viewpoint is a result of its position in the system or of its link to another partial infrastructure. **From both approaches it follows that the partial infrastructure criticality also influences the system that is a social partial infrastructure created by public administration, business subjects, educational and research institutions and civic clubs.**

Adopting the findings from the systems system safety management [10] the set of partial infrastructures in a region is critical one, if it is only capable to ensure activities at which there is only ensured human surviving in a given region. For this purpose, there have been in the world performed the analyses of sectors to which individual partial infrastructure belong and they have been followed the dependences among sectors, and the safety management then respect both, the conditions for functionality of individual partial infrastructures and the conditions for functionality of set of infrastructures; aggregated (critical) infrastructure. The term "criticality" was firstly used in a connection with the nuclear reaction where it denoted the threshold after which the spontaneous chain reaction followed. In connection with partial infrastructures and with critical infrastructure (set of infrastructures), the criticality is the most competently expressed by phrases:

(1.) Criticality is a relative measure of impacts of frequently occurred defects and failures.

(2.) Criticality is expressed by conditions that describe a transition between quality differ conditions.

(3.) Criticality is a condition of extensive urgency.

From the given criticality definitions, it is possible to derive that the criticality is a threshold value that may be designed and that can relate to event, process/function parameter, type of defects and resistance.

The determination of criticality is consistently related to a size of impacts caused by loss of functionality of each infrastructure on the society [10]. From this reason, at the criticality determination, it is necessary to consider:

(1.) Concentration of humans and assets (especially protected ones).

(2.) Sectors of economy (sector analysis).

(3.) Types of mutual dependences among the partial infrastructures/sectors:

  (a) On which item the assets of given sector are dependent?

  (b) What is the mutual dependence of assets among sectors?

(4.) Types of services for public:

  (a) How long has been taken the renovation of services furnishing?

  (b) Which compensations/substitutes can be accessible and available?

(5.) Public confidence in the public administration institutions:

  (a) Can defect of assets/public services result in a fall of moral of citizens, a loss of national prestige, panic, rebellion or civic disorders?

  (b) Can defect of assets induce some impacts/changes in the environment?

The determination of criticality in service of territory goes from the hazard assessment for disasters possible in a given region, considering the vulnerability of partial infrastructures in a given region, the mutual interconnections of partial infrastructures in a given region, i.e. theoretically the same principle as in analysis and assessment of risks in a region, at which several protected interests is considered. Therefore, the criticality determination process is the following:

(1.) Characteristics of assets (there are considered physical, cyber and human assets).

(2.) Determination of criticality (hazard analysis and consideration of assets vulnerabilities in a given site).

(3.) Assessment of impacts on assets (concentration of humans and assets, economic impacts, mutual dependences, reliability).

(4.) Assessment of consequences of losses, victims, damages and harms of assets.

(5.) Determination of priorities according to the given rules.

(6.) The criticality is mostly determined by scoring, i.e. by decision making matrix.

The criticality matrix of infrastructure shows scaling the infrastructure vulnerability vs. infrastructure importance (i.e. its damage causes the infrastructure failure). For safe infrastructure operation there are used the tools: for middle criticality assets the continual monitoring and risk management plans for important risks; and for high criticality assets the operational crisis plans and continuity plans [2].

It is true that above described procedure shows that assessment of infrastructure/technology/set of infrastructures according to two criteria, namely measure of vulnerability and measure of importance of service in a region is not a result of objective computation of process analysis but rather result of subjective estimations, that is only tolerable in case of determination of basic frame. More complex it is the determination of criticality for some process.

At scoring the vulnerability and importance of service it is necessary according to [2] to consider following items: duration of renovation of infrastructures and technologies; impact of failure of infrastructures and technologies on human lives and security; caused detriment, harms and loses; impacts on environment; and induced adverse situation.

In the frame of ensuring the human system security and sustainable development it is necessary permanently to perform the measures that reduce an infrastructure criticality in a region. By building the new infrastructure it is necessary to ensure suitable number and regional distribution of objects of important infrastructure that are sufficiently resistant to expected disasters in a given region, and by that systematically to reduce infrastructure criticality.

Expenses for critical infrastructure are not only costs for its design and building but they also include costs for its operation, maintenance, repair and modernisation. Therefore, the risks connected with each infrastructure must also include the risks from just given domains and the region management must know how to deal with them. It is necessary to assess the risks from disasters that can be denoted as financial market failure because with them it is connected failure of finances for maintenance, operation, repair and modernisation of objects of critical infrastructure. It is caused by the fact that infrastructure criticality increases if not good maintenance and good repair are performed (which cause the vulnerability increases).

Because nothing is out of defects, it must be prepared the plan for renovation of each infrastructure, namely critical one. This plan needs to be proactive, properly assessed; it needs to contain transparently managed risks and answers to questions as:

(1.) What to do?

(2.) How to do?

(3.) In which time interval?

(4.) Do not risks for other protected interests in crease?

etc.

**Risk reduction in the context of safety management covers several topics**: safety of processes; the protection of workers' health and safety (safety of work); and reducing the impacts on the environment. Therefore, in practice, it was introduced that the analysis of the impacts of management on the safety of the facility shall be carried out according to the Reason model of organizational accident [11]. The causes of organizational accidents are in three basic aspects: organizational processes; the conditions which cause the origin of errors or infringements of rules; and no solved problems, which permit the errors and/or violation of regulations.

Safety management is increasingly focused on resilience due to increasing complexities and connectivity of real technological facilities. This is based on the concept that it is increasingly difficult to identify all the hazards and unwanted accidents, and therefore, to avert and reduce the consequences of various disorders it is important the resilience. Investigation of failures and accidents of complex technological systems indicate that these are often caused by a combination of several improbable accidents and the capability of their predictions means to avoid combinations that have the potential to cause accidents, accompanied by large losses, which should enhance the safety. The procedures and tools are described in [2].

## 4. Data on railway system criticality and accidents

The railway system including the trans-European transport network corridors and also the local specific rails creates the complex transportation infrastructure. In many cases it goes on the critical infrastructure, because the railway system ensures the state basic functions for human survival in the territory, state and may be also on the continent level at critical conditions. The elements of critical infrastructure, therefore, need the special attention, study and approaches for increasing their resilience, i.e. it is necessary to ensure their robustness, durability and adaptability with regard to the origin of non-acceptable events. In other words, it means to secure the systems under consideration in which the individual elements are located.

Individual elements shall also to have inherent safety so that they and their surrounding (i.e. public assets in their vicinity) might not be endangered by their imperfection and failure. Certain level of safety shall be also provided the less important local elements of systems with less importance, the location and nature of which can cause at their failure the significant problems to the whole system, and at huge failures they could cause the losses on public assets (including the human lives and health) in immediate or far off surrounding [9]. By introducing the new technologies which are not well verified in practice, and by increasing the system interdependences caused by interface of cyber, material, energetic, economic, social etc. technologies, the systems are becoming more complex. It is the fact that the complexity influences the system safety, because it leads to increasing number of possible systems' conditions, and also to the origin of non-assessable emergent phenomena, i.e. phenomena which occur at certain conditions suddenly and unpredictably [2].

In work [12] the criticality rates for individual types of transportation infrastructure in the Czech Republic were judged by experts from the areas: transportation; transportation management in the territory; supply chains; public administration; and the Integrated Rescue System. The experts assessed 14 factors and the result was determined by using the Multi-attribute Utility Theory. The result showed that the rail transport has very high criticality rate. Regarding to just describe research results, it is necessary to trade-off with risks very carefully and to use the advanced tools of risk engineering.

For investigation of railway accidents, two databases were compiled [13]. The first one was created for the whole world by help of internet [14] with using the passwords "rail disasters", "railway disasters", "rail accidents" and "railway accidents", especially from the sources [15–18]. The second one was created on the basis of national data that are given in the database of The Rail Safety Inspection from the period 2006 up to 2015 [19]; it contains 204 special reports on railway accidents in the Czech Republic and in some reports the description of similar accidents that happen in another sites since 2006 and were not often the object of investigation of inspection.

## 5. Methods used at data processing

The data on railway traffic accidents in database [13] are judged in the context of integral safety of railway system, i.e. not only from the viewpoint of railway system, but from the human security and development. The data are processed by current statistic methods and by special risk engineering procedures as the CBA, separation of accidents into seven accident sources' categories, determination of logic interconnections among the accident sources and their expression by fish-bone diagram [20].

## 6. Items important for safety improvement of railway traffic in the Czech Republic

Data summarizes in [13] show that the railway accidents have been reported since 1650. The first described accident originated in Whickham, County Durham, UK - two boys die when they are run down by a wagon on a wooden coal tramway. The continuous reports are after the accident in Philadelphia, County Durham, UK on July 15, 1815 that was described by words - thirteen or sixteen people, mainly spectators, are killed and 40 are injured by the boiler explosion of the experimental locomotive.

Comparison of data in [13] shows that the worst train disaster in the rail history was caused by tsunami on Sri Lanka at December 26, 2004 – the death of over 1700 people. From the same source it follows that the railway accidents often occur in India; the biggest accident was in the State of Bihar in June 6, 1981, it died more than 800 people when passenger train derailed when it had crossing the bridge over the Bagmati River.

The huge consequences have the railway accidents of freight trains shipping the hazardous substances. The huge railway accidents with presence of hazardous substances was on the January 6, 2005 in the US, Graniteville, South Carolina at which 9 people died, more than 250 people were injured when the freight train collided head-on with a parked local freight train near the Avondale Mills plant in Graniteville. 16 wagons (including a tank car that ruptured 90 tons of chlorine gas into the air) derailed in the accident. The US NTSB determined that the cause of the accident was the failure of the local freight's crew members to realign the switch for mainline operations.

Very great accident of freight train was on the July 6, 2013 in Lac-MÃĭganic, Quebec, Canada (Figure 3). The freight train containing 72 tank cars of crude oil runs away unattended and derails. Several wagons explode, destroying over 30 buildings in the town's centre, roughly half of the downtown area, and requiring the demolition of all but three of the remainder of the buildings in the downtown area due to contamination by petroleum from the train; these combine to require the evacuation of 2,000 people, a third of the town's population. 42 are confirmed killed, along with 5 missing and presumed dead, making this the fourth-deadliest rail accident in Canadian history.

Figure 3. Consequences of freight train accident in Lac-Méganic, Quebec, Canada on July 6, 2013 [19].

The results of detail study of railway accidents with presence of hazardous substances are in [3]. The analysis of consequences of railway accidents in the Czech Republic given in [13] shows that there is only considered the direct loses on humans and rail traffic components. To the accidents' costs there are not included the costs on responses performed by the Integrated Response System, the costs on renovation and the costs for alternative traffic serviceability.

The sites of rail accidents in the Czech Republic in the period 2006 up to 2015 are shown in Figure 4. From this figure it follows that rail accidents occur on all railways; mostly on the railways with high frequency shipping. The main causes of accidents and near-misses in the Czech Republic supplemented by the accident causes from the world that are possible in our country due to present situation (e.g. cyber-attacks) were revealed in domains [21]:

- technical – related to rail traffic vehicles,
- technical – related to rail infrastructure and railway station,
- railway operation control – organizational causes,
- railway operation control – cyber causes,
- control of rail traffic vehicles,
- attack on the train,
- legislative and other.

Founded technical causes related to rail vehicles (as locomotive, coach, car, wagon, freight car) are the following:

- errors in design or at construction of traffic vehicle (wrong wagon or locomotive construction from the stability viewpoint, inappropriate location of fuel tank or power conductor at a terminal block in the locomotive – possibility of short circuit etc.),
- wrong maintenance of locomotive or wagons,

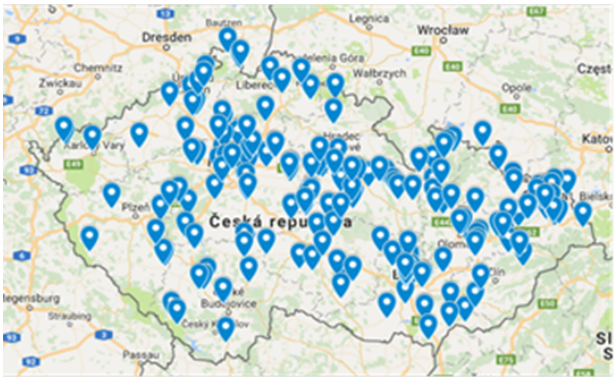


FIGURE 4. Places of railway incidents in the Czech Republic.

- wrongly performed technical overhaul of traffic vehicle,
- wrongly performed the repair of rail traffic vehicle (e.g. brake systems, mechanical parts of brake systems, mainly in the case of car hand brake),
- wrongly loaded wagons,
- wrongly closed wagon doors,
- sudden technical fault of locomotive or some of wagons (damage of axle bearing, engine broken, traction interruption, direction controller out of operation, or failure of another crucial device, outage of air-conditioning etc.),
- fuel shortages or power outage,
- failure of technical equipment of locomotive control system (broking the speedometer, outage of radio connection with control centre (dispatching) etc.),
- malfunction of redundant system when it is needed.

Founded technical causes related to rail infrastructure and railway station are the following:

- siting the railroad in the territory (steeper gradient, insufficient load capacity of rail track foundation, sharp rail swerve, a lot of unprotected crossings with roads or field roads, tall and lush vegetation caused the decrease of visibility etc.),
- construction errors at the railway station design and building (too short operating space, sitting the rails in the direction in which the tall buildings are, which decreases the view of engine-driver and switchmen (shunter operator) in the case of change of position of rail vehicle, headwind etc.),
- rail track condition (error in construction, disorder in the railway station area, wrong maintenance – ruggedness, ice, snow, rail track drift, cracked rail switch, unanchored rail track to sleepers etc.),
- missing the periodic overhauls of rail tracks,
- wrongly performed technical overhaul of rail tracks (no detection of cracked rail switch),
- failure of early repair execution of identified relevant faults on the rail track or on signalling equipment,
- missing the signalling equipment or it has insufficient power,
- sudden technical failure of operation control devices (insufficient maintenance, fault or failure of technical equipment of control system in operation control centre, etc.),
- equipment layout for service of rail vehicles (refuelling, loading and unloading of goods, entrance and exit of passengers etc.),
- physical damaging the railway station or rail tracks (war, robbery attack, terrorist attack, vandalisms etc.),
- siting the train to the wrong rail,
- obstacles on the rail tracks,
- insufficient radio equipment of railway station,
- deficit of knowledge and experience of railway station service (e.g. worker who operates the movement of rail vehicles on rail tracks in railway area etc.),
- out of function of warning system at railway station signalling the minimal safe distance between two trains that are on one rail track.

Founded causes related to railway operation control the – organizational causes are the following:

- wrong setting up the train route,
- failure of start-up of operation of crossbars, lights or sound signals before train arrival to crossing the rail tracks with road or field road,
- keeping the obstacles on the rail tracks,
- insufficient identification of rail track,
- insufficient identification of crossing the rail track with road or field road,
- guiding the train approaching to railway station on the incorrect rail track (train collisions, derailment etc.),
- bad decision of train dispatcher (wrong evaluation of report from police and stopping the train operation at another rail track than at this on which the obstacles were occurred,
- non-passing the information on fire to the engine-drivers of relevant trains,
- wrong consideration of meteorological conditions (wrong information to engine-driver),
- dispatching the wrong instructions to trains owing to the control system failure in dispatcher workplace (e.g. as a consequence of electricity outage, the PC outage etc.),
- dispatching the wrong instructions to trains owing to the dispatcher (controller) error or ignorance,
- chaos at operation control/dispatcher workplace/room (wrong information to engine-drivers, information delay etc.),

- deficiency in railway station staff (train collisions etc.),
- wrong maintenance or wrong platform lighting,
- wrong communication between train dispatchers at setting up the train routes,
- insecurity of movement of shunted vehicle,
- shunters are not furnished by a red signal lighting,
- insufficient training the shunters,
- insecurity of control at crossing the rail track with road or field road at train shunting,
- error of railway station staff (at train guidance, cleaning the railway station and rail tracks, rail station and rail tracks maintenance etc.),
- wrong communication between the operation control centre and companies which repair the rail tracks,
- wrongly distributed responsibilities at the operation control centre,
- insufficient communication among the engine-drivers in service area,
- insufficient knowledge and experiences of staff in the operation control centre,
- absence of instructions for support to engine-drivers who occur in unexpected emergency up to critical conditions.

Founded causes related to railway operation control – cyber causes are the following:

- distortion of data from monitoring – the operation data acquisition system (false information to the engine-drivers and from engine-drivers, chaos at operation control centre etc.),
- false software (it does not consider all possible variants of possible operational conditions, from which it follows the false instructions to engine-drivers and other staff),
- insufficient hardware (wrong data processing and evaluation, dispatching the false instruction to engine-drivers in operation owing to PC failure, delay of reports etc.),
- hacking attack to control centre of dispatch workplace.

Founded causes related to control of rail traffic vehicles are the following:

- error of engine-driver at train control – e.g. forbiddance of train drive behind the semaphore with signal forbidding the train drive (e.g. signal at danger), non-keeping the view conditions at bad visibility (owing to health conditions, tiredness, stress, wrong information from the rail operation control centre, failure of critical equipment of locomotive or other vehicle due to wrong maintenance, incorrect evaluation of situation as reduced speed signalling owing to effort to correct the disharmony with the time table, bump to obstacle on the rail track, turn off the functional device instead of faulty one – exit and entrance to the station, derailment, non-use of wedge at train stop at train shunting etc.),
- engine-driver fault at assessment of meteorological conditions (hoar, snow drifts, obstacles on the rail track etc.),
- engine-river fault at unexpected conditions occurrence (owing to insufficient preparation for coping with emergency conditions – storm, reduced visibility etc.),
- engine-drive fault at locomotive preparation for drive (bad instruction studying before the drive – e. g. regarding to freight, wrong setting the speedometer, false adjusted input data for the drive, e. g. at expensive goods shipping etc.),
- engine-driver fault at radio control,
- wrong co-operation of engine-driver, conductor and other train staff,
- fault of engine-driver at reporting (using the false train code – short distance between trains),
- fire or smoke in locomotive, passenger cars, in cargo wagons, or the engine fire,
- bad intent of engine-driver (change of speed, non-responding to instructions from the control – dispatcher – centre or from surrounding trains, etc.),
- engine-driver ignorance of procedures of train control (at unexpected emergency up to critical situations – e.g. obstacle on the rail track etc.).

Founded attacks on the train are the following:

- rocket/missile from another train or buildings lying outside the track (throwing the stones and other heavy objects from the bridge above the rail track on the train etc.)
- intent damage of rail track or track foundation,
- illegal act in the train,
- bad dispatcher intent,
- bad intent of railway station service staff (worker guiding the movement of train at the railway station),
- train collision with aircraft or another flying object.

Founded legislative and other causes are the following:

- lack of regulations which prevent the wrong track setting at railway station,
- missing the precise instructions for performance of maintenance of train body, rail tracks, track foundation and rail track vicinity,
- missing the texts of intelligible and precise instructions for communication between engine-driver and control operation centre,
- the absence of a uniform system of marking the railway crossings with roads and field roads serving

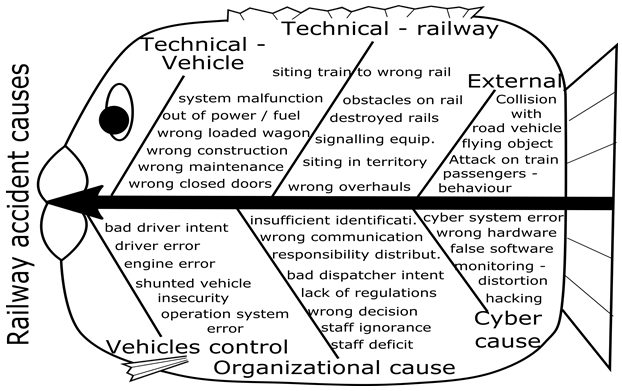


FIGURE 5. Causes of railway accidents in the Czech Republic.

to their identification from the viewpoint of rail and road topologies, enabling the direct designation and informing,

- inappropriate behaviour of passengers at boarding, train drive or exit from train (non-observing the instructions, indiscipline, poor care on children behaviour at the train),
- soggy or else damaged rail track foundation,
- behaviour of road vehicle drivers on the road and rail level crossing (non-respecting the traffic symbols, sound signals or obstructions).

The fish-bone diagram showing the main categories of railway accident causes is shown in Figure 5. It only contains six main categories of causes. The diagram helps the specialists and the paper readers to in-depth insight into the problem of railway accidents. We see the causes arranged according to affinity, which enables to look up the possible actions, i.e. the measures for railway system safety improvement, for the whole groups of accident causes.

Because some accident causes repeat, it is necessary to prepare quality technical and organisational measures. Sometimes, the relative simple measures can avert the accidents; the examples belonging to this category are for example the following:

- the many railway accidents are on the crossing the rail track with road or field road where safety is only ensured by the symbol on the road "cautionary cross",
- the huge material losses are at accidents of freight trains with expensive goods or with hazardous substances,
- all rail track crossings with field routes are not denoted by warning symbols,
- rail track crossings with routes are not clearly identified,
- many works do not respect simple rule "the responsible person for order is the person who gives it, and the responsible person for order implementation is the person, who has to carry out it".

Therefore, it is necessary to pay attention to freight trains, the check-up from the side of rail workers at train loading seems very necessary – for this purpose the special check lists are necessary to prepare. For communication at critical situations it is necessary to prepare the texts of reports that are clear, concise and comprehensible. There are necessary rules for maintenance, regular technical overhauls of rail tracks etc.

Generally, it is necessary to take into account that accidents can occur and for these cases to prepare both, the train personnel, especially the engine-drivers and the railway stations personal, especially those who set up the train rotes.

Because each train accident means the reduction of traffic service and also costs for responses that are performed by the Integrated Rescue System that is paid from the public sources, the state administration needs to prepare legislative for improvement the safety in rail sector.

## 7. Conclusion

The railway accidents in the Czech Republic were divided into seven categories according to the accident sources. Individual categories have the same domain of accident sources – technical – related to rail traffic vehicles; technical – related to rail infrastructure and railway station; railway operation control – organizational causes; railway operation control – cyber causes; control of rail traffic vehicles; attack on the train; legislative and other. For railway traffic safety improvement, it is necessary to pay attention to all categories and especially to this that lead to organizational accidents.

The critical analysis of railway accidents revealed that some of accident causes often repeat, e.g. the insufficient maintenance, low-class overhauls and renovation. They have immediate cause that is not the root cause of such accident type; the root cause is in poor safety culture in the sector and in deficits in training.

Our research will continue in preparation of real tools for individual sectors of followed domain such as check lists, risk management plans and operational crisis plans for great railway stations, especially those in which the hazardous substances in great amount are present.

### Acknowledgements

Authors thanks to Czech Technical University in Prague for support (grant SGS2015-17).

### References

[1] EU. *Directive 2004/49/EC of the European Parliament and of the Council of 29 April 2004 on safety on the Community's railways and amending Council Directive 95/18/EC on the licensing of railway undertakings and Directive 2001/14/EC on the allocation of railway infrastructure capacity and the*

*levying of charges for the use of railway infrastructure and safety certification (Railway Safety Directive).*

[2] D.Procházková. *Safety of complex technological facilities.* Saarbruecken: Lambert Academic Publishing, 2015. ISBN: 978-3-659-74632-1.

[3] D. Procházková, J.Procházka, H.Patáková, et al. *Kritické vyhodnocení přepravy nebezpečných látek po pozemních komunikacích v ČR.* ČVUT v Praze, 2014. ISBN 978-80-01-05599-1.

[4] G.Giannopoulos, R.Filippini, M. Schimmer. *Risk assessment methodologies for critical infrastructure protection. Part I: A state of the art.* European Commission, Joint Research Centre, Institute for the Protection and Security of the Citizen, EUR 25286 EN. Luxembourg: Publications Office of the European Union, 2012. ISBN:978-92-79-23839-0.

[5] D.Procházková. *Analýza a řízení rizik.* ČVUT v Praze, 2011. ISBN 978-80-01-04841-2.

[6] D.Procházková. *Strategie řízení bezpečnosti a udržitelného rozvoje území.* ČVUT v Praze, 2011. ISBN 978-80-7251-243-0.

[7] D.Procházková. *Rizika spojená s pohromami a inženýrské postupy pro jejich zvládání.* ČVUT v Praze, 2014. ISBN 978-80-01-05479-6.

[8] Ch.Bérenguer, A. Grall, C. G. S. (eds). *Advances in Safety, Reliability and Risk Management.* London: Taylor & Francis Group, 2012. ISBN 978-0-415-68379-1.

[9] D.Procházková. *Základy řízení bezpečnosti kritické infrastruktury.* ČVUT v Praze, 2013. ISBN 978-80-01-05245-7.

[10] D.Procházková. *Challenges connected with critical infrastructure safety.* Saarbruecken: Lambert Academic Publishing, 2014. ISBN: 978-3-659-54930-4.

[11] J.Reason. *Human error.* Cambridge: Cambridge University Press, 1990.

[12] J. Procházka, D.Procházková. *Criticality of transportation infrastructure in Czech Republic, IRICoN 2016.* Acta Polytechnica CTU Proceedings, 2016. ISBN: 978-80-01-06022-3, ISSN 2336-5382. 5.

[13] Archiv poznatků o pohromách a haváriích. ČVUT v Praze, Fakulta dopravní.

[14] Google. "www.google.com".

[15] Railway-technology. "www.railway-technology.com".

[16] Revolvy. "www.revolvy.com".

[17] Isdo. "www.isdo.org".

[18] U. DOT. Railway accident reports. "http://specialcollection.dot.library.dot.gov/Home".

[19] D. inspekce. Archiv. "http://www.dicr.cz".

[20] D.Procházková. *Metody, nástroje a techniky pro rizikové iženýrství.* ČVUT v Praze, 2011. ISBN 978-80-01-04842-9.

[21] T.Kertis, D.Procházková, J.Procházka. *Railway accidents in the Czech Republic, causes of risks and their mitigation, In: ESREL 2017 proceedings.* London: CRC Pres / Balkema. In print.