Use of risk assessment methods in maintenance for more reliable rolling stock operation

Juraj Grenčík[1,*], *Roman* Poprocký[1], *Jana* Galliková[1], *Peter* Volna[1]

[1]Department of Transport and Handling Machines, Faculty of Mechanical Engineering, University of Žilina, Univerzitná 8215/1, 010 26 Žilina, Slovak Republic

Abstract. Operation of the rolling stock is associated with a number of risks. The consequences of failures are sometimes very serious - safety or the environment, sometimes only economic. A significant factor affecting the safe operation of railway vehicles is maintenance. The paper presents methods of risks assessment and possibilities of their reduction in design, operation and maintenance of railway vehicles. Special attention is given to the new "silent brakes" and safety related issues for freight wagons.

Keywords: risk assessment, railway safety, reliability

1 Introduction

It is well known fact that European railways are the safest mode of land transport. The safety level has improved at impressive pace over the past decade and the railway industry can be proud of its achievements, mostly achieved through technical advances. However, although extremely rare, catastrophic, multi-fatality have a heavy impact on the confidence of passengers, customers, public founders and investors. As well as the human cost, every accident, whether they result in injuries or not, represents a significant business cost in a highly competitive environment. Catastrophic accidents have the potential to close otherwise viable businesses and reduce services altogether.

Security issues are also addressed by institutions at the top level, for example European Union Agency for Railways (ERA). Monitoring safety performance is a priority task of the Agency in its mission to promote a harmonised approach to railway safety in Europe. A harmonised Safety Management System (SMS) is the foundation for managing and controlling risks, and building trust among railway undertakings and infrastructure managers in the European Union [1].

Common Safety Indicators (CSIs) are used by National Safety Authorities to gather information from railway undertakings and infrastructure managers, which combined with other relevant data, makes a comparative analysis possible, and serves as basis for policy recommendations at EU level. CSIs are a common set of rail safety data, gathered to facilitate the assessment of achievement of Common Safety Targets (CSTs) and monitor the development of safety in Member States [2].

* Corresponding author: juraj.grencik@fstroj.uniza.sk

Reviewers: *Marcin* Kubiak, *Ivan* Kuric

Common safety indicators are divided into the following groups:

- Indicators relating to accidents,
- indicators relating to dangerous goods,
- indicators relating to suicides and attempted suicides,
- indicators related to precursors of accidents,
- indicators to calculate the economic impact of accidents,
- indicators related to technical safety of infrastructure and its implementation.

Common Safety Targets (CST) are the qualitative measures for assessing the railway safety risk in the Member States of the Union. Rail transport is the only mode of transport for which these objectives have been prescribed by European legislation. The common safety targets are EU-wide maximum risk and the National Reference Values (NRVs) are the maximum risk values for each Member State. The level of risk is measured in terms of the number of killed and severely injured persons per train kilometre. There are categories of risk for passengers, employees, crossings users, unauthorized persons on railway and others, as well as society as a whole [3].

Around 2 000 significant accidents occur each year on the railways of the EU Member States. Collisions and derailments represent a mere ten per cent of them. Accidents to persons caused by rolling stock in motion and level-crossing accidents constitute the majority of significant accidents, excluding suicides. The number of significant accidents per accident type in the period 2012–2014 is presented in the Fig. 1. The number of significant accidents increased by 5 % in 2014 year-over-year in EU-28 Member States. This is the first Year over Year (YoY) increase in ten years [4].

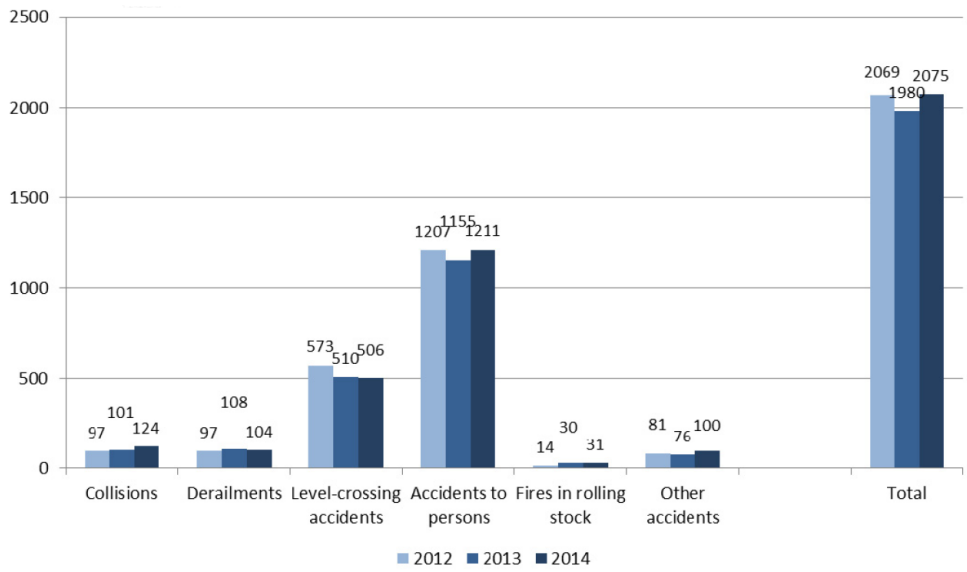

Fig. 1. Significant accidents per type of accidents [4]

2 Risks in general

Every process, system, or human activity is affected by risks that can have both a positive and a negative impact. In relation to maintenance activities, the occurrence of each failure is a negative phenomenon that can be expressed in terms of the magnitude of the risk depending on the probability of the occurrence of the disorder being encountered and the

consequences. Hazards such as sources of potential damage must be analysed in relation to all activities of the organization. These sources can be, for example:

- Technical equipment, technological processes, chemicals and materials,
- safety requirements and health protection at work,
- political activities,
- environment and its impacts,
- legal and commercial relations,
- economic aspects in the country of operation,
- market situation,
- the level and method of management,
- logistics, etc.

In general, an accident prevents the build-up of faults in a device or a deviation from its normal operation. This phase may take minutes, hours, sometimes even years. Defects or deviations from normal activity do not yet cause an accident but not create appropriate conditions for it. Operators usually do not notice this phase if they are not performing the prescribed work or do not have information about functioning of the object. That's why they do not feel threatened. In the next phase a sudden event arises, which will significantly change the situation. If operators try to restore the normal operation of the technological process and do not have complete information, they only exacerbate the development of the accident. In the last phase there is a sudden event that represents the impulse, after which the technical system ceases to be subordinated to a man and there is a negative phenomenon.

The source of risks is sometimes nature, sometimes human being, sometimes technology or technological processes. Any undesirable event may have a link to a certain loss associated with the risk object.

The risk factors in connection with reliability, safety and maintenance in transportation systems are analysed in a complex manner e.g. by Dhillon in [5, 6].

The relationship of the risk object to adverse events allows the risk to be divided into:

- Individually,
- technical,
- ecological,
- social,
- economical,
- other risks.

Each type of risk has characteristic sources and factors (Table 1.).

Table 1. Objects, resources and undesirable consequences of the different types of risks

Type of risk	Object of risk	Source of risk	Undesirable consequences
individual	person	live conditions	illness, trauma, disability, death
technical	technical systems and objects	technical incompetence, disruption of the operation of technical systems and objects	crash, explosion, fire, catastrophe, destruction
environmental	ecological systems	anthropogenic interference with the natural environment, unusual situations technogenous	environmental catastrophes, natural disasters
social	social groups	unusual situation, reduced quality of life	group trauma, illness, death of people, increase in mortality
economical	material resources	reducing the safety of production or the natural environment	increased security costs, damage caused due to lack of protection

3 Risk management

Risk management is the systematic application of management policies, procedures and established practice. It is a complex of coordinated management and control activities with respect to risk. This process is dependent on the experience, knowledge, imagination, creativity and ability of the team (individuals) performing these activities. Applying these procedures, without involving teamwork and competent staff, cannot provide proper and thorough risk analysis results. An important step is to choose the appropriate risk assessment method. The risk assessment based on a risk analysis assesses the severity of the estimated magnitude of the risk and assesses the need to reduce it.

Risk management is a structured sequence of logical steps (Fig. 2.), where the first step is a risk analysis that examines the potential negative consequences that may result from failures in the performance of technical systems, deviations in technological processes, or errors by service personnel. This also means that negative impacts on humans and the surrounding environment even in the normal operation of the technical system can be investigated. Subsequently, it is necessary to identify the likelihood and extent of the consequences of a negative event resulting from a given work or other activity of equipment or a system. Based on hazard identification, the magnitude of the risk is estimated [7, 8].

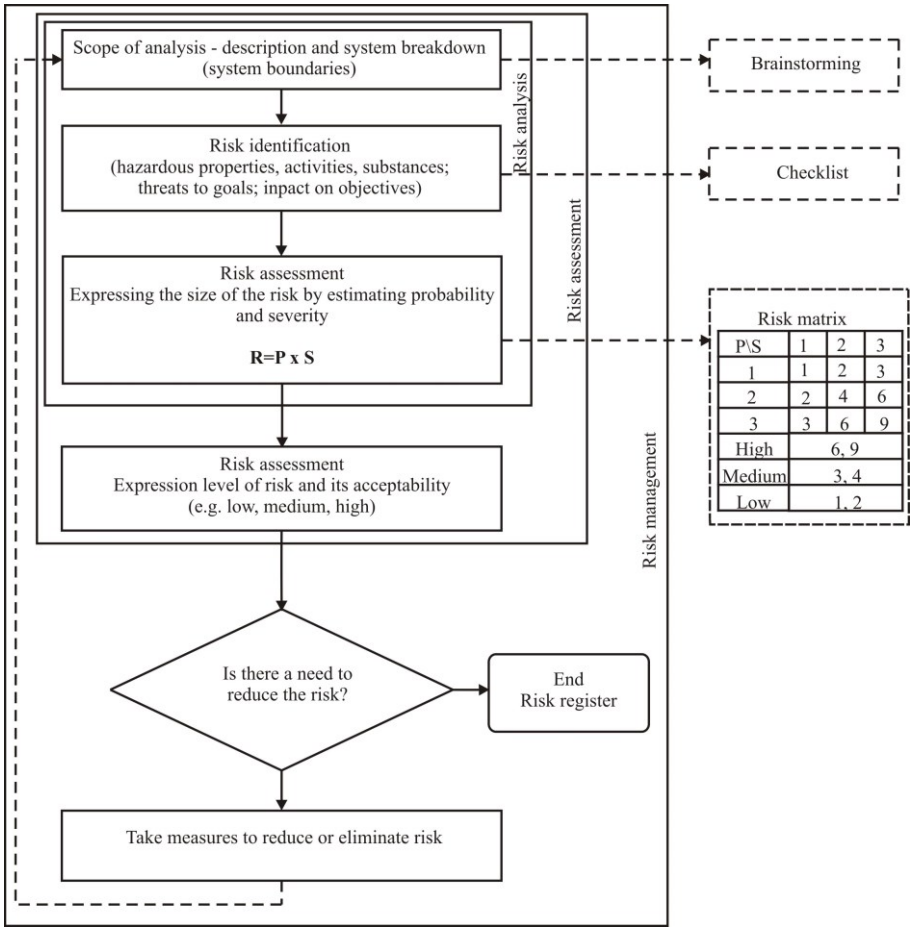

Fig. 2. Risk management chart flow (adapted from [8])

The main task of risk identification is to identify and accurately describe all possible risks that may arise in the given system, based on system information, results of expertise and experience from similar systems. This is an important stage of the analysis, because if the risks are not identified at this stage, then they are not analysed. It is very important to anticipate possible human errors and failures and to consider the relationship "human-system-environment". There are a number of formal risk identification methods.

Risk evaluation is the process of determining risk parameters and their relationship. The risk associated with the type of threat is a function of the severity of the damage (consequence) that may cause and the likelihood of this damage occurring.

The initial information and the results of the risk assessment (risk assessment) must also be documented. In principle, the risk analysis process can be completed at the stage of its identification. After the risk identification phase, the risk assessment stage follows. The final step is to develop risk-mitigation recommendations (risk management) if the level of risk is higher than the admissible level. The risk assessment process is closely linked to the risk analysis. It is a process aimed at determining the magnitude (extent) of the risk of the hazard analysed for the protection of human health, material values, the environment and other situations associated with the emergence of danger. Risk assessment can be defined as a systematic process of evaluating and interpreting real system information that identifies the threat, the consequences of the threat, and quantifying or qualitatively assessing the magnitude of the risk and deciding whether or not it is acceptable.

In assessing the risk, it is first necessary to obtain an overall risk estimate that we can derive from a combination of the likelihood of occurrence of the risk and the severity of its consequences. By combining them we get a matrix of risk. Consequently, the risk can be expressed, even though it is actually invisible and intangible [9].

Risk assessment is the step in which the identified risks must be compared on the basis of criteria with an acceptable level of risk to eliminate the hazard with an unacceptable level of risk. This step serves as a basis for developing recommendations and risk mitigation measures. Acceptable risk criteria as well as risk assessment results can be expressed qualitatively, quantitatively or semi-quantitatively.

In the process of risk management, the so called principle of ALARP ("as low as reasonably practicable") is usually applied, the fundament of which is to reduce the risk to the level that is reasonably acceptable. This principle works with risks located in an acceptable area (Fig. 3.).

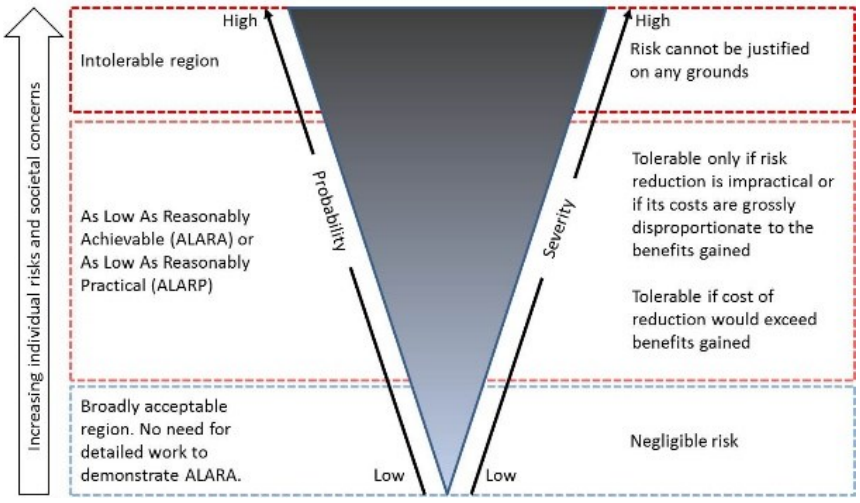

Fig. 3. ALARP principle [8]

When risk management measures are adopted, residual risk must be documented, regularly monitored and reviewed in cooperation with stakeholders. It is necessary to take into account the effectiveness and efficiency of the measures. Bad management decision made on the basis of ignorance or lack of experience may to increase the risk or create a different type of threat by adopting inappropriate measures.

3.1 Safety criticality – ERA approach

EU member states have until now developed their safety rules and standards mainly on national lines, based on national technical and operational concepts. Simultaneously, differences in principles, approach and culture have made it difficult to break through the technical barriers and establish international transport operations.

Directive 91/440/EEC, 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 provide the first steps towards regulation of the European rail transport market by opening the market for international rail freight services. However, the provisions on safety have proved to be insufficient and differences between safety requirements remain, which affect the optimum functioning of rail transport in the Community. It is of particular importance to harmonise the content of safety rules, safety certification of railway undertakings, the tasks and roles of the safety authorities and the investigation of accidents [10].

Important role in railway operation safety was recognised in the area of maintenance. Therefore, ERA (European Railway Agency) is responsible for certification of ECM (Entities in Charge of Maintenance) with the aim of enhancing maintenance system, in the first stage, of freight wagons, focused on risk reduction by properly managed and executed maintenance works. Each freight wagon has to have its ECM registered who is responsible for its maintenance.

In 2016, the 4th railway package1 introduced the term “safety critical components” [1]. EU railway legislation does not contain though any clear definition of which component can be characterised as safety critical. In 2016, ERA conducted several informal and formal consultations to define the state of play in the area. In general terms, the only output of the consultation conducted was that currently there is no list defining which components of the railway system are safety critical [11].

A harmonised list could vary among the different railway systems in the EU member states, utterly considering potential diverse factors present in the different member states, such as the environmental conditions including the geographical scope, the safety objectives, the km or the operational hours, the operational processes, the maintenance context, the time (lifecycle) and the design of each different railway system. Hence, depending on the situation, a harmonised list for all EU member states could be either non-complete or too exhaustive, which could unavoidably result in non-sustainable increase of cost in design, use and maintenance of the technical systems.

Safety criticality approach is closely related not only with the systems but also with the human’s performance. Multi-disciplinary teams should be assigned in order to identify and classify significant Safety Critical Events by taking into account not only the probable failures but also the operational and maintenance procedures which contribute to the limitation of the failures.

4 Selected safety critical components on railway vehicle

Undoubtedly, wheelsets and brake are safety critical components on a railway vehicle. However, their failures have different potential consequences which is discussed below.

4.1 Serial systems

Typical subsystems on rolling stock without possibility of redundancy (back-up) are running gears, in general consisting of wheelsets (2 wheels pressed on axle), bearings, suspensions and wheelsets guidance. In particular wheels and axles are exposed to high dynamic loads exposed to very high number of loading cycles – typical for fatigue loads. Any serious damage on wheels or axle will result in serious accident.

Serial system (system, where failure on a single subsystem causes failure of the whole system) is schematically shown in (Fig. 4.).

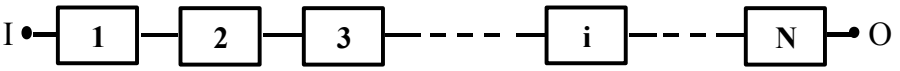

Fig. 4. Reliability block diagram of a serial system

Reliability of the serial system $R_S(t)$ consisting of N components (subsystems)can be calculated by multiplication of reliabilities of the individual components $R_i(t)$ [13]:

$$R_S(t) = R_1(t) \cdot R_2(t) \cdot \ldots\ldots\ldots \cdot R_i(t) \cdot \ldots\ldots\ldots \cdot R_N(t) = \prod_{i=1}^{i=N} R_i(t) \tag{1}$$

In case the components have exponential reliability distribution with failure rate λ_i, the reliability of the serial system can be calculated by multiplication of reliabilities of the individual components (subsystems):

$$R_S(t) = \exp(-\lambda_S \cdot t) = \prod_{i=1}^{i=N} \exp(-\lambda_i \cdot t) = \exp\left[-\sum_{i=1}^{i=N} \lambda_i \cdot t\right] \tag{2}$$

According to [2] for technical systems where a functional failure has credible direct potential for a catastrophic consequence, the associated risk does not have to be reduced further if the rate of that failure is less than or equal to $\lambda = 10^{-9}$ per operating hour.

Typical component with such catastrophic failure consequences is a wheelset. Just to have an idea what this requirement means let us consider a typical freight train composed of 25 four-axle wagons, which is with 100 wheelsets. With “rough” estimation of 2500 hours operation per year we get 0.99975003125 reliability of the train related to running gears, or 0.00024996875 failure probability.

For estimation of real failure rate of broken wheelsets in Europe (EU28) we use the statistics on European railways during the years 2012-14 (Fig. 5) where there are about 70 failures on average per year. From the statistics of freight transport in EU28 [4] we get about 800 million train kilometres per year which gives about 8000 freight trains operated 2500 hours at average velocity of 40 km/h within one year in the EU28. Using the assumed composition of trains (100 wheelsets) we get failure rate $\lambda = 10^{-7.456}$ per operating hour. Comparing with the required value of $\lambda = 10^{-9}$ there is still space for improvements (more than 10 times) resulting in about 5 broken wheelsets on freight trains in Europe per year.

Sufficiently low enough? The estimated numbers are "rough" and highly simplified, but prove a realistic value of 10^{-9} requirements for failure rate of safety critical components.

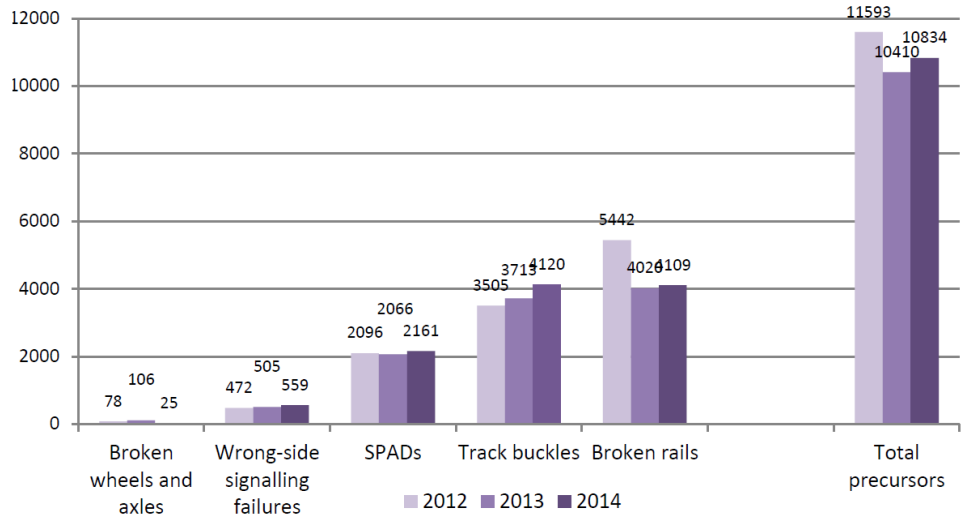

Fig. 5. Accident precursors (EU28. 2012- 2014)

4.2 Parallel (redundant) systems

It may seem strange, but a subsystem on a train that has multiple redundancies is a brake system. Many railway people say that brake system is the most important from the reliability point of view. This is only partly true – stop safely train is very important, but failure of the individual brake on a wagon in a long train creates almost no problem as there are other functioning brakes in the remaining wagons of the train.

Parallel system where failure on a single subsystem is backed-up by other subsystems is schematically shown in the Fig. 6.

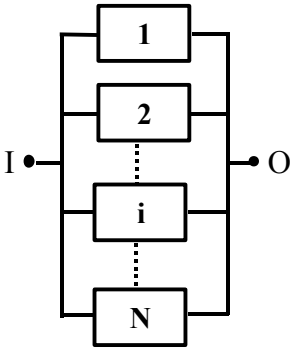

Fig. 6. Reliability block diagram of a parallel system

Reliability of the parallel system $R_S(t)$ consisting of N components (subsystems)can be calculated by multiplication of reliabilities of the individual components $R_i(t)$:

$$R_S(t) = 1 - \prod_{i=1}^{i=N} \left[1 - R_i(t)\right] \tag{3}$$

Failure probability $F_S(t)$ of the whole system is:

$$F_S(t) = 1 - R_S(t) = \prod_{i=1}^{i=N} [1 - R_i(t)] = \prod_{i=1}^{i=N} F_i(t) \tag{4}$$

To be more accurate, the brakes are not fully backed up. In fact, in 25 wagons freight train when on brake does not work, the braking effect is reduced by 4%, but still sufficiently high for effective braking. For emergency stopping the train usually 80% of active brake could be sufficient, which on 25 wagons train represent 20 wagons with functioning brake.

For this calculation of reliability, it is more appropriate to use case of components in a k-out-of-n configuration. In this case, the reliability of the system with such configuration can be evaluated using the binomial distribution:

$$R_S(k, n, R) = \sum_{r=k}^{n} \binom{n}{r} R^r (1 - R)^{n-r} \tag{5}$$

where n is the total number of units (subsystems), k is the minimum number of units required for system success, R is the reliability of each unit.

So when we take data recorded from freight wagons maintained by one maintenance workshop in Slovakia (Fig. 7.), where there were 280 brake failures on 346 wagons during 5-year period. Count represents Pareto analysis of number of failures during 5-year period. Brake failure modes are coded "3XX" and one can see that among the top 6 most frequent failures 4 of them are brake failures (on X-axis). From the data we get 0.162 failures on each wagon per year on average, which is $6.474 \cdot 10^{-5}$ failure rate per operating hour; much higher (about 10^{-4}) than required for safety critical components.

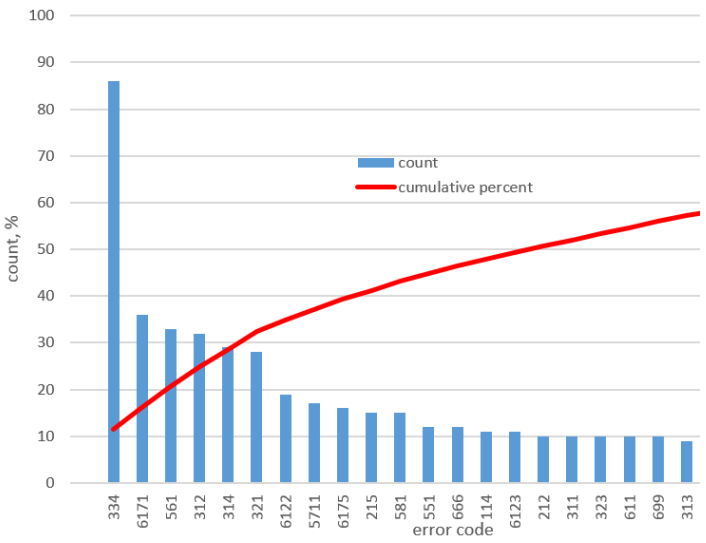

Fig. 7. Pareto analysis of failures on monitored freight vehicles

But if we consider 20 wagons with functioning brake out of 25 sufficient for fail-safe braking of a train, substituting to (5) we receive $R_S = 0.84$, which is acceptable value. In Fig. 8 is a diagram showing increasing reliability with decreasing number of functioning brakes needed for fail-safe (emergency) stop of a freight train.

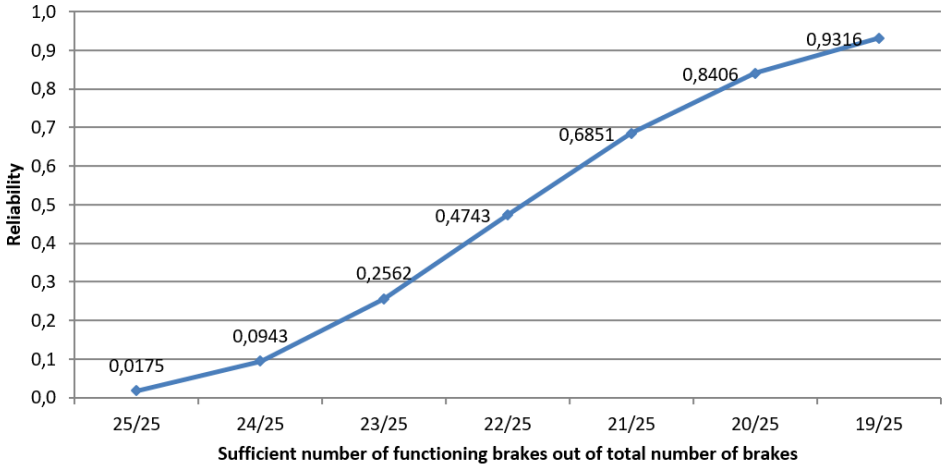

Fig. 8. Reliability of brake on train considering k-out-of-n configuration

Conclusion - play with risks

A "risky combination" is envisaged on European railways. We have discussed situation with accidents where there are some 70 broken wheels and axles annually in EU28 countries. Not too high but should be less if target failure rate of safety critical components will be achieved. However, there are projects with replacement of standard cast iron brake shoes with composite brake shoes. The reason is that they are silent during braking, but have lot of side effects literally threatening railway safety as they damage wheel running surface and in worst case they cause cracks of wheels (Fig. 9). Wheels are typical and perhaps the most important safety critical components used on railway vehicles. There are strict rules to be kept in operation and maintenance to avoid unacceptable damage and to prevent accidents, which usually end in serious consequences. So it is a risky play to change operational conditions caused by new material of brake shoes on a proven design of railway wheelset. Or railway operators must be very cautious with introducing new type of brakes.

Fig. 9. Damaged wheel [14]

The paper was supported by the Scientific Grant Agency of the Ministry of Education of the Slovak Republic and the Slovak Academy of Sciences in project no. VEGA 1/0766/15 "Research sources of noise emissions from rail transport".

References

1. Directive (EU) 2016/798 of the European Parliament and of the Council of 11 May 2016 *On Railway Safety* (2016)
2. Commission Regulation (EC) No 352/2009 of 24 April 2009 On the adoption of a common safety method on risk evaluation and assessment (2009)
3. D. Jovovic, *Collection of examples of risk assessments and of some possible tools supporting the CSM Regulation*. European Railway Agency. Valenciennes: European Railway Agency (2009)
4. Railway safety performance – biennial report, European Union Agency for Railways, ISBN 978-92-9205-049-8 (2016)
5. B. S. Dhillon, *Human Reliability, Error and Human Factors in Engineering Maintenance*. USA: CRCpress. ISBN 978-4398-0383-7 (2009)
6. B. Dhillon, *Transportation Systems Reliability and Safety*. (CRC Press, Boca Raton, ISBN 978-1-4398-4640-7, 2011)
7. H. Pačaiová, J. Sinay, J. Glatz, *Safety and risks of technical systems*. (Vienala, Košice, ISBN 978-80-553-0180-8-60-30-10, 2009)
8. H. Pačaiová, Š. Markuliak, A. Nagyová, *The importance of risk in management systems*. (BEKI Design, s.r.o., Košice, ISBN 978-80-553-2618-4, 2016)
9. P. Baybutt, *Calibration of risk matrices for process safety*. Journal of Loss Prevention in the Process Industries **38**, 163-168 (2015)
10. P. Zvolenský, V. Stuchlý, J. Grenčík, R. Poprocký, *Evolution of maintenance systems of passenger and freight wagons from the ECM certification point of view*. Communications: scientific letters of the University of Žilina **16** (3A), 38-45 (2014)
11. 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 (2001)
12. Commission Regulation (EU) No 445/2011 on a system of certification of entities in charge of maintenance for freight wagons and amending Regulation (EC) No 653/2007 (2011)
13. V. Stuchlý, R. Poprocký, *Údržba strojov a zariadení*. (Žilinská univerzita, 359 p., ISBN 978-80-554-0845-3, 2013)
14. Letter ANSF protocol 003081/2017 pf 21/03/2017, Update of the Safety Alert related the broken wheel (Manufacturer RAFIL) (2017)