Development of multilevel models for assessment of risk of train derailment

D O Reznikov
Mechanical Engineering Research Institute of the Russian Academy of Sciences, 101990, 4 Maly Kharitoniesky lane, Moscow, Russia
mibsts@mail.ru

Abstract. The paper presents a multilevel model for assessing risk of train derailment. The model is based on the toolkit of Bayesian nets and allows accounting for the influence of human and organizational factors as well as factors of safety regulation regimes on the occurrence of stochastic events that compile various scenarios of railroad accidents.

1. Introduction
The statistics of major accidents at rail transport facilities indicates that these accidents are, to a large extent, related to errors of employees of the railway company, as well as to organizational and management factors and to factors of safety regulation imposed by supervising agencies. According to existing estimates, the number of accidents that is associated with human and/or organizational factors varies for different sectors of the economy in the range from 50 to 90% of their total number [1]. Such a significant scatter in data is determined by the difference in the interpretation of the concepts of technical failure and failure associated with the human error since failures of the technical system components at the operational stage is often caused by human errors made at the stages of their design, construction, maintenance, monitoring, etc. Therefore, if you follow the chain of cause-and-effect relationships far enough, then almost any technical failure can be attributed to a human error in the recent or more distant past.

Issues related to the human factor, in one degree or another, are taken into account when conducting a classical risk analysis of the railway infrastructure and rolling stock facilities. In particular, errors of drivers, dispatchers, or repair workers can be included in failure scenarios as initiating or intermediate events. However, it often happens that human errors only affect the probability of failure of elements of a technical system. If these errors only lead to the weakening of individual components of the system such errors often cannot be explicitly taken into account in the framework of the traditional risk analysis. For example, violations of maintenance procedures often lead to a decrease in the reliability of components of a technical system, but are not a direct cause of their failure.

In addition, the construction of failure scenarios of the technical system does not allow taking into account the fact that human errors, in turn, are often associated with organizational and management problems: for example, an inadequate economic incentives for employees of a railway company, insufficient professional training of personnel, or unreasonable limitation of investments in safety at the company level. It must also be taken into account that organizational and management factors operating within a separate company are formed under the influence of safety regulation regime,
which is expressed both in the form of direct regulation of safety measures that are to be implemented and in the form of economic incentives for companies to reduce risk.

When conducting a quantitative risk analysis, one has to face the uncertainty associated with: (1) the limited knowledge about the technical system in normal and emergency conditions, and (2) the variability of the parameters of the technical system and the external environment of the system. In the case of the inclusion of the human factor, the level of uncertainty increases even more, due to the inability to accurately predict the physical and psychological state of the employees (the driver, dispatcher, or repair worker) at various points in time during normal and emergency situations, and, therefore, to predict possible errors. The latter, as a rule, are not independent events, but are caused by the influence of the organizational environment in which the company employees operate. The influence of organization and management factors on the actions of employees also cannot be unambiguously calculated.

In any case, human and organizational factors, as well as factors of transportation safety regulation should be explicitly taken into account when conducting a quantitative analysis of risks generated by the railway infrastructure. Therefore, the model for integrated risk assessment should have four levels and include: (1) a probabilistic analysis of the failure scenarios of the technical system; (2) analysis of decisions and actions of operators that affect basic events in the failure scenarios of a technical system; (3) the study of management factors within the company that affect the decisions and actions of operators; (4) factors of transportation safety regulation, under the influence of which management principles are formed at the company level. Probabilistic relationships between model parameters related to these four levels should be quantified using the available theoretical concepts, statistics, and expert estimates. The idea of development of the multilevel risk assessment models was proposed by E.Pate-Cornell and D.Murthy in [2].

2. Building a multi-level risk management model
The organization of the work and the management regime at the level of the railway company are factors that determine the likelihood of inadequate/unauthorized actions by personnel. Organizational and management factors are risk management levers that include, in particular, staff selection and training mechanisms; organization of monitoring systems for the technical condition of the facility. These control levers can affect the state of an individual employee (the level of fatigue, professional and psychological training, etc.), they can also create an environment that affects decision-making (for example, through material interest, information support for the decision-making process, approved rules and procedures actions in regular and contingency situations, methods for selecting and training personnel, a system of fines for violations of safety regulations and incentives for their observance, budget gender enterprise ethics regarding investing in monitoring and control systems for the technical condition of rolling stock and infrastructure facilities, etc.).

The mechanisms of transportation safety regulation and incentives for the organizations of the Russian Railways holding to ensure safety at the facilities they operate can be considered as top-level factors affecting the safety practices applied within individual companies.

In order to take into account the four-level structure of influences, an integrated model must be developed (figure 1) that includes the assessment of:

- failure scenarios of the technical system (level 1);
- human factor, including the systematic identification and probabilistic description of decisions and actions of operators that affect the probability of the occurrence of basic events of failure scenarios (level 2);
- organizational and management factors at the level of the railroad transportation company that affect the likelihood of making certain decisions and actions (level 3);
- factors of state safety regulation (level 4).
The four-level model allows comparing different methods for managing risk generated by the railway infrastructure and the rolling stock: improving the elements of the technical system, reducing the likelihood of errors and unauthorized actions by operators, improving the organization and management within the company, optimizing the state regulation regime. The structure of the relationship between the technical system, the actions of the operator (personnel) and management factors are shown in figure 1.

Analysis of the multi-level model should start from the bottom [2, 3].

Level 1. Technical system

Changes occurring in the technical system designed to ensure the implementation of the transportation process can be presented as a path in the space of the technical system states. The path defines the transition from the initial state (IS) of the system (putting it into operation, figure 1) to its end state or decommissioning (ES₀) [4]. When it is possible to ensure such a transition, they say that the system has implemented the specified scenario or success scenario (S₀). If an initiating event occurs (IE) in the system (a component failure or extreme external impact), it can deviate from the scenario and proceed to implement new scenarios ending with end states (ESᵢ) different from the designed end state (ES₀).

In this case, we can say that a failure occurred in the system due to its inability to reach the required end state.

When considering first the technical system itself, according to the total probability theorem, the probability of a system failure can be written as:

$$P(F) = \sum_{i} P(F \mid IE_i) \cdot P(IE_i)$$  \hspace{1cm} (1)
where $P(IE_i)$ is the probability of occurrence of the initiating event, $P(F|IE_i)$ is the conditional probability of failure in the case of the initiating event occurrence.

In the general case multiple failure scenarios leading to different end states ($ES_1$, $ES_2$, ..., $ES_m$) can be implemented in the system. Probabilities of occurrence of various end states $P(ES_h)$ can be obtained as:

$$P(ES_h) = \sum_i P(ES_h | IE_i) \cdot P(IE_i), \ h = 1, 2, 3, \cdots, m$$  \hspace{1cm} (2)

**Level 2. Human Factor**

The action (decision) made by the operator at the time of decision-making ($t_*$) is considered as a random variable (event) that takes one of possible values $\{d^{(i_1)}_1, d^{(i_2)}_2, \cdots, d^{(i_m)}_m\}$ (options for the actions of the operator). The choice of an option is determined by the physical and psychological state of the employee at the time of decision-making, the level of his professional qualification and awareness of the real state of the system, the existing rules of action in emergency situations and incentives. Thus, all options for the actions of employees in the process of escalation of an accident are grouped into categories $d^{(i_1)}_1, d^{(i_2)}_2, \cdots, d^{(i_f)}_f$ corresponding to different points in time of decision-making. Each occurrence of the process of escalation of the accident will proceed with a certain set of decisions made by operators $d^{(i_1)}_a, d^{(i_2)}_b, \cdots, d^{(i_f)}_e$. The combination of selected employee options for all categories (moments of decision making) constitutes a complex random event $D_j = [d^{(i_1)}_a; d^{(i_2)}_b; \cdots; d^{(i_f)}_e]$ that is described by the random variable state of human factor. In this case, the set of complex events $D_1, D_2, \cdots, D_s$ will form a complete group of events.

The decisions and actions of the operators affect both the probabilities of initiating events and the conditional probabilities of failures due to the corresponding initiating event. With this in mind, expression (1) can be written as:

$$P(F) = \sum_i \sum_j P(F | IE_i, D_j) \cdot P(IE_i | D_j) \cdot P(D_j)$$  \hspace{1cm} (3)

When various damaged end states are considered and taking into account expressions (2) the following set of equations can be formed instead of equation (3):

$$P(ES_h) = \sum_i \sum_j P(ES_h | IE_i, D_j) \cdot P(IE_i | D_j) \cdot P(D_j); \ h = 1, 2, 3, \cdots, m$$  \hspace{1cm} (4)

**Level 3. Organizational and management factors**

The organizational principles and safety management procedures adopted by the company (such as the principles of conducting technical inspections, personnel selection and training procedures, principles of budgeting) are also considered random variables and are differentiated into categories $m^{(1)}, m^{(2)}, \cdots, m^{(p)}$. The current value (implementation) of the complex event state of the organizational and management factor $M_k$ is determined by the combination of values accepted within each category $m^{(1)}$, $m^{(2)}$, $m^{(3)}$, $m^{(p)}$ differential organizational and management factors. The set of complex events $M_1, M_2, \cdots, M_s$ form a complete group of events.

The values taken by organizational factors within each category are random variables that have a probabilistic influence on the variables state of the human factor $D_j$.

Therefore, the expression (3) and (4) can be written in the form (5) and (6):

$$P(F) = \sum_i \sum_j \sum_k P(F | IE_i, D_j, M_k) \cdot P(IE_i | D_j, M_k) \cdot P(D_j | M_k) \cdot P(M_k)$$  \hspace{1cm} (5)
\[ P(ES_h) = \sum_i \sum_j \sum_k P(ES_h | IE_i, D_j, M_k) \cdot P(IE_i | D_j, M_k) \cdot P(D_j | M_k) \cdot P(M_k) \] (6)

**Level 4. Factors of safety regulation**

Factors of safety regulation are also grouped into categories \(g^{(1)}, g^{(2)}, \ldots, g^{(p)}\) etc. (such as applicable standards and norms, levels of tolerable and acceptable risk, options for economic incentives for the companies to introduce safe technologies). Next, a complex random event factor of safety regulation \(G_q\) is introduced, which is determined by a combination of differential factors from each category. The set of complex events \(G_1, G_2, \ldots, G_e\) form a complete group of events.

The values of the organizational factors \(M_k\) that are in effect in the company are in a probabilistic dependence on the factors of safety regulation \(G_q\) chosen by the regulatory agency.

The nature of this dependence is determined by the probabilities \(P(M_k | G_q)\) of choosing appropriate solutions in the framework of company management \(M_k\) under various options of safety regulation \(G_q\). Thus, taking into account expressions (5) and (6), probabilistic relationships are established between the factors of safety regulation \(G_q\) and failures of the technical system.

Consequently, the probabilities of the system failure can be estimated as:

\[ P(F | G_q) = \sum_i \sum_j \sum_k P(F | IE_i, D_j, M_k) \cdot P(IE_i | D_j, M_k) \cdot P(D_j | M_k) \cdot P(M_k | G_q) \] (7)

Or when multiple end states are considered:

\[ P(ES_h | G_q) = \sum_i \sum_j \sum_k P(ES_h | IE_i, D_j, M_k) \cdot P(IE_i | D_j, M_k) \cdot P(D_j | M_k) \cdot P(M_k | G_q) , h = 1, 2, 3, \ldots m \] (8)

Expressions (2), (4), (6) and (8) enable assessing the probability of the occurrence of damaged end states of the system corresponding to various options of the actions of operators and to various options of organization and management within the company and government regulatory regimes. Using special probability conversion algorithms, the quantities \(P(ES_h | IE_i, D_j, M_k), P(IE_i | D_j, M_k), P(D_j | M_k)\) and \(P(M_k | G_q)\) and can be calculated as functions of the probabilities of intermediate events that follow the initiating event and lead to the end state. A numerical analysis of the probabilistic relationships between random variables of the multilevel model can be carried out using the mathematical apparatus of Bayesian networks and influence diagrams.

**3. Application of Bayesian nets for development of multilevel models**

Bayesian nets are an effective tool for the development of multi-level risk assessment models [5-7]. The following Bayesian network was constructed to assess the risk of a train derailment (figure 2).

Analysis of the model should start from the bottom. At Level 1, the scenario of a technical system failure is considered: The initiating event is a brake failure, after which (depending on the actions of the dispatcher) a traffic signal for a prohibiting traffic signal may follow. Another possible factor in the accident may be the excess of the permissible speed of the train that, in combination with the incorrect operation of the turnout switch, can also create conditions for the derailment of the train. Further, the accident can develop according to various scenarios depending on whether a collision with another train or a fixed structure occurs, or whether a fire occurs or not.
Level 2 presents the influence of the human factor on the development of the failure scenario. The probability of events, the scenario graph of the technical system is determined, including the variables of the state of the human factor by the quality of the maintenance procedures. The derailment of the train and subsequent events of the escalation of the accident are in probabilistic connection with the level of professional qualifications of the driver and dispatcher.

In turn, the state of the variables related to Level 2 model depends on the organization and safety management factors at the company level (Level 3). The qualifications of the personnel and the level of maintenance depend on the principles of personnel selection and training adopted by the railway company, as well as on the costs of ensuring safety.

Finally, the variables located at Level 3 are probabilistically dependent on the type of safety regulation regime at the national/sectoral level (Level 4). In this example, two regimes liberal and administrative are distinguished.

Node 1 Safety Regulation Regime is a decision node. The values of the variable that determines its state are selected by the regulator out of two alternatives: (1) liberal regime that corresponds to soft requirements and limited expenditures on ensuring safety, and (2) administrative regime corresponding to strict requirements and significant investments in safety systems. Node 1 Safety regulation regime is the root node of the diagram.

Nodes 2-19 are random network nodes. The states of each of the non-root nodes are set by the table of conditional probabilities under various states of their parents.

The probability field for the liberal regime of transportation safety regulation is presented in figure 3. The random variable Accident that determines the end states of the system is presented by random node 19. The probabilities of the occurrence of various accident scenarios are determined using the Bayesian net. The estimates of losses occurring in case of occurrence of various scenarios
are determined on the basis of expert assessments and available statistics. The values are set based on how experts evaluate losses that correspond to various accident scenarios.

The presented diagram is part of the graphical interface of the GeNie 2.0 software package [8].

**Figure 3.** Probability field under the liberal regime of transportation safety regulation.

The values of risk for liberal and administrative transportation safety regulation regimes are estimated using the expression $R = \Sigma P_i U_i$ and amount to 122.61 thousand dollars under liberal and administrative regulatory regimes and 14.48 thousand dollars, respectively. The presented calculations show that in the transition from a *liberal* to an *administrative transportation safety regulation regime*, the likelihood of severe scenarios and the magnitude of risk decrease significantly. This means that by changing the factors of transportation safety regulation, a significant effect can be achieved without investments in changing the technical system.

The advantages of influence diagrams include the fact that they allow recalculating the probability field and the magnitude of risk upon additional information is received from monitoring systems about the state of individual model variables, thereby clarifying the obtained estimates. Suppose that for the example in question (figure 4) there is additional information about that under the liberal transportation safety regulation regime a *turnout error* occurred (that is, a random variable becomes deterministic), in this case the probabilistic field of the model changes significantly. In particular, an a priori estimate of the probability of a successful passage of a section decreases from 0.846 (a priori estimate) to a value of 0.603 (a posteriori estimate). At the same time, the probability of accident scenarios increase accordingly, and the posterior assessment of the risk increases to 307.90 thousand dollars compared to a priori estimate of 122.61 thousand dollars.
When solving risk management problems associated with the operation of a hazardous facility, it is necessary to use an integrated approach that involves a combination of actions aimed both at improving the elements of the technical system, building a more effective safety management system, and increasing the professional training of operators and personnel. To achieve it, multilevel risk assessment models must be built that allow accounting for the influence of human and organizational factors, as well as factors of safety regulation on the occurrence of various failure scenarios in the technical system.

Bayesian networks are an effective tool to analyze such multilevel models with a high level of uncertainty, as well as to refine the estimates obtained upon receipt of additional information on the values of random variables appearing in the model.

References
[1] Bea R 2002 Human and Organizational Factors in Reliability Assessment and Management of Offshore Structures. Risk Analysis 22 1 29-45
[2] Pate-Cornell E and Murthy D 1996 Human and management factors in probabilistic risk analysis: the SAM approach and observations from recent application Reliability Engineering and System Safety 53 2 115-126
[3] Pate-Cornell E 2002 Finding and Fixing Systems Weaknesses: Probabilistic Methods and Applications of Engineering Risk Analysis Risk Analysis 22 2 319-334
[4] Makhutov N A and Reznikov D O 2019 Assessment of large-scale catastrophes in complex engineering systems IOP Conference Series: Materials Science and Engineering 481 012002
[5] Charniak E 1991 Bayesian Networks without Tears AI Magazine 12 50-63
[6] Pearl J 1988 Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference Morgan Kaufmann, San Mateo, California 19882
[7] Makhutov N A and Reznikov D O 2007 The use of Bayesian networks for assessing terrorist risks and choosing the optimal strategy for countering the terrorist threat Problems of Safety and Emergency Situations 5 43-63

[8] GeNle 2.0. Decision System Laboratory, University of Pittsburgh Available at: http://genie.sis.pitt.edu