USE OF SCIENTIFIC APPROACHES AND METHODS FOR PERFORMANCE APPROVEMENT OF SAFETY MANAGEMENT SYSTEMS IN RAILWAYS

Assoc. Prof. N. Georgiev, PhD.[1]
Faculty of Transport Management – Higher School of Transport, Bulgaria [1]

safetyniky@mail.com

Abstract: *Recently, the issue of safety has not been whether or not Safety Management Systems are necessary to secure a high level of operational safety in railways but if they could eventually be improved. The answer is yes and that improvement can be done on the basis of well known (and adapted to the problems of safety) scientific approaches and methods. In other words, safety understanding will be developed into a new stage - Modern Safety Management System. The present paper discusses the possibilities for the introduction of some scholarly methods into safety management in railways.*

Keywords: RAILWAY OPERATING SAFETY, SAFETY MANAGEMENT SYSTEM, BAYESIAN NETWORK

1.Introduction

The understanding of railway operational safety and its primary role for securing quality of the overall transportation process has evolved over the past several decades. The process of evolution started at a stage when safety was identified only as the number of incidents (accidents) which occurred within a given period. Railway safety experts usually call this stage the traditional approach to safety understanding. This initial attitude to safety is characterized only by incident (accident) reporting, spontaneous (unplanned) inspections, design and enrichment of operational regulations on the basis only of accident consequences, poor level of awareness, separate examination of the human factor, equipment and technology, etc. The second stage of safety understanding is marked by evolution of the elements (separately or in combination) of the first stage, for example: complex analysis of the relation between staff and equipment, more comprehensive and developed on the basis of consistent analysis rules, increasing role of personal liability, planned supervision and increasing supervisor's role, etc. The third stage of safety understanding is called Safety Management. Safety Management is based on a system-based approach that stresses the interactive nature and interdependence of external and internal factors in a structure (for instance: railway undertaking). In this connection, all written procedures and regulations, operating (management) logic and company's strategy for decision-making is named Safety Management System (SMS). Recently, the question has not been whether or not Safety Management Systems are necessary to secure a high level of operational safety in railways but if they could eventually be improved. The answer is yes and that improvement can be done on the basis of well known (and adapted to the problems of safety) scientific approaches and methods. In other words, safety understanding will be developed into a new stage - Modern Safety Management System. The present paper discusses the possibilities for introduction of some scholarly methods into safety management in railways.

2.Fundamentals of SMS

2.1.Background

The idea of a Safety Management System is inextricably connected with the concept of system safety. This concept itself has a long history beginning in the late 1950s when it wss recognized as a separate scientific discipline. Prior to the 1950s, designers, engineers and managers relied mainly on a fundamental method of solving safety problems known as the *trial-and-error method*. Initially this simple approach gave a modest contribution towards the achievement of safety design. But with the growth of complexity of systems, this approach began to be unsuitable for qualitative decision-making process in the field of safety. The primary reason for this was the increased sensitivity of society regarding safety. The old model of creation of safety rules after a technical failure, incident or accident was no longer able to give enough positive results to prevent the future occurrence of similar failures or accidents. A new approach was necessary for better results in prevention.

Thus, *trial-and-error approach gradually* developed into a *system-based approach* of the attitude to safety. System-based approach to system safety considers safety problems in their entirety and its specific characteristic can be summarized as: *instead of waiting for something bad to occur it is better to take action to prevent this occurrence*.

All the above apply to a variety of industries including railways. It could be said that the increased complexity of railway technical and technological systems played the role of a catalyst for the origin, gradual adoption and present utilization of the concept of system safety in railway industry. Nowadays, the system safety approach is extensively used by a variety of railway undertakings and its practical realization is known as Safety Management System.

2.2.Pillars of Safety Management in railways

In order to illustrate the possibilities for the utilization of scholarly approaches and methods in design and functioning of a railway SMS, it is firstly necessary to define its nature and foundations. The next three items form the basics of the concept of Safety Management System:

-**Key definitions**:

-*System.* The term *system* is mentioned in [1], [7] and [8]. But from the point of view of railway technical exploitation and operational management, the following definition is probably more accurate: A *railway system is a combination of people, procedures and/or specific equipment all functioning within a specified working environment to accomplish a specific task or set of tasks for conveyance of people and commodities* (adapted to [6]). A railway undertaking (company) could be considered as a *technological system* including a variety of technical objects (also called *technical systems*/*subsystems*: vehicles, specific equipment, etc.), natural resources, people (designers, managers, operators, and customers), scientific and technical knowledge, regulations, norms of culture and behaviour, etc.

-*Hazard.* This is a situation that can occur within the transportation process capable of causing harm, injury, death, and/or damage.

-*Risk.* According to [2] risk is the probable rate of occurrence of a hazard causing harm and the degree of severity of that harm.

-*Safety management.* Application of engineering, technological, economical and management principles, criteria, and techniques to optimize the operating process of transportation on a level where all potential risks are tolerable in line with predefined railway authority requirements.

-**Principles and related conclusions**:

-Every man-machine system entails some kind of risks (nothing can be perfect). As a matter of fact, whatever the railway undertaking (Carrier or Infrastructure operator), it consists of a variety of subsystems which are usually a complex mixture of man-machine systems and could be a source of risk. *Therefore, only a qualitative, profound and system based analysis will identify risks and assess their elements, probability of occurrence and possible consequences.*

-Identified and assessed risks do not require managerial confusion or relief (no need of prejudice). It is well known that within transportation process total absence of risks is practically impossible, a fact that should not be taken for granted or as source for panic. *Therefore, only a reasonable and well-balanced identification, monitoring and controlling of risks will lead to an adequate response (in compliance with company's features, knowledge and experience about safety, regulations, etc.) to whatever internal or environmental changes influencing the operating process.*

-There are no obvious safety issues within an operating process, just engineering, technological and managerial ones which could cause serious mishaps (nothing can be absolutely obvious). Therefore, It is very important to define clear purposes regarding subsystems to be analysed (including their attributes, components interrelations, role in the overall operating process, inherent potential risks, etc.) and employ appropriate scholarly analytical tools (econometric, statistical, probabilistic, simulation, etc.).

-Whatever safety issue leads to the necessity for solution (mitigation measure), that can never be the best, just optimal. Therefore, decision-making needs to be put in place in order to achieve a reasonably practicable option of possible solutions.

-Most events and conditions influencing safety have a stochastic and unique nature. Therefore, a knowledge based approach to decision making with permanent involvement of operating staff in it is very important in safety management.

-Hazards may happen any time (and also many times) and in transport industry they usually impact not only the system where they occur but others (other companies, local people, etc.). Therefore, continuous efforts for safety improvement with mutually beneficial results are needed.

-**Basic components**:

-*Safety Policy* - It is company's commitment that safety is a key element of the entire operating process. This commitment is usually in form of written document from highest level of management and should be circulated to all operating staff. The safety commitment has three elements: *design and future improvement of SMS (including all company's rules, procedures and standards), encouragement of the staff acting on all levels of the operating process* and *ensuring all needed resources are available to meet safety requirements.*

-*Safety encouragement* – It is a company's duty to promote the right understanding of safety at all levels of technical exploitation. It includes: *safety behaviour (safety culture), training of the staff regarding structure and requirements of SMS and the exchange of knowledge (communication).*

-*Risk management* – This is an analytical procedure used to make decision regarding the nature of potential risks and the necessity for their reduction, involving the following main subtasks: *hazard identification, risk assessment, defining* and *implementation of mitigation measures.*

-*Safety monitoring* – It is a general and permanently implemented procedure to ensure that a railway undertaking follows the defined safety policy. It includes: *company's scheme of periodical audits (internal or/and external)* and *procedure of corrective actions.*

3.Possibilities for monitoring of SMS components with utilization of scholarly methods

The achievement of a safe transportation process is a very important task. At the same time even with well-established and good working SMS, this is a complex requirement, not easily achieved. The main reason for that is that a variety of processes and events typical for the above-mentioned components of SMS are characterized by complexity, uncertainty and ambiguity. A number of scientific approaches and methods exist that could be successfully utilized in SMS design, implementation and further improvement. The application of a very popular analytical method to improve the functioning of SMS will be presented within this section.

3.1.Bayesian network relevance to SMS

3.1.1.Background

Bayesian networks (also known as Bayesian belief networks) are probabilistic graphical models that make it possible to arrive at a decision regarding the sequence and interdependence of defined events at the conditions of uncertainty and ambiguity [3], [4], [5]. A Bayesian network consists of nodes (vertices) and arcs (direct edges). The nodes $X = X_1,..,X_2,..,X_n$ of the network represent random variables (or events) whilst the arcs describe their causal relationship. In other words, the arc $X_i \to X_j$ represents a statistical dependence between events X_i and X_j , that is: the first event (also named *parent event*) can cause the second one (also known as *child event*). Due to the fact that an event may have some "parents", a Bayesian network can be deemed as a mixture of "descendant" sets (sets of nodes that can be reached by a direct connection from the considered node) and "ancestor" sets (sets of nodes from which the considered node can be reached by a direct connection). A basic property of Bayesian networks is their acyclic design - there is no causal feedback in their structure (the graph does not involve nodes which are their own ancestor or descendant).

Each event (variable) in a Bayesian network is characterized by a probability set (table). For a child event, the table consists of some conditional probabilities covering all combinations of states of an event's parents. Depending on the number of parents the probability tables can dramatically increase.

Events without parents have simpler probability tables consisting just initial probability distribution.

The design of a Bayesian network encompasses two basic stages:

-*Definition of consequence (hypothesis) events.* These are events for which the investigator wants to know the probability distribution allowing him to make a respective solution.

-*Definition of initial events.* These are events giving evidence (initial) information about the process under consideration.

-*Definition of intermediate events*. These are events providing additional information regarding the process under consideration.

-*Graphical design of the network*. Construction of the network is made by connection of events (arcs) having logical relationship (in the context of the investigated process). It is very important to follow causality direction.

-*Constructing the probability tables*. Tables can be filled by using subjective probabilities (on the basis of expert's knowledge), statistical methods and gathered data, simulation, etc.

-Reasoning. Depending on the analysis Bayesian networks can be used for two types of reasoning (conclusions):

-Top-down reasoning (follows the direction of the network arcs) – *predictive reasoning* from the information about causes to the beliefs (expressed by conditional probabilities) in effects.

-Bottom-up reasoning (follows the opposite direction of the network arcs) - *diagnostic reasoning* from consequences to causes

3.1.2.Feasibility

The ability to make effective SMS decisions largely depends on the presence of sufficient information about different operating situations. Unfortunately, due to the essence of the transportation process, it is almost impossible to gain as much reliable information as safety managers would like to have. Therefore, an appropriate analytical tool used to handle uncertainty (basic problem for an effective decision-making) is to be used. Due to the fact that Bayesian networks use probability to represent uncertainty and ambiguity (and in such a way the respective operating scenarios connected with them) they are a very good example of such an analytical tool.

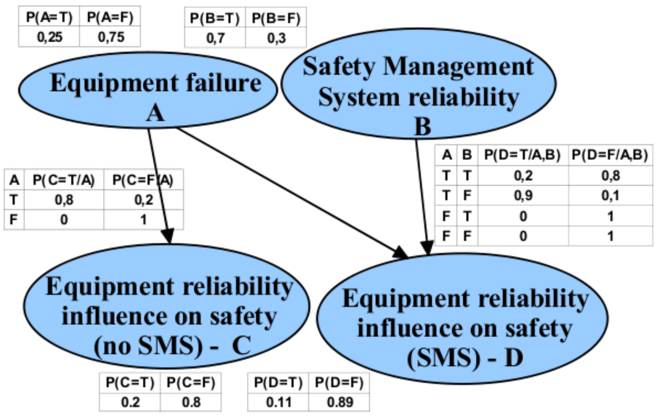

Fig.1. Exemplary Bayesian network

There are lots of possible applications of Bayesian networks within the procedures of implementation of SMS. Let us consider a simple example that illustrates some of the characteristics of Bayesian networks and their specific feasibility in railway SMSs (Fig.1). The example describes the influence of SMS over transportation process safety. More specifically, it considers railway technical equipment reliability and its impact on safety in two possible scenarios – with and without SMS - of the railway undertaking. Furthermore, the network takes into consideration the SMS reliability that can be defined as its possibility to encompass all possible safety issues (risk assessment, scope of safety rules, adequacy of procedures, etc.). So, in this operational diagnosis example, we might ask whether and to what extent SMS presence (and its efficiency) mitigates the equipment imperfection. All network variables (events) are binary, i.e.: they are either *TRUE* (denoted by "T") or *FALSE* (denoted by "F"). For instance: equipment reliability is described by event *A* - *"equipment failure"* with probability of occurrence $P(A=T)=0.25$, such as SMS reliability is represented by event *B* - *"SMS failure to detect and prevent an equipment failure from developing into a mishap"* with probability of occurrence $P(B=T)=0.3$. Conditional probability tables describing all possible scenarios of dependence between events are shown beside each node. Following the network topology and quantifying the relationship between connected events (by using conditional probability distribution about each one of the nodes) it is possible to determine the final events (effects). In the present example they are events *C* and *D*. There are two scenarios of equipment reliability influence over safety and it is very easy to notice the effect of SMS. The presence of a well-established and properly working SMS (within the operating process of a given railway undertaking) helps to diminish almost two times the impact of equipment over operating safety represented by the probability of accident occurrence $\rightarrow$ $P(C=T)=0.2$ and $P(D=T)=0.11$.

The example above of Bayesian network can be deemed as a causal model of relationship between some predefined safety attributes and their strengths. Similar models could be developed regarding many safety management problems and could successfully be used to implement qualitative decision-making.

3.2.Using simulation in Bayesian networks

As it is explained above, the inference through Bayesian network relies on a set of probability tables representing uncertain events. Sometimes, there is no need to compute the exact value of the unknown probability but only its approximate assessment (which could be improved later by using supplementary computing resources). That could be done by stochastic simulation and such an approach is applicable in safety management where a decision-maker must urgently respond to the occurrence of specific events (changes) within operating environment. Thus, the manager would have permanent knowledge (although not too precise) about the specifics of the operating environment. This approach will be illustrated in the following example.

Let us have a Bayesian network describing a given scenario of accident occurrence B caused by two causes A and C (Fig.2). Probabilities of occurrence of causes A and C which are under consideration regarding the investigated type of accident are $P(A=T)=0.75$ and $P(C=T)=0.25$. The conditional probabilities of event B are also depicted in figure 2. As a matter of fact, they represent all possible scenarios of accident occurrence B as a result of occurrence (or not occurrence) of cause *A* and/or cause *C*. The diagnostic reasoning of constructed in such a way Bayesian network allows obtaining probability of occurrence of cause *A* given that accident *B* has not happened - $P(A=T/B=F,C=F)$. In other words, this is the probability of occurrence of cause (causal factor) A which is under investigation within the operating process of transportation. The diagnostic reasoning could be implemented by simulation following the next algorithm involving three main steps:

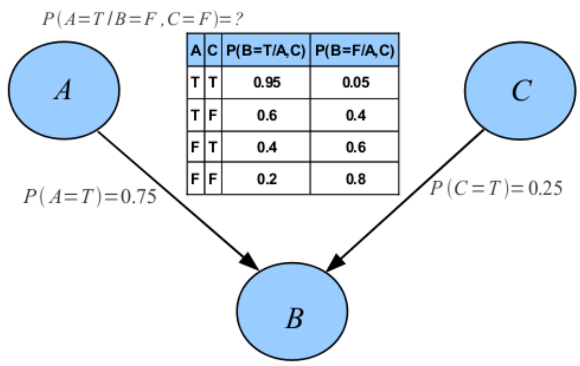

Fig.2. Accident scenario B with causes A and C

Step 1: Simulation of event A following previously predefined prior probability - $P(A=T)=0.75$.

For this purpose a random variable $R_A \in [0,1]$ is generated. Each value of R_A as a single representative of event *A* has to be compared to prior probability $P(A=T)$. If $R_A < 0.75$ event A can be considered as *TRUE* (A) otherwise as *FALSE* $(\neg A)$. The simulation process regarding event A is shown in figure 3.

Step 2: Simulation of event B.

Depending on the results connected with the first step of simulation, the respective conditional probability of event B has to be chosen for continuation of the simulation process following the same approach as this on step 1, namely:

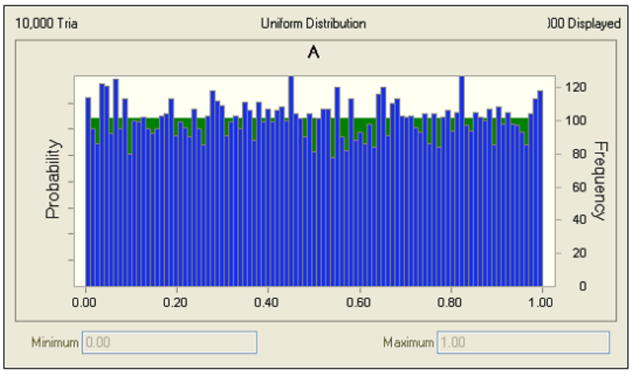

Fig.3. Simulation of event A

-If after the first step $A = TRUE$ then a random variable $R_B \in [0,1]$ is generated and compared to conditional probability $P(B = T / A = T, C = F) = 0.6$. If $R_B < 0.6$ event B can be regarded as TRUE (B) otherwise as FALSE $(-B)$.

-If after the first step $A = FALSE$ then a random variable $R_B \in [0,1]$ is generated and compared to conditional probability $P(B = T / A = F, C = F) = 0.2$. If $R_B < 0.2$ event B can be regarded as *TRUE* (B) otherwise as *FALSE* $(-B)$.

The simulation process including steps one and two should be fulfilled many times (K) and each iteration of implementation increments two counters - $K_1 = K_{A=TRUE,B=FALSE}$ and $K_2 = K_{A=FALSE,B=FALSE}$ with one, that is.:

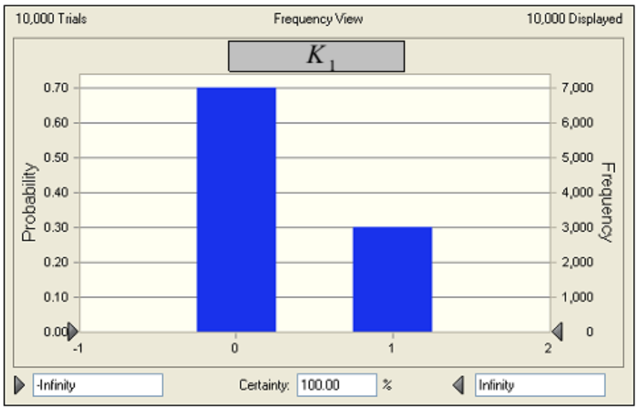

Fig. 4. Estimation of parameter K_1

- $K_1 = K_1 + 1$ if A=TRUE, B=FALSE;

- $K_2 = K_2 + 1$ if A=FALSE, B=FALSE.

The ratios K_1 / K and K_2 / K represent probabilities $P(B = F)$ and $P(A = T \wedge B = F)$. Having their values and by the usage of conditional probability formula the obtaining of probability $P(A = T / B = F, C = F)$ is very easy to calculate as the ration $K_2 / K_1 = 0.66$. The results about parameters K_1 and K_2 are shown in figures 4 and 5.

4. Conclusion and Discussion

The successful management of operational safety in railway industry requires understanding of railway undertaking as a complex system. Such a system could never be designed perfectly and every constituent of it can be subject to failure - technical equipment, operating staff, procedures and rules, etc. System failures entail incidents which are usually considered as normal to occur (it is impossible to absolutely prevent them from occurring). At the same time, serious ones (accident) could and should be prevented and that can be done by implementing certain measures, e.g. company's knowledge of incidents. On this basis and by the usage of appropriate scholarly approaches and methods, the risk management regarding incidents and serious accidents becomes not only possible but extremely effective.

The present article demonstrates that Bayesian networks are applicable in designing and functioning of Safety Management Systems of the railway undertakings. The possibility to manage reasoning and decision making under uncertainty is their main advantage. It all makes them appropriate tools for analysis of

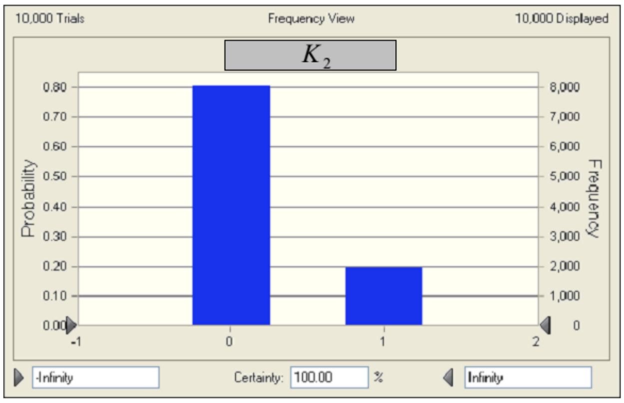

Fig.5. Estimation of parameter K_2

interactions and relationships characterising a railway undertaking which under certain conditions could turn into causal factors of accidents, e.g.: organizational deficiencies, operating environment influence, etc. Due to their simplicity to use, applicability and comprehensive results, Bayesian networks will become more popular analytical tool within all components of railway undertakings' SMSs.

References

[1] Directives 2004/49/EC on the safety on the Community's railways.

[2] EN 50126-1:1999 *Railway applications – The specification and demonstration of Reliability,Availability, Maintainability and Safety (RAMS)* – Part 1: Basic requirements and generic process.

[3] Murphy, K. *A brief introduction to graphical models and Bayesian networks*. http://www.cs.ubc.ca/murphyk/Bayes/bnintro.html.

[4] Neil, M., Fenton, N. *Building Large Scale Bayesian Networks.* Knowledge Engineering Review. 2000.

[5] Premchaiswadi, W. *Bayesian notworks*. InTech, 2012, ISBN 978-953-51-0556-5

[6] Stephenson, J. *System Safety*, Van Nostrand Reinhold, New York. 1991.

[7] 96/48/EC on the Interoperability of the trans-European high speed rail system

[8] 2001/16/EC on on the interoperability of the trans - European conventional rail system