III INTERNATIONAL CONFERENCE
TRANSPORT SYSTEMS TELEMATICS TST`03

ZESZYTY NAUKOWE
POLITECHNIKI ŚLĄSKIEJ 2003
TRANSPORT z.51, nr kol. 1608

railway signalling systems

Karol RÁSTOČNÝ[1]
Aleš JANOTA
Jiří ZAHRADNÍK

SOME PARTICULARITIES IN DEVELOPMENT PROCESS OF A SAFETY-RELATED SYSTEM

Railway signalling systems are typically designed to behave in accordance with principles of fail-safety. Although there is a certain risk and it cannot be completely eliminated. For that reason the term "safety" must be seen in a relative sense. Generally risk analysis should be realised in initial phases of system life cycle though. In the main the article deals with communication that is the most important aspect during the entire process of system development.

WYTYCZNE WDRAŻANIA SYSTEMU ZWIĄZANE Z BEZPIECZEŃSTWEM

Systemy sygnalizacji kolejowej są zazwyczaj projektowane tak, aby zachowywały się zgodnie z zasadami bezpieczeństwa w razie uszkodzeń. Jednakże istnieje pewne ryzyko, którego nie można całkowicie wyeliminować. Dlatego też termin „bezpieczeństwo" musi być rozpatrywany jako coś względnego. Ogólna analiza ryzyka powinna być zatem realizowana we wstępnych fazach cyklu życia systemu. Artykuł odnosi się przede wszystkim do komunikacji, która stanowi najważniejszy aspekt podczas całego procesu wdrażania systemu.

1. INTRODUCTION

Railway signalling systems are typically designed to behave in accordance with principles of fail-safety. Considering an achieved level of knowledge, limited technical and economic resources we must actually admit that a certain risk exists and cannot be completely eliminated. For that reason the term "safety" must be seen in a relative sense. Speaking of a safe system does not mean the system is absolutely safe but the fact that the level of its safety comes up to given safety requirements. Successful safety solution requires a system approach that can be characterised as a process of looking for an optimal strategy to ensure safety that covers all phases of system life cycle. Ensuring safety of a safety-related system pre-production phases of system life cycle are dominant (see Fig.1) since the system must "be born" with safety – safety cannot be "added" to the system. The standard [1] defines

[1] Department of Control and Information Systems, University of Žilina, Veľký diel, Žilina 010 26, Slovak Republic, karol.rastocny@fel.utc.sk, ales.janota@fel.utc.sk, jiri.zahradnik@fel.utc.sk

procedures and tasks for individual phases of system life cycle that must be realised to achieve ability of the system to perform required functions with respect to reliability, availability, maintainability, safety and their mutual effects [6].

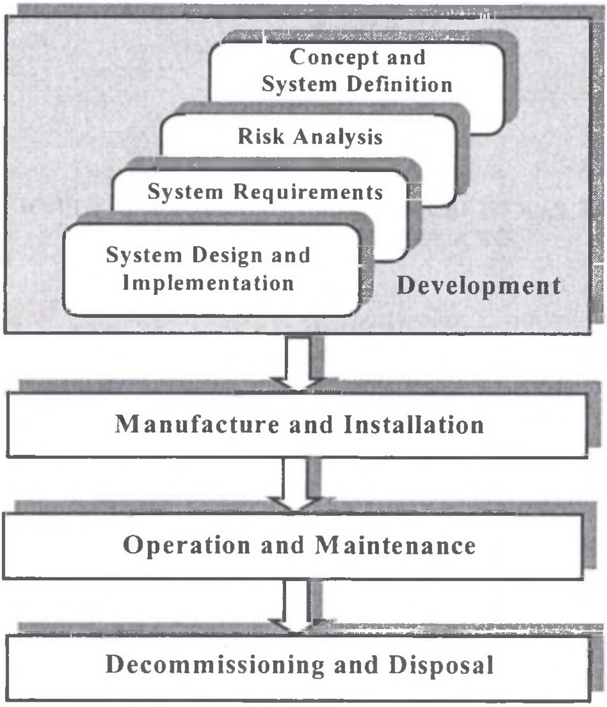
Concept and System Definition
Risk Analysis
System Requirements
System Design and Implementation
Development
Manufacture and Installation
Operation and Maintenance
Decommissioning and Disposal

Fig.1. Basic phases of railway signalling life cycle

2. RISK ANALYSIS

To define safety requirements for a safety-related system we need to know risk resulting from system application and tolerable risk. Generally risk analysis should be realised in initial phases of system life cycle, i.e. hazards and their consequences should be identified for individual required control functions. Combination of probabilities of hazard occurrences and hazard consequences represents risk associated with process control. Exact risk quantification is practically impossible or very difficult. To simplify risk estimation those factors are considered that have effects on a kind of hazard and hazard rate.

There is connection between risk resulting from failure of individual control functions and safety requirements for realisation of these functions. If safety requirements are defined for individual control functions, then system requirements and requirements for sub-systems and equipment are also defined according to how they relate to functions performance.

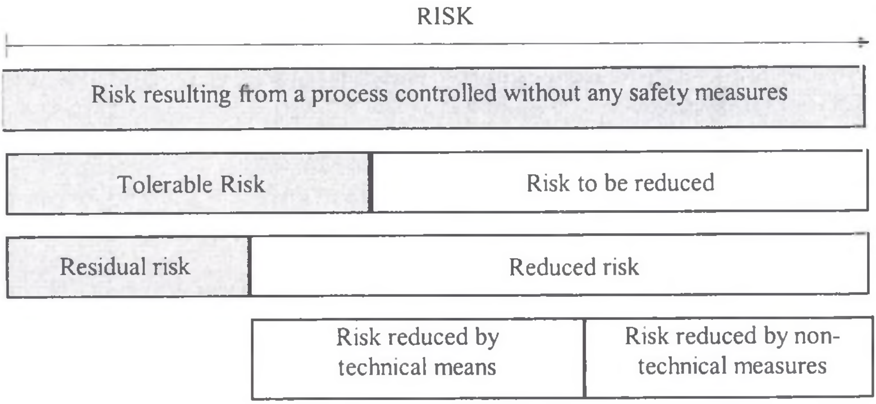
RISK
Risk resulting from a process controlled without any safety measures
Tolerable Risk
Risk to be reduced
Residual risk
Reduced risk
Risk reduced by technical means
Risk reduced by non-technical measures

Fig.2. Risk reduction

Relationship between acceptable risk and risk to be reduced is shown in Fig.2. Ris can be reduced by a proper technical solution or by using other means and procedues (e.g. organisational measures). Residual risk represents hazard rate and must be lower orequal to tolerable risk. Designing a safety-related system one must know both its safety reqtrements and methods and measures to realise them. A set of technical and non-echnical (organisational) measures corresponding to each level of safety must be fulfilled tcperform considered activity with risk lower or equal to tolerable risk. Technical and non-echnical measures can complement or partially substitute one by another. However, preset traffic control systems are designed to have the highest safety integrity level (SIL). This aproach to safety requirements definition is quite conservative but by no means is primary cntrary to safety requirements of railway transport. The fact is that safety-related systems (or teir parts at least) for some applications are unnecessarily over-dimensioned and thus cost less ffective. The whole process from risk analysis to system requirement specification is depictedn Fig.3.

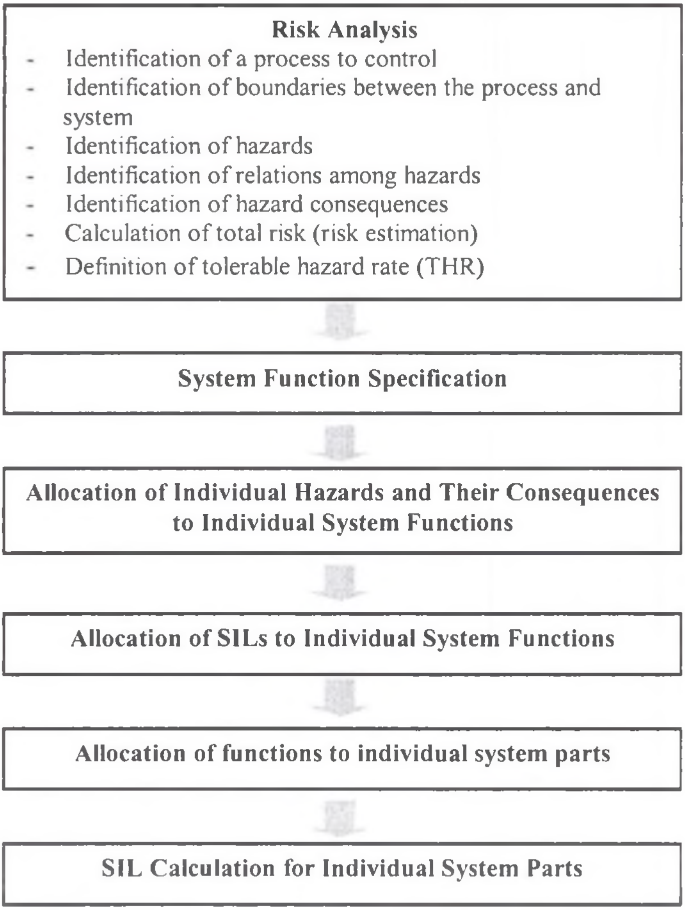
Risk Analysis
- Identification of a process to control
- Identification of boundaries between the process and system
- Identification of hazards
- Identification of relations among hazards
- Identification of hazard consequences
- Calculation of total risk (risk estimation)
- Definition of tolerable hazard rate (THR)
System Function Specification
Allocation of Individual Hazards and Their Consequences to Individual System Functions
Allocation of SILs to Individual System Functions
Allocation of functions to individual system parts
SIL Calculation for Individual System Parts

Fig.3. Process from risk analysis to system requirement specification

3. SYSTEM REQUIREMENTS SPECIFICATION

System requirements specification is one of the most important activities in development of a safety-related system. It is an obligatory document concluded between a supplier and a customer. System specification represents one of basic documents the system development is based on. It must be:

- Unambiguous;
- Understandable;
- Complete;
- Consistent;
- Verifiable.

There is a recommendation to create a model that makes testing complexity and soundness of specification possible and that helps to remove potential „white spaces" or inconsistencies in informal specifications. Natural languages and other informal notations are generally seen to have a lot of disadvantages if used for technical descriptions. Using these notations there is a problem to make specification with required level of accuracy in such a way that it could be uniquely transformed to system software or hardware solutions. A system model based on the use of semi-formal and formal methods (usually supported by suitable software tools) helps to create complete, unambiguous and logical descriptions of system functionality [10], [11]. This way of modelling is time-consuming; therefore such methods and procedures must be chosen in order to make a model directly usable in next phases of system life-cycle (e.g. for partial or complete code generation). For this purpose object oriented modelling (*OOM*) can successfully be used. One of the most suitable object oriented techniques that can be used to create a model is the *UML (Unified Modeling Language)*. It is the best-known and most spread standard of object modelling language that is supported by growing number of software tools (e.g. Rhapsody by I-Logix, Rose by Rational Software etc.) providing capabilities of direct and/or reverse engineering, model animation etc. [7], [9]. Contributions of applying *OOM* to the field of safety-related systems design can be seen as follows:

- Unification of principles and procedures of document preparation;
- Simplification of software design process;
- Creating a suitable environment for communication among development teams, subjects active in the process of system verification, validation, acceptance etc.

Since functional safety of the system will noticeably be based on the used tool and its outputs, its selection must be consulted with relevant safety authority.

Indicated approach to system design significantly makes process of system design, development and approval more effective and increases its quality in accordance with requirements included in European standards for railway applications. Errors caused in the phase of specification are often detectable as late as when integration tests are performed. Error is a deviation from the intended design, which could result in unintended system behaviour or failure. If no errors are detected by tests before putting the system into operation, existing errors can cause occurrence of systematic failures. To remove them, supplementary and usually high costs are required.

4. STRUCTURE SELECTION

Railway signalling systems can be characterized by long life time (15-20 years) and by relatively high costs spent on development in relation to a number of applications (especially for safety reasons). For that reason it is necessary to note that the system may not become outdated before putting it into operation or during first years of production (development process and process of approval usually lasts several years but technology development in the field of semiconductor elements is very fast). On the contrary, just safety requirements represent the main reason for applying a conservative approach to selection of proper technology. It must be based on components (and tools) whose features were sufficiently proved in operation of other applications (not necessarily safety-related ones) and positive and/or negative references are available. The use of modules with exactly defined interfaces can solve future problems resulting from conservative approach to selection of system elements.

It is necessary to ensure that the system/sub-system/equipment meets its THR in the event of single random fault. It is necessary to ensure that SIL 3 and SIL 4 systems remain safe in the event of any kind of single random hardware fault, which is recognised as possible. Faults whose effects have been demonstrated to be negligible may be ignored. This principle, which is known as fail-safety, can be achieved in several different ways [3]:

- Inherent fail-safety;
- Reactive fail-safety;
- Composite fail-safety.

Each of given techniques requires a specific procedure in system design and safety proof. Whichever technique or combination of techniques is used, assurance that no single random hardware component failure mode is hazardous shall be demonstrated using appropriate structured analysis methods.

Majority of railway signalling systems is based on inherent fail-safety. For these systems it is typical that required functions are realised by single functional units with assumption of no occurrence of hazardous state during system operation (it does not mean impossibility of its occurrence). Logical functions are usually realised by specially constructed components (special safe relays, safe logical elements, etc.) with asymmetric fault occurrence. In case of a fault their outputs always get to a pre-defined logical states. As an example of a typical system using principles of inherent fail-safety we can mention a relay-based interlocking system.

Standard electronic elements and computer components have symmetric fault occurrence (output change from logical "0" to logical "1" due to fault of a logical element is approximately as probable as output change from logical "1" to logical "0"). Thus safety-related systems based on processor technique cannot use principles of inherent fail-safety as a basic way of reaching fail-safety. Instead of using special components there is a trend to base system development on commercially available components (*COTS – Components of the Shelf*).

Technique of reactive fail-safety allows a safety-related function to be performed by a single item, provided its safe operation is assured by rapid detection and negation of any hazardous fault (for example, by encoding, by multiple computation and comparison, or by continual testing). Although only one item performs the actual safety-related function, the checking/testing/detection function shall be regarded as a second item, which shall be independent to avoid common-cause failures. Functional check of an interface between a control unit and a controlled process is based on comparison of the output signal of the control unit and the feedback signal informing on states of controlled objects (necessity of a feedback). Using reaction fail-safety in railway signalling systems is not typical.

To improve reliability or safety characteristics of safety-related systems concept of redundancy is used to react "somehow" to faults. From this point of view redundancy can be used for:

- Fault detection;
- Fault masking;
- Fault negation.

With technique of composite fail-safety, each safety-related function is performed by at least two items. Each of these items shall be independent from all others, to avoid common-cause failures. Non-restrictive activities are allowed to progress only if the necessary number of items agrees. A hazardous fault in one item shall be detected and negated in sufficient time to avoid a co-incident fault in a second item. Railway applications typically use systems with:

- ❑ Two-channel structure and comparison (also known as „2 out of 2" systems);
- ❑ Three-channel structure and voting (also known as „2 out of 3" systems).

Generally systems may have identically solved channels (the same hardware and the same software) or channels solved in a different way.

The choice of structure in systems with composite fail-safety is very important affecting safety and reliability targets. A proper structure results from a compromise between the cost of the system on one side and system integrity and availability on the other side.

5. FAILURE MODES AND EFFECTS ANALYSIS

According to the standard [3] safety case must be elaborated for any safety-related system. As far as its form is concerned it must be transparent and checkable by relevant safety authority or assessment body. Safety case must give evidence that the system fulfils system requirements specification. In a case of failure occurrence the system must react in an exactly defined way to avoid hazardous situations in railway traffic.

Known attributes of failures and faults make basic assumptions for taking measures against their occurrence and for negation of their effects. There is necessity to know, where, when and which failures can occur, what are their causes and consequences. From this point of view failures in electronic safety-related systems may be classified to:

- Systematic failures;
- Random failures;
- Failures caused by environmental conditions;
- Failures caused by inadequate manipulation.

Failures caused by inadequate manipulation. They can be caused by ignorance, unaccountability or mistake made by the staff during installation, operating, maintenance or reparation. Intentional failures are excluded from safety considerations. Failures caused by inadequate manipulation rise both before and after putting the system into operation.

Systematic failures. They exist in computer system components from starting their operation. They go unnoticed for quite a long time and occur only under certain operational conditions. They can originate from both hardware and software. Hardware failures can be caused by logical masked faults of integral circuits, defective manufacturing (short-circuits, interruptions, other defects) and installation, inadequate use of components etc. Software failures are caused by human mistakes when programming and programme implementing, or result from incomplete, inexact or incorrect system requirements specification. Software is not subject to mechanical wear; therefore software failures are exclusively systematic failures. Faults causing systematic failures occur especially in the period before putting the system into operation.

Systematic failures do not occur due to ageing the system, their occurrences results from a specific situation and system conditions. To analyse effects of systematic failures qualitative methods are usually used because quantitative analysis needs information on type and parameters of distribution of systematic failure occurrence. This occurrence can be reduced to a tolerable value [2], [3] by consistent application of analytical methods within system development.

Failures caused by environmental conditions. They are caused by noisy effects of operational environment of the system (heat, electromagnetic, mechanical, chemical etc.) but also by influences from other systems. These effects can have temporal consequences (disturbance) or permanent consequences (destruction). External effects can generally be characterised as n-dimensional random process with time-dependent random quantities (temperature, voltage, electromagnetic interference etc.) of n-dimensional random vector. Assessing effects of such a random process on operation of the safety-related system is possible provided that we know its marginal, binding and conditional characteristics. This complex task belongs to the field of mathematical statistics. Data analysis must result in identification of a process and making prognosis for whole useful life of the safety-related system. External effects also depend on a specific operational environment of the system (local conditions). For time and cost reasons the whole analysis of external effects cannot be performed individually for each operational environment.

In real life it is acceptable that system requirements specification defines limit values of monitored random variables and such technological and circuitry solutions (barriers) are used that make full or partial ignoring external effects possible. However, operational environment must be chosen in accordance with system requirements specification. Such a solution will exclude possibility to break mutual independency of system elements (in the sense of failure occurrence) by acting of external effects. External effects usually cannot be ignored in data transmission [4], [5].

Random failures of hardware. They occur due to ageing of the system after putting it into operation. Ageing process can be described as failure occurrence in a given time period [8]. Let the system structure contains n mutually independent elements and let the process of structure ageing is characterised as n-dimensional random process with time-dependent random quantities of n-dimensional random vector. The i-th random item of the random vector represents failure-probability density of the i-th element of the structure.

Failure detection has a key importance for assurance of the required level of system safety. Let there is n-dimensional random quantity with random vector $\boldsymbol{T}=\{T_1,T_2,...,T_n\}$ and distribution function (joint distribution function) of the random vector $\boldsymbol{T}$

$$F_{(t_1,t_2...,t_n)}=P_{(T_1\le t_1,T_2\le t_2,..T_n\le t_n)} \tag{1}$$

Let the random vector $\boldsymbol{T}$ has continuous type distribution, then

$$f_{(t_1,t_2...,t_n)}=\frac{\partial^n F_{(t_1,t_2...,t_n)}}{\partial t_1....\partial t_n} \tag{2}$$

where $f_{(t_1,t_2,\dots,t_n)}$ is probability density (joint probability density) of the random vector $\boldsymbol{T}$.
Probability that the vector $\boldsymbol{T}$ occurs in the n-dimensional space (that is bounded by inequalities $a_1 \langle T_1 \leq b_1, \dots, a_n \langle T_n \leq b_n$) is

$$P_{(a_1 \langle T_1 \leq b_1, \dots a_n \langle T_n \leq b_n)} = \int_{a_1}^{b_1} \dots \int_{a_n}^{b_n} f_{(t_1,\dots,t_n)} dt_1 \dots dt_n \tag{3}$$

Let detection-and-negation mechanism works as follows: if failure was detected at time interval $\langle (k-1)t_0, k\,t_0 \rangle$, in the end of this interval the system gets into the pre-defined safe state; if no failure was detected at time interval $\langle (k-1)t_0, k\,t_0 \rangle$, the system goes on failure-free (where k = 1, 2, 3, ...). From safety point of view probability of hazardous state of the system at this time interval must be known. If n-dimensional random quantity with time vector $\boldsymbol{T} = \{T_1, T_2, \dots, T_n\}$ has continuous type distribution with joint probability function $P_{(T_1=t_1, T_2=t_2 \dots T_n=t_n)}$, then conditional probability of element failure occurrence for all n elements at time interval $(t, t + t_0\rangle$ under condition that no element failure occurred to time t is

$$P_{(t\langle T_1 \leq t+t_0, t\langle T_2 \leq t+t_0, \dots, t\langle T_n \leq t+t_0 | T_1 \rangle t, T_2 \rangle t, \dots, T_n \rangle t)} = \frac{P_{(t\langle T_1 \leq t+t_0, t\langle T_2 \leq t+t_0, \dots, t\langle T_n \leq t+t_0, T_1 \rangle t, T_2 \rangle t, \dots, T_n \rangle t)}}{P_{(T_1 \rangle t, T_2 \rangle t, \dots, T_n \rangle t)}} = \frac{P_{(t\langle T_1 \leq t+t_0, t\langle T_2 \leq t+t_0, \dots, T_n \rangle t)}}{P_{(T_1 \rangle t, T_2 \rangle t, \dots, T_n \rangle t)}} \tag{4}$$

Calculated values must relate to the whole system and resulting value of probability of unwanted event occurrence (value of probability of a system hazardous state) must be confronted with the required value from risk analysis.

One of the most popular and successfully usable techniques of safety analysis is fault tree analysis (FTA). FTA is a deductive analysis method aimed at exact finding of causes or combinations of causes that can lead to occurrence of a defined top event. The top event can represent hazardous conditions or inability of the system to operate. Construction of the fault tree begins with definition of the top event as output of the top gate. Output events of gates situated on lower levels represent possible causes and conditions of top event occurrence. Each input event of the gate on a higher level can become an output event of the gate on a lower level.

Fault tree analysis can be both qualitative (logical) and quantitative (numeric). Qualitative analysis is used to find out mutual relations among primary events or relations between the top event and primary events. If the fault tree contains n primary events and u_i is the indicator of the i-th primary event (i = 1, 2, …, n), then relationship between primary events of the fault tree and the top event can be described by logical function

$$\psi(\mathbf{u}) = \coprod_{j=1}^{m} R_j(\mathbf{u}) \tag{5}$$

where $R_j(u)$ is logical function of the j-th minimal cut and $\boldsymbol{u} = (u_1, u_2, \dots\, u_n)$ is vector of primary events.

Quantitative analysis aims at calculation of probability of top event occurrence or occurrence of a set of events. Results of numeric analysis also support and supplement results obtained by logical analysis. To make numeric evaluation of fault trees possible, probabilities of failure occurrences on the level of system elements must be known and from them derived probabilities of primary event occurrences at considered time interval. Event occurrence can be seen as a phenomenon. Generally if phenomena A_1, ... A_n:

- are mutually dependent then probability of their conjunction is

$$P_{\left(\bigcap\limits_{i=1}^{n} A_i\right)} = P_{(A_1)} . P_{(A_2|A_1)} . P_{(A_3|A_1A_2)} \dots P_{(A_n|A_1A_2 \dots A_{n-1})} \tag{6}$$

- are not mutually exclusive, then probability of their disjunction is

$$P_{\left(\bigcup\limits_{i=1}^{n} A_i\right)} = \sum_{i=1}^{n} P_{(A_i)} - \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} P_{(A_i \cap A_j)} + \sum_{i=1}^{n-2} \sum_{j=i+1}^{n-1} \sum_{k=j+1}^{n} P_{(A_i \cap A_j \cap A_k)} \dots + (-1)^{n-1} P_{\left(\bigcap\limits_{i=1}^{n} A_i\right)} \tag{7}$$

- are mutually independent then probability of their conjunction is

$$P_{\left(\bigcap\limits_{i=1}^{n} A_i\right)} = \prod_{i=1}^{n} P_{(A_i)} \tag{8}$$

- are mutually exclusive, then probability of their disjunction is

$$P_{\left(\bigcup\limits_{i=1}^{n} A_i\right)} = \sum_{i=1}^{n} P_{(A_i)} \tag{9}$$

If primary events are statistically independent and probabilities of their occurrences are known then probability of top event occurrence will be determined as a consequence of occurrences of primary events of the minimal cut R_j, using the equation

$$P_{(R_{j(u)}=1)} = P_{Rj} = \prod_{i=1}^{n} P_{(u_i=1)} \tag{10}$$

where $P(u_i)$ is probability of occurrence of the i-th primary event. Only those primary events are considered that are involved in the minimal cut R_j.

Since every minimal cut leads to top event occurrence, probability of the top event is

$$P_{(\varphi_{(u)}=1)} = 1 - \prod_{j=1}^{m} \left[1 - P_{Rj}\right] \tag{11}$$

if individual minimal cuts are statistically independent. In the case of statistical dependency of cuts the equation (7) for full probability must be used to calculate probability of top event occurrence.

6. CONCLUSIONS

Communication is the most important aspect during the entire process of system development. This holds good not only for communication among individual members of developing teams but also for communication with the bodies responsible for safety approval or communication with a customer (if there is any known yet). Good communication is based on keeping documents in a good and workmanlike manner during entire system life cycle. Documents of poor quality make communication hard and can also become a source of errors and consequent hazardous failures. As a typical example we can mention changes made in the system (supplement to the specification, defects removal, improving a technical level of the system etc.). Slightest change if not included in documents can cause serious problems in future.

The paper was written under support of the Grant Agency of the Slovak Republic *VEG1*, Grant No. 1/1044/04 *Theoretical Apparatus for Implementation of e-Safety Principles to Intelligent Transportation Systems.*

BIBLIOGRAPHY

[1] EN 50 126: Railway applications: The specification and demonstration of dependability, reliability, availability, maintainability and safety (RAMS).

[2] EN 50 128: Railway applications: Software for railway control systems and protection systems.

[3] EN 50 129: Railway applications: Safety related electronic systems.

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

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

[6] KUNHART M.: Desing of Interlockings Rams Parameters. 11th International Scientific Conference, University of Žilina, Žilina 17-19 September 2003, pp.141-144.

[7] RÁSTOČNÝ K.; ZAHRADNÍK J.; JANOTA A.: An Object Oriented Model of Railway Safety-Related Control System. Scientific journal Communications No. 4/2002. ŽU in Žilina, pp. 32 - 39.

[8] RÁSTOČNÝ K.: Probability model of failure effects analysis. In: 4th international scientific conference ELEKTRO 2001, Section 2 & 3: Telecommunication systems and services & Control of Information and Safety Systems, 22 - 23 May 2001, EDIS Žilina, Slovak Republic 2001, pp. 84 – 89.

[9] ZAHRADNÍK J.; RÁSTOČNÝ K., JANOTA A.: UML - based Specification of a Railway Interlocking and Signalling System. International Workshop on Software Specification of Safety relevant Transportation Control Tasks, 23 - 24 April 2002, Braunschweig, pp. 131- 142.

[10] STOYTCHEVA N.; GEORGIEVA M.: Using of formal methods in railway safety-critical control systems. In: Proc. of the 13th International Conference of Higher School of Transport "T. Kableshkov TEMPT 2003-Transport on the XXI Century", Sofia, 2003.

[11] TARNAI G.; SÁGHI B.: Einsatz von Formalen Methoden in der Eisenbahnsicherungstechnik. In: Proc. of int. symposium ŽEL 2000, ŽU Žilina, 30-21 May 2000, pp. 80-88.

Reviewer: Ph. D. Jerzy Mikulski