SAFETY OF TRANSPORT PROCESS

J. Zahradník, A. Janota

Department of Control and Information Systems, Faculty of Electrical Engineering, University of Žilina, Univerzitná 8215/1, 010 26 Žilina, Slovakia, e-mail: jiri.zahradnik@fel.utc.sk, ales.janota@fel.utc.sk

Summary The paper deals with formulation of general rules and principles needed for ensuring safety of the transport process.

1. INTRODUCTION

When controlling some processes, the control system is required to behave in such a way that its failure must not cause endangering of human lives, environment damaging or other unacceptable consequences. Generally, such a process is called safety-related and a technical means performing a control law is called the *safety-related control system*. Therefore safety-related systems are required not only to realize correct functions but also to ensure safe reaction to failures. In case of failure occurrence such a control system must fully recover the original function with a defined probability, or impose limitations on its realization, or interrupt it in a pre-defined way. Control of all kinds of transport should be considered to be safety-related processes.

Every transport process requires a special sort of services that are provided through interconnection of humans, technical means and procedures. It is apparent, that quality of the transport process depends on human involvement in these services and human abilities, on quality of used technical means (especially of the safety-related control systems) and on quality of procedures utilized when providing services within the transport process.

Safety is one of the quality attributes of the transport process. The term "safety" should be taken in a relative sense. If the transport process is said to be safe, it does not mean "absolutely safe" but indicates such a level of safety, that meets defined safety requirements.

Safety of the transport process is ensured by a set of technical and organizational measures. However, human participation in control and supervision of the transport process increases the share of organizational measures for ensuring safety of this process. Practical experiences show that failure rate of failures caused by human mistakes is several order higher than failure rate of failures caused by technical means. It means that human involvement in control and supervision of the transport process has significant impact on its safety.

Safety of safety-related systems is based on applying adequate measures to avoid both human mistakes and random faults. Measures taken against human faults and random faults (including measures for fault negation) must be balanced to ensure required functioning of safety-related systems. For that reason four safety integrity levels (SIL 1 to 2) have been defined. They come up to probabilities that the system performs its safety-related functions with. We must be aware that strict requirements defined for safety-related systems and applied for instance in air and/or railway transport (SIL 4) are hardly provable by tests or practice results. For that reason producers of these systems must prove in a pre-defined way that required safety integrity level is reached and ensured.

This paper concentrates on formulation of general policies and principles of safety management of these transport processes based on performed analysis of air, road and railway transport processes.

From comparison of technologies applied in these kinds of transport the following differences have been identified:

- If a railway signalling system is in a free-failure state (normal operation), technical measures significantly prevail over organisation measures when ensuring operation safety (provided that relevant technical means are in free-failure conditions); if technical means in air transport are in a failure-free state, air traffic control is based on both human and technical system activity with considerable role of humans; in road transport organisation measures prevail over technical measures (applied mostly in crossroad signalling, motor-way traffic, road tunnel operation); i.e. safety of railway transport is also considerably influenced by humans. These conclusions could be supported by Table 1 stating death risk values for air, road and railway transport [4];
- Another differences result from a mode of operation: railway transport act in the high demand (continuous) mode operation, air transport and road transport in the low demand operation (this comparison is valid on the general level only).

Tab. 1. Travelling risks resulting from the use of different transport means

ACTIVITY	TYPICAL DEATH RISKS
Travelling by air	24×10^{-6} per year
Travelling by car	200×10^{-6} per year
Travelling by train	15×10^{-6} per year

Differences among air, road and railway transport make an impact on techniques and methods applicable when ensuring required safety.

Safety integrity against human mistakes is a unquantifiable part of safety integrity of transport process control that is closely connected with irreplaceable role of humans in control of some transport processes (typically in air and road transport) and with hazardous systematic failures of those hardware and software safety-related systems that control vehicle movements. Integrity against such failures can be reached mostly through organisation measures within quality management and safety management processes.

This implies that the purpose of quality and safety management is to reduce occurrence of human mistakes related to safety. This results in decreasing of the residual risk of occurrence of undesired hazardous events. Therefore, reducing a number of human mistakes related to safety must target the following activities: quality management, safety management of the life-cycle of a safety-related system, safety management of operation control (including the staff involved and actively participating in control and supervision of the transport process), safety management of driving transport means by drivers, safety management of transport under crisis situations.

2. QUALITY MANAGEMENT

The first condition to be fulfilled is: quality of the transport process is managed and will be managed through an effective quality management system (it means that the safety-related system also is managed and will be managed through an effective quality management system during its whole lifetime). Basic parts of the quality management system are:

- Quality planning – is aimed at definition of quality objectives and specification of necessary operational processes and related sources for meeting quality objectives;
- Quality management – is aimed at meeting quality requirements;
- Quality assurance – is aimed at confidence in meeting quality requirements.

3. SAFETY MANAGEMENT

The second condition to be fulfilled is: safety of operation management, safety of traffic management under crisis situation and safety of a safety-related system is managed and will be managed within an effective process of safety management. The safety management process consists of many phases and activities mutually interconnected in order to create a safe life cycle. The safety management process must be realized under control of a proper safety organization, employing competent persons having specific tasks. Assessment and documenting of employees qualification including their technical knowledge, competences, relevant experience and proper training must be performed in accordance with implemented standards and valid legislation. The use of this process of safety management is mandatory for safety integrity levels 1 to 4 including.

3.1 Safety Management of the Safety-related Systems Life Cycle

Safety management of the life cycle of a safety-related system ensures correct performing of procedures that are followed to enable identification and meeting of all safety requirements for such a system. The document specifying processes of safety management that should be applied for a particular system is called a safety plan. This plan must identify a structure of safety management, safety-related activities and must also involve requirements for revision of the plan in proper intervals.

3.2 Safety Management of Operation Control

Safety management of operation control is ultimate for safety of air transport. Principles of safety management are stated first to identify overall targets and practice of organisation in the safety area. These principles define a basic approach to organisation of safety management. Then, based on these principles, requirements must be specified to be fulfilled by the safety management programme. After definition of basic policies and principles another task of safety management is to prepare directives for their implementation to safety management process. Directives identify tasks that should be fulfilled to meet declared objectives and responsibilities must be assigned to perform individual tasks.

3.3 Safety Management of Transport Control under Crisis Situations

Management of systems under crisis situations is dealt with crisis management. Crisis management must plan needed operations for the case of potential occurrence of emergency situations (risk prevention and negation) as well as issue orders for operation management in the case of a real incidence. Crisis management defines basic procedures of a relevant organisation towards management of crisis situations. They represent miscellaneous oral or written orders, regulations and instructions. Their efficiency is limited, however, in the complex approach to solving safety tasks they are legitimate.

4. TECHNICAL SAFETY

The third condition to be fulfilled is implementation of such technical measures that will (together with other accepted measures) ensure required safe operation of a safety-related system.

Generally it is true that pre-production phases are dominant in ensuring safety of a safety-related system during its life cycle; i.e. requirements specification, suitable concept selection, design and development.

Technical safety of safety-related systems is made up of two components: functional safety and safety integrity. Functional safety is ensured through rigorous specification of all functions of a safety-related system supported by the use of formal and semiformal methods and proper tools that help not only with solving problems related to specification (its complexity and soundness) and coding but also with solving problems related to validation of designed SW solution.

Safety integrity is related to ability of a safety-related system to perform required safety functions and consists of two components: safety integrity against systematic failures and safety integrity against random failures.

Measures applied to ensure adequately safe control of transport process, i.e. intended safety integrity level (SIL), are depicted in Figure 1. This figure implies that it is necessary to ensure balanced quality management, safety management of the life cycle of a safety-related system, safety management of operation control and technical safety (technical measures). In this case safety integrity levels are used as means for harmonization of measures for prevention of systematic failures and human mistakes in the process of operation control (qualitative approaches) and measures taken to manage random failures (quantitative approaches).

From the safety viewpoint, driving a car by the human driver represents significant risk. Measures increasing vehicles safety are aimed at equipping a vehicle with driving assistance systems and smart systems for active safety. These systems consider not only a driver and vehicle, but also environment around the vehicle. Cooperation systems make exchange of basic safety information mutually between vehicles and between a vehicle and its infrastructure. Thus these systems will be capable of assessing a possible risk of accident. Then they may warn a driver in such a way that a driver can take necessary steps, or these steps may be initiated independently without human involvement. If an accident seems to be unavoidable, systems may utilise the same information for optimisation of passive safety systems. In this way risk of injury can be minimised. Systems of active safety may also automatically call for help.

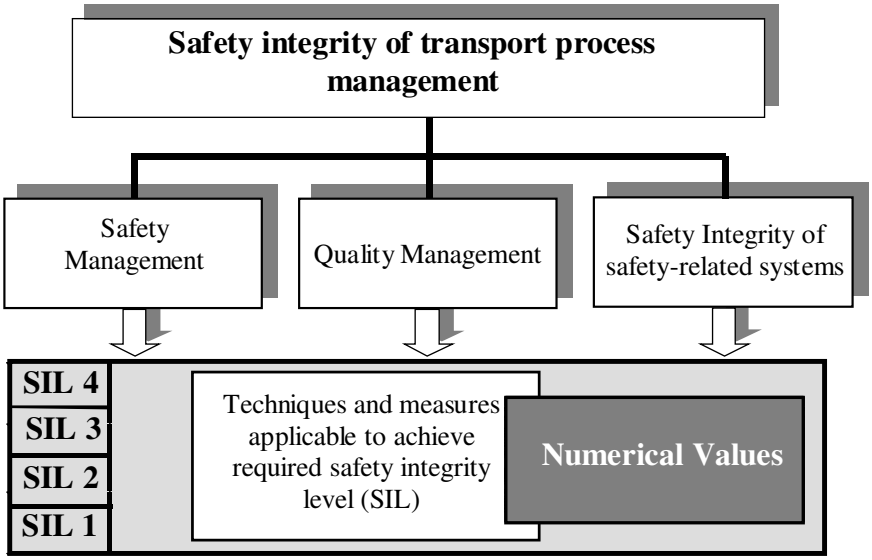

Fig. 1. Basic structure of measures applied to ensure required SIL of transport process

REFERENCES

[1] Zahradník, J., Rástočný, K., Kunhart, M.: *Bezpečnosť železničných zabezpečovacích systémov,* Monograph, EDIS Žilina, 2004

[2] STN EN 61508: Funkčná bezpečnosť elektrických / elektronických / programovateľných elektronických bezpečnostných systémov, 2002.

[3] Havel, K.: Manažment bezpečnosti, unpublished materials for the project VTP TaSID, Žilina, 2004.

[4] Melchers, R. E.: *Structural Reliability, analysis and prediction*. John Wiley & Sons, New York, 1987.