Functional safety of railway automation systems :methods and models

E. N. Rozenberg,

I. B. Shubinsky

Russian Research, Development and Planning Institute for Railway Information Technology, Automation and Telecommunication, Moscow, 2005

Monograph

The monograph contains analysis of today's theoretical and practical state of mathematical simulation of railway automation, remote control and telecommunication systems' functional safety as well as state of harmonization of the branch norms and regulatory documents in the field of functional safety according to relevant international standards.

The monograph contains proposals of strict and approximate graph-oriented Markov and semi-Markov methods of functional safety calculation and forecasting for sophisticated systems including recoverable systems with limited efficiency of supervision and latent failures. A set of functional safety models for single-channel and double-channel recoverable and non-recoverable systems with latent failures has been elaborated and investigated. Investigation has also included possibilities of channel restart in double-channel systems and devices in cases of channel failures and functional safety of double-channel recoverable devices limited efficiency of supervision and restartable channels.

Structural principles of multilevel safe systems consisting of non-safe components and a set of functional safety models for multilevel systems have been developed. The states have been determined, when the multilevel systems give a large gain in safety as compared with initial systems.

The monograph contains proposals concerning a technology for complex estimation of the system's functional safety including accelerated field tests and harmonization of the branch normative base according to relevant international standards.

Reviewed by: Mr. D. V. Shalyagin, D-r of Technical Sciences,

Mr. A. Ya. Kalinichenko, D-r of Technical Sciences.

CONTENTS

Introduction

Modern railway is a complex transport system having clear hierarchical structure including many (interconnected) interoperating and interdependent subsystems. Specific functional tasks of the components are submitted to the general purpose of the system’s functioning, i. e. passenger and freight transportation.

The technology of passenger and freight transportation is a process having the highest responsibility for safety of human life, of equipment and goods, and of the environment. Any deviation from normal operation may lead to consequences of different severity. In such a case the assurance of train traffic safety becomes an actual problem. Therefore it is necessary to consider processes of passenger and freight transportation and processes of train traffic safety assurance in their inseverable interconnection as an indivisible global target function of a railway transport system.

Efficiency of the way by means of which this main task of the railway transport system can be fulfilled depends on many factors. Main factors can be determined by internal conditions of the railway transport system:

- Technical equipment state of each subsystem (service).
- Functional efficiency of technical equipment.
- Reliability of technical equipment.
- Functional organization of each subsystem (service).
- Level of professional training of operators of the subsystem (service).
- Psychophysiological condition of the operators (dispatcher, locomotive driver etc.).
- Discipline of the operators.
- Function quality supervision of subsystems (services) and of the entire system.

In general, it can be said that efficiency and safety of train traffic are determined by the state of technical equipment (in our case we have to consider not only characteristics of reliability in wide sense but also technical solutions development level) and by the grade of efficiency of «man - technical equipment» interoperation during all phases of the system’s lifecycle.

Technical devices ensuring train traffic safety which form a part of the railway transport system are first specific means having been introduced practically simultaneously with appearance of the railway by itself. Now main technical means ensuring train traffic safety are so called railway automation and remote control systems.

At the present time, the existing railway automation and remote control systems are greatly obsolete. Modernization of them basing on standard methods leads to significant and non-justifiable expenditures, giving only small grade of safety increase and having long repay times. It can lead, also, to degradation of personnel qualitative and quantitative level, and, consequently, to increase of the human factor role. The situation becomes also more complicated due to growth of vandalism.

Existing tendency to improve the efficiency of train traffic control by increasing a length of train dispatcher sections leads to definition of new requirements to grade of control and management automation which must provide necessary throughput and safety of the train traffic. Therefore, the approach to development of railway automation and remote control systems must transit from equipment with local functions (electric interlocking, centralized traffic control (CTC), automatic block system etc.) to integrated (in sense of technology) systems of train traffic control and management including shunting and hump-yard operations.

To obtain efficient train traffic control at the railways, the management structure is to be improved aiming at reduction of costs and ensuring required train traffic safety level. Construction of digital telecommunication networks (Fig. 1) and introduction of new information technology along with centralization of dispatcher control functions has allowed to change the control and management system and to enhance its functions. Microprocessor-based railway automation and control systems have created the possibility of real-time working thus increasing the efficiency of the entire transportation process. Implementation of complex reconstruction projects of railway lines in Russia as well as of international projects requires not only use of traditional railway automation and remote control systems to increase safety, but also to involve additional resources based on information technology and digital telecommunication networks.

In this context main purpose of the present work is development of scientific and practical basis for increase of functional efficiency and safety of train traffic using a multilevel system for control and safety provision, including composite devices and subsystems which are inhomogeneous from safety point of view as well as increase of efficiency and cost-effectivity of methodological and technical solutions ensuring increase of functional safety of complex reconstruction projects for specific railway sections. The research tasks are formulated for a railway automation, remote control and telecommunication system including locomotive on-board automation equipment.

The structure of the present research work has been determined by these tasks. The monograph comprises introduction, five chapters and conclusion. Bibliography lists are given at the end of the book.

Chapter 1 is devoted to solution of problems concerning analysis of state and assurance of functional safety in railway automation, remote control and telecommunication systems. This chapter contains basic terms and definitions used in the field of functional safety and considers various aspects of assurance of functional safety in railway automation, remote control and telecommunication systems along with analysis of their influence upon cost-effectiveness of automation, remote control and telecommunications services as well as of control of rolling-stock.

Methods of functional safety probabilistic analysis of hardware are also dealt with in this chapter. Analysis of possibilities and limitations of these methods used for estimation of reliability and safety of railway control systems is also considered.

This chapter deals with state of the branch normative base concerning functional safety and harmonization according to international standards.

Chapter 2 deals with elaboration of practical engineering methods of calculation and forecasting of functional safety and reliability parameters applied to recoverable systems and devices of railway automation, remote control and telecommunication whose behaviour is determined by Markov as well as semi-Markov random processes. Several methods are proposed for calculation of functional safety and reliability parameters of various systems and devices of railway automation, remote control and telecommunication including operational (service) data networks and digital radio communication systems, namely the graph semi-Markov calculation method and approximate graph semi-Markov calculation method based on approximate calculation of graph decomposition weights as well as approximate method based on T-transformation. This chapter contains generalized formulas and algorithms for above mentioned methods intended for computer calculations using standard procedures of path and contour search on graphs.

Chapter 3 is devoted to elaboration of functional safety models for microprocessor-based railway automation, remote control and telecommunication systems, by means of which formulas of stationary probabilistic and time safety and reliability parameters of single-channel recoverable devices with embedded hardware supervision were obtained. This chapter contains grounds of recommendations concerning efficiency and volume of supervisory equipment whose fulfilment ensures nearly optimal reliability and functional safety parameters of recoverable devices with latent failures. Functional safety models of double-channel devices with equivalent failures both with and without channel restart have been built and investigated. Restart of individual channels in double-channel railway automation, remote control and telecommunication systems for recovery of their working state is shown to be necessary and possible. The example of the «FSS» device (a computer device generating locomotive control commands based on signal aspects at high-speed railway lines) allows to show that use of channel restart makes it possible to reach a velocity of trains twice or more than without channel restart or with limited number of restart procedures. Much importance in this chapter is given to problems concerning elaboration of a system of information security parameters and of composite parameters of functional safety and information security of railway automation, remote control and telecommunication systems.

Chapter 4 contains definitions and formulations of multilevel safety assurance principles, structural concept of multilevel automatic train traffic control and safety assurance system (MS), definition of requirements to the structure of MS and proposal of the MS structure diagram. This chapter contains also investigation of conditions ensuring efficiency of multilevel protection and proposal of rational architecture of the MS.

Chapter 5 is devoted to investigation of problems concerning improvement of normative documents concerning functional safety of production process control. A variant of selection of an analytic method of functional safety proof of the system being designed is proposed along with elaboration of a complex approach to rational usage of analytic and experimental methods of safety proof including integration of inhomogeneous information.

An analysis is given of methods allowing to accelerate functional safety tests of systems along with proposal of accelerated field tests. Practical steps to implement accelerated field tests of sophisticated hardware/software complexes are described.

This chapter contains research results concerning elaboration of safety norms and standards for railway automation, remote control and telecommunication systems in accordance with requirements of CENELEC standards.