Mechanics Transport Communications
Academic journal

ISSN 1312-3823
issue 3, 2011
article № 0526
http://www.mtc-aj.com

MODELLING SAFETY AND SECURITY OF RAILWAY TRANSPORTATION PROCESS

Margarita Peltekova
mpeltekova@hotmail.com

Assistant Professor, MSc.-Math, University of Transport, Sofia, 158 Geo Milev
BULGARIA

Abstract: *Safety of the railway transport has been the major concern of the railways since they exist. The security of the railway transport is a new request faced with attacks against passengers, goods or environment. A problem of safety can be due to technical failures or unintentional human behaviour. A problem of security is always due to a negative willing of human factor. The safety cause is internal and the security cause is external to the railway process. In this paper we have presented an approach for quantitative assessment of security attributes for an railway system. A state transition model that describes the dynamic behavior of such a system is used as a basis for developing a stochastic model. This is a generic model that enables the study of different impacts of a human-operator unintentional errors and intentional security attacks. Several general probability distribution functions can be used to describe the attacker behavior and t solve the proposed Semi Markov Model for safety and security related attributes.*
Keywords: *Modeling Railway Safety, Security, Human factor*

INTRODUCTION

Hardware or software failures experienced by a railway system are almost invariably accidental system failures. Such failures are caused either by the design faults, physical wear and tear, and environmental conditions. In contrast, security intrusions are caused by deliberate human actions. It is, however, quite possible that a security intrusion may manifest itself as a failure.

Railway Control System configurations varied considerably depending on control system functionality. In all cases, the architecture and boundaries of the systems are widely distributed. Complex nature of railway control systems requires assessment of safety and security of such systems to consider system configuration, system vulnerabilities, as well as common factors influencing safety and security of the transportation system/process, such as intensity of the train traffic movement, environmental conditions, human factors and natural phenomena.

Railway systems are easily accessible and vulnerable. As a result, these systems have become prone to security intrusions. The range of security intrusions may vary from minor mischief to criminal intent for stealing or destroying systems' components. This has brought security attribute of a system to the forefront of system safety and security specifications.

It is imperative for well-designed safety-critical railway systems to meet certain requirements, such as reliability, availability, safety and security. Therefore, we need to quantify security attributes so that a railway system may be able to meet specified levels of security. Reconfiguring a system after a security attack is one possible solution to system design concepts.

GENERAL CONCEPT FOR MODELING SAFETY AND SECURITY OF RAILWAY TRANSPORTATION PROCESS

Railway transportation process is predicated upon the behavioral states of the railway system technical devices, humans involved or not involved in the process, working environment and natural phenomena. Safety and security of the transportation process can be violated from inappropriate human action, environment and unsafe failure of the technical device.

However, human errors/violations cannot create unsafe state if the system is working properly and is protected properly. They influence the transportation process when maintaining (the system is in fail-safe state), when the system is in dangerous state and human errors occur or when there is intentional human security attack, which aims at destroying the system or its components.

The proposed model in this paper represents the railway devices' states, giving the probability of unsafe system states due to technical device failures and due to human factor (Figure 1). For the model to be accurate, it is important to estimate accurately the model parameters i.e., mean sojourn times and the transition probabilities. In this paper, however, the focus is primarily on developing a methodology for analyzing quantitatively the security attributes of a railway system rather than accurate model parameterization.

For the model to be accurate, it is important to estimate accurately the model parameters i.e., mean sojourn times and the transition probabilities for every state of the transportation process.

The proposed model gives two dangerous system states – probability of unsafe human behavior P3 and well-known probability of dangerous failures of the railway system - P4.

For the probability of unsafe human behavior (P3) are considered not only the human errors during maintenance but also intentional workforce, vandalism and unreasonable imprudent unsafe human behavior during working conditions of the system.

Figure 1 represents the states of our model, and the arcs represent state transitions. Each system device is denoted by states: S = (W, P2, P3, P4) including the situations that the device is properly working (P1), in fail-safe state (P2), in fail-dangerous state due to technical failure (P3), and fail-unsafe state due to human factor (P4), respectively. The system fails at rate λ and is repaired at rate μ. Transitions represented by dashed arcs represent the system states influenced by human factor.

The states of the transportation system can be described as follows:
P1 – System working, no violation on system safety-critical states.
P2 – System/human in fail-safe mode
P4 – System in undetected fail-dangerous state due to human violation.
P3 – Undetected fail-dangerous device failure
λ - Failure rate
μ - Repair rate
C - Coverage
Phe - Probability of human error
λDh - Human violation failure rate
μo - Repair rate after device fail-dangerous failure
μhr - Human error recovery rate
μr - Recover rate after fail-dangerous state

For the probability of unintentional errors of human/operator (dispatcher) on railway traffic control desk we assume: 1.10^{-2} - 1.10^{-3} (probability of correct operation: 0,8-0,95) and for λDh (unsafe human violation failure rate) – 10^{-3}-10^{-6}. [5]

For the probability of unintentional errors of human/operator (dispatcher) on railway traffic control desk we assume: 1.10^{-2} - 1.10^{-3} (probability of correct operation: 0,8-0,95) and for λDh (unsafe human violation failure rate) – 10^{-3}-10^{-6}. [5]

The probability of system being in a particular state can be found by solving the homogeneous differential equations that describe the Markov model below (Fig.1):

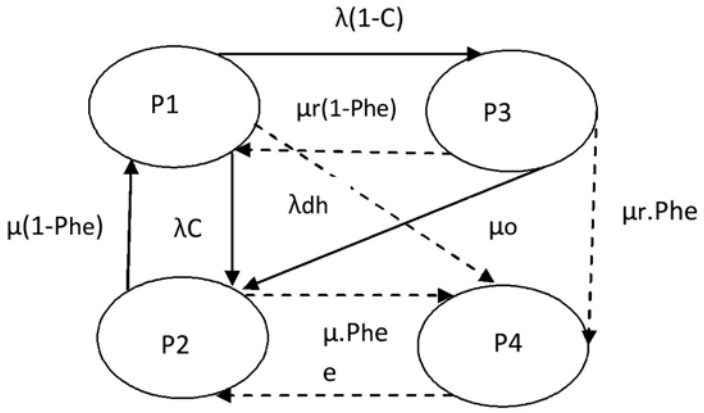

Fig. 1.

$$\frac{dP1(t)}{dt} = -(\lambda + \lambda dh)P1(t) + \mu(1 - Phe)P2(t) + \mu r(1 - Phe)P3(t)$$

$$\frac{dP2(t)}{dt} = \lambda.C.P1(t) - \mu.P2(t) + \mu o.P3(t) + \mu hr.P4(t)$$

$$\frac{dP3(t)}{dt} = \lambda(1 - C)P1(t) - (\mu o + \mu r)P3(t)$$

$$\frac{dP4(t)}{dt} = \lambda dh.P1(t) + \mu.Phe.P2(t) + \mu r.Phe.P3(t) - \mu hr.P4(t)$$

$$P1(t) + P2(t) + P3(t) + P4(t) = 1$$

For steady state probabilities we obtain:

$$P1 = \frac{\mu\mu hr((\mu o + \mu r)(1 - Phe)}{\mu\mu hr(1 - Phe)(\mu o + \mu r) + \mu hr(\lambda + \lambda dh)(\mu + \mu r) + \lambda(1 - C)\mu hr(1 - Phe)(\mu - \mu r) + \mu(\mu o + \mu r)(\lambda dh + \lambda Phe)}$$

$$P2 = \frac{\mu hr((\mu o + \mu r)(\lambda + \lambda dh) - \mu r\lambda(1 - C)(1 - Phe))}{\mu\mu hr(1 - Phe)(\mu o + \mu r) + \mu hr(\lambda + \lambda dh)(\mu + \mu r) + \lambda(1 - C)\mu hr(1 - Phe)(\mu - \mu r) + \mu(\mu o + \mu r)(\lambda dh + \lambda Phe)}$$

$$P3 = \frac{\mu\mu hr\lambda(1 - C)(1 - Phe)}{\mu\mu hr(1 - Phe)(\mu o + \mu r) + \mu hr(\lambda + \lambda dh)(\mu + \mu r) + \lambda(1 - C)\mu hr(1 - Phe)(\mu - \mu r) + \mu(\mu o + \mu r)(\lambda dh + \lambda Phe)}$$

$$P4 = \frac{\mu(\mu o + \mu r)(\lambda dh + \lambda Phe)}{\mu\mu hr(1 - Phe)(\mu o + \mu r) + \mu hr(\lambda + \lambda dh)(\mu + \mu r) + \lambda(1 - C)\mu hr(1 - Phe)(\mu - \mu r) + \mu(\mu o + \mu r)(\lambda dh + \lambda Phe)}$$

Given the steady-state probabilities, various measures, may be computed. The probability of P4 (Fig.1) gives the quantity value of the influence of human-factor (operator, maintainer, attacker) on the safety of the railway system.

In this paper we have presented an approach for quantitative assessment of security attributes for railway system. This is a generic state transition model that enables the study of impact of human error and security attack. Since the memory less property of exponential distribution implies the absence of aging and learning, it does not seem appropriate for modeling human behavior. One of the goals of our future work is to design and conduct experiments based on available statistical data.

These experiments should provide us with a better understanding of the human behavior; help us to refine its stochastic description and better estimates of the model parameters.

While the methods for quantitative assessment of dependability attributes such as reliability, availability, and safety are well established, so far the security attributes have been mostly assessed

It is possible to apply human error prediction and assessment methods at any type of technological process, however, there will always exist inevitable trade-offs between the accuracy and validity of predictions. In railway operation, several safety-critical tasks are assigned to the operators and are not controlled by signaling and interlocking systems. Many tasks are necessary in situations occurring very rarely. Train control systems have associated accident risks from non-human failures (i.e., mechanical, electrical, and electronic, materials) as well as they need to associate from not intentional or intentional human failures. Therefore, there is a need to develop an approach for assessing the human failures in train control systems of different types, and to be able to estimate the probabilities of these failures.

CONCLUSION

Train control systems have associated accident risks from non-human failures (i.e., mechanical, electrical, and electronic, materials) as well as they have to associate from human failures. Therefore, there is a need to develop an approach for assessing the human failures in train control systems of different type, and to be able to estimate the probabilities of these failures.

The aim of this work was to propose evaluation of dependability attributes of railway systems that are relevant to security.

REFERENCES:

[1] Jorge E. Núñez Mc Leod and Selva S. Rivera, *Human Error Management Optimization in CAREM NPP,* Proceedings of the World Congress on Engineering 2009 Vol I WCE 2009, July 1 - 3, 2009, London, U.K.

[2] L. Schnieder; E. Schnieder; T. Ständer, Technische Universität Braunschweig, Institute for Traffic Safety and Automation Engineering,, Langer Kamp 8, 38106 Braunschweig, Germany, Railway Safety and Security – Two Sides of the Same Coin? !

[3] A. Kumar, P. Sinha Mechanical Engineering Department, National Institute of Technology, India, Human Error Control in Railways.

[4] Andrew Rae, System Safety and Quality Engineering, 11 Doris St Hill End Queensland 4101

[5] Хр. Христов, Основи на осигурителната техника, София 1990, България

[6] L. M. Kaufman, Ted C. Giras, Simulation of rare events in transportation systems, Center of Safety-Critical Systems, University of Virginia,

МОДЕЛИРАНЕ НА БЕЗОПАСНОСТТА И СИГУРНОСТТА НА ЖЕЛЕЗОПЪТНИЯ ПРЕВОЗЕН ПРОЦЕС

Маргарита Пелтекова

Университет по Транспорта, София, Гео Милев 158
БЪЛГАРИЯ

Ключови думи: *безопасност на железопътната техника, сигурност на железопътния процес, човешки фактор*

Резюме: *Безопасността на железопътния превозен процес е основна грижа на железопътната осигурителна техника, от началото на нейното създаване. Оценката на сигурността и защитата на железопътния транспорт е нова необходимост, наложена като противодействие на зачестилите умишлени или неумишлени инциденти с пътници, товари или околна среда. Безопасността на железопътния транспорт може да бъде нарушена както от техническа неизправност на осигурителната система, така и от неумишлена човешка грешка. Сигурността на железопътния процес се нарушава в резултат негативна намеса на човешкия фактор. В настоящия доклад се разглежда един подход за оценка на безопасността и сигурността на железопътна осигурителна система. Предложен е математически модел на железопътната осигурителна система система, позволяващ оценка на влиянието на човешкия фактор върху безопасността и сигурността на железопътния транспортен процес.*

.