The FTTD Method Application to the Safety Analysis of Changeable Block Distance System

Jan Magott1, Andrzej Lewiński2, Piotr Skrobanek1, and Andrzej Toruń3

1 Wrocław University of Technology, Institute of Computer Engineering, Control and Robotics
Wybrzeże Wyspiańskiego 27, 50-370 Wrocław, Poland
{jan.magott, pawel.skrobanek}@pwr.wroc.pl

2 Technical University of Radom, Faculty of Transport & Electrical Engineering
Malczewskiego 29, 26-600 Radom, Poland
a.lewinski@pr.radom.pl

3 Railway Institute
J. Chłopickiego 50, 04-275 Warsaw, Poland
atorun@ikolej.pl

Abstract. The paper deals with the safety of a new train control method based on the Changeable Block Distance. Such method applies the open radio transmission standards including GPS and GSM-R for trains positioning, monitoring and controlling in a typical dispatcher area. The CBD method may be treated as a new technological overlay on classical train control systems, because it can improve the capacity of a railway line assuring the same, high level of safety (SIL4). The applied method of a Fault Tree with Time Dependencies allows to regard the time parameters of transmission connected with delays, interferences and interrupts together with reactions of the dispatcher system and of the railway staff. The results of the FTTD analysis confirm the assumed measures and suggest the trends in future applications of open transmission wireless standards in the railway control and management.

Keywords: Changeable Block Distance, Fault Tree with Time Dependencies, Safety of Railway Control and Management System.

1 Introduction

Traditional train monitoring system used FBD (Fixed Block Distance) rule of traffic control corresponding to sequential occupancy of insulated rail sections [4]. The FBD method requires the highest level of safety (SIL4) but has important limitation of railway line capacity. It is related to assurance of minimum length of block section necessary to breaking distance . (Technical implementation of the FBD rule does not require any additional track-train transmission systems (TTT class). This method allows the drive a train with maximum running speed to 160 km/h corresponding to correct interpretation of railway signaling system signals by the train driver. Therefore, higher running speed than 160 km/h require the use of additional TTT class systems, in which the information about actual allowed speed profile and free route
distance is passed directly to the driver’s cab as an MA (Movement Authority (– permission for a train to run to a specific location within the constrains of the infrastructure) on the DMI (Driver Machine Interface – device to enable communications between TTT system and the train driver).

For this purpose, a control systems TTT class: ATP – Automatic Train Protection, ATC - Automatic Train Control, ATO – Automatic Train Operation, assigned to safety SIL-4 level [7] for which according to the railway safety standards (EN-50129) must be analyzed with respect risk analysis. For this type of TTT class systems the methods such FTA (Fault Tree Analysis) and FMEA (Failure Mode and Effect Analysis) are recommended as standard methods of risk analysis [1, 2].

Currently used TTT class systems on Europe Railways, allow the safety drive a train with speed above 160 km/h, but still existing the FBD rule decreases the efficient management of trains. To improve the capacity of the railway line the CBD (Changeable Block Distance) rule can be used as an alternative method of safety time distance control base on the existing signaling track equipment. Implementation of the CBD rule proposed in the presented concept assumes data transmission between RBC (Radio Block Centre) and trains via open public radio network standards (GSM-R, WiFi, WiMax). The typical risk aspects such: delays, interferences, interrupts or integrity code faults in data transmission or unauthorized attempts of reception are required in safety data transmission procedures between RBC and communicating trains.

In this paper the influence of the mentioned transmission aspects for proper operation of CBD system is analyzed using the FTTD (Fault Tree with Time Dependencies) method.

2 Fault Tree with Time Dependencies

Fault Tree Analysis (FTA) is one of the most commonly used techniques for an analysis of safety systems. The technique involves an identification of dangerous situations, so called faults, and causes (events) that may lead to its occurrence. The faults are situations which directly, or through initiating sequence of events, may lead to an accident. FTA is a top-down approach [1, 2]. First, dangerous situations (faults) are identified in a system. Next, one fault tree (FT) for each of faults is constructed. Fault is the top-event. A next level of the FT is constructed using direct causes of the top-event. The top-event and its causes are connected using a logical gate, as will be shown. Then, in the same way, a next level of the FT is constructed (for causes of the causes of the top-event). The FT is finished on a specific level of details or on event for which we cannot or do not need to specify the reasons.

In contrast to the classical FTA, the Fault Tree with Time Dependencies Analysis (FTTDA) allow, additionally, for analysis of timing relationships between events, as will be shown in Chapter 4.

The time parameters determined usually by experts on basis of system construction (minimal and maximal period of time for opening a valve, for message sending etc.)