




Tolerable Hazard Rate Allocation for Urban Rail Automatic Train Control System

Xiaoqing Zeng¹, Yungen Fang¹, and Tengfei Yuan^{2,3}(✉) 

¹ The Key Laboratory of Road and Traffic Engineering, Ministry of Education, China, School of Transportation Engineering, Tongji University, 4800 Cao'an Road, Shanghai, China

² SHU-UTS SILC Business School, Shanghai University, Shanghai 201800, China
yuantengfei@shu.edu.cn

³ Shanghai Engineering Research Center of Urban Infrastructure Renewal, Shanghai 200032, China

Abstract. To improve the reliability and safety of urban rail Automatic Train Control System, it is Query ID="Q1" Text="As Per Springer style, both city and country names must be present in the affiliations. Accordingly, we have inserted the country name in the affiliation 2. Please check and confirm if the inserted country name is correct. If not, please provide us with the correct country name." necessary to allocate the tolerable hazard rate (THR) of the Automatic Train Control (ATC) system to each subsystems and components during the design and implement of specific urban rail transit signaling system. In the beginning, this research analyzes the architecture of ATC system, as well as safety functions and overall safety requirements for the urban rail transit signaling system. Next the specific requirements and principles of equal apportionment technique, safety impact-based apportionment technique and complexity-based apportionment technique are discussed. Combined with the ATC system architecture, safety logic model and specific engineering design parameters, these three safety allocation methods are used to allocate the THR to each subsystems of ATC as the requirements. At last, the comparison of allocation for these techniques shows that the allocation method based on system complexity is the most suitable for the actual conditions of the project, which can meet the requirements of the Urban Rail Automatic Train Control System. Therefore, this research is proved to be meaningful to improve the reliability and safety of urban rail transit to some extent.

Keywords: Automatic Train Control (ATC) · Tolerable Hazard Rate (THR) · Allocation method · Safety Requirement

1 Introduction

For the modern urban rail transit systems, in order to ensure safe operation of trains, Automatic Train Control (ATC) systems are used to implement the necessary safety functions such as train overspeed protection, maintaining train running intervals, and preventing train collisions. During the construction of an engineering projects, the rail transit systems owner or the operation manager will set a top-level safety requirement

for ATC system, a definitive Tolerable Hazard Rate (THR) value, and requires the final delivered ATC system to meet this targeted safety requirements. At current project practice, the typical urban rail transit Automatic Train Control system is a geographically distributed system, which distribute on the train, track, depot and operation control center, these distributed equipment in different locations cooperate with each other and work together to implement the function of train operation safety control.

However, the distributed Automatic Train Control system devices often come from different equipment suppliers or design institute. During the design and manufacturing process, only the safety requirements of a single device, such as Safety Integrity Level (SIL), Tolerable Hazard Rate (THR) and Tolerable Functional Failure Rate (TFFR) are concerned by the equipment suppliers or design institute. When integrating these devices into the train control system of an urban rail transit line without any unified safety requirements planning, allocation and coordination, the system safety performance achieved by the overall ATC system may not be able to meet the safety requirements set initially. In order to ensure that the final deliverable of overall ATC system of the rail transit line can meet the established safety requirements, the THR need to be allocated during the plan and design stages to guide the design and manufacture activities of individual equipment, which is necessary to ensure the project delivery meet the ATC system operational safety requirements.

2 ATC System Architecture and Safety Requirements

In general, the typical ATC system in current urban rail transit project adopts the communication-based train control (CBTC) system. The architecture and safety requirements of the CBTC system are analyzed as follows.

2.1 CBTC System Architecture and Safety Requirement

According to the definition from IEEE [1], the CBTC system is a continuous ATC system utilizing high-resolution train location determination, independent of track circuits; continuous, high capacity, bidirectional train-to-wayside data communications; and train-borne and wayside processors capable of implementing vital functions. The architecture with its subsystem location is shown in the Fig. 1.

In CBTC system, the Automatic Train Protection (ATP) maintains fail-safe protection against collisions, excessive speed, and other hazardous conditions through a combination of train detection, train separation and interlocking. Computer interlocking (CI) is the interface between CBTC and external trackside field equipment, which establishes the interlocking relationship between signals, switches and routes, in order to avoid the conflicting train operation routes to be set, and to prevent one resource from being occupied by two trains at the same time, both the ATP and CI are safety critical systems which usually meet the highest safety requirements (SIL4). The Automatic Train Operation (ATO) performs the functions of speed regulation, programmed stopping, door control, performance level regulation and other functions otherwise assigned to the train operator. Automatic Train Supervision (ATS) is the subsystem that monitors trains, adjusts the performance of individual trains to maintain schedules, and provides

data to adjust service to minimize inconveniences otherwise caused by irregularities. Both the ATO and ATS are safety relevant system which usually have the moderate safety requirements (SIL2).

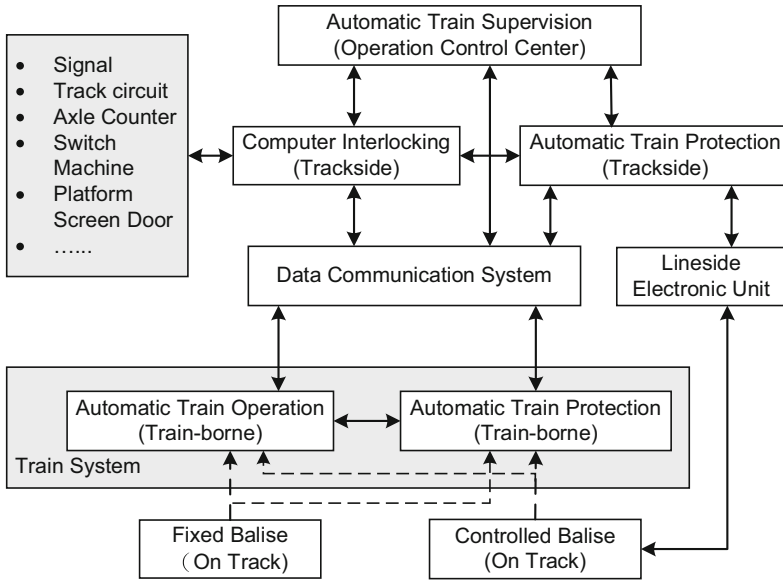


Fig. 1. CBTC system architecture and external interface

In addition to the ATP, CI, ATO and ATS systems, CBTC also includes Data Communication System (DCS) and Balise Transmission System. The DCS is to transmit bi-direction information transmission between trackside equipment and vehicle-mounted equipment. The Balise transmission system is divided into fixed Balise and controlled Balise. The fixed Balise is mainly used for train positioning and position calibration, and controlled Balise is used to transmit some variable temporary commands, such as speed limit information and route information. The external interfaces of the CBTC system include train, platform screen doors, platform emergency buttons, integrated supervision and control system and other systems. These external systems provide input to the CBTC system and execute the control commands issued by the CBTC.

2.2 CBTC System Safety Requirements

As shown in Fig. 2, the ATC system requirements can be divided into safety requirements and non-safety requirements. The safety requirements are derived from the hazard, which are measured via Tolerable Hazard Rate (THR) as the system top level safety goal. The functional safety requirement is part of the safety requirement, it is measured via Tolerable Functional Failure Rate (TFFR), the THR is derived from the TFFR. The functional safety requirements include safety functions and safety integrity, which use the Safety Integrity level (SIL) to define their requirement. The relation between the SIL

and TFFR is shown in Table 1. The SIL is the safety performance index used for the defined safety function. The SIL 4 has the highest level of safety integrity. For safety integrity, it includes the Systematic Failure Integrity and Random Failure Integrity and depends on the system design. The systematic failure shall meet the SIL requirement, and the Random Failure shall meet both the SIL and Failure Rate (FR) requirements.

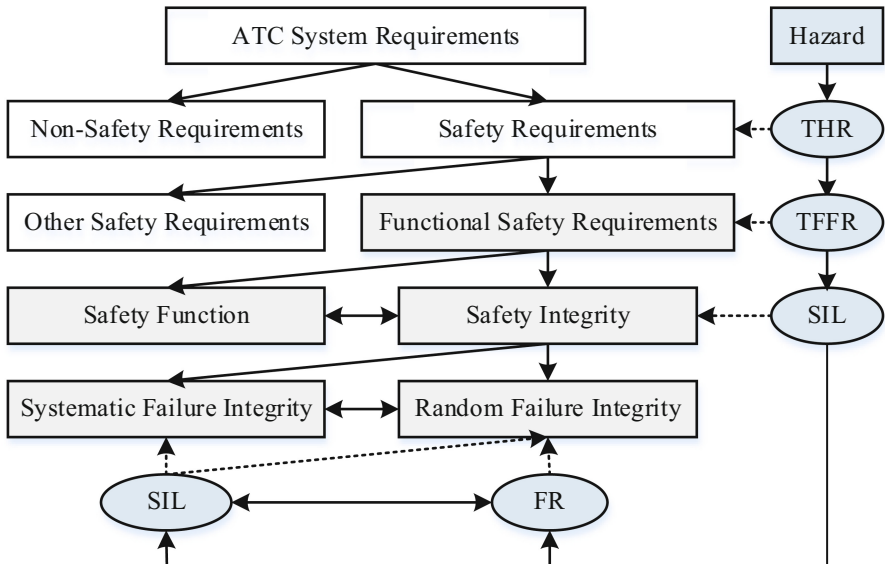


Fig. 2. System Requirements architecture and THR allocation process

In order to ensure the safe train operation, the ATC system shall implement the necessary safety function to prevent the hazard “exceeding speed and/or distance limits advised to ATC, and the THR to this hazard is $10^{-9}/h$, the relevant safety function can be decomposed to (1) ensure safe route, (2) ensure safe separation of trains, (3) ensure safe speed, (4) control acceleration and braking [2]. These functions shall meet the TFFR which is allocated from the THR, and if the equipment used to implement these safety function, the equipment should meet the relevant SIL and FR.

As a typical urban rail ATC system, it has following core safety functions: (1) Train location/train speed determination, (2) Safe train separation, (3) Overspeed protection and brake assurance, (4) Rollback protection, (5) End-of-track protection, (6) Parted consist protection and coupling and uncoupling of trains, (7) Zero speed detection, (8) Door opening control protection interlocks, (9) Departure interlocks, (10) Emergency braking, (11) Route interlocking, (12) Traffic direction reversal interlocks, (13) Work zone protection, (14) Broken rail detection, (15) Restricted route protections, (16) Level-crossing protection. These safety function should be implemented by trackside equipment Computer Interlocking (CI) and Zone Controller (ZC) and train borne equipment Onboard Controller (OC), that means the CI, ZC and OC shall meet the SIL 4 requirement with the THR less than THR is $10^{-9}/h$ [3].

Table 1. The correlation between SIL and TFFR

No.	TFFR per hour and per function	Safety Integrity Level
1	$10^{-9} \leq \text{TFFR} < 10^{-8}$	4
2	$10^{-8} \leq \text{TFFR} < 10^{-7}$	3
3	$10^{-7} \leq \text{TFFR} < 10^{-6}$	2
4	$10^{-6} \leq \text{TFFR} < 10^{-5}$	1

3 Safety Requirement Allocation Method

From the process of ATC system implement the safety control function, it shows that if any of the CI, ZC and OC failed, an accident may happen in the urban rail line, which will lead to the overall THR goal cannot be met. From the safety point of view, the CI, ZC and OC of the ATC system form a series system as described in Fig. 3.



Fig. 3. ATC system safety control logic model

As rail authority may only focus on the safety requirements of ATC system level but not the subsystem CI, ZC, and OC, but for subsystem manufacturers, the safety requirements of ATC system level need to be allocated to CI, ZC and OC subsystems. From the definition of safety requirements, the safety integrity level is divided into two parts: the non-quantifiable SIL and the quantifiable TFFR (FR). For various components that performs one safety function, if there is no redundancy, the components will directly inherit the non-quantifiable SIL from the system, that is, the SIL for CI, ZC, and OC subsystems are the same as the SIL of ATC system, and they are all SIL4 components. For the quantifiable part of the safety requirements, we need have allocation methods to allocate the ATC system THR and TFFR to CI, ZC, and OC and make sure the final total subsystem TFFR is less than the ATC system TFFR and the hazard THR, which is described in Eq. (1).

$$\sum_i^X TFFR_{Ci} + \sum_i^Y TFFR_{ZCi} + \sum_i^Z TFFR_{OCi} \leq TFFR_{ATC} \leq THR \quad (1)$$

3.1 Equal Apportionment Technique

If we ignore the specific subsystem (CI, ZC and OC) detail property and all the subsystems are operated in series as shown in Fig. 3, equal apportionment to each subsystem would seem reasonable. The equal apportionment technique assumes a series of “n”

subsystems, each of which is to be assigned the same safety goal [4]. A prime weakness of the method is that the subsystem goals are not assigned in accordance with the degree of difficulty associated with achievement of these goals. For this technique, the model is:

$$S_{ATC} = S_{CI} \times S_{ZC} \times S_{OC} \quad (2)$$

$$TFFR_{CI} = TFFR_{ZC} = TFFR_{OC} = \frac{TFFR_{ATC}}{x + y + z} \quad (3)$$

S_{ATC} means the safety goal of ATC system, and S_{CI} , S_{ZC} , S_{OC} represent the safety goal of CI, ZC and OC subsystems respectively. $TFFR_{ATC}$, $TFFR_{CI}$, $TFFR_{ZC}$, $TFFR_{OC}$ are the TFFR value for ATC, CI, ZC and OC subsystems. The x , y and z are the numbers of CI, ZC and OC deployed in the specific urban rail line separately.

3.2 Safety Impact-Based Apportionment Technique

The ATC system is made up from various subsystems, and the safety impact of the different subsystems to the ATC system is different, that is, if a subsystem has a dangerous failure, it will have different safety impact on ATC system in comparison with others, and it will cause different accident severity. Therefore, different safety goals need to be assigned to different subsystems depending on the safety impact. For subsystems with a bigger safety impact, the safety goal should be more stringent.

For the ATC system, according to the magnitude of the safety impact of the CI, ZC and OC subsystems on the rail line ATC system, the safety impact weight factor is defined in the Table 2. The safety impact number a , b and c mean 1 failure in CI, ZC and OC will cause a , b and c others subsystem enter into dangerous status. Taking the CI subsystem as an example, the safety impact weight factor for the CI can be defined as the ratio of:

$$w_{CI} = \frac{a - (a + b + c)/3}{(a + b + c)/3} = \frac{2a - b - c}{a + b + c} \quad (4)$$

For the ATC system, its safety goal can be expressed as:

$$TFFR_{ATC} = TFFR_{CI} \times x + TFFR_{ZC} \times y + TFFR_{OC} \times z \quad (5)$$

Let $TFFR_a$ as the base TFFR for the subsystem of ATC, then the

$$TFFR_{ATC} = TFFR_a \times (1 + w_{CI}) \times x + TFFR_a \times (1 + w_{ZC}) \times y + TFFR_a \times (1 + w_{OC}) \times z \quad (6)$$

The $TFFR_a$ can be derived from formula (6)

$$TFFR_a = \frac{TFFR_{ATC}}{x + y + z + w_{CI} \times x + w_{ZC} \times y + w_{OC} \times z} \quad (7)$$

Then the allocated TFFR for subsystem are:

$$TFFR_{CI} = TFFR_a(1 + w_{CI}) \quad (8)$$

$$TFFR_{ZC} = TFFR_a(1 + w_{ZC}) \quad (9)$$

$$TFFR_{OC} = TFFR_a(1 + w_{OC}) \quad (10)$$

3.3 Complexity-Based Apportionment Technique

It is true that if a system contains more basic components, its reliability should be worse, and the probability of failure will be higher, so its safety performance will be worse. Therefore, when allocating the THR, we must consider the number of basic components including sub-systems. The more components contained in the subsystem, the less safety goal should be assigned to that subsystem.

Assuming that the subsystems in ATC is composed of same basic components, these basic components have the same failure rate, so we can use the number of basic components contained in a subsystem to express the complexity of the subsystem. We use the numbers l , m and n to represent the complexity of CI, ZC and OC subsystems. For a specific urban rail ATC system containing x CIs, y ZCs and z OCs, the complexity factor can be expressed as Eqs. (11), (12) and (13).

$$cw_{CI} = \frac{x \times l}{x \times l + y \times m + z \times n} \quad (11)$$

$$cw_{ZC} = \frac{y \times m}{x \times l + y \times m + z \times n} \quad (12)$$

$$cw_{OC} = \frac{z \times n}{x \times l + y \times m + z \times n} \quad (13)$$

Therefore, the assigned TFFR value of a single CI, ZC and OC are described as follows:

$$TFFR_{CI} = \frac{TFFR_{ATC} \times cw_{CI}}{x} = \frac{TFFR_{ATC}}{x \times l + y \times m + z \times n} \times l \quad (14)$$

$$TFFR_{ZC} = \frac{TFFR_{ATC} \times cw_{ZC}}{y} = \frac{TFFR_{ATC}}{x \times l + y \times m + z \times n} \times m \quad (15)$$

$$TFFR_{CI} = \frac{TFFR_{ATC} \times cw_{OC}}{z} = \frac{TFFR_{ATC}}{x \times l + y \times m + z \times n} \times n \quad (16)$$

4 Apportionment Result Comparison

In order to verify the difference and applicability for the allocation results of the THR using the three different allocation methods, this research applies the allocation method proposed in the previous section to calculate the allocation results, as well as the ATC system THR allocation results are analyzed in a specific urban rail project.

4.1 Assumptions of the Specific ATC System

As shown in Fig. 4, in the specific ATC system of urban rail transit project, only the CI, ZC and OC are responsible for the vital safety functions. The ATC system includes the number of CI, ZC and OC subsystems which are x , y and z , where x is equal to 6, y is equal to 3, z is equal to 30. For the entire ATC system, the overall safety goal proposed by the operator is that THR should be less than $10^{-9}/h$.

For the safety impact of the CI, ZC, and OC subsystems, we define one failure in CI, ZC, and OC subsystems that can impact the number of other subsystems are a , b and c . where $a = 4$, $b = 10$, and $c = 2$.

For the complexity of the system, we define each CI, ZC and OC subsystem is composed by l , m and n basic components respectively, where l is equal to 10, m is equal to 8, and n is equal to 12.

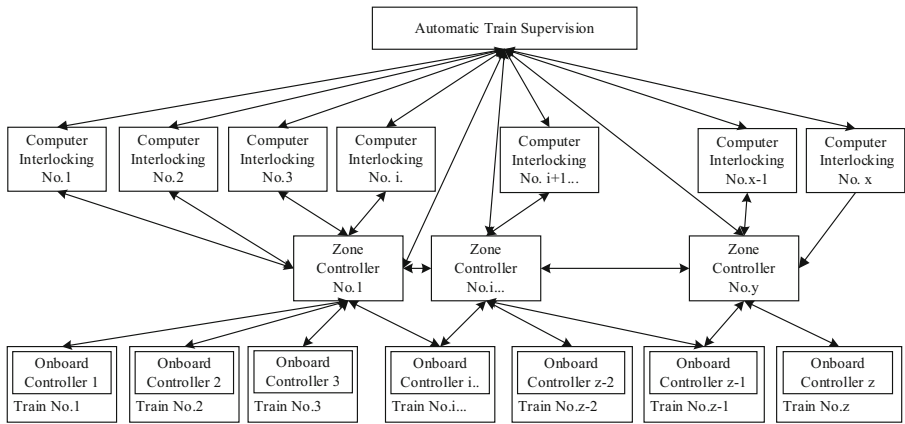


Fig. 4. A Specific ATC System Configuration

4.2 Safety Requirement Allocation Result

Based on the above assumptions the specific ATC System, we used the three different methods to allocate the THR as the ATC system safety requirements in Sect. 3. The ATC system data of calculation required is show in Table 2, and the allocation results are shown in Table 3.

From the above allocation results shown in Table 3, it can be seen that the allocation results of the dangerous failure rate (FR) of each subsystem obtained by using three different methods are all in the same order of magnitude. However, the specific values have certain differences, it can show that all the three methods are feasible. Comparing the calculation results with the actual situation of urban rail project, we think that the allocation method based on complexity is most reasonable. The THR Allocation Results of CI, ZC, and OC subsystems for Complexity-based Apportionment method are less than the EqualApportionment method as well as Safety Impact-based Apportionment method. For the method based on safety impact, since both the overall number

Table 2. The ATC system data

Subsystem	Subsys No.		Safety Impact		Complexity	
	x	7	a	4	l	10
Computer Interlocking (CI)	y	3	b	10	m	6
Zone Controller (ZC)	z	30	c	2	n	12

Table 3. THR Allocation Results

Subsystem	Equal	Safety Impact-based	Complexity-based
Computer Interlocking (CI)	2.5×10^{-11}	3.39×10^{-11}	2.23×10^{-11}
Zone Controller (ZC)	2.5×10^{-11}	8.47×10^{-11}	1.34×10^{-11}
Onboard Controller (OC)	2.5×10^{-11}	1.69×10^{-11}	2.68×10^{-11}

of subsystems and safety impact are considered in the allocation, the final allocation result is more sensitive to the number of subsystems than the safety impact. Except the Complexity-based Apportionment method, the other two method lead the bigger safety impact had been assigned a relatively loose safety value. Therefore, we consider the allocation method based on system complexity is the most suitable for the actual conditions of the project, which not only can meet the requirements of the Urban Rail Automatic Train Control System, but also can improve the reliability and safety of urban rail transit to some extent.

5 Conclusions

From the above analysis, it can be concluded that using the ATC system level THR as the safety requirements of the subsystems without any allocation cannot meet the overall system safety goals of the rail transit line. Therefore, using the different THR allocation methods will result in different subsystem TFFR, but the same order of magnitude. By comparing with the actual engineering demands, the allocation method based on complexity is the more applicable than the other two allocation methods, due to the allocation method based on complexity considers the specific characteristics of the subsystems.

Eventually, no matter which allocation method is adopted, we need to consider not only the logical architecture of the system, but also the specific number of each subsystem in the line system. At last, a reasonable allocation result of Complexity-based Apportionment Technique can be obtained. It is indicated from the results of the allocation that the larger the scale of the rail transit line is, the more subsystems it contains, and the more stringent and stricter safety requirements for the subsystems should be allocated.

Acknowledgments. The project is supported by Science and Technology Commission of Shanghai Municipality (20DZ2251900), as well as the Natural Science Foundation of Shanghai

(21ZR1423800). The work is also sponsored and supported by the Key Laboratory of Road and Traffic Engineering, Tongji University and Shanghai Engineering Research Center of Urban Infrastructure Renewal, Shanghai University. The authors are grateful for the reviewer of initial drafts for their helpful comments and suggestions.

References

1. IEEE, IEEE 1474.1, IEEE Standard for Communication-Based Train Control(CBTC) performance and functional Requirements. IEEE, New York (2004)
2. IEEE, IEEE 1474.3, IEEE Recommended Practice for Communication-Based Train Control(CBTC) System Design and Functional Allocations. IEEE, New York (2008)
3. CENELEC. EN 50129, Railway applications: safety related electronic systems for signaling. 3.CENELEC, Brussels, (2018)
4. Department of Defense: MIL-HDBK-338B. Electronic Reliability Design Handbook. Department of Defense, New York (1998)