文章编号：0253-374X(2022)01-0001-05　　**DOI**：10.11908/j.issn.0253-374x.21438

基于复杂度算法的安全指标分配分析

曾小清[1]，林海香[1,2]，方云根[1]，王奕曾[3]，刘　源[1]，马忠政[4]

(1. 同济大学 道路与交通工程教育部重点实验室，上海 201804；2. 兰州交通大学 自动化与电气工程学院，甘肃 兰州 730070；；3. 香港城市大学 计算机科学系，香港 999077；4. 上海申通地铁建设集团有限公司，上海 201103)

摘要：城市轨道交通信号工程建设过程中，信号设备供应商需要将业主设定的总体运营安全指标分配给信号系统的各个子系统。首先分析城市轨道交通信号系统的体系架构、安全功能和安全指标，然后针对设计的三种安全指标分配方法，分析这些方法的具体要求和原则，结合系统架构、安全逻辑模型和具体工程建设参数，利用三种不同方法，将整个系统总体安全指标分配到各个设备，最后比较不同分配方法计算出的分配结果。从分配结果的比较来看，三种分配方法得出的结果均处于同一数量级，均为可行的分配方法，但从系统安全性的角度而言，基于系统复杂度的分配方法最优，更适合信号系统设计和制造的需求。

关键词：安全指标；分配；信号系统；安全完整度等级；可容忍危险率

中图分类号：U239.5　　**文献标志码**：A

Safety Target Assignment Analysis Method Based on Complexity Algorithm

ZENG Xiaoqing[1], *LIN Haixiang*[1,2], *FANG Yungen*[1], *WANG Yizeng*[3], *LIU Yuan*[1], *MA Zhongzheng*[4]

(1. Key Laboratory of Road and Traffic Engineering of the Ministry of Education, Tongji University, Shanghai 201804, China.; 2. School of Automation and Electrical Engineering, Lanzhou Jiaotong University, Lanzhou 730070, Gansu, China; 3. Department of Computer Science, City University of Hong Kong, Hong Kong 999077, China; 4. Shanghai Metro Construction Group Co., Ltd., Shanghai 201103, China)

Abstract: In the urban rail signalling engineering project, signalling equipment suppliers need to allocate the overall operation safety target set by the owner to each subsystem of signalling system. At first, the system architecture, safety function, and safety target of the signalling system was analyzed. Then, the specific requirements and principles of the three designed safety target allocation methods were discussed. Considering the system architecture, safety control logic, and specific engineering construction parameters, three different allocation methods were used to allocate the overall system safety target to each subsystem. Finally, the allocation results calculated via the three different allocation methods were compared. The results obtained from the three allocation methods are in the same order of magnitude, which are all feasible. However, from the perspective of system safety, the allocation method based on system complexity is the preferable one, which is more suitable for urban rail system design and manufacturing.

Key words: safety target; allocation; signaling system; safety integrity level; tolerable hazard rate

在轨道交通工程建设项目中，为了保证列车的安全运行，基于通信的列车控制系统(communication based train control，CBTC)被用来实现列车超速防护、保持列车运行间隔、防止列车碰撞等运行所必须的安全功能，为此业主或运营单位一般会为整条建设线路的信号系统制定一个安全指标，如设定容许危险率(tolerable hazard rate，THR)值或安全完整度等级(safety integrity level，SIL)，并要求最终交付的CBTC系统满足这些设定的安全指标。目前典型的CBTC信号系统是分布在列车上、轨道上、轨旁信号机房、车辆段内和运行控制中心中的多场所分布系统，这些分布在不同位置的设备相互配合，共同实现列车运行安全控制功能，在分配安全指标的时候需要将这些分布的设备整体考虑。

由于信号系统设备往往来自不同的设备供应

收稿日期：2021-09-24
基金项目：上海市科学技术委员会项目(20DZ1202900，19DZ1204200)；上海市住房和城乡建设管理委员会项目(JS-KY18R022-7)
第一作者：曾小清(1969—)，女，教授，博士生导师，工学博士，主要研究方向为轨道交通控制与安全.
E-mail：zengxq@tongji.edu.cn
通信作者：王奕曾(1998—)，女，硕士生，主要研究方向为智能交通大数据分析.
E-mail：yizenwang2-c@my.cityu.edu.hk

论文拓展介绍

商,在设计和制造过程中,设备供应商只关心各自供应的单个设备的安全要求,缺乏总体统一规划、分配和协调,导致这些设备集成为一条运行线路的信号系统所达到的系统安全性能无法满足最初设定的安全要求。为确保最终交付的信号系统能够满足设定的安全要求,需要在设计和建设过程中综合考虑安全指标的分配,以指导各设备的设计和制造活动,确保交付的系统能够满足轨道交通线路运行安全指标。

1 地铁运行控制系统架构

根据IEEE定义[1],CBTC系统是一个连续的列车自动控制系统,它利用高分辨率列车位置确定,独立于轨道电路,连续、高容量、双向列车与地面数据通信,以及能够实现关键安全功能的车载和地面处理器实现列车运行控制和安全防护功能。CBTC系统的结构及其子系统分布如图1所示。

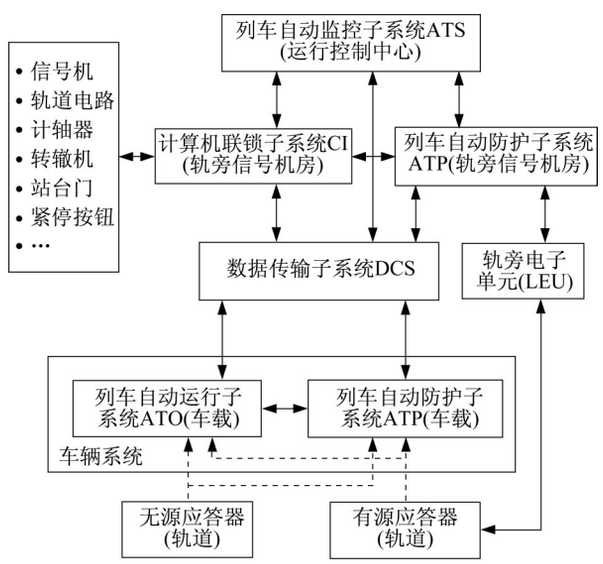

图1 CBTC系统架构

Fig. 1 Frame of communication based train control system (CBTC)

在CBTC系统中,列车自动防护(ATP)子系统用于通过列车检测、列车间隔和联锁的组合,对碰撞、超速和其他危险情况保持故障导向安全防护。计算机联锁(CI)子系统用于CBTC与外部轨旁现场设备的接口,从而建立信号机、道岔、进路之间的联锁关系,以避免形成冲突的列车运行进路。列车自动运行(ATO)子系统用于执行速度调节、按计划停车、性能水平调节或其他分配给列车操作员的功能。列车自动监控(ATS)子系统用于监控列车,调整单个列车的性能以维持时刻表,并提供数据以调整服务。ATO和ATS都是安全相关系统,通常具有中等安全要求(SIL2)。

除了ATP、CI、ATO和ATS系统外,CBTC还包括数据通信系统(DCS)和应答器传输系统。DCS是在轨旁设备与车载设备之间传输双向信息的传输,应答器传输系统分为有源应答器和无源应答器,无源应答器主要用于列车定位和定位校准,有源应答器用于传输一些可变的临时控制命令。

2 安全指标的分配方法

如图2所示,系统需求可分为安全要求和非安全要求;安全要求来源于危害,以可容忍危害率(THR)作为系统顶层安全目标。可容许功能失效率(tolerable functional failure rate, TFFR)代表着对特定安全功能危险失效发生频率的容忍程度或接受程度,通过这一指标来衡量功能安全需求,THR由TFFR导出。功能安全要求包括安全功能和安全完整性,使用安全完整性等级(SIL)来定义其要求,SIL和TFFR之间的关系如表1所示。SIL是用于定义安全功能的性能指标,SIL4具有最高级别的安全完整性。安全完整性包括系统故障完整性和随机故障完整性,根据系统设计,系统性失效应满足SIL要求,随机性失效应同时满足SIL和故障率(FR)要求。

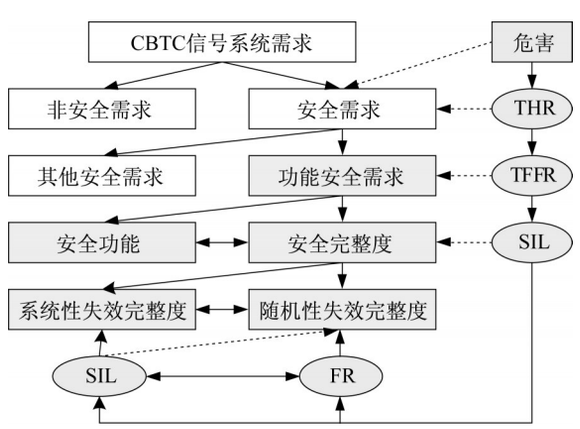

图2 安全需求分解及其对应指标

Fig. 2 Security requirement decomposition and its corresponding index

从CBTC系统实现安全控制功能的过程来看,如果计算机联锁、区域控制器和车载控制器中的任何一个失效,都有可能在城市轨道交通线路上发生事故,导致整个系统THR目标无法实现。从安全角度看,CI、ZC和OC形成一个串联系统,如图3所示。

表 1　TFFR 与 SIL 之间的关系

Tab. 1 Relationship between TFFR and SIL

序号	每功能小时的 TFFR	安全完整度等级
1	$10^{-9} \leqslant \text{TFFR} < 10^{-8}$	4
2	$10^{-8} \leqslant \text{TFFR} < 10^{-7}$	3
3	$10^{-7} \leqslant \text{TFFR} < 10^{-6}$	2
4	$10^{-6} \leqslant \text{TFFR} < 10^{-5}$	1

由于业主主要关注整体 CBTC 系统的安全要求，而不关注子系统 CI、ZC 和 OC，但对于子系统制造商，需要将系统的安全要求分配给 CI、ZC 和 OC 等子系统。从安全要求的定义出发，将安全完整性水平分为两部分：不可量化的 SIL 和可量化的 TFFR(FR)。对于执行一个安全功能的各种组件，如果没有冗余，组件将直接从系统继承不可量化的 SIL，即 CI、ZC、OC 子系统的 SIL 与 CBTC 系统的 SIL 相同，均为 SIL4。对于安全指标的可量化部分，需要采用具体的分配方法，将系统的 THR 和 TFFR 分配给 CI、ZC 和 OC，并确保最终的总子系统 TFFR 小于 CBTC 系统的 TFFR 和危险 THR，如式(1)所示。

$$\sum_{i}^{X}\text{TFFR}_{\text{CI}i}+\sum_{i}^{Y}\text{TFFR}_{\text{ZC}i}+\sum_{i}^{Z}\text{TFFR}_{\text{OC}i}\leqslant \text{TFFR}_{\text{CBTC}}\leqslant\text{THR} \tag{1}$$

2.1　等分配法

如果不考虑特定子系统(CI、ZC 和 OC)的细节属性，并且所有子系统都如图 3 所示的方式以串联模式运行，那么对每个子系统应承担的安全指标是相等。等分配法假设一系列“n”个子系统，每个子系统分配相同的安全目标[2]。该方法的一个主要缺点是子系统目标的分配不符合实现这些目标的难度。针对 CBTC 系统，可以表示为式(2)和式(3)：

$$S_{\text{CBTC}}=S_{\text{CI}}\cdot S_{\text{ZC}}\cdot S_{\text{OC}} \tag{2}$$

$$\text{TFFR}_{\text{CI}}=\text{TFFR}_{\text{ZC}}=\text{TFFR}_{\text{OC}}=\frac{\text{TFFR}_{\text{CBTC}}}{x+y+z} \tag{3}$$

式中：S_{CBTC} 为 CBTC 系统的安全指标；S_{CI}、S_{ZC}、S_{OC} 为计算机联锁、轨旁区域控制器和车载控制器子系统的安全指标；$\text{TFFR}_{\text{CBTC}}$、$\text{TFFR}_{\text{CI}}$、$\text{TFFR}_{\text{ZC}}$ 和 TFFR_{OC} 为 CBTC 系统、计算机联锁、轨旁区域控制器和车载控制器子系统的 TFFR 值；x、y 和 z 是特定城市轨道交通线路中配置的计算机联锁、轨旁区域控制器和车载控制器子系统的数量。

2.2　基于安全影响的分配

CBTC 系统由不同的子系统组成，不同的子系统对 CBTC 系统的安全影响是不同的，即如果一个子系统发生危险故障，它对 CBTC 系统的安全影响与其他子系统不同，造成的事故严重程度也不同。因此，安全指标的分配可以根据安全影响大小进行分配[3]。对于安全影响较大的子系统，安全目标应更加严格。

对于 CBTC 系统，根据计算机联锁、区域控制器和车载控制器对整个轨道交通 CBTC 系统安全影响的大小，安全影响系数定义见表 2。安全影响数 a、b 和 c 表示一个计算机联锁、轨旁区域控制器和车载控制器发生的故障将导致 a、b 和 c 其他子系统进入危险状态，以计算机联锁子系统为例，其安全影响权重系数可定义为

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

该权重系数表示单个子系统的安全影响与系统中所有子系统平均安全影响的一个比例。

表 2　安全影响系数

Tab. 2　Safety influential factors

子系统	安全影响数	安全影响系数 w
计算机联锁 CI	a	$w_{\text{CI}}=(2a-b-c)/(a+b+c)$
区域控制器 ZC	b	$w_{\text{ZC}}=(2b-a-c)/(a+b+c)$
车载控制器 OC	c	$w_{\text{OC}}=(2c-a-c)/(a+b+c)$

对于 CBTC 系统，其安全目标与子系统的安全指标关系可以表示为

$$\text{TFFR}_{\text{CBTC}}=\text{TFFR}_{\text{CI}}\cdot x+\text{TFFR}_{\text{ZC}}\cdot y+\text{TFFR}_{\text{OC}}\cdot z \tag{5}$$

设 TFFR_a 为 CBTC 子系统的平均 TFFR，则：

$$\text{TFFR}_{\text{CBTC}}=\text{TFFR}_a\cdot(1+w_{\text{CI}})x+\text{TFFR}_a\cdot(1+w_{\text{ZC}})y+\text{TFFR}_a\cdot(1+w_{\text{OC}})z \tag{6}$$

可由式(6)导出 TFFR_a 为

$$\text{TFFR}_a=\frac{\text{TFFR}_{\text{CBTC}}}{x+y+z+w_{\text{CI}}\cdot x+w_{\text{ZC}}\cdot y+w_{\text{OC}}\cdot z} \tag{7}$$

则为计算机联锁、区域控制器、车载控制器子系统分配的 TFFR 为

$$\text{TFFR}_{\text{CI}}=\text{TFFR}_a(1+w_{\text{CI}}) \tag{8}$$

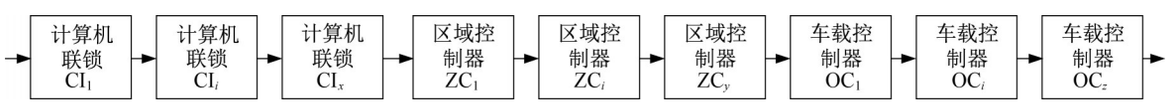

图 3　CBTC 信号系统关键安全控制功能逻辑

Fig. 3　Functional logic of key safety control in CBTC signaling system

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

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

2.3 基于复杂度的分配

假设系统的安全性与可靠性成正比例关系,按照系统的可靠性原理,如果一个系统包含更多的基本部件,它的可靠性会更差,失效的概率也会更高,则它的安全性能会更差。因此,在分配THR时,考虑子系统所包含的基本组件的数量作为分配的依据[4]。子系统中包含的组件越多,分配给该子系统的安全目标就严格。

假设CBTC中的子系统由相同的基本部件组成,这些基本部件具有相同的故障率,因此可以用子系统中包含的基本部件的数量来表示子系统的复杂性。使用l、m和n来表示CI、ZC和OC子系统包含基本部件的数量。对于包含x个计算机联锁、y个区域控制器和z个车载控制器的特定CBTC系统,其复杂度因子C可用式(11)、(12)、(13)表示。

$$C_{CI}=\frac{xl}{xl+ym+zn} \quad (11)$$

$$C_{ZC}=\frac{ym}{xl+ym+zn} \quad (12)$$

$$C_{OC}=\frac{zn}{xl+ym+zn} \quad (13)$$

则为计算机联锁、区域控制器、车载控制器子系统分配的TFFR为

$$TFFR_{CI}=\frac{TFFR_{CBTC}\cdot C_{CI}}{x}=\frac{TFFR_{CBTC}}{xl+ym+zn}l \quad (14)$$

$$TFFR_{ZC}=\frac{TFFR_{CBTC}\cdot C_{ZC}}{y}=\frac{TFFR_{CBTC}}{xl+ym+zn}m \quad (15)$$

$$TFFR_{CI}=\frac{TFFR_{CBTC}\cdot C_{OC}}{z}=\frac{TFFR_{CBTC}}{xl+ym+zn}n \quad (16)$$

3 分配结果比较

作为一个典型的城市轨道交通CBTC信号系统,它具有以下核心安全功能:(1)列车位置/列车速度的确定,(2)列车安全间隔,(3)超速保护和制动保证,(4)列车回溜保护,(5)轨端保护,(6)列车分块保护和联挂、解挂,(7)零速检测,(8) 开门控制保护联锁,(9)发车联锁,(10)紧急制动,(11)进路联锁,(12)交通方向反转联锁,(13)工作区保护,(14)断轨检测,(15)限制进路保护,(16)水平交叉口保护。这些安全功能通过轨旁设备计算机联锁(CI)和区域控制器(ZC)以及车载控制器(OC)来实现,即CI、ZC和OC应满足SIL 4要求,集成的系统THR应小于为$10^{-9}h^{-1}$[5]。

为了验证不同方法在安全指标分配结果上的差异性和适用性,利用第2节中提出的等分配法、基于安全影响的分配、基于复杂度的分配三种方法对某城市轨道交通项目CBTC系统THR分配进行了计算和分析,以上海市轨道交通地铁17号线项目为例。该工程项目为了保证列车运行的安全,信号系统应实现必要的安全保护功能,以防止“超过建议的速度和/或距离限制”的危害,该危害的THR值为$10^{-9}h^{-1}$,针对这一危害,相关的安全功能可分解为(1)确保进路安全,(2)确保安全隔离(3)保证列车的安全速度,(4)控制列车的加速和制动[6]。这些功能应满足从THR分配的TFFR,如果设备用于实现这些安全功能,则设备应满足相关SIL、TFFR和FR。

3.1 具体CBTC系统的仿真配置

如图4所示,在上海市轨道交通地铁17号线项目CBTC系统中,只有计算机联锁、区域控制器、车载控制器负责关键安全功能(SIL4)。CBTC系统包括计算机联锁、区域控制器、车载控制器子系统的数量分别为$x=6$、$y=3$和$z=30$。对于整个CBTC系统,运营方提出的总体安全目标是THR应小于$10^{-9}h^{-1}$。

对于计算机联锁、区域控制器、车载控制器子系统的安全影响,将计算机联锁、区域控制器、车载控制器子系统中的一个故障可能引起$a=4$、$b=10$和$c=2$个其他子系统的危险影响。

考虑到系统的复杂性,定义了每个计算机联锁、区域控制器、车载控制器子系统分别由$l=10$、$m=8$和$n=12$个基本元器件组成。

3.2 安全指标分配结果

基于第3.1节具体CBTC系统的仿真配置假设和表2中的数据,使用第2节中提到的等分配法、基于安全影响的分配、基于复杂度分配三种不同方法来分配CBTC系统的量化安全指标,计算结果如表3所示。

从表4所示的分配结果可以看出,用三种不同方法得到的各子系统危险失效率(FR)的分配结果都在同一个数量级,和实际的工程数据相符,可以看出三种方法都是可行的。但具体指标数值大小有一定的差异,结合城市轨道交通工程的实际情况进行比较,认为基于复杂性的分配方法所得的结果与工程建设实际数据最接近,是最适合的分配方法。

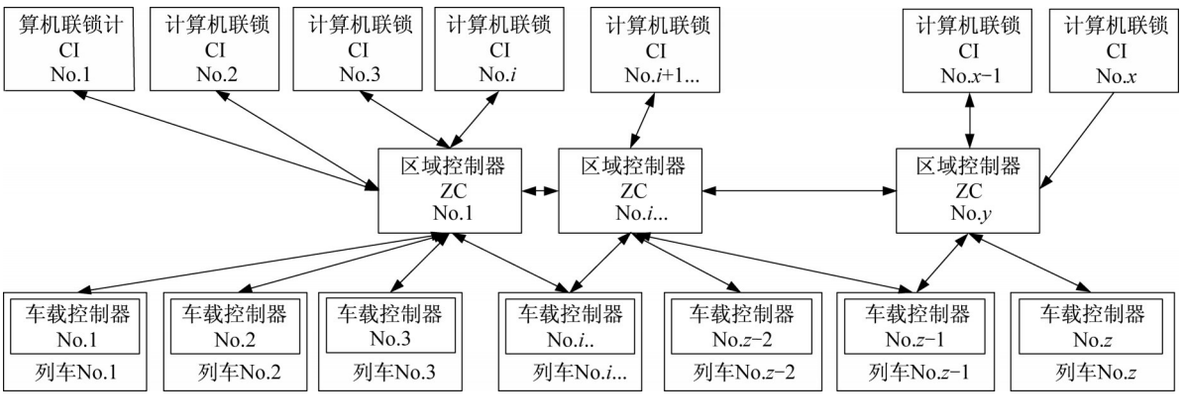

图 4　线路中 CBTC 系统关键系统配置

Fig. 4　Key system configuration of CBTC system in urban rail transit lines

表 3　CBTC 系统参数

Tab. 3　System parameters of CBTC

子系统	子系统数量		安全影响数		复杂度	
计算机联锁(CI)	x	7	a	4	l	10
区域控制器 (ZC)	y	3	b	10	m	6
车载控制器 (OC)	z	30	c	2	n	12

表 4　分配结果比较

Tab. 4　Comparison of allocation results

子系统	等分配法	基于安全影响的分配	基于复杂度的分配
计算机联锁(CI)	2.5×10^{-11}	3.39×10^{-11}	2.23×10^{-11}
区域控制器 (ZC)	2.5×10^{-11}	8.47×10^{-11}	1.34×10^{-11}
车载控制器 (OC)	2.5×10^{-11}	1.69×10^{-11}	2.68×10^{-11}

4　总结

从以上分析可以看出,采用CBTC系统级THR作为子系统的设计安全要求,不进行任何配置,无法满足轨道交通线路的整体系统安全目标。采用不同的THR分配方法将导致不同的子系统TFFR,与实际工程实践相比,基于复杂性的分配方法比其他两种分配方法更适用,由于基于复杂度的分配方法考虑了子系统规模复杂度与系统安全性紧密相关这一具体特点。

最后,无论采用哪种分配方式,不仅要考虑系统的逻辑架构,还要考虑线路系统中各子系统的具体数目,才能得到正确的分配结果。从分配结果可以看出,轨道交通线路规模越大,包含的子系统越多,对子系统的安全要求就越严格。

目前研究的分配方法是从系统安全影响度、复杂性等单因素考虑的,在未来的研究中除了增加考虑的影响安全指标分配的因素外,还可以对所有影响因素进行综合考虑,使系统安全指标分配不但能符合设备制造和工程建设的实际情况,也能满足轨道交通运营维护的需求。

作者贡献声明:

曾小清:安全指标分析,数据处理,学术指导。

林海香:安全完整度等级分析,论文撰写与修改。

方云根:可容忍危险率分析,论文撰写。

王奕曾:数据分析,公式编辑。

刘　源:图表制作与论文修改。

马忠政:学术指导与论文修改。

参考文献:

[1] IEEE. IEEE standard for communication-based train control (CBTC) performance and functional requirements:IEEE 1474.1 [S]. New York: IEEE, 2004 .

[2] Department of Defense. Electronic reliability design handbook: MIL-HDBK-338B[S]. New York: Department of Defense, 1998 .

[3] 张玉刚,孙杰,喻天翔.考虑不同失效相关性的系统可靠性分配方法[J]. 机械工程学报, 2018, 54(24): 206.
ZHANG Yugang, SUN Jie, YU Tianxiang. A reliability allocation method considering failure correlation based on vine copula[J]. Journal of Mechanical Engineering, 2018, 54(24): 206.

[4] 李鸣章,冷坤,聂华菊.航空发动机安全性指标分配方法及流程研究[J].质量与可靠性, 2019(1) : 30.
LI Mingzhang, LENG Kun, NIE Huaju. A study of allocation method and process of safety index for aero engines[J]. Quality and Reliability, 2019(1): 30.

[5] CENELEC. Railway applications: Safety related electronic systems for sig-nalling 3:EN 50129[S]. Brussels: CENELEC, 2018.

[6] IEEE. IEEE recommended practice for communication-based train con-trol(CBTC) system design and functional allocations: IEEE 1474.3[S]. New York: IEEE, 2008.