

城市轨道交通车辆系统安全完整性等级指标的定量分析与分配

秦姣梅 潘德敏 范开江

(中车青岛四方车辆研究所有限公司, 266031, 青岛)

摘要 [目的]随着城市轨道交通列车全自动运行系统的发展应用,对城市轨道交通车辆系统的安全性提出更高要求,在新的全自动运行的运营场景下,应对城市轨道交通列车从顶层重新梳理安全需求,以确定城市轨道交通车辆关键系统的安全完整性等级。[方法]综合采用 FTA(故障树分析)、风险矩阵、FMECA(故障模式影响和危害分析)方法,从列车全线系统级到车辆级、车辆子系统级逐层进行危害识别、风险分析以及定量指标分配。[结果及结论]由分析得出城市轨道交通车辆关键系统的安全需求及 SIL(安全完整性等级)。牵引系统的安全功能包括紧急制动牵引切除功能、方向控制功能、牵引使能功能和制动控制功能,它们的安全完整性等级,除“紧急制动牵引切除功能”为 SIL3 外,其余均为 SIL2;制动系统的安全功能包括整车紧急制动功能、防滑控制功能、常用制动功能和保持制动功能,它们的安全完整性等级分别为 SIL4、SIL3、SIL2、SIL2;网络系统的安全功能包括保持制动功能、司机室激活功能、方向管理功能、牵引制动指令管理功能和级位管理功能,它们的安全完整性等级都为 SIL2。

关键词 城市轨道交通;车辆系统;安全完整性等级;风险分析

中图分类号 U298:U270

DOI:10.16037/j.1007-869x.2024.06.040

Quantitative Analysis and Allocation of Safety Integrity Level Indexes for Urban Rail Transit Vehicle System

QIN Jiaomei, PAN Demin, FAN Kaijiang

(CRRC Qingdao Sifang Rolling Stock Research Institute Co., Ltd., 266031, Qingdao, China)

Abstract [Objective] Development and application of FAO (fully automatic operation) system in urban rail transit train requires higher safety of urban rail vehicle system. Under the new operation scenario where FAO needs to be confirmed, it is necessary to sort through the safety requirements for urban rail transit train from the top level, determine the SIL (safety integrity level) of the critical system in urban rail transit vehicle. [Method] FTA (fault tree analysis), Risk Matrix and FME-

CA (failure mode, effects and criticality analysis) are all used to conduct hazard identification, risk analysis, and quantitative index allocation layer by layer from the system level of entire train line to the vehicle system level, the vehicle subsystem level. [Result & Conclusion] The safety requirements and the SIL of urban rail transit vehicle system are obtained through analysis. The safety functions of the traction system include emergency braking traction cut off function, direction control function, traction enable function, and braking control function, except the first one belongs to SIL3, all other three functions are SIL2. The safety functions of the braking system include emergency braking function, anti-skid control function, service braking function, and brake holding function, belonging to SIL4, SIL3, SIL2, and SIL2 respectively. The safety functions of the network system include brake holding function, driver's cabin activation function, direction management function, traction braking command management function, and level management function, all belonging to SIL2.

Key words urban rail transit; vehicle system; SIL; risk analysis

安全是轨道交通运营的首要前提。随着城市轨道交通列车全自动运行,需确认技术的发展应用,对列车车辆关键系统的安全性提出了更高的要求。

既往非全自动运行列车中,对车辆牵引、网络等系统的安全完整性等级要求较低,而全自动运行需进行列车场景下的,从全线系统级到车辆关键子系统级的安全分析。本文综合采用各风险分析方法,对城市轨道交通列车从顶层梳理安全需求,得出城市轨道交通车辆牵引、制动、网络关键子系统的安全需求及定量指标。

1 风险分析方法

轨道交通各系统功能的 SIL(安全完整性等级)划分及定量指标如表 1 所示。对于各系统功能安全

完整性等级的确定,需在项目初期进行风险分析和 SIL 分配工作。常用的风险分析方法如表 2 所示,可组合采用多种方法。

表 1 安全完整性等级定量指标

Tab.1 SIL quantitative index

小时 TFFR	SIL
$10^{-9} \sim < 10^{-8}$	SIL4
$10^{-8} \sim < 10^{-7}$	SIL3
$10^{-7} \sim < 10^{-6}$	SIL2
$10^{-6} \sim < 10^{-5}$	SIL1

注:TFFR 为可容忍危险功能失效率。

表 2 常用的风险分析方法

Tab.2 Risk analysis method in common use

方法	说明	适用情况
风险矩阵	对初步危害进行识别、分类和等级划分	半定量或定量分析;和其他方法组合使用
HAZOP(危害和可操作性研究)	基于正常运作的偏差,运用引导词进行系统参数遍历分析,得出初步危害清单	适用于初步危害识别
FMECA(故障模式影响和危害分析)	分析系统中所有可能产生的潜在故障模式及其对系统造成的影响,并按每一个故障模式的严重程度、发生频度予以分类的一种归纳分析方法	适用于单通道或并行结构
ETA(事件树)	基于二进制逻辑,识别和评估潜在事故场景中由初始事件引发的事件序列和最终结果	适用于定性的危害后果分析
FTA(故障树)	自上而下通过原因分解进行分析的方法	适用于初步危害后的分解与定量分配
CCF(共因分析)	系统多个元素之间由相同原因导致同时发生危害的分析	与 FMECA 互补使用;FTA 中用于与门分析
Markov(马尔科夫)法	对系统状态进行建模,并根据模型计算达到各种系统状态的概率	适用于建模和状态转移分析
RBD(可靠性框图)	利用互相连接的方框来显示系统的失效逻辑	配合 HAZOP 或 FTA
风险图	采用可能性、后果、处于危险区域的时间和避免危害事件的可能性 4 个参数来确定安全完整性水平	适用于顶层功能的定性和 SIL 的确定

上述方法中,风险图法较易进行分析,在信号系统的风险分析中得到了广泛应用^[1]。风险图不依赖于定量指标即可定义 SIL,但只能定性分析且比较依赖于分析人员的能力。本文综合风险矩阵、FTA、FMECA 等方法,对城市轨道交通车辆系统进

行 SIL 指标的定量分析与分配。

2 SIL 指标的定量分析与分配

SIL 指标的定量分析与分配过程共包含 5 个阶段的工作:①根据场景分析和事故清单,对列车事故进行识别。②对识别的事故进行全线系统级的危害及后果分析,得出初步的危害发生率,即初始的 THR(可容忍危害失效率)定量指标。③对全线系统级危害进行分解,得到车辆系统级危害清单及 THR 定量指标。④对系统级 THR 定量指标进行修正。⑤对系统级危害进行子系统级分解,得到车辆牵引、网络、制动子系统的安全需求及 TFFR 定量指标。

2.1 事故识别

事故识别需确定线路的运营场景,并按照历史数据和经验确定项目的通用顶层事故清单。其可参考的资料包括:参考线路的危害日志,其他历史发生的事故记录,系统定义/功能定义等。

2.1.1 运营场景

运营场景与运营线路的列车功能、线路环境等条件有密切关系,运营场景分析得详尽与否,会影响事故识别是否完整。分析时可注意场景的同类合并和优化,以便减少后期分析的工作量。

目前我国的全自动运行地铁线路中,北京燕房线^[2]和上海轨道交通 14、15、18 号线 3 条新线^[3]针对全自动运行系统的运营场景进行了具体分析。

本文安全分析对象为城市轨道交通列车车辆系统,参考上述场景分析结果,并对场景进行合并,以表 3 的 21 种运营场景进行列车的危害性分析。

表 3 列车运营场景

Tab.3 Train operation scenario

序号	运营场景	序号	运营场景
1	三轨上电	12	列车在正线退行
2	车载控制器自检	13	列车在正线反向跳跃
3	车辆自检	14	列车在正线正向跳跃
4	车辆出库	15	列车在正线反向运行
5	列车在车辆段正向运行	16	车站上下客
6	司机上下车	17	列车站前折返
7	列车在车辆段退行	18	列车站后折返
8	洗车	19	乘客疏散
9	车辆出入场段	20	联挂救援
10	列车在正线正向运行	21	维修作业
11	列车在联络线转线作业		

2.1.2 事故清单

事故清单可采用行业、历史经验及事故记录等信息。在城市轨道交通领域,从潜在事故角度来说,主要存在撞击、脱轨、人身伤害、触电、火灾和恶劣天气等六大风险。表4列出本研究分析的事故清单。

表4 事故清单
Tab.4 Accident list

事故名称	事故场景初步分解	事故场景细化解
撞击	车车相撞	列车追尾相撞 列车侧面相撞 列车迎面相撞
	车和物体相撞	列车与线路设备相撞 列车与侵限物体相撞
	人车相撞	列车撞到乘客或工作人员
脱轨	列车脱轨	列车失去运行方向引导 列车运行过程中失稳 列车脱轨进入其他轨道
人身伤害	人员跌入轨道区域	人员从站台跌落 人员从列车跌落 人员被夹在列车与站台的间隙
	人员在列车内跌倒	乘客在列车客室跌倒 司机等员工在司机室跌倒
触电	触电	
火灾	窒息	
	中毒	
恶劣天气	洪水/地震/强风	

2.2 事故的危害及后果分析

2.2.1 全线系统级危害识别

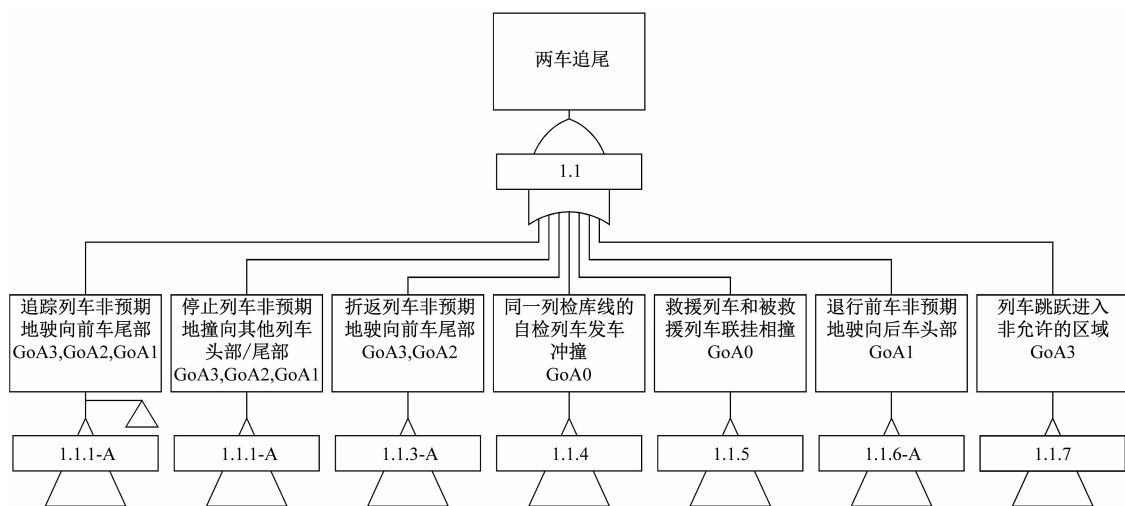
对每一个运营场景,遍历事故源清单,识别特定场景的事故。对识别的事故逐项进行 FTA 分析,得到列车的全线系统级危害。图1为两车追尾事故的 FTA 分析举例,得到可能引起两车追尾事故的全线系统级危害。

2.2.2 危害后果分析

对分析所得的全线系统级危害采用风险矩阵(见表5)的方法进行风险是否可接受分析。根据历史经验数据,评估危害发生频率以及后果的严重性,确定危害的初步风险等级。通过施加安全需求,可将危害降到可接受的风险等级内。该安全需求及事故发生频率即为线路级安全需求及其定量指标。危害后果分析过程案例如表6所示。根据表6可以得出,“追踪列车非预期地驶向前车尾部”危害的小时 THR 指标为小于 10^{-9} 。

2.3 线路级危害分解

对线路级危害同样采用 FTA 法分解,将危害发生率按照平分的模式分配到各系统危害,得到列车各系统危害及 THR 指标。对“追踪列车非预期地驶向前车尾部”系统级危害进行 FTA 分解,得出车辆子系统级的危害:①执行紧急制动时无法保证在安全距离内停车,小时 $\text{THR} < 8.33 \times 10^{-11}$;②列车发生打滑时紧急制动距离变长,小时 $\text{THR} < 8.33 \times 10^{-11}$;③紧急制动的同时施加了非预期牵引,小时 $\text{THR} < 8.33 \times 10^{-11}$ 。



注:GoA 为自动控制等级。

图1 顶层危害的 FTA 分析

Fig.1 FTA of top-level hazard

表 5 风险矩阵
Tab.5 Risk matrix

风险发生 概率等级	风险发生概率描述	风险发生 频率/(次/h)	风险等级				
			轻微事故	严重事故	危急事故	重大事故	特别重大事故
A	每周发生数次或更多	$\geq 10^{-2}$	R1	R1	R1	R1	R1
B	每月发生数次	$\geq 10^{-3} \sim < 10^{-2}$	R1	R1	R1	R1	R1
C	每年发生数次	$\geq 10^{-4} \sim < 10^{-3}$	R2	R1	R1	R1	R1
D	十年内发生数次	$\geq 10^{-5} \sim < 10^{-4}$	R2	R1	R1	R1	R1
E	百年内发生数次	$\geq 10^{-6} \sim < 10^{-5}$	R3	R2	R1	R1	R1
F	不大可能出现	$\geq 10^{-7} \sim < 10^{-6}$	R3	R3	R2	R1	R1
G	非常不可能出现	$\geq 10^{-8} \sim < 10^{-7}$	R4	R3	R3	R2	R1
H	发生可能性最少	$\geq 10^{-9} \sim < 10^{-8}$	R4	R4	R3	R3	R2
I	不可能发生	$\geq 10^{-10} \sim < 10^{-9}$	R4	R4	R4	R3	R3
J	难以置信的	$< 10^{-10}$	R4	R4	R4	R4	R3

注:R1 为除特殊情况外,必须消除该类风险;R2 为必须将风险减低至最低实际可行的水平;R3 为可忍受的风险,但仍须按成本效益尽量降低风险;R4 为可接受的风险。

表 6 危害后果分析案例
Tab.6 Case of hazard consequence analysis

顶层 危害	顶层 危害 分解	标识	线路级 危害	后 果	严重 程度	是否 广泛 接受	施加安全需求前风险等级			施加安全需求后残余风险等级			小时 THR
							风险发生 概率等级	事故后果 严酷度	风险 等级	风险发生 概率等级	事故后果 严酷度	风险 等级	
1 撞 击	1.1 两车 追尾	1.1.1	追踪列车非预期 地驶向前车尾部	追尾	3 至 49 人死亡	否	E	重大 事故	R1	I	重大 事故	R3	$< 10^{-9}$
		1.1.2	停止列车非预期 地撞向其他列车 头部/尾部	追尾	3 至 49 人死亡	否	E	重大 事故	R1	I	重大 事故	R3	$< 10^{-9}$
		1.1.3	折返列车非预期 地驶向前车尾部	追尾	3 至 49 人死亡	否	E	重大 事故	R1	I	重大 事故	R3	$< 10^{-9}$

2.4 THR 修正

得到初步的 THR 指标后,可通过外部屏障的方式降低事故发生频率和事故严重性,从而对 THR 指标进行修正,以进一步提高事故安全目标。本文参考 MODSafe^[4]方法对得到的初步 THR 指标进行修正。通过对所有系统危害进行线路级危害分解和 THR 修正后,得到车辆系统级危害清单以及经修正后的 THR 指标如表 7 所示。

2.5 系统级安全指标分解

在该阶段,采用 FTA 分析完成从车辆系统级到牵引、制动、网络子系统的危害分解和 TFFR 指标的分配。

HA4 危害“保持制动下列车发生溜车”的 FTA 分析如图 2 所示,得到制动系统的保持制动功能的小时 TFFR 指标为 4.1×10^{-7} 。根据小时 TFFR 指

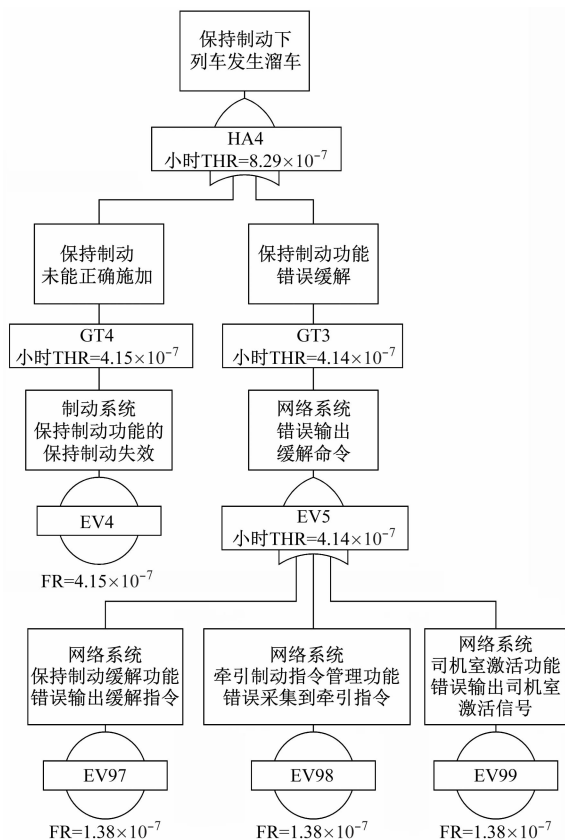
表 7 车辆系统危害清单及 THR 指标

Tab.7 Vehicle hazard list and THR (tolerable hazard rate) index

标识	子系统级危害	小时 THR
HA1	系统执行紧急制动时无法保证在安全距离内停车	$< 8.3 \times 10^{-9}$
HA2	列车发生打滑时紧急制动距离变长	$< 8.3 \times 10^{-8}$
HA3	紧急制动的同时施加了非预期牵引	$< 8.3 \times 10^{-8}$
HA4	保持制动下列车发生溜车	$< 8.3 \times 10^{-7}$
HA5	车辆非预期牵引	$< 8.3 \times 10^{-7}$
HA6	执行常用制动时无法让列车按预期减速	$< 5 \times 10^{-6}$

标,制动系统的保持制动功能安全完整性等级为 SIL2,其危险侧为保持制动失效;网络系统的保持制动缓解功能、牵引制动指令管理功能、司机室激活功能的小时 TFFR 指标为 1.83×10^{-7} ,根据小时

TFFR 指标,其功能需求均为 SIL2;“保持制动缓解功能”的危险侧为错误输出“保持制动缓解指令”,“牵引制动指令管理功能”的危险侧为错误输出“牵引指令”,“司机室激活功能”的危险侧为错误输出“司机室激活信号”。



注:GT、EV 为软件的标识号;FR 为失效率。

图2 子系统危害的 FTA 分析

Fig.2 FTA of subsystem hazard

3 车辆核心控制系统的 SIL

根据上述分析方法,对车辆核心控制系统进行 SIL 的定量分析及指标分配,得出城市轨道交通列车车辆牵引、网络、制动子系统的安全需求及其定量指标如表 8 所示。

4 结语

本文提出了一种 SIL 定量分析与分配流程,从列车顶层进行安全分析和指标分配,可得出列车全线系统级、系统级、子系统级各层级的安全需求及定量指标。在全自动无人驾驶列车场景下,针对城市轨道交通列车的车辆关键系统采用此流程进行具体分析,得出城市轨道交通车辆牵引、网络、制动

表 8 子系统安全需求及 TFFR 指标

Tab.8 Subsystem safety requirements and TFFR (tolerable functional failure rate) index

系统	功能	小时 TFFR	SIL
制动系统	整车级紧急制动功能	8.3×10^{-9}	SIL4
	防滑控制功能	8.3×10^{-8}	SIL3
	常用制动功能	8.3×10^{-7}	SIL2
	保持制动功能	4.1×10^{-7}	SIL2
牵引系统	方向控制功能	2×10^{-7}	SIL2
	紧急制动牵引切除功能	8.3×10^{-8}	SIL3
	牵引使能控制功能	2×10^{-7}	SIL2
	制动模式控制功能	8.3×10^{-7}	SIL2
网络系统	保持制动缓解功能	1.38×10^{-7}	SIL2
	司机室激活管理功能	1.04×10^{-7}	SIL2
	方向指令管理功能	1.04×10^{-7}	SIL2
	牵引制动指令管理功能	1.38×10^{-7}	SIL2
	级位信息管理功能	8×10^{-7}	SIL2

子系统安全功能的完整性等级及定量指标。本文的分析结果可为城市轨道交通列车车辆系统安全分析提供参考。

参考文献

- [1] 李彦华. 轨道交通信号系统 SIL 定级实例探讨[J]. 铁路通信信号工程技术, 2018, 15(10): 91.
LI Yanhua. SIL determination cases of urban rail transit signal systems [J]. Railway Signalling & Communication Engineering, 2018, 15(10): 91.
- [2] 宁滨, 郜春海, 李开成, 等. 中国城市轨道交通全自动运行系统技术及应用[J]. 北京交通大学学报, 2019, 43(1): 1.
NING Bin, GAO Chunhai, LI Kaicheng, et al. Technology and application of fully automatic operation system for urban rail transit in China [J]. Journal of Beijing Jiaotong University, 2019, 43(1): 1.
- [3] 施挺. 上海城市轨道交通全自动运行系统运营场景研究[J]. 城市轨道交通研究, 2020, 23(增刊2): 160.
SHI Ting. Research on operation scenarios of Shanghai urban rail transit automatic operation system [J]. Urban Mass Transit, 2020, 23(S2): 160.
- [4] WIGGER P. MODSafe-modular urban transport safety and security analysis [J]. Procedia-Social and Behavioral Sciences, 2012, 48: 2616.

· 收稿日期:2021-11-26 修回日期:2022-02-22 出版日期:2024-06-10
Received:2021-11-26 Revised:2022-02-22 Published:2024-06-10
· 通信作者:秦姣梅,高级工程师,qinjiaomei_ss@crrecg.com
· ©《城市轨道交通研究》杂志社,开放获取 CC BY-NC-ND 协议
© Urban Mass Transit Magazine Press. This is an open access article under the CC BY-NC-ND license