

# 城市轨道交通列车关键子系统的安全完整性等级分析

李葛亮<sup>1</sup> 刘 明<sup>1</sup> 吕远斌<sup>2</sup>

(1. 南宁轨道交通集团有限责任公司, 530029, 南宁; 2. 中车株洲电力机车有限公司, 412001, 株洲//第一作者, 工程师)

**摘 要** 合理确定城市轨道交通各专业设备系统的 SIL(安全完整性等级)、避免刻意追求安全功能造成资源浪费是非常必要的。针对列车客室侧门、网络控制、空气制动等关键子系统发生故障可能会导致乘客碰撞、夹伤、摔伤甚至死亡的安全事故,对影响乘客安全的列车安全功能进行评估。从列车各关键子系统的安全功能角度出发,在介绍 HAZOP(危险与可操作性分析)风险识别方法的基础上,阐述了 SIL 的划分及其评估方法。以南宁轨道交通 4 号线列车为例,将该 SIL 评估方法应用到实际的工程项目中,合理确定该车型各子系统的 SIL。

**关键词** 城市轨道交通; 车辆; 安全完整性等级; 安全评估; 危险与可操作性分析

**中图分类号** U298.1<sup>+</sup>1

DOI:10.16037/j.1007-869x.2021.07.021

## Analysis on Safety Integrity Level of Urban Rail Transit Train Key Subsystems

LI Geliang, LIU Ming, LYU Yuanbin

**Abstract** It is necessary to reasonably determine the SIL (safety integrity level) of professional equipment systems of urban rail transit and to avoid the waste of resources caused by deliberate pursuit of safety functions. In view of accidents that may result in collision, entrapment, fall or even death of passengers due to faults of key subsystems such as train passenger compartment doors, network control and air braking, the safety functions of train that affect passenger safety are evaluated. From the perspective of the safety function of various key subsystems of the train, based on the introduction of risk identification method of HAZOP (hazard and operational analysis), the division of SIL and its evaluation method are expounded. Taking the train of Nanning Rail Transit Line 4 as an example, the SIL evaluation method is applied to actual engineering project to reasonably determine the SIL of each subsystem of the train.

**Key words** urban rail transit; vehicle; safety integrity level; security assessment; hazard and operational analysis

**First-author's address** Nanning Rail Transit Co., Ltd., 530029, Nanning, China

20 世纪 90 年代,欧洲着手开展轨道交通领域信号、车辆系统的安全性研究,引入 RAMS(可靠性、可用性、可维修性、安全性)管理体系,制定了安全相关系统功能安全的基础标准——IEC 61508—2000《电气/电子/可编程电子安全系统的功能安全》,并在此基础上制定了 EN 50126—1999《铁路应用—可靠性、可用性、可维护性和安全性》、EN 50128—2001《铁路应用—通信、信号和处理系统—铁路控制和防护系统软件》和 EN 50129—2003《铁路应用—通信、信号、处理系统—信号安全相关电子系统》。随后我国发布了对应的标准——GB/T 21562—2008《轨道交通可靠性、可用性、可维修性和安全性规范及示例》、GB/T 28808—2012《轨道交通 通信、信号和处理系统控制和防护系统软件》和 GB/T 28809—2012《轨道交通 通信、信号和处理系统 信号用安全相关电子系统》。

在进行车辆系统设计时,按照上述标准对系统进行风险评估,分析和评估系统的 THR(可容忍的危害率),确保安全子系统和安全功能满足相应的 SIL(安全完整性等级)要求<sup>[1]</sup>。SIL 用于确定安全功能的安全完整性要求的不连续界别,分为 1 级至 4 级。级别越大,表示系统安全功能的完整性要求越高,需要采用更复杂、更高成本的技术来实现<sup>[2]</sup>。因此,在满足安全需求的前提下,避免资源的过度投入和成本支出,合理确定系统的 SIL 是非常必要的。本文从城市轨道交通列车客室侧门、网络控制、空气制动等关键子系统的安全功能角度出发,通过 HAZOP(危险与可操作性分析)识别系统的潜在风险,在其基础上进行 SIL 分析,并将 SIL 评估方法应用到实际的工程项目中。

## 1 基于 HAZOP 原则的风险识别

HAZOP 旨在对系统的用户需求、设计开发、生产组装过程及工艺流程等方面进行安全评估,找出在此过程中可能产生的风险及其后果,并进行详细

分析,最后给出相应的预防措施。HAZOP 是一种具有系统性、创造性的分析方法<sup>[3]</sup>,适用于城市轨道交通车辆系统的风险识别,能够较为全面地识别危害。基于 HAZOP 技术,可将列车的设计、制造全过程分为以下几个主要阶段:

- 1) 对系统进行定义,明确系统的功能需求,选择专业团队,确定风险矩阵,进行初步危害分析;
- 2) 收集系统危害及损失的数据,编制风险识别流程计划,进行系统危害分析;
- 3) 将整个系统划分为相关的子系统,定义每个子系统的功能设计,进行子系统危害分析、接口危害分析、操作和支持危害分析;
- 4) 确定风险等级,提出建议措施;
- 5) 确定列车整体系统的设计、生产制造方案;
- 6) 跟踪方案的实施,做好过程记录,最后输出分析报告。

## 2 SIL 分析

### 2.1 安全完整性

在对风险进行识别后,确定其后果严重度,依据最低合理可行的风险接受准则可得到风险的 THR。系统功能的安全完整性可通过结构、方法、工具和技术的有效组合来实现,并且与其安全功能失效的 THR 相关。

安全完整性的定义是“在所有规定条件下和规定时间内,系统实现安全功能的可能性”<sup>[4]</sup>,通常是定量因素(硬件失效)和非定量因素(技术、文件、程序等的失效)的组合。风险的产生是由于其相对应安全功能失效造成的,因此必须根据各子系统安全功能的影响程度,将系统的 THR 按一定的比例分配,每个安全功能均应有对应的 THR 值  $R_{th}$ 。IEC 61508—2010 规定了 SIL 与  $R_{th}$  的关系,如表 1 所示。

表 1 SIL 与 $R_{th}$ 的关系	
SIL	$R_{th}/h$
4	$10^{-9} \sim <10^{-8}$
3	$10^{-8} \sim <10^{-7}$
2	$10^{-7} \sim <10^{-6}$
1	$10^{-6} \sim <10^{-5}$

### 2.2 SIL 分析方法

SIL 分析的方法主要有定性、定量 2 类,其中:定性分析方法采用定性的描述,通过风险可能性及后果确定 SIL,主要有风险图法、风险矩阵法;定量

分析方法通过计算  $R_{th}$  得到对应的 SIL,主要有保护层分析法<sup>[5]</sup>。在实际操作中,大多采用基于风险矩阵法的半定量分析方法,根据风险矩阵为每个安全功能分配 SIL,但这种方法可能会导致系统对 SIL 的过度要求。为了更合理地确定 SIL,本文采用半定量的分析方法<sup>[6]</sup>。确定 SIL 的基本步骤如下:①通过 HAZOP 原则中的子系统危害分析确定系统/子系统的安全功能风险,分析可能的故障和安全问题;②定义后果严重度和相关的  $R_{th}$ ;③明确风险减轻因子,分别为风险群体成员/乘客暴露在危险下的可能性  $E$ 、减少事故的可能性  $P$  及减轻后果的可能性  $C$ ;④分配 SIL 给系统/子系统的安全功能。

后果严重度等级的定义如表 2 所示。风险减轻因子定义及参数的取值<sup>[7]</sup>如表 3 所示。

表 2 后果严重度等级定义		
严重程度	描述	$R_{th}/h$
灾难性的	人员死亡;大量的重伤人员;重大的环境破坏	$<10^{-8}$
严重的	大量的重伤人员;严重的环境破坏	$10^{-8} \sim <10^{-7}$
不严重的	少量的轻伤人员;对环境有严重威胁	$10^{-7} \sim <10^{-6}$
微不足道的	可能有轻伤人员	$\geq 10^{-6}$

注:不同严重程度对应的描述,可以为同时发生,也可以仅为其中任 1 种情况。

表 3 风险减轻因子的定义及参数选取			
参数	等级	定义	取值
乘客暴露可能性 $E$	$E_1$	危害情况发生时风险乘客一直或频繁暴露在危害中	1.00
	$E_2$	保守认为乘客暴露在危害中是罕见的	0.10
	$E_3$	保守认为乘客暴露在危害中是非常罕见的	0.01
减少事故的可能性 $P$	$P_1$	保守认为没有额外的措施来减轻风险演变成事故的概率	1.00
	$P_2$	只有 1 种措施能明确地降低风险演变成事故的概率	0.10
	$P_3$	存在 2 种措施能独立地降低风险演变成事故的概率	0.01
减轻后果的可能性 $C$	$C_1$	保守认为没有额外的措施来避免乘客遭受风险后果的伤害	1.00
	$C_2$	保守认为只有 1 种措施能避免乘客遭受风险后果的伤害	0.10
	$C_3$	保守认为有 2 种以上的措施能避免乘客遭受风险后果的伤害	0.01

根据后果严重度的定义可以得到安全功能风险可容忍率的初始值  $R_{th-i}$ , 结合  $EPC$  风险减轻因子  $E、P、C$  的取值, 计算出该安全功能最终的  $R_{th}$ , 再根据  $R_{th}$  与 SIL 的对应关系可以确定该功能的 SIL。 $R_{th}$  的计算式为:

$$R_{th} = R_{th-i} / (EPC)$$

(1)

此 SIL 分析方法考虑了系统在运营中可能产生风险的非技术条件, 可更合理地确定安全功能的 SIL, 避免安全性的过度设计。

3 应用实例

本文以南宁轨道交通 4 号线的列车安全完整性分析工作为例, 从列车车门、列车网络控制、空气制动等关键系统必须实现的安全功能出发, 通过 HAZOP 识别出系统的潜在风险, 确定各子系统的  $R_{th-i}$ , 在此基础上进行风险减轻因子的 SIL 分析, 最终确定该线列车关键系统安全功能的 SIL。列车关键子系统主要安全功能的 SIL 分析如表 4 所示。

表 4 列车关键子系统主要的安全功能的 SIL 分析表

子系统	安全功能描述	可能的后果	后果严重度	$R_{th-i}/h$	风险减轻因子						$R_{th}/h$	SIL
					$E$		$P$		$C$			
					暴露在危险中的可能性	取值	减轻事故的措施	取值	减轻后果的措施	取值		
客室侧门		列车运行中车门打开,导致乘客跌落、受伤或死亡	灾难性的	$10^{-9}$	频繁	1.00	门控在 3 个信号 (门使能、开门控制、门零速) 同时给出时才允许开门	0.01	无	1.00	$10^{-7}$	2
	乘客上下车时开关门	错误侧开门,导致乘客跌落、受伤或死亡	灾难性的	$10^{-9}$	频繁	1.00	只有门使能、开门命令都处于同一侧才允许打开车门	0.01	无	1.00	$10^{-7}$	2
		门打开状态下列车启动,导致乘客跌落、受伤或死亡	灾难性的	$10^{-9}$	频繁	1.00	车门未关闭状态下封锁牵引;安全回路旁路开关设置铅封;信号系统对开门情况进行保护	0.01	无	1.00	$10^{-7}$	2
列车网络控制	牵引制动控制	牵引制动控制失效,可能导致撞车,乘客受伤或死亡	灾难性的	$10^{-9}$	频繁	1.00	列车网络控制单元做限速保护	0.10	司机操作紧急牵引模式	0.10	$10^{-7}$	2
	信号系统隔离时列车限速	列车超速,可能导致撞车,乘客受伤或死亡	灾难性的	$10^{-9}$	频繁	1.00	列车超速时系统自动施加紧急制动;超速时切除牵引	0.01	司机拍紧急停车按钮	0.10	$10^{-6}$	1
空气制动系统	常用制动	常用制动力不足,可能导致撞车,乘客受伤或死亡	灾难性的	$10^{-9}$	频繁	1.00	无	1.00	切除对应转向架气路,列车限速运行;信号系统施紧急制动	0.01	$10^{-7}$	2
	防滑	防滑失效,导致车轮损伤,制动距离过长	严重的	$10^{-8}$	频繁	1.00	无	0.01	防滑报故障后,司机切除对应转向架气路,列车限速运行	0.10	$10^{-7}$	2
	紧急制动	紧急制动失效,可能导致撞车,乘客受伤或死亡	灾难性的	$10^{-9}$	频繁	1.00	无	1.00	无	1.00	$10^{-9}$	4

注: 为便于分析, 表中的  $R_{th}$  采用固定值。

该线列车为4动2拖编组的B型车,线路等级速度为80 km/h。列车客室侧门采用双扇电控塞拉门,车门的电控电动装置采用微处理器控制的电动机驱动装置,可与列车总线网络进行通信;列车采用总线网络及后备列车导线控制方式,总线由具有冗余结构的多功能车辆总线组成,可对关键区域提供部分冗余;该车型采用架控的模拟式空气制动系统,主要实现常用制动(含快速制动、保持制动)、紧急制动、防滑以及停放制动等功能。

通过HAZOP识别出上述关键子系统主要的安全功能有:乘客上下车时开关门、牵引制动控制、列车限速运行、常用制动、防滑、紧急制动。这些安全功能一旦失效,可能会造成乘客的跌落、受伤或死亡,以及列车碰撞、车轮损伤。分析上述安全功能的后果严重度,确定各子系统的 $R_{th-i}$ ,采用EPC分析方法得到最终的 $R_{th}$ ,最后确定SIL。

根据目前的行业经验及运营安全需求,各关键子系统目前采用的安全完整性等级如下:客室侧门的安全完整性等级为SIL2,网络控制的安全完整性等级为SIL2,制动系统中常用制动功能的安全完整性等级为SIL2,紧急制动功能的安全完整性等级为SIL4。与表4相比可得到结论,客室侧门及空气制动系统的安全功能均符合目前的行业及运营需求,而网络控制的部分安全功能可通过设置风险减轻措施,适当降低其SIL的要求,从而避免为追求安全性而造成过度的资源浪费。

## 4 结语

目前国内的城市轨道交通领域尚缺少一个系

统、完整的安全完整性等级知识体系,许多用户、产品设计人员、RAMS管理人员并未完全理解SIL的概念并掌握SIL的分析方法,刻意追求安全功能的SIL等级,或是将SIL作为产品竞争的要素之一,造成了资源的过度浪费,曲解了安全完整性的意义。本文阐述的SIL分析方法有助于合理地确定列车关键子系统的安全完整性等级,可为从事相关工作的人员提供参考。

## 参考文献

- [1] 郭其一,冯江华,刘可安,等. 可靠性工程与故障诊断技术[M]. 北京:科学出版社,2016:66.
- [2] 燕飞,唐涛,闫宏伟. 安全完善度等级SIL的概念与划分原则研究[J]. 北京交通大学学报,2017(5):79.
- [3] 莫志刚,骆汉宾. 基于HAZOP及ALARP的地铁信号系统安全评估[J]. 机电传动,2018(3):85.
- [4] 董锡明. 轨道列车可靠性、可用性、维修性和安全性(RAMS)[M]. 北京:中国铁道出版社,2009:123.
- [5] 李娜,孙文勇,宁信道. HAZOP、LOPA和SIL方法的应用分析[J]. 中国安全生产科学技术,2012(5):101.
- [6] 杨娟,张小林. 基于EPC因子的有轨电车信号系统安全完善度等级(SIL)评估[J]. 城市轨道交通研究,2018(4):57.
- [7] European Commission. Analysis of safety requirements for MODsafe continuous safety measures and functions[EB/OL]. (2011-1-21) [2019-06-01]. [http://www.modsafe.eu/fileadmin/documents/deliverables/DEL\\_D4\\_2\\_UITP\\_WP4\\_110121\\_V2\\_0.pdf](http://www.modsafe.eu/fileadmin/documents/deliverables/DEL_D4_2_UITP_WP4_110121_V2_0.pdf).

(收稿日期:2019-06-14)

# 拉林铁路6月25日开通运营 复兴号动车组首次开上青藏高原

拉林铁路(拉萨至林芝)于6月25日开通运营,复兴号高原双源动力集中动车组同步投入运营。拉萨至山南、林芝最快1 h 10 min、3 h 29 min 可达。拉林铁路起自拉萨市,经山南市贡嘎县、扎囊县、乃东区、桑日县、加查县和林芝市朗县、米林县,终至林芝市区,全长435.48 km,设计时速160 km,为国家I级单线电气化铁路,初期开通运营办理客货运输业务的有贡嘎、扎囊、山南、桑日、加查、朗县、米林、岗嘎、林芝等9个车站。拉林铁路位于青藏高原冈底斯山与喜马拉雅山之间的藏南谷地,90%以上的线路在海拔3 000 m以上,16次跨越雅鲁藏布江,沿线山高谷深,相对高差达2 500 m,施工难度极大。2015年3月开工建设以来,国铁集团集成运用我国铁路建设实践经验,集中力量对“强岩爆、高地温、冰碛层、风积沙、大变形”等工程难题进行攻关,安全优质建成了47座隧道、121座桥梁,其中有国内最大埋深的巴玉隧道、高地温的桑珠岭隧道和创高海拔、大跨度世界第一的藏木雅鲁藏布江特大桥。拉林铁路开通运营初期,开行拉萨至林芝动车组列车3对,其中2对在客流高峰时期开行;日喀则至林芝开行动车组列车1对;拉萨至林芝开行普速直达特快列车1对。

(摘自2021年6月25日《中国日报》网,记者 达穷、华旦尼玛报道)