

基于风险矩阵的轨道交通车辆安全完整性等级分析

张冬梅 刘 伟

(中车青岛四方机车车辆股份有限公司, 266111, 青岛//第一作者, 工程师)

摘 要 以风险矩阵为基础, 根据可容忍风险边界确定可容忍风险概率。基于 IEC 61508, 考虑潜在风险影响因素, 对可容忍风险概率进行校正, 最终确定轨道交通车辆系统安全功能的安全完整性等级 (SIL)。通过子系统安全功能的 SIL 确定子系统风险承受能力, 采取适当措施管控子系统级风险, 保障列车运行安全。以车门子系统为例, 进行 SIL 分析, 分析结论验证了该方法的合理性, 可为轨道交通车辆 SIL 分析方法提供了理论依据。

关键词 轨道交通; 车辆; 安全完整性等级 (SIL); 风险矩阵; 可容忍风险概率; 安全功能

中图分类号 U270.1

DOI: 10.16037/j.1007-869x.2020.08.015

Research on Safety Integrity Level Analysis of Rail Transit Vehicle Based on Risk Matrix

ZHANG Dongmei, LIU Wei

Abstract Based on the risk matrix, the tolerable risk probability is determined according to the tolerable risk boundary. Based on IEC 61508, the tolerable risk probability is adjusted by considering potential risk factors, thus the safety integrity level (SIL) of the safety function is determined in the end. Through the subsystem safety function SIL, the risk tolerance of the subsystem can be determined, the safety of train operation could be ensured by taking appropriate measures to manage and control the risks. Finally, SIL analysis is carried out based on a train door subsystem, the conclusion verifies the rationality of the method and provides a theoretical basis for rail transit vehicle SIL analysis.

Key words rail transit; vehicle; safety integrity level (SIL); risk matrix; tolerable risk probability; safety function

Author's address CRRC Qingdao Sifang Co., Ltd., 266111, Qingdao, China

轨道交通车辆安全问题应受高度重视。如何更好地通过安全完整性等级 (Safety Integrity Level, 简为 SIL) 分析, 对轨道交通车辆系统失效状态进行评估, 并通过采取管控措施来降低车辆系统风险,

已成为轨道交通车辆安全性研究的重要课题。国内在这方面的研究仍处于初级阶段。

本文以风险矩阵为基础, 结合 IEC 61508: 2000^[1], 针对轨道交通车辆系统安全功能进行安全完整性等级分析, 以确定车辆系统的风险承受能力, 并通过采取适当措施, 使其风险降低到可接受水平, 保障列车运行安全。以某车辆车门子系统为例进行了 SIL 分析, 结论验证了该方法的合理性。

1 SIL 分析

1.1 安全完整性

安全完整性是指安全相关设备在规定的运营环境和时间内, 实现其必须具备的安全功能的能力^[2]。安全完整性与执行安全功能的安全相关系统性能有关。安全完整性由随机失效安全完整性和系统安全完整性组成。

1.2 SIL

SIL 是一种定量指标, 反映的是车辆系统所要求的安全完整性水平。根据安全功能失效的频率和产生风险的严重程度, 安全完整性等级一般分为 SIL4、SIL3、SIL2、SIL1 4 个等级。安全完整性等级越高, 系统完成其安全功能失效的可能性就越小^[3]。

2 SIL 分析方法

2.1 风险矩阵

本文采用半定量分析方法, 以风险矩阵为基础, 确定风险承受能力。

参考 EN 50126: 1999^[3] 中的风险评估表, 总结得到的轨道交通车辆行业惯用的风险矩阵如表 1 所示。

风险等级仅依据风险概率 F 和风险后果的严重程度 S 确定, 其中 S 的取值比如表 2 所示。

表 1 轨道交通车辆风险矩阵

风险发生 概率	风险发生 概率描述	发生频率/(次/h)	风险等级						
			S=7	S=6	S=5	S=4	S=3	S=2	S=1
A	每周发生数次或更多	$\geq 1\times 10^{-2}$	R3	R1	R1	R1	R1	R1	R1
B	每月发生数次	$1\times 10^{-3}\leq <1\times 10^{-2}$	R4	R2	R1	R1	R1	R1	R1
C	每年发生数次	$1\times 10^{-4}\leq <1\times 10^{-3}$	R4	R2	R2	R1	R1	R1	R1
D	十年内发生数次	$1\times 10^{-5}\leq <1\times 10^{-4}$	R4	R3	R2	R1	R1	R1	R1
E	运营以来发生过 1 次	$1\times 10^{-6}\leq <1\times 10^{-5}$	R4	R3	R3	R2	R1	R1	R1
F	不大可能出现	$1\times 10^{-7}\leq <1\times 10^{-6}$	R4	R4	R3	R3	R2	R1	R1
G	非常可能出现	$1\times 10^{-8}\leq <1\times 10^{-7}$	R4	R4	R4	R3	R3	R2	R1
H	发生可能性极少	$1\times 10^{-9}\leq <1\times 10^{-8}$	R4	R4	R4	R4	R3	R3	R2
I	不可能发生	$1\times 10^{-10}\leq <1\times 10^{-9}$	R4	R4	R4	R4	R4	R3	R3
J	难以置信的	$< 1\times 10^{-10}$	R4	R4	R4	R4	R4	R4	R3

注：R1 级为不可容忍的风险，除特殊情况外，必须消除该类风险；R2 级为不希望的风险，必须将该类风险降低至最低实际可行的水平；R3 级为可接受的风险，但仍须按成本效益尽量降低风险；R4 级为可接受的风险；S 为风险后果的严重程度

表 2 S 的取值及其描述

S	严重程度	安全指标			服务指标		
		死亡 数/人	重伤 数/人	轻伤 数/人	系统中 断	线路中 断	车站服 务中断
1	惨重	>50			1 月	数月	1 年
2	灾难性	3~49	>50		1 星期	1 月	数月
3	危急	<3	3~49	>50	1 d	1 星期	1 月
4	严重		<3	3~49	数小时	1 d	1 星期
5	轻微			<3	<30 min	数小时	1 d
6	极轻微					<30 min	数小时
7	微不足道						<30 min

风险矩阵中的灰色区域即 R3 风险等级为可接受的耐受性区域，黑色折线为风险耐受线，表示风险耐受极限。随着 S 的增加，必须通过降低风险概率使风险降到可容忍区域。通过风险耐受线可以确定每个严重度等级的可容忍风险概率（THR）的目标值 R_{TH} 。根据 EN 50129:2018, R_{TH} 和 SIL 的关系如表 3 所示。

表 3 R_{TH} 和 SIL 等级关系

严重度	$R_{TH}/(次/h)$	THR 等级	SIL
惨重	$< 1\times 10^{-10}$	THR4	SIL4
灾难性	$1\times 10^{-10}\leq <1\times 10^{-9}$	THR4	SIL4
危急	$1\times 10^{-9}\leq <1\times 10^{-8}$	THR4	SIL4
严重	$1\times 10^{-8}\leq <1\times 10^{-7}$	THR3	SIL3
临界	$1\times 10^{-7}\leq <1\times 10^{-6}$	THR2	SIL2
微不足道	$1\times 10^{-6}\leq <1\times 10^{-5}$	THR1	SIL1
不重要	$\geq 1\times 10^{-2}$		

风险矩阵法认为，发生的危险将直接导致事故、造成伤害，其对风险作了保守的估计。表 3 中的 THR 等级直接对应 SIL。因此，只需要评估风险潜在后果的严重度类别，就可以确定 SIL。由于风险评估忽视了其他的风险影响因素，所以对安全完整性要求的更多，特别是对于风险后果小于灾难性的风险，要对其 R_{TH} 进行校正。

2.2 R_{TH} 的校正

为了证明各种实际使用的 SIL 分配方法之间的兼容性，本文参考 IEC 61508:2000 系列标准，考虑潜在的风险影响因素，对 R_{TH} 进行校正，即

$$R_{TH,m} = R_{TH}/(EPC), (m = 1, 2, 3, 4)$$

式中：

- $R_{TH,m}$ ——经过校正的可容忍风险概率；
- R_{TH} ——根据风险矩阵确定的未校正可容忍风险概率。

E ——危险暴露的概率；一般情况下，当暴露在危险中的概率是频繁或永久的时， E 取 1；当暴露在危险的概率很小，或只在一些特殊情况（如倒车时有乘客、乘客进入隧道等）下发生时， E 取 0.1；当只在非常罕见的情况下（如在车站的乘客）暴露在危险中，且该情况可以被预料到时， E 取 0.01。

P ——减轻风险或事故发生的概率。当没有额外高效方法或措施来降低风险演变为事故的可能性时， P 取 1；当存在某种措施或情况可明显降低风险演变为事故的可能性时， P 取 0.1；当存在两种或以上措施或情况可明显地独立降低风险演变为事故的可能性时， P 取 0.01。

C ——减轻风险或事故严重度的概率。一般情况下，当没有充分理由支持保守地假定风险群体成员可避免遭受某种风险带来的后果时， C 取 1；当有充分理由支持保守地假定风险群体成员（乘客等）可以避免遭受某种风险带来的后果时， C 取 0.1；当有两个或以上独立的充分理由能保守地假定风险群体成员（乘客等）可以避免遭受某种风险带来的后果时， C 取 0.01。

2.3 SIL 分析步骤

确定车辆安全相关子系统的 SIL 主要步骤包括：

- 1) 车辆系统定义;
- 2) 危害识别及风险评估,确定车辆安全相关子系统并识别子系统的安全相关功能;
- 3) 可容忍风险概率的确定及校正;
- 4) SIL 的确定。

2.3.1 车辆系统定义

对车辆系统进行明确定义,包括车辆系统的功能概要、系统范围、技术指标、相关接口等,以便为车辆系统风险分析提供明确的输入条件。

2.3.2 风险识别及评估

在明确车辆系统后,识别车辆各状态或特征存在的潜在风险,以明确车辆系统的相关风险。风险识别可以采用头脑风暴方法,也可以建立在经验总结的基础上。

根据风险矩阵,对所识别风险的发生可能性及严重程度进行评估。根据识别的风险及其缓解措施,确定车辆安全相关子系统并识别子系统的安全相关功能。

2.3.3 可容忍风险概率的确定及校正

根据风险矩阵可容忍边界确定 R_{TH} ,利用式(1)对 R_{TH} 进行校正得到 $R_{TH,m}$ 。

2.3.4 SIL 确定

根据各子系统安全功能的 $R_{TH,m}$ 值和表 2 来确定 SIL。在得出单个安全功能的 SIL 后,选择各子系统中最高的 SIL 等级作为车辆安全相关子系统的 SIL 等级。

这说明,一个子系统的 SIL 等级是子系统中各个安全功能的最大 SIL,即对于一个子系统的各安全功能来说,有可能存在 SIL1、SIL2、SIL3、SIL4,但对于子系统,必须满足子系统最大安全要求。

3 SIL 分析法的应用

本文以某城市轨道交通车辆车门子系统为例,对其进行 SIL 分析。车门子系统常见的风险及后果严重度见表 4。

表 4 车门设备主要风险识别及评估

序号	部件或功能	位置	风险类别	风险描述	风险原因	后果描述	风险概率	严重程度	风险等级
1	门控部件	站台	意外	到站车门未打开	①EDCU(电子门控单元)故障;②门锁闭装置故障;③门电路故障;④信号系统未传输信号;⑤关门按钮卡住;⑥未接收到零速信号	乘客因情绪失控造成挤压受伤	D	5	R2
2	门控部件	站台	意外	到站后非站台侧车门打开	①信号系统传输错误指令;②EDCU故障;③门电路故障;④司机操作失误(人工驾驶模式)	乘客掉落后续电伤亡	G	2	R2
3	门控部件	正线	意外	列车在运行中,某个车门意外打开	①EDCU 故障;②门锁闭装置故障;③门电路故障;④信号系统意外发出车门开启信号;⑤门板与驱动机构分离;⑥机械部件失效	乘客跌落,导致乘客伤亡	F	3	R2
4	门控部件	正线	意外	列车在运行中,一侧客室车门意外打开	①EDCU 故障;②门电路故障;③信号系统意外发出车门开启信号	乘客掉落轨道上导致伤亡	G	2	R2
5	门控部件	正线	意外	列车紧急情况下车门无法打开	①EDCU 故障;②门锁闭装置故障;③门电路故障;④信号系统没有给出车门打开信号;⑤开门按钮故障;⑥零速信号丢失,无零速信号下操作内紧急由于电机堵转导致车门很难打开	乘客无法逃生导致伤亡	F	3	R2
6	障碍物探测	正线	意外	车门夹住乘客物品,导致乘客不能移动	①乘客疏忽;②车门没有防挤压功能或其功能失效;③夹着物体体积太小或太薄;④车门关门力过大;⑤EDCU故障	乘客伤亡	F	3	R2

车门安全功能正常的表现为:车门在站台能够准确打开,为乘客提供上下列车的通道;在运行线路中车门保持关闭,为乘客提供封闭的空间;列车发生紧急情况时,车门可被打开以供乘客逃生;车门能检测障碍物,防止夹住乘客及其他物品等。根据车门子系统的上述风险分析,可确定车门子系统安全功能的严重度,以进行 SIL 分析。相关 SIL 分

析列表见表 5。

根据表 5,选择等级最高的 SIL2 作为车门子系统安全完整性等级。这一结论符合当前国内外车门子系统开发设计等级。

目前的轨道交通车辆车门子系统均已取得 SIL2 等级证书。

表 5 车门设备的安全功能 SIL 分析表

安全功能	无此功能的影响	严重程度	<i>E</i>	<i>P</i>	<i>C</i>	<i>E、P、C</i> 的取值依据	R_{TH}	$R_{TH,m}$	SIL
准确打开车门	车门打不开,紧急情况下乘客无法逃生。到站后非站台侧车门打开	2	0.1	0.01	1	<i>E</i> :只在紧急模式下; <i>P</i> :设有紧急解锁装置;司机室设有两套开门按钮; <i>C</i> :无措施	$1\times10^{-10}\leqslant$ $<1\times10^{-9}$	$1\times10^{-7}\leqslant$ $<1\times10^{-6}$	SIL2
车门保持关闭	车门意外打开(或车门误打开),乘客跌落至轨道	2	0.1	0.01	1	<i>E</i> :在少数情况下发生 <i>P</i> :车门装有锁闭系统;只有同时接收到零速度列车线信号和开门指令列车线信号车门才能打开; <i>C</i> :无	$1\times10^{-10}\leqslant$ $<1\times10^{-9}$	$1\times10^{-7}\leqslant$ $<1\times10^{-6}$	SIL2
车门紧急解锁	车门无法解锁,紧急情况下乘客无法逃生	3	0.1	0.01	1	<i>E</i> :只在紧急模式下; <i>P</i> :设置有内外紧急解锁装置;司机室设有两套开门按钮; <i>C</i> :无	$1\times10^{-9}\leqslant$ $<1\times10^{-8}$	$1\times10^{-6}\leqslant$ $<1\times10^{-5}$	SIL1
障碍物检测	未检测到障碍物,乘客被夹住不能移动,列车运行导致乘客伤亡	3	0.1	0.1	0.1	<i>E</i> :在少数情况下发生; <i>P</i> :设置防挤压功能;当车门夹着物体时,车门自动打开,释放物体; <i>C</i> :设置防夹胶条	$1\times10^{-9}\leqslant$ $<1\times10^{-8}$	$1\times10^{-6}\leqslant$ $<1\times10^{-5}$	SIL1
列车需在车门全部关闭和锁闭状态下启动	车门开着而列车启动,乘客跌落导致伤亡	2	0.01	0.01	1	<i>E</i> :极少情况下发生; <i>P</i> :当车门未全关闭会切除牵引;司机通过车门检测系统检测到; <i>C</i> :无	$1\times10^{-10}\leqslant$ $<1\times10^{-9}$	$1\times10^{-6}\leqslant$ $<1\times10^{-5}$	SIL1

4 结语

本文以风险矩阵为基础,通过可容忍风险边界确定可容忍风险概率;基于 IEC 61508:2000 标准,对可容忍风险概率进行校正,对轨道交通车辆系统安全功能进行 SIL 分析。通过分析系统 SIL 以确定系统风险承受能力,采取适当措施对风险进行管控,保障列车运行安全。以某车辆车门子系统为例,进行了 SIL 分析方法应用,结论验证了该方法的合理性,为车辆各子系统 SIL 分析研究提供了理论依据。

参考文献

[1] International Electro technical Commission Std. Functional Safe-

(上接第 61 页)

在施工过程中除考虑混凝土施工工艺外,还需注意土体回填过程中土体的回填速度产生的荷载大小及压实过程中动荷载的大小。切实从施工各阶段抓起,贯彻好“预防为主”的思想。只有这样,才能有效减少施工过程中混凝土结构的裂缝。

参考文献

[1] 齐锋,陈晓宝. 对复合式地铁站内衬墙开裂原因的探讨[J]. 施工技术,2006(10): 55.
[2] 谭谨. 地铁车站主体结构混凝土开裂温度场数值分析[D]. 长沙:湖南工业大学,2015.
[3] 张翠强,田力达,李六连,等. 基于监测数据的地铁车站混凝土早期开裂风险评估[J]. 建筑结构,2017(增刊1): 939.
[4] 许尚农,钟可,黄毅翔,等. 长沙地铁 4 号线车站侧墙带模板

ty of Electrical/Electronic/Programmable Electronic Safety-Related Systems; IEC 61508;2000[S]. Geneva;International Electro technical Commission Std,2010.
[2] CENELEC. Railway applications-Communications,signaling and processing systems. Safety related electronic systems for signaling; EN 50129;2018[S]. Brussels;CENELEC,2018.
[3] CENELEC. Railway Applications-The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)-Part 2;Systems Approach to Safety; EN 50126; 1999 [S]. Brussels;CENELEC,2017.
[4] WEI G. Prediction of soil settlement caused by double-line parallel shield tunnel construction [J]. Disaster Advances, 2013 (6): 23.

(收稿日期:2018-10-26)

养护技术研究[J]. 施工技术,2017(20): 87.
[5] 段岳强,林金华. 浅谈地铁车站结构侧墙裂缝控制的施工技术[J]. 城市建设理论研究,2018(1): 139.
[6] 陈肇元,崔京浩,朱金铨,等. 钢筋混凝土裂缝机理与控制措施[J]. 工程力学,2006(增刊1): 86.
[7] 朱耀台,詹树林. 混凝土裂缝成因与防治措施研究[J]. 材料科学与工程学报,2003(5): 727.
[8] 袁敬强,陈卫忠,黄世武,等. 全风化花岗岩注浆加固特性试验研究[J]. 岩石力学与工程学报,2016(增刊1): 2876.
[9] 周振强. 连拱隧道浅埋暗挖法施工对地面下沉控制与试验研究[C]//中国市政工程协会. 城市地下空间开发与地下工程施工技术高层论坛论文集. 北京:北京市市政工程总公司(集团),2004.

(收稿日期:2018-10-19)