

# 基于 MODSafe 方法的 APM 安全完整性等级分配

王一先 陈 瑱 管佩瑶

(中车浦镇阿尔斯通运输系统有限公司, 241060, 芜湖)

**摘 要** [目的] APM(旅客捷运系统)对安全性的要求非常高,既有的 SIL(安全完整性等级)分配方法难以高效、准确满足 APM 项目的需求。为确保 APM 的安全性和可靠性,应对 APM 的 SIL 分配、确定安全目标进行更为深入的研究。[方法] 阐述了 APM 既有的 SIL 分配方法,提出采用目前已获得多方认可的 MODSafe(模块化城市交通安全保障分析)方法对 APM 的 SIL 进行分配。介绍了 MODSafe 方法的基本步骤,明确了高安全需求、低安全需求 2 种模式下 APM 的 SIL 分配步骤。进一步以 APM 的列车冲击控制功能为例,阐述了基于 MODSafe 方法进行 SIL 分配的技术思路。[结果及结论] 在设计初期就对安全功能进行识别并且确认安全目标,对 APM 项目的安全交付和开通运营等至关重要。MODSafe 方法可用于定量确定 APM 安全功能的 THR(可容忍危害率)及 SIL。

**关键词** 城市轨道交通;旅客捷运系统;安全完整性等级;可容忍危害率;模块化城市交通安全保障分析方法;列车冲击控制

中图分类号 U298:U239.8

DOI:10.16037/j.1007-869x.2024.09.013

## SIL Allocation of APM Based on MODSafe Method

WANG Yixian, CHEN Zhen, GUAN Peiyao

(CRRC Puzhen Alstom Transportation Systems Ltd., 241060, Wuhu, China)

**Abstract** [Objective] APM (automated people mover) has very high requirements for safety, and the existing SIL (safety integrity level) allocation method cannot meet the demand of APM projects efficiently and accurately. In order to ensure the safety and reliability of APM, further in-depth research should be conducted on the allocation of SIL and the determination of the safety targets for APM. [Method] The existing methods for SIL allocation in APM are elaborated, and a widely recognized method MODSafe (modular urban transport safety and security analysis) is proposed and applied for SIL allocation of APM. The basic steps of the MODSafe method are introduced, and the respective SIL allocation steps are clarified under the two modes of high and low safety demands. The technical idea for conducting SIL allocation based on MODSafe method is

further elaborated with the train jerk control function of APM as the example. [Result & Conclusion] Identifying safety functions and determining safety targets in the initial design phase is crucial for the safe delivery, operation and other aspects of APM projects. The MODSafe method can be used to quantitatively determine the THR (tolerable hazard rate) and SIL of APM safety functions.

**Key words** urban rail transit; APM; SIL; THR; MODSafe method; train jerk control

APM(旅客捷运系统)是城市轨道交通 GOA4(无人干预列车运行)的“交钥匙”工程。基于 APM 的整体安全目标考虑,设计时将安全目标分配至 APM 各子系统(信号、车辆、供电、站台门等),以保证整体集成具有较高的可靠性、可用性和安全性。既有的 SIL(安全完整性等级)分配方法难以高效、准确满足 APM 项目的需求。为确保 APM 的安全性和可靠性,本文对 APM 的 SIL 分配、确定安全目标进行更为深入的研究。

## 1 APM 安全完整性等级分配的方法

### 1.1 SIL 的概念

SIL 在城市轨道交通系统集成项目中应用广泛。EN 50126:2017 *Railway Applications-The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)* 要求,在项目初期应对系统进行安全需求识别,并基于系统的安全功能分配相应的 SIL。根据 EN 50128:2011 *Railway Applications-Communications, Signaling and Processing Systems-Software for Railway Control and Protection Systems* 和 EN 50129:2018 *Railway Applications-Communications, Signaling and Processing Systems-Safety-related Electronic Systems for Signaling* 的要求,应通过安全技术手段(如采用冗余结构等)来降低硬件的随机失效率,并通过优化质量管控和安全管理流程来保证降低系统性失效的目

标得以实现。

确定 SIL 的过程主要包括以下步骤:①从功能要求清单中确定与系统相关的安全功能;②识别可能的故障及安全隐患;③确定相应危害的严重程度及其可容忍危害率;④识别危害的风险影响因素;⑤为子系统分配 SIL。

## 1.2 SIL 分配的既有方法

IEC 61508:2010 *Functional safety of electrical/electronic/programmable electronic safety-related systems* 中定义了 SIL 分配的一些方法,如风险图法、LOPA(保护层分析)法等。风险图法主要基于不同风险,对人员、环境、财产的影响程度和发生频率等方面,以及不期望事件发生的频率、是否能避免事故发生等进行分析,进而确定 SIL。LOPA 法是一种简化的风险评估方法,通过对现有保护措施的可操作性进行量化评估,以确定其消除或降低风险的能力。上述方法仅为 SIL 分配提供了理论基础,并没有提供具体的分配步骤及实施的技术路线。

目前 APM 列车一般采用 CBTC 移动闭塞信号系统。不同于常规的城市轨道交通列车,APM 车辆子系统并没有自身的制动控制单元,而是通过 TCMS(列车控制与管理系统)来实现对列车的电制动与空气制动转化、列车的空气制动控制。由于 APM 车辆子系统控制方式的特殊性,且 APM 低安全需求的安全功能越来越受到了城市轨道交通业主的关注,既有的 SIL 分配方法很难高效、准确地满足 APM 项目的需求。

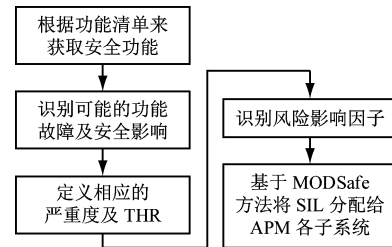
2012 年,德国学者 Wigger 提出了 MODSafe(模块化城市交通安全保障分析)方法。该方法可为定量的 SIL 分配提供具体的分配步骤。MODSafe 方法是一种半定量的方法,依据 CENELEC(欧洲电工技术标准化委员会)编写的 EN 50126:1999 *Railway applications-The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)*,该法有效地将功能安全需求分解到复杂

的系统结构中,并通过定性和定量的方法将安全指标分配到各子系统的安全功能中。MODSafe 方法同时还提供了高安全需求和低安全需求 2 种模式下的 SIL 分配步骤。

## 2 基于 MODSafe 方法的 SIL 分配

### 2.1 MODSafe 方法的基本步骤

基于 MODSafe 方法的 SIL 分配步骤如图 1 所示。



注:THR—可容忍危害率。

图1 基于 MODSafe 方法的 SIL 分配步骤

Fig.1 SIL allocation steps based on MODSafe

### 2.2 高安全需求模式下的 SIL 分配

本文进一步对 APM 高安全需求和低安全需求 2 种模式下的 SIL 分配步骤进行研究。MODSafe 方法采用半定量的方法来分配 SIL,即:仅根据危害的严重程度来决定 SIL,而不考虑其他的因素。这种半定量的方法因忽略了影响到系统安全的部分风险(大多为不会导致产生灾难性后果的风险),可能会产生过于严苛的 SIL 要求。为了避免此问题的发生,MODSafe 方法参照 IEC 61508:2010 及其他标准,引入了 3 个可能影响危害的因子来修订 SIL。这 3 个因子分别是:危险暴露的可能性  $E$ 、减少事故的可能性  $P$ 、减少后果的可能性  $C$ 。结合 ASCE(美国土木工程师协会)编制的 ASCE 21:2021 *Automated People Mover Standards* 的风险矩阵,通过严重程度等级可获得 THR,设  $r_{TH}$  为在单位时间(1 h)内每个功能的 THR 值,通过  $r_{TH}$  获得对应的 SIL,如表 1 所示。

表1 严重度与  $r_{TH}$ 、SIL 的对应表

Tab.1 Correlation between Severity,  $r_{TH}$  and SIL

严重度等级 $n$	严重度表述	事件的后果	$r_{TH}/h$	SIL
$n=1$	灾难性的	人员死亡;系统重大损失;环境被严重破坏	$10^{-9} \sim < 10^{-8}$	SIL4
$n=2$	危险的	人员重伤或患严重的职业病;主要系统或环境发生较严重损害	$10^{-8} \sim < 10^{-7}$	SIL3
$n=3$	最低限度的	人员轻伤或患轻微职业病;系统或环境有轻微损害	$10^{-7} \sim < 10^{-6}$	SIL2
$n=4$	可忽略的	人员轻伤或患微乎其微职业病;系统或环境有微乎其微损害	$10^{-6} \sim < 10^{-5}$	SIL1

高安全需求模式下, APM 的 SIL 分配步骤如下:

步骤 1 根据表 1 中的严重度确定  $r_{TH}$ , 通常根据最恶劣的情况取值。

步骤 2 确定风险影响因子的值。考虑是否有使  $E$  数量级减少的可能性, 设定永久暴露在危险区域时  $E = 1.00$ , 很少暴露在危险区域时  $E = 0.10$ , 非常少暴露在危险区域时  $E = 0.01$ ; 没有防护措施时  $P = 1.00$ , 有 1 个防护措施时  $P = 0.10$ , 有 2 个防护措施时  $P = 0.01$ ; 没有任何防护措施能减轻后果时  $C = 1.00$ , 有 1 个防护措施能减轻后果时  $C = 0.10$ , 有 2 个防护措施能减轻后果时  $C = 0.01$ 。

步骤 3 根据式(1)计算修正后的 THR, 此时得到的 THR 值为  $r_{TH,C}$ , 然后根据  $r_{TH,C}$  和 SIL 的对应表(见表 2), 查找得出对应 SIL。

$$r_{TH,C} = r_{TH} / (EPC) \quad (1)$$

表 2  $r_{TH,C}$  和 SIL 的对应表

Tab. 2 Correlation between  $r_{TH,C}$  and SIL

$r_{TH,C}/h$	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
$\geq 10^{-5}$	BI

注: 根据 EN 50126:2017, BI 为基础完整性, 即最低的安全完整性要求。

### 2.3 低安全需求模式下的 SIL 分配

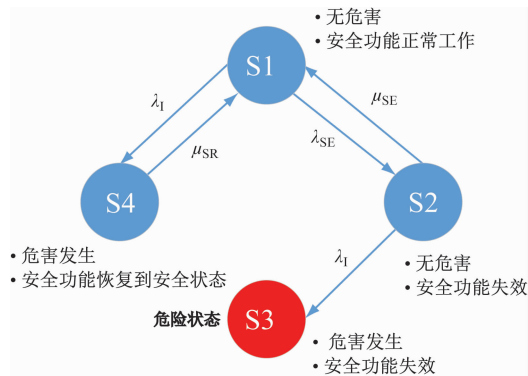
大多数安全功能需要始终或持续处于工作状态, 部分安全功能仅在有需要时才施加防护。一般来说, 低安全需求模式指的是: ①安全功能的失效不会立刻导致系统处于危险状态; ②使用高安全需求显得过分保守; ③安全功能的使用频率很低。

目前, EN 50126:2017 没有低安全需求功能这一概念, 但 IEC 61508:2010 中同时包含了高安全需求和低安全需求的条件。IEC 61508:2010 规定: 对低安全需求的功能, 在需要执行功能时, 将此类功能的平均失效率下限定为  $10^{-5}/h$ , 功能的使用频率则取决于危害的具体情况, 其值应小于等于 1 次/年。

对于此类低安全需求功能, MODSafe 方法提供了 3 种不同的概率: 危害发生概率  $\lambda_1$ 、安全功能失

效率  $\lambda_{SE}$ 、安全功能检查/修复概率  $\mu_{SE}$  (不含无法检查的故障发生概率)。假设系统的健康状态没有采取非持续检查方式 (如采用校验、目视检查、诊断等), 而是基于  $\mu_{SE}$  进行检查 ( $\mu_{SE}$  远大于失效率及危险事件发生率)。对于检测到的故障而言, 假设故障可被消除, 则系统可恢复到安全状态。

图 2 为低安全需求模式下各系统状态间的关系网。



注: S1、S2、S3、S4—系统不同状态;  $\mu_{SR}$ —危害修复概率。

图 2 低安全需求模式下各系统状态间的关系网

Fig. 2 Relation network of all system states under the mode of low safety demand

根据图 2 所示的关系网, 可以通过对应的流程来确定低安全需求模式下的 SIL:

步骤 1 对潜在的非安全事件, 评估其  $\lambda_1$ ;

步骤 2 若该事件会导致事故, 则确定该事件的后果, 并参照表 1 将严重度转换为  $r_{TH}$  (通常按最不利情况取值);

步骤 3 设  $\lambda_{sys}$  为系统的总失效率, 通过式(2)调整  $\lambda_{SE}$  和  $\mu_{SE}$  的关系:

$$\lambda_{sys} \approx r_{TH} = \lambda_{SE} \lambda_1 / \mu_{SE} \quad (2)$$

步骤 4 计算得到  $\mu_{SE}$ , 然后根据  $\lambda_{SE}$  和 SIL 的对应表(见表 3), 得到  $\lambda_{SE}$ , 进而确定对应的 SIL。

表 3  $\lambda_{SE}$  和 SIL 的对应表

Tab. 3 Correlation between  $\lambda_{SE}$  and SIL

$\lambda_{SE}/h$	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
$\geq 10^{-5}$	BI

### 3 列车冲击控制功能的 SIL 分配

以 APM 的列车冲击控制功能为例进行研究。该功能属于高安全需求,执行该功能的相关子系统的 SIL 分配结果如表 4 所示。

表 4 高安全需求下列车冲击控制功能的 SIL 分配表

Tab.4 SIL allocation of train jerk control function under the high safety demand mode

安全功能	功能失效的影响	功能失效导致的安全后果	执行功能的设备	严重度	$r_{TH}/h$	$E$	$P$	$C$	$r_{TH,C}/h$	SIL	$E、P、C$ 的取值依据
列车加速、保持列车牵引速度	列车加速度过大,或电制动减速度过大	可能导致车内乘客跌倒或滑倒	牵引控制单元	危险的 ( $n=2$ )	$1.0 \times 10^{-7}$	1.00	0.01	0.10	$1.0 \times 10^{-4}$	BI	存在持续暴露危险, $E=1.00$ ;信号和 TCMS 均有冲击控制功能, $P=0.01$ ;客室内有扶手和横杆, $C=0.10$
列车冲击控制	列车加速度过大,或制动减速度过大	可能导致车内乘客跌倒或滑倒	TCMS	危险的 ( $n=2$ )	$1.0 \times 10^{-7}$	1.00	0.10	0.10	$1.0 \times 10^{-5}$	BI	存在持续暴露危险, $E=1.00$ ;信号有冲击控制功能, $P=0.01$ ;客室内有扶手和横杆, $C=0.10$
自动调节列车运行速度	无法控制列车运行(因出现了过大的加速度或减速度)	可能导致车内乘客跌倒或滑倒	ATC	危险的 ( $n=2$ )	$1.0 \times 10^{-7}$	1.00	0.10	0.10	$1.0 \times 10^{-5}$	BI	存在持续暴露危险, $E=1.00$ ;最恶劣情形下,仅在摩擦制动下 TCMS 有冲击控制功能, $P=0.01$ ;客室内有扶手和横杆, $C=0.10$

在 APM 处于降级或紧急模式下(如发生信号宕机等情况),需要人工驾驶列车将乘客送往目的地。考虑到 APM 的降级或紧急模式为低安全需求条件,因此,采用低安全需求的 SIL 分配方法对牵引

由表 4 可知:在高安全需求下,牵引控制单元、TCMS 和 ATC 对列车冲击控制功能的 SIL 均为 BI,这与 APM 子系统设计的软件和硬件要求均符合。ATC 尽管涉及到安全子系统,但执行列车冲击控制功能时,ATC 的 SIL 并不需要高于 BI。

控制单元和 TCMS 的安全功能进行验证,相关子系统的 SIL 分配结果如表 5 所示。由表 5 可知:牵引控制单元和 TCMS 在低安全需求下仍然只需要符合 BI 要求,这与高安全需求下的 SIL 要求一致。

表 5 低安全需求下列车冲击控制功能的 SIL 分配表

Tab.5 SIL allocation of train jerk control function under the low safety demand

安全功能	功能失效的影响	功能失效导致的安全后果	执行功能的设备	严重度	$r_{TH}/h$	$\lambda_I$	$\mu_{SE}$	$\lambda_{SE}$	SIL	$\lambda_I$ 及 $\mu_{SE}$ 的取值依据
列车加速、保持列车牵引速度	列车加速度过大,或电制动减速度过大	可能导致车内乘客跌倒或滑倒	牵引控制单元	危险的 ( $n=2$ )	$1.0 \times 10^{-7}$	$1.1 \times 10^{-4}$	0.54	$4.91 \times 10^{-4}$	BI	$\lambda_I$ 由手动驾驶占空比及列车每年的使用频次来决定; $\mu_{SE}$ 根据牵引控制单元的检查周期及自检周期换算得到
列车冲击控制	列车加速度过大,或制动减速度过大	可能导致车内乘客跌倒或滑倒	TCMS	危险的 ( $n=2$ )	$1.0 \times 10^{-7}$	$1.1 \times 10^{-4}$	1.04	$9.47 \times 10^{-4}$	BI	$\lambda_I$ 由手动驾驶占空比及列车每年的使用频次来决定; $\mu_{SE}$ 根据 TCMS 的检查周期及自检周期换算得到

注:手动驾驶占空比指采用手动驾驶模式的时长在整个运营时长中的占比。

根据目前行业经验及 APM 设计的通用安全架构,APM 各关键子系统安全功能的 SIL 要求如下:牵引控制单元的 SIL 为 BI;TCMS 的 SIL 为 BI;ATO 的 SIL 为 BI。这与本文采用 MODSafe 方法计

算得到的各关键子系统所有安全功能的 SIL 分配结果一致,进而验证了该方法在城市轨道交通中应用的有效性。

(下转第 86 页)



间计算最短路径,使得根据最短路径计算应急救援站备选点的覆盖范围时更为精确。此外,本文考虑了时间、救援关系、成本 3 个方面的约束条件,建立了以最小化系统最大救援时间为目标的  $P$ -中心选址模型。

以武汉市轨道交通应急救援站选址为对象应用该模型,结合网络中心性与站点性质分析确定了必选点与备选点,运用自适应遗传算法在 MATLAB 软件中进行编程求解,最终确定设置 25 座应急站,最大救援时间为 11.611 2 min 的最佳选址方案。与相似研究进行对比,本方案投入更少但效益更大,这证明本研究具有先进性。

目前城市轨道交通线网应急救援站选址的研究中,选取备选点与必选点的过程仍具有一定的主观性。如何提高量化分析的比重,进一步降低选址研究的主观性,值得进一步深入研究。

## 参考文献

- [1] 孙彩红. 基于网络化的地铁应急救援站选址方法研究[J]. 科技信息, 2010(28): 775.  
SUN Caihong. Research on the location method of subway emergency rescue station based on network[J]. Science & Technology Information, 2010(28): 775.
- [2] 李刚. 基于网络中心性的城市轨道交通应急救援站选址研究[D]. 北京: 北京交通大学, 2014.  
LI Gang. Research on location of urban rail transit emergency res-

cue stations based on network centrality[D]. Beijing: Beijing Jiaotong University, 2014.

- [3] 祝蕾. 基于复杂网络理论的城市轨道交通应急救援站选址研究[D]. 南京: 东南大学, 2018.  
ZHU Lei. Research on location of urban rail transit emergency rescue stations based on complex network theory [D]. Nanjing: Southeast University, 2018.
  - [4] 冉连月. 基于复杂网络的城市轨道交通灾害风险与脆弱性研究[D]. 武汉: 华中科技大学, 2019.  
RAN Lianye. Research on disaster risk and vulnerability of rail transit based on complex network[D]. Wuhan: Huazhong University of Science and Technology, 2019.
  - [5] 曹璇, 胡锐, 郭兆能, 等. 城市轨道交通应急资源选址和配置方法研究[J]. 交通运输研究, 2016, 2(4): 54.  
CAO Liu, HU Rui, GUO Zhaoneng, et al. Emergency resource location and distribution of urban rail transit[J]. Transport Research, 2016, 2(4): 54.
  - [6] 张梅. 城市轨道交通线网应急救援站的选址应用研究[D]. 天津: 天津大学, 2018.  
ZHANG Mei. Study on the application of location selection of urban rail transit emergency station[D]. Tianjin: Tianjin University, 2018.
- 收稿日期:2022-05-09 修回日期:2022-09-08 出版日期:2024-09-10  
Received:2022-05-09 Revised:2022-09-08 Published:2024-09-10  
· 通信作者:吴莹,助理工程师,wuying5584@cug.edu.cn  
· ©《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

(上接第 79 页)

## 4 结语

在设计初期对安全功能进行识别并分配安全目标,对 APM 项目的安全交付和开通运营至关重要。此外,通过安全目标的识别和验证,还可以防止 SIL 的过度使用,避免由此带来的资源浪费。MODSafe 方法作为一种获得多方认可的 SIL 分配的通用方法,为半定量分析高安全需求模式和低安全需求模式下的 SIL 及 SIL 分配提供了简单可行的方法论,填补了既有标准中的空白。随着城市轨道交通的进一步发展及业内对安全认证需求的持续提升,本文阐述的 SIL 分配方法可为 APM 等集成类系统 SIL 的确定及评估提供参考。

## 参考文献

- [1] 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, 41(5): 79.

- YAN Fei, TANG Tao, YAN Hongwei. Research on concept and allocation principle of safety integrity level[J]. Journal of Beijing Jiaotong University, 2017, 41(5): 79.
- [2] WIGGER P. MODSafe-modular urban transport safety and security analysis[J]. Procedia-Social and Behavioral Sciences, 2012, 48: 2616.
- [3] 娄琦. 旅客自动运输系统(APM)全自动驾驶应用解析[J]. 城市轨道交通研究, 2016, 19(增刊2): 16.  
LOU Qi. Application analysis of automatic passenger transportation system (APM) driving[J]. Urban Mass Transit, 2016, 19(S2): 16.

· 收稿日期:2022-05-24 修回日期:2022-06-22 出版日期:2024-09-10  
Received:2022-05-24 Revised:2022-06-22 Published:2024-09-10  
· 通信作者:王一先,工程师,wang.yixian@pats-crrc.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