城市轨道交通全自动运行车辆系统初步隐患分析

宋小广
（上海申通轨道交通研究咨询有限公司，200070，上海//工程师）

摘　要　介绍了城市轨道交通FAO（全自动运行）车辆系统的特点，剖析了FAO项目中车辆系统初步隐患分析的现状。基于RAMS（可靠性、可用性、可维修性、安全性）相关标准及规范提出了一套初步隐患分析的方法，包括隐患识别、风险评估和风险控制等。将该方法应用于某FAO项目中，对车辆系统的顶层危害进行分析并得出安全隐患事件风险的消除和控制措施，为系统安全保证奠定了基础。

关键词　城市轨道交通；全自动运行；车辆系统；初步隐患
中图分类号　U298：U270
DOI：10.16037/j.1007－869x.2023.02.012

Preliminary Analysis of Urban Rail Transit FAO Vehicle System Hidden Hazard

SONG Xiaoguang

Abstract　The characteristics of urban rail transit FAO (fully automatic operation) vehicle system are introduced. The current situation of FAO project vehicle system hidden hazard preliminary analysis is analyzed. Based on the standards and specifications related to RAMS (reliability, availability, maintainability, safety), a set of hidden hazard preliminary analysis methods is proposed, including hidden hazard identification, risk assessment and risk control. This method will be applied to a FAO project, where the top-level hazard of the vehicle system will be analyzed and the risk elimination and control measures will be obtained, laying foundation for ensuring system safety.

Key words　urban rail transit; FAO; vehicle system; hidden hazard

Author's address　Shanghai Shentong Rail Transit Research & Consultancy Co., Ltd., 200070, Shanghai, China

T/CAMET 04017.1—2019《城市轨道交通全自动运行系统规范第1部分：需求》在GB/T 32590.1—2016《轨道交通城市轨道交通运输管理和指令控制系统 第1部分：系统原理》的基础上，从列车运行过程所需完成各项功能的人和设备职责划分的角度，定义了适应于我国城市轨道交通的不同运行自动化等级。由于FAO（全自动运行）自动化程度高，要求系统关键设备具有更加完备的冗余性、高集成性、可维护性及高安全性。而车辆系统作为运输服务的主体，对其进行安全性分析和研究十分重要。

1　FAO车辆系统的特点

与非FAO车辆相比，FAO车辆在系统架构、系统接口、系统功能和性能等方面均有所完善和提高。具体体现在：

1）在系统架构方面，最显著的特点是车厢内司机室的变化，即取消司机室或隐藏司机室座椅，取消后端墙，对司机台进行全封闭，取消了司机的驾驶行为，实现无人驾驶。从车底架构进行比较，FAO车辆系统均设置了障碍物检测装置、车辆脱轨检测装置和走行部在线检测系统。在车辆行驶过程中，实时检测走行部关键部位状态信息并将其上传至TCMS（列车控制和管理系统）及控制中心。在车辆行驶发生异常时接收到障碍物检测和脱轨检测信息后，触发紧急制动，同时将此信息发送至TCMS，起到了监控轨道并减少损失的作用[1]。

2）在系统功能和接口方面，智能化的系统控制和联动功能，能够实现列车从全自动的唤醒自检到回库休眠的投入/退出运营流程，提高了列车的运行控制水平。在关键设备出现故障时，TCMS可以处置相关故障信息并将其上传控制中心，以实现远程人工处置，增强了安全监控和应急管理能力。

3）在车辆系统性能方面，对紧急疏散门、紧急制动、常用制动及牵引系统等关键功能的安全完整性等级，以及关键设备的可靠性有了更高的要求，从而使故障导向安全的设计理念不断增强。因此，随着FAO功能的不断智能化和集成化，对其功能的安全需求进行全面的识别和分析变得非常重要。

2　FAO车辆系统初步隐患分析

2.1　初步隐患分析与系统安全保证

BS EN 50126-1：2017 *Railway applications*：*the*

specification and demonstration of Reliability, *Availability*, *Maintainability and Safety*（*RAMS*）描述了风险分析的方法，指出基于风险的方法是 RAMS（可靠性、可用性、可维护性和安全性）管理过程的基础。因此，可通过该方法识别风险得出安全需求，并采取措施以避免或控制风险。

风险分析和评估在生命周期各阶段是不断更新迭代的。随着设计的进展，风险评估应在整个设计进度的适当阶段重复进行，同时应达到适当的深度。为了对安全隐患事件的风险进行全方位的分析和管理，实现系统的安全保证，需要从 FAO 系统、车辆系统、子系统、组件、系统间接口，以及人为操作方面对隐患进行分析。分析方法一般包括初步隐患分析、子系统隐患分析、接口隐患分析、操作与支持分析、故障模式影响及危害度分析等，如图 1 所示。

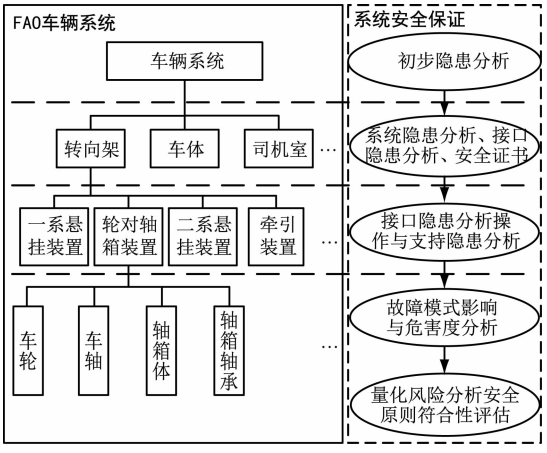


图 1　FAO 车辆系统初步隐患分析层次图

Fig. 1　Hierarchy diagram of hidden hazard preliminary analysis of FAO vehicle system

在项目生命周期开始时，由于没有足够的信息来进行详细的风险评估，初步隐患分析通常仅限于初步识别隐患。初步隐患分析目的是在系统设计之前提前识别并分析潜在危害，为后续风险分析奠定基础，所以初步隐患分析至关重要。因此，应在重大设计活动开始前进行初步隐患分析。

2.2　初步隐患分析现状

以某 FAO 线路的建设为例。某车辆系统初步隐患分析如图 2 所示。车辆供应商通过收集经验数据的方式进行隐患的识别与统计。在对隐患风险评判时，参考已投入应用相同系统的安全水平。对于不可接受安全水平的隐患采取了开会讨论的方式进行评估，进而采取相应的控制措施，最后将危害关闭。

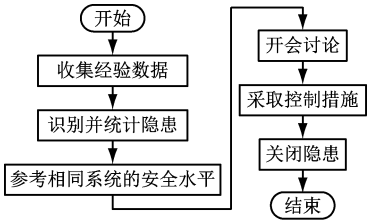


图 2　某 FAO 车辆系统初步隐患分析步骤

Fig. 2　Steps of hidden hazard preliminary analysis of a FAO vehicle system

通过分析上述流程，发现如下缺点：

1）初步隐患的识别只是基于以往的数据经验，缺乏系统性和综合性的识别方法，从而导致隐患识别不全面。

2）对于隐患的评判只是参考已投入应用的相同系统的安全水平，对隐患的风险评估未进行定性或定量的分析，导致风险评估可信度不高。对于不确定的隐患只是进行开会讨论，并未采取明确的控制措施。

3）隐患分析未输出与车辆系统设计相关的安全需求，导致此过程分析流于形式，未体现出风险分析的价值。

3　基于 RAMS 要求的初步隐患分析方法

根据 RAMS 的相关规范，进行初步隐患分析时，需满足如下要求：

1）需运用系统专业知识和安全知识发现并总结 FAO 系统的隐患，即顶层潜在危害。

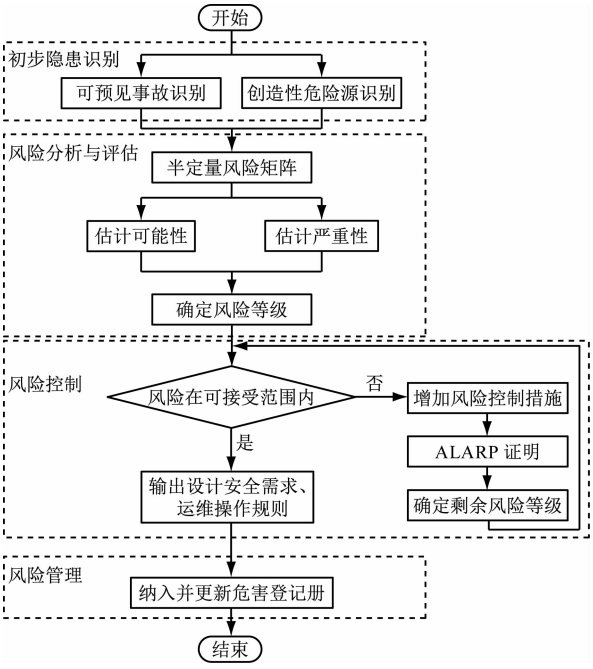
2）对总结的顶层危害进行风险评估，并尽可能降低不可接受的风险程度。

3）输出隐患发生的原因、影响、频次、后果程度及采取的措施等信息。

为优化和完善初步隐患分析方法和流程，根据 RAMS 的相关要求和 FAO 项目现状，提出初步隐患分析流程，如图 3 所示。

3.1　初步隐患识别

为了全面识别 FAO 线路存在的潜在危害，引入以可预见的事故为主、以创造性危险源识别为辅的初步隐患识别方法。因为事故是由隐患与触发因素的叠加而产生的，所以通过分析可预见的事故对隐患进行识别是非常必要的。在识别可预见事故的过程中，主要从如下方面进行收集和筛选安全隐



注:ALARP 为最低合理可行。

图 3　某 FAO 车辆系统初步隐患分析优化步骤

Fig. 3　Steps of hidden hazard preliminary analysis and optimization of a FAO vehicle system

患事件:①参考上海申通地铁集团有限公司和国内其他地铁公司已有的隐患风险经验数据。②RSSB(铁路安全和标准委员会)、中国城市轨道交通协会等国内外协会发布的安全风险模型和安全要求。③GB/T 32588. 1—2016《轨道交通 自动化的城市轨道交通(AUGT) 安全要求 第 1 部分:总则》规定的 FAO 系统的危害事件和安全需求等。

通过可预见事故的收集、筛选和分类,得出碰撞、脱轨、火灾、爆炸等 11 类通用的顶层危害一级事件及其隐患识别分析表,其部分内容及格式如表 1 所示。

表 1　FAO 车辆可预见事故隐患识别分析表

Tab. 1　Identification and analysis of FAO vehicle predictable accidents and hidden hazard

顶层危害一级事件编号	顶层危害一级事件描述
01	碰撞

为了提高隐患分析的准确性,可以针对每一类通用危害进行细化,得到相关的二级甚至更细致的隐患事件。在识别顶层危害后,即可根据 FAO 项目的具体特点对与各机电核心系统相关的顶层危害事件进行分析和评估。

FAO 场景充分体现了运营需求,较为接近运营的实际情况,是建设需求的补充,同时也涉及到了各机电核心系统的功能需求[2]。因此,提出基于 FAO 场景说明书的创造性危险源识别法,即除已识别的可预见事故,根据每个场景对应的子场景进行头脑风暴识别,或根据安全隐患和可操作性研究方法制定并应用运行场景隐患识别分析表,如表 2 所示。

表 2　FAO 车辆系统运行场景隐患识别分析表

Tab. 2　Identification and analysis of FAO vehicle system operation scenarios and hidden hazard

模式	场景	顶层危害事件编号	车辆系统顶层危害事件描述
应急模式	区间人员有序疏散	03-00-01	列车静止时,车门紧急解锁装置被激活后,车门在不允许打开的情况下可以被打开
		03-00-02	列车运行时车门可以通过紧急解锁手柄打开
		03-00-03	非安全侧车门被打开

3.2　隐患风险分析与评估

BS EN 50126:1999 提供了一种用于评估风险等级的工具,即“频率等级-后果等级”矩阵。但此工具比较宽泛,需要根据具体的 FAO 项目进行频率等级和后果等级的细化。

为了使 FAO 系统的风险评估可信度更高,在 FAO 项目中利用该工具,并引入隐患评判的关键因素:在后果影响层面,参考《安全生产法》等相关要求,按照人员安全和正线服务中断时间等因素对事故后果等级进行划分(见表 3);在频率层面同样划分了六级事故发生频率(见表 4),制定 6 ×6 半定量的应用性风险矩阵(见表 5)。在风险等级矩阵中,风险等级 R1 表示除特殊情况外,必须消除该类隐患;R2 表示必须将风险减低至最低实际可行的水平;R3 表示可接受的风险,但仍须按成本效益尽量减低风险;R4 表示可接受的风险。通过判断某个安全隐患事件发生的频率及其影响后果程度即可评估该隐患的风险等级,通过频率等级和后果等级的叠加即可对隐患的风险度进行排名。

为了将初始风险等级为 R1 和 R2 的危害控制在可接受范围,制定采取措施的原则如下:①采取措施后能够实际避免事故的发生;②可以将危险的出现频率降低到可接受的水平;③使危险变成事故的频率尽可能低;④减少事故造成损失的严重程度。

3.3　隐患风险控制与管理

为了证明所采取措施的有效性,需根据 ALARP

表 3 危险事故后果等级

Tab. 3 Hazard level of hazardous event consequences

危险事故后果等级	人员伤亡	正线运营中断时间/h
6(极轻微)	可能有轻微受伤	0.5 ~ <2.0
5(轻微)	重伤 1 ~2 人或轻伤 1 ~3 人	2.0 ~ <6.0
4(一般)	重伤 3 ~9 人或轻伤 4 ~49 人	6.0 ~ <12.0
3(较大)	重伤 10 ~49 人或轻伤≥50 人	12.0 ~ <24.0
2(重大)	死亡 10 ~29 人或重伤 50 ~99 人	24.0 ~ <48.0
1(特别重大)	死亡≥30 人或重伤≥100 人	≥48.0

表 4 危险事故发生的频率等级

Tab. 4 Frequency level of hazardous events every year

危险事故发生的频率等级	等级内容描述	发生频率/次
1	每周发生次数	≥100
2	每月发生次数	10 ~ <100
3	每年发生次数	1 ~ <10
4	10 年发生次数	0.1 ~ <1
5	不大可能出现	0.01 ~ <0.1
6	非常不可能出现	0.001 ~ <0.01

原则进行剩余风险评估。为了达到控制或消除隐患的目的,对措施分类后需分别输出至各相关方并记录隐患的关闭状态。对初步隐患分析后需将其纳入隐患登记册,并随着工程项目的深入进行更新和跟踪,实现隐患的闭环管理。

表 5 危险事故不同频率等级、不同后果等级下的风险等级矩阵

Tab. 5 Risk level matrix of hazardous events at different frequency levels and hazard levels

危险事故发生的频率等级	危险事故不同后果等级下的风险等级					
	6(极轻微)	5(轻微)	4(一般)	3(较大)	2(重大)	1(特别重大)
1	R1	R1	R1	R1	R1	R1
2	R2	R1	R1	R1	R1	R1
3	R2	R2	R1	R1	R1	R1
4	R3	R2	R1	R1	R1	R1
5	R3	R3	R2	R1	R1	R1
6	R4	R3	R3	R2	R1	R1

4 实例应用分析

在某 FAO 项目中应用初步隐患分析方法,分析过程如下。

4.1 FAO 车辆系统初步隐患识别

根据运行场景、设备工况及乘客操作维护等的接口界面,对火灾事故进行更新并细化,见表 6。

表 6 FAO 车辆系统火灾隐患识别表

Tab. 6 Fire hazard identification of FAO vehicle system

顶层危害一级事故		顶层危害二级事故		顶层危害三级事故	
编号	描述	编号	描述	编号	描述
03	火灾	03-01	载客列车发生火灾	03-01-01	在站台有效区内的列车上发生火灾
				03-01-02	在区间运行的列车上发生火灾
		03-02	轨旁发生火灾	03-02-01	运行列车附近的轨旁发生火灾
		03-03	车站内发生火灾	03-03-01	运行列车附近的车站内发生火灾
		03-04	车辆段发生火灾等	03-04-01	运行列车附近的车辆段、停车场、侧线发生火灾

4.2 FAO 车辆系统初步隐患分析

火灾隐患分析如表 7 所示。首先,根据危害描述分析危害后果。其次,根据风险矩阵判断该隐患的初始风险等级。由于该风险等级为 R1,因此需要根据危害处理原则制定相应措施。通过采取相应措施,再次评估火灾风险,得到风险等级为 R4,即可接受的风险。

FAO 车辆系统 11 类顶层危害风险分析结果如表 8 所示。由表 8 可见,在初始风险等级中,碰撞事故、载客列车事故、上下车区域事故和火灾事故的隐患风险较高,需要重点关注并采取控制措施。FAO 车辆系统可预见事故隐患分析结果如图 4 所示。由图 4 可见,在 102 条隐患事件中,R1、R2 等级占比分别为 32%、37%,且通过剩余风险分析后其占比均为 0;在 300 条风险控制措施中,与车辆相关的设计措施占比高达 64%,则这些措施可在设计联络会上输出与车辆系统设计相关的安全需求,同时与设计人员确认并落实。与运营方相关的措施则

表 7　FAO 车辆系统火灾隐患分析

Tab. 7　Fire hazard analysis of FAO vehicle system

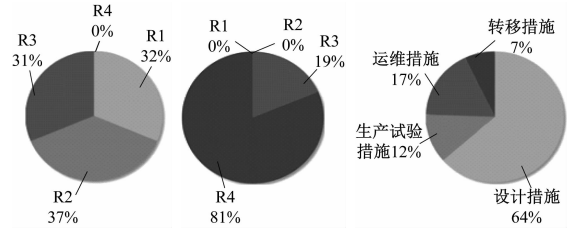
顶层危害三级编号	危害描述	危害后果	初始风险			危害致因
			频率等级	后果等级	风险等级	
03-01-01	在站台有效区内的列车上发生火灾	若停站时，发生火灾并紧急疏散，可能导致踩踏而发生轻微事故；若离站时，发生火灾且发生区间迫停，则可能导致特别重大事故	6	1	R1	①乘客纵火；②电气设备过热或短路；③列车防火不满足要求；④火灾报警系统未能检测到火灾；⑤TCMS 未将火灾报警信息上传至地面控制中心

建议采取的措施	措施类别	剩余风险			状态
		频率等级	后果等级	风险等级	
①运营方加强进站安检；②车载电气设备应进行过压、过流、短路的防护设计；③列车防火符合 EN 45545-2；2020《铁路运用-铁路车辆防火-材料和部件的防火性能要求》；④火灾报警功能满足 SIL2（安全完整性等级 2 级）要求；⑤TCMS 将各子系统发出的故障报警传输给外部通信接口，并满足 SIL2 要求；⑥当检测到发生火灾后，所有空调停机；⑦当发生火灾报警后，系统可以触发 CCTV（闭路电视）联动；⑧在客室内配置灭火器装置；⑨控制中心可以通过远程广播指导乘客进行区间疏散	①、⑧、⑨为基于运营操作的措施；②—⑦为基于设计的措施	7	2	R4	关闭

表 8　FAO 车辆系统 11 类顶层危害风险分析结果

Tab. 8　Risk analysis results of FAO vehicle system 11 types of top-level hazard

风险等级		危害事件数/次										
		碰撞	脱轨	火灾	爆炸	隧道/轨旁事故	车站事故	上下车区域事故	载客列车事故	车辆段/停车场事故	非法入侵	自然灾害
初始风险	R1	11	0	2	1	1	1	3	6	2	1	2
	R2	2	2	3	1	0	0	3	5	0	0	0
	R3	1	0	0	1	0	0	1	1	0	0	0
	R4	0	0	0	0	0	0	0	0	0	0	0
剩余风险	R1	0	0	0	0	0	0	0	0	0	0	0
	R2	0	0	0	0	0	0	0	0	0	0	0
	R3	7	0	0	1	0	0	0	0	2	1	2
	R4	7	2	5	2	1	1	7	12	0	0	0



a）原始风险占比　b）剩余风险占比　c）风险控制措施占比

图 4　FAO 车辆系统可预见事故隐患分析结果

Fig. 4　Analysis results of FAO vehicle system predictable accidents and hidden hazards

作为安全限制条件输出给运营方并由其进行确认。当所有措施落实后，危害状态即可关闭。将所有 FAO 车辆系统初步隐患分析纳入隐患登记册进行备查、追踪和管理，最终形成车辆系统全生命周期的隐患数据库。

5　结语

阐述了车辆系统作为关键系统需要进行初步隐患分析的必要性，对初步隐患分析的方法进行了优化。引入了可预见事故和创造性危险源识别的方法，并制定了实用性风险矩阵。通过制定初步隐患分析表，对初步隐患进行全面分析，输出的控制措施为车辆系统的设计提供了一定程度的安全保证。因此，提出的初步隐患分析方法对 FAO 车辆的安全保证具有一定的借鉴和推广意义。

（下转第 64 页）