

城市轨道交通全自动运行系统中安全相关系统的确定及安全保证模式探讨

盛伊琳 梁贺程

(上海申通轨道交通研究咨询有限公司, 200070, 上海//第一作者, 高级工程师)

摘 要 城市轨道交通 FAO (全自动运行) 系统安全保证工作的内容为: 依据系统功能、应用场景及其故障影响等因素, 确认安全相关系统的范围及安全功能; 对安全相关系统的安全功能展开系统化分析, 分配和确定其 SIL (安全完整性等级)。以某轨道交通线路 FAO 系统中综合监控系统为例, 探讨充分、合理及可行的安全保证工作, 研究安全相关系统满足其 SIL 需求的安全保证模式。

关键词 城市轨道交通; 全自动运行系统; 安全相关系统; 安全保证模式

中图分类号 U298: U231

DOI:10.16037/j.1007-869x.2023.02.016

Determination of Safety-related System and Safety Assurance Mode for Urban Rail Transit FAO System

SHENG Yilin, LIANG Hecheng

Abstract The safety assurance work of urban rail transit FAO (fully automatic operation) system includes: to define the safety-related system scope and functions according to factors such as system functionality, application scenario and fault impact; to carry out systematic analysis of the safety functions of the safety-related system and to assign and determine the SIL (safety integrity level). Taking the ISCS (integrated supervisory control system) of certain rail transit line FAO system as an example, the sufficient, reasonable and feasible safety assurance work are discussed, and the safety assurance mode of the safety-related system to meet the safety function SIL requirements is studied.

Key words urban rail transit; FAO system; safety-related system; safety assurance mode

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

城市轨道交通 FAO (全自动运行) 系统是基于现代计算机、网络通信及自动控制等技术的具备较高集成度的列车行车自动化综合系统。该系统整

体的设计需保障列车行车、乘客搭乘以及相关工作人员操作等的安全。为保障系统的安全, ISO (国际标准化组织) 研究并制定了相关的标准和规范, 如 IEC 61508:2010《电气/电子/可编程电子安全相关系统的功能安全》^[1-2] 是国际电子电气行业关于系统功能安全的通用标准, BS EN 50126-2:2017《轨道交通可靠性、可用性、可维护性和安全性规范》^[3] 是在 IEC 61508:2010 的基础上对轨道交通行业电子控制系统功能所做的安全标准。这些标准给出了安全、安全功能及安全相关系统等的定义, 并提出了安全相关系统和产品设计应用的通用框架和要求、各阶段的基本安全工作要求和安全技术等。

对于复杂的城市轨道交通 FAO 系统中安全相关系统的内容, 包括具体要实现的安全功能及其相应的 SIL (安全完整性等级) 的确定, 以及安全要求和目标确定后的安全管理、安全验证证明、安全评估等安全保证工作等, 上述标准和规范并无明确的要求。特别是对于综合监控、通信等系统, 在传统非 FAO 系统中主要按常规城市轨道交通运营规范实施, 但在 FAO 系统中这些系统需承担更多辅助监控及其与控制中心调度互动的任务, 因此, 这些系统中安全功能和 SIL 目标的确认, 如何实施安全保证工作, 建设方、运营方、供应商有无具体的要求和统一的做法, 以及安全保证工作范围是否合理、适度且可行, 都是 FAO 系统项目实施过程中经常遇到的问题。

本文在轨道交通行业标准和规范通用要求的基础上, 提出 FAO 系统中安全相关系统、安全功能及安全需求的分析和确定方案, 并结合实际案例探讨安全相关系统实施安全保证工作的模式, 进而开展合理、充分及可行的系统安全保障工作。

1 FAO 系统中安全相关系统及安全功能的确定

IEC 61508-2:2010 针对受控的电子电气系统及其控制系统,提出基于风险的功能安全管理方法,即在对系统危害和风险分析的基础上,开展所有安全相关系统及安全功能的设计与实现等活动。当这些系统可能引发对人员直接或间接的危害和风险时,就需要将其设计为安全相关系统。安全相关系统的特点如下:

- 1) 负责实现一定的安全功能,使受控的电子电气系统达到或保持安全状态;
- 2) 设计的主要目的是防止危害事件发生;
- 3) 该系统可减轻危害事件的影响和后果,从而降低风险。

根据安全相关系统的定义和特点,用于使系统达到或保持安全状态的功能以及减轻危害及风险的功能就是安全功能。安全功能的主要目的就是确保安全。

图 1 为 IEC 61508:2010 提出的系统风险、安全相关系统及安全功能的模型。图 1 中,受控系统是实现主要功能和用途的设备系统,控制系统是辅助其工作的设备系统。在运行过程中受控系统和控制系统均可能引发危害事件,需识别并分析可能的危害事件,并评估相应的风险是否可接受以及是否需采取措施降低风险。其中,用于降低风险的措施即安全功能。

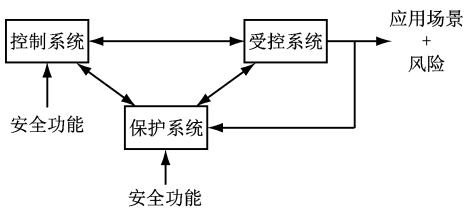


图 1 系统风险、安全相关系统及安全功能模型
Fig. 1 Model of system risk, safety-related system and safety function

具体到城市轨道交通系统中,主体受控的电子电气系统就是与列车及行车直接相关的电子系统,其他控制系统包括用于确保列车安全地按计划时间和路线运行、载客和停止的电子电气控制系统,如列车控制系统、制动系统的电子部分、车门系统的电子部分、站台门系统的电子部分等。根据图 1 建立的模型,从安全相关系统的应用场景考虑,分

析在列车行车的各种场景模式下可能会产生的危害事件,如撞车、脱轨、火灾、人员被碰撞等;针对危害事件,可采用如 HAZOP(危害和可操作性分析)方法进行识别与分析,同时需考虑正常运营、故障模式、可能的异常及错误操作等情况。

识别的危害事件需基于安全相关系统的特点进行风险分析评估,应综合考虑危害事件的发生频率及严重度,评估其风险是否可接受以及是否需要辅助的防护。通过危害分析即可判别安全相关系统的设备类型、安全功能的范畴,这些就是在项目全过程中需要实施安全保障工作的对象。

2 安全功能 SIL 的确定

通过危害和风险分析明确安全相关系统和安全功能后,需要进一步确定安全功能的特定目标要求。安全功能及其安全目标要求共同组成了完整的安全需求。

安全功能是用于降低风险的。根据可接受的风险准则,针对不同风险,安全功能需要降低的等级不同,其对应的目标就是相应风险需要降低的等级,即 SIL。SIL 可更清晰地达到并验证安全功能的目标。SIL 越高,其提供的防护程度亦越高。通常对系统安全防护要求越高,其发生非安全的故障即危险故障的概率越低。安全完整性即为安全相关系统在所有规定条件下、规定时间内满足执行所需安全功能的可能性。通常发生危险故障的概率较难通过精确的数据衡量,BS EN 50126-2:2017 定义了安全功能完整性要求量化范围的 4 个级别,即 SIL(见表 1)。

表 1 SIL 量化范围目标	
Tab. 1 Target of SIL quantitative scopes	
SIL 级别	R_{TFF}/h
4	$10^{-9} \sim < 10^{-8}$
3	$10^{-8} \sim < 10^{-7}$
2	$10^{-7} \sim < 10^{-6}$
1	$10^{-6} \sim < 10^{-5}$

注: R_{TFF} 为安全功能可接受的危险故障率。

安全功能的 SIL 受系统性失效(主要针对软件)和随机性失效(主要针对硬件电子系统)的影响,因此,在确定 SIL 目标时,需从上述两方面进行考虑。对于随机性失效,主要通过 R_{TFF} (见表 1)来实现;对于系统性失效,则主要是消除或降低系统

开发及应用过程中的人为因素影响,这主要通过全过程的质量管理、安全管理流程及技术安全措施等来控制。

安全相关系统设计实施后还需对安全功能 SIL 目标的实现进行说明和论证,以表明安全相关系统的安全功能满足量化目标、适当的系统保证流程及定性要求。为使安全论证工作更具可信度,可由独立于项目实施团队的有资质的机构对系统实施特定的安全评估,并审核评估系统的安全功能是否达到项目应用所需的 SIL 目标。

在项目实施过程中,还需注意安全功能 SIL 的正确使用,防止错误使用或滥用。总体而言,SIL 使用时需注意:

1) SIL 应在系统危害识别和风险分析后,基于风险可接受判定在独立的安全功能层级进行分配。

2) 不能将 SIL 分配给非功能性需求,如防止人员滑倒跌落的安全措施;不能将 SIL 分配给非电子系统功能,SIL 只能定义电子系统或机电功能中的电子部分所实现的功能。

3) SIL 针对的是安全功能而非系统,不能将其描述成“这是 SIL4 的系统”。

因此,在安全需求分配的过程中,只能将 SIL 分配给电子相关系统,而不能分配给非电子控制系统,如:① 机械系统,如车门、车窗、波纹管、贯通道、电缆槽、支架等;② 气动系统,如压缩机、软管、管道、阀门、气动执行机构;③ 液压系统,如泵、软管、管道、阀门、液压执行机构。

上述非电子系统部件均不在 IEC 61508-2:2010 及 BS EN 50126-2:2017 要求的安全保证范围内。通常这些系统部件的选择均遵循行业成熟的惯例,其涉及安全的要求一般建议遵循标准要求和行业规范,本文提出的安全功能的确定与安全保证过程并不适用。

3 安全相关系统的应用

基于上述对安全相关系统及安全功能的分析判定、分配,以及确定安全功能 SIL 目标的方法及过程,以某市 FAO 轨道交通线路的综合监控系统为例,说明其需重点识别分析的安全功能、安全相关子系统,并将其纳入安全相关系统的保证和管理工程中。

3.1 安全相关系统危害分析及风险分析评估

该 FAO 线路项目的综合监控系统是与信号系

统中列车自动监控系统、PSCADA(电力监控)、FAS(火灾自动报警)、BAS(环境与设备监控)、门禁、不间断供电等系统集成行车综合自动化系统。综合监控系统适用于 FAO 线路项目的运营模式,满足线路特定的全自动运营场景要求。该系统配备中心级和车站级系统设备,主要用于实现列车运营、线路设备的状态监视,以及特定情况下的远程联动控制。

首先实施初步危害分析,根据全自动运营场景和综合监控系统的运营需求,基于同类项目的类似运营经验以及可能发生的事故和危害,确定与综合监控系统有关的主要危险源。在该项目中识别的初步危险源列举如下:

1) 列车发生火灾而远程火灾应急监控及联动功能失效,造成人员伤亡。

2) 乘客及工作人员在区间(如进行疏散或维护工作时)因设备监控失效,造成触电伤亡。

根据项目事先确定采用的风险矩阵^[4]和风险可接受准则,上述识别的 2 条危险源均可能引发多个人身伤亡,其对应的风险均不可接受,需要综合监控系统提供相应的风险减轻措施,以避免或减轻危险源的发生及相应的风险。

3.2 安全功能确定

针对初步危害分析识别的不可接受风险危害,根据安全相关系统的架构和功能、接口设置等情况,进一步进行详细的系统危害分析,确定其引发原因以及对应的控制措施。

列车发生火灾而远程火灾应急监控及联动功能失效:该危害主要由于安全相关系统未处理火灾报警系统发来的信息以及车辆发出的火灾信号,导致无法进行相应火灾应急处置。可考虑选用热备冗余的控制中心及车站服务器,采用多机工作以降低系统设备的故障失效率;同时,设置 IBP(综合后备操作盘),在紧急情况下可通过 IBP 直接控制现场设备;将系统设计为具备多种运营模式,如控制中心和车站就地可相互切换操作。

乘客及工作人员在区间(如疏散或维护工作时)因设备监控失效:PSCADA 功能、禁止操作功能失效,可考虑在综合监控与 PSCADA 接口设置冗余链路,对现场 PSCADA 设备的带电、失电及异常状态进行实时监控,并由相应声光报警;综合监控系统软件设计有二次提醒功能,可提示工作人员减少命令误下发;另外,当综合监控系统与 PSCADA 接

口失效时,需确保 PSCADA 系统自身可独立操作。

上述两条危害的风险控制措施均可作为综合监控系统的安全功能。这些安全功能涉及到综合监控系统专用平台及其集成的火灾报警联动控制子系统与 PSCADA,相应的子系统应作为安全相关系统,需对其实施安全保障工作。

3.3 SIL 目标分配

对已识别综合监控系统的安全功能,采用第 2 节中的方法对其分配 SIL 目标。根据 2 条危害的风险等级以及安全功能对风险等级降低的要求,最终确定 R_{TFF} 需控制在 $[10^{-7}, 10^{-6})$ 范围内,即需达到 SIL2 的目标。因此,负责实现相应安全功能的安全相关子系统的软硬件均需达到 SIL2 的安全目标要求。

3.4 安全论证及评估

参考 T/CAMET:04017.2—2019《城市轨道交通全自动运行系统技术规范》^[5] 的要求,提出“综合监控系统涉及安全的功能宜达到 SIL2 级”。这仅是比较宽泛的要求,在 FAO 线路项目的整个安全保障工作中缺少实施的对象和目标。通过第 3.1 节—第 3.3 节的操作,在明确安全相关系统、安全功能,以及安全功能的 SIL 目标要求后,负责设计并实施综合监控系统及其相应子系统的供应商需确定特定的范围和目标,随后可按照 IEC 61508-5:2010 及 BS EN 50126-2:2017 中对相应 SIL 安全相关系统的要求,采用合适的设计工具和技术进行安全相关系统的开发和实施,并对安全功能进行测试以及对功能有效性、危险故障率进行计算,以证明综合监控系统提供的安全功能 R_{TFF} 低于 10^{-6} ,从而表明其安全目标和任务的实现。

4 安全相关系统的安全保证工作模式

本文通过对安全相关系统及安全功能 SIL 目标分析过程的描述,以及在 FAO 线路项目综合监控系统实施过程中的应用,结合 BS EN 50126-2:2017 中对安全相关系统安全生命周期工作的要求,提出安全相关系统的安全保证工作模式,如图 2 所示。

图 2 列出了安全相关系统各阶段主要的安全保证工作和安全工作成果。

1) 阶段 1—阶段 3:对应标准中的危害和风险分析阶段。重点工作是基于全自动运营场景和需求,对系统展开危害识别和风险评估。依据项目的风险可接受准则,筛选出不可接受的风险和相应的

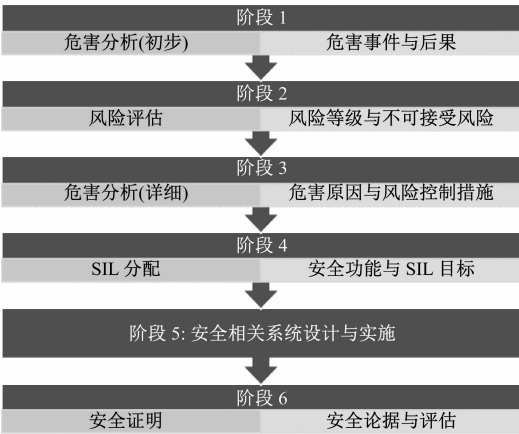


图 2 安全相关系统的安全保证工作模式
Fig. 2 Safety assurance work mode of safety-related system

风险减轻控制措施,进而确定安全相关系统和安全功能。

2) 阶段 4:对应标准中的安全需求定义和安全分配阶段。重点工作是根据风险控制的等级要求、分配安全功能的危险故障率要求及 SIL 目标要求,形成包括安全功能及其 SIL 目标的完整的安全需求。

3) 阶段 5:对应标准中的系统设计和实现阶段。主要的安全保证工作为:根据分配的安全功能的 SIL 目标要求,选择适当的设计开发方法和技术措施,开展安全相关系统及安全功能的设计和实施工作。

4) 阶段 6:对应标准中的系统安全确认和接收阶段。其重点工作是证明前阶段定义和分配的安全要求已达到,包括安全需求的确认、论证和接收工作,通过相关案例说明安全需求及安全功能等目标的实现。另外,针对不同 SIL 目标要求的安全功能及安全相关系统,如 SIL2 及以上等级,需要独立的安全评估方实施安全评估工作,从而为安全相关系统的安全接收提供有力的支撑依据。

5 结语

城市轨道交通 FAO 系统具有更多的控制系统承担列车的行车控制和防护,并配置承担风险控制及安全防护的安全相关系统,因而需开展合理且有针对性的安全保证工作。本文在通用标准的基础上,重点围绕安全相关系统和安全功能的分析和确定、安全功能 SIL 目标的制定展开讨论,并提出相应的安全保证流程及模式,为 FAO 系统安全相关系统

(下转第 85 页)