

面向延伸线信号系统多厂商的互联互通认证

乐 梅¹ 张晋恺² 胡妃俨²

(1. 重庆市轨道交通(集团)有限公司, 401120, 重庆;

2. 交控科技股份有限公司, 100070, 北京//第一作者, 正高级工程师、高级经济师)

摘 要 随着重庆轨道交通信号系统互联互通国家示范性工程顺利开通,取得互联互通跨线、共线试运营安全授权,论证了轨道交通信号系统互联互通建设的可行性和安全性,为同一城市轨道交通线路延伸线采用不同厂商互联互通标准的信号系统提供理论和工程经验支持。主要阐述延伸线信号系统多厂商的互联互通信号系统的安全保证和认证。

关键词 城市轨道交通; 互联互通; 信号系统; 安全认证

中图分类号 U231.7

DOI:10.16037/j.1007-869x.2020.09.041

Multivendor Interconnection Certification for the Extension Line Signaling System

LE Mei, ZHANG Jinkai, HU Feiyan

Abstract The successful operation of national demonstration project with rail transit signaling system interconnection in Chongqing City has obtained the safety authorization for cross-line and co-line trial operation interconnection, verified the feasibility and safety of the rail transit signaling system interconnection. The project provides theoretical and engineering experience support for the extension line of the same line that adopts multivendor signaling systems with different interconnection standards. In this paper, the safety assurance and certification of interconnection signaling system provided by multiple manufacturers for the extension line are described.

Key words surban rail transit; interconnection; signaling system; safety certification

First-author's address Chongqing Rail Transit (Group) Co., Ltd., 401120, Chongqing, China

随着我国城市地铁建设的飞速发展,轨道交通信号系统自主开发厂商日益增多。但各厂商技术来源不同:有的是直接引进国际主流信号厂商设备(西门子、阿尔斯通、庞巴迪、日立等);有的是国际厂商国产化联合开发和全自主化研发。虽然各自系统结构和功能基本一致,但功能分配、接口协议和电子地图等关键技术具体实现存在差异,导致国内

信号厂商不能实现互联互通。目前国内缺少成熟、已经被安全论证的轨道交通信号系统规范或法规,国内信号系统用户需求及系统设计受当地业主的使用习惯和定制化影响大,且无独立机构对各子系统进行规范符合审核和安全批准。这些因素导致国内不同厂商信号系统未能实现互联互通^[1-2]。

随着重庆轨道交通信号系统互联互通国家示范性工程顺利开通,成功实现了不同信号厂商系统共线、跨线的互联互通。以此为基础,在延伸线引入其他厂商信号系统从而实现与首通段开通线路无缝互联互通是可行的。

1 互联互通系统安全要求

1.1 互联互通信号系统服务安全要求统一

为保证延伸线和既有线无缝连接,多厂商互联互通信号系统具备下列功能:延伸线与既有线能实现在各运营级别无缝切换控制列车运营;延伸线与既有线系统架构、功能安全指标分配一致;延伸线与既有线接口协议和应用数据安全要求一致;延伸线与既有线安全性能要求一致;延伸线与既有线安全功能故障时,导向安全侧故障处理一致;延伸线与既有线对运营、维护人员操作与维护安全要求一致。

1.2 互联互通信号系统安全边界统一

信号系统作为整个轨道交通系统的控制大脑,与运营人员共同完成运营服务安全。为统一互联互通信号系统安全边界,针对列车运营的基本功能,按照不同运行级别,确定系统安全防护责任方。重庆轨道交通信号系统互联互通国家示范性工程系统安全边界如表1所示。

1.3 统一互联互通信号系统保护对象

1.3.1 人员的定义域

人员划分为乘客、公众和员工,包括外部应急服务人员。CBTC(基于通信的列车控制)互联互通信号系统防护对象是乘客及员工,外部应急服务人

表 1 重庆轨道交通信号系统互联互通国家示范性工程系统安全边界

列车运营的基本功能		非限制人工 驾驶模式	限制人工 驾驶模式	列车自动防护下的 人工驾驶模式	列车自动 驾驶模式
		EUM	RM	CM	AM
确保列车安全运行	确保安全进路	H 并 S(道岔控制由系统实现)	H 并 S	S	S
	确保列车安全间隔	H	H 并 S	S	S
	确保安全速度	H	S	H 并 S	H 并 S
驾驶列车运行	控制牵引和制动	H	H 并 S	H 并 S	S
轨道监控	防止和障碍物碰撞	H	H	H	H
	防止和人员碰撞	H	H	H	H
乘客乘降监控	控制乘客通行的车门	H	H	H 并 S	H 并 S
	防止车体之间或站台与列车之间的人员伤亡	H	H	H	H
	确保安全发车条件	H	H 并 S	H 并 S	H 并 S
单车运营	投入或退出运营	H 并 S	H 并 S	H 并 S	H 并 S
	监控列车状态(包含列车完整性、紧急制动实施、车门状态)	H	S	S	S
确保紧急情况的检测和管理	列车性能诊断,烟/火检测,紧急情况处理(呼叫/疏散,监控)	H	H	H	H

注:H——运营人员职责;S——由信号系统实现;并——运营人员和系统共同实现安全功能

员及公众不在该系统考虑的范围之内。

1.3.2 乘客

乘客为通过轨道交通系统从一个车站到另一个车站,通过付费或经过授权(如与交通部门相关的)使用系统提供服务的人员,可根据个人意愿选择任一特定时间使用系统。

乘客对应急情况的认知水平、行动能力和反应能力是有区别的,乘客可能会有几种类型:携带大小、形状不一物品的人员;携带儿童或怀抱婴儿(包括婴儿车内的儿童等)的人员;儿童;行动不便人员(老人、身有残疾的人);理解能力受限人员(语言不通、受酒精或药物影响);患有智力障碍者;患有听力或视力障碍者等。

城市轨道交通主管部门应与安全主管部门协商,在风险评估中分析乘客应对能力水平的不同以及带儿童、行李和物品的情况。

1.3.3 员工

员工为受雇于城市轨道交通部门或其他相关机构的人员。

员工有不同类型,如运营人员、维护人员、营救人员、外部工作人员(安检和清洁人员)。

1.3.4 物资

物资包括整个系统的基础设施、列车、CBTC(基于通信的列车自动控制)互联互通系统设备、邻近系统边界的物品和系统周边设施,还有乘客携带的物品等。

2 延伸线互联互通信号系统安全接口

由于采用了不同厂商的信号系统,相对于单个信号系统的项目而言,安全接口及安全假设需重新定义。根据互联互通信号系统架构,主要考虑如下因素:系统的安全边界和安全假设差异;设备的系统架构和安全功能分配差异;设备的内部接口差异;设备的外部接口差异;线路数据描述及数据准备过程差异;系统运营组织差异等。重庆轨道交通信号系统互联互通国家示范性工程系统架构如图 1 所示。

互联互通接口采用 FEMA 方法分析,按以下步骤进行:

步骤 1 输入文件收集。依据系统接口文档,明确分析接口对象,接口数据内容,接口协议。

步骤 2 接口字段用途识别。依据子系统需求/接口文档,识别接口字段的用途,即相关功能。

步骤 3 故障模式识别。建立所分析接口的故

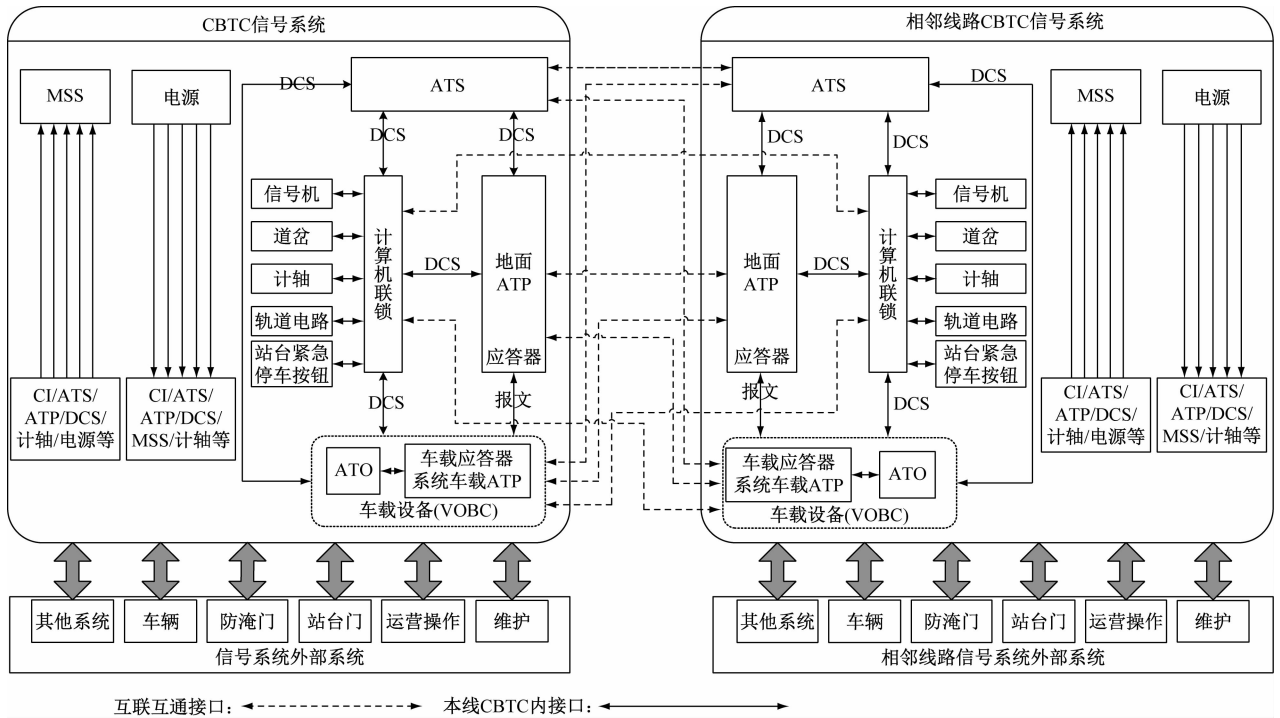


图1 重庆轨道交通信号系统互联互通国家示范性工程系统架构

障模式清单,分析造成故障模式的原因。

步骤4 故障影响分析、故障后果分析。分析各种故障模式对系统的影响,根据最终影响确定各种故障模式的后果,进行危害识别,识别对应的风险。

步骤5 制定减轻措施。针对各种故障模式、原因和影响,提出可能的设计改进措施及使用补偿措施,降低风险频率或后果,并分析剩余风险。

步骤6 危害日志管理。根据分析结果将具有安全风险的影响列入危险源清单。

3 延伸线安全保证方法

运用V模型生命周期工程交付思路,将互联互通视为集成大系统,各厂商地面、车载设备为子系统的安全评估策略,形成统一的安全评估标准和评估原则,统一安全评估过程及活动,这其中包括过程与活动、交付物、版本升级管理等。

延伸线采用多厂商信号系统互联互通的方式,延伸线信号厂商系统安全保证过程遵循GB/T 21562、GB/T 28808、GB/T 28809或等同系列标准,引入独立评估方对产品开发、工程项目过程进行安全评估,保证项目全生命周期安全^[3-6]。互联互通工程项目生命周期模型如图2所示。

运用全生命周期管理的思路,将互联互通视为多线路集成大系统,各线路地面、车载设备为子系

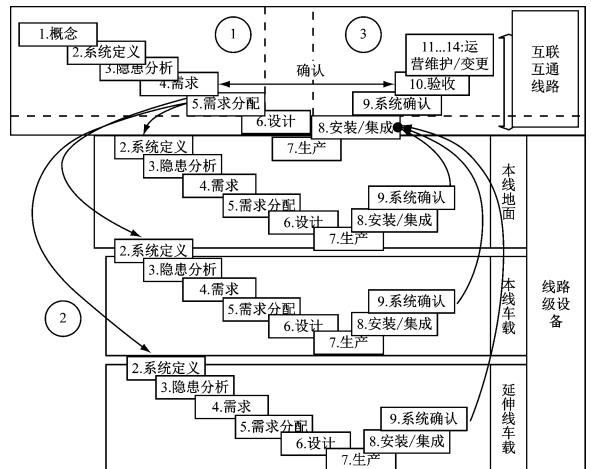


图2 互联互通工程项目生命周期模型

统的集成安全评估策略:①以互联互通系列规范为顶层系统设计,各线路地面设备、车载设备、接口及数据设计满足规范要求;②各线路集成商保证通用产品、通用应用满足互联互通系列规范和专题方案安全评估,互联互通安全评估间取信;③以互联互通系列规范和专题方案为依据,开展互联互通跨线安全评估:取得本线安全评估授权,取得多线路列车共线运行安全评估结论,取得本线列车进入他线地面跨线安全评估授权,取得本线地面接收他线列车跨线安全评估授权。

对于接口间及系统架构与功能的差异,互联互

通信信号系统厂商在进行系统开发时,遵循 TCAME/T 040013 系列规范,以互联互通系列规范为顶层系统设计,统一车地通信接口、ZC 间的接口、CI 间的接口、ATS 间的接口和共有电子地图等。各线路地面设备、车载设备、接口及数据设计满足规范要求。各集成商保证通用产品,通用应用满足互联互通系列规范和专题方案安全评估,并开展互联互通安全评估、互联互通安全评估取信。

4 延伸线与既有线互联互通安全评估相互认可

互联互通通用产品和通用应用全生命开发过程由设备提供厂商负责按照 TCAME/T 040013 系列技术规范开发,通过 EN5012X 系列(或等同标准)的独立评估。在互联互通特定应用安全评估过程中,采用安全评估结论相互认可原则。在通用产品或通用应用原有互联互通安全评估证据的基础上,互联互通特定应用安全评估方应对通用产品或通用应用开展相互认可评估活动,以判断通用产品或通用应用是否满足特定工程应用的要求。

信号系统厂商对已经评估过的原有通用产品或通用应用与特定工程应用的差异进行分析,确定通用产品或通用应用的应用环境、功能和性能、安全和接口需求,以及 RAM(可靠性、可用性、可维护性)指标和 THR(可容忍危险概率)是否满足特定应

用要求。差异分析的评估主要关注如下内容:差异分析是否充分;相关差异是否会带来通用产品或通用应用的变更;由差异引起的风险是否已经被控制。

5 延伸线安全验证和评估

基于 GB/T 21562. 2—2015、GB/T 28808—2012(适用时,采用 EN 50128—2011)及 GB/T 28809—2012 标准,独立安全评估方在开展互联互通特定应用安全评估过程中,主要安全评估活动包括但不限于:生命周期阶段文档审核;测试见证;现场质量安全审核。

生命周期阶段文档审核及现场质量安全审核可参考 T/CAMET 40013. 2—2018《城市轨道交通基于通信的列车运行控制系统(CBTC)互联互通工程规范第2部分:安全评估》。本文就以测试见证为主要介绍内容,多厂商信号系统实现工程项目互联互通,主要开展包括但不限于如下测试工作:互联互通实验室测试;延伸线信号系统静态调试;延伸线联锁开通;延伸线列车单车调试;延伸线列车多车动车调试;与首通段互联互通调试(联锁、单车、多车);与首通段互联互通试运行;与首通段互联互通试运营。

表2为互联互通测试活动及评估情况。

表2 互联互通测试活动及评估

测试阶段	提交文档	评估活动
互 联 互 通 实 验 室 测试	互联互通测试计划	①文档审核;②测试见证
	互联互通实验室测试规范及案例	
	互联互通实验室测试报告	
延 伸 线 系 统 静 态 试验	地面设备/子系统调试规范及案例	①文档审核,主要关注信号设备/子系统/系统功能测试;②一致性试验,牵引、制动功能试验
	地面设备/子系统调试报告	
	车载设备/子系统调试规范及案例	
	车载设备/子系统调试报告	
延 伸 线 列 车 动 车 调试	延伸线线路数据	①文档审核,信号系统功能试验,运行试验,牵引、制动功能测试,移动授权,停车点防护、列车定位;②本线单车动车授权;③测试见证
	延伸线列车动车测试规范及案例	
	延伸线列车动车测试报告	
延 伸 线 系 统 联 调 和 空 载 试 运行	延伸线线路数据	①文档审核,主要关注信号系统功能试验、信号系统运行试验,牵引、制动功能试验,列车追踪,移动授权,停车点防护,列车定位;②本线系统联调和空载试运行授权;③测试见证
	延伸线系统联调和空载试运行测试规范及案例	
	本线系统联调和空载试运行测试报告	
互 联 互 通 载 客 试 运营	空载试运行图	①文档审核;②互联互通载客试运营授权
	运行故障记录	

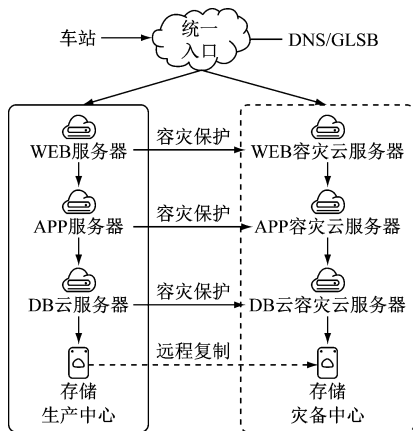


图5 容灾切换

5 结语

城轨云平台在为业务系统提供计算、存储、网络资源的同时,通过技术手段将备份还原、容灾保护等复杂的技术实现封装为简单易操作的服务,将业务人员从复杂的底层技术细节中解脱出来,使其更专注于业务本身。通过城轨云平台的引入,使传

(上接第183页)

互联互通特定应用测试阶段各承包商(集成商)/供应商需提交的文档及安全评估方所开展的安全评估活动,表2仅是测试阶段、提交文档和评估活动的建议,承包商(集成商)/供应商可根据实际情况调整测试阶段、提交文档和评估活动。

6 结语

目前,城市轨道交通逐步向互联互通的方向发展,国内各轨道交通信号系统厂商均在进行互联互通信号系统的开发研制,延伸线采用其他厂商互联互通信号系统,突破既有信号系统厂商捆绑,具备工程技术可行性和工程应用安全性。互联互通信号系统的安全认证也将成为其重要一环,而确定互联互通信号系统安全要求、互联互通安全接口、安全保证方法、测试验证范围和安全评估原则,是实现不同厂商信号系统互联互通关键技术之一。实践证明:本文提出的互联互通信号系统安全保证和安全认证方法能满足延伸线多厂商信号系统互联互通安全使用的要求,为延伸线采用互联互通不同信号厂商设备提供了良好的借鉴作用,推动了城

轨模式下除保护信号系统、综合监控、自动售检票等业务外,其他生产系统也可以较低成本实现更高等级保护。基于云平台架构的容灾保护有利于增强企业IT能力,提升企业信息化水平。

参考文献

- [1] 刘跃,宋兵. 信息系统异地容灾技术探讨[J]. 中国传媒科技, 2012(23):74.
- [2] 刘淑鹤,王芳. 数据容灾技术研究[J]. 网络安全技术与应用, 2013(9):45.
- [3] 张华,徐娟. 灾备技术的现状与发展[J]. 宜宾学院学报,2012(6):88.
- [4] 周斌. 浅谈数据备份技术与实践[J]. 通讯世界,2013(13):61.
- [5] 张赞,杨林曼,闫倩如. ATS系统双中心热备运行研究[J]. 自动化应用,2019(6):59.
- [6] 刘志宏. 地铁综合监控系统的数据备份与恢复系统研究[J]. 通讯世界,2018(5):21.
- [7] 谢新标. IT系统应急容灾技术介绍与选型[J]. 通讯世界,2016(13):228.

(收稿日期:2020-05-21)

市轨道交通信号系统互联互通技术的开发和安全评估。

参考文献

- [1] IEC. 轨道交通:城市自动化轨道交通运输(AUGT)安全性要求:IEC 62267—2009[S]. Geneva: IEC, 2009.
- [2] 张凯. 轨道交通信号系统独立安全评估的原理和方法综述[J]. 城市轨道交通研究,2017(6):7.
- [3] 中国城市轨道交通协会. 城市轨道交通 基于通信的列车运行控制系统(CBTC)互联互通工程规范:第2部分:安全评估:TCAME/T 040013.2—2018[S]. 北京:中国城市轨道交通协会,2018.
- [4] 中华人民共和国国家质量监督检验检疫总局. 轨道交通:可靠性、可用性、可维修性和安全性规范及示例第2部分:安全性的应用指南:GB/T 21562.2—2015[S]. 北京:中国标准出版社,2015.
- [5] 中华人民共和国国家质量监督检验检疫总局. 轨道交通:通信、信号和处理系统 控制和防护系统软件 GB/T 28808—2012[S]. 北京:中国标准出版社,2012.
- [6] 中华人民共和国国家质量监督检验检疫总局. 轨道交通:通信、信号和处理系统 信号用安全相关电子系统:GB/T 28809—2012[S]. 北京:中国标准出版社,2012.

(收稿日期:2020-05-09)