URCC
LAB
whitepaper

白皮书编号：NELURCC-WP-2017002

全自动运行系统安全报告

签发时间：2017年11月

签发版本：第一版（V1.0）

签发人： 

我们的使命

城市轨道交通列车通信与运行控制国家工程实验室由交控科技股份有限公司牵头，采用“政产学研用”协同创新模式，联合北京交通大学、北京市轨道交通建设管理有限公司、北京地铁车辆装备有限公司共同申报，并经国家发改委批复成立的第一个国家级城轨信号系统科技平台。

我们致力于推广全自动运行系统，专注于不断提高轨道交通系统可靠、安全运行能力。

我们相信，通过技术创新、严谨的安全分析、全面的安全管理、和多层次的测试、验证与确认手段，全自动运行系统将成为中国乃至世界城市轨道交通更安全、高效、节能的解决方案。

白皮书是国家工程实验室的重大研究成果发布形式之一，旨在为城市轨道交通建设业主方提供决策依据，为设计方提供设计指南，为运营方提供运营维护指导。

全自动运行系统研发过程中，需要从安全文化、安全管理体系到安全设计与全方位测试、确认等多方面共同努力以辨识危害并控制危害。在北京市政府和相关委办局，以及中国城市轨道交通协会多年持续支持下，北京市轨道交通建设管理有限公司依托北京轨道交通燕房线，建设了我国第一条自主化全自动运行线路，国家发改委已批准将其列入国家战略性新兴产业示范工程。在北京燕房线即将投入载客运营之际，城市轨道交通列车通信与运行控制国家工程实验室总结燕房线全自动运行系统研发与系统集成经验，发布《全自动运行系统安全报告》。

在报告中，将从安全体系、安全系统架构设计和测试、确认保障等方面进行论述，阐述全自动运行系统如何在正常情况、异常情况和特殊环境中始终保障安全。

对本报告有任何问题或建议，欢迎与我们联系。

联系电话：010-52824660；邮箱：whitepaper@bj-tct.com

目录

1 全自动运行系统能够更安全的运行

随着城市轨道交通快速发展、城市化进程的加快，对城市轨道交通设备系统在保证行车安全、提高运输效率、节能环保方面提出了新的需求。采用技术先进、性能稳定、效率优先的全自动运行系统成为中国轨道交通建设的迫切需求。全自动运行系统是以现代信息及自动化技术提升运营服务水平，增强系统装备的功能和性能为目的的新一代城市轨道交通系统，是城市轨道交通列车运行控制系统的发展趋势，全球新建线路中将有 75%采用全自动运行系统，改造线路中也将有 40%采用全自动运行系统，国内主要城市已将全自动运行系统建设纳入规划。

全自动运行作为先进的轨道交通列车运行控制技术，在未来有广泛的发展应用空间。在城市轨道交通建设中采用全自动运行技术，能够进一步增强系统装备的功能和性能，进一步提升轨道交通安全与效率。

安全是全自动运行系统的核心关注点之一。

近年来，由于公路交通日渐拥堵，越来越多的人选择轨道交通出行方式。2016 年度，中国城轨线路客运量为 160.9 亿人次。在北京，人们每天的地铁通勤时间达到 97 分钟。城市轨道交通的安全演变为普通民众最为关心的话题。

据统计，1946-2002 的 57 年间，仅英国国内，因铁路事故导致死亡的人员总数达到 8861 人，其中 32%为乘客， 51%为职工， 17%为社会人员。最大的死亡类别是移动事故中的职工死亡，占到死亡总数的 41%。

	乘客	职工	社会人员	总数
列车事故	868	267	502	1637
移动事故	1774	3675	821	6270
非移动事故	183	577	194	954
事故总数	2825	4519	1517	8861

轨道交通领域，人为因素是造成运营事故的重要原因，每年都会发生由于司机、维护人员、现场指挥人员或调度人员的错误造成运营延误甚至人身伤亡事故。随着轨道交通系统复杂度不断增加、运营压力随着客流增长不断增大，操作人员由于业务不精或身体因素造成判断失误、错误操作、违章作业时有发生。

2014 年，德国铁路共发生事故 1739 起，其中人员事故为 898 起，占总比例的 51.6%，且在 2010 至 2014 年间，人员事故百分比呈逐年上升趋势。人在应对日趋复杂的轨道交通系统时，越来越容易出错。

年份	相撞	脱轨	人员事故	平交道口	列车火灾	其他事故	总数	人员事故百分比
2014	365	230	898	172	71	3	1739	51.64%
2013	350	262	799	158	53	7	1629	49.05%
2012	396	239	798	176	64	9	1682	47.44%
2011	307	289	670	178	66	12	1522	44.02%
2010	401	321	643	221	60	16	1662	38.69%

国内，同样存在许多人为因素导致的伤亡事故。2007 年上海地铁 2 号线由于司机未对车门与屏蔽门间隙是否安全进行认真确认就盲目动车，造成一名乘客与安全护栏碰撞跌落站台后死亡。2014 年北京地铁五号线惠新西街南口站，一名乘客被夹在闭合的安全门和车门间隙，随后车子开动，该乘客被挤后跌落站台，抢救无效身亡。

事故伤亡让人警醒，引发思考，我们期望，由设备代替司机或运营人员来操作，给人们提供更安全

的轨道交通系统。

在城市轨道交通系统领域，从潜在事故角度来说，主要存在碰撞、脱轨、人身伤害、火灾、触电和恶劣天气六大风险。下表列出传统 CBTC 系统和全自动运行系统能够处理六大风险的对比（其中，“√”表示列车运行控制系统参与/主导防范该风险）。

风险分类及细化描述		传统 CBTC		全自动运行	
		正线	车辆段	正线	车辆段
碰撞	列车追尾	√	×	√	√
	列车侧面相撞	√	×	√	√
	列车迎面相撞	√	×	√	√
	列车与轨道上的物体相撞	×	×	√	√
	列车与系统结构物相撞	√	×	√	√
脱轨	列车超速	√	√	√	√
	未确保安全时列车进入道岔区域	√	×	√	√
	不安全的道岔移动	√	×	√	√
人身伤害	人员受困	×	×	√	√
	人员摔倒跌落	√	×	√	√
	人员被设备撞伤	×	√	√	√
火灾	区间火灾	×	×	√	√
	列车火灾	×	×	√	√
触电		×	×	√	√
恶劣天气		×	×	√	√

从轨道交通系统列车运营的基本功能来说，根据 IEC62267:2009《城市自动化有轨交通系统安全需求》，列车运营的基本功能包括确保列车安全运行、驾驶、轨道监控、乘客乘降监控、单车运营和确保紧急情况的检测和管理，传统 CBTC 系统（GoA2）和全自动运行系统（GoA4）由信号系统实现（下表中用“S”标识）和运营人员负责（下表中用“X”标识）的内容如下表所示。

列车运营的基本功能		传统 CBTC	全自动运行系统（GoA4）
确保列车安全运行	确保安全路径	S	S
	确保列车安全间隔	S	S
	确保安全速度	S	S
驾驶	控制牵引和制动	S	S
轨道监控	防止和障碍物碰撞	X	S
	防止和人员碰撞	X	S
乘客乘降监控	控制乘客通行的车门	X	S
	防止车体之间或站台与列车之间的人员伤亡	X	S
	确保安全启动条件	X	S
单车运营	投入或退出运营	X	S
	监控列车状态	X	S
确保紧急情况的	列车性能诊断，烟/火检测，脱轨检测，紧	X	S 并/或 OCC 人员

检测和管理	急情况处理（呼叫/疏散，监控）		

全自动运行系统相对于传统 CBTC 系统而言，可以提供全方位的安全防护：

- 从列车运营角度，全自动运行系统可以为正线运营与车辆段车辆运行提供全面风险防控能力。传统 CBTC 系统仅为正线运营提供碰撞和脱轨安全功能的防护，在车辆段，一般由司机负责列车运行安全，系统仅提供基础超速防护功能。
- 从现场作业的职工角度，全自动运行系统引入无人区概念，构建出封闭的列车运行轨道，同时增加轨旁 SPKS 开关，提供进入无人区后的安全防护，确保轨旁作业员工安全。传统 CBTC 系统无法提供自动防护手段，职工现场作业安全完全靠管理手段完成。
- 从乘客乘降角度，城市轨道交通系统需要考虑乘客换乘过程中车门和站台门的安全联动，列车具备启动条件检查，避免乘客在车厢间、车辆和站台间受到伤害，确保乘客乘降过程的安全。全自动运行系统通过增加安全检测设备，对单个车门和站台门进行授权等手段，全面防护各类异常场景，实现乘客乘降安全的全面自动防护。传统 CBTC 系统乘客乘降安全主要由司机负责，司机通过瞭望、一系列操作规程和信号系统有关车门的允许指令保证乘降安全。
- 从应急角度，轨道交通系统面临最多的紧急情况主要包括火灾、轨面障碍物检测、人员触电和恶劣天气。全自动运行系统通过增加检测设备、将成熟的应急预案操作过程纳入系统范畴，在出现异常的情况，系统第一时间自动进行安全防护，保证轨道交通系统安全高效运作，仅当设备无法进一步处理紧急事件时，才要求运营人员介入系统安全防护工作。传统 CBTC 系统在出现上述紧急情况时，会将列车驾驶权完全交给司机、运营方制定各类应急预案，通过应急演练等方式确保应急安全。

根据人因工程研究，即使是经过良好培训的有经验的操作人员，其失误概率也高达 10^{-3} 到 10^{-4}，而全自动运行系统关键安全控制设备的故障概率均小于等于 10^{-8} 到 10^{-9}。全自动运行系统通过自动化技术和智能化运行，从运营角度、现场作业职工角度、乘客乘降角度还是应急角度，大量通过设备或技术手段替代人员操作、固化人员经验，不仅提高相关操作的可靠性，同时也大大提升了整体系统的安全性。

2 安全管理体系：全生命周期风险管控

2.1 全自动运行系统安全涉及领域

全自动运行系统安全涉及五个不同的安全领域：行为安全，运营安全，功能安全，应急安全和环境安全。信号系统作为全自动运行系统的核心，需要与车辆、通信（含 PIS）、站台门、综合监控、车辆基地等综合协调，共同确保全自动运行系统的安全运行。

行为安全：

行为安全是指全自动运行系统的驾驶决策和行为的安全。全自动运行系统能够像人类司机一样进行驾驶活动，遵守运营规则，并且可以在各种预期或意外场景下安全驾驶。全自动运行系统综合使用场景分析、实验室模拟测试和现场验证，识别运营可能遇到的各种情况，进而开发出安全需求，同时指导系统进行全方位测试和验证。全自动运行系统可完全代替司机进行运营作业，充分考虑了列车唤醒、列车休眠、站台乘降作业、列车折返等常规运营场景；在火灾、雨雪恶劣天气的情况下，同样可以模拟司机采用特殊策略进行驾驶，保证安全。

运营安全：

运营指列车和乘客之间的相互作用。运营安全可以确保乘客在列车上拥有安全舒适的体验。通过危险源分析、采用现有安全标准、经过广泛的测试并参照各行业的最佳实践，建立一个安全的全自动运行系统。例如，在列车上安装了紧急呼叫设备和紧急手柄，当乘客遇到问题，可通过应急通讯与中心即时联系，获得专业的处理策略指导，通过紧急手柄可让列车在紧急情况下以最快的速度停车。

功能安全：

功能安全旨在确保列车存在系统故障时也可以安全运行。全自动运行系统建立了系统层和设备层的备用和冗余关系来应对意外状况。例如，所有的列车均配备了冗余的自动驾驶系统，当出现故障时，可以无缝切换至另一个系统进行工作，对系统运行不造成影响。当两套系统均发生故障时，安全防护系统可使列车安全停车（即最小的风险）。同时，系统还具有多级后备模式，即使由于意外情况系统无法继续进行全自动运行，系统还能够通过一系列安全操作，使列车停留在站台，等待站务人员处理后继续自动运行或降级为普通 CBTC 列车继续由人驾驶运行。

应急安全：

应急安全是指出现意外事故后的应急救援以及逃生通道。全自动运行系统可保证列车不会出现碰撞的风险，同时，因为一些异常情况，例如对于地上线路，大风使得树木折断，侵入轨道，系统安装有障碍物检测装置，即使出现这样的异常情况，仍可使列车安全停车，将伤害降低至最低的程度，实时通知中心，指导乘客安全撤离。

环境安全：

全自动运行系统保证可能与车辆有相互作用人员的人身安全。系统在设计过程中，不仅考虑了乘客的安全，同样对维修人员、闯入轨道的人员的安全进行了防护。例如，在车辆段和区间，设置有 SPKS 开关用于人员进入轨道区域进行临时作业的防护，确保列车无法进入作业区域。同时，系统具有完善的管理措施。

2.2 全生命周期、全方位的危害管理体系

全自动运行系统的研发与系统集成符合 EN50126/50128/50129 标准规定的系统安全管理体系，其约束了技术研发和测试过程中如何确保安全。如今，该体系已成为一个全面而完善的管理方法，可称之为

“全生命周期安全风险管理”。

“全生命周期安全风险管理”意味着从产品需求阶段开始考虑安全性，将安全纳入每个系统级别和开发的每个阶段，从设计、编码到测试和验证。该管理方法从多个方面全方位考虑，其基础是各种行业的最佳实践，包括航空航天，汽车和国防（包括 IEC61508、EN50126、EN50128、EN50129 等方面）。

全生命周期安全风险管理制定了相应流程来保证产品安全。用以减少潜在危害风险的安全需求可以在系统内部被识别，在设计中得以解决，然后经过验证和确认，以证明安全风险已经降低到分析中确定的水平。

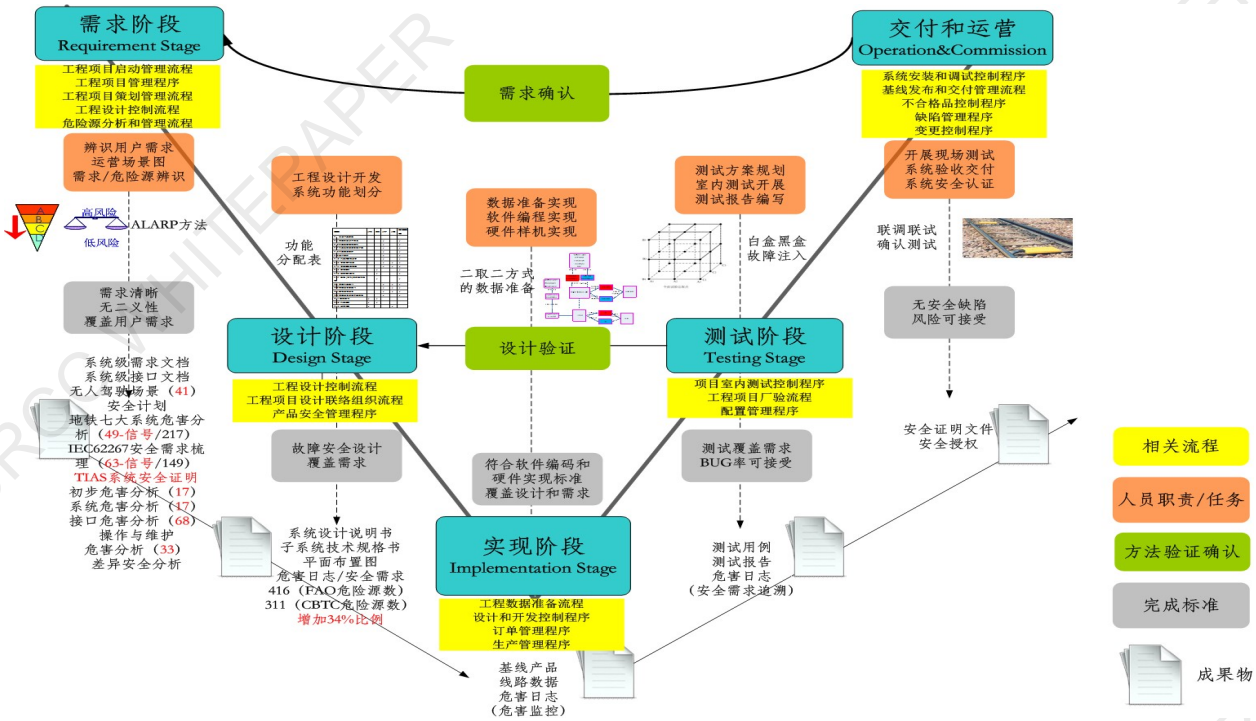

图 1 全生命周期安全风险管理体系

根据各行业的最佳实践，全自动运行系统的每个场景均经过安全分析和设计，每个子系统都经过完备的测试、验证和确认，以确保所有子系统在集成为一个完整的全自动运行系统时能够安全地工作。这个方法还有助于在燕房线实际线路上验证全自动驾驶列车可以自动地安全工作，并识别系统组件，子系统或其他方面的任何部分的变化或失效如何导致整个无人驾驶系统其余部分发生变化。

这个过程使得全自动运行系统拥有许多关键安全功能，包括冗余关键安全系统，使得车辆在技术故障的情况下能够安全停止，使用具有相同功能的冗余传感器，以及大量的计划帮助研发工程师快速改进全自动运行技术。

全生命周期安全风险管理保证了系统从需求到交付的逐层控制和闭环确认。

风险管理过程开始于识别危险场景及确定可以通过实施以减少风险的潜在缓解措施。这些缓解措施可能包含各种形式，如软件或硬件设计需求，硬件或软件设计原则，程序控制或其他分析原则。该管理可确保客户、员工和分包商的健康和安全，并提供安全风险在可接受水平内的产品。

安全风险分析过程有助于确定我们全自动运行系统架构，子系统和组件的需求。通过使用一系列子系统和系统分析技术，各种系统工程流程以及学习 IEC 国际标准，从而得到这些安全需求。该分析还支持对安全测试的需求开发，以及系统如何检测和处理故障。

在安全风险评估过程中，为确保评估的独立性和可信性，通常情况下，评估过程由第三方认证团队来进行。

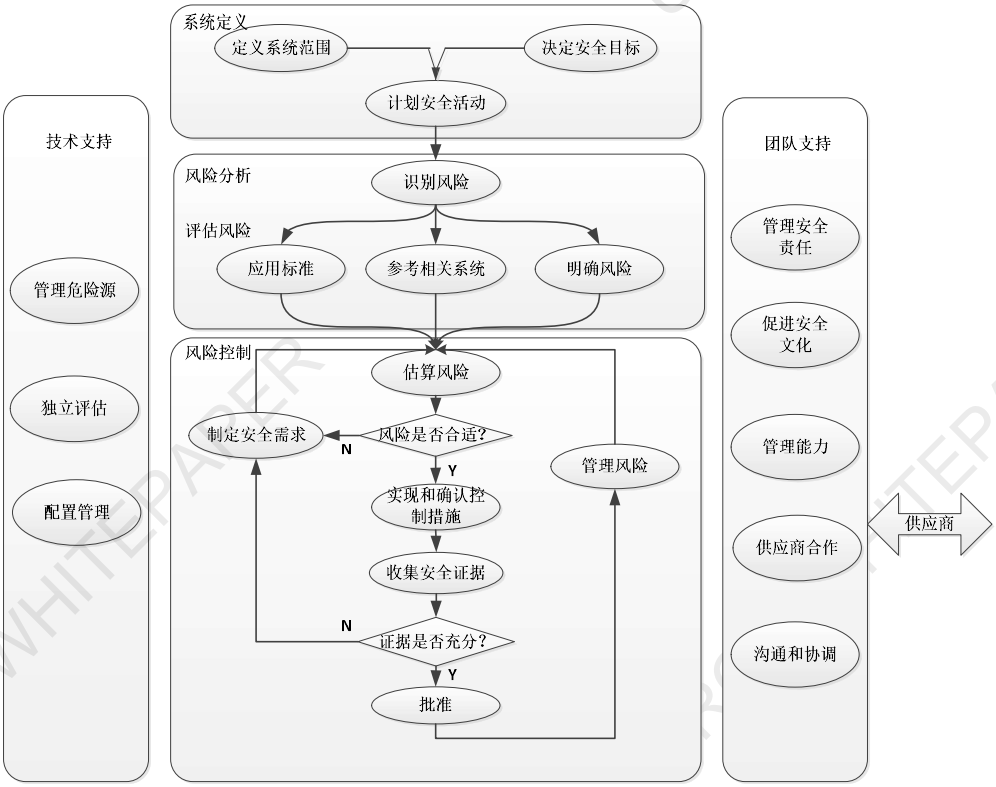

图 2 风险管控流程

全自动运行系统作为一个涉及多专业、多场景的复杂系统，其安全分析包含轨道交通层安全分析、信号系统安全分析、设备层安全分析三个层次。分析过程与持续的工程测试活动和安全工程分析相结合。具体安全活动主要包括初步危害分析（PHA）、系统危害分析（SHA）、子系统危害分析（SSHA）、接口危害分析（IHA）、操作及支持危害分析（O&SHA）、定量危害分析等需要计划生命周期活动开展的离散安全保障活动和危害日志维护、阶段验证、安全确认、内部独立安全审核、内部独立安全评估等持续进行的连续安全保障活动。

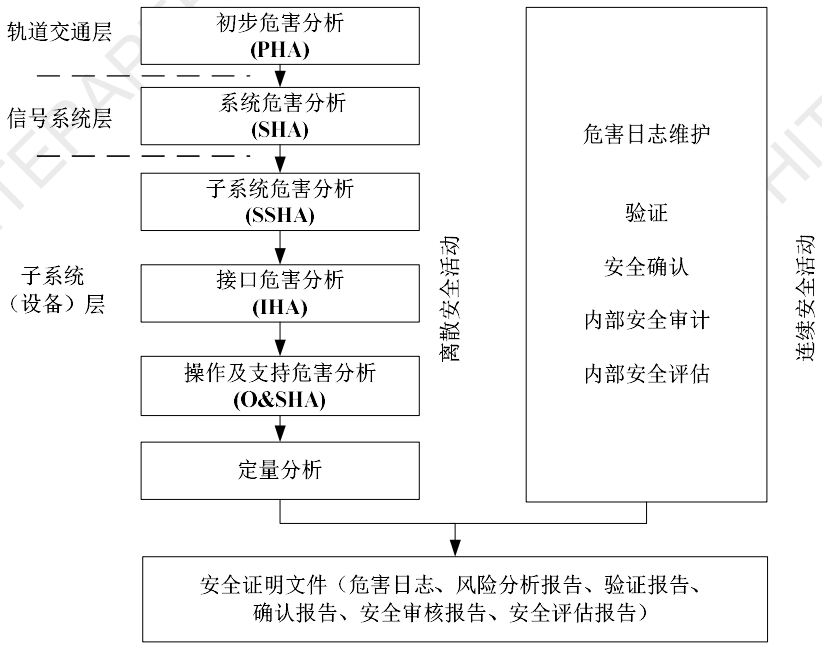

图 3 安全管理活动示意图

不同层次的危害分析，由于分析对象的复杂性、综合性等特征，会采用不同的方法。

在全自动运行系统中，信号系统与其他系统的关系与大脑与四肢等身体其他部位的关系类似，是整个人体（轨道交通系统）的核心，因此在轨道交通层面和信号系统层面进行综合性的危害分析，对于在设计中保证安全至关重要。

在燕房线全自动运行系统中，综合传统 HAZOP、FMEA、SWIFT 等方法的优势，创新性的构建了基于引导词的危害模式识别技术（GHMIT），用于针对轨道交通层面和信号系统层面这种跨专业、综合性强的场景进行安全分析。GHMIT 技术的实施流程图如下。

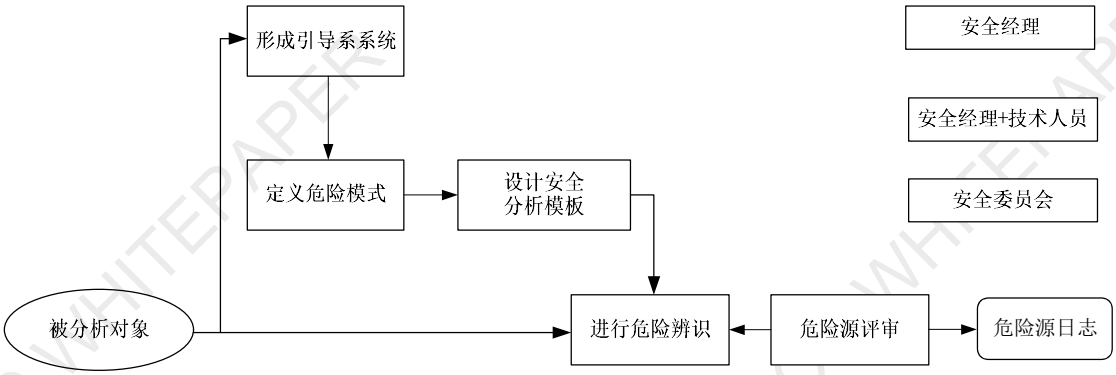

图 4 基于引导词的危害模式识别技术

考虑信号系统层和子系统（设备）层由于全自动运行增加的功能众多，且设备之间的时序、安全相关约束复杂，引入基于系统理论事故模型 STAMP 的危害识别技术 STPA（系统理论过程分析）方法，进行细化层级的安全分析。

通过全生命周期、全方位的危害管理，全自动运行系统通过设计保证安全，所有危害均被控制在运营可接受程度，其安全性远高于既有 CBTC 系统。

3 全自动运行列车控制系统如何工作

全自动运行系统(Fully Automatic Operation，简称 FAO)是一种全自动化的、高度集中控制的列车运行控制系统，是基于现代计算机、通信、控制和系统集成等技术实现列车运行全过程自动化的新一代城市轨道交通系统。

全自动运行系统可应用于以下制式的系统中[IEC62290]：

- 点式或者连续数据传输
- 通过列车保护曲线对列车的连续监视
- 通过轨旁设备的列车定位或者报告列车位置定位方式

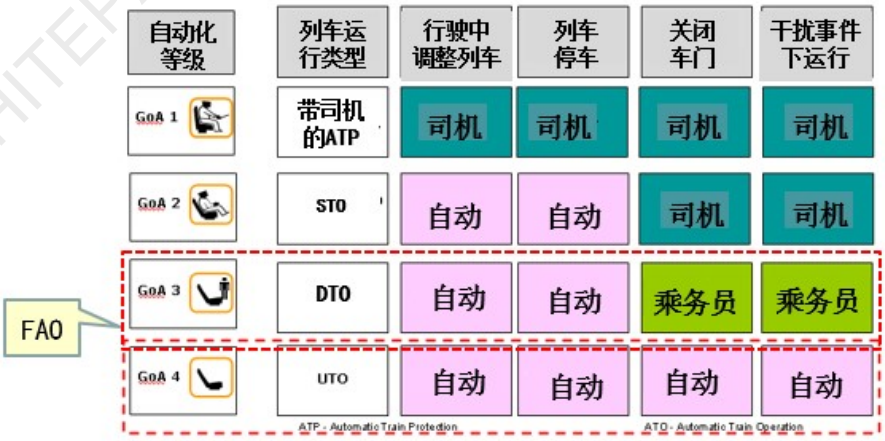

图 5 列车运行系统自动化等级划分

全自动运行系统具备很好的互操作、互换和兼容性，可以被用于很多类型的城市轨道交通运行控制系统。针对特定应用的专用 FAO 运营需求取决于此线路所需要的自动化等级。为形象说明轨道交通运行的自动化程度，习惯根据列车上是否有运营人员说明运行系统的自动化等级。

全自动运行系统可支持 GoA4 等级，同时向下完全兼容。GoA4 级运行时，列车上不再安排任何工作人员。在正常情况下，GoA 3（DTO）和 GoA 4（UTO）一样，由设备自动完成各项操作；在故障条件下，GoA 3 与 GoA 2 一样，由车上的司乘人员处置故障，而 GoA 4 等级则需由地面派人到车上进行处置。全自动运行系统进一步提升城市轨道交通运行系统的安全与效率。

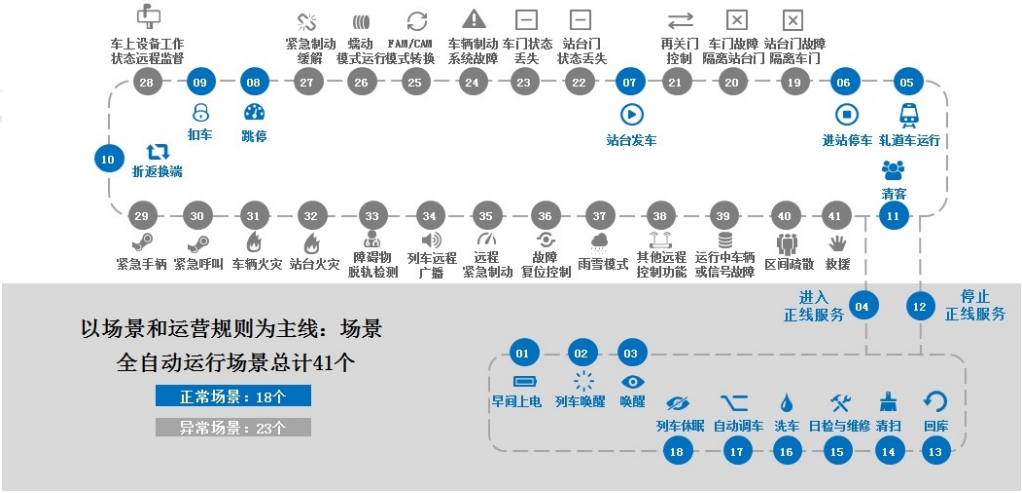

图 6 全自动运行场景示意图

全自动运行系统中共有 41 个场景，其中运行中的正常场景 18 个，异常处理场景 23 个。

全自动运行系统是由 7 大专业、31 个子系统，数十万个驱采点组合实现安全高效运输的复杂巨型系统。这些子系统共同有秩序地运行，确保交通安全，对应 GOA 等级的要求。运营管理和监督主要通过设备的使用来实现。它包括在正常、受到干扰和故障情况下保证运营的所有手段。

全自动运行系统可确保轨道交通系统内部的安全。

3.1 行为安全--像司机一样进行驾驶活动

全自动运行系统可以替代由司机执行的全部控车操作和测试工作，实现列车运行全过程（包括正线、车辆基地）的自动安全防护，像司机一样进行驾驶活动和安全保证。

全自动运行系统车载设备应具备在进入全自动运行区域前检验列车状态的能力，以保证车载设备能执行后续无人驾驶过程中的全部操作[IEC62290]。全自动运行系统可根据运行图自主的从休眠状态自动唤醒，自动完成列车上电自检、设备自检、静态测试、动态测试 30 余项的全面列车检查，包括以往人工不进行的测试项和无法实现检查的测试项，如：车辆设备自检、车载设备自检、网络通信自检、照明测试、开门测试等。测试完成后，列车将检查结果自动上报给控制中心，控制中心根据上报的检查结果，自动决定是否唤醒备用列车，大大降低列车在正线运营故障发生的概率，保证运营效率。

图 7 列车自动唤醒功能

系统具备根据时刻表自动驾驶列车投入正线运营，完成站间行驶、到站精准停车、自动开闭车门、自动发车离站、自动回库、自动休眠、自动洗车等一系列功能。列车运行全过程自动化，将司机从单一重复的作业中解放出来，进一步降低运营人员的工作强度，减少人为因素对运营的影响，从而减少人为误操作导致的安全事故，提升系统安全性、运营能力、自动化程度和运营维护功能。

图 8 无人驾驶室与自动洗车

在恶劣天气下，因为结冰或者下雨（尤其是小雨）导致轨面湿滑，列车停车距离将变得更长，造成

同其它列车发生相撞的发生频率大大增加。根据 IEC62267 要求，全自动运行系统应考虑此风险，通过加热轨道或者使用恶劣天气的特定列车防护曲线来确保列车的安全间隔。系统应具备雨雪模式下的控车功能。控制中心工作人员通过对天气的实时观测，确认和下发雨雪模式后，系统根据轨面适合特性，固化司机雨雪天气驾车最佳实践，通过降低平直轨道上车辆能够保证的紧急制动最小减速度，加大列车的安全防护距离，降低牵引制动力和运行速度，实现列车在雨雪天气下安全低速控车。

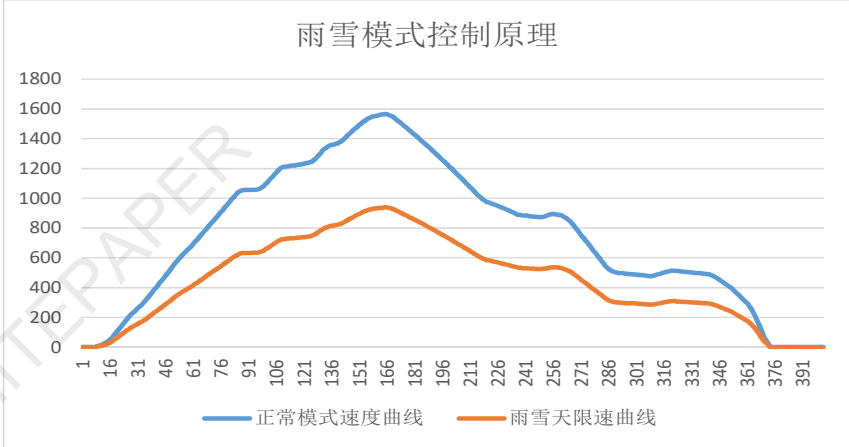

图 9 雨雪模式控制原理

全自动运行系统中涉及到行为安全场景如下：

序列号	行为场景	序列号	行为场景
1	早间上电	13	自动调车
2	列车唤醒	14	站台火灾
3	唤醒	15	车辆火灾
4	进入正线服务	16	日检与维修
5	进站停车	17	车辆制动系统故障
6	站台发车	18	跳停
7	折返换端	19	扣车
8	停止正线服务	20	车门状态丢失
9	回库	21	站台门状态丢失
10	列车休眠	22	车上设备工作状态远程监督
11	洗车	23	轨道车运行
12	雨雪模式	24	清客

3.2 运营安全--与乘客互动

全自动运行系统包含确保乘客安全换乘的所有功能和需求，应考虑以下几点[IEC62290]：

- 从初始的开门到最后的关门
- 乘客换乘过程
- 乘客换乘结束后的发车条件，包含与乘客换乘非直接相关的其他约束。

全自动运行系统可实现对乘客上下车及车内的安全防护。列车在车站已经检测为零速而且停车范围在精度要求范围内，系统打开列车车门和相应的站台门。同时，在车门打开时，避免列车移动。当发现未授权门打开时，系统应将列车信息提供给外部。如果站台比列车长，只有与车门对应的站台门才授权被打开[IEC62290]。

当列车车门未被授权(仅对人工切除车门适用)时，本列车停站时对应的站台门应能保持锁闭不参与

停站的开、关门作业，并对乘客进行指示灯提示和车门隔离故障广播提示，确保乘客的安全乘降。当车站站台门故障或被人工锁闭隔离后，列车在该站台时，该侧站台的所有列车相对应的车门也保持锁闭，不参与停站的开、关门作业，并对乘客进行指示灯提示和车门隔离故障广播提示，确保乘客的安全乘降。

同时，全自动运行系统可监视诊断设备，以阻止人员跌落，包括在两个车厢之间、站台边缘和车厢主体之间的跌落［IEC62290］。

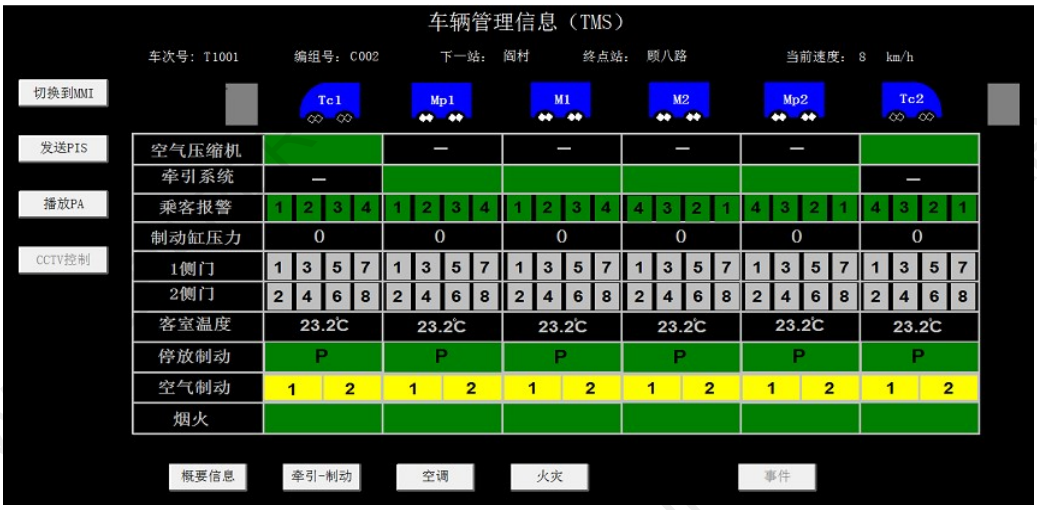

图 10 对位隔离功能

列车上安装紧急停车按钮（紧急刹车手柄）供乘客使用，紧急停车需求激活时应告知控制中心。操作紧急停车按钮时应启动紧急程序停车，但是不允许列车在站外停车，也不能在隧道或没有安全区域的地方停车。一旦列车在站内停车，没有控制中心命令授权列车不能继续运行。如果由于其他原因列车停于两站之间，列车门未打开，列车应该继续运行到下一站。如果列车停站后有车门打开，不能再重启列车，将该种情况视为疏散。列车具有在指定区域停车功能，例如站外安全避难所的位置，可以有效疏散列车上的乘客。

列车上安装紧急呼叫设备。该设备可保证乘客和控制中心之间的通信。紧急消息具有较高权限。紧急设备的提供可保证运营人员能够及时评估该情况，并快速采取适当措施（例如，立即停止运营并启动相关运营程序）。

全自动运行系统自动化程度的提高，使系统可以快速、有效的应对运营过程中乘客的需求，具备更强调整能力，进一步提升城市轨道交通运行系统的安全与效率。

全自动运行系统中涉及到行为安全场景如下：

序号	运营安全
1	紧急手柄
2	紧急呼叫
3	车门故障隔离站台门
4	站台门故障隔离车门
5	列车远程广播

3.3 功能安全--充分的冗余配置

全自动运行系统需要全系统支持全天候（7*24 小时）不间断运行，如果系统中任意一点出现故障，就有可能造成服务质量的下降甚至行车的大面积延误，在系统故障的情况下，仍旧需要保证系统安全运行。全自动运行系统使用了充分的备用和冗余来应对意外状况。信号在既有设备冗余的基础上，增强了

冗余配置，包括：头尾终端设备冗余、ATO 冗余配置、与车辆接口冗余配置，二乘二取二，三取二，控制中心和备用控制中心等。车辆加强了双网冗余控制，增加与信号、PIS 的接口冗余配置等。

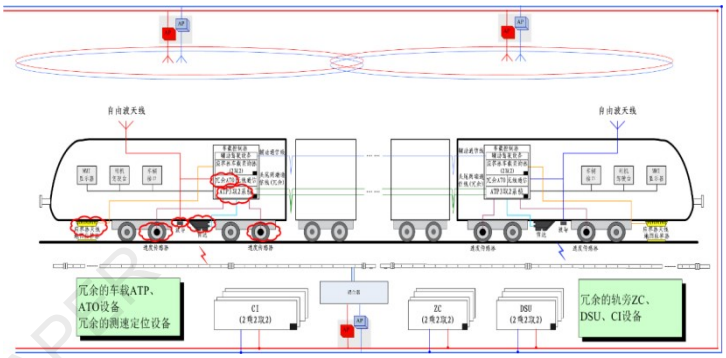

图 11 头尾冗余原理图

传统 CBTC 系统具备联锁、点式及 CBTC 三级控制模式。按照 UTO 等级建设的全自动运行系统，在常规驾驶模式的基础上，增加了 FAO（全自动运行，含 FAM 模式和 CAM 模式）模式。UTO 等级建设的线路具备完整的驾驶模式，可支持从传统的 CBTC 运营应用模式平滑过渡到全自动运行运营应用模式，详见下表。

序号	驾驶模式	
1	FAM	全自动驾驶模式
2	CAM	蠕动模式
3	CBTC-AM	CBTC 级别下的列车自动驾驶模式
4	CBTC-CM	CBTC 级别下的列车自动防护下的人工驾驶模式
5	ITC-AM	ITC 级别下的列车自动驾驶模式
6	ITC-CM	ITC 级别下的列车自动防护下的人工驾驶模式
7	RM	限制人工驾驶模式
8	EUM	非限制人工驾驶模式

在全自动驾驶条件下，当车辆网络故障，或车辆网络与信号网络之间通信故障时，列车在中心授权后进入蠕动模式，列车以蠕动模式进站停车后保持车门打开，并施加紧急制动防止列车移动，等待中心指挥人员上车转人工驾驶。

全自动运行系统同时解决传统无线干扰的问题。由于现有车地通信依据 WLAN 提出，既有线路存在使用公网频段导致抗干扰性差、覆盖范围窄导致的切换频繁以及高速移动性能差等不足，改善车地通信可靠性迫在眉睫。全自动运行系统采用 LTE 车地通信方案，解决了长距离覆盖，避免频繁切换的问题，为高速移动提供了保障。

全自动运行系统涉及到功能安全的场景如下：

序号	功能安全
1	蠕动模式运行
2	FAM/CAM 模式转换

3.4 应急安全--应急救援和响应

在运营过程中，全自动运行系统应能够响应各种突发紧急事故，发出告警信息并及时采取措施，快速恢复正常运营，将乘客风险和事故影响范围控制在最小。如障碍物/脱轨防护、紧急停车按钮、轨道或站台下的避难所等。全自动运行系统提供了一系列措施和方法去协助解决在监控列车运行过程中的运

营故障[IEC62290]。

站台紧急停车按钮应该设置于站台，如果乘客发现站台或站台轨道上有危险情况，能够在站台激活该按钮。紧急停车按钮被激活后，阻止预先定义的危险区域以外的列车进入；预先定义的危险区域内的列车停车；阻止预先定义的危险区域内的列车发车。

车载障碍物/脱轨检测装置能降低乘客的伤害和防止对人员和财产损失的事故升级。列车检测到障碍物或者脱轨，全自动运行系统应实施紧急制动、切除牵引[IEC62290]。同时将障碍物/脱轨信息传递给控制中心。全自动运行系统根据事故列车的位置信息自动形成安全防护区域。对于安全防护区域内的列车，接近故障列车应实施紧急制动，远离故障列车应继续运行，远离危险区域。且不允许安全防护区域外的列车进入到危险区域，防止事故影响扩大[IEC66290]。

控制中心收到报警后，同时联动区间 CCTV，查看现场情况，并通知人工到事发地点处理，清除障碍物，确认故障解除以及轨道上没有作业人员且具备继续无人驾驶条件后，对障碍物/脱轨导致紧急的列车实施远程缓解紧急制动的故障恢复。障碍物/脱轨情况引起的系统反应行为只有通过调度人员相关命令才可以进行释放，否则一直保持[IEC66290]。

图 12 障碍物/脱轨检测

全自动运行系统应能够响应各种突发紧急事故，同时具备故障恢复的能力。如在雨雪天气情况下，控制中心远程设置雨雪模式，保证列车的行车安全，降低了同其它列车相撞的可能。在雨后转晴天气，若仍在雨雪模式下运行会影响列车的运行效率。控制中心对天气进行实时观测，通过二次确认方式远程确认和下发取消雨雪模式，恢复列车正常的牵引制动力和运行速度，保证安全的前提下恢复列车的运行效率。

控制中心实现系统间快速联动、非正常情况下的应急处置和故障恢复，为用户后期扩展联动功能和决策支持提供了技术支撑，提高了全自动运行系统的安全性、可靠性，提升运行组织的灵活性，使系统具备更强的调整能力。

全自动运行系统中涉及到应急安全场景如下：

序号	应急安全	序号	应急安全
1	障碍物/脱轨检测	5	紧急制动缓解
2	再关门控制	6	运行中车辆或信号故障
3	救援	7	区间疏散
4	故障复位控制	8	其他远程控制

3.5 环境安全--与外界如何交互

全自动运行无人区域包括正线和车辆基地。分别在站台设置站台端门、站台边沿相关警告措施、站台护栏、半高站台封闭，防止乘客进入无人区域发生危险。

操作人员和维护人员进入站间轨道、侧线、站台轨道无人区进行作业，或者在紧急情况下或列车滞

留时列车上的乘客进入无人区疏散至站台，全自动运行系统增设人工作业按钮 SPKS 开关。在控制中心允许的前提下，乘客和工作人员在进入全自动运行区域之前，由值班员控制 SPKS 开关，将 SPKS 开关置于防护位。全自动运行系统自动建立安全防护区域。安全防护区域内的列车实施紧急制动停车，安全防护区域外的列车不允许驶入到该区域内，保证人员在该防护区域内安全行走。全自动运行系统对于建立的安全区域一直保持，直到值班员控制 SPKS 开关置于非防护位。

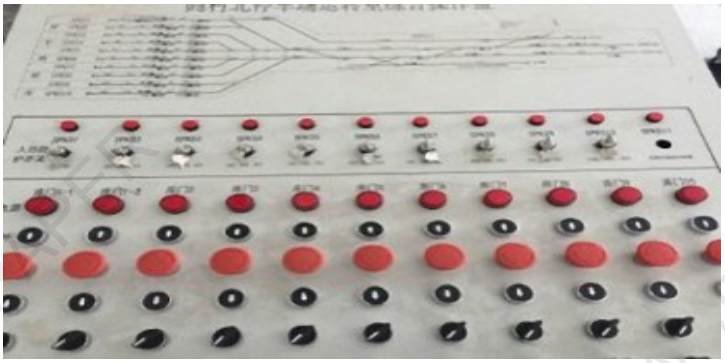

图 13 SPKS 开关

乘客存在跌下站台的危险，乘客可能会受到来自移动列车的威胁，站台人员可以通过站台紧急停车按钮，或者控制中心可以通过设置单车紧急制动，使列车立即停车，保证列车和乘客的安全。突发状况消失后，中心可对单车或者全线列车设置缓解紧急制动，使得列车快速投入运营。

图 14 综合监控下发命令

全自动运行系统中涉及到环境的安全场景如下：

序号	环境安全
1	远程紧急制动
2	清扫

4 测试、验证和确认手段：系统可靠安全的保障

4.1 多层次、全覆盖的测试、验证和确认体系

全自动运行系统的各个子系统必须经过严格的硬件、软件集成测试和系统级测试，将各个子系统集成为全自动运行系统，并经过对整体系统进一步测试、验证和确认，确保整个全自动运行系统符合系统设定的所有安全要求。

全自动运行系统特点

全自动运行系统是以行车为核心，将信号、车辆、综合监控和通信等子系统深度集成的巨型、复杂、高安全（SIL4 和 SIL2）系统；全自动运行系统具有系统化、网络化、信息化的特点；全自动运行系统运行环境复杂，功能强大，测试验证难度远大于一般应用，复杂度也远大于一般安全苛求系统。

全自动运行系统是一个基于计算机技术的功能完善、层次分明的复杂安全苛求系统。如果漏测或者误测很有可能导致事故的发生，该系统的功能和性能也直接影响轨道交通的服务质量和运营水平，仅仅依靠现场测试难以充分完备，因此开通运营前进行了全面、有效、深入的室内测试。

为确保全自动运行系统安全运行，整个系统从开发到应用，在遵循轨道交通行业标准的基础之上，还需要构建保证全自动运行系统测试过程完全受控的测试验证确认体系，从测试过程上保证全自动运行系统验证的完备性。

完全受控的测试验证确认体系

在参照 EN50126、EN50128、EN50129 标准基础上，需要对每个阶段严格定义准入条件和准出条件，用以构建多层次、全面的测试体系。

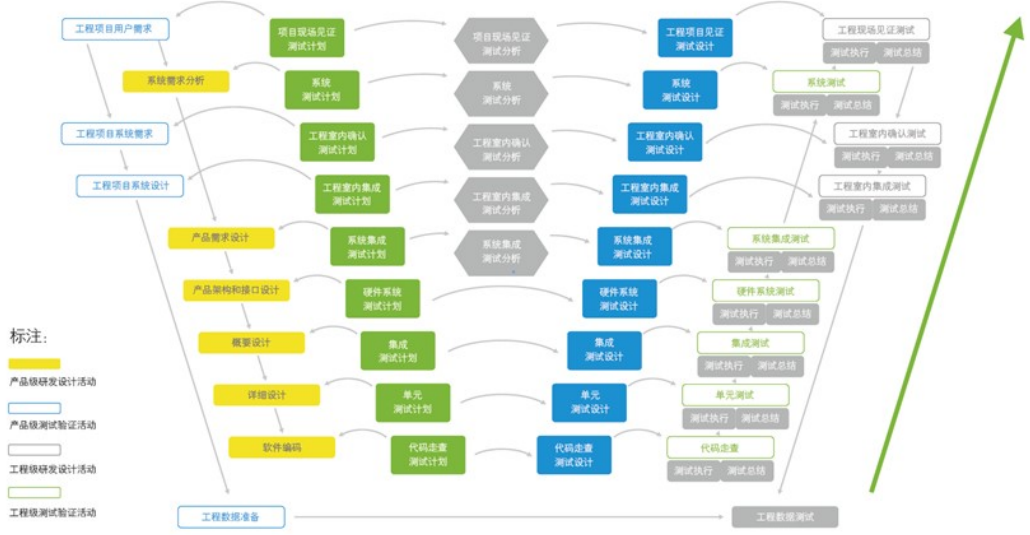

图 15 全生命周期的测试流程要求

充分考虑全自动运行系统的特点，除了通过遵循行业标准的测试验证体系保证测试过程的完备性和有效性，还应从测试技术和测试手段上保证测试内容的完备性和有效性。

成熟的测试技术-多层次的各级测试

为保障全自动运行系统的可用性、可靠性和安全性，需要开展广泛的测试、验证和确认活动。

模块级测试主要针对软件/硬件具体实现进行验证。由于全自动运行系统属于安全苛求产品，根据安全最佳实践要求，需要通过一系列的模块级测试，在软硬件实现层面尽可能的发现和解决实施过程中引入的缺陷，确保实施细节的任何瑕疵都不会被放过。

针对安全苛求产品，在产品定型（系统级确认）测试中，除传统 CBTC 级别针对 VOBC、ZC、DSU 等子系统的确认测试外，需要增加针对信号系统层级和 FAO 系统层级场景的相关测试，确保所有场景和系统在异常状态下的表现与设计预期一致。

在 FAO 产品应用于特定轨道交通线路上之前，需要结合线路布置特点、车辆特点、通信系统等其他系统特点进行多轮次、多层级的现场测试验证，通过室内测试、现场单体调试、现场动车调试、现场多车调试、现场跑图试运行调试等多个测试验证环节，确保所有风险被控制在业主可接受程度。

丰富的测试手段

过程手段

- 流程和平台工具保证 100%测试用例覆盖系统需求

室内阶段

- 覆盖全面的软、硬件模块级测试
- 完备的测试设计和测试案例
- 硬件在环的室内模拟测试
- 多专业联动测试调试
- 完全按照运营策略的场景测试
- 专项测试和复杂性场景
- 故障恢复测试
- 性能测试

现场阶段

- 现场单车、多车测试
- 根据全自动运行 41 个场景设计全自动运行系统现场联调联测大纲，保证无场景遗漏。

4.2 不遗漏任何细节：模块级测试

模块级测试是一个高可靠、高安全的复杂系统达到高 RAMS 的基础，全自动运行系统对硬件设备可靠、安全运行和软件正确性都提出了更高的要求。

覆盖全面的软、硬件模块级测试

- 硬件模块测试至少应涉及单元测试、EMC、单板信号完整性、热性能测试等。
- 软件白盒测试至少应采用代码走查、范根检查、静态分析、动态测试、自底向上的集成等手段对软件进行全方位测试。
- 燕房线全自动运行系统除进行常规的模块级测试外，还开展了单板及插箱热仿真验证，确保系统的高可靠性。

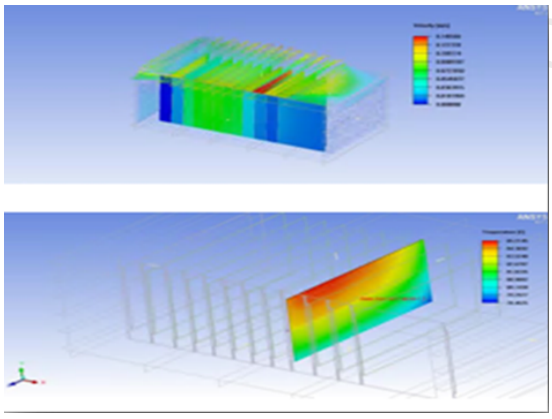

图 16 通过热仿真测试验证系统热性能

4.3 不遗漏任何场景：产品定型（系统级确认）测试

为了全面的验证全自动运行系统接口、功能、性能的有效性，室内应从测试内容、测试设计、模拟仿真、多专业联动、专项测试、性能、故障恢复等多维度进行产品定型测试，确保系统层面测试的完备性和有效性。

产品定型（系统级确认）测试

- 室内产品级测试，完成全自动运行系统信号专业各系统产品级单体测试、系统间集成测试和集成后的大系统联测。例如，联锁单体测试、ATP/ATO 单体测试、TIAS 单体测试等等。
- 进一步地，在实验室内，通过使用特定工程线路的线路数据，进行大量的数据测试，从数据层面完成全自动运行系统的广泛测试验证，在产品应用到实际运营线路之前，更多地暴露产品问题，保证系统的可靠安全。
- 全自动运行系统与多专业深度集成，实验室内尽可能的模拟注入现场不能或者不容易产生的多专业间的场景，完成多专业联动的联调联测，测试验证信号（含综合监控）、车辆、广播、乘客信息、视频监控、站台门等多专业联动。

测试设计和测试案例

测试设计是非常重要的一个环节。

测试案例设计中，测试输入项的完整程度直接影响测试案例的完整程度，全自动运行系统的测试应加入测试分析，通过收集全自动运行系统的标准规范、场景图、运营规则、系统需求、设计等相关输入，使测试设计工作前移，一些设计方面的缺陷和不足能够在早期被发现，保证运营场景均被覆盖，并作为测试案例的设计基础。

测试案例是测试验证的灵魂。针对全自动运行系统的测试，应构建基于功能交互和业务场景的测试案例库。传统 CBTC 系统具备联锁、点式及 CBTC 三级控制模式。按照 UTO 等级建设的全自动运行系统，在常规驾驶模式的基础上，增加了 FAO（全自动运行）模式，测试案例设计工作繁重复杂。以燕房线为例，仅基于 FAO 场景的实验室模拟测试案例数量达 5 万余条。

多专业联动的全自动运行综合技术实验室

为保证系统测试的完备性，建设了全自动运行综合技术实验室，实验室搭建了系统级测试验证平台，构建与全自动运行相适应的信号、综合自动化、通信、模拟车辆、列车模拟仿真等测试验证最小系统。全自动运行综合技术实验室具备模拟全自动运行系统各种运营场景，完成全自动运行系统运行控制，支撑全自动运行控制系统的测试。通过系统功能、性能、数据及异常处理场景各阶段的测试，保证系统完全满足各项设计要求。

图 17 全自动运行综合技术实验室

考虑到该全自动运行系统“高度自动化、多专业系统集成度深、各系统高效联动控制”特点，实验室环境内测试应考虑多专业的联动，能够针对 FAO 新增和增强功能进行专项测试；同时，测试关注故障导向安全和故障恢复时保证全自动运行系统的安全运行。以燕房线为例，给出一些全自动运行系统典型

测试场景。

多专业的功能联动验证-障碍物脱轨检测的测试

全自动运行系统的核心是信号及综合监控、车辆、LTE、CCTV、PIS。

通过模拟车辆（车辆）已经检测（CCTV）到障碍物，验证车辆将障碍物信息传递给全自动运行信号系统的车载设备，系统输出紧急制动停车（信号），同时汇报（LTE）给全自动运行系统的地面设备并建立保护区，后续安装全自动运行系统的车辆会停在保护区之外（信号），联动区间 CCTV，同时全自动运行系统将报警信息传给中心（综合监控）以供运营人员进行后续运营处理（PIS）。

同时，测试内容还包括了障碍物脱轨故障清除过程中、清除后本列车及追踪运行的一系列列车的恢复运行，保证恢复运营的过程中全自动运行系统的安全性。

这些测试完成之后，能够保证涉及多专业的障碍物脱轨监测的功能在遇到障碍物脱轨的运行场景时，能够安全正确的运作。

多专业的功能联动验证-车辆火灾的测试

模拟列车（车辆）将火灾报警信息及 CCTV 画面发送给中心 TIAS；列车（车辆）自动运行到最近的站台打开车门不关闭（信号）；如中心（综合监控）确认火灾确实发生，触发乘客广播；如火灾为误报，中心复位火灾报警后，可继续运行。该测试完成后可以保证涉及多专业的车辆火灾的功能正确运行。

同时，测试内容还包括了车辆火灾清除过程中、清除后本列车及追踪运行的一系列列车的恢复运行，保证恢复运营的过程中全自动运行系统的安全性。

多专业的功能联动验证-车站火灾的测试

模拟车站火灾，车站 FAS 系统触发车站火灾联动，并将车站火灾报警信息传送给 TIAS 系统（信号和综合监控）。中心防灾调度与车站电话确认火灾情况，环调也可以通过 CCTV 确认现场火灾情况，确认后，电话通知行调该车站是否真实存在火灾情况；乘客调触发车辆广播、站台广播、车辆 PIS（车辆）显示；车站火灾情况下，车站广播强制转入消防应急广播状态，AFC 闸机打开。

同时，测试内容还包括了车站火灾清除过程中、清除后列车运行的一系列列车的恢复运行，保证恢复运营的过程中全自动运行系统的安全性。

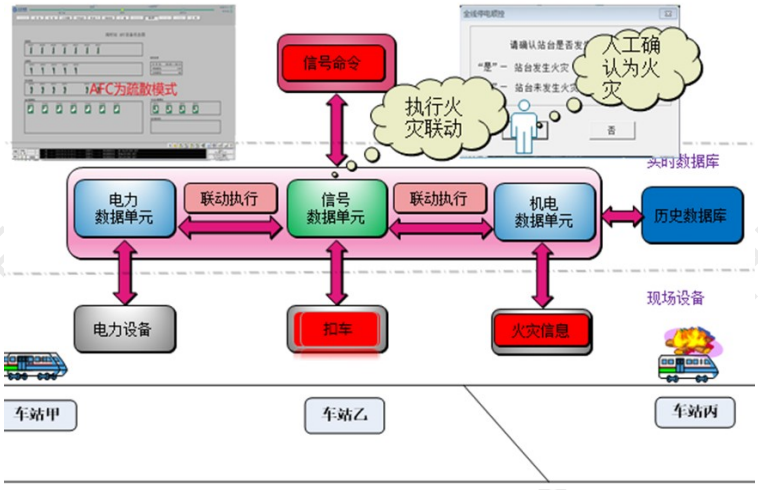

图 18 多专业的功能联动验证-车辆火灾

专项测试

室内模拟专项测试考虑列车出现越标或欠标的工况下，信号和车辆联动实现对标的各种情况下跳跃的测试验证。同时考虑了自动洗车专项测试和其他列车工况处理。

故障恢复测试

测试过程中还考虑了故障恢复时的场景，例如：

- 在区间时，故障列车作为追踪列车故障恢复时，故障列车不会追尾前车。

- 在区间时，故障列车作为被追踪列车故障恢复时，对后续追踪列车的影响，以保证运营安全。
- 在站台时，故障列车作为追踪列车故障恢复时，故障列车不会追尾前车。
- 在站台时，故障列车作为被追踪列车故障恢复时，对后续追踪列车的影响，以保证运营安全。

实验室系统级确认测试不仅应关注功能，更应关注性能及全自动运行系统特有故障测试。由于许多故障场景很难在真实环境下得以验证，所以通过室内仿真平台验证现场不可测的安全防护功能是必要选择，例如空转打滑、过欠标、溜车、车站火灾、车辆火灾、障碍物脱轨检测。

完全按照运营策略进行的场景测试

针对全自动运行场景，应编制全自动运行联调大纲，一对一进行场景覆盖。

全自动运行系统实验室模拟测试应包含但不限于以下功能：列车上电、自检、段内行驶、正线区间行驶、车站停车及启动、清客、端站折返、列车回段、休眠断电、洗车等全过程自动控制以及故障和应急情况下多专业的联动控制。

性能测试

应开展实验室系统级性能测试，比如地面的一个区域控制器系统（全自动运行系统的子系统）最多管理的列车数量等。

不同运行等级转换、混跑的复杂性测试

实验室内应通过模拟和注入故障，充分考虑运营过程中会遇到的 FAM、CAM、CBTC、点式和联锁级下运行等级的转换和混跑的各种情况。

4.4 不遗漏任何风险：现场测试验证

在全自动运行系统工程应用前，应在特定工程项目进行一系列现场测试验证活动，确保所有风险均降低到了可接受程度。

一般情况下，现场测试验证按停车场测试阶段、样板段测试阶段、全线测试阶段有计划的推进。

停车场测试阶段，针对每列车的静动态性能测试保证配备了全自动运行系统的列车无故障运行的同时，进一步的验证系统与现场各真实设备的无障碍联动。

停车场测试调试阶段目标及工作内容

- 信号（含综合监控），完成全自动运行系统信号专业各子系统产品级测试。
- 车辆，实现车辆故障信息落地，完成列车动态静态测试。
- 通信，无线列调、广播、视频监控，LTE 综合承载应用，验证综合承载车地通信性能。
- 多专业联动测试，实现全自动运行系统停车场全部场景测试； 试车线验证正线相关场景测试。
  - 全自动出入库功能测试
  - 车辆自动休眠唤醒功能测试
  - 实现全自动洗车功能测试
  - 车库门联动功能测试
  - 完成停车场全自动运行场景调试

样板段测试阶段，主要关注完成系统性能参数测试，车辆调、乘客调联动功能，工作内容应包括，折返能力测试、运营图兑现测试、车辆调列车控制及联动功能、覆盖全自动运行系统 41 个场景的多专业联动测试。

全线测试阶段，除进行常规的单车调试、多车调试外，在跑图测试阶段，还应该进行 8 车、11 车、16 车的多车跑图试运行压力测试。在测试过程中对以下各项指标进行考核：

- 兑现率
- 正点率
- 车库门开关成功率
- 站台门开关成功率

- 站台门对位隔离车门成功率
- 车门对位隔离站台门成功率
- 紧急呼叫成功率
- 自动折返成功率
- 紧急拉手成功率
- 休眠唤醒成功率
- 自动洗车成功率

全自动运行综合联调联测

工作内容覆盖工程全部过程，管理范围涵盖全部专业，从范围、管理上保证并验证了全自动运行系统的安全、质量。基于全自动运行的系统运行级别的联调联测范围包括：

- 系统能力测试
- 供电系统满负荷测试
- 牵引供电系统运行模拟联调
- 弱电设备抗干扰联调
- 无线通信系统与信号、车辆、电话联调
- 时钟系统与关联系统联调
- 传输系统与关联系统联调
- 车辆与乘客信息系统（PIS）联调
- 信号系统综合联调
- 信号系统与车辆、屏蔽门联调
- 综合监控系统与 FAS 系统、屏蔽门、信号系统、AFC 系统、CCTV、广播系统及 PIS 系统联调

以燕房线为例，停车场测试共执行了 3.8 万余条用例，其中全自动运行用例占比约 60%，顺利完成了全自动运行系统的停车场功能测试。其中，系统功能测试 647 条，系统数据测试 12283 条， FAO 新增系统数据测试 23587 条，FAO 新增接口测试 365 条，FAO 新增功能测试 869 条，多专业联动专项 558 条。

图 19 燕房线停车场

样板段测试执行了 2.4 万余条用例，其中全自动运行用例占比约 60%，顺利完成了全自动运行系统样板段的功能测试。其中，系统功能测试 860 条，系统数据测试 12508 条， FAO 新增系统数据测试 8846 条，FAO 新增接口测试 360 条，FAO 新增功能测试 580 条，多专业联动专项 1154 条。

全线测试阶段，燕房线增加了故障演练、多系统稳定性考核等手段，结合既有测试工作，通过多角度、全方面的测试验证，为产品的质量、安全、后续每一条使用该全自动运行线路的开通提供足够的信心、奠定坚实的基础。

燕房线稳定性测试预期指标与实际指标对比					
测试项	休眠唤醒	车库门开关	站台门开关	车门隔离站台门	站台门隔离车门
预期成功率	99.79%	99.72%	100.00%	99.99%	99.99%
成功率	99.80%	99.78%	100.00%	100.00%	100.00%
紧急呼叫	洗车机	紧急拉手	折返成功率	运营图兑现率	运营图正点率
98.14%	98.77%	98.14%	99.98%	99.94%	99.94%
100.00%	100.00%	100.00%	100.00%	100.00%	100.00%

5 与乘客的交流互动

全自动运行系统运营的主要目的就是快速、高效的将乘客送达预定地点，因此全自动运行系统关注与乘客的交流互动感受。

乘客从进入站台到安全到达目的地离开站台，时刻都与全自动运行系统产生交互：

- 灵活的运营组织应对突发客流：全自动运行能够根据运输需求灵活地调整发车间隔，不受司乘人员的限制。通过在车站增加存车线，灵活加减车，适时调整运能，可以提高系统对突发大客流的响应能力；全自动运行系统兼容有人驾驶 CBTC 运行模式，发生紧急情况时中心远程可随时介入处理，GoA3 级车上人员也可随时就地处理。运营的调整不会与乘客进行直接交互，但是运营组织对客流的灵活调整，可以减小乘客滞留站台时间、减少列车拥挤程度，从而改善乘客乘车环境。

图 20 灵活的运营组织应对突发客流

- 乘客在站台或在乘车：乘客进入站台后或进入列车后，乘客信息系统、广播系统等会为乘客提供列车运行与到站预告信息，协助乘客获得列车信息。在通常条件下，全自动运行系统与传统 CBTC 系统给候车乘客的信息是没有本质区别，但是在紧急情况下，如列车或车站火灾时，旅客信息系统、广播系统等可以通过更多的联动功能，为乘客提供更完善的应急响应指引。
- 乘客乘降过程：乘客乘降过程是城市轨道交通运营中与乘客交互互动风险较大的阶段，全自动运行系统需要考虑换乘过程中车门和站台门的安全联动，列车具备启动条件检查，避免乘客在车厢间、车辆和站台间受到伤害，确保乘客乘降过程的安全。
  - 全自动运行系统相对于传统 CBTC 系统增加了车门故障隔离站台门和站台门故障隔离车门功能，当某个站台门或车门发生故障时，列车进站中，故障对应的站台门故障指示灯点亮，乘客应根据指示有序选择其他站台门准备上车；车上会通过广播告知乘客对应的车门无法打开，乘客应根据广播有序选择其他车门准备下车。
  - 当由于拥挤、乘客故意扒门或其他情况，车门自动尝试三次关闭仍无法关闭时，由于全自动运行系统中车上无司机进行确认，系统会进入防夹状态，只有在站台综合站务员确认可以关门后，按压站台关门按钮，再次关闭车门和站台门后，列车才能继续行驶。一方面系

统通过故障安全原则确保运营安全，另一方面也给乘客提出更高要求，应在给定时间内尽快完成乘降，以免影响列车运行效率。

- 由于车辆关门后，无法像常规 CBTC 系统那样由司机确认乘客未被夹在车辆和站台门间，因此全自动运行系统通过增加安全检查设备等手段，对每个车门关闭后与站台门之间的空闲情况进行检查，只有安全检查设备认为车辆与站台间无杂物时，才输出满足车辆启动安全条件，允许车辆发车，确保乘客乘降过程的安全。

- 乘客乘车中发生意外的紧急处理：乘客由于个人原因或发现车辆无法处理的紧急情况时，应通过列车上安装的紧急呼叫设备与控制中心进行通信，紧急消息具有较高权限，运营人员进行应急处理时，乘客也可在运营人员的指导下，快速开展应急响应。乘客认为需要立刻停车时，可使用全自动运行系统在列车上安装的紧急停车按钮（紧急刹车手柄）。紧急停车需求激活并不直接引起列车紧急制动，而是通过系统告知控制中心，由中心相关人员与乘客通过 PA 等手段确认列车现场情况后，根据预设的应急处理要求进行处理。操作紧急停车按钮时应启动紧急程序停车，但是不允许列车在站外停车，也不能在隧道或没有安全区域的地方停车。
- 全自动运行系统应急时对乘客的防护：由于全自动运行系统并不要求必须有司机或其他工作人员在列车上值守，因此在出现紧急情况时（如行驶过程中车辆车门状态丢失、车辆发生火灾、车辆网络故障等），常规 CBTC 列车会立即紧急制动或切除牵引，全自动运行即使列车可能已经紧急制动停在区间，但只要站台是安全的，全自动运行系统就会将列车开入站台对位停车后，根据应急处理程序，通过广播、乘客信息系统等手段，协助乘客疏散，最大限度的保证乘客安全，同时减少乘客滞留在列车中的时间。

全自动运行系统已经充分考虑了列车与乘客可能的交互场景，并针对全自动运行的特点进行了一系列互动策略和处理措施优化，能够确保乘客可以获得比传统 CBTC 系统更便捷、高效和安全的交互体验。

6 结论

全自动运行系统旨在利用全自动手段全方位解决城市轨道交通领域面临的行为安全、运营安全、功能安全、应急安全和环境安全五大安全问题，信号系统作为全自动运行系统的核心，与车辆、通信（含PIS）、站台门、综合监控、车辆基地等综合协调，通过系统性、综合性、多层次的安全场景分析和专项安全设计、全覆盖的测试、验证与确认和北京燕房线的工程示范实践，能够有效保障全自动运行系统提供比既有系统更安全的服务。

7 附录一

下表给出本白皮书论述中使用的全自动运行场景与 IEC62267 中安全需求的对应关系。

IEC62267		全自动运行场景
一级需求	二级需求	功能场景
01 一般需求		
	01 保护轨道的公共工作规章	/
	02 防火	车辆火灾 站台火灾
	03 系统和设备	ALL
	04 乘客行为的规定	紧急呼叫 列车远程广播 进站停车 站台发车 车门故障隔离站台门 站台门故障隔离车门 再关门控制 车门状态丢失 站台门状态丢失
02 监控 AUGT 系统		
	01 OCC 员工监控	运行中车辆或信号故障 故障复位控制 紧急制动缓解 紧急呼叫 雨雪模式 救援
	02 运营人员的活动	区间疏散 救援
	03 通信系统	紧急呼叫 列车远程广播
03 运营规定		
	01 乘客救援规定	救援
	02 火灾情况的规定	车辆火灾 站台火灾
	03 可预见的人为破坏规定	/
	04 轨道限界检查规定	轨道车运行
	05 投入和停止运营规定	进入正线服务 停止正线服务 早间上电 清客

	06 车辆段内的列车操作规定	回库 清扫 洗车 早间上电 列车唤醒 唤醒 列车休眠
	07 列车投入运营和退出运营的规定	清客 故障复位控制 紧急制动缓解 FAM/CAM 模式转换
	08 清除滞留列车的规定	救援
04 站台安全措施		
	01 封闭和开放站台基本安全保障	站台门状态丢失 站台火灾
	02 封闭式站台	车门故障隔离站台门 站台门故障隔离车门 进站停车 站台门状态丢失
	03 带检测系统的开放式站台	/
05 列车安全保障		
	01 关门监控	车门状态丢失 站台发车
	02 乘客乘降门解锁	进站停车 车门故障隔离站台门 站台门故障隔离车门
	03 车门解锁	紧急手柄 区间疏散 车门状态丢失
	04 紧急出口	区间疏散 车门状态丢失
	05 车载障碍物检测装置	障碍物/脱轨检测
	06 脱轨检测装置	障碍物/脱轨检测
	07 车载视频监控	清客
	08 公共广播系统（列车）	列车远程广播
	09 列车退出运营的车载公告	清客 列车远程广播
	10 车载紧急停车请求	紧急手柄
	11 车载紧急呼叫设备	紧急呼叫
	12 火灾和烟雾探测（列车）	车辆火灾

	13 列车状态监测和测试	唤醒 日检与维修 车辆制动系统故障 运行中车辆或信号故障 车上设备工作状态远程监督
	14 人工操作	FAM/CAM 模式转换
	15 自动编组下的安全速度	/
	16 列车意外移动的反应	其他远程控制
	17 车载疏散警告的方式	列车远程广播
06 乘客乘降区安全保障		
	01 乘客换乘期间列车不动	车门状态丢失 站台门状态丢失 其他远程控制
	02 列车开门的安全保障	车门状态丢失
	03 列车关门的安全保障	车门状态丢失 车门故障隔离站台门 站台门故障隔离车门
	04 站台上标记列车门区域	/
	05 运营人员监控	其他远程控制 跳停 扣车
	06 列车和站台间隙的安全防护措施	车门故障隔离站台门 站台门故障隔离车门
	07 车厢连接处安全防护措施	/
	08 列车与站台屏蔽间隙安全防护措施	车门故障隔离站台门 站台门故障隔离车门
	09 防止乘客坠入间隙后触电的安全防护措施	/
07 轨道安全防护措施		
	01 轨道隔离	/
	02 轨道沿线的警告方式	/
	03 轨道沿线的物理屏障	/
	04 桥梁上的物理防护屏障	/
	05 站台轨道及站间轨道间的入侵检测设备	障碍物/脱轨检测
	06 轨道入侵检测设备	障碍物/脱轨检测
	07 轨旁障碍物检测设备	障碍物/脱轨检测
	08 带有门禁控制的站台端门	/
	09 物理隔离轨道区间的紧急出口	/
	10 火灾及烟雾探测（站间区段）	站台火灾
	11 水灾防护	/
	12 道口	/
	13 施工区域	/
08 转换区域及车辆段的安全防护区域		回库 自动调车