文章编号:1671-4598(2025)03-0313-10 DOI:10.16526/j.cnki.11-4762/tp.2025.03.039 中图分类号:TP391 文献标识码:A

高速磁浮车载控制系统预期功能安全验证评估研究

苗 欣[1],刘纪龙[1],李 琳[1],许琼晓[1],王友彪[2],居法云[3]
(1.中车青岛四方机车车辆股份有限公司,山东 青岛 266100;
2.中国铁道科学研究院集团公司铁道科学技术研究发展中心,北京 100081;
3.北京航天测控技术有限公司,北京 100041)

摘要:车载控制系统是高速磁悬浮列车安全运行的核心组件,安全等级为SIL4;由于其高度自动化、智能化和复杂性,常规的系统试验台测试和功能安全分析验证已经难以适用于该系统复杂失效的分析识别;预期功能安全(SOTIF)是评估和确保复杂系统在预期操作条件下安全性的重要方法,已在智能网联汽车领域成功应用;通过开展高速磁悬浮车载控制系统的预期功能安全验证评估系统研究,构建典型预期功能安全场景和场景测试用例,设计验证评估系统,旨在为车载控制系统批量生产提供技术支撑,为提升高速磁悬浮列车的安全提供重要的技术保障。

关键词:车载控制系统;预期功能安全;典型测试场景;半实物仿真

Research on High-Speed Maglev Vehicle Control System SOTIF Verification and Assessment

MIAO Xin[1], LIU Jilong[1], LI Lin[1], XU Qiongxiao[1], WANG Youbiao[2], JU Fayun[3]
(1. CRRC Qingdao Sifang Co., Ltd., Qingdao 266100, China;
2. Railway Science & Technology Research & Development Center, China Academy of Railway Sciences Corporation Limited, Beijing 100081, China;
3. Beijing Aerospace Measurement & Control Technology Co., Ltd., Beijing 100041, China)

Abstract: The vehicle control system is the core component for the safe operation of high-speed maglev trains, with a safety level of SIL4. Due to its high degree of automation, intelligence, and complexity, it is difficult for conventional system testing on the test bench and functional safety analysis verification to analyze and identify complex failures. safety of the intended functionality (SOTIF) is an important method for assessing and ensuring the safety of complex systems under expected operating conditions, which is successfully applied in intelligent connected vehicles. By studying the expected functional safety verification and assessment of high-speed maglev on-board control system, the typical expected function safety scenarios and scenario testing cases are constructed, and the verification and assessment system is designed, which provides technical support for mass production of vehicle control systems and important technological guarantee for enhancing the safety of high-speed maglev trains.

Keywords: vehicle control system; SOTIF; typical test scenarios; hardware-in-the-loop

0 引言

我国成功研制并下线了具有完全自主知识产权的国产化时速600公里高速磁浮交通系统,这一里程碑事件不仅展示了我国在高速磁悬浮技术领域的重大突破,也标志着我国在该领域的自主研发能力已趋于成熟。经过近二十年的不懈努力和技术创新,我国已经具备了从设计到制造的全链条自主研发能力,并建立了完整的工程化技术和自主控制的产业链。目前,这一高速磁悬浮交通系统已从理论研究和开发阶段,顺利过渡到了高速测试和实际应用阶段,正在向示范运行和产业化方向稳步推进。下一步,600公里每小时的高速磁悬浮系统将在

收稿日期:2024-11-11; **修回日期**:2025-01-06。
基金项目:高速磁浮系统技术研究及工程化示范(2021CCZ002);明线运行条件下高速磁浮铁路气动特性研究(2022YJ139)。
作者简介:苗 欣(1973-),女,正高级工程师。
引用格式:苗 欣,刘纪龙,李 琳,等.高速磁浮车载控制系统预期功能安全验证评估研究[J].计算机测量与控制,2025,33(3):313-322.

实际轨道环境中进行性能测试和速度测试，以验证其高速运行的稳定性和安全性；需要开展高速运行条件下基础理论验证与高速试验评估；需要开展高速运行动态性能评估和运行考核、高速运行条件下耦合机理、高速系统模型的验证[1]。

车载控制系统作为高速磁悬浮列车的核心组件，直接影响列车运行效率和安全性。该系统负责传输列车的悬浮、导向、涡流制动、车载电网、车门等核心控制指令并实现相关状态监测，保障高速磁悬浮列车在高速下稳定运行。磁悬浮列车运行速度的不断提升，使得车载控制系统面临的潜在风险也日益复杂，而确保车载控制系统在不同运行场景下始终保持安全的有效预防手段之一，就是进行预期功能安全测试评估。

虽然安全测试评估是开展预期功能分析和确认的基础，但现阶段预期功能安全的研究工作大量集中在测试场景构建方面。比亚迪汽车有限公司的陈景龙等人开展了智能网联汽车智能制动系统的预期功能安全分析及测试技术研究[2]；清华大学的吴思宇等人提出基于关键场景的预期功能安全双闭环测试验证方法[3]；鄢航等人进行基于特征场景预期功能安全分析的量化评估[4]；陈浩等人进行智能汽车预期功能安全风险评估方法研究[5]；针对场景化安全评估中的标准化难题，ISO34502[6]制定了一系列场景构建和评估的步骤，这些步骤专门针对SOTIF（预期功能安全）的常见触发因素进行了考量。

ISO/DIS 21448-2021 中的三支柱测试体系包含模拟仿真测试、实车测试等内容，通过功能、性能、安全性的全面评估和验证，可以发现系统设计不足，实现未知不安全场景到已知不安全场景的转化，最终将风险控制到合理的水平。由于模拟仿真测试在揭示问题上的不足，而实车测试又远滞后于磁悬浮列车研制过程，这些限制因素大幅增加了问题识别和优化的成本。因此，本研究依托于车载控制系统的预期功能安全需求，初步建立了一个预期功能安全的测试场景库，设计了场景测试案例，并深入探究了车载控制系统预期功能安全的验证与评估体系。

1 车载控制系统和预期功能安全测试

1.1 车载控制系统

1.1.1 功能组成

车载控制系统的主要功能是传输控制指令和状态反馈信号，通过车载控制系统将车载安全计算机发出的诸如悬浮、导向、涡流制动、车载电网、车门的安全指令传达给车辆各个子系统，并将子系统的指令状态监控、乘客紧急、火灾报警等信号回传至车载安全计算机[7]。

车载控制系统的输入和输出信号都是以双通道一冗余方式传输，与车上其他各个系统关联采用硬线连接。车载控制系统通过通讯接口（如 CAN 总线、以太网总线）与车载诊断系统连接。

1.1.2 现有测试方法

现阶段高速磁悬浮车载控制系统主要采取功能测试的方式进行状态确认，包括地面台架测试、单车测试和编组测试[8]。

1）地面台架测试：

用于对车载控制系统所有的指令信号和状态信号的供电、信号电平、负载电流进行测试，车载控制器包含多个指令和状态反馈信号处理单元，如将车载控制的这些单元的所有排列组合进行测试，测试项点多达上万条。

2）单车测试：

实现各个分系统之间的导通测试，通过运控系统模

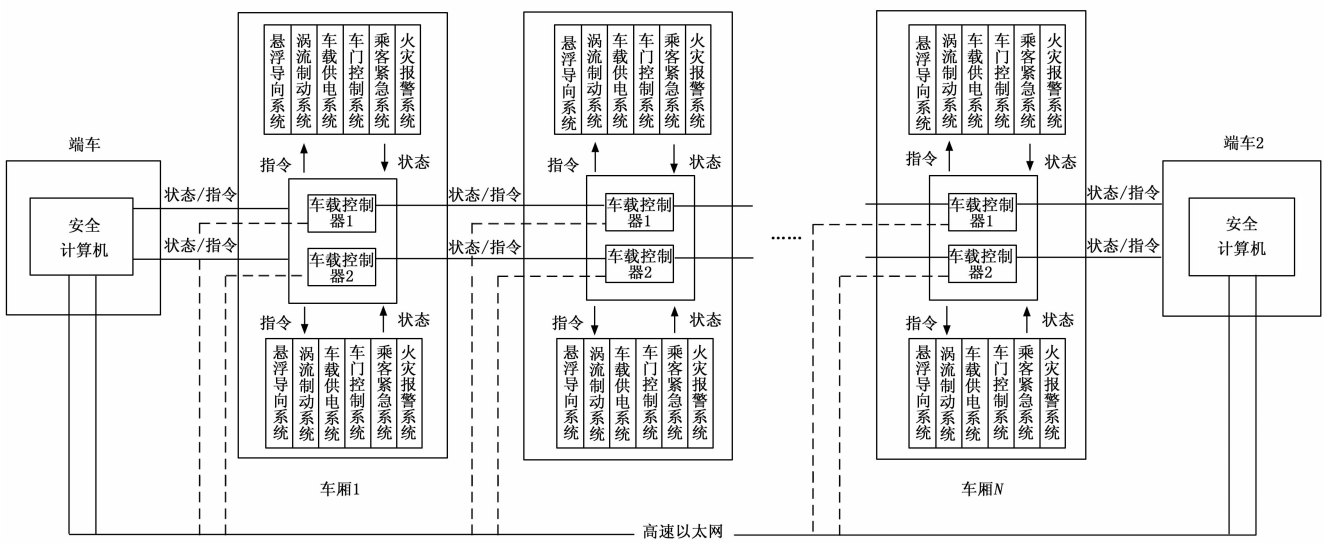

图 1 车载控制器工作原理图

拟指令信号，在操作台显示屏测试对应信号变化是否满足设计需求。

3）编组测试：

测试车载控制器冗余功能，当切断其中一个车载控制器，列车各个系统的功能完整性不受影响。

1.2　预期功能安全

1.2.1　预期功能安全的定义和范围

预期功能安全（SOTIF）的国际标准是 ISO/DIS 21448-2021，该标准主要关注功能安全之外的预期功能安全风险问题。预期功能安全是指：不存在因车级的“预期功能”规范不足或系统中的 E/E 元件的实现上规范不足或性能限制而导致的风险[9]。

ISO 21448 强调在真实环境中进行充分的功能验证和测试，确保系统能够在预期之外的场景中保持安全。高速磁悬浮列车由于涉及多种新型技术，在运行中可能会面临超出传统安全评估的风险。通过将 ISO 21448 标准引入磁悬浮车载控制系统的验证评估过程，可以增加识别和预防系统在未预见场景下的潜在风险的能力。例如，在高速行驶中，如果列车的控制系统遇到瞬间干扰，系统需要具备自我修复能力，以防止列车脱轨或停运。此外，控制系统在面对天气变化、环境电磁干扰等不可控因素时，也需要进行充分的冗余设计和验证测试。

1.2.2　预期功能安全研究路线

设计和规范、危害识别与评估、潜在功能不足和触发条件识别与评估、功能改进、验证和确认策略和定义、已知危险场景评估、未知危险场景评估、SOTIF 发布标准、运行阶段活动[10]等要素共同构成了 SOTIF 设计和开发的全面框架，确保系统在面对各种潜在风险时能够保持安全和可靠。

开展预期功能安全研究时，首先根据设计和规范开展危害识别和评估，识别潜在的功能不足和触发条件；然后根据相关条件构建场景，进行已知/未知危险场景测试分析及验证，实现车载控制系统运行设计域（ODD）内的安全测试评估和运行设计域（ODD）外的安全边界确认，SOTIF 设计开发基本内容逻辑流程如图 2。

1.3　面临的安全挑战与需求

600 公里磁悬浮交通系统基于常导电磁悬浮技术，其电磁悬浮通过电磁铁和铁磁轨道之间产生的吸引力来实现悬浮[11]。常导电磁悬浮系统本质上属于开环控制系统，理论上存在不稳定性，因此必须依赖于一个精确的主动控制机制来确保系统的动态稳定性，以维持车辆与轨道之间大约 10 毫米的恒定间隙[12]。

1）复杂系统架构带来的分析难度：

随着控制技术的演进，系统逐渐展现出集成化、智能化、网络化和软件化的趋势，这使得系统设计变得更加复杂。在这样的背景下，系统安全分析的任务变得更加艰巨。传统上依赖于功能安全分析的方法往往带有很强主观色彩，分析结果精确度很大程度上取决于工程师

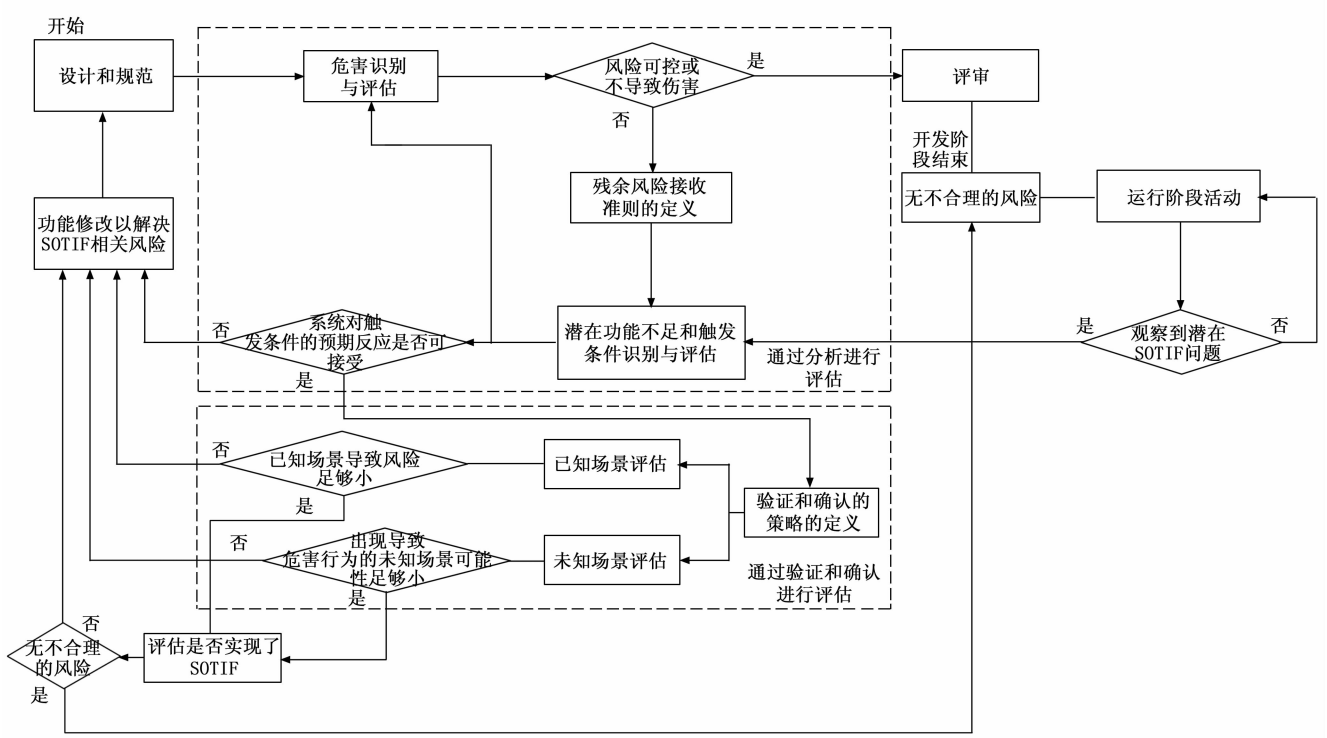

图 2　SOTIF 设计开发基本内容逻辑流程[10]

的专业能力。对于同一系统，不同工程师可能会构建出截然不同的安全和可靠性模型。在处理那些具有动态重构特性、故障时序关联和逻辑关联的复杂系统时，仅依赖人工推理来分析系统的故障逻辑联系变得不太现实，即便能够进行分析，其结果的完整性和精确度也难以确保。

2）高速运行环境的特殊要求：

高速运行状态下，磁悬浮列车面临空气动力效应、气动噪声以及车轨之间的耦合振动等多种挑战。当列车处于高速行驶时状态下，上述因素对车辆稳定性的影响变得尤为显著，仅依靠悬挂系统的参数调整和优化已不足以确保良好的动态性能。为有效应对影响，需要车载控制系统进行综合优化控制。随着磁悬浮列车速度达到 600 km/h 后，外部对车辆系统的干扰将变得更加剧烈，对车辆系统平稳性和稳定性提出了更高要求。因此，车载控制系统必须解决在高速运行时如何有效抵御外部多因素扰动等一系列技术难题。

3）技术更新与迭代的影响：

随着信息技术的蓬勃发展，高速磁悬浮列车的智能化成为可能，车载控制系统作为磁浮列车的关键系统，担当了应对上述技术挑战以及进一步提升高速磁浮交通系统稳定性、平稳性的重任。此外，车载核心控制芯片的架构已从单核向多核方向发展，可靠性设计与功能安全保障技术也变得十分复杂。

4）多因素交互作用的复杂性：

高速磁悬浮列车的功能安全研究需要考虑多种因素的交互作用，如气动外形、运行环境、线路参数和人员安全等，这些因素之间存在复杂的相互作用和影响，使得功能安全的研究变得更加复杂。气动外形的改变会影响气动阻力、升力、侧向力等气动载荷，进而影响列车的运行平稳性；列车的运行环境，如强风、交会及进出隧道等场景，也会对列车的气动性能产生显著影响。

因此，需要采用系统工程的方法，进行多学科的协同设计和优化，深入探寻复杂运行环境下的运行安全边界，以全面评估和确保高速磁悬浮列车的安全性和可靠性。

1.4 预期功能安全验证形式

车载控制系统开展预期功能安全验证的流程主要包括场景生成/提取、场景库建立、场景选择、测试执行、评价指标等主要内容[10]。首先需要从知识场景或者数据驱动场景提取场景及参数，构建相应的测试场景库，然后按照场景代表性、覆盖度及测试成本确定测试任务，选择合适的验证方式，开展验证。测试形式包括虚拟仿真、硬件在环、整车在环和试验线测试等。

虚拟仿真由于测试成本低、可扩展性高、方便快捷等优势得到了广泛的应用。硬件在环测试通过将部分硬件接入测试环境可以提高相应功能的真实性，比如间隙传感器在环可用于对已知和未知的感知 SOTIF 触发条件测试。整车在环测试是指结合真实车辆和虚拟环境的测试，可用于评估软硬件功能不足等在整车层面造成的影响和危险，同时可以用于司机合理可预见误操作的测试。试验线测试进一步引入了真实环境，可设置更贴合实际的雨雪雾、特殊道路条件等环境条件，提高测试准

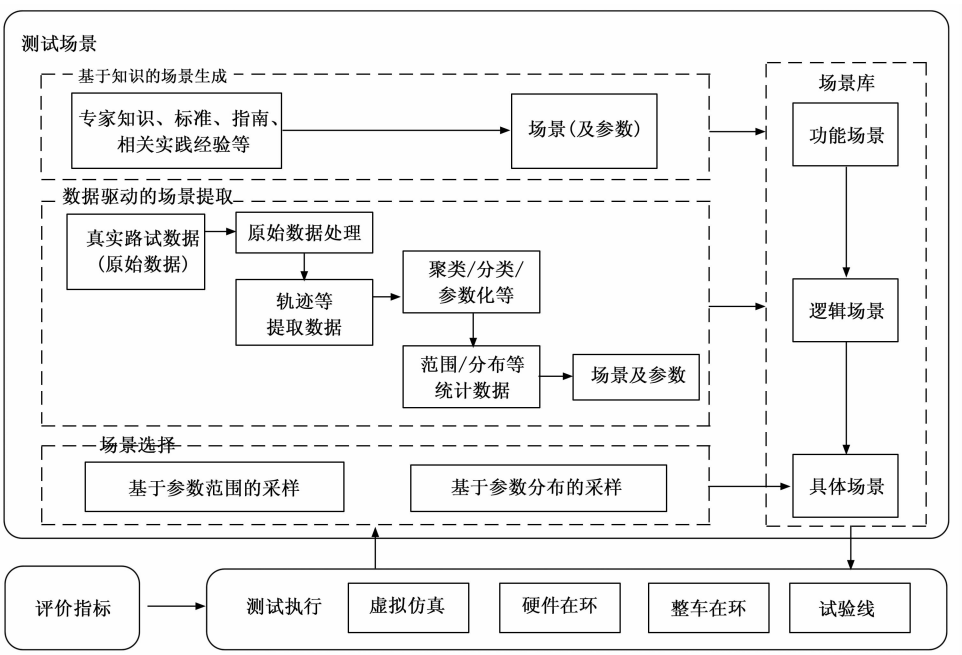

图 3 车载控制系统预期功能安全的验证评价架构[10]

确性，但也会造成测试灵活性的降低和时间、经济、安全风险等方面成本的上升。SOTIF 验证确认需要结合实际情况合理分配不同形式的测试任务，在能够满足安全要求的前提下，优先使用成本更低的仿真、硬件在环等测试方案。

2　预期功能安全验证评估系统设计

预期功能安全的验证评估不同于车载控制系统的功能测试。它不仅仅评估车载控制系统是否满足设计运行的要求，还深入探讨了其实际安全运行的边界。通过预期功能安全的验证评估，明确车载控制系统的安全操作范围，将现有系统中的潜在不安全区域转化为明确的安全区域。此外，通过开发更全面的预期功能安全场景和测试策略，可以有效地实现这一目标。

现有的测试系统通过对车载控制系统已知域的参数进行地面台架测试，测试合格的产品集成到车辆系统后，进行整车调测试时，已经发现了诸如通讯故障、系统耦合故障问题。地面台架测试可较为充分的考核逻辑方面的功能，但对于环境干扰和系统架构等因素所带来的预期功能安全问题，其验证手段就显得较为单薄了。如采取单车或者编组方式静态/动态测试，不仅成本高风险系数也大，因此本研究借鉴半实物仿真测试思想，开展车载控制系统安全验证评估系统方案设计。主要包括场景构建、场景测试用例和验证评估系统三部分。

2.1　预期功能安全场景构建

在交通运输范畴内，所谓的“场景”一般涵盖了道路条件、交通流动性以及其它相关的影响力。针对本项研究，车载控制系统的场景（包括测试场景和实际运行场景）主要涉及系统与其任务阶段、操作环境等关键要素在特定时间范围内的综合动态描述。这些要素的构成是由系统旨在实现的任务和具体功能所决定的[10]。

表 1　预期功能安全场景元素

场景类型	场景来源	场景元素
基于知识的场景	技术文件、标准	从技术文件和标准中获取与控制系统相关的车载电网控制单元、升压斩波器、制动控制单元、悬浮控制单元、导向控制单元、车门控制、230V 车载电网配电器、车载逆变器、车载运控系统、蓄电池等组成单元的阈值参数
	基础设施数据	道路结构、交通基础设施
	气象、环境数据	气象信息、光照信息、建筑物信息、电磁干扰
数据驱动的场景	上海磁浮示范线路试数据	包含道路结构、交通基础设施、气候环境、通信状态、自车状态等静态数据，以及轨迹和动作等动态数据

场景是仿真测试的关键要素，通过构建半实物试验室场景开展验证评估，能够有效避免现阶段线路测试数据匮乏、关键场景难以重复、极端危险场景无法复现等问题，在减少测试成本和危险性的同时，保证测试结果的可信度。高速轨道交通行业尚未建立如同智能网联汽车行业标准的预期功能安全场景库，本研究参照 ISO21448 和 ISO34501-34505，从基于知识的场景生成、数据驱动的场景提取和生成场景。

车载控制系统中出现的异常操作及其触发因素，能够被重新构想为与系统的任务阶段和运行环境等相关的一系列动态行为和关键事件，进而构建成车载控制系统的 SOTIF 测试场景。这些场景通常涉及到系统在非常规操作状态下的响应。主要包括如下。

1）接口数据异常情况：涉及外部接口数据的各种异常状况，通过引入特定的异常参数来模拟。例如，可以设定输入数据的值超出正常范围或者在一定时间内无变化等。

2）控制流程异常情况：在车载控制器执行控制任务过程中可能出现的异常，通过添加异常参数或进行环境模拟来构建。例如，可以设定控制规则在长时间内没有产生输出，或者输出结果超出预定范围等。

3）设备交互异常情况：控制器与外部设备交互过程中的异常，可以通过模拟设备状态或进行仿真来构建。例如，可以模拟外部控制器突然断电、执行机构无信号输出、局部网络中断或流量过载等情况。

4）冗余决策异常情况：冗余系统中的决策异常，可以通过模拟冗余系统或进行仿真来构建。例如，可以模拟主备系统切换异常、决策算法失效、特殊故障、冗余通道失效等情况。

5）状态转换异常场景：在冗余车载控制系统中，工作状态间的转换可能出现异常，可以通过添加异常数据或进行仿真来构建场景。例如，可以设定状态转换超时、主备冲突、备机失效导致冗余功能失效、状态同步失败、故障切换过程中的无响应时间等情况。

2.2　场景测试用例要求

在所构建的 SOTIF 测试场景基础上，建立异常控制行为、SOTIF 要求与用例输入，以及预期输出之间的关联，设计 SOTIF 测试用例[13]。

1）输入数据设定：依据系统异常控制行为的特征，确定接口数据的取值标准，挑选特定的数值或等效的数值类别，用作 SOTIF 测试案例的输入数据。

2）测试限制设定：依据系统异常控制行为的特征，选择相应的功能执行逻辑、操作环境或外部条件等因素，作为 SOTIF 测试案例的执行限制。

3）预期结果与验收标准：依据车载控制器的 SO-

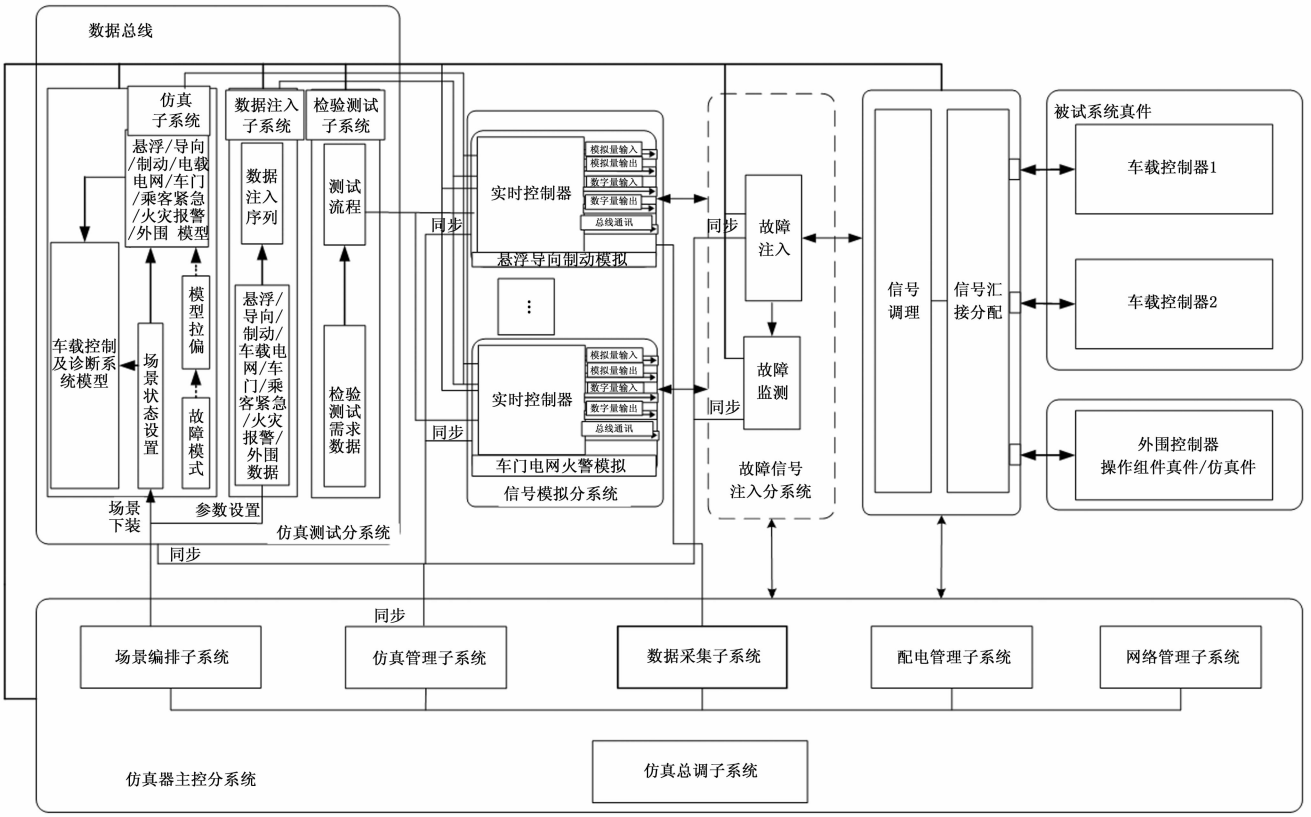

图 4 安全验证评估系统原理

TIF 规范和异常控制行为，明确测试案例的预期结果，即车载控制器的异常控制行为应被有效抑制或不发生。一般而言，测试案例的执行结果应与预期输出值完全匹配。然而，在风险等级较低的情况下，验收阈值可以适度放宽。

4) SOTIF 测试案例结构：根据外部接口控制文档，确定输入接口数据的通讯协议格式。结合接口通讯格式和相关数据取值，构建可执行的 SOTIF 测试案例。

2.3 验证评估系统设计

2.3.1 系统架构

验证评估系统通常由主控分系统、仿真测试分系统、信号模拟分系统、故障注入监测分系统、信号汇接分配系统与平台软件组成，系统软硬件协同工作，构成半实物验证评估环境。

仿真测试分系统通过实时数据接口与信号模拟分系统硬件进行关联映射，驱动相应的硬件设备进行信号模拟及仿真测试工作，产生的模拟信号经过信号汇接分配系统输出到被试系统硬件，模拟信号在通过信号汇接分配系统前可进行故障信号注入，同时通过对模拟信号进行实时监控，验证评估系统产生的所有数据信号，包括信号模拟系统产生的数据信号、故障注入系统数据信号等，通过主控分系统的数据采集子系统进行数据采集及监测。

场景编排子系统对整个验证评估系统数据信息进行统一管理；仿真管理子系统实现各种验证评估信息管理功能；配电管理子系统用于实现对各个分系统及被测对象的供电、断电、电压及电流状态监测；网络管理子系统主要用于各个系统计算机之间进行大量数据交互和存储。

2.3.2 工作模式

通过安全验证评估系统，车载控制系统可进行单系统集成、车载网络系统交联、全物理试验、虚实结合验证 4 种不同层次的系统验证评估。

仿真验证平台的两台真实控制器互为冗余备份，与安全无关的控制器真件/仿真件，通过车载网络系统接入系统；与安全相关的控制器真件/仿真件，通过硬线接入系统；当真件/仿真件不接入试验时，半物理仿真验证平台能通过仿真模型实现与车载网络、车载控制器的交互。

1) 单系统集成试验场景：

验证评估系统支持控制器硬件在环（HIL）的单系统集成试验，通过配置激励和采集资源，测试各系统控制部分的逻辑功能完备性，支持在线调参。信号汇接分配系统将外围控制器组件、车载网络切换至仿真（模

型）状态，将车载控制器切换至真件状态，开展车载控制系统接口及功能测试。

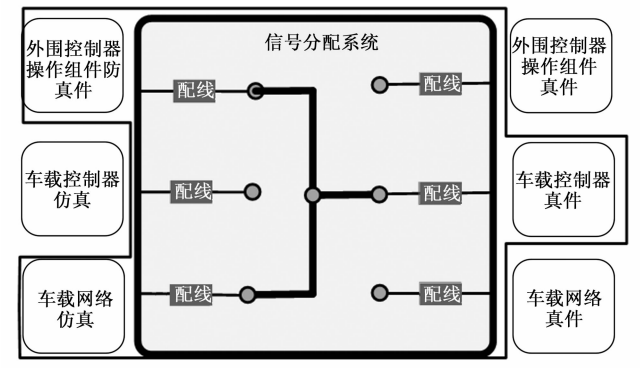

图 5　单系统集成试验场景

2）车载网络系统交联验证场景：

验证评估系统支持与车载网络系统开展交联试验，测试各系统与车载网络的接口正确性、数据一致性和逻辑完整性。信号汇接分配系统将外围控制器操作组件切换至仿真状态，将车载控制器和车载网络切换至真件状态，各验证平台通过车载网络互连在一起，开展多系统交联试验。

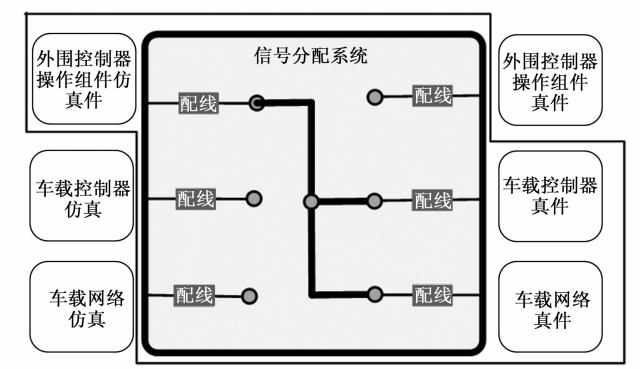

图 6　车载网络系统交联试验模式

3）全物理验证场景：

验证评估系统与车载控制器交联试验，测试各真件与车载控制器交互的功能正确性、响应实时性，测试各系统的带载能力，构建系统全物理试验。信号汇接分配系统将外围控制器操作组件、车载控制器和车载网络切换至真件状态，开展系统级测试。

开展全物理试验时，非安全组件真件通过车载实时以太网接入系统；与安全相关的组件真件通过硬线连接实现对车载控制器的信号激励。车载控制系统半物理仿真验证平台逻辑架构如图 7 所示。

4）“虚实结合”集成测试场景：

验证评估系统支持通过实时网络与数字样机环境进行交互，也支持基于高速实时网络的交互，利用其时间

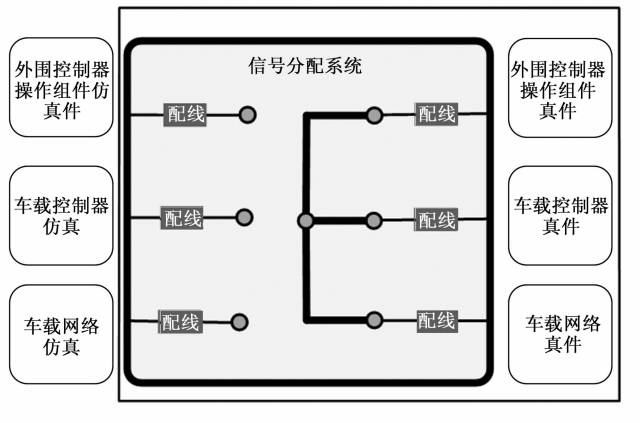

图 7　全物理试验模式

敏感特性，构建低延时、远距离通讯和数据传输环境，最后实现“虚实结合”的动态集成测试。基于信号汇接分配系统将车载控制器切换至真件状态，支持集成数字磁悬浮样车模型进行整车级动态运行试验验证。

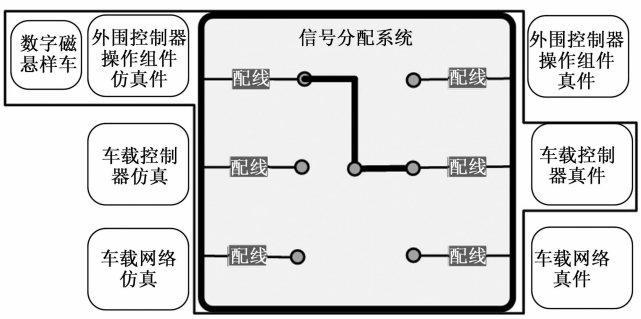

图 8　“虚实结合”集成测试场景

2.3.3　硬件功能设计

本研究以试验以太网（非实时）和高速实时通讯网（反射内存网络，实时）为基础，构建验证评估系统通用硬件架构。

主控分系统、仿真测试分系统、信号模拟分系统、故障注入监测分系统、信号汇接分配系统与平台软件协同工作，构成半实物验证评估环境。系统采用通用接口适配，实现平台的构型接入和被测对象的测试接入；在主控分系统的控制下，实现对被试对象的数据监测，实现基于模型、数据和测试流程的仿真测试功能；可针对硬线接口信号进行基于短路、开路等故障模式的故障注入。

1）仿真测试：

仿真测试系统主要由实时仿真服务器、实时仿真目标机及反射内存板卡等组成。实时仿真服务器与实时仿真目标机间通过实时以太网进行数据交互，实现仿真模型下载、仿真运行监控、数据采集等数据交互功能。

2）主控系统：

主控系统包含试验管理计算机、仿真测试上位机、数据采集系统、数据与模型管理计算机、磁盘阵列等组成。组成单元之间通过以太网进行数据交互，生成的所有数据存储于磁盘阵列。

3）信号模拟：

信号模拟系统主要由标准仪器板卡、信号调理板卡等组成。信号模拟板卡采用 PXI/PXIe 总线标准模块集成到目标仿真机中，主要资源包括 TRDP 总线接口模块、CAN 总线接口模块、数字量 IO 模块、模拟量输出模块、反射内存模块等[14]。

4）故障注入监测：

故障信号注入系统主要由故障注入器、故障注入监测设备等组成。故障注入器通过“串接”方式串入回路，实现“通、断、短”乃至“噪声、阻抗变换、延时”等故障，集成在数据采集系统中的故障注入监测设备实现故障注入状态的监测。

5）信号汇接分配：

信号汇接分配主要由通用接口、试验构型适配器、接口面板及线缆等组成。实现控制器信号、电源信号打断与引出，以便信号测试与故障诊断。通用接口为各分系统信号引出端；试验构型适配器为实现不同试验测试构型而设计，实现不同分系统之间的按需连接。

2.3.4 软件功能设计

半物理仿真平台软件包括实时仿真管理软件、数据与模型管理软件、数据采集判读软件、试验管理软件部署在各分系统计算机中，如图 10 所示。

2.3.4.1 实时仿真管理软件

实时仿真管理软件是整个软件的核心，实现模型仿真配置、数据注入仿真、检验测试配置、数据监视与数据回放等功能。

1）模型仿真配置：

导入全局配置系统接口数据，根据任务要求，形成全系统配置数据：通过仿真总线协议及其他设备专用控制协议，控制平台系统各功能节点的协同运行。

2）数据注入仿真：

通过数据注入仿真管理软件，对系统中涉及的所有设备接口及仿真模型接口进行统一、完整的描述。基于系统接口数据信息，用户进行后续的测试系统构型配置、仿真总线发布订阅关系配置，并支持运行时总线数

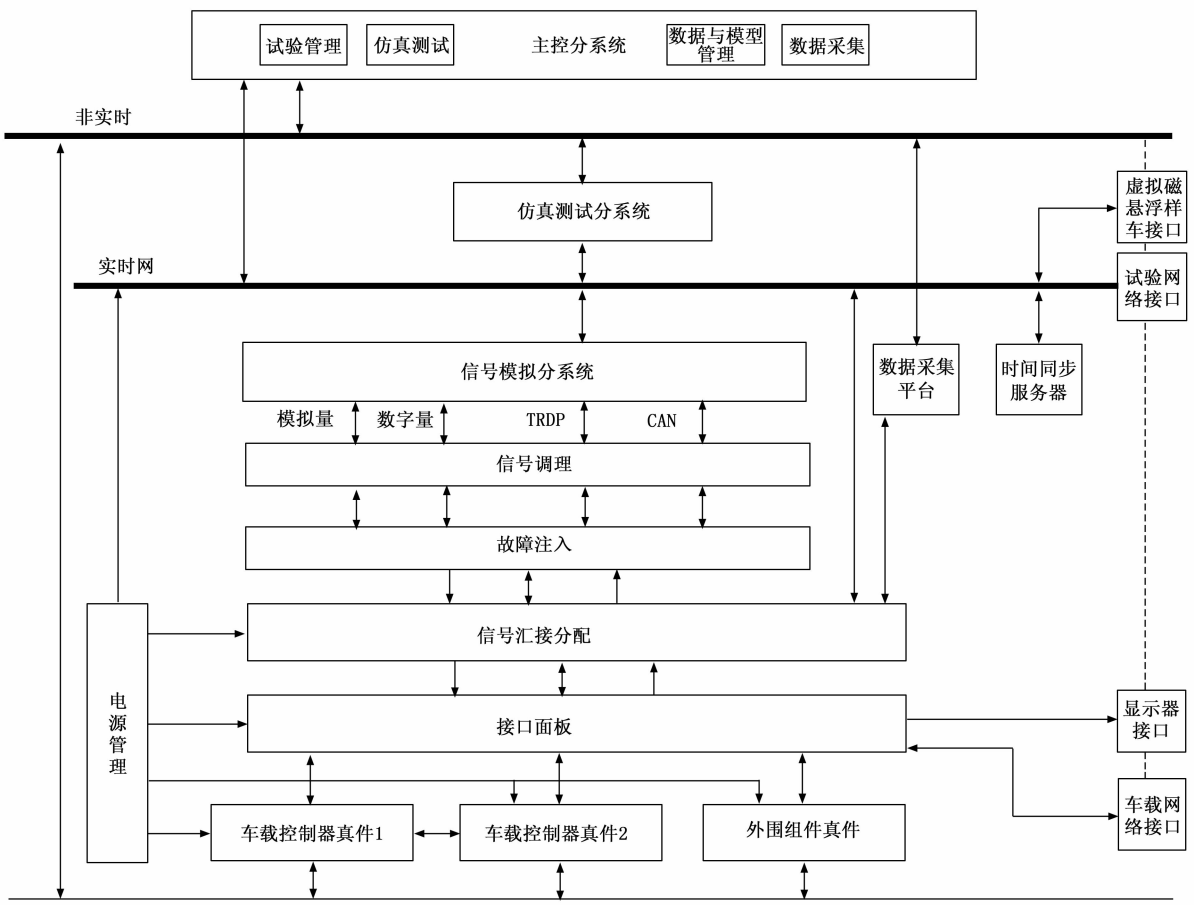

图 9 验证评估系统硬件拓扑

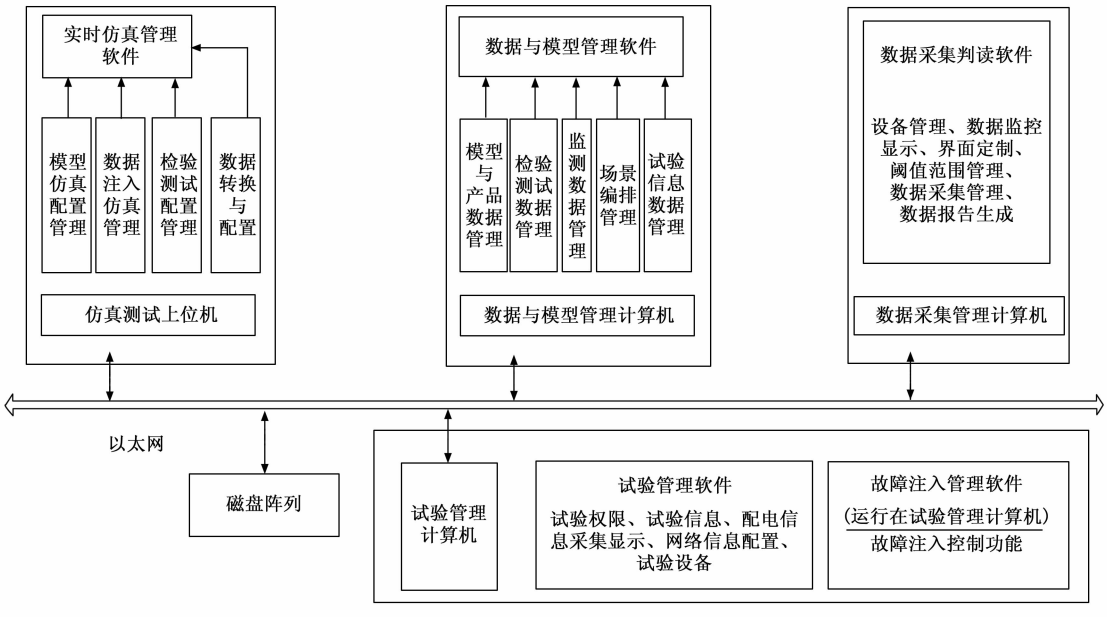

图 10　半物理仿真平台软件部署图

据的自动组帧、解帧。

3）检验测试配置：

检验测试配置管理软件与仿真总线紧密集成，完成测试管理系统和测试执行系统（测试引擎）功能。测试管理系统显示测试序列编辑、测试运行监控、测试数据分析与报告生成、测试序列转译。测试执行系统在后台通过运行 Python 解释器来执行测试脚本。

4）数据监视与数据回放：

反射内存作为全局数据空间，保存所有过程数据的当前值。反射内存数据监视软件对反射内存上定义的数据对象进行访问，并与协议关联，能够对原始帧当前值及历史值进行显示、解析，并支持工程量以表盘、曲线等形式进行图形化显示。反射内存监视软件基于仿真总线协议，根据仿真总线配置文件，对仿真总线传输层的数据进行在线图形化监视。

5）实时仿真软件包：

实时仿真软件包提供仿真模型实时运行环境和 I/O 硬件的 Simulink 封装模块，将 Simulink 模型自动生成目标代码并实现实时仿真全过程管理。

2.3.4.2　数据与模型管理软件

数据与模型管理软件提供统一的数据管理平台，实现对地面台架测试数据、单车/编组测试数据、路试测试数据以及模型数据的导入、导出及数据查询检索功能。

数据与模型管理软件构建注入数据数据库实现对车载控制器模型、设计与试验数据、路试数据的管理，配置数据库实现车载控制器特征数据管理及故障模式与拉偏数据管理，试验数据库实现对试验信息数据、监测数据、检验测试数据的管理。场景编排模块设置评估场景、场景内元素参数，并生成测试场景。数据与模型管理软件通过反射内存网络共享数据信息。

2.3.4.3　数据监测判读软件

数据监测判读软件是专门设计用于在试验过程中对数据进行实时监控、展示、分析、存储和管理的工具。主要功能包括如下。

1）数据采集：提供仪器设置、数据采集参数配置、监控配置以及参数阈值设定等功能。

2）实时监控与记录：能够对实验信号进行实时监控，实现数据的采集、保存、查看和回放。

3）数据展示：支持以波形图、数据列表和用户自定义格式等多种方式展示数据信号。

4）数据管理：具备数据上传、检索查询、回放功能，以及生成、导出和打印采集数据报告的能力。

2.3.4.4　故障注入软件

故障注入软件实现命令发送与数据采集、层次化故障注入执行和故障管理功能。命令发送与数据采集模块通过多种接口适配完成总线、数字信号、模拟信号等信号数据采集控制、数据传输和故障注入过程监测。层次化故障注入执行实体则根据故障类型，从协议层、电气层、物理层 3 个层次注入故障，层次化故障注入执行实体将底层采集的数据信息实时存储到数据库中供上层调用。故障管理模块主要完成系统故障模式集管理与故障信息数据分析处理。

2.3.4.5　信号实时监控软件

信号实时监控软件实现仿真对象输出接口的故障注

入信息监控与采集，在实时采集过程中需要实时显示信号波形或以数据表格的形式显示，具有实时查看采集数据并记录，并提供离线数据分析功能。

2.3.4.6 试验管理软件

试验管理软件可实现各种试验信息管理，包括试验权限、试验信息、配电信息采集显示、网络信息配置以及试验设备参数的管理与存储。

3 结束语

随着高速磁悬浮交通系统研究的不断深入和设计的多次迭代，系统发生随机失效和系统性失效产生硬件、软件故障的概率越来越小，因外部环境或人为因素产生的不安全事故却越来越多。通过车载控制系统预期功能安全验证评估系统研究，可为提升高速磁悬浮列车的安全提供重要的技术保障。

本文分析了车载控制系统工作原理，进行了预期功能安全场景构建和测试用例设计，并研究了基于半实物仿真的验证评估系统。通过该系统可以解决虚拟仿真暴露问题不充分，减少整车在环和试验线测试测试效率低、优化改进成本高和风险大的问题；避免现阶段线路测试数据匮乏、关键场景难以重复、极端危险场景无法复现等问题。在减少测试成本和危险性的同时，保证测试结果的可信度。

参考文献：

[1] 丁叁 叁，付善强，梁 鑫. 中国高速磁浮交通工程实践与展望 [J]. 前瞻科技，2023，2 (4)：40－48.

[2] 陈景龙，张明朗，崔华芳，等. 智能制动系统的预期功能安全分析及测试技术研究 [C] //中国汽车工程学会 (China Society of Automotive Engineers). 2023 中国汽车工程学会年会论文集 (1)，比亚迪汽车工业有限公司，2023.

[3] 吴思宇，于文浩，邢星宇，等. 基于关键场景的预期功能安全双闭环测试验证方法 [J]. 汽车工程，2023，45 (9)：1583－1607.

[4] 鄢 航. 基于特征场景预期功能安全分析的量化评估方法研究 [D]. 重庆：重庆大学，2021.

[5] 陈 浩. 智能汽车预期功能安全风险评估方法研究 [D]. 合肥工业大学，2023.

[6] ISO. ISO 34502 road vehicles—engineering framework and process of scenario-based safety evaluation [S]. 2018.

[7] 刘纪龙，吴冬华，苗 欣，等. 一种新型车载控制系统部件设计 [J]. 计算机测量与控制，2022，30 (8)：7－13.

[8] 丁叁叁，等. 时速 600 公里高速磁浮交通系统 [M]. 上海：上海科学出版社，2022.

[9] ISO. ISO/FDIS 21448 road vehicles—safety of the intended functionality [S]. Geneva，Switzerland：ISO：2022.

[10] 李 骏，王长君，程 洪. 智能网联汽车预期功能安全测试评价关键技术 [M]. 北京：机械工业出版社，2022.

[11] 邓自刚，刘宗鑫，李海涛，等. 磁悬浮列车发展现状与展望 [J]. 西南交通大学学报，2022，57 (3)：455－474.

[12] 熊嘉阳，邓自刚. 高速磁悬浮轨道交通研究进展 [J]. 交通运输工程学报，2021，21 (1)：177－198.

[13] 姜梦岑，温晓玲，李海峰. 面向机载软件的预期功能安全分析验证过程及方法研究 [J]. 测控技术，2024，43 (3)：61－69.

[14] 苗 欣，闫德顺，茜元臣，等. 高速悬浮列车车载控制器综合试验台研制 [J]. 计算机测量与控制，2020，28 (4)：257－260.

(上接第 286 页)

[13] SABITRI P，SANGMAN M. Taskassignment algorithms for unmanned aerial vehicle networks：A comprehensive survey [C] // Vehicular Communications，2022，ISSN：2214－2096

[14] 胡 木，李春涛. 无人机在线航路规划技术研究及其工程实现 [J]. 四川兵工学报，2010，31 (3)：14－17.

[15] 马骋乾，谢 伟，孙伟杰. 强化学习研究综述 [J]. 指挥控制与仿真，2018，40 (6)：68－72.

[16] MADHI N，SHIVA K，JAMAL D. Deen. Brain-Inspired Cognitive Decision Making for Nonlinear and Non-Gaussian Environments [J]. IEEE，2019：180910－180922.

[17] 陈新泉. 一种基于近似类抽样的组合聚类方法 [J]. 上饶师范学院学报，2008 (3)：71－75.

[18] VYACHESLAV P，FARIZA T，VLADIMIR A，et al. Evaluation of the iterative method of task distribution in a swarm of unmanned aerial vehicles in a clustered field of targets [J]. Journal of King Saud University-Computer and Information Sciences，2023，35 (3)：283－291.

[19] ZHANG D，WEI Q，CUI M，et al. Knowledge representation learning based on SoftMax [C] // Abstracts of 2019 IEEE International Conference on Computer Science and Educational Informatization (IEEE CSEI 2019)，IEEE，2019：1. 10. 26914.

[20] 李 琛，李茂军，杜佳佳. 一种强化学习行动策略 ε-greedy 的改进方法 [J]. 计算技术与自动化，2019，38 (2)：141－145.

[21] 周同乐，陈 谋，韩增亮，等. 基于改进狼群算法的多无人机协同多目标分配 [J]. 导航定位与授时，2022，9 (5)：46－55.