

动车组高安全等级列车网络控制技术研究

曾维康

株洲中车时代电气股份有限公司, 湖南 株洲 412001

DOI: 10.61369/TACS.2026050012

摘 要 : 随着铁路的快速发展, 动车组不断向数字化、智能化发展, 列车网络控制系统逐渐承担更加重要的角色, 采用安全性和可靠性更高的网络控制技术来提升网络控制系统的安全等级是当前发展的重要趋势。基于此, 本文结合网络通信标准, 对列车网络控制系统的安全隐患和风险进行分析识别, 研究不同网络拓扑的可靠性及安全性, 设计具备高安全性的核心网络设备实现技术方案, 提出应对网络通信常见危害的安全防御措施, 全方位满足列车网络控制系统的安全使用需求。

关 键 词 : 动车组; 高安全等级; 列车; 网络控制技术

Research on High-Safety-Level Train Network Control Technology for EMUs

Zeng Weikang

Zhuzhou CRRC Times Electric Co., Ltd., Zhuzhou, Hunan 412001

Abstract : With the rapid development of railways, EMUs (Electric Multiple Units) are constantly moving towards digitization and intelligence, and the train network control system has gradually assumed a more important role. Adopting network control technology with higher safety and reliability to improve the safety level of the network control system has become an important trend in current development. Based on this, combined with network communication standards, this paper analyzes and identifies potential safety hazards and risks of the train network control system, studies the reliability and safety of different network topologies, designs technical schemes for implementing core network equipment with high safety, and proposes safety defense measures to address common hazards in network communication, so as to fully meet the safe operation requirements of the train network control system.

Keywords : EMUs (Electric Multiple Units); high safety level; train; network control technology

一、动车组网络控制系统安全需求

(一) 功能安全需求

功能安全关注系统发生内部故障情况下仍能够被控制, 防止由于部件失效而造成危险情况发生。系统应当具有“故障导向安全”设计理念, 即当发现有异常或者故障时能够自动转到预先定义好的安全状态中去^[1]。系统结构上要防止单点故障导致整个系统瘫痪, 采用冗余方式使得主、备设备可以互相备份, 在一条线路或者一个单元出现问题时, 另外一条线路上的设备可以直接接手工作保证控制不间断。

(二) 信息安全需求

列车与调度中心、维护平台之间通信增多, 增加了被植入恶意代码、非法访问、信息泄露或者篡改的可能性, 因此需要有完善的安全保障措施, 在系统中配置网络流量检测模块, 对突然大规模的数据包、非法地址等进行监控并阻止其传播, 以免造成列车控制系统被破坏。

(三) 实时性与可靠性需求

牵引、制动、车门、空调等多个子系统的状态信息及命令都需要通过网络进行传递, 而这些控制回路的时间常数一般要在毫秒级

以下, 在速度较高的情况下, 即使是极短的时间也会造成较大的误差, 在列车上经常会遇到较强的电磁干扰、机械震动以及温湿度变化等因素的影响, 因此对于传输介质及接口电路的要求也较高, 需要使用屏蔽双绞线或者光纤进行传输, 用差分信号等方式提高信号质量, 保证整个控制系统能够在各种环境下正常工作^[3]。

二、动车组高安全等级列车网络控制系统的风险分析

(一) 核心设备风险

一方面, 输入输出模块用于获取来自传感器、按钮、继电器等现场设备的状态信号以及向执行器发出控制指令。如果该模块内部电路出现故障、信号采集通道受到干扰或者不能进行有效输出, 都可能导致一些重要状态信息丢失或者是控制命令不能下发。比如牵引使能信号不能正确输出会使列车意外停车, 而紧急制动反馈信号误报则会引发不必要的制动, 给行车带来安全隐患及影响。

另一方面, 网关负责不同子系统间协议转换以及数据转发, 使列车各个功能域相互配合工作。如果网关发生协议解析错误、数据包丢失或者路由规则问题, 则会破坏信息传递一致性及及时

性,造成子系统间“失声”^[4]。尤其是在影响到行车安全的重要通讯通道失效情况下,例如制动力分配器与主控单元之间通信中断,会降低整个列车控制能力。

(二) 系统通信风险

网络控制系统是动车组运行的重要中心环节,在动车组中起到连接牵引系统、制动系统、输入输出系统、烟火报警系统等各个重要子系统的桥梁作用。而网络控制系统的通信链路上的数据需要有较高的及时性和安全性,如果在这个通信链路上的数据发生时延、丢失、乱序或者被篡改等情况都可能会影响到列车的操作流程,造成严重的后果。

制动控制单元制动控制信息基于中央控制单元向制动控制单元发送制动控制信息,而这些信息数据包在网络中出现丢失或者延迟情况,会造成制动力不能够及时施加或者缓解,影响列车制动距离可控性。传动控制单元牵引施加以及封锁命令也对时延要求较高,通信问题会导致牵引力错误施加或者本应该被封锁而不被封锁,使列车速度过高或者在不允许牵引区域进行牵引操作,危及行车安全。

三、动车组高安全等级列车的网络控制技术分析

(一) 拓扑结构设计

在动车组内,为了提高整个系统的可用性和容错性,在网络拓扑设计上是非常重要的。根据 IEC61375 中 TCN 架构要求,把网络分成列车级以太网骨干网(ETB)以及车辆级以太网编组网(ECN)。ETB 用于编组之间的重要控制命令及状态等信息传递,而 ECN 用于一个编组内部各个子系统的通信。交换机是连接这两层的关键部件,可以实现不同协议间的转换以及数据传输,使信息可以在不同的层次上传输。

ETB 网络拓扑多为线性拓扑,物理链路上采用两路通信链路冗余结构,避免单路故障引起 ETBN 之间通信异常。ECN 网络拓扑,按照 IEC61375-3-4 中规定的拓扑结构,列车 ECN 网络拓扑主要有线形拓扑、环形拓扑和梯形拓扑结构。若采用单线形拓扑,任一车辆级交换机发生硬件故障或链路中断,都将导致整条支路通信失效,存在显著安全隐患,因此该结构不适用于高安全等级要求场景。为提高可用性,可采用双线形网络结构,如图 3-1 所示。通过布置两条独立但并行的通信路径,数据能够在主备通道之间切换。当某一节点出现异常时,相邻节点可通过备用线路维持通信,避免全车网络瘫痪。

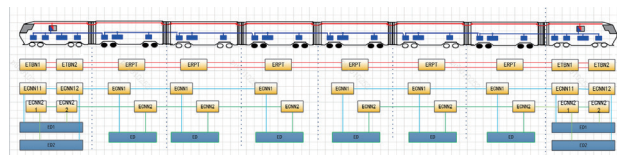


图 3-1 双线形网络拓扑

相比之下,环形网络具有更好的鲁棒性,在此情况下,每台交换机连接前后相邻两个结点并且构成闭环,如图 3-2 所示。正常工作状态下,信息以一种方向流动,若发生某条链路或者某个结点故障,则可以重新建立一条新的路由避开故障区域而使整个

网络仍然连通。

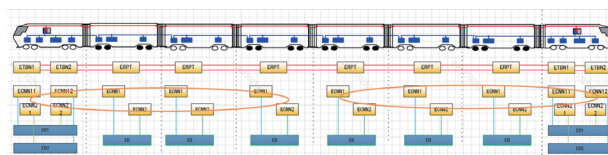


图 3-2 单环形网络拓扑

为了进一步提高安全性,在此基础上可以搭建双环网冗余结构,见图 3-3。两个环网同时运行并且互相作为备用,在一个环网完全不能使用时,另外一个环也可以单独支持整个系统的正常运行从而达到 SIL 的要求。因此,双环网加上智能路由算法可以在几毫秒内进行故障检测以及恢复操作保证在列车受到干扰的情况下还能保持正常工作。

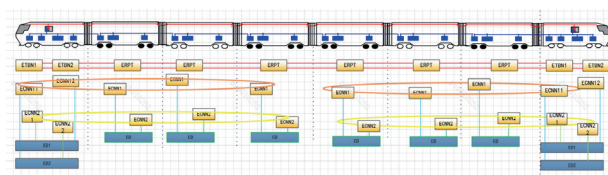


图 3-3 双环形网络拓扑

(二) 功能安全架构

安全输入输出架构是动车组高安全等级列车网络控制系统的重要部分,负责重要的信号采集以及控制输出工作。该架构具有完全独立的双冗余结构形式,两套硬件设备各自独立,当发生供电故障、通信故障、输出短路或者开路等常见问题时,可以做到平滑切换而不影响正常运行。

安全数字量输入输出板卡用于采集及驱动重要开关量信号,有完备回路自检功能。在输入端对来自车辆各个子系统状态信号定期读取,通过电气隔离以及滤波消除干扰避免误判。而在输出端使用高可靠度驱动电路,在发送指令的同时发送回来一个检查程序,把已出信号返回到主板上做比较。如果发现输出不符合要求或者反馈有问题时,马上切换到安全状态,断开相应回路并且保存错误日志。

依据《铁路应用通信、信号和处理系统用于信号的安全相关电子系统》(EN 50129),对基于完全独立的双冗余架构实现的安全输入输出模块,进行风险分析活动,识别出该系统主要安全功能为数字量信号采集功能和数字量信号输出功能^[9]。所有诊断动作以高频率循环执行,覆盖上电初始化、运行中监测与突发异常响应全过程,形成闭环安全管理,适用于对安全性与可用性双重严苛的高速列车控制场景。

(三) 信息安全防护

随着列车控制系统向数字化、智能化方向发展,网络互联程度不断提高,系统面临的外部攻击和内部数据泄露风险显著增加^[9]。

第一,车载网络使用专门通信协议例如 TRDP 通信具有一定的封闭性。对于这种类型的攻击,需要在接入层面部署身份认证以及访问控制的技术手段,所有的外设连接均需经过数字证书认证以及分权管理,保证仅有的被允许的设备可以接入到列车网络中去。

其次，在数据传输上，重要的控制命令及状态数据使用加密处理，避免数据被篡改，在列车网络系统中，在其边界部署有防火墙，根据预先设定的安全规则对恶意的数据包进行屏蔽，阻止其进一步扩散；而对于涉及到牵引、制动及信号等重要子系统的通信，使用 TRDP 安全协议可以实现动车组网络控制系统安全通信的目的，避免网络通信过程中经常出现的一些问题，是一种适用于基于以太网的列车网络通信控制系统的安全通信协议。

由此，整个信息安全架构从设备选型、系统集成到运维管理全过程实施安全生命周期管理，形成集预防、检测、响应于一体的信息安全闭环，全面提升动车组网络控制系统的抗攻击能力与

运行可靠性。

四、结束语

网络控制系统作为动车组的神经系统和指挥中枢，在列车不断向智能化、高安全性发展进程中，起着至关重要的作用。随着我国铁路的快速发展以及列车信息化、智能化程度越来越高，列车通信网络技术的应用将占据越来越重要的地位。高安全等级网络控制系统研究，可以为将来动车组的设计起到规范指导作用，从而使列车达到更安全、更可靠的要求。

参考文献

[1] 梁北辰, 赵红卫. 基于时间敏感网络的高速动车组网络拓扑仿真测试 [J]. 铁道机车车辆, 2024, 44(6): 41-50.

[2] 刘洋, 李帅, 李常贤. 基于区间预测的高速列车无线网络控制时延补偿方法 [J]. 铁道学报, 2025, 47(5): 77-88.

[3] 李辉. 基于量子密钥分发的智能列车通信安全体系研究 [J]. 智能物联技术, 2025, 57(3): 111-114.

[4] 党小刚, 宋伟, 赵薇. 基于车地协同的新一代动车组车载网络安全运维管理体系研究 [J]. 铁路计算机应用, 2025, 34(10): 74-79.

[5] 薛树坤, 赵婧, 尹光辉. 我国列车网络控制系统研究回顾与展望——基于知识图谱的可视化分析 [J]. 石家庄铁路职业技术学院学报, 2025, 24(4): 62-67.

[6] 马昊天. 机电一体化系统高速通信网络架构及数据同步技术研发 [J]. 中文科技期刊数据库 (引文版) 工程技术, 2025(8): 191-194.

[7] 张清妍, 李超. 智能通信技术在继电保护设备中的应用研究 [J]. 通信电源技术, 2025, 42(16): 62-64.

[8] 王国曦. 基于时间敏感网络的配电自动化系统通信架构研究 [J]. 通信电源技术, 2025, 42(20): 155-157.

[9] 敖璐磊. 通信网络拓扑变化对配电网差动保护稳定性的影响与应对策略 [J]. 通信电源技术, 2025, 42(23): 228-230.

[10] 肖磊, 郭洋洋, 李文波, 杨勇, 张陈林. 智能轨道快运系统功能安全研究 [J]. 控制与信息技术, 2020(1): 62-65.

[11] 白金磊, 王跃, 江帆, 等. 基于参数随机分布特性的多质点重载列车安全制动模型研究 [J]. 控制与信息技术, 2024, (04): 44-52.

[12] 金文斌, 张佳辉, 姚柏伶, 等. 基于事件触发预测控制的高速列车轨迹跟踪 [J]. 机车电传动, 2024, (04): 148-154.