铁路 CTC 系统安全风险识别与防控研究

李兆元
中国铁路乌鲁木齐局集团有限公司乌鲁木齐电务段，新疆 乌鲁木齐 830011

[摘要]调度集中系统是高速铁路运输调度指挥的中心设备，调度集中系统的运行安全直接影响行车秩序和旅客安全。文章从设备层、软件层、人员层和外部环境四个方面对 CTC 系统存在的安全风险进行了系统的识别，并且根据目前的技术状况，提出了智能监测预警、大数据风险分析、人工智能故障诊断和网络安全主动防御等关键技术的应用。高速铁路信号系统信息安全防护体系要以网络安全防护为基础，保证业务系统可靠、可用、可维护、安全。研究表明，必须创建起涵盖设备、软件、人员和环境的综合防控体系，从而达成对安全风险的主动识别并实施精准干预的目的，给我国铁路运输事业发展赋予技术支撑。

[关键词]CTC 系统；安全风险；风险识别；智能监测；主动防御
DOI：10.33142/sca.v9i7.20032　　中图分类号：U229　　文献标识码：A

Research on Safety Risk Identification and Prevention of Railway CTC System

LI Zhaoyuan
Urumqi Electric Power Depot of China Railway Urumqi Group Co., Ltd., Urumqi, Xinjiang, 830011, China

Abstract: The centralized dispatch system is the central equipment for high-speed railway transportation dispatch and command. The operation safety of the centralized dispatch system directly affects the order of train operation and the safety of passengers. The article systematically identifies the security risks of CTC system from four aspects: device layer, software layer, personnel layer, and external environment. Based on the current technological status, key technologies such as intelligent monitoring and early warning, big data risk analysis, artificial intelligence fault diagnosis, and active network security defense are proposed for application. The information security protection system of high-speed railway signal system should be based on network security protection, first ensuring the reliability, availability, maintainability, and security of the business system. Research has shown that it is necessary to establish a comprehensive prevention and control system that covers equipment, software, personnel, and environment, in order to actively identify safety risks and implement precise interventions, and to provide technical support for the development of China's railway transportation industry.

Keywords: CTC system; security risks; risk identification; intelligent monitoring; active defense

引言

调度集中系统是铁路调度指挥的重要技术装备，行车调度员在调度中心对辖区内的各个车站的信号设备进行集中控制和动态监视，并且统一调度列车运行。分散自律调度集中系统很好地考虑了我国铁路客货混跑、调车作业复杂的情况，实现了对列车和调车作业的统一控制。由于直接影响行车安全，CTC 系统必须实行独立组网、封闭运行，不能和其它网络直接相连。伴随着高速铁路网络的迅速发展，CTC 系统的规模不断增大，网络接口和接入节点的数量急剧增加，功能安全和信息安全相互交织叠加，给系统安全运行带来了很大的压力。目前 CTC 系统运维仍然以人工值守、日常巡检、周期维护为主，自动化、智能化水平低，不能满足智慧铁路建设的需求。因此，从设备层、软件层、人员层和外部环境四个方面对 CTC 系统安全风险进行系统分析，并提出相应的防控关键技术，有重要的理论意义和工程应用价值。

1 CTC 系统在铁路运输组织中的作用

CTC 系统在我国铁路运输组织中居于中枢地位，起到行车调度指挥、列车运行控制和运输信息管理的作用。行车调度指挥上，CTC 系统把调度中心对辖区各站信号设备集中控制和动态监视的能力发挥出来，调度员可以随时了解列车运行状况、线路占用情况和设备工作情况，根据实际情况随时改变运行计划。CTC 系统在列车运行控制上是以列车运行调整计划为基础，用自律模块来自动办

理列车、调车进路，从而完成从计划编制到进路执行的全过程自动化管理。FZh-CTC 系统总体功能可以分为以列车运行调整计划为基础的列车监督控制功能、以列车运行调整计划和调车作业单为基础的调车监督控制功能、综合维修管理功能和系统维护功能等几个部分。CTC 系统又是核心信息的来源，也是微机联锁、列控中心、无线闭塞中心、临时限速服务器、GSM-R 系统和运输调度管理系统相联系，从而形成一个从调度中心到车站再到机车的全过程信息闭环。

2 铁路 CTC 系统安全风险识别分析

2.1 设备层安全风险识别

设备层的安全风险是由硬件设备老化失灵、接口通讯出问题、电源供应不稳等造成的。CTC 系统中部署了大量的服务器、工作站、自律分机、路由器、交换机、协议转换器等重要设备，这些设备一直处在不间断的运行状态中，随着使用年限的增加，元器件的老化、性能的下降等问题越来越严重，很容易造成设备故障。路由器、交换机、终端设备（协议转换器）、网线等重要网络设备或部件都具有冗余配置，系统广域网结构采用冗余路由的方式，即传输通道冗余和拓扑结构冗余，但是故障大多出现在协议转换器和光接入设备之间。通过现场故障数据分析可知，协议转换器运行过程中突然出现内部性能下降的情况，是造成网络局部瘫痪的主要原因，部分站点通信机械室与信号机械室的地电位不同，引起通道可靠度降低，造成路由器串口输入、校验和帧等出错，严重影响通道稳定。另外，电源系统稳定性也属于设备层的风险点，供电中断或者电源波动都会造成系统重启、数据丢失或者设备损坏。

2.2 软件层安全风险识别

软件层的安全风险主要是由程序缺陷、数据异常、版本兼容性问题、系统漏洞等造成的。CTC 系统软件架构复杂，包括应用软件、数据库管理系统、操作系统、各种中间件等，任何一个层次的缺陷都会给系统的稳定运行造成很大的影响。程序缺陷会造成进路控制逻辑错误、调度命令执行失败或者系统死机等严重后果；数据库异常会造成运行图数据丢失、车次信息错乱，直接对调度指挥造成影响。软件测试是发现系统漏洞、保证系统长期稳定运行的重要手段，随着 CTC 系统向云架构演进，软件测试的关注点也变得越来越宽广和深入，因此有必要对它进行系统的探究[1]。另外，不同的软件模块之间存在兼容性问题，在系统升级或者功能拓展的时候，新的版本软件与旧的版本软件共存就会造成接口通讯出现异常、数据解析出错等问题。为了保证系统的稳定运行，在高铁信号系统建成后一般不会对操作系统版本进行频繁的升级和安全补丁的更新，杀毒软件的病毒库、入侵检测的特征库不能及时更新，使系统存在漏洞和病毒等威胁。

2.3 人员层安全风险识别

人员层的安全风险主要是调度员、运维人员在使用 CTC 系统时由于误操作、违章作业、应急处置不当等造成的。CTC 系统是调度员和行车指挥系统之间交互的主要界面，操作比较繁杂，在高峰时段和应急情况下调度人员的工作压力较大，容易造成操作失误。由于 CTC 系统存在作业过于复杂的问题，容易造成接发车错办，引发安全事故。调车侵路、转非常站控、转车站操作、强制执行、人工排路、删除序列、修改序列、人工触发、取消进路等非常规作业是风险高发环节，任何一个操作出现失误，都会造成系统报警混乱或者列车错办、进路冲突甚至安全事故。高速铁路调度员在安排调度任务时出现决策失误的情况越来越多，但是监控和下达指令的错误却越来越少，说明自动化可以减轻程序性负荷，但是也会带来新的问题，即“脱环不熟悉”。除了操作层面的风险之外，运维人员对系统出现异常状态时的识别和处理能力也被归入安全因素中。当系统发出报警信息的时候，运维人员能否准确地判断出报警含义，迅速找到问题所在并做出正确的处理措施，直接影响到故障的影响范围以及恢复时间，人员的经验不同、个体差异也使安全风险增大。

2.4 外部环境安全风险识别

外部环境安全风险有网络攻击、电磁干扰、极端天气、物理环境等对 CTC 系统运行造成的影响。随着铁路信息化水平的不断提高，CTC 系统同外部系统的数据交互越来越多，网络攻击的威胁面也越来越大。CTC 系统同 TSRS、RBC 之间采用单独组网的方式进行物理隔离，并且使用铁路信号安全通信协议来防止调度集中向信息安全控制网络渗透的问题。但是系统内部的维护端口、远程接入通道等仍然是攻击者入侵的突破口。GSM-R 使用无线公共信道，这就使铁路信号系统网络成为专网，从而给铁路信号系统网络的安全性带来了更大的威胁，也给铁路信号系统网络信息安全带来了新的挑战。电磁干扰属于另一个不可小视的外部风险源，无线通信频段拥挤、大功率设备电磁辐射都会造成 CTC 系统通信中断或者数据差错[2]。另外，雷电、暴风雨等恶劣天气也会直接破坏室外的设备、通信设施，造成系统大面积故障，尤其是一次雷击，它不但会造成监测设备的烧毁，还会使联锁机和 CTC 之间的光电隔离设备一起遭到破坏。外部环境风险的复杂性、不可预见性给 CTC 系统容错设计、防护能力提出了更高的要求。

表 1 CTC 系统外部环境安全风险分类及防护要点

风险类别	主要风险源	典型表现	防护要点
网络攻击	恶意入侵、病毒传播、近源攻击	非法登录、数据篡改、系统瘫痪	网络隔离、主动防御、入侵检测
电磁干扰	无线频段拥挤、设备辐射、信号衰减	通信中断、数据差错、控制失效	屏蔽接地、频率管理、冗余通信
极端天气	雷电、暴风雨、冰雪、高温	设备损坏、通信中断、供电异常	防雷接地、温控保护、容灾备份
物理环境	振动、温湿度、地电位差	设备松动、性能下降、接口异常	防振加固、环境监测、等电位连接

3 铁路 CTC 系统安全风险防控关键技术应用

3.1 智能监测预警技术应用

就设备层的安全风险而言，智能监测预警技术依靠在设备层设置各种感知终端以及边缘计算节点，从而达成对 CTC 系统设备运行状况的即时采集、剖析并发出警报的目的。以云边协同技术为依托，创建 CTC 智能运维架构，该架构把 CTC 云平台当作根基，按照铁路总公司-铁路局-车站的三级架构来进行设计与部署，并且会把云中心的部分功能下沉到靠近数据源的边缘侧，从而达成本地数据预处理和故障诊断的目的，在保证运维响应速度的同时，极大地削减了云中心的通信流量负担。对路由器、交换机、协议转换器等核心设备安装智能感知终端，对这些设备的运行参数实行 24h 在线监测，使用边缘计算完成本地的数据预处理以及异常检测。当监测到设备性能指标下降或者出现异常波动的时候，系统就会发出多级告警，并且用可视化的界面来呈现故障的位置以及影响的范围，给运维人员给予准确的故障定位指引。同时使用简单网络管理协议定时获取各类设备性能指标，实现全时段设备状态跟踪，很好地弥补了传统人工巡检的滞后性、盲区。

3.2 大数据风险分析技术应用

针对软件层安全风险，大数据风险分析技术通过整合 CTC 系统运行日志、报警记录、维护工单等多源异构数据，构建统一的数据中台，利用数据挖掘和统计分析手段实现风险的量化评估与趋势预测。目前铁路 CTC 系统要同时处理来自大量的轨道电路、信号机、列车等实时状态数据，数据吞吐量很大。基于改进博弈论和云模型的高速铁路 CTC 系统风险评估方法，首先使用 STPA 对 CTC 系统进行风险分析并构建风险评估指标，然后采用模糊层次分析法、模糊决策实验室法和熵权法分别计算主观权重、相对权重和客观权重，通过博弈论组合获得各指标的组合权重，利用云模型处理评估过程中的主观性和不确定性，实现 CTC 系统的有效风险评估[3]。从风险分析角度出发，从故障特征信息中提取风险指标，用机器学习算法进行权重计算，建立安全事件损失数学模型，得到客观的风险评估结果，为安全防护策略选择提供依据。

3.3 人工智能故障诊断技术应用

就人员层的安全风险而言，人工智能故障诊断技术依靠创建以知识图谱或者深度学习模型为基础的专家系统，从而达成对 CTC 系统故障的迅速识别、原因剖析以及处置提议的推送，进而缩减人工经验的个体局限性给故障处置带来的影响。为了解决调度集中系统故障诊断效率低的问题，根据系统故障日志文本提出了一种基于知识图谱的故障诊断方法，对系统故障日志文本进行预处理得到结构化元素，使用语义角色标注方法提取故障实体，构造实体关系模板，用模式匹配挖掘实体间的联系，采用依存句法特征相似度进行实体融合。当故障出现的时候，系统可以借助图谱快速找到故障节点以及传播途径，自动对应起历史故障案例里的处理办法，帮助运维人员作出正确的判断。信号智能运维系统利用知识图谱技术创建专家知识库，搭建起智能化算法模型调度、参数调整、监控以及管理为一体的模型管理平台，达成故障自动诊断和辅助处置建议的目的，改善了故障应急处置水平。该技术的使用可以降低对个人经验的依赖，加强故障处理的标准化程度和响应速度。

3.4 网络安全主动防御技术应用

就外部环境的安全风险而言，网络安全的主动防御技术由原来的被动防护转向了主动防御，创建起安全管理中心支撑的安全计算环境、安全区域边界以及安全通信网络这三个层面的防护体系，从而达成对整个网络的安全策略进行集中管控的目的。CTC 系统安全生产边界以主动防御为原则，用端口控制来创建安全防护体系，保证 CTC 系统不受侵害。在具体的实践过程中，从加强网络隔离措施、终端安全管理、密码策略升级、物理安全加强这四个角度提高系统的防护能力。在 CTC 查询终端和查询系统之间设置网络隔离设备，进行安全加固，统一下发主机防病毒策略，实现生产系统和查询系统有效隔离[4]。对于无线通信的安全威胁，采取分区域、纵深防御的安全防护策略，重点加强网管系统、接入终端、系统边界等各方面的安全防护能力。我国铁路信号系统信息安全防护已从小规模、简易防护、被动防护向系统防护、主动防护的过程发展，具备安全功能的 CTC 系统通过系统风险分析识别安全功能，在系统结构设计、软件安全防护、系统交互机制设计以及安全措施的综合运用下，使 CTC 系统安全功能达到 SIL2 安全等级要求。采用主动防御方式可以有效地防范非法登录、病毒传播等各种网络威胁，给 CTC 系统

长久稳定的运转提供有力的保证。

4 结语

CTC 系统属于铁路调度指挥的关键技术平台，它所处的安全状况直接影响行车安全以及运输效率。本文从设备层、软件层、人员层、外部环境四个方面对铁路 CTC 系统安全风险进行了系统的识别，分析了各个方面的主要风险点，分别论述了智能监测预警、大数据风险分析、人工智能故障诊断、网络安全主动防御等技术的应用。经过研究发现，CTC 系统安全风险具有多源化、交织化的特点，单个方面所采取的防护手段很难对抗复杂的威胁，必须建立起包含设备、软件、人员以及环境在内的全方位防控机制。随着云边协同、知识图谱、云模型等智能化技术不断深入的应用，CTC 系统安全风险防控将会由原来的被动应对转变为主动预防、由经验主导转变为数据驱动，从而给我国铁路运输事业高质量发展提供强有力的安全技术支撑。

[参考文献]

[1]王伟,曲范乾,廖玉仓.基于风险预警的铁路车务系统安全管理策略研究[J].价值工程,2026,45(15):52-54.

[2]高峰,白利洁,齐威,等.基于 CTC 系统的列车区间交会风险防控方法研究[J].铁道运输与经济,2026,48(2):80-87.

[3]李瑞峰,王建功.铁路信息系统安全的风险评估与管理分析[J].信息记录材料,2019,20(11):130-131.

[4]周益江.铁路工务系统安全风险与综合评价研究[J].设备管理与维修,2018,1(11):8-9.

作者简介：李兆元（1995—），毕业于兰州交通大学电子信息工程专业，研究方向为 CTC 系统网络安全和 CTC 网络架构优化。