DOI：10.13890/j.issn.1000-128X.2023.01.011　　文章编号：1000-128X(2023)01-0078-08

列车通信网络安全现状分析及应对方案研究

邹智荣，陈超群，陈　勃，唐　品
（中车株洲电力机车研究所有限公司，湖南 株洲　412001）

摘　要：随着以太网技术在列车网络控制系统中的深入应用，列车通信网络面临的安全挑战日益增加。文章结合列车网络控制系统的业务特点及网络架构，对列车通信网络中存在的各种网络安全隐患和风险进行了分析，同时参考GB/T 22239《信息安全技术 网络安全等级保护基本要求》和IEC 62443《工业过程测量、控制和自动化网络与系统信息安全》系列标准中的安全要求，研究了适合列车网络控制系统的网络安全防护方案，为后续列车通信网络安全体系建设提供指导。

关键词：列车通信网络；网络安全；安全风险；安全防护
中图分类号：TP393　　**文献标识码：**A

Current status analysis and countermeasure exploration for train communication network security

ZOU Zhirong, CHEN Chaoqun, CHEN Bo, TANG Pin

(CRRC Zhuzhou Institute Co., Ltd., Zhuzhou, Hunan 412001, China)

Abstract: With the in-depth application of Ethernet technology in the train networked control system, the train communication network is facing increasing cybersecurity challenges. Based on the analysis on various cybersecurity vulnerabilities and risks in the train communication network, considering the service characteristics and network architecture of the train networked control system, this paper explored a cybersecurity protection solution tailored to the train networked control system, referring to the security requirements specified in the *Information Security Technology-Baseline for Classified Protection of Cybersecurity* (GB/T 22239) and IEC 62443 series of standards for *industrial process measurement/control automatic network and system information security*, as a guidance for the subsequent security system construction over the train communication network.

Keywords: train communication network; cybersecurity; cybersecurity risk; cybersecurity protection

0　引言

近年来，全球网络安全攻击手段和规模不断升级，网络安全事件频发，如“震网”病毒事件、乌克兰电网遭攻击事件、勒索病毒Wannacry事件等影响巨大。国家陆续出台《中华人民共和国网络安全法》《信息安全技术网络安全等级保护基本要求》《信息安全技术网络安全等级保护测评要求》《信息安全技术网络安全等级保护安全设计技术要求》《关键信息基础设施安全保护条例》[1-3]等网络安全相关法律法规、政策及技术标准。国家对公共通信和信息服务、能源、交通、水利、公共服务等重要行业和领域的关键信息基础设施，在网络安全等级保护的基础上，实行重点保护[4-5]。同时，

通信作者：陈超群（1987—），女，硕士，工程师，主要从事轨道交通列车通信网络技术及网络安全关键技术研究与应用；
E-mail: chencq@csrzic.com

引用格式：邹智荣, 陈超群, 陈勃, 等.列车通信网络安全现状分析及应对方案研究[J]. 机车电传动, 2023(1): 78-85.
Citation: ZOU Zhirong, CHEN Chaoqun, CHEN Bo, et al. Current status analysis and countermeasure exploration for train communication network security[J]. Electric Drive for Locomotives, 2023(1): 78-85.

2020年到2035年我国城市轨道交通迈入城轨智慧化发展时期，自动驾驶、多网融合导致网络拓扑更加复杂，数据信息互联互通的要求更高，网络安全面临巨大挑战，一旦出现网络安全事故将会造成不可估量的损失[6]。国内外运营商也纷纷开始重视轨道交通网络安全的投入，明确提出网络安全能力建设的要求。在此之前，列车通信网络属于完全封闭的网络，已经开通运营的线路大部分没有考虑网络安全。

因此，为了提高列车通信网络系统的安全性，需要分析新形势下轨道交通列车通信网络系统面临的安全风险、威胁和隐患。本文结合国内外工业控制系统领域网络安全相关标准的要求以及轨道交通列车通信网络的特点，研究建立适合轨道交通列车通信网络安全防护的方案。

1　系统网络安全分析

列车通信网络是一种面向控制的数据通信系统，也是分布式列车网络控制系统的核心组成部分，在保障列车安全、可靠和高速运行中起到了至关重要的作用[7]。列车网络控制系统应用多种技术，将分布在全列车上的计算机应用系统或完成特定功能的智能设备互连起来，不仅有利于信息交换、资源共享，而且可以全面、实时、可靠地掌握与列车运行及状态相关的信息，实现分散监测、协同工作及安全运行，是保证列车运行安全的重要系统。列车通信网络就是在这一控制系统之上逐步发展起来的传输列车控制命令、故障诊断及显示信息的数据通信网络[8]，是列车的“中枢神经”。

1.1　系统架构

列车通信网络分为列车级和车辆级共2级网络架构，如图1所示。列车级网络即骨干网主要负责传输列车级的控制和状态信息，车辆级网络即编组网负责收集和传输车辆内各个设备的控制和状态信息[9]。列车网络控制系统与乘客信息系统（PIS系统）采用以太网连接，与地面系统通过无线通信交互数据。列车网络控制系统中既有用于监视设备运行状况的状态数据，又有用于控制列车运行的控制数据，有的列车中，状态数据会通过无线通道实时传输到地面。

1.2　风险分析

在CLC/TS 50701《铁路应用–网络安全》中提到对于铁路应用的风险分析，应该至少考虑到对人员健康和安全、业务可用性、经济性等方面的影响[10]。

从威胁源来分析，主要分为内部因素和外部因素，内部攻击主要包括内部人员误操作和有意破坏，外部攻击主要是指外部人员或组织对系统进行攻击，列车网络控制系统面临的威胁源如表1所示[10]。

表1　威胁源分类

Table 1　Classification of threat source

分类	威胁源
内部因素	操作人员
	维护人员
	工程师
	承包商和服务提供方
	供应商
外部因素	网络恐怖分子
	滋事团体
	前员工和承包商
	国家安全人员
	黑客
其他	具有报复心理的乘客，如携带受感染的设备接入、制造恐怖事件等

根据列车通信网络示意图，从攻击面来看，可以

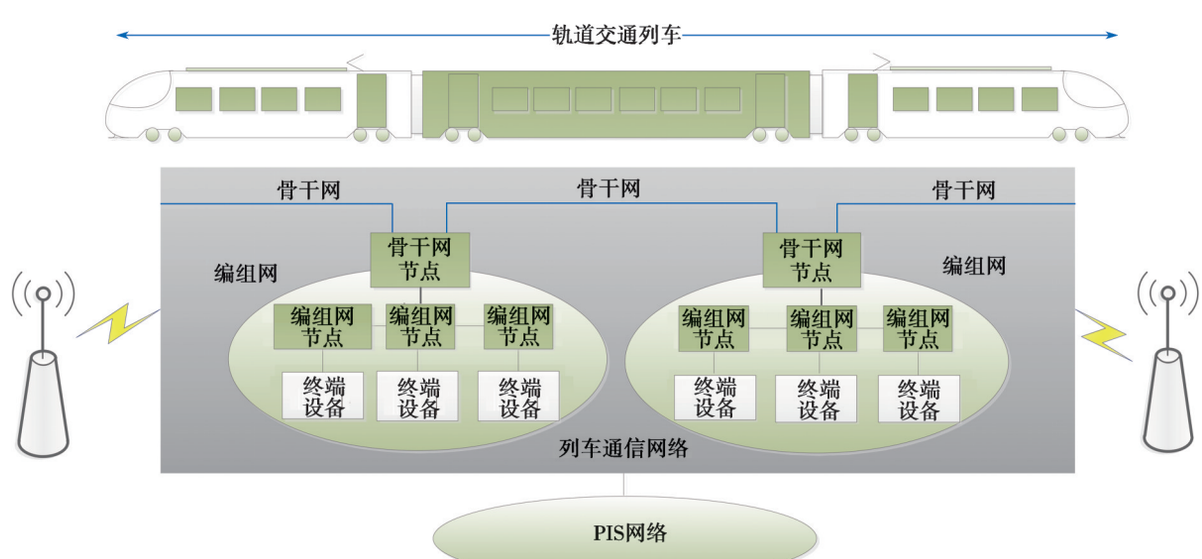

图1　列车通信网络示意图

Fig. 1　Schematic diagram of the train communication network

被威胁利用的攻击面主要来自车地无线通道（Wi-Fi、4G/5G）、车载设备物理接口（USB、以太网、调试口）、运维调试设备、乘客信息系统。

1）车地无线通道

列车网络控制系统通过车地无线通信通道，将文件及数据传输至地面，攻击者可通过破解无线密码，窃取数据，入侵系统控制设备。

2）乘客信息系统

列车网络控制系统与PIS系统通过以太网连接，攻击者可能通过PIS网络作为跳板攻击列车网络控制系统。

3）车载设备物理接口

系统中的网络设备和终端设备存在USB接口、以太网口及调试口等，外部可通过物理接口植入病毒、恶意代码进行攻击。

4）运维调试设备

可通过运维调试设备接入操作而带入病毒。

从攻击结果分析，可能造成的影响主要有：

① 非法获取控制设备的数据、程序，造成重要信息的泄漏；

② 修改或控制列车控制指令，造成列车网络控制的异常；

③ 通过DoS（Denial of Service，拒绝服务）攻击引起列车控制设备及网络故障，造成列车停运。

由此可见，列车通信网络风险主要来自外部的恶意攻击和内部的操作，包含边界风险、通信风险、设备本身的风险。

2 网络安全建设指导标准

目前，国内外都在积极推进网络安全的标准建设，其中系列国际标准IEC 62443《工业过程测量、控制和自动化网络与系统信息安全》和国家标准GB/T 22239—2019《信息安全技术 网络安全等级保护基本要求》均对工业控制系统作出了网络安全的要求。

网络安全等级保护制度是我国网络安全领域的基本制度，于2007年开始在全国范围内推进实施。从2019年开始，标准升级为等级保护制度标准2.0（以下简称等保2.0），包含GB/T 22240—2020《信息安全技术 网络安全等级保护定级指南》、GB/T 22239—2019《信息安全技术 网络安全等级保护基本要求》和GB/T 28448—2019《信息安全技术 网络安全等级保护测评要求》3个标准。该系列标准强调纵深防御的原则，以分区分域为基础划分等级进而开展防护体系建设，技术要求如图2所示。2017年6月1日实施的《中华人民共和国网络安全法》和2021年9月1日实施的《关键信息基础设施安全保护条例》明确了我国实行网络安全等级保护制度，对关键信息基础设施进行重点防护。轨道交通作为关键信息基础设施之一，其很多国内运营商已经陆续提出按照等保2.0进行网络安全合规性建设的要求。

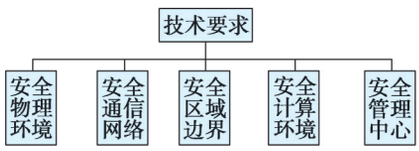

图2 等保2.0技术要求

Fig. 2 Technical requirements of classified protection system 2.0

IEC/TC65/WG10（工业过程测量、控制与自动化/网络与系统信息安全工作组）与国际自动化协会ISA 99成立联合工作组，共同制定了IEC 62443《工业过程测量、控制和自动化 网络与系统信息安全》系列标准[11]。2002年，国际自动化协会（ISA）制定了ISA-99标准，为工业自动化领域的企业网络安全威胁防范提供建议，当时，网络安全问题尚未成为热点话题。ISA标准发布后，网络安全开始受到越来越多的关注。为与使用频率更高的国际电工委员会（IEC）相关标准命名统一，ISA-99更名为IEC 62443。该系列标准对工业控制系统的安全策略与规程、系统安全要求、组件安全要求等进行了规范，涵盖了所有的利益相关方，即资产所有者（用户）、系统集成商、组件供应商[12]，受到世界各国工控安全专家们的广泛认可。目前，国外轨道交通行业对网络安全的需求基本都提到需满足IEC 62443标准要求。对于产品供应商，需重点考虑产品的安全开发过程标准IEC 62443-4-1和产品网络安全技术要求标准IEC 62443-4-2，从而将安全融入产品开发的每一个阶段，从设计之初考虑安全因素，将安全风险降低到最低[12-15]。

3 网络安全防护方案

通过对列车网络控制系统的系统架构和风险进行分析，同时参考等保2.0和IEC 62443系列标准中的技术要求，列车通信网络安全防护可从区域边界、通信网络、设备安全3个方面进行建设。区域边界防护如图3，车地无线传输系统如图4。

首先对列车通信网络进行区域划分，列车网络控制系统为安全域，即内网。与之相连接的PIS系统和车地无线系统为非安全域，即外网。内网与外网的分界处为该系统的边界。

3.1 区域边界防护

从列车通信网络示意图可知，列车通信网络边界主要包括列车网络控制系统与地面通信的边界、列车网络控制系统与PIS系统通信的边界。因此，采用了在车地无线系统边界处部署车载防火墙进行逻辑隔离，

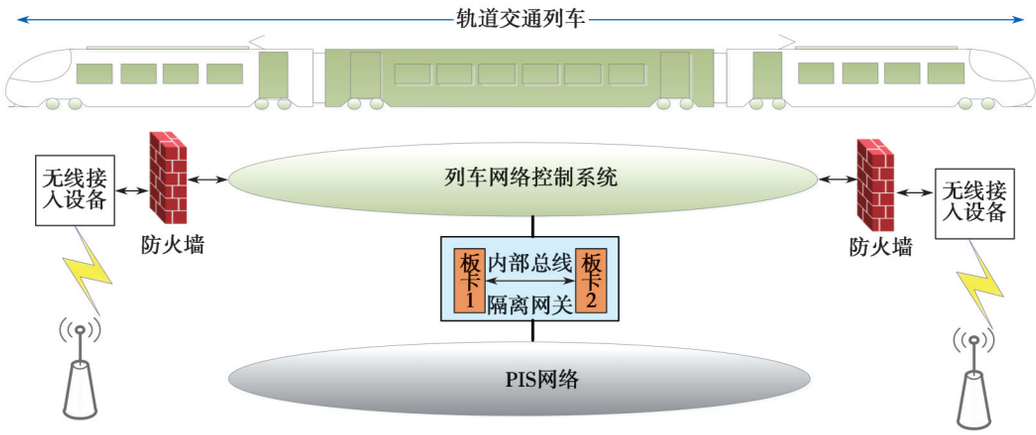

图3　区域边界防护示意图

Fig. 3　Schematic diagram of protection at area boundary

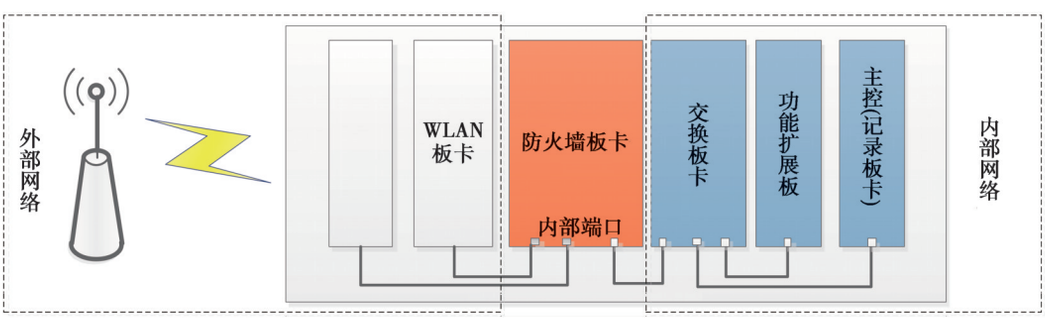

图4　车地无线传输系统

Fig. 4　Train-ground wireless transmission system

在列车网络控制系统与PIS系统边界处设置隔离网关进行物理隔离的区域边界防护方案。如图3所示。

车载防火墙采用板卡形式集成在无线传输系统机箱内，防火墙所有接口均支持旁路功能（bypass），从硬件设计上保证对列车网络控制系统的“零影响”。将背板以太网配置为安全域，前面板网口配置为非安全域，用于外接非安全域内的设备。利用防火墙深度包解析引擎和内容检测技术，结合访问控制白名单技术，对内部与外部连接系统执行访问控制规则，确保只有经过允许的数据流才能接入到系统中，如图4所示。

隔离网关由2块CPU板卡组成，通过总线进行通信，示意图如图5所示，可从通信传输物理层对外部攻击进行阻断，防止病毒入侵。

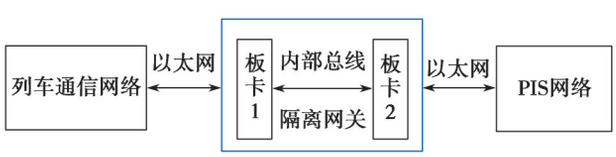

图5　隔离网关示意图

Fig. 5　Schematic diagram of the isolation gateway

3.2　通信网络防护

通信安全主要分网络系统内部通信安全和车地通信安全，需要考虑通信传输协议的安全性和数据的完整性。对于关键控制数据和车地数据采用加密传输，在数据接收使用的过程中进行合法性判断。同时采用通信链路的冗余、流量限制、异常流量监测等技术措施实现网络通信安全。

1）数据加密

对车地通信数据和重要的车载控制数据采用多因子对称加密算法进行传输。数据密钥由多因子组合后采用SM3散列算法动态生成（密钥生成算法不公开，通过软件库形式提供给各系统），通过不同因子的设置和组合管理来区别不同用户的加密密钥，这些因子包括初始密钥、时间因子、种类因子等，即采用SM4对称加密算法进行加密保证数据机密性；采用SM3散列算法生成校验码保证数据完整性。

2）通信及设备冗余

列车网络通信采用冗余方案，对于关键的子系统通过独立双以太网接口接入系统，实现通信链路的冗余备份。车辆级通信通过交换机组成环网，实现环网通信冗余，环网中任意1个节点故障均不影响环网通信。每列车配置2个中央控制单元（CCU），每个CCU配备2块主控板实现冗余切换，这样在板卡级和设备级均实现了热备冗余，任意一个CCU故障，均不影响列车运行。

3）流量限制

通过广播风暴抑制，可以限制交换机内允许传输的最大广播流量，多余的广播会被丢弃以减少广播对

终端设备的影响。根据交换机端口实际的数据流量，限制入口速率和出口速率，防止过高的通信率造成终端设备负荷过高。

4）安全审计

在2个头车部署安全审计系统，将其与网络交换机相连，通过镜像方式接收防火墙（外部接入）和CCU（内部核心设备）的网络流量。基于对列车通信网络控制协议的深度解析，实时监测网络内是否存在网络攻击、违规操作、非法设备接入以及蠕虫、病毒等恶意软件的传播；同时基于网络流量、协议和应用进行全方位的审计记录，以便发生安全事件后能够快速对事件进行分析溯源。

3.3 设备安全防护

由上面章节的分析可知，系统中的多数车载设备基本没有考虑网络安全的因素，因此参考等保2.0中的安全计算环境和IEC 62443-4-2中产品技术要求，可从以下几个方面进行改进。

1）身份鉴别

设备[FTP（文件传输协议）、Telnet（远程登录）、Web（全球广域网）、串口]的登录密码长度不少于8个字符，包含数字、大小写字母、特殊字符3种类型。

对设备进行远程管理时，采用传输信息加密方式，如SSH（安全外壳协议）、HTTPS（超文本安全传输协议）等。

当设备（FTP、Telnet、Web、串口）登录次数达到非法登录次数（5次）时，则主动结束当前会话、断开连接且锁定一段时间；当前登录会话超时，则主动结束当前会话并断开连接。

地面服务器、HMI（人机接口单元）关键设备和PTU（便携式维护工具）软件登录时采用口令、密码技术、生物技术等方法中2种或2种以上组合的鉴别技术对用户进行身份鉴别，且其中1种鉴别技术至少应使用密码技术来实现。若只采用口令技术，则密码复杂度需要满足不少于8个字符，且包含数字、大小写字母、特殊字符这3种类型信息。

2）访问控制

终端设备以太网通信应基于默认拒绝、例外允许的原则，仅开放必须的应用于软件工作的系统服务和网络端口。

关闭或拆除控制设备的USB接口、串行接口、多余网口等，确实需保留的接口通过管理手段实施严格的监控管理。

终端设备对接收到的数据包进行边界检查，丢弃接收到的超长包（大于1 518字节）和超短包（小于64字节），防止对后续正确数据包接收的影响和缓冲区溢出对未授权信息的访问。

对终端设备的访问必须通过PTU，访问控制权限通过PTU实现，仅启动相关用户的系统服务。PTU设置3种用户权限：系统管理员负责操作系统及底层软件的配置；应用管理员负责应用软件配置等操作；维护管理员负责终端设备上运行应用软件的日常操作。

3）安全审计

终端设备的审计内容包括安全事件（异常报文，非法任务，进程终止，端口异常开启，端口流量超限，无流量探测，网络攻击，广播风暴等）和操作记录（访问设备，更新程序，修改配置，下载程序等）。

审计记录应包括日期和时间、事件类型及相关描述信息；各设备采用统一审计记录格式，如Syslog格式；审计记录应定期进行备份，保存周期不少于6个月，记录存储满后按照先进先出的方式覆盖历史记录。

4）恶意代码防范

终端设备启动进程白名单控制，周期性地依据设备的白名单策略检查相关进程或任务，一旦检测到非法进程或任务则主动禁止运行，同时主动告警并记录详细信息。

5）数据完整性检查

配置、程序、日志、故障记录等文件增加校验机制，如CRC校验，MD5校验。在程序加载前进行完整性校验检查，在对配置、日志、故障记录等文件读取时进行校验结果检查。

PTU更新程序时需要进行完整性校验，采用密码技术对升级包及升级包相关信息（包括但不限于版本信息、发布时间、升级方式、发布者信息）进行数字签名，确保列车网络设备升级包的真实性、完整性。列车网络设备升级时，应对升级包的数字签名信息进行验证，校验升级包的完整性与真实性。校验失败时，应阻断升级流程，并记录相应日志。

6）数据备份与恢复

对关键配置文件和程序进行备份处理，一旦文件或程序被破坏可恢复到上一个正常状态。

7）数据保密性处理

对配置、日志、重要故障记录等文件采用国密算法进行加密处理，对这些文件读取时进行相应的解密操作。

4 方案验证

对列车网络控制系统的网络安全防护方案进行研究后，在实验室搭建了试验台模拟现场真实业务，并在系统中部署了安全防护相关技术和产品。所有车载设备均按照上述方案进行安全配置，拓扑示意图如图6所示。相关测试结果如表2所示。

为在该试验台上验证网络安全防护方案的可行性，

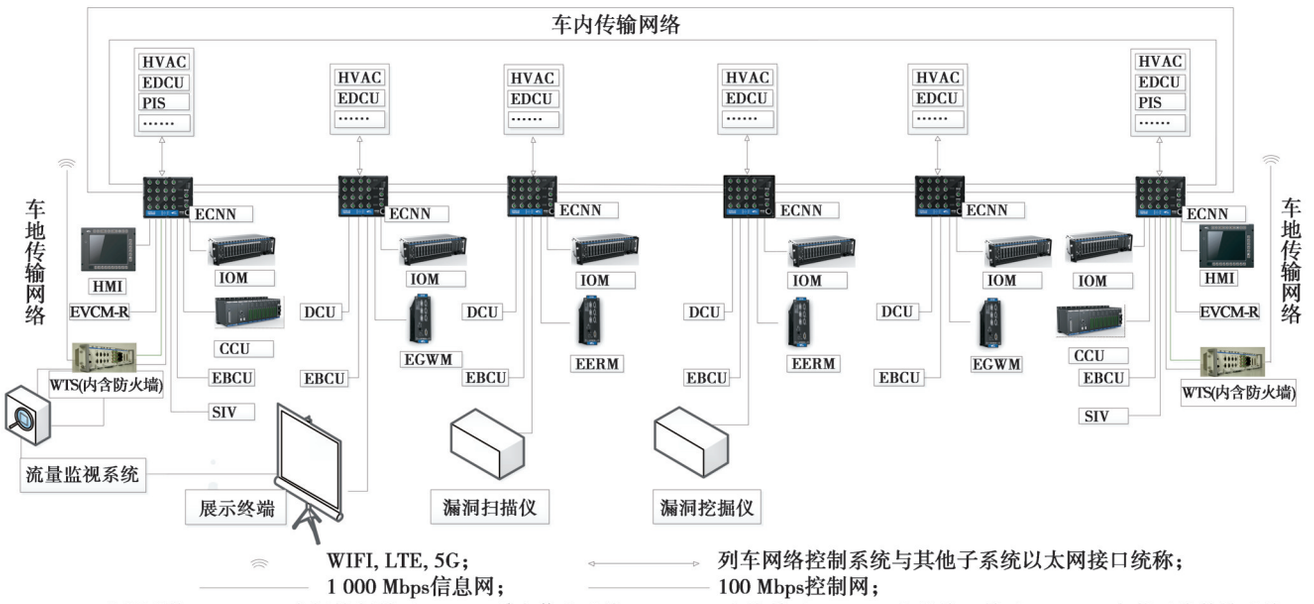

图6　列车网络控制系统拓扑示意图

Fig. 6　Topology of train network control system

表2　测试结果

Table 2　Test results

测试项	测试要求	测试结果
边界防护	核查指定受控端口是否进行跨越边界通信	边界处部署的车载防火墙在传统工业防火墙功能的基础上，考虑了适应列车网络控制系统应用场景，能够识别系统私有协议，并基于协议进行访问控制和安全过滤。结果符合GB/T 28448—2019要求
	核查是否防止非授权设备接入内部网络	
	核查是否防止内部用户非法外联	
	核查是否存在多余或无效的访问控制策略	
	核查设备的访问控制策略中是否设定了源地址、目的地址、源端口、目的端口和协议等相关配置参数	
	测试验证设备访问控制策略是否能够对进出网络的数据流实现基于应用协议和应用内容的访问控制	
	核查相关系统或组件是否能够检测网络攻击行为	符合GB/T 28448—2019要求，车载防火墙支持抗DoS攻击和端口扫描
恶意代码防范	核查是否安装了防恶意代码软件或相应功能的软件	采用软件进程白名单，当启动进程白名单之外的进程时，可以检测到该进程，并禁止进程运行，日志记录的详细信息包括进程名称、进程时间等符合GB/T 28448—2019要求
安全审计	核查是否开启了安全审计功能	在网络中分别进行以下典型操作，查看日志是否记录对应信息：① 正常运行的进程突然终止；② 端口通过的流量超过了设定值；③ 设备检测到来自外部的攻击报文；④ 设备被登录；⑤ 设备程序被更新；⑥ 设备配置被更新。当发生上述事件和行为时，日志均有详细记录。结果符合GB/T 28448—2019要求
	核查是否对重要的用户行为和重要安全事件进行审计	
	核查审计记录信息是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息	
身份鉴别	核查用户在登录时是否采用了身份鉴别措施	登录设备采用了用户名和密码的鉴别方式；通过用户名字典、密码字典、用户名密码组合字典进行扫描检测，均未发现设备存在弱口令；当登录次数超过5次，账户立刻锁定，10 min之内无法使用。结果符合GB/T 28448—2019要求
	核查用户鉴别信息是否具有复杂度	
	核查是否配置并启用了登录失败处理功能	
访问控制	核查是否为用户分配了账户和权限及相关设置情况	用户通过PTU对列车网络控制系统中的设备进行访问，系统管理员只能进行操作系统及底层软件的配置，应用管理员只能进行应用软件配置，维护管理员只能进行应用软件的日常操作，无法越权操作。结果符合GB/T 28448—2019要求
数据保密性	核查是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性	对配置、程序、日志、故障记录等文件进行读取，所有文件无法打开，需要进行解密操作。结果符合GB/T 28448—2019要求
通信传输	测试验证在通信过程中是否对数据进行加密	利用wireshark对车地通信数据进行抓包分析，所有数据都是密文，无法获取有效信息。结果符合GB/T 28448—2019要求

进行了安全测试，包括系统渗透测试和等保自评估。

试验时，列车网络控制系统通过WTS设备中的无线设备与地面进行通信，模拟常见黑客所使用的攻击手段对车地无线设备进行入侵，验证防护措施的有效性。

在未部署防护措施的情况下，使用攻击套件获取无线设备与地面的通信数据，进而伪造无线接入点，利用无线设备渗透进入了列车网络控制系统。攻击示意图如图7所示。

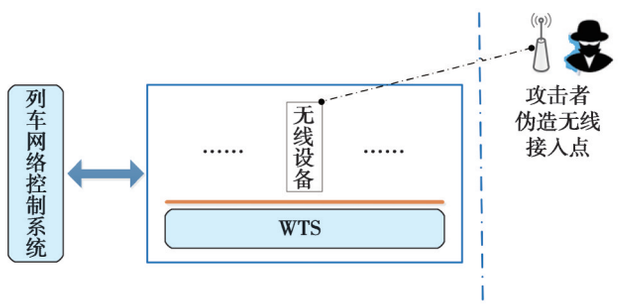

图7 车地无线攻击示意图

Fig. 7 Schematic diagram of vehicle-ground wireless attack

部署防火墙及安全策略之后，攻击套件渗透进入无线设备获取了最高权限，但是无法绕过防火墙，渗透内网失败。

根据GB/T 28448—2019《信息安全技术 网络安全等级保护测评要求》中安全通信网络、安全区域边界、安全计算环境等要求对列车网络控制系统进行测评，结果如表2所示。

从测试结果可以看出，本防护方案满足相关标准的规定，可有效地增强列车网络控制系统的安全性，适合应用于列车通信网络系统中，具有可行性。但安全是无边界的，随着攻击手段日益复杂化和以太网技术的多样化发展，需要定期开展安全测试，不断升级防护方案，及时发现和消除系统中的安全隐患。

5 结语

本文通过对列车通信网络存在的内外部安全风险进行分析，参考目前国内外权威信息安全标准建设要求，充分考虑列车通信网络的实际情况，重点从区域边界、通信网络、设备安全3个方面建立整体防护体系；遵循可执行性的原则，研究了纵深防御体系方案并开展了方案的验证；验证结果表明，本文的方案可最大化地发现安全问题和网络攻击，并及时做出响应。该方案实现了“主动检测、主动防护、主动响应”，可避免遭受重大损失，保障列车安全运行。但是，网络安全是动态的，安全威胁来源和攻击手段在不断变化，后续需要不断优化技术方案，同时加强安全管理，以适应新的网络安全要求。

参考文献：

[1] 全国信息安全标准化技术委员会(SAC/TC260). 信息安全技术 网络安全等级保护基本要求: GB/T 22239—2019[S]. 北京: 中国标准出版社, 2019.
National Information Security Standardization Technical Committee (SAC/TC260). Information security technology —Baseline for classified protection of cybersecurity: GB/T 22239—2019[S]. Beijing: Standards Press of China, 2019.

[2] 全国信息安全标准化技术委员会(SAC/TC260). 信息安全技术 网络安全等级保护测评要求: GB/T 28448—2019[S]. 北京: 中国标准出版社, 2019.
National Information Security Standardization Technical Committee (SAC/TC260). Information security technology —Evaluation requirement for classified protection of cybersecurity: GB/T 28448—2019[S]. Beijing: Standards Press of China, 2019.

[3] 全国信息安全标准化技术委员会(SAC/TC260). 信息安全技术 网络安全等级保护安全设计技术要求: GB/T 25070—2019[S]. 北京: 中国质检出版社, 2019.
National Information Security Standardization Technical Committee (SAC/TC260). Information security technology —Technical requirements of security design for classified protection of cybersecurity: GB/T 25070—2019[S]. Beijing: China Quality Inspection Press, 2019.

[4] 中华人民共和国网络安全法[EB/OL]. (2016-11-07)[2022-11-27]. http://www. npc. gov. cn/npc/c30834/201611/270b43e8b35e4f7ea98502b6f0e26f8a.shtml.
Network Security Law of the People's Republic of China [EB/OL]. (2016-11-07) [2022-11-27]. http://www. npc. gov. cn/npc/c30834/201611/270b43e8b35e4f7ea98502b6f0e26f8a.shtml.

[5] 中国共产党中央委员会办公厅, 中华人民共和国国务院办公厅. 国家信息化领导小组关于加强信息安全保障工作的意见 [EB/OL]. (2003-09-07) [2022-11-21]. https://www.zhuangpeitu.com/article/47756632.html.
General Office of the Central Committee of the CPC, General Office of the State Council of the People's Republic of China. Opinions of national informatization leading group on strengthening information security insurance work[EB/OL]. (2003-09-07) [2022-11-21]. https://www. zhuangpeitu. com/article/47756632.html.

[6] 中国城市轨道交通协会. 智慧城市轨道交通 信息技术架构及网络安全规范 第1部分: 总体需求: T/CAMET 11001.1—2019[S]. 北京: 中国铁道出版社有限公司, 2019.
China Association of Metros. Smart urban rail transit—Specification for information technical architecture and cybersecurity-Part1: General requirement: T/CAMET 11001.1—2019[S]. Beijing: China Railway Publishing House Co., Ltd., 2019.

[7] IEC/TC9. Electronic railway equipment - Train communication network (TCN) - Part 1: General architecture: IEC

61375-1: 2012[S]. Geneva: International Electrotechnical Commission, 2012.

[8] 李蕾. 列车通信网络拓扑结构及采用技术初探[J]. 铁道技术监督, 2009, 37(6): 42-45.
LI Lei. Discussion on the topological structure of train communication network and the technologies adopted[J]. Railway Quality Control, 2009, 37(6): 42-45.

[9] 邓箴, 谷萧君. 城市轨道交通网络系统中信息安全的评估方法研究[J]. 价值工程, 2016, 35(10): 229-231.
DENG Zhen, GU Xiaojun. Research on the evaluation method of information security for urban rail transportation network system[J]. Value Engineering, 2016, 35(10): 229-231.

[10] CLC/TC 9X. Railway applications - Cybersecurity: CLC/TS 50701: 2021[S]. Brussels: European Committee for Electrotechnical Standardization, 2021.

[11] 王建, 王天屹, 翟亚红, 等. IEC 62443 系统安全要求与等级保护基本要求对比研究[J]. 华电技术, 2021, 43(2): 72-76.
WANG Jian, WANG Tianyi, ZHAI Yahong, et al. Comparative study on IEC 62443 and the baseline for classified protection of cybersecurity[J]. Huadian Technology, 2021, 43(2): 72-76.

[12] IEC/TC65. Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models: IEC TS 62443-1-1: 2009[S]. Geneva: International Electrotechnical Commission, 2009.

[13] IEC/TC65. Industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems: IEC/TR 62443-3-1: 2009[S]. Geneva: International Electrotechnical Commission, 2009.

[14] IEC/TC65. Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements: IEC 62443-4-1: 2018[S]. Geneva: International Electrotechnical Commission, 2018.

[15] IEC/TC65. Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components: IEC 62443-4-2: 2019[S]. Geneva: International Electrotechnical Commission, 2019.

收稿日期：2022-04-08
修回日期：2022-12-08