ICS 45.120
CCS S70

团 体 标 准

T/CITSA 44-2024

轨道交通车辆
以太网控制网络安全审计产品技术要求

Rail transit vehicle — Technical requirements for security audit product for Ethernet control network

2024-10-16 发布　　2024-11-30 实施

中国智能交通协会　发 布

目　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中车南京浦镇车辆有限公司提出。

本文件由中国智能交通协会归口。

本文件起草单位：中车南京浦镇车辆有限公司、中车株洲电力机车有限公司、中车青岛四方机车车辆股份有限公司、中车大连机车车辆有限公司、中车大连电力牵引研发中心有限公司、公安部第三研究所、杭州中电安科有限公司、北京威努特技术有限公司。

本文件主要起草人：张军贤、张潜、林业、王乐、涂本荣、黄众、崔玉龙、张朋、王建强、邹春明、苗维杰、姜晓波。

轨道交通车辆
以太网控制网络安全审计产品技术要求

1 范围

本文件规定了城市轨道交通车辆以太网控制网络安全审计产品的运用条件、安全技术要求和检验要求等。

本文件适用于城市轨道交通车辆，其它轨道交通车辆可参照执行。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 20945—2023 信息安全技术 信息系统安全审计产品技术规范

GB/T 21563 轨道交通 机车车辆设备 冲击和振动试验

GB/T 25069 信息安全技术 术语

GB/T 25119—2021 轨道交通 机车车辆电子装置

GB/T 28029.4 轨道交通电子设备 列车通信网络（TCN） 第2-3部分：TCN 通信规约

GB/T 32347.1 轨道交通 设备环境条件 第1部分：机车车辆设备

GB/T 37941 信息安全技术 工业控制系统网络审计产品安全技术要求

3 术语和定义

GB/T 20945—2023和GB/T 25069—2022界定的及下列术语和定义适用于本文件。

3.1

安全审计 security audit

对网络、信息系统及其组件的记录与活动的独立评审和考察，以测试系统控制的充分程度，确保对于既定安全策略和运行规程的符合性，发现安全违规，并在控制、安全策略和过程三方面提出改进建议。

[来源：GB/T 20945—2023, 3.4]

3.2

车辆以太网控制网络 vehicle Ethernet control network

基于以太网构建的轨道交通车辆控制网络，实现列车控制、诊断、显示告警及存储分析等功能。

3.3

车辆以太网控制网络通信协议 vehicle Ethernet control network communication protocol

应用于轨道交通车辆以太网控制网络中各控制器设备之间的网络通信报文规约。

3.4

车辆以太网控制网络安全审计产品 vehicle Ethernet control network security audit products

部署于车载以太网控制网络中，对网络流量进行采集、记录和分析，并针对特定事件采取相应匹配动作的产品。

4 缩略语

下列缩略语适用于本文件。

CPU：中央处理器（Central Processing Unit）

FTP：文件传输协议（File Transfer Protocol）

HTTP：超文本传输协议（Hyper Text Transfer Protocol）

IP：网际互联协议（Internet Protocol）
MAC：媒体接入控制（Media Access Service）
MDI：与介质有关的接口（Medium Dependent Interface）
SDTv2：安全数据传输v2版本（Safe Data Transmission version 2）
SNMP：简单网络管理协议（Simple Network Management Protocol）
TCMS：列车控制和管理系统（Train Control and Management System）
TRDP：列车实时数据协议（Train Real-time Data Protocol）
VCU：车辆控制单元（Vehicle Control Unit）
URI：统一资源标识符（Uniform Resource Identifier)
URL：统一资源定位符（Uniform Resource Locator)

5 产品描述

车辆以太网控制网络安全审计产品是应用于轨道交通车辆车载以太网控制网络中，通过对网络通信流量采集、分析，监测车辆以太网控制网络中的非法活动或行为，并提供报警，对车辆以太网控制网络流量完成审计功能的产品。

设备可以是一体化硬件设备，也可以是分体式硬件设备，采用旁路方式接入到轨道交通车辆车载以太网控制网络中。

设备应满足轨道交通车辆环境和安全功能的特定要求。

车辆以太网控制网络安全审计产品应用场景见附录A。

6 运用条件

6.1 设备安装在车体内。

6.2 设备的高低温、交变湿热、电源过电压、电磁兼容、绝缘、低温存放等性能应满足 GB/T 25119 的要求，见本文件 8.1。

6.3 设备的冲击和振动应满足 GB/T 21563 中 1 类 B 级的要求。

6.4 环境温度范围：-25℃～+45℃，允许在不低于-40℃的环境下存放。

6.5 因各城市所处地区不同而存在气候条件的差异，超出以上规定条件时，由供需双方按 GB/T 32347.1 的规定值协商确定。

6.6 产品应满足国家网络安全专用产品的监管要求，由具备资格的机构安全认证合格或者安全检验符合要求，具有安全认证证书或者安全检测证书。

6.7 设备装车运用前应通过车载产品相关设备型式检验并取得报告。

7 技术要求

7.1 审计功能要求

7.1.1 审计数据采集

7.1.1.1 产品应支持基于策略的数据采集，包括：

a) 支持基于网络层要素的数据采集策略：至少包括源/目的 MAC 或源/目的 IP、传输层协议、目的端口；
b) 支持基于列车以太网控制网络传输协议的数据采集策略；
c) 支持全流量报文的采集。

7.1.1.2 产品应能根据源/目的 MAC 或 IP 地址、协议类型、日期时间段等对流量进行监测审计。

7.1.1.3 产品应能够在实际的系统环境和网络带宽下及时生成审计数据，并支持以统计报表的形式输出。

7.1.1.4 对数据的实时采集监测不应影响车辆以太网控制网络正常运行。

7.1.2 审计数据还原

7.1.2.1 产品应支持对网络层通信协议的数据进行还原，至少包括源/目的 MAC、源/目的 IP、传输层协议、源/目的端口、应用层协议类型、日期和时间。

7.1.2.2 产品应支持对 HTTP、FTP、Telnet、SNMP 等网络通用协议应用数据的解析、分析和还原。至少包含但不限于：

a) HTTP 通信：目标 URL；
b) FTP 通信：使用的账号、输入命令；
c) Telnet 通信：使用的账号、输入命令；
d) SNMP 通信：使用的账号、输入命令。

7.1.2.3 产品应支持对 Modbus-TCP 等通用协议应用数据进行解析、分析和还原。至少包含但不限于：

a) 组态变更，包括上传、下载；
b) 指令变更，包括写指令及相关参数，如控制点位地址、控制值等；
c) 负载变更。

7.1.2.4 产品应能够对车辆以太网控制网络专用 TRDP 及 TRDP SDTv2 安全传输协议数据的解析、分析和还原。协议应符合 GB/T 28029.4。至少包含但不限于：

a) 通信标识符，源和目的 URI；
b) 数据集标识符、数据集标志、数据集大小；
c) 操作码及相关参数，如数据地址、数据值等。

7.1.3 审计事件识别和分析

7.1.3.1 产品应支持基于白名单规则分析和对审计信息的识别。

7.1.3.2 产品应支持白名单规则的定义，包括：

a) 网络通信白名单：支持基于源/目的 MAC 或源/目的 IP、传输层协议、目的端口等要素进行规则定义；
b) 车载以太网控制网络协议通信白名单：支持基于协议格式规约、控制命令、控制点位、控制阈值等要素进行规则定义。

7.1.3.3 产品应支持学习模式，对网络流量进行自学习，建立车辆通信模型基线，且能够自动生成推荐性规则，至少包括网络层规则和车载以太网控制网络协议应用层规则。

7.1.3.4 产品应支持对以下异常事件的识别：

a) 通信异常：不合规的通信链路，包括源 IP、源 MAC、源端口、目的 IP、目的 MAC、目的端口等；
b) 车辆以太网控制网络通信协议出现异常的控制命令、控制点位、控制值；
c) 不符合协议规约规定格式的车载以太网控制网络协议报文；
d) 端口报文异常：端口报文速率突变、超过阈值、长时间无报文；
e) 车辆以太网控制网络通信协议应用层通信中断及中断后的恢复等。

7.1.3.5 产品应支持基于统计方式对审计事件进行分析，同时支持事件的关联分析。

7.1.3.6 对异常事件，产品应支持全报文审计，以利于事后分析。

7.1.4 事件报警

7.1.4.1 事件告警：产品应具备对车辆通信行为与基线进行对比分析告警的能力，并根据系统安全策略定义将事件进行分级及告警。

7.1.4.2 产品宜支持将告警信息发送到 TCMS 系统主机，也宜支持通过车地无线通道实时发送告警信息到地面监控系统。

7.1.4.3 告警过滤：产品应允许管理员定义安全告警过滤策略。

7.1.4.4 事件合并：产品应能对高频度发生的相同安全事件进行合并告警。

7.1.5 审计记录与报表

7.1.5.1 产品应具备审计记录功能。

7.1.5.2 产品应按照事件的分类和级别，生成包含事件主体、客体、发生的日期和时间、类型、级别、审计源身份、事件的描述、车载控制协议的深度解析内容（包括控制命令、控制点位、控制阈值等）的审计记录。
7.1.5.3 产品应提供查阅审计记录的工具，查阅的结果应以用户易于理解的方式和格式提供，并且能支持以文本或表格等通用文件格式导出。
7.1.5.4 产品应确保除授权人员之外，其他用户无权对审计记录进行查阅。
7.1.5.5 审计记录应能按一定的条件进行选择、搜索、分类和排序，生成自定义审计报表，并应以文本或表格等通用文件格式生成报告及导出。
7.1.5.6 报表支持周报及月报统计。
7.1.5.7 产品应支持以标准格式将审计数据外发至其他系统，以作进一步的分析处理。
7.1.5.8 产品应提供安全机制保护审计记录数据免遭未经授权的删除或修改，任何对审计记录数据的删除或修改都应生成系统自身安全审计记录，应对审计记录进行完整性保护。

7.1.6 安全配置

7.1.6.1 产品应提供安全策略配置功能，应支持安全策略的导入和导出。
7.1.6.2 产品应能对现有车辆应用层协议端口进行重新设定。
7.1.6.3 产品应允许管理员对攻击事件进行自定义，自定义的内容应包括攻击目标、攻击特征和事件等级。
7.1.6.4 产品应支持添加新的车辆以太网控制网络协议。

7.2 管理要求

7.2.1 设备管理

7.2.1.1 产品应具有分布式部署及自管理或集中管理功能。设备上电自启动到正常工作时间不超过60s。
7.2.1.2 产品应提供友好的管理员界面用于管理和配置，管理配置界面应包含配置和管理产品所需的所有功能。
7.2.1.3 业务接口和管理接口应采用不同的网络接口。
7.2.1.4 产品应能对远程管理本系统的主机地址进行身份鉴别和访问控制，支持配置访问控制策略；应采用校验技术或密码技术保证传输数据的保密性和完整性；应采取必要措施防止鉴别信息在网络传输过程中被窃听。
7.2.1.5 产品应支持遵循最小安装的原则，仅安装需要的组件和应用程序。
7.2.1.6 产品应关闭不需要的系统服务、默认共享和高危端口，宜伪装需要的系统服务端口。
7.2.1.7 产品应能够发现可能存在的已知漏洞，并及时修补漏洞，在交付前提供漏洞扫描报告。
7.2.1.8 产品应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。审计记录应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。
7.2.1.9 产品应对审计进程进行保护，防止未经授权的中断。
7.2.1.10 产品应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。
7.2.1.11 产品应支持通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制。
7.2.1.12 产品应具有通过本地和远程进行产品升级的功能。
7.2.1.13 产品应具有通过自管理接口或管理平台进行升级的功能。
7.2.1.14 产品应具有升级包校验功能，防止得到错误或伪造的升级包，升级过程应进行双向身份鉴定。

7.2.2 用户管理

7.2.2.1 产品应支持用户管理，包括添加、激活、禁止、删除用户。
7.2.2.2 产品应支持强制重命名或删除默认账户，支持强制修改默认账户的默认口令。
7.2.2.3 产品应支持删除或停用多余的、过期的账户，避免共享账户的存在。
7.2.2.4 产品应支持可信主机、口令强度、身份鉴别、分级分权配置。

7.2.2.5 产品应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度并支持定期更换；若采用口令鉴别方式，应支持对口令的强度进行检查，如口令长度、是否需要包含数字、特殊字符等。
7.2.2.6 产品应具有登录超时重新鉴别功能。在安全策略设定的时间段内没有任何操作的情况下，能够锁定或终止会话，需再次进行身份鉴别才可重新登录。
7.2.2.7 当用户鉴别尝试失败达到指定次数后，产品应在安全策略设定的时间段内阻止用户进一步的鉴别请求。
7.2.2.8 产品应保护鉴别数据不被未授权查阅和修改。
7.2.2.9 产品应支持权限划分，为每一使用者设置安全属性信息，包括全局唯一标识、鉴别数据、授权信息或管理组信息、其它安全属性等。
7.2.2.10 产品应支持授予管理用户所需的最小权限，实现管理用户的权限分离，实现管理权限相互制约。

7.2.3 数据存储

7.2.3.1 产品应具备审计数据及安全报警事件存储功能。
7.2.3.2 存储容量至少满足 6 个月以上的日志记录需求，存储于掉电非易失性存储介质中。
7.2.3.3 告警及事件存储应分文件或分数据块，同时文件或数据块名称带日期时间信息，支持选择下载部分或全部存储数据。
7.2.3.4 存储的数据应包括事件发生的日期、时间、事件主体、事件类型、事件发生的位置、事件描述和结果等。
7.2.3.5 存储应具备存储空间告警功能，触发告警的剩余存储空间限值支持由管理员设定；当存储空间超过设定值时，应及时告警；存储空间满时，应采用先进先出的方式。
7.2.3.6 产品应具备存储数据的访问授权管理功能。
7.2.3.7 产品应能对存储的数据进行保护，避免受到未预期的删除、修改或覆盖等。
7.2.3.8 产品应具备配置备份、恢复功能，能够提供重要数据的本地数据备份与恢复功能。
7.2.3.9 产品应采用校验技术或密码技术保证数据在存储过程中的完整性，包括但不限于鉴别数据。
7.2.3.10 产品应采用密码技术保证数据在存储过程中的保密性，包括但不限于鉴别数据。

7.2.4 审计日志

7.2.4.1 产品应对与自身安全相关的以下事件生成审计日志，包括但不限于：
a) 身份鉴别，包括登录成功和退出、登录失败的详细信息；
b) 因鉴别失败次数超过了阈值而采取的禁止进一步尝试的措施；
c) 管理员的增加、删除、修改；
d) 审计策略的增加、删除、修改；
e) 时间同步；
f) 超过保存时限的审计记录和自身审计日志的自动删除；
g) 审计日志和审计记录的备份与恢复；
h) 存储空间达到阈值报警；
i) 升级；
j) 其他事件。
7.2.4.2 审计日志内容至少应包括日期、时间、事件主体、事件客体、事件描述和结果，远程管理主机地址（如采用）等。
7.2.4.3 产品应将自身审计日志与审计记录数据分开记录保存，以不同的记录文件或其它方式，方便用户查阅和分析。审计日志存储的最短期限不少于 6 个月。
7.2.4.4 产品应支持审计设备日志信息进行集中下载及存储，宜支持将审计信息通过车地无线通道发送到地面监控系统。
7.2.4.5 产品应采取相应措施来保证敏感信息的保密性和完整性，如对用户口令进行加密存储。

7.3 性能要求

7.3.1 百兆系统单口采集流量不应小于 90Mbit/s。

7.3.2　千兆系统单口采集流量不应小于 0.9Gbit/s。

7.4　其它要求

7.4.1　硬件要求

7.4.1.1　设备具有从异常状态中自动恢复的能力。
7.4.1.2　若与其它功能集成，设备应具备电源冗余功能且具有一定的负载能力。
7.4.1.3　各模块均应具有当电源中断 10ms 时不影响正常运行的能力。主控模块在识别电源故障 1ms 后通告 CPU，以便采取可能的自保护措施。

7.4.2　接口要求

7.4.2.1　设备应配备不同物理接口，分别用于配置管理和网络数据监听报警等。
7.4.2.2　设备安装应符合轨道交通车载电气柜安装要求，可采用 3U 标准机箱式安装或标准导轨、墙面安装等安装方式。
7.4.2.3　设备电源接口采用连接器连接。
7.4.2.4　设备采用 DC24V 或 DC110V 供电，其范围为 DC16.8V～30V 或 DC77V～137.5V。
7.4.2.5　设备在介于 0.6 Un～1.4 Un（Un：标称电压）之间的电压波动，如果持续时间不超过 0.1s，处于运行状态的设备不应引起功能偏差。
7.4.2.6　设备在介于 1.25 Un～1.4 Un 之间的电压波动，如果持续时间不超过 1s，不应引起设备损害。
7.4.2.7　百兆以太网口应采用 4 芯 M12-Dcode。
7.4.2.8　千兆以太网口应采用 8 芯 M12-Xcode 接口，应能接 4 芯电缆自适应为百兆口使用。
7.4.2.9　以太网接口支持 MDI/MDI-X 线序自动识别与切换。
7.4.2.10　设备侧 M12 连接器应采用插孔式。
7.4.2.11　产品在启动及运行期间，应具备运行状态自检功能，包括自身硬件状态、安全重要功能、配置文件、组件连接状态等，检测至少为最小可更换单元。自检信息应能够通过 TRDP 协议发送至车辆以太网控制网络主机。
7.4.2.12　产品应支持通过 TRDP 发送生命信号到 TCMS 系统主机；应具备 TRDP 心跳数据采集接收、心跳参数配置功能。
7.4.2.13　产品应具备自身时钟及时钟同步功能。应支持通过 TRDP 等协议与车辆以太网控制网络主机进行时钟同步，时钟信息通过 TRDP 协议包发送，应具备自身时钟功能，以便在没有同步时钟时保证时钟正确。
7.4.2.14　产品应支持通过标准协议对设备的状态进行检测，如 CPU、内存使用率，接口状态等。

7.4.3　软件要求

7.4.4　网络安全审计产品应能通过浏览器登录方式进行自管理配置操作。
7.4.5　网络安全审计产品应能通过地面管理平台软件进行集中配置操作。
7.4.6　应具备维护软件，用于下传到地面通用服务器的日志解析及分析。

8　检验

8.1　检验分类

检验分为三类:
a)　型式检验；
b)　出厂检验；
c)　装车试验。
型式检验及出厂检验应符合表1的规定，并出具型式检验及出厂检验报告。

表 1　检验要求

序号	检验项目	型式检验	出厂检验	检验方法及验收要求
1	目视检查	√	√	GB/T 25119—2021 12.2.2
2	性能试验	√	—	GB/T 25119—2021 12.2.3
3	低温试验	√	—	GB/T 25119—2021 12.2.4
4	高温试验	√	—	GB/T 25119—2021 12.2.5
5	交变湿热试验	√	—	GB/T 25119—2021 12.2.6
6	电源过电压试验	√	—	GB/T 25119—2021 12.2.7
7	浪涌、静电放电（ESD）	√	—	GB/T 25119—2021 12.2.8
8	射频试验	√	—	GB/T 25119—2021 12.2.9
9	绝缘试验	√	—	GB/T 25119—2021 12.2.10
10	冲击和振动试验	√	—	GB/T 25119—2021 12.2.12
11	低温存放试验	√	—	GB/T 25119—2021 12.2.15
注：√表示必做项目；—表示取决于供需双方之间的合同要求。				

8.2　型式检验

型式检验用于验证产品符合规定的要求。
型式检验应满足GB/T 25119—2021中12.1.2所规定的要求。

8.3　出厂检验

出厂检验用于验证产品特性符合型式检验的测量结果。
供应商对每台设备均应做出厂检验。

8.4　装车试验

产品功能测试应符合GB/T 37941的要求。
设备装车前，应进行系统通信联调测试。
设备装车前，宜进行各功能策略验证。
测试应确保安全功能测试充分性及完整性。

附 录 A
（资料性）
车辆以太网控制网络安全审计产品应用场景

车辆以太网控制网络安全审计产品是应用于轨道交通车辆车载以太网控制网络中，通过对网络通信流量采集、分析，监测车辆以太网控制网络中的非法活动或行为，并提供报警，对车辆以太网控制网络流量完成审计功能。

车辆以太网控制网络安全审计产品既要满足通用网络安全审计产品的基本要求，同时需要满足轨道交通车辆环境及应用场景的特殊要求。车载以太网控制网络安全审计产品主要应用在车辆以太网控制网络内部关键节点。

车辆以太网控制网络：车辆骨干网采用以太网总线技术，贯穿于全列车，用于列车各系统及运行状态信息收集，同时下发列车相关控制指令，实现列车控制、诊断、显示告警及存储分析等功能。

车辆以太网控制网络安全审计产品常见应用如下：

——车辆以太网控制网络内部关键节点通信流量审计，如图A.1所示；

——通常将VCU设备连接的交换机定义为关键节点，该交换机将其所有端口流量镜像到一个指定端口（以下称为镜像端口）；网络安全审计产品分别部署在两端，与该交换机的镜像端口连接，以采集交换机镜像流量；

——网络安全审计产品分别通过两个以太网接口与1台关键节点交换机连接，其中链路L11和L21为安全审计设备获取镜像流量专用通道，L12和L22为设备与车辆主控单元VCU通过TRDP交换数据的通道。

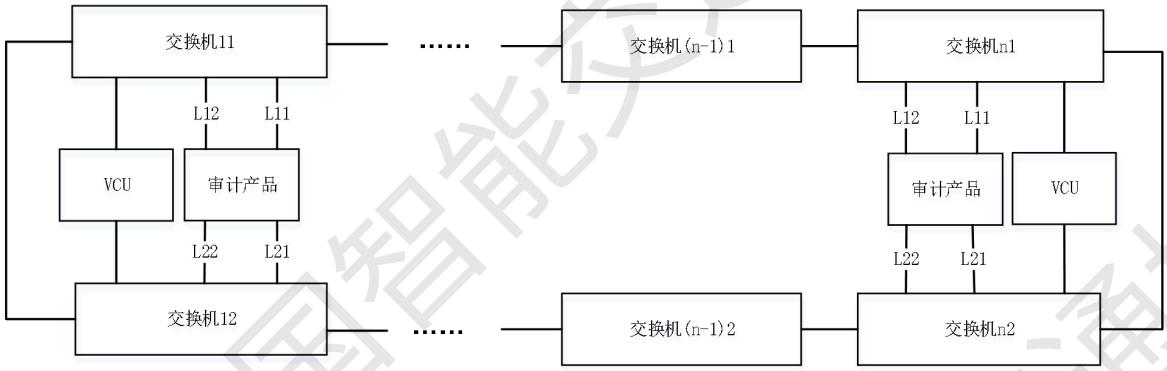

图 A.1 车辆以太网控制网络安全审计产品配置方案（示例）