ICS 45.120
CCS S70

团 体 标 准

T/CITSA 43-2024

轨道交通车辆
以太网控制网络防火墙技术要求

Rail transit vehicle — Technical requirements for firewall 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、中车青岛四方机车车辆股份有限公司、公安部第三研究所、中车大连电力牵引研发中心有限公司、中车大连机车车辆有限公司、杭州中电安科现代科技有限公司、中车青岛四方车辆研究所有限公司、北京珞安科技有限责任公司、同济大学、上海泽高电子工程技术股份有限公司。

本文件主要起草人：陈美霞、齐玉玲、林业、茅迥、王春萌、唐婧、邹春明、于人生、丛培鹏、张俊峰、张中豪、陆学鹏、沈拓、薛腾辉、邓辰鑫。

轨道交通车辆
以太网控制网络防火墙技术要求

1 范围

本文件规定了城市轨道交通车辆以太网控制网络防火墙的运用条件、技术要求及检验要求等。
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 20281—2020 信息安全技术 防火墙安全技术要求和测试评价方法
GB/T 21563 轨道交通 机车车辆设备 冲击和振动试验
GB/T 25069—2022 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 32347.1 轨道交通 设备环境条件 第1部分：机车车辆设备
GB/T 37933—2019 信息安全技术 工业控制系统专用防火墙技术要求
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 20281—2020和GB/T 25069—2022界定的以及下列术语和定义适用于本文件。

3.1

防火墙 firewall

对经过的数据流进行解析，并实现访问控制及安全防护功能的网络安全产品。

[来源：GB/T 20281—2020，3.1]

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防火墙 vehicle Ethernet control network firewall

部署于车辆网络控制系统中不同的安全域之间或安全边界处，具备网络层访问控制及过滤、车载通信协议规约检查和过滤功能，并具备高可用性，能够适应于轨道交通车载使用环境的安全网关类产品。

4 缩略语

下列缩略语适用于本文件。

ARP：地址解析协议（Address Resolution Protocol）
CPU：中央处理器（Central Processing Unit）
DNAT: 目的地址转换（Destination Network Address Translation）
ESD：静电放电（Electro-Static Discharge）
FTP：文件传输协议（File Transfer Protocol）
HTML: 超文本标记语言（Hyper Text Markup Language）
HTTP: 超文本传输协议（Hypertext Transfer Protocol）

ICMP：因特网控制报文协议（Internet Control Message Protocol）
IP：网际互连协议（Internet Protocol）
LTE：长期演进（Long Term Evolution）
MAC：介质访问控制（Media Access Control）
MCG：移动通讯网关（Mobile Communication Gateway）
MDI：介质相关类设备（Medium Dependent Interface）
MDI-X：介质相关类交叉设备（Medium Dependent Interface cross-over）
NAT：网络地址转换（Network Address Translation）
PDF：便携式文档格式（Portable Document Format）
RTSP：实时流传输协议（Real Time Streaming Protocol）
SFTP：安全文件传输协议（Secret File Transfer Protocol）
SNAT：源网络地址转换（Source NAT）
SNMP：简单网络管理协议（Simple Network Management Protocol）
SSH：安全外壳协议（Secure Shell）
TCMS：列车控制和管理系统（Train Control and Management System）
TCP：传输控制协议（Transmission Control Protocol）
TRDP：列车实时数据协议（Train Real-time Data Protocol）
UDP：用户数据报协议（User Datagram Protocol）
VCU：车载控制单元（Vehicle Control Unit）
VLAN：虚拟局域网（Virtual Local Area Network）
WLAN：无线局域网（Wireless Local Area Network）

5 产品描述

车辆以太网控制网络防火墙是应用于轨道交通车辆车载控制系统安全边界的一类特殊防火墙，既要满足GB/T 37933中防火墙的基本要求，又要满足轨道交通车辆环境下的特殊要求，其典型部署场景见附录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 功能要求

7.1.1 访问控制功能

7.1.1.1 产品应基于五元组的安全策略：源 IP、目的 IP、源端口、目的端口、传输层协议类型，应支持 MAC 地址、时间的部分或全部组合。
7.1.1.2 产品应支持针对协议的数据过滤，包括但不限于 TCP/IP、UDP、Telnet、SFTP、SSH、RTSP 等。

7.1.1.3 产品应支持基于连接状态的检测结果来决定允许或拒绝数据流通过。
7.1.1.4 产品应支持协议白名单及协议格式规约检查，不准许不符合协议规约的通信。
7.1.1.5 产品应支持基于流量的白名单自学习，能通过自动学习生成白名单列表。
7.1.1.6 产品应支持深度包检测，能够对 FTP 等协议的操作类型、操作对象、操作范围等参数进行控制。
7.1.1.7 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。
7.1.1.8 产品应支持通过 TRDP 发送生命信号到 TCMS 系统；支持 TRDP 心跳数据采集接收、心跳参数配置功能。

7.1.2 组网部署

7.1.2.1 产品应支持主-备部署模式。
7.1.2.2 产品应支持 VLAN 透传、封装、解封装，提供 802.1Q 模式。
7.1.2.3 产品应支持 VLAN 接口响应 ARP、ICMP 报文。
7.1.2.4 产品应支持静态路由和策略路由。
7.1.2.5 产品应支持透明传输模式、路由转发模式、混合等多种部署模式。
7.1.2.6 产品应支持多种运行模式，具体技术要求如下：

a) 支持学习模式，记录运行过程中经过防火墙的所有策略、资产等信息，支持工控协议的深度内容检测策略学习，学习深度与工业协议深度内容检测深度一致，形成白名单策略集；
b) 支持验证模式或测试模式或告警模式，仅对防护策略进行告警，但不拦截；
c) 支持正常工作模式或防护模式，应按照防护策略进行过滤等动作拦截和告警。

7.1.2.7 产品宜支持负载均衡功能，能根据安全策略将网络流量均衡到多台业务设备上。
7.1.2.8 产品应提供联动接口，能接受其他网络安全产品联动请求，如执行其他网络安全产品下发的安全策略等。

7.1.3 NAT 功能

产品应支持至少1路静态SNAT，支持一对一静态NAT、多对一SNAT、一对多DNAT等多种模式。

7.1.4 攻击防护功能

7.1.4.1 产品应具备抵御扫描行为的功能，能够检测和记录扫描行为，包括对防火墙自身和受保护网络的扫描，如 TCP 扫描（阈值可配），UDP 扫描（阈值可配），同时具备主机抑制功能（时长秒级可配）等。
7.1.4.2 除具有 GB/T 37933 中所要求的抗拒绝服务攻击能力外，产品还应具有以下抗攻击能力（包括但不限于）：

a) ARP Flood 攻击，
b) IP Flood 攻击，
c) HTTP Flood 攻击，
d) Smurf 攻击，
e) Winnuke 攻击。

7.1.4.3 产品应支持检测并阻断经逃逸技术处理过的攻击行为。

7.1.5 资产发现

根据通过防火墙的流量，产品应能自动发现网络中的设备资产，识别设备资产之间的网络连接关系，识别网络中的协议类型，分析网络传输协议并自动生成资产对象。

7.1.6 日志审计与报表

7.1.6.1 产品应满足 GB/T 37933—2019 中 6.2.2.2 对增强级防火墙安全审计的相关要求，包括记录事件类型、记录内容、日志管理等要求。
7.1.6.2 产品应支持网络会话、日志详情、日志存储、日志查询、日志统计与日志备份。

7.1.6.3 存储容量至少满足 75 万条记录存储且满足 6 个月以上的日志记录需求，掉电后存储内容至少保存 6 个月。
7.1.6.4 报表支持输出流量统计结果，包括告警统计、协议流量、网络流量、并发会话、流量与会话 IP 等至少前 10 统计。
7.1.6.5 报表应支持 PDF 及 HTML 等格式输出报表。
7.1.6.6 应支持周报及月报统计。
7.1.6.7 应支持第三方设备对车辆以太网控制网络防火墙日志信息进行集中下载及收集存储。
7.1.6.8 防火墙设备应能通过以太网接口连接到无线系统设备，用于车辆到库后根据接收到的日志下载触发信息，自动将记录的日志信息下发到地面服务器进行存储。存储到地面的日志信息应能解析为通用格式进行分析查看，如 txt、csv 等，并且具有筛选统计等功能。
7.1.6.9 产品告警信息应支持通过以太网接口（采用 TRDP 协议，仅发送告警状态信息）发送到 TCMS 系统主机。告警信息内容如下：

a) 告警发生的时间，应包括年、月、日、时、分、秒；
b) 应包括数据包的协议类型、源地址、目标地址、源端口、目标端口、应用层协议名称；
c) 协议的深度内容检查信息及告警信息；
d) 应根据告警内容设置告警级别，包括但不限于紧急、告警、严重、错误、警告等多个级别。

7.1.6.10 产品应支持通过 SNMPv2/v3 协议对防火墙的状态进行检测，如 CPU、内存使用率，接口状态等。

7.2 性能要求

7.2.1 吞吐量

在10条策略规则和不丢包的情况下，一对相应速率的端口应达到的双向吞吐量要求如下：

a) 对于 64 字节短包，百兆防火墙不应小于线速的 30%，千兆防火墙不应小于线速的 40%；
b) 对于 256 字节中长包，百兆防火墙不应小于线速的 70%，千兆防火墙不应小于线速的 80%；
c) 对于 512 字节的长包，百兆防火墙不应小于线速的 50%，千兆防火墙不应小于线速的 55%。

7.2.2 延时

延时视不同速率的防火墙有所不同，在吞吐量90%条件下，应满足如下要求：

a) 对于 64 字节短包、256 字节中长包、512 字节长包，百兆防火墙平均延迟不应超过 1ms；
b) 对于 64 字节短包、256 字节中长包、512 字节长包，千兆防火墙平均延迟不应超过 200us。

7.2.3 会话限制

限制单个IP的最大并发会话连接数，支持限制范围为0～3 000个。

7.2.4 并发连接数

最大并发连接数视不同速率的防火墙有所不同，要求如下：

a) 百兆防火墙的最大并发连接数不应少于 60 000 个；
b) 千兆防火墙的最大并发连接数不应少于 300 000 个。

7.2.5 最大连接速率

最大连接速率视不同速率的防火墙有所不同，要求如下：

a) 百兆防火墙的最大连接速率不应少于 1 500 个/秒；
b) 千兆防火墙的最大连接速率不应少于 5 000 个/秒。

7.3 自身安全要求

7.3.1 运维管理

7.3.1.1 产品应支持设备自管理、图形化配置、命令行、配置及策略导入导出功能、设备心跳、版本升级、恢复出厂设置、重启等功能。

7.3.1.2 产品应具有自检功能，能够在初始化期间及设备运行期间对硬件、安全重要功能、配置等文件进行自检，检测至少为最小可更换单元，自检信息应能通过 TRDP 协议发送至车辆以太网控制网络主机。发现异常时告警，并有自动恢复的能力。设备上电到正常工作时间不超过 60s。

7.3.1.3 产品应支持可信任主机、口令强度、身份鉴别、分级分权：

a) 应提供一个可信任主机列表，启用后、仅在该列表中的 IP 地址可以访问设备的管理接口；
b) 应提供一种机制以验证口令强度，满足口令的最小长度为 8 位，且复杂度满足大写字母、小写字母、特殊字符和数字的组合；
c) 应对每一个访问授权管理员进行唯一的身份鉴别，支持鉴别失败策略的配置，包括但不限于：鉴别失败最大次数、限制登录时间等；
d) 应支持授权管理员的角色划分，划分为系统管理员、安全操作员和安全审计员，且支持将管理用户权限进行分离。

7.3.1.4 产品应提供联动接口，以支持安全管理设备的集中管理。通过联动接口应能获取防火墙状态信息（运行状态、规则库版本等）、安全策略管理（包括策略下发、策略查询、策略修改等功能）、策略备份与恢复、日志数据同步。联动接口应保证数据传输的机密性、完整性、可靠性。

7.3.2 管理安全

7.3.2.1 产品应支持授权管理员的口令鉴别方式，且口令设置满足安全要求。

7.3.2.2 产品应为每个级别规定的授权管理员提供一套唯一的为执行安全策略所必需的安全属性。

7.3.2.3 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要求并定期更换。

7.3.2.4 产品应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数，登录连接超时自动退出等相关措施。

7.3.2.5 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。

7.3.2.6 产品应对需登录的用户分配账户和权限。

7.3.2.7 产品应具备重命名或删除默认账户，修改默认账户的默认口令功能。

7.3.2.8 产品应具备及时删除或停用多余的、过期的账户功能，避免共享账户的存在。

7.3.2.9 产品应能授予管理用户所需的最小权限，实现管理用户的权限分离。

7.3.2.10 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。

7.3.2.11 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。

7.3.2.12 产品应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。

7.3.2.13 产品应对审计进程进行保护，防止未经授权的中断。

7.3.2.14 产品应遵循最小安装的原则，仅安装需要的组件和应用程序。

7.3.2.15 产品应关闭不需要的系统服务、默认共享和高危端口。

7.3.2.16 产品应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。

7.3.2.17 产品不应包含已知存在的高危和中危漏洞。

7.3.2.18 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，并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。

7.3.2.19 产品应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据。

7.3.2.20 产品应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据。

7.3.2.21 产品应具有重要数据的本地数据备份与恢复功能。

7.3.2.22 产品应支持上电自启动功能；应从软件实现、硬件配置上考虑列车停运断电等非正常关机场景，确保设备在生命周期内不会因非正常关机导致故障。

7.4 软件要求

7.4.1 车辆以太网控制网络防火墙应能通过浏览器登录并进行配置操作。

7.4.2 应具备将存储的日志信息下传到地面通用服务器的维护软件，用于地面日志解析及分析。

7.5 接口要求

7.5.1 设备应配备不同的物理接口用于配置管理。
7.5.2 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。
7.5.3 设备电源接口应采用连接器连接。
7.5.4 设备采用 DC24V 或 DC110V 供电，其范围为 DC16.8V～30V 或 DC77V～137.5V。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。
7.5.5 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。
7.5.6 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。
7.5.7 百兆以太网口应采用 4 芯 M12-Dcode。
7.5.8 千兆以太网口应采用 8 芯 M12-X 接口，应能接 4 芯电缆自适应为百兆口使用。
7.5.9 以太网接口支持 MDI/MDI-X 线序自动识别与切换。
7.5.10 设备应具备 bypass 功能。
7.5.11 设备应采用无风扇散热设计，参见 GB/T 37933。
7.5.12 设备侧 M12 连接器应采用插孔式。

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/T25119—2021 12.2.2
2	性能试验	√	—	GB/T25119—2021 12.2.3
3	低温试验	√	—	GB/T25119—2021 12.2.4
4	高温试验	√	—	GB/T25119—2021 12.2.5
5	交变湿热试验	√	—	GB/T25119—2021 12.2.6
6	电源过电压试验	√	—	GB/T25119—2021 12.2.7
7	浪涌、静电放电（ESD）	√	—	GB/T25119—2021 12.2.8
8	射频试验	√	—	GB/T25119—2021 12.2.9
9	绝缘试验	√	—	GB/T25119—2021 12.2.10
10	冲击和振动试验	√	—	GB/T25119—2021 12.2.12
11	低温存放试验	√	—	GB/T25119—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防火墙应用场景

车辆以太网控制网络防火墙是应用于轨道交通车辆车载网络控制系统安全边界的一类特殊防火墙，其既要满足通用防火墙的基本要求，同时需要满足轨道交通车辆环境下的特殊要求。车辆以太网控制网络防火墙主要应用在车辆控制系统边界处，用于不同控制系统间或控制系统与无线接口间。

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。

车地无线通信系统：用于列车车载及地面无线数据传输，主要采用WLAN、LTE、4G/5G等方式。

车辆以太网控制网络防火墙常见应用如下：

——车载各系统间的安全防护，图A.1示出了在乘客信息系统及列车网络控制系统间的安全防护；

——车辆以太网控制网络无线边界安全防护，图A.2示出了在车辆以太网控制网络无线边界处的安全防护。

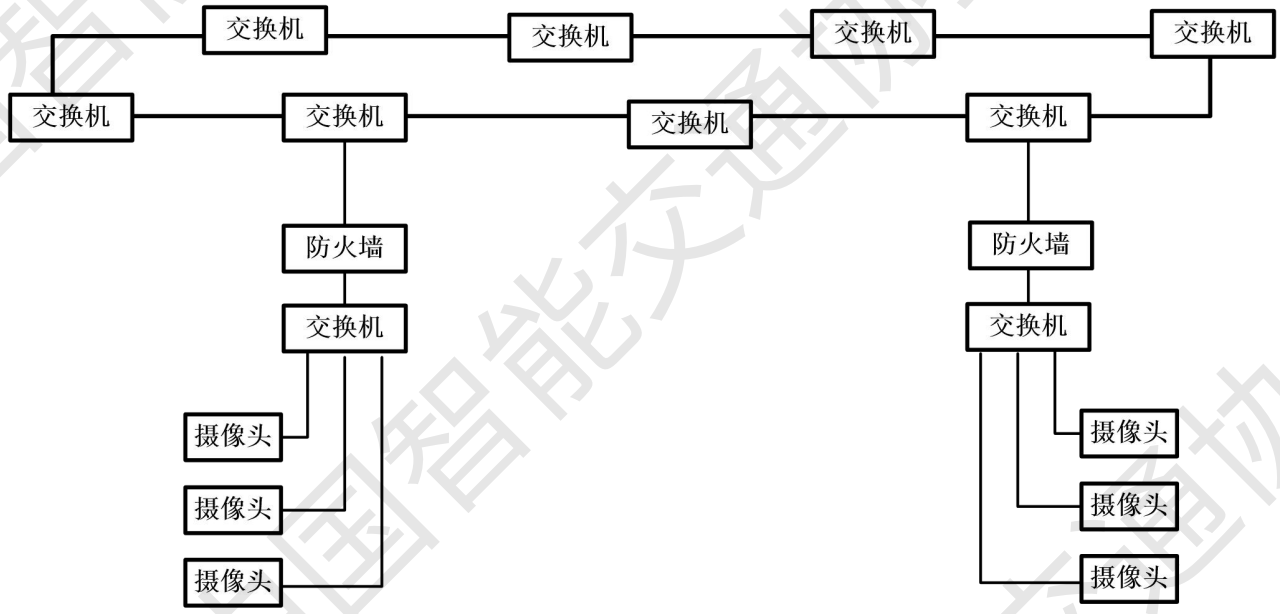

图 A.1 系统间的安全防护

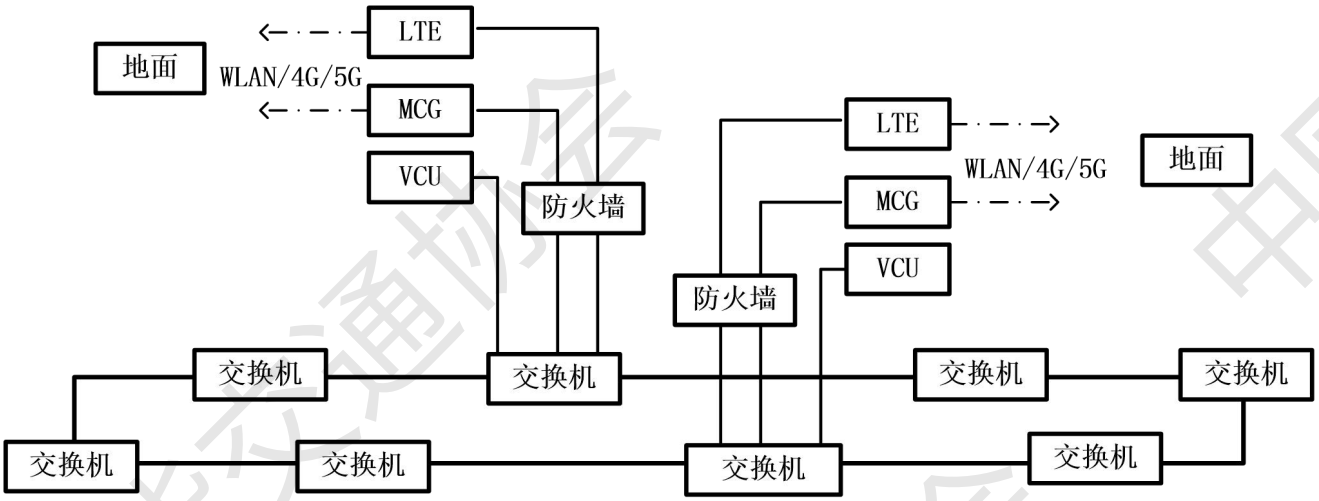
地面
LTE
WLAN/4G/5G
MCG
VCU
防火墙
LTE
WLAN/4G/5G
MCG
VCU
防火墙
地面
交换机
交换机
交换机
交换机
交换机
交换机
交换机

图 A.2 无线边界防护