ICS 45.120
CCS S70

# 团 体 标 准

T/CITSA 45-2024

# 轨道交通车辆
# 以太网控制网络入侵检测系统技术要求

Rail transit vehicle——Technical requirements for intrusion detection system 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、中车唐山机车车辆有限公司、中车青岛四方机车车辆股份有限公司、中车长春轨道客车股份有限公司、中车株洲电力机车有限公司、中车青岛四方车辆研究所有限公司、中车大连机车车辆有限公司、公安部第三研究所、北京威努特技术有限公司、杭州中电安科现代科技有限公司、上海泽高电子工程技术股份有限公司。

本文件主要起草人：张军贤、黄涛、高琦、郑殿科、王峥、高兴华、刘泰、张尧、肖曦、彭兴伟、王嵩淞、邹春明、唐智南、毛庆威、邓辰鑫、谢兰欣。

# 轨道交通车辆
# 以太网控制网络入侵检测系统技术要求

## 1 范围

本文件规定了城市轨道交通车辆以太网控制网络入侵检测系统的运用条件、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 20275—2021 信息安全技术 网络入侵检测系统技术要求及测试评价方法

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 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 37953—2019 信息安全技术 工业控制网络监测安全技术要求及测试评价方法

## 3 术语和定义

GB/T 20275—2021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

**安全事件 incident**

对网络和信息系统或者其中的数据造成危险的事件。

[来源：GB/T 20275—2021，3.1]

3.2

**入侵 intrusion**

对网络或联网系统的未授权访问，即对信息系统进行有意或无意的未授权访问，包括针对信息系统的恶意活动或对信息系统内资源的未授权使用。

[来源：GB/T 25069—2022，3.495]

3.3

**入侵检测 intrusion detection**

检测入侵的正式过程，该过程一般特征为采集如下知识：反常的使用模式，被利用的脆弱性及其类型、利用的方式，以及何时发生和如何发生。

[来源：GB/T 25069—2022，3.498]

3.4

**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。

3.5

**车辆以太网控制网络入侵检测系统 intrusion detection for vehicle Ethernet control network**

部署于车辆以太网控制网络中，以实现针对车辆以太网控制网络行为的安全事件监测、审计、告警和管理等功能的系统。

3.6

**误报 false positive**

没有攻击或故障时检测系统却有报警的情况。

[来源：GB/T 25069—2022，3.647]

3.7

**漏报 false negative**

安全事态或事件发生时检测系统没有报警的情况。

[来源：GB/T 25069—2022，3.365]

## 4 缩略语

下列缩略语适用于本文件。

FTP：文件传输协议（File Transfer Protocol）

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

IP：网际协议（Internet Protocol）

LTE：长期演进（Long Term Evolution）

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）

TCP：传输控制协议（Transport 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）

WLAN：无线局域网（Wireless Local Area Network）

## 5 系统描述

车辆以太网控制网络入侵检测系统是应用于轨道交通车辆车载环境，通过监测车辆以太网控制网络内的数据报文，实时获取数据包进行解析，检测车辆以太网控制网络中的入侵行为和异常行为，并及时告警的系统。

系统应满足特定车载环境和安全功能要求，能对车辆以太网控制网络边界或内部各区域进行检测保护，发现非法入侵活动，根据监测结果实时报警、响应，达到主动发现入侵活动、确保网络安全的目的。

车辆以太网控制网络入侵检测系统应用场景见附录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 系统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 流量监测

7.1.1.1 系统应支持业务接口被动方式进行流量监测，业务接口不应外发数据包影响车辆以太网控制网络正常运行。
7.1.1.2 系统应能监测网络内的流量数据包，实时获取数据包用于检测分析。
7.1.1.3 系统应能监测指定的协议或 IP 地址的流量数据包，且不影响车辆以太网控制网络正常运行。
7.1.1.4 系统应监测整个网络或者某一特定协议、地址、端口的报文流量和字节流量。

### 7.1.2 车辆通信协议分析

7.1.2.1 对于在车辆以太网控制网络内获取的数据包，系统应能够分析其承载的车载通信协议报文。
7.1.2.2 系统应能够分析 Modbus、TCP/IP、UDP 等通用协议。
7.1.2.3 系统应能够分析轨道交通车辆以太网控制网络专用 TRDP 及 TRDP SDTv2 安全传输协议，协议应符合 GB/T 28029.4。
7.1.2.4 系统应能够分析车辆以太网控制网络内传输的互联网协议数据包：HTTP、FTP、Telnet、SNMP。

### 7.1.3 攻击行为监测

7.1.3.1 系统应具备特征库，能够通过特征匹配、机器学习等方法发现攻击行为。
7.1.3.2 系统应能够发现车载协议漏洞攻击。
7.1.3.3 系统应能够发现车辆以太网控制网络系统应用漏洞攻击。
7.1.3.4 系统应能够发现操作系统漏洞、中间件类漏洞、控件类漏洞攻击。
7.1.3.5 系统应能够发现车载控制设备漏洞攻击。
7.1.3.6 系统应支持恶意代码识别的功能，能够监测网络中蠕虫病毒、木马等攻击行为的发生。
7.1.3.7 系统应能发现躲避或欺骗检测的行为，如 TCP 流重组、协议端口重定位等。
7.1.3.8 系统应支持对攻击行为进行全原始数据包存储，以便事后分析。
7.1.3.9 系统应支持检测经逃逸技术处理过的攻击行为。

### 7.1.4 安全事件响应

7.1.4.1 事件告警：对于攻击行为或异常行为，系统应能按照事件严重程度将事件分级，通过车地无线通道实时发送告警信息到地面监控系统，以采取屏幕实时提示等直观有效的方式传达告警信息。
7.1.4.2 告警过滤：系统应允许管理员定义安全策略，对被检测车辆以太网控制网络中的指定主机或事件不予告警。
7.1.4.3 事件合并：系统应能对高频度发生的相同安全事件进行合并告警，避免出现告警风暴。
7.1.4.4 定制响应：系统应允许管理员定义安全策略，对车辆以太网控制网络中事件定制响应方式。

### 7.1.5 安全配置

7.1.5.1 系统应提供安全策略配置功能，应支持安全策略的导入和导出。
7.1.5.2 系统应内置车辆以太网控制网络相关漏洞知识库，内容应包括：
——车辆以太网控制网络协议漏洞、应用漏洞、操作系统漏洞和车载控制设备漏洞；
——漏洞风险级别；
——详细漏洞修补方案和可采取的对策。
7.1.5.3 攻击特征库支持在系统使用期内的更新。
7.1.5.4 系统应内置车辆以太网控制网络攻击检测特征库，事件风险级别，详细的修补方案和可采取的对策。
7.1.5.5 系统应能对车辆 TRDP 协议端口进行重新设定及解析。
7.1.5.6 系统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。
7.1.5.7 系统应支持添加新的车辆以太网控制网络协议，并支持对其进行分析。

## 7.2 管理要求

### 7.2.1 运维管理

7.2.1.1　系统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系统所需的所有功能。
7.2.1.2　系统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应超过60s。
7.2.1.3　系统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。
7.2.1.4　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。
7.2.1.5　系统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。
7.2.1.6　系统应对审计进程进行保护，防止未经授权的中断。
7.2.1.7　系统应遵循最小安装的原则，仅安装需要的组件和应用程序。
7.2.1.8　系统应关闭不需要的系统服务、默认共享和高危端口。
7.2.1.9　系统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。
7.2.1.10　系统应能够发现可能存在的已知漏洞，并及时修补漏洞，在交付用户前提供漏洞扫描报告。

### 7.2.2　数据存储

7.2.2.1　系统应具备安全事件及报警事件存储功能。
7.2.2.2　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。
7.2.2.3　告警及事件存储能分文件或数据块，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。
7.2.2.4　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。
7.2.2.5　系统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。
7.2.2.6　存储数据应能以文本及表格等格式输出报表。
7.2.2.7　支持周报及月报统计。
7.2.2.8　系统应支持第三方设备对入侵检测系统信息进行集中下载及收集存储。应能通过车辆到库后自动（根据接收到的日志下载触发信息）将记录的日志信息下发到地面服务器进行存储。
7.2.2.9　日志信息应能解析为通用格式进行分析查看，并且具有筛选统计等相关功能。
7.2.2.10　系统应具备存储数据的访问授权管理功能。
7.2.2.11　系统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。
7.2.2.12　系统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。
7.2.2.13　系统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。
7.2.2.14　系统应具备配置备份与恢复功能，能够提供重要数据的本地数据备份与恢复功能。

### 7.2.3　升级管理

7.2.3.1　系统应具有通过本地和远程升级的功能。
7.2.3.2　系统应具有通过自管理接口或管理平台进行升级的功能。
7.2.3.3　系统应具有本地和远程升级车辆以太网控制网络相关漏洞知识库和检测特征库的功能。
7.2.3.4　系统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。

### 7.2.4　用户管理

7.2.4.1　系统应支持用户管理，包括添加、激活、禁止、删除用户。
7.2.4.2　系统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。
7.2.4.3　系统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。
7.2.4.4　系统应支持可信主机、口令强度、身份鉴别、分级分权配置。
7.2.4.5　系统应对登录的用户进行身份标识和鉴别，身份标识应具有唯一性，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。

7.2.4.6 系统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，应能锁定或终止回话，需再次进行身份鉴别才可重新登录。
7.2.4.7 当用户鉴别尝试失败达到指定次数后，系统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。
7.2.4.8 系统应允许使用者锁定当前交互会话，锁定后需要再次进行身份鉴别才可重新登录。
7.2.4.9 系统应保护鉴别数据不被未授权查阅和修改。
7.2.4.10 系统应支持权限划分，为每一使用者设置安全属性信息、包括唯一标识、鉴别数据、授权信息或管理组信息、其它安全属性等。
7.2.4.11 系统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。
7.2.4.12 系统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。应采取必要措施防止鉴别信息在网络传输过程中被窃听。

#### 7.2.5 日志管理

7.2.5.1 系统应满足 GB/T 37953—2019 中 6.1.2.3 对日志管理的相关要求。
7.2.5.2 系统应对监测策略的创建、修改、删除、应用提供访问控制等安全措施，并记录相关审计日志。
7.2.5.3 系统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 误报率

系统应将误报率控制在应用许可的 10%以内，不应对正常使用产品产生较大影响。

#### 7.3.2 漏报率

系统应将漏报率控制在应用许可的10%以内，不应对正常使用产品产生较大影响。

#### 7.3.3 流量监控能力

7.3.3.1 百兆系统单口监控流量不应小于 90Mbit/s。
7.3.3.2 千兆系统单口监控流量不应小于 0.9Gbit/s。

#### 7.3.4 并发连接数监控能力

7.3.4.1 百兆系统单口监控并发连接数不小于 10 000 个。
7.3.4.2 千兆系统单口监控并发连接数不小于 100 000 个。

### 7.4 其它要求

#### 7.4.1 硬件要求

7.4.1.1 若与其它功能集成，设备需具备电源冗余功能且具有一定的负载能力。
7.4.1.2 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。
7.4.1.3 串联部署时设备应能够在突发掉电情况下，自动实现每一对输入输出通信端口的物理导通。

#### 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 设备电源接口通过连接器连接。
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-X 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　设备在启动及工作时，应具备运行状态自检功能，包括自身硬件状态、组件连接状态等，检测至少为最小可更换单元，自检信息应能通过 TRDP 协议发送至车辆以太网控制网络主机。
7.4.2.11　系统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。
7.4.2.12　系统支持通过 TRDP 发送生命信号到 TCMS 系统主机；支持 TRDP 心跳数据采集接收、心跳参数配置功能。
7.4.2.13　系统应提供与外部服务器进行时钟同步的功能。宜支持通过 TRDP 等协议与车辆以太网控制网络系统主机进行时钟同步，时钟信息通过 TRDP 协议包发送。
7.4.2.14　系统应具备自身时钟功能及手动设置时钟的功能，以便在没有同步时钟时保证时钟正确。
7.4.2.15　设备替换后，应能够通过车载连接或地面远程进行信息恢复。

### 7.5　软件要求

7.5.1　应能通过浏览器登录方式对系统进行自管理配置操作。
7.5.2　应能通过地面管理平台软件对系统进行集中配置操作。
7.5.3　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/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

系统功能测试应符合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入侵检测系统应用场景

车辆以太网控制网络入侵检测系统是应用于轨道车辆以太网控制网络安全区域边界或内部的专用系统，通过监测车辆控制网络内的数据报文，实时获取数据包进行解析，检测车辆以太网控制网络中的入侵行为和异常行为，并及时告警的系统。

车辆以太网控制网络入侵检测系统既要满足通用入侵检测系统的基本要求，同时需要满足轨道交通车辆环境及应用场景的特殊要求。车辆以太网控制网络入侵检测系统主要应用在车辆控制系统区域边界处（包括不同控制系统间或无线接口间、维护操作边界处等），以及控制网络内部。

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：基于车载无线设备及地面AP构建的车地无线数据传输系统，用于车辆数据实时或入库后传输到地面，主要采用WLAN、LTE专网、4G/5G等方式。

维护操作边界：用于人工维护操作接入处，如交换机维护接口等。

车辆以太网控制网络入侵检测系统常见应用如下：

——车辆以太网控制网络系统边界安全检测，见图A.1中入侵检测系统1；

——车辆以太网控制网络内部安全检测，见图A.2中入侵检测系统2；

——车辆各系统域间的安全检测，见图A.3中入侵检测系统3。

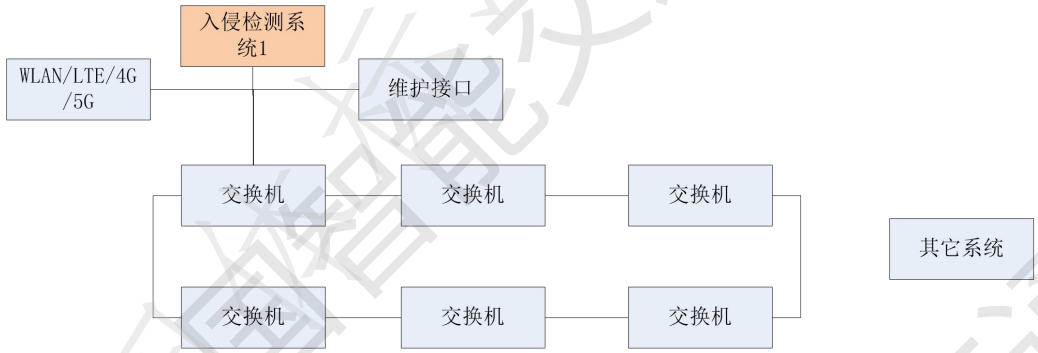


图 A.1 边界安全检测

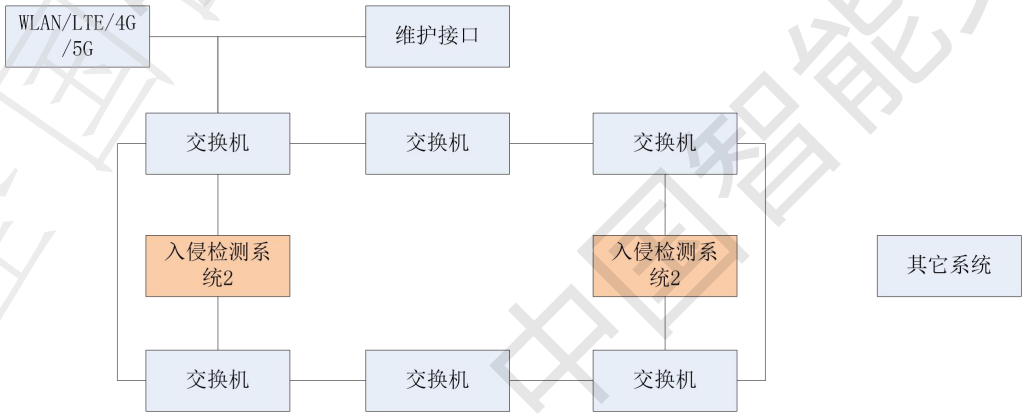


图 A.2 车辆以太网控制网络内部安全检测

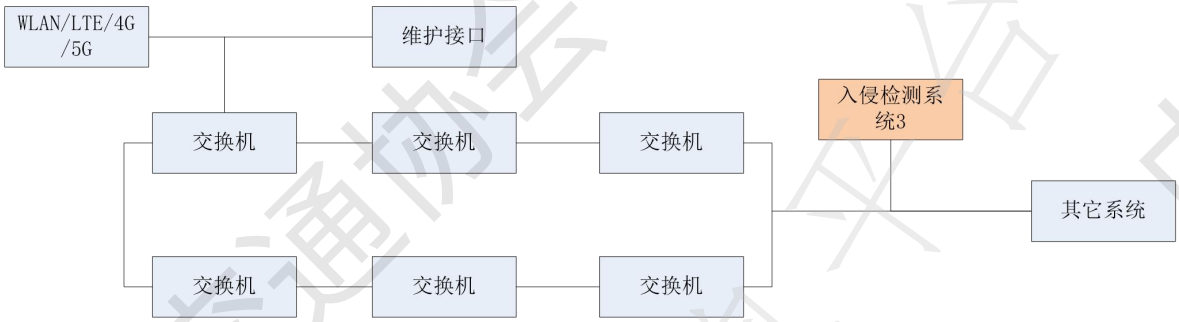


图 A.3 车辆各系统域之间安全检测