ICS 43.020
CCS T 40

团 体 标 准

T/CSAE 295.7—XXXX

车路云一体化系统
第 7 部分：信息安全规范

Vehicle-road-cloud integrated system—
Part 7: Information security specification

（报批稿）

（本草案完成时间：2025.09.02）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布 XXXX－XX－XX 实施

中国汽车工程学会 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。

本文件为T/CSAE 295《车路云一体化系统》的第7部分。T/CSAE 295已经发布了以下部分：

——　第1部分：系统组成及基础平台架构；
——　第2部分：车云数据交互规范；
——　第3部分：路云数据交互规范；
——　第4部分：云云数据交互规范；
——　第5部分：平台服务场景规范；
——　第7部分：信息安全规范。

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。

本文件由中国智能网联汽车产业创新联盟提出。

本文件由中国汽车工程学会标准化工作委员会归口。

本文件起草单位：西部智联数字科技（重庆）有限公司、国汽（北京）智能网联汽车研究院有限公司、联通智网科技股份有限公司、斯润天朗（无锡）科技有限公司、国汽大有时空（安庆）科技有限公司、北京万集科技股份有限公司、北京百度智行科技有限公司、湖南湘江智能科技创新中心有限公司、山石网科通信技术股份有限公司、宁波路特斯机器人公司、清华大学、上海控安智科软件有限公司、中国第一汽车股份有限公司研发总院、吉利汽车研究院（宁波）有限公司、广州高新兴网联科技有限公司、蘑菇车联信息科技有限公司、中汽创智科技有限公司、易图通科技（北京） 有限公司、云控智行科技有限公司、长安汽车、上海零数众合信息科技有限公司、沈阳美行科技股份有限公司、深圳市城市交通规划设计研究中心股份有限公司、阿里云计算有限公司。

本文件主要起草人：李克强、宋雪冬、辛克铎、乌尼日其其格、薛宇、刘璟、周光涛、程军峰、巩金亮、赵晓宇、刘杰、刘志杰、李庆建、陈灿东、徐智凯、马春香、路宏、朱双贺、刘凯、胡锐、吴疆、何伊圣、刘翔、樊伟、孙卫萍、罗禹贡、高博麟、王博文、张璇、刘枫、王冰、梁嘉琪、张晓东、吴冬升、曾少旭、朱磊、郭杏容、杨彦召、张平、汤咏林、阿拉坦套力古拉、杨梦燕、尉晓昌、刘岱、兰春嘉、杨珍、刘秋平、许建荣、王森 、王琳、刘彦斌。

引　　言

T/CSAE 295通过提出车路云一体化系统的组成及架构、数据交互要求、场景服务及质量、信息安全规范、测试规范等要求，支撑车路云一体化共性关键技术研究，实现基础数据互联互通，保障基础设施共享共用，促进车路云一体化系统组成要素的建设。

T/CSAE 295拟分为9个部分。

——第 1 部分：系统组成及基础平台架构。目的在于对车路云一体化系统相关概念进行统一，对系统组成及基础平台三层云架构进行规范，打破现有信息壁垒、实现基础数据互联互通、保障基础设施的共享共用。

——第 2 部分：车云数据交互规范。目的在于规范车路云一体化系统下车云交互的数据项目。

——第 3 部分：路云数据交互规范。目的在于规范车路云一体化系统下路云交互的数据项目。

——第 4 部分：云云数据交互规范。目的在于规范车路云一体化系统下云控基础平台内部的边缘云、区域云、中心云之间交互的数据项目。

——第 5 部分：平台服务场景规范。目的在于明确车路云一体化系统基础平台的服务分类、服务方式、系统相关设备及通信等的要求。

——第 6 部分：平台服务质量规范。目的在于规范车路云一体化系统基础平台面向不同用户提供服务的质量要求。

——第 7 部分：信息安全规范。目的在于规范车路云一体化系统云控平台的信息安全技术及管理要求以及相应的证实方法。

——第 8 部分：云控基础平台测试规范。目的在于规范车路云一体化系统云控基础平台功能和非功能测试及应用场景测试。

——第 9 部分：建设指南。目的在于指导和规范车路云一体化系统云控平台的建设，保障车路云一体化系统服务和运营能力，促进系统的落地应用。

T/CSAE 295车路云一体化系统系列文件的关系如图1所示。

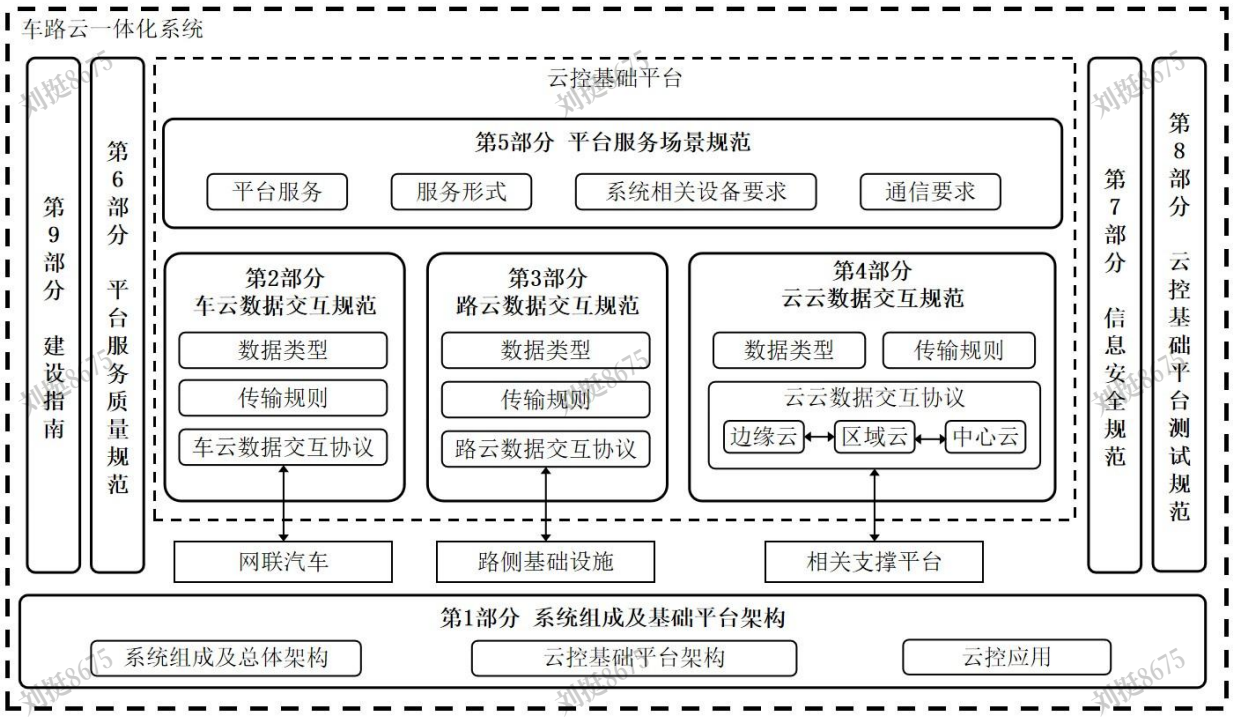


图 1　T/CSAE 295 车路云一体化系统系列文件关系图

车路云一体化系统 第7部分：信息安全规范

1 范围

本文件规定了车路云一体化系统云控平台的信息安全架构、安全要求和证实方法。

本文件适用于对车路云一体化系统云控平台使用过程中的信息安全管理，智能网联汽车行业其他智慧交通平台参照使用。

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 17901.1-2020 信息技术 安全技术 密钥管理 第1部分：框架

GB/T 17901.3-2021 信息技术 安全技术 密钥管理 第3部分：采用非对称技术的机制

GB/T 20984-2022 信息安全技术 信息安全风险评估方法

GB/T 20985.1-2017 信息技术 安全技术 信息安全事件管理 第1部分：事件管理原理

GB/T 20986-2023 信息安全技术 网络安全事件分类分级指南

GB/T 21053-2023 信息安全技术 公钥基础设施 PKI系统安全技术要求

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求

GB/T 28827.3-2012 信息技术服务 运行维护 第3部分：应急响应规范

GB/T 31509-2015 信息安全技术 信息安全风险评估实施指南

GB/T 32907-2016 信息安全技术 SM4分组密码算法

GB/T 32918.1-2016 信息安全技术 SM2椭圆曲线公钥密码算法 第1部分：总则

GB/T 32918.2-2016 信息安全技术 SM2椭圆曲线公钥密码算法 第2部分：数字签名算法

GB/T 32918.4-2016 信息安全技术 SM2椭圆曲线公钥密码算法 第4部分：公钥加密算法

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 38645-2020 信息安全技术 网络安全事件应急演练指南

GB/T 39412-2020 信息安全技术 代码安全审计规范

GB/T 43698-2024 网络安全技术 软件供应链安全要求

GB/T 44464-2024 汽车数据通用要求

GB 50174-2017 数据中心设计规范

YD/T 3957-2021 基于LTE的车联网无线通信技术 安全证书管理系统技术要求

T/CSAE 295.1-2023 车路云一体化系统 第1部分：系统组成及基础平台架构

T/CSAE 313-2023 车路云一体化系统数据分类分级指南

3 术语和定义

GB/T 43698-2024、T/CSAE 295.1-2023界定的以及下列术语和定义适用于本文件。

3.1

云控平台 cloud control platform

由云控基础平台以及云控应用组成。云控基础平台汇聚车辆和道路交通动态信息，融合地图、交管、气象和定位等平台的相关数据，进行综合处理后，以标准化分级共享的方式支撑不同时延要求下的云控应用需求。在此基础上建立面向智能网联汽车产业的云控应用，为车辆增强安全、节约能耗以及提升区域交通效率提供服务。

[来源：T/CSAE 313-2023，3.7]

3.2

路侧基础设施 roadside infrastructure

部署在道路两侧及相关区域的用于支撑车路云一体化系统实现交通运行、信息交互和安全管控的各类设施的总称。

注：路侧基础设施信息安全关系到云控平台的边缘云设施安全和安全管控类设施安全。

3.3

软件供应链安全图谱 software supply chain security graph

对软件产品信息、软件物料清单（SBOM）、安全信息等内容及其关联关系的描述和表示。

注：一般以文本形式存储,支持通过知识图谱方式展示，增强软件供应链的可追溯性和可审计性。

[来源：GB/T 43698-2024，3.9，有修改]

4 缩略语

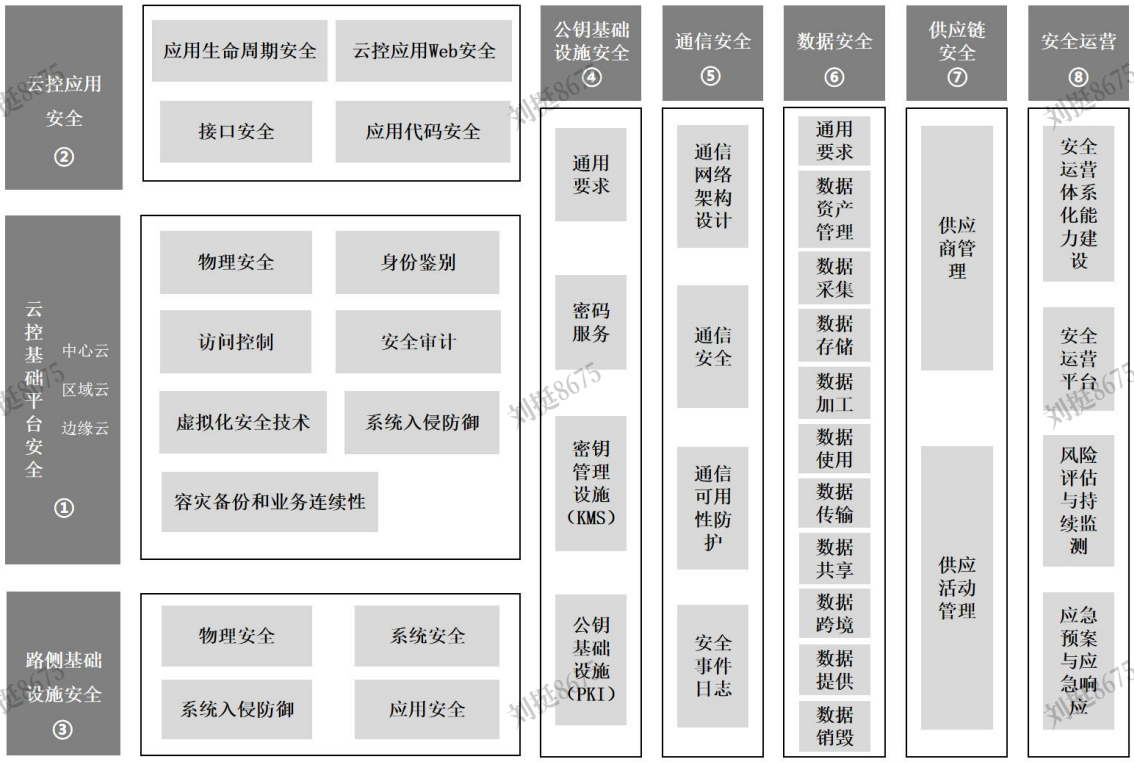
下列缩略语适用于本文件。

AES：高级加密标准（Advanced Encryption Standard）
API：应用程序接口（Application Program Interface)
CA：证书颁发机构（Certification Authority）
CoAP：受限应用协议（The Constrained Application Protocol）
CSRF：跨站请求伪造（Cross Site Request Forgery)
DDoS：分布式拒绝服务攻击（Distributed Denial of Service）
DES：数据加密标准（Data Encryption Standard）
DNS：域名系统（Domain Name System）
DoS：拒绝服务攻击（Denial of Service）
ECC：椭圆曲线密码学（Elliptic Curve Cryptography）
HTTPS：超文本传输安全协议（Hypertext Transfer Protocol Secure）
ICMP：互联网控制报文协议（Internet Control Message Protocol）
IDS：入侵防御系统（Intrusion Detection System）
IPS：入侵防御系统（Intrusion Prevention System）
ISP：互联网服务提供商（Internet Service Provider）
KMS：密钥管理系统（Key Management System）
LAN：局域网（Local Area Network）
MD5：消息摘要算法5（Message Digest Algorithm 5）
MQTT：消息队列遥测传输（Message Queuing Telemetry Transport）
OSC：开源软件委员会（Open Source Community）
OTA：空中下载技术（Over The Air）
PC5：近端通信（Proximity Communication）
PKI：公钥基础设施（Public Key Infrastructure）
RA：注册机构（Registration Authority）
RSA：公钥加密算法（Rivest-Shamir-Adleman Algorithm）
SBOM：软件物料清单（Software Bill of Materials）
SHA：安全哈希算法（Secure Hash Algorithm）
SLA：服务水平协议（Service Level Agreement）
SM2：椭圆曲线公钥密码算法（Public key cartographic algorithm SM2 based on elliptic curve）
SM3：密码杂凑算法（SM3 cartographic hash algorithm）
SM4：分组密码算法（SM4 Block Cipher）
TLCP：传输层密码协议（Transport Layer Cryptography Protocol）
TLS：传输层安全性协议（Transport Layer Security）

VA：验证机构（Validation Authority）
V2X：车联网无线通信技术（Vehicle to Everything）
WAF：Web应用防火墙（Web Application Firewall）
WLAN：无线局域网（Wireless Local Area Network）
XSS：跨站脚本攻击（Cross Site Scripting）

5 车路云一体化系统云控平台信息安全架构

车路云一体化系统云控平台信息安全架构包括云控基础平台安全、云控应用安全、路侧基础设施安全、公钥基础设施安全、通信安全、数据安全、供应链安全和安全运营的安全要求和证实方法，见图2。



注：此图中的编号代表各项内容主题在本文件中的章节顺序。

图 2 车路云一体化系统云控平台信息安全架构

6 安全要求

6.1 云控基础平台安全要求

6.1.1 物理安全要求

6.1.1.1 通用要求

云控基础平台的基础设施若使用公有云服务，应选择具备GB/T 22239-2019规定的安全等级3级及以上等保备案资质的云计算服务商。云控基础平台的基础设施若使用自建数据中心，机房选址及环境建设应符合GB 50174-2017中B级的相关规定。

6.1.1.2 物理访问控制和访客访问记录要求

物理访问控制和访客访问记录要求包括：

a) 应对数据中心进行合理的区域划分，区域划分应符合 GB 50174-2017 中 4.2 的相关规定，并设置安全隔离区，保证对外来人员有效的物理访问控制；
b) 应采用密码等鉴别技术进行物理访问身份鉴别，保证重要区域进入人员身份的真实性；
c) 应建立数据中心的访客访问记录并独立保存，访客记录信息包括：访客姓名、身份信息、访问缘由、访问时间、离开时间、所带物品工具、访客所在单位信息等，访问记录保存时间不应低于 180 天；应采用密码技术保证电子门禁系统进出记录数据的存储完整性。

6.1.1.3 物理环境监控记录要求

物理环境监控记录要求包括：
a) 应对数据中心机房内部及建筑物周边设置不间断运行的网络视频监控系统，监控系统应具备报警功能，视频监控数据应单独存储在与数据中心其它数据不同的位置，视频监控记录应至少保存 180 天；
b) 应采用密码技术保证视频监控音像记录数据的存储完整性。

6.1.1.4 电力系统安全要求

电力系统安全要求包括：
a) 系统设计建设应符合 GB 50174-2017 中 8.1 供配电的相关要求；
b) 应对电力系统的紧急断电装置进行保护，防止非授权或意外触发；
c) 应提供备份供电系统包括 UPS 和柴油发电机，防止停电造成整个数据中心宕机。

6.1.1.5 人员管理要求

人员管理要求包括：
a) 应设置系统管理员、审计管理员和安全管理员岗位，应明确各岗位在安全系统中的职责和权限，制定遵循三权分离原则的规定，包括岗位配置、职责授权和审计分离；
b) 应制定人员培训制度、保密制度和人员调离制度，明确各类安全系统相关管理人员离职、退休或换岗前移交规范；
c) 应制定人员考核制度，各类安全系统相关管理人员每年应接受单位的考核，考核不达标者应重新参加培训，考核严重不合格者应调离本岗位。

6.1.2 身份鉴别要求

身份鉴别要求包括：
a) 应确保所有的用户身份标识具备全局唯一性；
b) 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对登录的用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现；
c) 应要求登录的用户身份标识具有复杂度并定期（每 1 个月～3 个月）更换；
d) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；
e) 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。

6.1.3 访问控制要求

访问控制要求包括：
a) 应部署访问控制设备，如网闸、防火墙、路由器、交换机和无线接入网关设备等提供访问控制功能的设备或相关组件；
b) 应设置访问控制规则，默认情况下除允许通信外，受控接口拒绝所有通信；
c) 应定期（每 3 个月～6 个月）核查并删除多余或无效的访问控制规则；
d) 应定期（每 3 个月～6 个月）核查不同的访问控制规则之间的逻辑关系及前后排列顺序是否合理；
e) 应设定对源地址、目的地址、源端口、目的端口和协议等相关配置参数，以允许/拒绝数据包进出；
f) 应采用会话认证等机制，能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力；

g) 应验证设置的访问控制规则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；
h) 应对登录的用户分配账户和权限，确保用户只能访问其权限范围内的资源；并定期（每 3 个月～6 个月）对系统账户和权限进行进行审计和稽核。

6.1.4 安全审计要求

安全审计要求包括：

a) 应统一定义云控基础平台中的可审计事件，其中信息安全事件的定义应按照 GB/T 20986-2023 的规定对云控基础平台中的安全事件进行记录，应建立安全审计机制，对网络安全进行全面的监测和审计；
b) 应具备对系统中各软硬件设备在工作过程中产生的安全事件的审计能力，应启用安全审计功能，在网络边界、重要网络节点进行安全审计，确保审计记录内容的全面完整，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，审计内容包括事件类型、事件发生的时间、位置、事件采集来源、事件结论以及相关的主客体信息，针对车路云一体化系统的业务应用还应包括应用的会话、连接、活动、网络通信数据、主客体的各类指纹信息等；
c) 应建立基于国家权威授时中心提供的时钟同步系统作为全局日志生成的时间戳；
d) 应保证审计记录存储符合客户信息保存的要求，并保证审计数据的独立性、可靠性、可用性和安全性，应对审计记录进行保护，定期（至少每 6 个月）备份，避免受到未预期的删除、修改或覆盖等；
e) 应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析；并根据对审计记录的分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等；
f) 应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；
g) 应定期（至少每个月）组织相关人员对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施。

6.1.5 虚拟化安全技术要求

6.1.5.1 宿主机安全要求

宿主机系统应采用必要的身份鉴别、访问控制、剩余信息保护、入侵防御、恶意代码防范手段保护宿主机安全。

6.1.5.2 虚拟化计算安全要求

虚拟化计算安全要求包括：

a) 应对虚拟化监视器和虚拟化操作系统镜像进行完整性校验，确保系统未被篡改；
b) 应支持虚拟机之间、虚拟机和宿主机之间的安全隔离能力，包括 CPU、GPU、硬盘、内存等资源的隔离，确保某个虚拟机崩溃后不影响宿主机及其他虚拟机。

6.1.5.3 虚拟存储安全要求

虚拟存储安全要求包括：

a) 应采取措施对虚拟化中重要数据完整性进行保护，确保系统未被篡改；
b) 系统虚拟化安全应保证镜像文件完整性、可用性和保密性；
c) 应支持对虚拟磁盘进行加密；
d) 应支持虚拟化的冗余数据保护能力，包括内存、存储空间、镜像、快照等资源完全清除回收；
e) 存储虚拟化安全应保证安全控制方法对逻辑存储设备和物理存储设备都有效。

6.1.5.4 虚拟网络安全要求

虚拟网络安全要求包括：

a) 应保证关键网络设备及虚拟化网络设备的业务处理能力具备冗余空间，满足业务高峰期需要；
b) 应能监控虚拟机之间、虚拟机与宿主机之间的流量；

c） 应支持网络安全域划分，确保虚拟机之间的网络安全隔离；
d） 应避免部分虚拟机对虚拟机网络资源的过度占用以及网络故障影响其他虚拟机的正常使用。

6.1.5.5 虚拟化管理安全要求

虚拟化管理安全要求包括：
a） 应具备对其系统虚拟化中的虚拟主机进行实时监控其运行状态、资源占用、网络负载等能力；
b） 应提供虚拟资源管理员权限分离机制，例如系统管理员、安全管理员、审计管理员等不同的管理员账户；
c） 云控基础平台的虚拟化管理平台的管理员按职能分割和最小授权原则，并形成相互制约、监督的关系；
d） 应支持在外部网络中对虚拟机管理平台和虚拟机的入侵行为进行检测，并在发生入侵事件时提供告警；
e） 应支持对虚拟化内部发起的攻击检测和防护能力，检测出发起攻击的虚拟机，并能记录攻击类型、攻击时间、攻击流量；
f） 云控基础平台的容器安全服务应提供镜像漏洞管理、容器安全策略管理功能，解决传统安全软件无法感知容器环境的问题；
g） 应提供容器进程白名单、文件只读保护和容器逃逸检测功能，有效防止容器运行时安全风险事件的发生。

6.1.6 容灾备份和业务连续性要求

6.1.6.1 业务系统备份要求

业务系统备份要求包括：
a） 应制定完善的系统级的备份方案，内容至少应包括定义备份间隔、备份方式和数据格式、验证备份数据完整性的方法以及恢复备份数据的操作规程等；
b） 应具备对各业务应用系统的状态、操作系统、应用数据定期（至少每 12 个月）备份和恢复的能力，备份时间间隔以业务的关键性为依据可按分钟、小时或天为单位；
c） 在备份业务应用的过程中应保护应用数据不可任意读取；
d） 应保证业务应用的备份数据的完整性、保密性和可用性；
e） 应针对关键业务配置异地系统备份系统，并根据其重要性确定备份方式（增量、全量）和间隔；
f） 应定期（至少每 12 个月）测试灾难恢复计划的可行性，包括从备份恢复数据的可恢复性、验证系统完整性以及验证备用设备的可用性。

6.1.6.2 业务连续性要求

业务连续性要求包括：
a） 系统管理员应定期（至少每 12 个月）开展针对云控业务连续性的风险分析，包括云控基础平台计算平台服务失效、ISP 网络连接中断、业务应用组件服务终止等，并将相关的风险信息告知系统运营方；
b） 系统管理员将应急响应计划、灾难恢复计划及支撑系统运营方实施业务连续性计划的有关措施告知系统运营方，并根据系统运营方的业务连续性计划的需要，对应急响应计划、灾难恢复计划进行调整；
c） 应保障系统冗余与高可用性，使用冗余的硬件、网络和系统组件，确保在关键设备或系统故障时能够无缝切换到备用设备；
d） 应定期（至少每 12 个月）审查和管理供应链安全，确保关键供应商和合作伙伴的网络安全措施符合要求。

6.1.7 系统入侵防御要求

入侵防御要求包括：
a） 应部署 IDS/IPS 设备对系统进行防护，确保其覆盖关键网络节点（如网络边界、数据中心入口等）；

b) 应具有实时收集流入目标网络内所有数据包的能力，以采集、识别、特征提取等方式，检测访问过程的安全性；
c) 能鉴别数据的新鲜性，避免历史数据的重放攻击；
d) 能发现躲避或欺骗检测的行为；
e) 能发现从内部发起的攻击行为；
f) 应对发现的入侵行为进行预先拦截，防止入侵行为进入目标网络，并及时发送安全警告；
g) 能对高频度发生的相同安全事件进行合并报警，具备避免出现报警风暴的能力；
h) 应将拦截行为生成审计记录，并保留与入侵事件相关的要素信息；
i) 应关闭不需要的系统服务，默认共享和高风险端口；
j) 应定期（至少每 12 个月）开展漏洞扫描工作，及时发现可能存在的漏洞，并在经过充分测试评估后，及时修补漏洞；
k) 能检测到对重要节点进行入侵的行为，并在发生严重入侵事件时报警；
l) 应严格对外来介质设备实行管控，并对各类硬件设备的外接存储接口进行限制或移除。

6.2 云控应用安全要求

6.2.1 应用生命周期安全要求

6.2.1.1 通用要求

云控应用安全应覆盖云控应用的生命周期进行全面安全管理，包括对云控应用的设计、开发、部署、测试、发布、调用、停用等环节分析安全问题，设计合理的云控应用的生命周期管理机制，解决管理过程中遇到的安全问题。

6.2.1.2 设计阶段

云控应用设计阶段安全要求包括：
a) 应明确云控应用的安全需求，包括身份验证、授权、数据保护和操作审计；
b) 定义安全架构，包括网络拓扑、安全层次结构和隔离策略；考虑业务流程的连贯性和可用性，同时确保安全性。

6.2.1.3 开发阶段

云控应用开发阶段安全要求包括：
a) 应保证云控应用代码安全符合 6.2.4 的要求；
b) 应确保云控应用开发文档的完整和保密。

6.2.1.4 部署阶段

云控应用部署阶段安全要求包括：
a) 应配置服务器和网络安全设备，以确保云控应用程序的安全性，包括网络防火墙、入侵防御系统、WAF、负载均衡、数据库防火墙等；
b) 应确保运行环境的隔离，以防止云控应用程序被其他应用程序或系统影响；
c) 应及时更新和修补云控应用程序披露的漏洞。

6.2.1.5 测试阶段

应对云控应用进行安全性测试，包括渗透测试、漏洞扫描和安全性评估。

6.2.1.6 发布和调用阶段

云控应用发布和调用阶段安全要求包括：
a) 应通过有效的工具或手段对云控应用的版本进行控制，确保只有受信任的版本被部署和调用；
b) 应为调用者提供安全的 API 接口和文档，调用 API 接口应进行有效的身份验证、授权要求和日志记录。

6.2.1.7 停用阶段

云控应用停用阶段安全要求包括：

a) 对于不再需要的云控应用程序，应分析其停用后的影响范围，在确保不影响其他业务的前提下安全地停用或卸载；
b) 应确保处理数据的安全销毁或迁移，确保敏感信息不被泄露。

6.2.1.8 持续改进

在整个生命周期中，应不断改进云控应用软件的安全性，监测应用软件的安全事件和漏洞并进行处置和修复。应建立安全运营体系定期（至少每12个月）更新安全政策、流程以适应新的威胁和技术。

6.2.2 云控应用 Web 安全要求

6.2.2.1 Web 服务器安全要求

云控应用Web服务器安全应包含针对Web服务器攻击的防御处理，包括：

a) 应通过使用预编译语句和存储过程，严格检查用户数据等技术手段来预防 SQL 注入攻击；
b) 应采用相关技术手段，排查 Web 服务器相关的漏洞所造成的问题，如 Apache、IIS、Nginx 等 Web 服务器的文件解析漏洞，防止文件上传漏洞；
c) 应通过判断当前用户身份和校验用户权限级别，来防止水平和垂直越权的权限漏洞；
d) 应采用定期（每 1 个月～3 个月）修改强密码，限制密码错误次数等措施来防止暴力破解；
e) 应针对 Web 层、客户端及 APP 拒绝服务攻击，采取相应的技术措施，包含限制每个客户端的请求频率，使用验证码过滤自动攻击，优化应用代码的性能、网络架构等；
f) 应对数据接口进行权限检查和访问限制，划分企业应用安全边界，限制内部数据外流等，防止敏感信息泄露；
g) 应针对业务场景进行全面检测，防止业务漏洞；
h) 应检查所有可能存在安全配置缺陷，在满足业务需求的情况下，最大化安全配置。

注：Web服务器攻击主要包含利用Web服务器的漏洞进行攻击，如IIS缓冲区溢出漏洞利用、目录遍历漏洞利用等，以及利用网页自身的安全漏洞进行攻击，如SQL注入、跨站脚本攻击等。

6.2.2.2 Web 客户端安全要求

云控应用Web客户端安全要求包括：

a) 应采取相应措施来防止反射型跨站脚本攻击（XSS）攻击、存储型 XSS 攻击、DOM 型 XSS 攻击等，如检查 Cookie 字段使用情况，所有用户可控输入等；
b) 应通过辅助验证方法，通用防护方法，其他防御措施（验证 HTTP Referer，拒绝不安全的来源）等，防止跨站请求伪造（CSRF）。

6.2.2.3 Web 通信信道安全要求

云控应用Web通信信道安全，主要包含云与车交互、云与路交互及云与云交互之间的通信安全，应满足以下要求：

a) 应采用安全通信协议保证通信协议自身安全，如采用 TLCP、TLS1.2 及以上等协议进行传输层安全保护；
b) 应采用基于国密算法的密码技术等对通信数据进行保密性和完整性保护；
c) 面向车载终端设备和其他智能交通参与终端提供应用服务，通过车联网无线通信技术进行信息交互时，应采用 V2X 通信证书确保其通信安全，V2X 通信证书应符合 YD/T 3957-2021 内容描述。

6.2.3 接口安全要求

6.2.3.1 端侧设备接入安全要求

云控平台可使用开放协议（HTTPS、MQTT、CoAP等）自主接入路侧基础设施、车载终端设备以及其他交通参与者携带的智能终端设备等端侧设备。端侧设备接入云控平台应满足以下要求：

a) 应通过身份鉴别技术控制设备接入权限，身份鉴别技术应采用设备密钥、X.509 证书等技术；

b) 应采用安全的 TLCP、TLS 加密传输协议确保通信安全，信息交互内容宜进行加密处理，如使用 TLCP 协议，应符合 GB/T 38636 的规定；
c) 应采用密码技术等对通信数据进行完整性保护；
d) 应通过指定安全策略如访问控制列表，实现对接入设备的访问控制，在设备接入云控平台时，应根据安全策略对接入设备进行权限检查；
e) 应对设备接入过程进行审计，并记录接入设备的身份标识、接入时间、接入类型等内容。

6.2.3.2 相关支撑平台接入安全要求

相关支撑平台接入云控平台要求包括：
a) 云控平台与相关支撑平台使用 HTTPS 和 WebSocket 协议进行信息交互时，应采用 OAuth2.0、数字证书等方式进行认证；
b) 云控平台与相关支撑平台使用 MQTT 协议进行信息交互时，应采用安全的 TLCP、TLS 的方式进行认证；
c) 应采用安全的 TLCP、TLS 等加密传输协议确保通信数据保密性要求；信息交互内容宜进行加密处理；
d) 信息交互内容宜采用密码技术对通信数据进行完整性保护；
e) 云控平台应负责管理、维护对相关支撑平台的接入授权；接口在接入时应告知云控平台是否需要授权，若必须授权，则应告知接口的授权范围。

6.2.4 应用代码安全要求

云控应用代码安全要求包括：
a) 为保障云控应用的安全，应对在云控平台上集成开发的云控应用在发布之前进行代码审计，识别云控应用的代码缺陷、安全缺陷以降低云控应用安全风险；
b) 云控应用代码审计应包括内部审计和外部审计，其中内部审计是对云控平台内部开发人员开展安全审计，外部审计是组织具备资质的第三方专业代码审计机构对云控应用开展审计；
c) 云控应用的代码审计工作应体系化，至少应包括 4 个阶段，即准备、实施、报告和持续跟踪等活动；
d) 云控应用代码审计内容至少应包括安全功能缺陷审计、应用代码实现安全缺陷审计、应用资源使用安全缺陷审计、应用环境安全缺陷审计等；
e) 云控应用安全功能缺陷审计应符合 GB/T 39412-2020 第 6 章中的规定；
f) 云控应用代码实现安全缺陷审计应符合 GB/T 39412-2020 第 8 章中的规定；
g) 云控应用环境安全缺陷审计应符合 GB/T 39412-2020 第 9 章中的规定。

6.3 路侧基础设施安全要求

6.3.1 物理安全要求

6.3.1.1 物理环境安全要求

路侧基础设施根据设施类型差异，应已通过防静电、防水、震动、电磁防护等测试，确保设施具备一定的外场环境适应性。

6.3.1.2 硬件安全要求

硬件安全要求包括：
a) 硬件不应存在后门或隐蔽接口；
b) 硬件的调试接口应禁用或设置安全访问控制；
c) 路侧基础设施应采用密码模块，且与设施有绑定关系，防止恶意拆解。

6.3.2 系统安全要求

6.3.2.1 安全启动要求

路侧基础设施应具备可信环境，保障操作系统的引导与加载安全，保护系统固件不被篡改，或确保被篡改后无法正常启动。

6.3.2.2 身份认证与鉴别要求

身份认证和鉴别要求包括：

a) 使用口令鉴别方式时，应支持首次管理设备时强制修改默认口令或设置口令，支持设置口令生存周期，支持口令复杂度检查等功能；口令应不低于 8 位，并包括英文大小写、数字和特殊字符；
b) 应具备可用于通信识别的唯一标识，可采用设备 ID、序列号、MAC 地址等；基于唯一标识进行身份认证和鉴别；
c) 应具备登录失败处理能力，限制非法登录次数。

6.3.2.3 访问控制要求

访问控制要求包括：

a) 应对不同的用户设置不同的账户和权限；
b) 应依据访问数据的不同类型与安全级别设计不同的访问控制策略；
c) 应仅开启默认状态下必要的服务和端口，且明示所有默认开启的服务、对应的端口及用途；非默认端口和服务，应由系统运营方评估并授权后方可开启；
d) 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许或拒绝数据包进出；
e) 应严格对 USB 设备、TF 设备等外部存储设备的管控，禁止非授权用户访问；
f) 在远程管理过程中，应使用安全的通信协议，登录超时时应自动退出。

6.3.3 系统入侵防御要求

系统入侵防御要求包括：

a) 部署入侵防御系统对系统进行防护；
b) 能够识别并记录密码爆破攻击、拒绝服务攻击、畸形报文攻击等攻击行为的日志；
c) 应对高频度发生的相同安全事件进行合并上报，避免出现告警风暴；
d) 安全事件信息至少包含事件发生时间、源地址、目的地址、事件等级、事件类型、事件名称、事件详细描述。

6.3.4 应用安全要求

应用安全要求包括：

a) 不应存在行业权威漏洞平台上发布的 6 个月及以上中高危安全漏洞；
b) 应用软件不应含有非授权收集或泄露用户信息、非法数据外传等恶意行为，不应以明文的形式存储用户敏感信息，如用户口令、私钥、证件号等，不应携带调试信息；
c) 软件应使用安全机制（例如混淆、加壳），对抗针对应用的逆向分析；
d) 应用软件升级前，应当立即对其执行真实性和完整性检查，并对未通过验证的升级包执行有效处置；
e) 应用软件升级时，应支持升级过程中断时的续升功能，或支持升级失败时的自动回滚功能，防止设备功能失效；
f) 应在升级成功后，擦除缓存中的升级包镜像和文件中的敏感信息并完成自检；不论升级成功与否，都应对升级过程记录日志，并采取适当的访问控制机制管理日志读取和写入的权限。

6.4 公钥基础设施安全要求

6.4.1 通用要求

公钥基础设施安全通用要求包括：

a) 公钥基础设施应采用密码基础设施提供密码相关服务，密码基础设施包括密码服务设施、密钥管理设施（KMS）和公钥基础设施（PKI），为云控基础平台、云控应用、路侧基础设施、通信

安全和数据安全等业务提供基于密码学为基础的数据加解密、数字签名、身份认证、数据完整性、 非抵赖性等安全服务；

b) 密码服务设施应采用基于国密算法（如 SM2/SM3/SM4/AES/ECC/RSA）进行设计，至少确保包含对称加密、非对称加密、签名验签的服务，并对密钥进行全生命周期安全管理；

c) 应建立数字证书管理系统，为云控平台内的网络和应用提供完整性、保密性、唯一性、不可抵赖性等相关安全特性的密码支撑；

d) 应建立密钥管理系统（KMS），为云控平台提供数据加密、OTA 升级等场景的密钥全生命周期安全管理；

e) KMS 的搭建应遵守 GB/T 17901.1-2020、GB/T 17901.3-2021 的要求进行；

f) PKI 的搭建理应遵守 GB/T 21053-2023 的要求进行。

6.4.2 密码服务要求

6.4.2.1 对称加密要求

对称加密要求包括：

a) 对称加密算法应支持 SM4 算法；SM4 算法应按照 GB/T 32907-2016 进行算法实现；SM4 算法应采用 128 bits 的密钥长度和分组长度，加密算法与密钥扩展算法都应采用 32 轮的密钥结构；

b) 如果对称算法采用 AES 算法，密钥长度应≥256 bits，加密的轮次应≥10 次；

c) 不应采用 DES 等已被证实不安全的加密算法。

6.4.2.2 非对称加密要求

非对称加密要求包括：

a) 非对称加密算法应支持 SM2 算法；SM2 密钥应按照 GB/T 32918.1-2016 进行算法实现；SM2 参数的选取应按照 GB/T 32918.1-2016 第 5 章的方式进行验证；使用 SM2 公钥进行加密时，应按照 GB/T 32918.4-2016 对公钥加密算法进行实现；

b) 如果非对称加密算法选用 ECC 算法，ECC 加密算法的密钥长度应≥256 位。

c) 如果非对称加密算法选用 RSA 算法，RSA 加密算法的密钥长度应≥2048 位。

6.4.2.3 签名验签算法要求

签名验签算法要求包括：

a) 签名验签算法应支持基于 SM2 的签名算法,SM2 算法应符合 6.4.2.2 中对 SM2 的规定;基于 SM2 的签名验签算法，按照 GB/T 32918.2-2016 的规定使用 SM3 作为杂凑算法进行实现，对于其中的 DIST ID 的选取，在云控基础平台没有特殊要求的情况下，应采用默认值。

b) 如果使用 ECC、RSA 进行签名验签算法的实现，应采用不产生碰撞情形的杂凑算法如 SHA256、SHA512 等。

6.4.3 KMS 要求

6.4.3.1 密钥生成要求

密钥在生成时应基于真随机数，保证生成密钥的不可预测性。

6.4.3.2 密钥储存要求

对于非对称密钥的储存，应保证私钥不能外泄，不应将私钥进行明文储存。对于储存的密钥，应定期（每1个月～3个月）进行更新。对于私钥的储存，应采用以下形式：

a) 使用具有安全等级认证的物理加密设施储存；

b) 使用密钥进行加密，密钥本身存于加密设备中；

c) 使用口令密码进行加密。

6.4.3.3 密钥分发要求

密钥的分发应通过KMS中的密钥分发服务完成，在进行密钥的分发时，应基于PKI系统中密钥请求方的数字证书进行请求方身份的认证和密钥的加密传输。

6.4.3.4 密钥撤销要求

当密钥被泄漏或过期时，应立即启动密钥撤销流程。撤销后的密钥应遵循以下原则：

a) 停止所有新用途：撤销后的密钥不应用于新的加密或签名操作，以防止进一步的安全风险；
b) 限制解密和验签操作：撤销后的密钥仅在必要时用于解密已加密数据或验证已签名数据，且应在严格控制的环境中进行（例如，仅在法律合规、审计或数据恢复等必要场景中使用）；
c) 实施访问控制：对撤销密钥的使用进行严格限制，仅授权特定人员或系统在特定条件下访问，并记录所有使用情况以备审计；
d) 安全存储与隔离：撤销后的密钥应与活跃密钥隔离存储，并确保其安全性和不可篡改性；
e) 定期（每 1 个月～3 个月）清理：撤销后的密钥应在完成所有必要的解密或验签操作后，根据安全策略进行安全销毁，以彻底消除安全风险。

6.4.3.5 密钥销毁要求

密钥需要销毁时，除去密钥本身，还应将密钥的备份进行销毁。

6.4.4 PKI 要求

PKI系统的基本架构见图3，PKI平台应至少保证具备以下模块：

a) RA：与云控基础平台的用户进行交互，将云控基础平台的证书申请请求转发至 CA；
b) CA：管理 PKI 中的证书的状态，可对证书进行颁发、冻结、解冻和撤销，将证书状态同步至 RA 与 VA；
c) VA：提供证书状态的查询接口，用于验证证书是否有效；
d) KMS：用于管理 PKI 系统中的私钥，保证私钥不可泄漏；
e) 审计模块：用于审计系统中的事件。

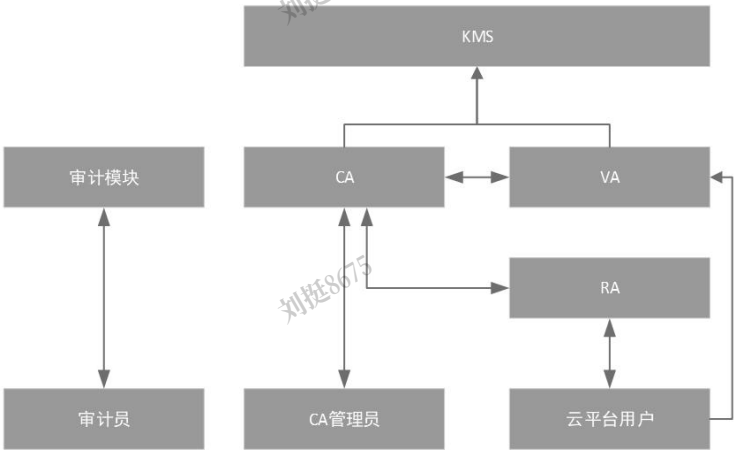


图 3 PKI 系统的基本架构

PKI系统在进行证书的管理或审计时，应使用CA管理员口令或审计员的口令保证操作的安全性，对于PKI系统中的口令，应保证长度为8字节以上，且为数字、字符、字母的混合体。

6.5 通信安全要求

6.5.1 通信网络架构设计要求

通信网络架构设计要求包括：

a) 应在网络架构设计时充分考虑安全因素，应按照 GB/T 22239-2019 中 8.1.2、8.2.2 的要求设计网络；
b) 应具备边界保护能力，在外部边界和内部关键边界实施通信监控；
c) 应在逻辑层面实现网络隔离，具备区分允许外部人员访问的组件与允许客户访问的组件的能力。

6.5.2 通信安全要求

通信安全要求包括：

a) 云控基础平台与车载终端设备、路侧基础设施通信过程中，应采用密码技术保证传输数据的保密性，使用校验技术或密码技术保证数据的完整性；应使用安全的通信协议，例如 TLCP、TLS 1.2 或 TLS1.3 等，保障通信数据的机密性和完整性；在安全协议中应采用使用数字证书进行双向身份认证，保障接入方与平台的身份真实合法；

b) 车辆与路侧基础设施的直连通信过程中，应满足 YD/T 3957-2021 的要求，对收发数据进行签名和验签；应采用安全机制保障通信数据的真实性和完整性，在证书验证过程中，应采用使用 YD/T 3957-2021 中规定的应用证书或假名证书进行证书有效性和合法性的验证；

c) 云控基础平台、车载终端设备、路侧基础设施采用的电子认证服务，应经商用密码认证机构认证合格方可使用；

d) 外界通过蓝牙、DSRC、WLAN、LAN 等发起通信连接时，路侧基础设施应进行身份鉴别和授权管理，在未经授权的网络设备接入时，具备发现和告警的功能；

e) 应对车路云数据传输过程中的异常情况进行监控告警，如异常大量数据传输、不明来源的传输请求等，并做好日志记录。

6.5.3 通信可用性防护要求

通信可用性防护要求包括：

a) 云控基础平台、车载终端设备、路侧基础设施应实现对各类基于网络通信协议的 DOS/DDOS 等常见网络攻击行为有效识别；

b) 当平台检测到 DOS/DDOS 时，应确保自身正常的功能和预先设定的性能不受影响，并对检测到的攻击数据包进行丢弃或者记录日志；

c) 云控基础平台、车载终端设备、路侧基础设施应实现对恶意数据包的识别；当检测到恶意数据包时，应确保自身正常的功能和预先设定的性能不受影响，并对检测到的攻击数据包进行丢弃或者记录日志；

d) 云控基础平台应具备面向网络出入口的恶意代码防护能力，应建立相应维护机制，确保恶意代码防护机制得到及时更新，如升级病毒库；应及时对恶意代码告警记录进行检查和分析。

注：各类基于网络通信协议的 DOS/DDOS 等网络攻击包括 SYN Flood、ACK Flood、FIN/RST Flood、TCP Flood、UDP Flood、ICMP Flood、DNS 反射攻击等。

6.5.4 安全事件日志要求

云控基础平台应对关键的通信安全事件进行日志记录，确保数据不可被篡改和伪造，且可追溯。

6.6 数据安全要求

6.6.1 通用要求

车路云一体化系统的数据安全应满足以下通用要求：

a) 在数据收集、存储、传输、使用、加工、传输、共享、跨境、提供和销毁等环节中涉及个人信息安全应满足 GB/T 35273-2020 的要求；

b) 系统运营方应建立数据安全管理体系，应覆盖数据全生命周期，应制定数据收集、存储、使用、加工、传输、共享、跨境和销毁等环节的具体分级防护要求和操作规程；

c) 应根据 T/CSAE 313-2023 的要求建立车路云一体化系统数据分级分类制度，形成数据资产管理台账；

d) 应建立数据安全风险管理制度，覆盖风险管理与事件处置机制，及时排查安全隐患；发生数据安全事件时，应立即采取处置措施，有效降低影响；

e) 系统管理员应定期（至少每 12 个月）开展车路云一体化系统数据安全风险评估工作；若涉及重要数据处理，需向属地主管部门报送风险评估报告；

f) 应采集路侧基础设施、云控基础平台的数据风险事件，并提供数据安全事件的预警，以便数据安全事件得到及时处置；

g) 系统管理员应按照 GB/T 28827.3-2012 的规定建立数据安全事件应急预案和应急响应机制，对各类数据安全事件进行及时响应和处置以及进行事后的总结改进；若发生涉及重要数据的安全

事件，应第一时间向属地主管部门报告，并在事件处置完成后在规定期限内上报处置情况；对可能损害用户合法权益的数据安全事件，应当及时告知用户，并提供减轻危害措施。

6.6.2 数据资产管理要求

车路云一体化系统在数据资产管理方面应满足以下要求：

a) 宜建立自动化数据资产分类分级的能力，支持通过数据库探测自动盘点数据资产并开展数据分级分类，及时发现并管理车路云一体化系统中新增的一般、重要及敏感数据资产；
b) 应具备对于密钥类数据资产在生存周期（生成、存储、使用、分发、更新、销毁等）内的安全管理能力。

6.6.3 数据采集安全要求

车路云一体化系统可按需收集各类接入设备的设备基础数据、设备运行状态数据和设备业务相关数据。车路云一体化系统在数据收集方面应满足以下安全要求：

a) 在收集外部资源等相关数据过程中，应明确收集数据的目的和用途、范围、期限和频次，确保数据收集的时效性和最小必要等原则要求；
b) 应对收集数据的数据源进行身份鉴别和记录，防止数据仿冒和数据伪造；
c) 应采用支持数据格式的标准化、规范化收集；
d) 应对收集的数据进行分类分级标识，根据标记可对数据安全等级进行识别，应按照数据级别确定并实施必要的安全管理策略和保障措施。

6.6.4 数据存储安全要求

车路云一体化系统在数据存储方面应满足以下安全要求：

a) 应采用有效校验技术和密码技术确保重要数据存储过程中的完整性，并在检测到完整性错误时采取必要的恢复措施；
b) 应依据最小够用原则存储数据，不应以任何形式存储非业务必需的数据；
c) 应明确数据存储的有效期，存储时间应为业务必需的最短时间，支持对数据存储时效性配置；
d) 应具备定期的数据备份和恢复功能，实现对存储数据的冗余功能，具备数据备份后进行可用性、完整性校验的功能；
e) 重要数据应存储在安全区域或以密文形式存储，应具备重要数据异地保护功能，确保重要数据的机密性、完整性和可用性。

6.6.5 数据加工安全要求

车路云一体化系统在数据加工方面应满足以下安全要求：

a) 在数据加工过程中应具备实时监测的功能，避免数据在加工过程中丢失、窃取、篡改，具备对数据溯源的功能，确保所有数据的流向都可追溯；
b) 通过在数据加工过程中采取适当的安全控制措施，防止数据挖掘、分析过程中有价值信息和个人隐私泄露的安全风险；
c) 数据加工过程中的算法提供者应对算法的安全性和可靠性，提供必要的验证与测试方案，确保算法使用的数据范围、周期、目的以及结果的应用范围等安全可控。

6.6.6 数据使用安全要求

车路云一体化系统在数据使用方面，应满足以下安全要求：

a) 应遵循最小化原则制定数据访问控制措施；应对不同角色的使用场景和使用规则进行区分，并配套建立审批授权机制，采用技术手段支持审批流程，并记录重要数据日志；应通过技术手段限制数据使用者的读写权限，只有获得相应的读写权限才可对数据进行操作使用，如读、 写、删、改等；
b) 应对重要及以上等级数据调用、流转过程进行监测，将访问账号、应用的访问和操作过程等详细记录在重要数据日志中，支持审计工作，并能够监测识别可疑的访问操作行为如大量数据下载、频繁调用、非预期时间内的访问，一旦发现异常行为，应及时响应告警，通知安全人员进行调查和应对，防止数据被恶意滥用造成损失；日志不可篡改和伪造，且可追溯；

c) 涉及处理个人数据时在使用前应去标识化、脱敏处理；
d) 应对数据挖掘、关联分析、访问读取等数据使用行为采取审计技术，审计信息保留期限不少于6个月。

6.6.7 数据传输安全要求

车路云一体化系统在数据传输安全方面应满足6.5.2的要求。

6.6.8 数据共享安全要求

车路云一体化系统在数据共享方面应满足以下安全要求：
a) 应与数据接收方在订立的相关合同中明确需承担的责任，明确数据接收方处理数据的目的、方式、范围，确保数据共享行为的合法、正当、必要；如有法律法规和管理规定要求，应向监管部门报备；
b) 数据共享接口的管理应符合 6.6.10 a)的要求；
c) 应具备对数据共享过程的实时监控能力和应急响应机制，采用必要的隐私计算技术对数据进行保护，做到数据共享可用而不可见；
d) 数据共享过程审计和记录应符合 6.6.10 b)的要求。

6.6.9 数据跨境安全要求

车路云一体化系统数据跨境方面，涉及降密、脱敏及去隐私后应满足以下安全要求：
a) 境内收集和产生的数据应在中华人民共和国境内存储与使用；
b) 存在向境外或在华外商投资企业及组织在线传输或离线拷贝车路云一体化系统数据行为或计划的，依据《数据出境安全评估办法》，必须依法申报数据出境安全评估。

6.6.10 数据提供安全要求

车路云一体化系统在数据提供方面应满足以下安全要求：
a) 应对数据提供的接口进行规范管理，管理内容包括数据共享接口类型、加密方式、传输周期、数据接收方的名称、联系方式、处理目的、处理方式、数据类别、数据级别、数据规模、使用用途、认证方式；
b) 应支持对数据提供过程进行审计并记录数据提供的过程状态，如提供时间、提供数据内容、数据接收方等，确保数据提供行为的可追溯。

6.6.11 数据销毁安全要求

车路云一体化系统提供者在数据销毁方面应满足以下安全要求：
a) 应建立数据销毁策略、明确销毁对象并规范销毁流程；
b) 应根据数据分类分级建立相应的数据销毁机制，明确不同数据类型的销毁方式和销毁要求；
c) 应配置必要的数据销毁工具，保证销毁后的数据不可再逆向恢复，防止因对存储介质中的数据内容进行恶意恢复而导致的数据泄漏风险。

6.7 供应链安全要求

6.7.1 供应链安全管理通用要求

a) 系统运营方应对云控平台中的软件资产进行识别，宜对软件资产按照等级进行分类，见 GB/T 43698-2024 附录 B；
b) 系统运营方宜确定云控平台中的各软件系统的重要性等级，见 GB/T 43698-2024 附录 C；
c) 系统运营方应遵循 GB/T 43698-2024 中 6.2 的要求构建软件供应链安全图谱并维护云控平台软件供应链安全图谱保持数据更新；
d) 系统运营方应明确云控平台软件供应链风险管理的范围和对象；
e) 系统运营方应定期（至少每 12 个月）对云控平台软件供应安全开展风险评估和安全检测。

6.7.2 供应商管理要求

a) 系统运营方应遵循 GB/T 43698-2024 中 7.1.4 的要求对供应商进行管理；

b） 系统运营方应保证供应商提供的供应信息的准确真实、完整可信，并采取措施保护信息不被篡改和泄露；
c） 系统运营方应要求供应商配合开展供应链安全监督和检查。

6.7.3 供应活动管理要求

6.7.3.1 知识产权管理要求

知识产权管理要求包括：
a） 系统运营方与供应商应充分了解双方的知识产权情况；如有必要，双方应采用单独签订知识产权相关合同，确保不被侵犯；
b） 系统运营方应同供应商在合同中明确知识产权权属情况、知识产权保护措施、知识产权风险承担责任等内容，防止不当使用、披露和窃取知识产权的行为；应约定供应商不得侵犯第三方的知识产权，不得提供非法获取的技术资料和信息；
c） 系统运营方与供应商合作过程中，应采用建立知识产权保护机制，包括~制定知识产权保护策略。

6.7.3.2 外部组件使用要求

外部组件使用要求包括：
a） 应禁止系统管理员使用难以验证来源的开源及第三方组件；
b） 应通过合同条款要求供应商承诺所使用的开源软件、第三方组件、自有软件在交付前应对已公开漏洞进行及时修复并持续对上述开源软件、第三方组件、自有软件在使用期间进行及时的漏洞管理；
c） 应与供应商应建立开源软件、第三方组件、自有软件的入库和使用审批机制，对开源软件、第三方组件、自有软件在入库前需进行完整性验证、安全性测试和依赖关系分析，保障来源可靠、风险可控；
d） 系统管理员与供应商应记录和保留开源软件、第三方组件、自有软件的供应方、OSC 以及主要开发贡献者等相关信息，保障可追溯性；
e） 系统管理员与供应商应持续跟踪所使用的开源软件、第三方组件、自有软件的使用状态、安全状态，对于存在安全风险的，应及时通报，对被识别为关键信息基础设施的云控应用，一旦开源软件、第三方组件、自有软件出现严重漏洞且无法及时修复的，应提前制定可替代方案。

6.7.3.3 交付要求

交付要求包括：
a） 云控平台运营方应根据协议要求对交付的产品或服务进行验收，为确保供应链符合安全要求，应对供应关系、供应活动进行评估分析，包括功能缺陷分析、服务断供风险分析、软件安全漏洞分析等安全风险分析；
b） 系统运营方应掌握第三方软件相关技术资料，包括中文版运行维护、二次开发、工具产品的使用场景和条件、权限和授权机制、工具产品使用说明书及测试报告等；
c） 系统运营方应确保供应商在交付产品或服务后，提供必要的技术支持和服务，包括系统的运行维护、升级更新、故障排查等，为满足特定的业务需求或技术要求而进行修改、扩展或增加新功能等操作，以确保它们不会对原始系统的功能产生负面影响；应该考虑安全性、可靠性、性能和可维护性等方面的因素，以确保开发的软件系统能够满足用户的需求，并能够在实际环境中稳定运行；
d） 系统运营方应要求供应商交付的产品符合交付范围要求，包括不能捆绑其他工具，不在产品中设置后门，不能利用软件产品的便利条件非法获取用户和系统数据，不可利用产品的依赖性谋取不正当利益，不得在未授权和提前告知的情况下对产品进行升级或更新换代；
e） 系统运营方应针对云控平台建立安全基线标准，并要求供应商对交付的软件实行安全基线配置，不符合云控平台相应安全基线的系统和产品无法上线；
f） 系统运营方宜要求供应商对交付的软件出具由第三方机构测试通过的功能、性能、完整性、安全性测试报告；

g) 系统运营方与供应商应注意信息保密，应通过保密协议约定供应链信息的知悉范围并严格履行各自责任义务；
h) 系统运营方应通过有效的合同条款管理供应商确保所交付的产品或服务的质量和安全性，符合国家和行业的标准及规范，不得存在质量缺陷或安全隐患；
i) 系统运营方应建立完善的安全管理制度，采取严格的安全措施和防范手段，确保供应链的安全稳定运行，并将供应商纳入管理体系，确保双方加强沟通和协作，及时通报和解决安全风险和问题，共同维护系统的安全稳定运行。

6.8 安全运营要求

6.8.1 安全运营体系化能力建设要求

安全运营体系化能力建设要求包括：
a) 应加强管理保障供应链安全的能力；
b) 应具备分级化管理的能力，能够对边缘云、区域云和中心云按照不同的管理范围和安全目标进行分级部署、集中监测、统一协同、快速响应、全局预警、全局分析；
c) 应具备对各个边缘云管辖范围内的路侧基础设施进行分级化安全运营管理的能力，对路侧基础设施应采用安全策略防护手段，对路侧基础设施升级提供安全防护；
d) 应具备对各安全设备的配置管理能力、变更管理能力、资源容量管理的能力、应用生命周期安全管理的能力、专业的组织安全管理能力、漏洞管理和补丁管理能力，并建立完善的管理机制；
e) 应具备安全事件管理和快速安全应急响应能力和可持续安全事件检测能力。

6.8.2 安全运营平台要求

6.8.2.1 通用要求

安全运营平台应提供用户账户注册、信息修改、状态变更与注销等基本管理服务，建立明确的账户管理、消息推送、认证管理、权限管理流程，管理目标车辆、云控基础平台和运营方不同角色与权限。

6.8.2.2 数据接入管理功能要求

数据接入管理功能包括：
a) 安全运营平台应支持资产数据、漏洞数据、终端安全数据、流量安全数据、互联网安全事件数据等多源安全数据采集，并为安全信息监管平台、云控平台数据共享预留相应的数据接口，保障数据的共享使用；
b) 安全运营平台应使用公开、安全、有效的密码学算法支撑采集数据的安全存储，建立相应的数据安全访问和安全销毁机制，防止平台数据泄漏和窃取。

6.8.2.3 设备状态管理功能要求

安全运营平台应支持对车载终端设备、路侧基础设施等进行设备管理和设备状态管理，管理功能要求包括：
a) 车辆管理应具备车型管理、品牌管理、OEM 管理、ECU 管理、系统入侵检测防御探针管理、OTA 管理和 IDPS 管理功能；车辆状态管理应具备车辆基本信息维护、车辆行驶信息监控、车辆 OEM 信息和车辆网络信息管理功能，通过汇总、筛选、统计等方式对车辆、车队和车型的安全状态进行监控；
b) 路侧设备等设备管理应具备设备类型管理、故障管理、升级和运维管理功能；设备状态管理应具备基本信息维护、工作模式、资源使用管理功能。

6.8.2.4 安全态势感知功能要求

安全态势感知功能要求包括：
a) 应对网络链路、安全设备、网络设备和服务器等的运行状态进行集中监测；
b) 应能对网络中发送的各类安全事件进行识别和报警；
c) 安全运营平台应基于网络基础信息和重要安全日志数据、安全事件数据以及平台业务数据，对云控平台安全态势进行宏观分析；

d) 应支持整体安全态势分析、车型安全态势分析、车辆资产态势分析、提供设备/零部件安全态势视图，提供安全事件的影响范围和趋势。

6.8.2.5 安全事件管理功能要求

安全事件管理功能要求包括：

a) 系统管理员应按照 GB/T 20985.1-2017 的规定对云控平台的安全事件进行结构化管理，发现、报告、评估和响应事件，以及进行经验总结；
b) 应按照 GB/T 20986-2023 对云控平台的安全事件进行定义；
c) 安全运营平台应支持安全事件数据监控，包括事件类型统计、来源统计、时间统计和攻击统计，根据攻击类型、风险等级等对事件进行属性和响应规则配置，借助热点分析、威胁态势分析、KPI 分析等数据挖掘技术对重大威胁进行识别、定位、预测和跟踪；
d) 应支持对访问 IP 属性、特征等基本信息进行记录，关联内外网情报，基于大数据关联计算对 IP 进行多维度画像和研判。

6.8.2.6 漏洞与预警管理功能要求

漏洞与预警管理功能要求包括：

a) 安全运营平台应支持漏洞管理，维护公开漏洞库、自有漏洞库、漏洞状态、漏洞利用情况；
b) 应支持对管理设备的组件的漏洞持续性追踪，定位漏洞影响的设备，支持漏洞的优先级确定、漏洞修复跟踪。

6.8.2.7 应急响应管理功能要求

应急响应管理功能要求包括：

a) 安全运营平台应支持应急响应预案管理，支持不同应急场景下的预案设计；
b) 应建立对外接口管理规则和应急响应规则，维护应急资源库，支持主动化的预警管理、多级安全响应管理、脆弱性管理、威胁情报应用管理、安全编排自动化等功能。

6.8.2.8 日志管理功能要求

安全运营平台应对云控平台产生的日志进行集中管理，对事件日志进行记录和分析，对平台异常记录进行实时监控和预警，支持对事件的追溯和定位。

6.8.3 风险评估与持续监测要求

风险评估与持续监测要求包括：

a) 系统运营方应按照 GB/T 20984-2022 的要求定期（至少每 12 个月）开展云控平台安全风险评估工作，风险评估对象包括云控基础平台中的边缘云、区域云和中心云、各个边缘云管辖范围内的路侧基础设施、云控安全运营管理及其管理的安全设备和软件、以及云控平台中所有供应链管理组件，包括软件、硬件供应商和与供应链相关的任何第三方服务；
b) 应具备针对边缘云、区域云和中心云的分级化管理能力，包括分级部署、集中监测、统一协同、快速响应、全局预警和全局分析的能力，以满足不同管理范围和安全目标的需求；
c) 各个边缘云管辖范围内的路侧基础设施应实施分级化安全运营管理，以及对路侧基础设施采用合适的安全策略防护手段，并在其升级时提供安全防护；
d) 云控安全运营管理应具备配置管理、变更管理、资源容量管理、应用生命周期安全管理、组织安全管理、漏洞管理和补丁管理的能力，以及具备完备的管理机制；
e) 系统运营方应在供应链管理中实施安全保护措施，制定供应链安全策略、进行供应商安全审计和风险评估，见《关键信息基础设施安全保护条例》；
f) 应按照 GB/T 31509-2015 的要求开展风险评估项目的组织、实施、验收等工作；
g) 应按照 6.1.7、6.4.3 规定的系统入侵防御要求对风险评估对象进行持续性安全监测，应按照 GB/T 20986-2023 中的安全事件定义将监测结果统一记录在安全运营平台中；
h) 应持续关注监测结果，并将监测结果应用至后续的车路云一体化系统安全风险评估工作中。

6.8.4 应急预案与应急响应要求

应急预案与应急响应要求包括：

a) 系统运营方应承担网络安全事件的预防和处置工作，见《国家网络安全事件应急预案》；应按照 GB/T 28827.3-2012 中 9.5 定义的网络安全事件等级制定不同级别的应急预案，并且建立安全事件响应流程，包括识别、评估、处理、信息收集；
b) 在发生安全事件后，严格按照应急预案的准备以及应急响应流程来实施；安全事件处理结束后，进行评估和总结，进而优化改进应急预案以及应急响应流程；
c) 应按照 GB/T 38645-2020 的要求定期（至少 12 个月）组织开展应急演练，包括制定应急演练工作计划、编写应急演练具体方案、组织实施应急演练方案、总结应急演练工作、优化改进应急响应机制及应急预案，测试和评估网络安全应急预案的可行性和有效性，不断更新改进云控平台安全应急响应水平；
d) 云控基础平台应具备应急资源库，包括云控基础平台信息安全漏洞库、恶意代码库、应急处置模板库、知识库等；
e) 云控基础平台应具备数据融合分析能力，将安全事件关联数据进行统计、对比、分析，预置多种应急处置技术分析与响应策略模板，快速应对突发安全问题。

7 证实方法

7.1 云控基础平台安全证实方法

7.1.1 物理安全证实方法

7.1.1.1 物理访问控制和访客访问记录证实方法

审查数据中心的门禁系统、视频监控系统、安保巡逻工作记录和培训资料，对云控基础平台的物理访问控制进行验证：

a) 门禁系统和视频监控系统是否已配备并能正常运行，检测内容是否已记录和存储；
b) 安保巡逻工作是否覆盖所有重要区域，巡逻频次是否能满足安全级别，是否对安保人员定期（至少每 12 个月）进行安全培训；
c) 检查访客登记材料、访客系统日志、结合使用访客系统查询功能，验证是否具备访问系统数据收集与存储能力、访问行为标识与追踪能力、访问数据分析能力和访问者隐私、等级、所有权等限制能力。

7.1.1.2 物理环境监控记录证实方法

在视频监控设备正常运行的情况下，通过长时间、多节点、大数据的调取监控数据对物理环境监控记录进行测试。

7.1.1.3 电力系统安全证实方法

检查设计方案、验收测试报告、检查现场设备仪表工作状态，验证绝缘、电压、电流、频率和功率数据是否符合设计要求。

7.1.1.4 人员管理证实方法

7.1.1.4.1 验证三权分离原则的实施情况，包括审查岗位设置、权限配置检查、账户管理检查和审计日志检查、实际操作测试，具体方法如下：

a) 审查岗位设置包括检查组织是否明确设置了系统管理员、审计管理员和安全管理员三个岗位；确认岗位职责是否明确划分，避免职责重叠或混淆；查阅岗位职责描述文件，确认是否符合三权分离原则（配置、授权、审计分离）；
b) 权限配置检查，包括检查系统中各管理员账户的权限配置，确保系统管理员负责系统的配置和运行管理，但无权进行授权和审计；安全管理员负责授权和安全策略配置，但无权查看审计日志；审计管理员负责审计日志的管理和分析，但无权进行系统配置或授权；通过系统权限管理工具（如Linux的sudoers文件、数据库的权限管理工具）验证权限分配是否符合要求；

c) 账户管理检查包括确认各管理员账户是否独立，不存在共享账户；检查是否存在多余或过期账户，及时清理；
d) 审计日志检查包括确认审计日志是否由审计管理员独立管理，且无法被其他管理员修改或删除；检查审计日志已记录系统管理员和安全管理员的操作行为，且审计员有权访问和分析这些日志；
e) 实际操作测试包括进行实际操作测试，验证各管理员是否只能在其权限范围内操作，且无法越权操作（如系统管理员无法修改审计策略）。

7.1.1.4.2 验证人员培训、保密和调离制度的实施情况包括审查制度文件、培训记录检查、保密协议检查、人员调离流程检查和访谈相关人员，具体方法如下：

a) 审查制度文件，检查组织是否制定了人员培训制度、保密制度和人员调离制度；确认制度中是否明确了培训内容、频率和考核方式；确认保密制度中是否包含保密协议、保密期限和违反保密规定的处罚措施；确认人员调离制度中是否明确了离职或换岗前的交接流程、权限回收和账户注销要求。
b) 培训记录检查，查阅培训记录，确认是否定期（至少每12个月）组织培训，培训内容是否涵盖安全系统操作、安全策略和最新安全技术；确认培训是否覆盖所有相关管理人员，并记录培训结果。
c) 保密协议检查，检查所有相关管理人员是否签署了保密协议，协议内容是否明确且具有法律效力。
d) 人员调离流程检查，查阅离职或换岗人员的交接记录，确认是否按照制度要求完成权限回收、账户注销和工作交接；确认离职人员的权限是否及时停用，避免权限滥用。
e) 访谈相关人员，与系统管理员、安全管理员和审计管理员进行访谈，了解他们对培训、保密和调离制度的知晓程度和执行情况。

7.1.1.4.3 验证人员考核制度的实施情况包括审查考核制度文件和访谈相关人员，具体方法如下：

a) 审查考核制度文件，检查组织是否制定了明确的人员考核制度，确认考核制度中是否明确了考核指标、考核频率和考核结果的应用；考核记录检查，查阅年度考核记录，确认是否对所有相关管理人员进行了考核；确认考核结果是否与培训和岗位调整挂钩，考核不达标者是否重新参加了培训，严重不合格者是否被调离岗位；考核指标合理性检查，评估考核指标是否合理，是否涵盖技术能力、安全意识和工作绩效等方面；
b) 访谈相关人员，与管理人员和考核负责人进行访谈，了解考核制度的执行情况和改进空间。

7.1.2 身份鉴别证实方法

审查鉴别技术、用户登录记录、网络安全防护系统等，对车路云一体化系统身份鉴别功能和技术措施进行验证。

7.1.3 访问控制证实方法

审查访问控制设备及配置参数、访问控制规则、会话认证机制等，对云控基础平台访问控制进行验证。

7.1.4 安全审计证实方法

审查安全审计机制、安全事件采集功能、用户行为和重要安全事件审计功能、审计记录及存储、审计管理员身份鉴别功能、监测和报警记录分析报告等，对云控基础平台安全审计进行验证。

7.1.5 虚拟化安全技术证实方法

7.1.5.1 宿主机安全证实方法

宿主机安全证实方法包括：

a) 登录验证宿主机系统，验证是否采用必要的身份鉴别机制；
b) 操作特殊权限命令，验证宿主机系统是否采用必要的访问控制；
c) 模拟攻击验证宿主机系统，验证是否采用安装了必要的入侵防御机制；
d) 模拟攻击验证宿主机系统，验证是否采用必要的恶意代码防范机制。

7.1.5.2 虚拟化计算安全证实方法

虚拟化计算安全证实方法包括：

a) 检查云控基础平台安全运营系统中的探针部署信息，查看监测信息，验证云控基础平台是否能够对虚拟化监视器的通讯进行监测，确保信息未被泄露或篡改；
b) 渗透测试中对宿主机与虚拟机以及虚拟机之间进行网络通信测试、存储隔离测试、内存隔离测试，验证云控基础平台是否能够支持虚拟机之间、虚拟机和宿主机之间以及 CPU、GPU、硬盘、内存等资源的隔离；
c) 查验云控基础平台稳定性和健壮性测试说明，验证云控基础平台是否能够确保某个虚拟机崩溃后不影响宿主机及其他虚拟机。

7.1.5.3 虚拟存储安全证实方法

虚拟存储安全证实方法包括：

a) 检查相关技术措施如加密技术等和渗透测试报告中对数据完整性的测试结果，验证云控基础平台是否采取措施对虚拟化中重要数据完整性进行保护；
b) 检查相关技术措施如加密技术措施、冗余备份技术措施等和渗透测试报告中对数据完整性的测试结果，验证云控基础平台是否能够保证镜像文件完整性、可用性和保密性；
c) 检查存储加密技术措施的建设及工作运行情况，验证云控基础平台是否支持对虚拟磁盘进行加密；
d) 检查技术手册结合查看渗透测试报告中对数据清除回收功能的测试结果，验证云控基础平台是否支持虚拟化的残留数据清理能力，如内存、存储空间、镜像、快照等资源完全清除回收；
e) 检查技术手册结合查看渗透测试报告中对访问控制的测试结果，验证云控基础平台是否能够保证安全控制方法对逻辑存储设备和物理存储设备都有效。

7.1.5.4 虚拟网络安全证实方法

虚拟网络安全证实方法包括：

a) 检查云控基础平台技术手册中对云控基础平台的压力峰值设计和配套的测试报告，验证是否能够保证关键网络设备及虚拟化网络设备的业务处理能力具备冗余空间，满足业务高峰期需要；
b) 检查云控基础平台的安全运营平台，验证是否能够监控虚拟机之间、虚拟机与宿主机之间的流量；
c) 检查云控基础平台的安全建设方案或等保测评方案的相关网络边界和安全域划分内容，验证是否支持网络安全域划分，确保虚拟机之间的网络安全隔离；
d) 检查云控基础平台技术手册及其验收测试报告中对应的测试结果，验证云控基础平台是否能够避免部分虚拟机对虚拟机网络资源的过度占用以及网络故障影响其他虚拟机的正常使用。

7.1.5.5 虚拟化管理安全证实方法

虚拟化管理安全证实方法包括：

a) 检查云控基础平台技术手册和查看云控基础平台自身的运行维护系统功能，验证云控基础平台是否能够对其系统虚拟化中的虚拟主机进行实时监控其运行状态、资源占用、网络负载等能力；
b) 检查云控基础平台技术手册和查看云控基础平台自身的管理系统功能，验证云控基础平台是否能够提供虚拟资源管理员权限分离机制，例如系统管理员、安全管理员、审计管理员等不同的管理员账户；
c) 检查云控基础平台技术手册和查看云控基础平台自身的管理系统功能，验证云控基础平台的虚拟化管理平台的管理员是否按职能分割和最小授权原则，并形成相互制约、监督的关系；
d) 检查是否部署入侵防御系统和查看云控基础平台的安全运营平台，验证是否支持在外部网络中对虚拟机管理平台和虚拟机的入侵行为进行检测，并在发生入侵事件时提供告警；
e) 检查是否部署入侵防御系统、行为监控系统和查看云控基础平台的安全运营平台，验证是否具备对虚拟化内部发起的攻击检测和防护能力，检测出发起攻击的虚拟机，并能记录攻击类型、攻击时间、攻击流量；
f) 检查是否部署入侵防御系统、恶意代码防护系统以及定期（每 6 个月～12 个月）通过漏洞扫描工具和开展渗透测试发现的漏洞，并查看云控基础平台的安全运营平台，验证云控基础平台

的容器安全服务是否提供镜像漏洞管理、容器安全策略管理功能，解决传统安全软件无法感知容器环境的问题；

g) 检查云控基础平台技术手册、建设方案和查看是否部署并运行了容器安全工具，验证云控基础平台的容器安全服务是否具备容器进程白名单、文件只读保护和容器逃逸检测功能，有效防止容器运行时安全风险事件的发生。

7.1.6 容灾备份和业务连续性证实方法

7.1.6.1 业务系统备份证实方法

业务系统备份证实方法包括：

a) 检查建设方案，验证云控基础平台是否制定完善的系统级的备份方案；
b) 检查备份方案、备份日志和应急演练预案，验证车路云一体化系统是否能够定期（每 6 个月～12 个月）对系统中的各业务应用系统进行备份和恢复；
c) 检查备份方案和备份系统的验收测试报告，验证车路云一体化系统是否能够保证业务应用的备份数据的完整性、保密性和可用性；
d) 检查备份方案和和备份系统的测试报告，验证车路云一体化系统是否能够针对关键业务配置异地系统备份系统；
e) 进行书面测试、演练测试、切换测试、并行测试，验证车路云一体化系统是否定期（每 6 个月～12 个月）测试灾难恢复计划的可行性。

7.1.6.2 业务连续性证实方法

业务连续性证实方法包括：

a) 检查风险评估报告、渗透测试报告、应急演练系统，验证车路云一体化系统是否定期（每 6 个月～12 个月）开展针对云控业务连续性的风险分析；
b) 检查应急预案和应急演练系统，验证车路云一体化系统是否将应急响应计划、灾难恢复计划及支撑客户实施业务连续性计划的有关措施告知客户；
c) 检查建设方案和验收测试报告查看系统功能模块的工作情况和日志记录，验证车路云一体化系统是否保障系统冗余与高可用性；
d) 检查合同签署内容、抽查供应链名单情况、供应商定期会议纪要等信息，验证车路云一体化系统是否定期（每 6 个月～12 个月）审查和管理供应链安全。

7.1.7 系统入侵防御证实方法

系统入侵防御证实方法包括：

a) 设备部署测试：查验 IDS/IPS 设备是否正常运行，包括硬件连接、软件配置和网络连通性；功能验证测试：模拟攻击（如 DDoS 攻击、端口扫描、恶意软件传播等）验证 IDS/IPS 是否能够检测并响应；检查设备是否能够生成警报并记录攻击行为；性能测试：测试 IDS/IPS 在高流量环境下的性能，确保其不会对网络性能产生负面影响；
b) 数据包捕获测试：使用网络抓包工具（如 Wireshark）验证 IDS/IPS 是否能够实时捕获网络流量；检查设备是否能够完整记录数据包的头部和负载信息；流量分析测试：验证设备是否能够对捕获的数据包进行分析，识别正常流量与异常流量；模拟不同类型的网络流量（如 HTTP、FTP、P2P 等）测试设备的分析能力；
c) 重放攻击测试：模拟重放攻击，发送之前捕获的合法数据包到目标系统；验证 IDS/IPS 是否能够识别并阻止重放攻击，同时检查是否生成相应的警报；时间戳验证测试：在数据包中添加时间戳，验证设备是否能够通过时间戳鉴别数据的新鲜性；测试设备是否能够拒绝过期或重复的时间戳数据包；
d) 欺骗攻击测试：模拟常见的欺骗攻击（如 IP 地址伪装、端口跳变、加密隧道攻击等）；验证 IDS/IPS 是否能够检测到这些攻击行为，并记录相关特征；避攻击测试：使用工具（如 Metasploit）模拟攻击者试图绕过 IDS/IPS 的行为；检查设备是否能够发现并阻止这些规避行为。

e） 检查安全运营平台建设方案，结合基于大数据处理技术的安全信息和事件管理技术，验证证车路云一体化系统是否能够将拦截行为生成审计记录，并保留与入侵事件相关的要素信息；
f） 检查安全运营平台建设方案，结合安全基线系统、网络和主机防火墙工具，验证车路云一体化系统是否能够关闭不需要的系统服务，默认共享和高风险端口；
g） 检查风险评估、渗透测试、护网行动等工作记录和是否配置有漏扫工具，验证车路云一体化系统是否能够定期（每 6 个月～12 个月）开展漏洞扫描工作，及时修补漏洞；
h） 检查安全运营平台建设方案，结合检查是否具有安全事件通报预警功能，验证车路云一体化系统是否能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警；
i） 检查安全运营平台建设方案，结合检查是否部署针对移动存储介质进行安全准入管理的系统或终端，验证检查车路云一体化系统是否能够严格对外来介质设备实行管控，并对各类硬件设备的外接存储接口进行限制或移除。

7.2 云控应用安全证实方法

7.2.1 应用生命周期安全证实方法

7.2.1.1 通用要求

云控应用安全对其生命周期进行全面管理，审查在设计、开发、部署、测试、发布、调用、停用等环节配套的审批、安全分析、设计方案、代码审查和安全测试报告、部署方案、安全测试和渗透测试报告、发布流程及执行情况记录、停用规则和流程及执行情况记录，检查安全监控系统运行日志是否符合要求。

7.2.1.2 设计阶段

云控应用程序在设计阶段的安全性证实方法包括：
a） 身份验证：模拟不同的用户和角色，尝试访问云控应用，验证是否只有经过身份验证的用户才能访问；
b） 授权：模拟不同的用户和角色，尝试执行不同的操作，验证是否只有被授权的用户才能执行特定的操作；
c） 数据保护：检查数据存储和传输的方式，验证是否采取了足够的加密和保护措施；尝试非法获取和修改数据，验证数据保护措施的有效性；
d） 操作审计：检查审计日志，验证是否记录了所有的操作；模拟非法操作，验证是否能够在审计日志中发现；
e） 安全架构：审查设计方案、安全建设方案、实施方案中的网络拓扑、安全层次结构和隔离策略等内容，验证安全架构的合理性和有效性；
f） 业务流程的连贯性和可用性：模拟正常和异常的业务流程，验证业务流程的连贯性和可用性，验证在保证连贯性和可用性的同时，是否也保证了安全性。

7.2.1.3 开发阶段

云控应用程序在开发阶段的安全性证实方法包括：
a） 代码安全合规：审查同云控应用开发服务提供商签订的相关合同约定和设计方案中确定的云控应用代码符合哪一项安全编码标准，并审查代码审查和静态代码分析工具结合约定好的安全编码标准进行检查的报告材料；
b） 代码安全执行标准：审查开发合同、开发文档和代码，验证是否有明确的代码安全执行标准，并且这些标准是否被正确地实施；
c） 静态代码审计：使用静态代码审计工具，检查代码中是否存在常见的安全问题，如SQL注入、XSS攻击等；
d） 开发文档的完整和保密：审查开发合同、设计文档、开发文档，验证文档的完整性；模拟非法访问，验证文档的保密措施的有效性。

7.2.1.4 部署阶段

云控应用程序在部署阶段的安全性证实方法包括：

a) 云控应用程序的安全性：审查服务器和网络设备的配置，验证是否已经正确配置了网络防火墙、入侵防御系统、WAF、负载均衡、数据库防火墙等；
b) 运行环境的隔离：模拟攻击和渗透测试，验证隔离措施的有效性；
c) 更新和修补漏洞：审查更新和修补的记录，验证是否及时更新和修补了云控应用程序披露的漏洞。

7.2.1.5 测试阶段

云控应用程序在测试阶段的安全性证实方法包括：
a) 渗透测试：模拟攻击者的行为，尝试从外部或内部对云控应用进行攻击，以发现和修复安全漏洞；记录和分析渗透测试的结果，确保所有发现的漏洞都已经被修复；
b) 漏洞扫描：使用至少2家厂商的漏洞扫描工具，交叉验证检查云控应用是否存在已知的安全漏洞；
c) 安全性评估：对云控应用的架构、设计、实现和运行进行全面的审查，评估其整体的安全性；审查安全性评估的报告，确保云控应用满足所有的安全要求。

7.2.1.6 发布和调用阶段

云控应用程序在发布和调用阶段的安全性证实方法包括：
a) 版本控制：审查发布流程和版本控制系统，验证是否只有受信任的版本被部署和调用；
b) 安全接口和文档：审查接口和文档，验证是否为调用者提供了安全的接口和文档；模拟非法接口调用，验证接口的安全性；
c) 身份验证和授权：模拟不同的用户和角色，尝试调用接口，验证是否进行了有效的身份验证和授权；
d) 日志记录：审查日志，验证是否对所有的接口调用进行了日志记录；模拟非法接口调用，验证日志记录的有效性。

7.2.1.7 停用阶段

云控应用程序在停用阶段的安全性证实方法包括：
a) 影响范围分析：审查安全评估报告中对云控应用程序影响范围分析的结果，确保停用或卸载操作不会影响其他业务；
b) 安全停用或卸载：实际执行停用或卸载操作，验证其安全性；监控停用或卸载操作的过程和结果，确保没有产生安全问题；
c) 数据处理：审查云控应用配套的数据销毁或迁移记录，确保敏感信息没有被泄露。

7.2.1.8 持续改进

云控应用程序在持续改进阶段的安全性证实方法包括：
a) 安全性改进：审查云控应用的更新记录、安全事件和漏洞的监测记录、处置和修复的记录，验证是否在整个生命周期中不断改进了云控应用的安全性；
b) 安全运营体系：检查是否部署了安全运营系统以及调研安全运营系统的运行情况，审查安全政策、流程的更新记录，并建立了定期（每6个月～12个月）更新安全政策和流程的安全运营体系。

7.2.2 云控应用 Web 安全证实方法

7.2.2.1 Web 服务器安全证实方法

Web服务器安全验证按照下列流程及要求依次进行：
a) 使用漏洞扫描工具对服务器进行漏洞检测，检测是否存在权威漏洞平台发布 6 个月及以上的高危安全漏洞；

注：服务器高危安全漏洞包括 SQL 注入漏洞、文件上传漏洞、权限漏洞、暴力拆解漏洞、拒绝服务攻击漏洞、信息泄露漏洞、业务逻辑漏洞、安全配置漏洞等。

b) 若存在高危漏洞，则检查该高危漏洞处置方案的技术文件。

7.2.2.2 Web 客户端安全证实方法

Web客户端安全验证按照下列流程及要求依次进行：

a) 使用漏洞扫描工具对客户端进行漏洞检测，检测是否存在权威漏洞平台发布 6 个月及以上的高危安全漏洞；

注：客户端高危安全漏洞包括跨站脚本攻击漏洞、跨站点请求伪造漏洞等。

b) 若存在高危漏洞，则检查该高危漏洞处置方案的技术文件。

7.2.2.3 Web 通信信道安全证实方法

Web通信信道安全验证按照下列流程及要求依次进行：

a) 检查传输层通信协议是否为 TLCP、TLS1.2 等安全协议；

b) 检查通信数据加密算法是否为 SM2 或 SM4，检查解密数据是否存在丢包、数据毁坏、数据被篡改等数据不完整的情况；

c) 检查 V2X 信息交互时 V2X 通信证书是否符合 YD/T 3957-2021 的规定。

7.2.3 接口安全证实方法

7.2.3.1 端侧设备接入安全证实方法

端侧设备接入安全验证包括：

a) 通过如 OpenSSL、Wireshark 等第三方工具检查设备密钥或 X.509 证书的有效性和完整性来验证设备的身份；可通过公钥基础设施（PKI）或其他密钥管理系统来实现；

b) 通过如 Wireshark、TCPdump 等第三方抓包工具，抓取和分析网络通信流量来验证是否使用了安全的 TLCP、TLS 加密传输协议；可检查信息交互内容是否已加密，并验证其加密强度；

c) 通过如 Wireshark、Ettercap 等第三方工具，修改通信数据，然后检查系统是否能够检测并拒绝这些修改来验证完整性保护；

d) 先审查相关设备或系统的安全策略，并尝试使用违法安全策略的方式，如未授权的 IP 或用户账号访问系统，查看系统是否能正确拒绝这些访问请求；可尝试使用现有账户权限访问非授权资源，或操作检查系统是否根据安全策略对合法账号进行了权限管理；

e) 检查审计日志，验证是否记录了设备的身份标识、接入时间、接入类型等内容；触发记录日志条件以便检查系统是否能够在设备接入时生成这些记录。

7.2.3.2 相关支撑平台接入安全证实方法

相关支撑平台接入安全证实方法包括：

a) 云控平台与相关支撑平台使用 HTTPS 和 WebSocket 协议进行信息交互时，采用如 OpenSSL、Wireshark 等第三方工具验证基于数字证书的 HTTPS 系统认证进行验证，利用 Spring Security OAuth2.0 开源框架或 Postman 对 OAuth2.0 的授权码认证进行验证；

b) 利用如 Wireshark、TCPdump 等第三方抓包工具，抓取和分析网络通信流量来验证云控平台与相关支撑平台使用 MQTT 协议进行信息交互时，是否使用了安全的 TLCP、TLS 加密传输协议；

c) 利用如 Wireshark、TCPdump 等第三方抓包工具，抓取和分析网络通信流量来验证信息交互内容是否采用安全的 TLCP、TLS 等加密传输协议；

d) 审查接入申请和审批材料，验证相关支撑平台的接入是经过授权管理的，申请接口调用时已告知接口的用途和授权范围；组织测试接口调用，验证接口调用是否按照申请的范围和授权方式进行管理。

7.2.4 应用代码安全证实方法

应用代码安全证实方法包括：

a) 审查云控平台的云控应用开发是否配置了代码审计工具和配套的代码管理制度，包括针对不同开发语言的安全编码标准、审计规划、人工审计记录或自动化审计工具审计报告等；并组织测试团队对审计结果进行验证确保审计工具运行正常；

b) 内部审计：审查内部审计的记录和结果，验证是否对内部开发人员进行了安全审计；

c) 外部审计：审查外部审计的记录和结果，验证是否组织了具备资质的第三方专业代码审计机构对云控应用进行审计；
d) 审查审计的流程和记录，验证审计工作是否包含准备、实施、报告和持续跟踪等活动形成工作体系；
e) 审查应用代码安全审计报告中的安全功能缺陷审计的记录和结果，验证是否符合GB/T 39412-2020第6章中的规定；
f) 审查应用代码安全审计报告中安全缺陷审计的记录和结果，验证是否符合GB/T 39412-2020第7章中的规定；
g) 审查应用代码安全审计报告中资源使用安全缺陷审计的记录和结果，验证是否符合GB/T 39412-2020第8章中的规定；
h) 审查应用代码安全审计报告中环境安全缺陷审计的记录和结果，验证是否符合GB/T 39412-2020第9章中的规定。

7.3 路侧基础设施安全证实方法

7.3.1 物理安全证实方法

7.3.1.1 物理环境安全证实方法

物理环境安全证实方法包括：
a) 防水措施：检查和确认设备外壳的防水等级（如IP67或IP68），应履行GB/T 4208-2017中不同防水等级的证实方法；
b) 防静电措施：检查和确认设备的防静电性能，宜进行表面电阻测试、摩擦电压测试（低于100V）等；
c) 电磁屏蔽措施：检查和确认设备的静电放电抗扰度和射频电磁场辐射抗扰度性能，应履行GB/T 17626.2-2018中静电放电抗扰度证实方法，应履行GB/T 17626.3-2023中射频电磁场辐射抗扰度证实方法；
d) 减震设计：检查和确认设备在振动环境下的稳定性，应履行GB/T 2423.10-2019中正弦振动证实方法；
e) 接地措施：检查接地系统是否正确安装，接地电阻是否小于10欧姆。

7.3.1.2 硬件安全证实方法

硬件安全证实方法包括硬件安全设计检查、安全配置检查和文档和记录检查，具体方法如下：
a) 后门或隐蔽接口检查：审查硬件设计文档，确认是否有未公开的接口或预留的调试接口；对硬件进行物理检查，包括拆解设备，检查是否有隐藏的接口或未标记的电路连接；使用 X 光检测设备对硬件内部结构进行扫描，查找潜在的隐蔽接口；
b) 密码模块检查：审查硬件设计文档，确认是否集成了密码模块（如 TPM、HSM 等）；使用硬件安全工具（如硬件扫描仪）检测密码模块的存在性；验证密码模块是否与硬件绑定，确保其不可移除或替换；
c) 调试接口禁用功能检查：审查设备的配置管理文档，确认调试接口（如 JTAG、UART 等）是否具备禁用功能；通过设备管理工具或命令行工具（如 jtag-disable 命令）验证调试接口是否已被禁用；检查设备的功能设置，确认调试接口是否被禁用；
d) 安全访问控制模块检查：审查硬件设计文档，确认是否部署了安全访问控制模块（如 PAM 模块、白名单机制等）；通过设备管理工具验证安全访问控制模块是否已启用；模拟未授权访问尝试，验证安全访问控制模块是否能够阻止非法访问；
e) 安全策略配置检查：检查设备的安全策略配置文件是否配置了相关安全策略；验证安全策略是否包括对访问控制、身份认证、日志记录等的要求；模拟攻击场景（如暴力破解、IP 扫描等），验证安全策略是否能够有效检测和阻止攻击行为。

7.3.2 系统安全证实方法

7.3.2.1 安全启动证实方法

安全启动证实方法包括：

a) 提取操作系统签名，使用软件调试工具对签名进行篡改，将修改后的签名写入到路侧基础设施内的指定可信区域内，检查是否正常工作；
b) 获取操作系统的系统固件等其他安全启动代码，使用软件调试工具对安全启动代码进行篡改，将修改后的启动代码写入到路侧基础设施内的指定区域，检查是否正常工作。

7.3.2.2 身份认证与鉴别证实方法

身份认证与鉴别证实方法包括：

a) 采用分析路侧基础设施登录方式文档，检查是否有口令、设备唯一标识定义、登录失败处理等策略；
b) 按照路侧基础设施登录方式文档，进行功能测试，检查功能是否完整。

7.3.2.3 访问控制证实方法

访问控制证实方法包括：

a) 采用分析用户权限配置文档和测试的方法，检查路侧基础设施是否分配不同的用户权限配置与不同安全级别的访问控制策略；
b) 遍历路侧基础设施的端口，查看是否只开启默认端口异界服务；尝试访问非授权端口测试是否拒绝访问；
c) 采用分析设计文档和测试的方法，查看是否对外部存储设备做访问控制策略；
d) 在远程登录设备的过程中，采用网络数据抓包攻击进行数据抓包，解析通信报文数据，检查通信协议是否安全。

7.3.3 入侵防御证实方法

入侵防御证实方法包括：

a) 采用分析入侵防御模块文档和测试的方法，检查路侧基础设施是否支持入侵行为的记录；
b) 采用分析入侵防御模块文档和测试的方法，检查路侧基础设施是否支持入侵时间上报，以及上报策略；
c) 采用分析入侵防御模块文档和测试的方法，检查路侧基础设施入侵时间记录格式是否完整。

7.3.4 应用安全证实方法

应用安全证实方法包括：

a) 使用漏洞扫描工具对路侧基础设施进行漏洞检测，检测是否存在权威漏洞平台发布6个月及以上的高危安全漏洞；若存在高危漏洞，则检查高危漏洞处置方案的技术文件；
b) 对应用软件中数据进行分析，检查应用软件对个人敏感信息是否存在非授权收集或泄漏、非授权数据是否外传等恶意行为；
c) 使用逆向工具进行风险审查，检查应用软件是否使用混淆、加壳等安全机制，对抗针对应用的逆向分析；
d) 采用分析软件与固件升级文档，检查升级前是否对升级包做真实性与完整性校验，针对校验错误的升级包是否有处置策略；
e) 采用分析软件与固件升级文档，检查升级时是否支持升级失败回滚或中断继续功能；
f) 采用分析软件与固件升级文档，检查升级成功后是否删除升级包和敏感信息；检查升级日志记录过程是否完整。

7.4 公钥基础设施安全证实方法

7.4.1 密码服务证实方法

7.4.1.1 对称加密证实方法

对称加密证实方法包括：

a) 对对称加密算法的正确性和安全性进行验证，使用实现的对称加密算法对指定数据进行加解密后，验证数据在加密前和解密后是否一致；审查相关设备的产品规格说明材料，确认对称加密算法没有使用未公开、未发布或已攻破的不安全算法，如 DES、3DES 加密算法等；
b) 对生成的对称密钥的长度进行检验，对于生成的密钥，选择开源或通用的第三方验证工具验证密钥长度是否满足 6.4.2.1 中所述要求。

7.4.1.2 非对称加密证实方法

非对称加密证实方法包括：

a) 对非对称加密算法的正确性进行验证，使用实现的非对称加密算法的公钥对指定数据进行加密后对数据使用私钥进行解密，对于加密前的数据与解密后的数据是否一致；
b) 对于非对称加密算法中的 SM2、ECC 加密算法，对其加密的随机性进行校验，分别多次加密数据后观察其结果是否一致，确认加密是否具有随机性；
c) 对非对称加密算法的密钥长度进行检验，使用开源或通用的第三方验证工具（如 OpenSSL）对非对称密钥中的公钥进行解析以获取非对称密钥的长度，验证密钥长度是否满足 6.4.2.2 所述要求。

7.4.1.3 签名验签算法证实方法

签名验签算法证实方法包括：

a) 对签名验签算法的正确性进行验证，使用实现的签名验签算法对指定数据进行签名，使用验签算法对签名进行验证，查看验证结果是否为通过；
b) 对签名算法使用的杂凑算法的碰撞性进行测试。

注：杂凑算法的碰撞性测试方法有生日攻击测试、雪崩效应测试、有偏性测试等可供选择。

7.4.2 KMS 证实方法

7.4.2.1 密钥生成证实方法

宜采用GM/T 0005-2021中的检测方法对生成密钥的随机性进行检验。

7.4.2.2 密钥储存证实方法

将密钥导入密钥储存区域后，读取密钥储存区域，对比读取出的密钥和导入前的密钥，判断密钥是否进行加密。

7.4.2.3 密钥分发证实方法

对密钥进行请求，抓取请求过程中的包，观察密钥是否被加密，如若未加密则测试不通过，如若加密则测试通过。

使用不合规的证书向KMS进行密钥请求，观察KMS是否返回正确的密钥，如若返回了请求的正确的密钥，则测试不通过，否则测试通过。

7.4.2.4 密钥撤销证实方法

在KMS中对密钥进行撤销后，通过KMS接口使用对应的密钥进行加密，若不能加密则测试通过，否则测试不通过。

7.4.2.5 密钥销毁证实方法

对密钥进行销毁后，通过KMS请求对应的密钥进行分发以判断密钥是否被销毁，若无法执行分发则测试通过。同时应检测对应的备份路径是否同样删除了密钥。

7.4.3 PKI 证实方法

检查PKI系统内的功能模块是否完备，对每一个模块执行下述测试。

a) RA 模块测试：由其他系统向 RA 模块发送证书申请 CSR，CA 管理员登陆 CA 系统检查证书申请是否被正确转发。
b) CA 模块测试：

1） 证书审核：在CA中审核对应的CSR后，通过VA查询证书是否被激活；
2） 证书冻结：在CA中冻结对应证书后，通过VA查询证书是否处于冻结状态；
3） 证书解冻：在CA中解冻对应证书后，通过VA查询证书是否被激活；
4） 证书撤销：在CA中撤销对应证书后，通过VA查询证书是否被撤销；
5） 用户认证：检查CA管理员登陆是否经过双因素认证。

c） VA 模块测试：检查 VA 是否具有 OCSP 和 CRL 协议，且通过 VA 查询的证书状态是否正确。

7.5 通信安全证实方法

7.5.1 通信网络架构证实方法

根据云控基础平台网络安全定级，按照GB/T 28448-2019中第6、7、8、9章对应级别的网络架构测评方法对云控基础平台进行测试，验证是否满足6.5.1的要求。

7.5.2 通信安全证实方法

依据6.5.2测试平台通信安全功能，按照如下证实方法，检验平台是否满足要求：

a） 采用网络数据抓包攻击进行数据抓包，解析通信报文数据，检查车路云通信认证过程是否为双向认证；
b） 采用网络数据抓包攻击进行数据抓包，解析通信报文数据，检查车路云数据传输过程是否经过加密或携带可信证书以及对应消息的签名；
c） 采用网络数据抓包攻击进行数据抓包，解析通信报文数据，检查数据传输携带证书以及对应消息的签名值是否与发送方匹配；
d） 采用网络数据抓包攻击进行数据抓包，解析通信报文数据，模拟中间人攻击方式，检查车辆是否无法建立通信连接；
e） 采用网络数据抓包攻击进行数据抓包，解析通信报文数据，将其篡改后发送篡改数据，检查是否校验失败、终止响应；
f） 分析路侧基础设施对外通信协议文档，是否具备身份鉴别功能，是否具备对身份鉴别失败的处理措施；对设备对外通信协议未配置身份鉴别功能的，分析设备对外通信链路，检查是否具备通信链路的保密性、完整性或真实性保护；
g） 进行大量数据传输、异常多次的数据传输、对应接口的模糊测试等操作，检查是否对异常情况进行监控告警。

7.5.3 通信可用性防护证实方法

依据6.5.3测试平台通信可用性防护功能，按照如下证实方法，检验平台是否满足要求：

a） 模拟各类针对网络通信协议的 DOS/DDOS（如 SYN Flood、ACK Flood、FIN/RST Flood、TCP Flood、UDP Flood、ICMP Flood、DNS 反射攻击等），向云控基础平台、车载终端设备、路侧基础设施发送攻击数据包，验证云控基础平台、车载终端设备、路侧基础设施是否具备有效识别攻击数据包的能力；
b） 基于 a）的验证方法，测试云控基础平台、车载终端设备、路侧基础设施在遭受 DOS/DDOS 时是否具备正常工作的能力；使用云控基础平台、车载终端设备、路侧基础设施的授权用户或工具，查看对攻击数据包的处理是否满足要求；
c） 模拟其他常见恶意数据包（如重放、篡改等），测试云控基础平台、车载终端设备、路侧基础设施在遭受攻击时是否具备正常工作的能力；使用云控基础平台、车载终端设备、路侧基础设施的授权用户或工具，查看对攻击数据包的处理是否满足要求；
d） 检查系统与通信保护策略与规程及系统设计说明书等相关文档、访谈平台管理员或安全管理员、检查恶意代码防护模块的实现机制，查看是否通过白名单、黑名单或其他方式在网络出入口部署恶意代码防护模块、是否建立并实施相应更新维护机制、是否能在检测到恶意代码后实时向管理员报警并采取相关措施。

7.5.4 安全事件日志证实方法

依据6.5.4测试平台安全事件日志记录功能，按照如下证实方法，检验平台是否满足要求：

构建并触发系统信息安全事件，使用授权的用户或工具，导出平台安全日志文件，验证文件记录的内容是否包含远程控制指令的日期、时间、发送主体、操作是否成功等信息，并记录验证结果。

7.6 数据安全证实方法

7.6.1 通用要求证实方法

数据安全通用要求证实方法包括：

a) 查验数据收集、存储、传输、使用、加工、传输、共享、跨境、提供和销毁等环节涉及个人信息安全是否符合GB/T 35273-2020的技术要求；
b) 查验系统运营方是否建立覆盖数据全生命周期的数据安全管理体系，并制定数据收集、存储、使用、加工、传输、共享、跨境和销毁等环节的具体分级防护要求和操作规程；
c) 查验是否根据T/CSAE 313-2023的要求建立数据分级分类制度，形成数据资产管理台账；
d) 查验是否建立覆盖风险管理与事件处置机制的数据安全风险管理制度，以保证安全隐患的及时排查和数据安全事件的及时处置。

7.6.2 数据资产管理证实方法

数据资产管理证实方法包括：

a) 评估车路云一体化系统是否建立数据资产管理相关工具，执行数据资产登记，通过数据库探测及时自动更新数据资产清单，并按照明确的数据分类分级策略实现数据的分类分级自动标识；
b) 评估车路云一体化系统是否建立密钥管理系统，实现对密钥类数据资产的全生存周期（生成、存储、使用、分发、更新、销毁等）的安全管理。

7.6.3 数据采集安全证实方法

数据采集安全证实方法包括：

a) 查验用户协议或隐私政策文件中业务功能及收集的外部数据或个人信息，是否明确数据采集的目的、用途和范围，规范数据采集的流程和方法；
b) 查验是否明确数据采集过程中外部数据或个人信息的知悉范围和安全控制措施，确保采集过程中的信息不被泄露；
c) 查验是否使用有效加密手段保障用户在线提交信息的安全性；
d) 车载终端设备进行数据收集时，查验用于数据收集的车载终端设备及系统的接入安全性；数据采集应履行GB/T 44464-2024中D.3的个人信息和重要数据收集试验方法；
e) 查验隐私政策或用户协议中是否明确在停止运营车联网服务、用户终止服务等情况时，停止对用户数据的采集；
f) 查验是否为用户提供注销号码或账号的服务，并且在用户注销账号时不得设置过多不合理的注销条件。

注：不合理的注销条件，例如，要求提交非必要的个人敏感信息。

7.6.4 数据存储安全证实方法

数据存储安全证实方法包括：

a) 重要数据存储过程中，篡改重要数据的摘要，检查存储过程是否重新执行；篡改重要数据，检查存储过程是否重新执行；
b) 检查系统的交互设计文档，检查是否存储了非业务必需的数据；
c) 检查系统的交互设计文档，检查数据存储是否有有效期，检查是否能够支持存储时效性的配置，检查存储的数据是否满足最短时间要求；
d) 验证是否具备定期的数据备份和恢复能力，检查备份数据文件，通过删除指定时间内的部分数据，确认是否能自动恢复，并且检查被删除的数据与被恢复的数据是否一致；
e) 尝试读取重要数据，检查重要数据是否进行了加密存储；检查重要数据是否采取异地保护功能，通过采用相同哈希算法对保存在异地的相同数据进行计算，检查其异地备份与原始数据是否一致；

f） 在云控平台的数据采集及传输系统中检查数据采集和传输的日志记录与存储，并通过销毁测试数据来验证销毁日志记录功能。。

7.6.5 数据加工安全证实方法

数据加工安全证实方法包括以下内容。

a） 检查系统是否部署了数据安全监测工具（如DLP系统、SIEM系统、数据加密工具等），并确保这些工具覆盖数据加工的全流程；模拟数据丢失、篡改或窃取场景（如未经授权的数据访问、数据包篡改等），验证系统是否能够实时检测到异常行为并触发警报。

b） 检查系统是否集成了数据溯源模块，并确保其能够记录数据的完整生命周期；模拟数据加工过程，验证系统是否能够完整记录数据的来源、处理过程和去向；检查系统是否记录了数据加工前后的字段映射关系，包括数据格式、处理逻辑等；使用自动化工具（如数据比对工具）验证数据处理前后的完整性，确保数据未被篡改。

c） 检查数据脱敏工具的配置，确保敏感信息被正确处理，模拟数据样本，验证脱敏后的数据是否仍可识别原始信息；检查数据在传输和存储过程中的加密状态，确保加密算法的正确性，使用加密工具对数据进行加密和解密测试，验证数据的完整性和保密性。

d） 数据加工算法安全性验证包括：

1） 数据范围验证包括数据边界测试，对算法输入数据的边界条件进行测试，确保算法不会处理超出范围的数据；数据类型检查，验证算法是否对输入数据类型进行了严格校验，防止非法数据输入；数据范围限制，进行代码审查和单元测试，确保算法在设计时已明确限制数据范围；

2） 数据目的验证包括需求文档审查，审查算法设计文档，确认其是否明确定义了使用目的；功能测试，模拟不同场景，验证算法是否仅用于预定义的业务目的；检查权限管理功能，检查算法的访问权限，确认其只能访问与业务目的相关的数据；

3） 结果应用范围验证包括结果用途测试，验证算法输出结果的使用场景是否符合预定义的应用范围；检查接口限制功能，检查算法输出接口的权限设置，确认结果只能被授权的应用访问；检查审计机制，进行日志审计，记录算法输出结果的使用情况，防止未经授权的使用。

7.6.6 数据使用安全证实方法

数据使用安全证实方法包括：

a） 检查系统的数据访问控制措施，确定是否遵循最小化原则；检查数据获取是否具备审批授权机制，并且记录了重要数据的访问和使用日志；尝试使用非授权的身份对数据进行增、删、改、查，检查是否能执行成功；

b） 使用合法账号调用重要数据，下载重要数据，检查相关操作是否被正确记录到日志中；对重要数据进行大量下载，频繁访问，非预期时间内访问，检查是否触发异常行为告警机制；

c） 合法访问个人重要数据，检查是否进行脱敏、去标识化；

d） 检查是否具备审计技术，并且检查审计信息的存储周期至少6个月。

7.6.7 数据共享安全证实方法

数据共享安全证实方法包括：

a） 查验数据共享相关审批记录，确认是否建立数据开放共享的审核制度和规范的数据共享审核流程，审核共享数据的数据内容，确认属于满足数据共享业务场景的需求范围及未超出授权范围开放共享数据；

b） 查验数据共享相关业务系统是否具备数据开放共享场景下的数据溯源方法（如对数据进行签名、添加数字水印等），防止数据被恶意删除、随意篡改和滥用；对于包含个人敏感信息的数据，是否能够及时跟踪、记录数据流向、数据接收者信息、处理操作等信息；在出现数据安全问题时，能够分析问题原因，追查数据出现问题的环节和责任人；

c） 查验个人信息开放共享制度，确认是否明确要求在违反法律法规规定或违反与个人信息主体的约定向合作方共享、转让个人信息，确认是否明确要求当个人信息主体要求删除信息时，立即停止共享、转让的行为，并通知合作方及时删除。

7.6.8 数据跨境安全证实方法

数据跨境安全证实方法包括：

a) 查验数据存储环境及使用环境是否位于中华人民共和国境内，是否存在与境外或在华外商投资企业及组织连接的数据传输接口或网络接口；

b) 查验是否存在向境外或在华外商投资企业及组织在线传输或离线拷贝车路云一体化系统数据的行为或计划；若有，查验是否依法申报数据出境安全评估，见《数据出境安全评估办法》中的数据出境安全要求。

7.6.9 数据提供安全证实方法

数据提供安全按以下证实方法进行验证。

a) 检查和确保对数据提供的所有接口进行了记录，包括接口类型、加密方式、传输周期、使用用途、认证方式等，证实方法如下：

1) 数据接口类型验证，审查接口文档，确认数据接口的类型（如 RESTful API、GraphQL、WebSocket 等）是否清晰、完整符合设计规范；接口功能测试，检查接口文档是否包含请求和响应的示例；使用 API 测试工具对不同类型的接口进行测试，验证其功能是否正常；模拟各种请求场景，确保接口能够正确处理请求并返回预期结果；

2) 加密方式验证，包括加密配置检查，检查接口配置，确认是否启用了加密传输（如 HTTPS），审查加密算法的选择是否符合安全标准技术（如 AES-256、RSA-2048）；数据传输测试，使用网络抓包工具（如 Wireshark）捕获数据传输过程中的数据包，验证数据是否被加密，检查加密数据的完整性，确保数据在传输过程中未被篡改；密钥管理验证，检查密钥的生成、存储和管理是否符合安全要求，确保密钥的安全性，验证密钥的更新机制是否有效，防止密钥泄露；

3) 数据传输周期验证，检查系统日志，确认数据传输的周期是否符合预设的时间表，使用日志分析工具统计数据传输的频率和时间分布；性能测试，模拟不同传输周期下的数据传输场景，验证系统的性能是否满足要求；检查数据传输的延迟和吞吐量是否符合预期；

4) 数据使用用途验证，审查业务需求文档，确认数据的使用用途是否明确，检查接口文档是否明确说明数据的使用范围和目的；功能测试，模拟不同的业务场景，验证接口是否仅提供符合使用用途的数据，检查接口是否对数据的使用范围进行了限制，防止数据被用于未经授权的用途；权限管理验证，检查接口的权限管理机制，确保只有授权用户才能访问和使用数据，验证接口是否对数据的使用行为进行了审计和记录；

5) 认证方式验证，审查接口的认证机制，确认是否采用了安全的认证方式，检查认证机制的实现是否符合行业标准（如 OAuth2.0 的授权码模式）；认证功能测试，模拟未授权访问场景，验证认证机制是否能够有效阻止非法访问，检查认证信息（如 Token、证书）的生成、存储和验证是否安全；日志审计功能检查，检查系统日志，确认认证行为是否被记录，包括认证成功和失败的记录，使用日志分析工具分析认证日志，确保认证机制的正常运行。

b) 检查数据提供过程的审计记录，确保数据提供过程状态可查，如提供时间、提供数据内容、数据接收方等。

7.6.10 数据销毁安全证实方法

数据销毁安全证实方法包括：

a) 查验数据共享相关业务系统，确认是否建立数据销毁策略，明确了销毁对象并规范销毁流程；

b) 查验是否建立分类分级的数据销毁机制，明确了不同数据类型的销毁方式和销毁要求；

c) 查验是否配置必要的数据销毁工具，能确保销毁后的数据不可再逆向恢复；尝试销毁可销毁的数据后检查系统是否有办法恢复。

7.7 供应链安全证实方法

7.7.1 供应链安全管理通用要求证实方法

供应链安全管理通用要求证实方法包括：

a) 检查系统运营方是否建立 SBOM 和关键资产清单，见 GB/T 43698-2024 附录 B；

b) 检查系统运营方是否建立业务场景分类清单，见 GB/T 43698-2024 附录 C；
c) 检查系统运营方是否遵循 GB/T 43698-2024 中 6.2 的要求构建软件供应链安全图谱并对其数据准确度进行维护；
d) 检查系统运营方是否创建云控平台软件供应链风险管理需求说明；
e) 检查系统运营方是否具备对云控平台软件供应安全开展风险评估和安全检测，查验评估报告和检测记录。

7.7.2 供应商管理证实方法

供应商管理证实方法包括：
a) 系统运营方应审查第三方机构的能力、资质、人员配置等，并审查第三方机构等级保护推荐证书副本的等级保护专用章或等保办印章以验证单位是否通过年审；
b) 针对供应商选择，审查是否具备相应的供应商甄选策略和制度，以及审查供应商目录的完整性和更新频率来进行检验；
c) 通过抽查、第三方信息查询验证供应商信息的准确性，并检查管理者是否已实施了适当的信息保护措施来对云控平台进行保护；
d) 审查包括风险评估报告、变更管理记录、安全策略和程序等相关材料以确定管理者是否对相关风险进行了有效管理，以及是否采取了相应的控制措施来进行检验；
e) 访谈供应商，审查合同、管理记录、检查报告等材料记录验证运营方是否要求供应商配合开展供应链安全监督和检查工作；
f) 审查招投标文件、合同和协议、官方网站、第三方机构的能力和资质证明等材料并检查其有效期，以验证运营方是否按照要求对第三方机构的能力和资质进行了检验。

7.7.3 供应活动管理证实方法

7.7.3.1 知识产权管理证实方法

知识产权管理证实方法包括：
a) 检查系统管理者与供应商双方是否建立知识产权管理规范，防止侵权发生；
b) 检查在合同中是否明确知识产权权属情况、知识产权保护措施、知识产权风险承担责任等内容，并具备交付时进行相应安全检查和审核的流程。

7.7.3.2 外部组件使用证实方法

外部组件使用证实方法包括：
a) 查验安装的开源及第三方组件是否具有可信来源，验证组件是可信发布者的签名和验证计算其哈希值（如 SHA-256）并与官方提供的哈希值进行比对，验证其完整性和真实性；
b) 查验供应商合同条款中是否明确所提供的开源软件、第三方组件、自有软件在交付前已对已公开漏洞进行修复并具有持续对上述软件在使用期间进行及时的漏洞管理；使用漏洞扫描工具检查组件是否存在已知漏洞，对开源组件的源代码进行静态分析，检查潜在的安全问题，在沙箱环境中运行组件，观察其行为是否符合预期；
c) 检查是否与供应商建立了供应商开源软件、第三方组件、自有软件的入库和使用审批机制，查验软件入库和使用审批文件是否包含完整性验证、安全性测试和依赖关系分析；
d) 查验是否保存了供应商软件记录文件，是否包含了开源软件、第三方组件、自有软件的供应方、OSC 以及主要开发贡献者等相关信息；可通过 SBOM 工具，检查是否完整记录了系统以及开源软件、第三方组件和自有软件的详细信息，如名称、版本号、许可证类型、供应方、开源合规（OSC）信息及主要开发贡献者等；进行文件完整性检查、信息一致性验证、许可证合规性检查及供应链透明度检查，确保软件来源可信、合规且无安全风险；
e) 检查是否与供应商建立了供应商软件管理规范和漏洞无法修复情况的解决预案，并查验安全管理记录、安全风险和漏洞检查报告等材料确定是否对所使用的开源软件、第三方组件、自有软件的使用状态、安全状态进行跟踪、风险识别、风险通报、漏洞修复等，并保留相关记录。

7.7.3.3 交付证实方法

交付证实方法包括：

a) 审查功能规格说明书和配套的功能测试报告和用户验收测试材料验证外部组件是否进行功能缺陷分析；
b) 模拟关键服务中断的情况，验证系统在服务中断时包括备份、恢复等应对能力；审查是否签订服务水平协议（SLA），并测试系统在正常和峰值负载下的性能，以评估系统是否能够满足SLA中的要求；
c) 审查合同相关技术条款是否明确相关软件代码应遵循相应的安全编码标准，审查静态代码分析报告、动态安全测试报告和漏洞扫描报告等验证分析安全漏洞和风险分析；
d) 审查第三方机构对供应链进行验证和审核发放的质量管理体系、信息安全管理体系、登记包括备案证书等认证资质，确保其符合相应的标准和规范；
e) 通过文档审查、分析测试报告、访谈交流等方式验证软件相关技术资料的完备性和准确性；
f) 审查合同中的技术支持协议条款或技术支持协议、模拟故障或问题、测试系统增删改查和升级更新、审查系统故障报告、运维日志和用户使用反馈等材料，验证软件系统是否满足用户的需求和安全稳定运行；
g) 审查验收测试报告、功性能测试报告、等级保护测评报告等对交付产品进行验证，宜采用安全检查扫描工具，组织开展渗透测试对交付系统和产品进行后门、非法数据获取、隐秘升级等行为进行识别；
h) 审查安全基线标准的完备性和适应性，是否及时更新，及时发布；通过基线检查工具定期（每6个月～12个月）检查供应商对交付的软件是否符合基线安全标准；
i) 审查第三方检测机构出具的测试报告；
j) 审查保密协议并定期（每6个月～12个月）检查保密工作的落实情况；
k) 审查合同相关技术条款，通过检查、风险评估、渗透测试等手段，验证交付产品或服务是否满足合同技术条款约定的技术指标；
l) 审查安全管理制度，通过访谈、检查、审计等方法验证对供应商的安全管理。

7.8 安全运营证实方法

7.8.1 安全运营体系化能力建设证实方法

7.8.1.1 安全策略证实方法

查验网络安全工作的总体方针策略类文档，核查网络安全工作的总体方针和安全策略文件是否明确机构安全工作的总体目标、范围、原则和各类安全策略。

7.8.1.2 管理制度要求证实方法

查验安全管理活动中的安全管理制度类文档、操作规程类文档，核查各项安全管理制度是否覆盖物理、网络、主机系统、数据、应用、建设和运维等管理内容；核查是否具有日常管理操作的操作规程，如系统维护手册和用户操作规程等。

7.8.1.3 制定与发布证实方法

查验授权部门/人员职责文件等、管理制度类文档和记录表单类文档，执行以下核查工作：

a) 核查是否由专门的部门或人员负责制定安全管理制度；
b) 核查制度制定和发布要求管理文档是否说明安全管理制度的制定和发布程序、格式要求及版本编号等相关内容；
c) 核查安全管理制度的收发登记记录是否通过正式、有效的方式收发，如正式发文、领导签署和单位盖章等。

7.8.1.4 评审和修订证实方法

评审和修订证实方法包括：

a) 访谈信息安全主管是否定期（每 6 个月～12 个月）对安全管理制度体系的合理性和适用性进行审定；

b) 核查记录表单类文档是否具有安全管理制度的审定或论证记录，如果对制度做过修订，核查是否有安全管理制度修订版本。

7.8.2 安全运营平台功能证实方法

7.8.2.1 数据接入管理功能证实方法

根据安全运营平台提供的数据接口，对资产数据、漏洞数据、终端安全数据、流量安全数据、互联网安全事件数据等不同类型输入数据的接入能力进行测试，流程方法如下：

a) 测试接口对于不同类型输入数据的处理能力，根据平台数据验证和处理机制，验证接口是否能正确验证和处理输入数据；
b) 测试接口在高并发情况下的性能，模拟大规模数据接入请求，验证接口是否能稳定处理大量请求；
c) 测试接口的集成能力，验证接口是否能与其他系统功能正常协同工作。

7.8.2.2 设备状态管理功能证实方法

根据安全运营平台支持的设备类型，测试平台对设备状态的管理、响应和监控能力，流程方法如下：

a) 测试平台对所支持设备状态变化情况下的响应能力，尝试变更车辆状态信息、路侧基础设施信息，验证平台在设备状态变化时是否能有效更新记录；
b) 测试平台对所支持设备状态管理的稳定性，尝试重启安全运营平台，模拟平台异常情况，验证平台是否能对设备状态数据进行保存和恢复。

7.8.2.3 安全态势感知及安全事件管理功能证实方法

根据安全运营平台支持的态势感知事件范围，测试平台对安全事件的感知、识别和响应能力，流程方法如下：

a) 测试平台对各类威胁和各类异常行为的感知和识别能力，模拟异常登录、非法访问等异常行为，验证平台是否能有效发现潜在威胁活动；
b) 测试平台对安全事件的响应速度，包括识别事件后的响应流程，验证平台是否能对安全事件进行及时告警和处理；
c) 测试平台对安全事件的分析和预测能力，提供安全数据和安全日志，验证平台是否能够基于历史数据和实时数据提供影响范围、趋势以及应对策略；
d) 依据 GB/T 20986-2023 的指南，检验平台是否能进行持续性安全监测，并统一记录监测结果；
e) 验证平台是否能根据 GB/T 20986-2023 的安全事件定义对安全事件进行有效管理。

7.8.2.4 漏洞与预警管理功能证实方法

根据安全运营平台的漏洞库和应急事件处理规则，测试平台对漏洞的管理能力和应急响应能力，流程方法如下：

a) 测试平台对安全漏洞的感知和预警能力，模拟公有漏洞库、自有漏洞库中的漏洞，验证平台是否能根据预置规则、触发条件和预警级别准确发出预警；
b) 测试平台对安全漏洞的响应流程和措施，模拟公有漏洞库、自有漏洞库中的漏洞，验证平台是否能根据预置方式进行自动化响应和漏洞修复跟踪。

7.8.2.5 应急响应管理功能证实方法

根据安全运营平台的应急响应管理要求，测试平台是否具备应急预案与应急响应能力，流程方法如下：

a) 查验平台是否按照GB/T 28827.3-2012的要求支持不同级别的应急预案和高效的安全事件响应流程设计；
b) 根据GB/T 20985.1-2017，评估平台在发现、报告、评估和响应安全事件，以及进行经验总结方面的能力；
c) 查验平台是否具备应急资源库，包括云控基础平台信息安全漏洞库、恶意代码库、应急处置模板库、知识库等；

d) 测试平台的数据融合分析能力，检验是否能预置多种应急处置技术分析与响应策略模板，并快速应对突发安全问题。

7.8.2.6 日志管理功能证实方法

根据安全运营平台的日志管理要求和规则，测试平台对日志的分析处理能力，流程方法如下：

a) 测试平台对日志的收集、存储、分析与处理能力，在正常运行状态下，验证平台是否能够对各种来源的日志（如操作系统日志、应用日志、网络设备日志）进行全面收集、记录和存储；
b) 测试平台对日志的分析和搜索能力，通过关键词搜索、事件关联等方式，验证平台是否可快速搜索日志和分析日志；
c) 测试平台对日志的完整性保护和访问控制能力，通过非授权账户对日志进行篡改、删除和越权访问，验证日志信息的完整性和安全性。

7.8.3 风险评估与持续监测证实方法

7.8.3.1 供应链安全管理评估方法

针对云控平台中所有供应链管理组件，包括软件、硬件供应商，以及与供应链相关的任何第三方服务，验证系统是否在供应链管理中实施了适当的安全保护措施，见《关键信息基础设施安全保护条例》，。证实方法按下列内容进行。

a) 供应链安全策略核查：
   1) 详细政策审查：逐项检查系统中的供应链安全策略，确保它们详细且具体，涵盖所有关键领域，如供应商选择、产品安全性、交付过程监控等；
   2) 合规性评估：评估这些策略的合规性，确保策略完全符合条例要求，见《关键信息基础设施安全保护条例》；
   3) 政策执行情况检查：实地或远程审核，检查这些安全策略在实际操作中的执行情况和效果。
b) 供应商安全审计：
   1) 审计流程设计：为每个供应商制定一个详细的审计流程，包括安全实践、历史表现和响应策略的审查；
   2) 现场或远程审计实施：对供应商进行现场或远程审计，评估其安全措施的实施情况；
   3) 供应链透明度评估：审查供应链的透明度，包括供应链的每个环节是否可追溯和审计。
c) 供应链风险评估：
   1) 风险识别和分类：识别供应链中的潜在风险，包括技术、法律和操作风险，并进行分类；
   2) 风险量化和优先级排序：量化这些风险的可能性和影响，确定它们的优先级；
   3) 应对策略评估：评估系统对识别出的风险采取的应对措施和策略的有效性。

7.8.3.2 云控基础平台分级化管理能力评估方法

针对云控基础平台的边缘云、区域云和中心云，以及相关的管理和监控组件，验证系统是否具备针对边缘云、区域云和中心云的分级化管理能力，包括分级部署、集中监测、统一协同、快速响应、全局预警和全局分析的能力，以满足不同管理范围和安全目标的需求。证实方法按下列内容进行。

a) 分级部署核查：
   1) 部署策略细节审查：对边缘云、区域云和中心云的部署策略进行详细审查，确保策略明确、合理且实施有效；
   2) 实际部署情况评估：实地或远程检查这些云服务的实际部署情况，包括硬件布局、软件配置和网络连接；
   3) 安全配置和维护能力测试：评估系统在配置安全措施和进行定期维护方面的能力，特别是在更新安全策略和应对新威胁时的表现。
b) 集中监测和协同能力测试：
   1) 监测系统功能检验：验证集中监测系统的功能完整性，包括数据收集、事件记录和警报生成；
   2) 协同操作模拟：模拟安全事件，测试不同云环境之间的协同操作和信息共享效率；
   3) 实时数据处理和分析：评估系统在处理大量实时数据并提供准确分析的能力。

c） 快速响应和全局预警系统评估：
1） 响应时间测试：模拟安全事件，记录从事件发生到系统反应的时间，评估响应速度；
2） 预警机制有效性验证：模拟潜在威胁，测试预警机制的有效性和及时性；应急流程和恢复策略评估：检查应急流程的完整性和恢复策略的实用性，确保在面临严重安全威胁时能够有效应对。
d） 全局分析能力验证：
1） 数据分析能力测试：引入复杂的数据集，测试系统的数据处理和分析能力；
2） 洞见生成和报告功能评估：验证系统在生成安全洞见和详细报告方面的能力；
3） 趋势识别和预测能力检验：检查系统在识别安全趋势和预测潜在威胁方面的效率。

7.8.3.3 边缘云管辖范围内的路侧基础设施分级化安全运营管理能力证实方法

针对边缘云管辖范围内的路侧基础设施，以及路侧基础设施及其安全组件，验证系统是否能对边缘云管辖范围内的路侧基础设施实施分级化安全运营管理，以及对路侧基础设施采用合适的安全策略防护手段，并在其升级时提供安全防护。证实方法按下列内容进行。

a） 分级化管理能力核查：
1） 设备和服务分类测试：检查系统是否能够根据安全级别、功能和用途对边缘云中的路侧基础设施进行分类管理；
2） 策略实施和效果评估：模拟不同级别的安全威胁，测试各类设备对应的安全策略的实施效果；
3） 访问控制和权限管理测试：评估系统在设备访问控制和用户权限管理方面的有效性。
b） 安全策略和防护手段验证：
1） 策略细节审查：仔细审查路侧基础设施的安全策略，包括防火墙规则、入侵防御系统配置和加密措施；
2） 实际应用场景模拟：模拟各种安全攻击场景，测试这些策略在实际应用中的有效性；
3） 安全策略更新能力测试：检验系统对安全策略进行更新和调整的能力，以适应新的安全威胁。
c） 升级过程中的安全防护测试：
1） 安全审计和风险评估：在进行升级前，执行安全审计和风险评估，确保升级过程中不会引入新的安全漏洞；
2） 升级过程模拟：模拟升级过程，包括软件更新和硬件更换，以测试在此过程中的安全防护效果；
3） 后升级安全验证：升级后，进行全面的安全测试，确保新系统保持或提升了原有的安全水平。

7.8.3.4 云控安全运营管理能力评估

针对云控安全运营管理及其管理的安全设备和软件，验证云控安全运营管理是否具备配置管理、变更管理、资源容量管理、应用生命周期安全管理、组织安全管理、漏洞管理和补丁管理的能力，以及是否有完备的管理机制。证实方法按下列内容进行。

a） 管理能力评估：
1） 模拟管理场景：设计具体的管理场景，如配置更改、资源分配、应急情况处理等，评估管理者的决策和执行能力；
2） 策略制定和执行测试：检验管理者在制定和执行安全策略方面的能力，包括策略的适应性和实用性；
3） 团队协作和沟通效率：观察和评估管理者如何与团队成员协作，以及沟通策略的有效性。
b） 组织安全管理测试：
1） 安全策略审查：审查组织当前的安全策略，确保其符合最新的安全标准和法规要求；
2） 员工培训和意识提升：测试管理者在提升员工安全意识和培训方面的能力，包括定期（每6个月～12个月）举行的安全培训和演练；

3) 安全文化评估：评估组织内部的安全文化，包括员工对安全政策的遵守程度和安全意识的普及。

c) 漏洞和补丁管理效率检验：

1) 漏洞识别和响应测试：引入已知漏洞，测试管理者识别和响应漏洞的速度和效果；
2) 补丁管理流程审查：评估补丁的选择、测试、部署和验证流程，确保其符合组织的安全要求；
3) 风险评估和报告：评估管理者在处理漏洞和补丁时的风险评估能力，以及其在整个过程中的报告和记录准确性。

7.8.4 应急预案与应急响应证实方法

验证云控平台的安全运营管理及其安全监控和响应系统是否具备有效的安全事件管理、快速安全应急响应和可持续安全事件检测能力。证实方法按下列内容进行。

a) 安全事件管理能力测试：

1) 模拟安全事件：创建多种安全事件的模拟场景，如网络入侵、数据泄露、系统故障等；评估管理员识别并分类这些事件；
2) 事件处理流程检验：评估管理员在处理模拟事件时采取的步骤，包括但不限于立即的响应措施、问题诊断、解决方案的实施，以及后续的修复措施；
3) 事件报告和记录：检查管理员在事件发生后的报告记录是否完善，包括事件详细信息、处理过程、结果分析及未来预防措施的记录。

b) 快速应急响应演练：

1) 应急响应演习：模拟严重的安全威胁或实际系统故障（如 DDoS 攻击、关键系统组件故障），评估管理员执行应急响应流程和决策能力；
2) 响应时间评估：记录从安全事件发生到管理员响应的时间，评估其快速反应的能力；
3) 恢复和缓解策略有效性：分析管理员实施的恢复和缓解策略的有效性，以及对系统运行的影响。

c) 持续安全监测效能评估：

1) 持续监控系统设置检查：审查系统的安全监控配置，确保能够持续检测各类安全威胁；
2) 威胁检测能力测试：引入新的、未知的安全威胁模拟样本，测试系统对新威胁的检测能力；
3) 数据分析和报告生成：评估系统在收集安全事件数据、进行分析和生成报告方面的能力，特别是在处理大量或复杂数据时的表现。

参 考 文 献

[1] GB/T 2423.10-2019 环境试验 第2部分：试验方法 试验Fc：振动(正弦)
[2] GB/T 4208-2017 外壳防护等级（IP代码）
[3] GB/T 17626.2-2018 电磁兼容 试验和测量技术 静电放电抗扰度试验
[4] GB/T 17626.3-2023 电磁兼容 试验和测量技术 第3部分：射频电磁场辐射抗扰度试验
[5] GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南
[6] GB/T 24363-2009 信息安全技术 信息安全应急响应计划规范
[7] GB/T 31168-2023 信息安全技术 云计算服务安全能力要求
[8] GB/T 37092-2018 信息安全技术 密码模块安全要求
[9] GB/T 37373-2019 智能交通 数据安全服务
[10] GB/T 37376-2019 交通运输 数字证书格式
[11] GB/T 37973-2019 信息安全技术 大数据安全管理指南
[12] GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型
[13] GB/T 39204-2022 信息安全技术 关键信息基础设施安全保护要求
[14] GB/T 39335-2020 信息安全技术 个人信息安全影响评估指南
[15] GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求
[16] GB/T 40861-2021 汽车信息安全通用技术要求
[17] GB/T 41479-2022 信息安全技术 网络数据处理安全要求
[18] GM/T 0005-2021 随机性检测规范
[19] YD/T 3594-2019 基于LTE的车联网通信安全技术要求
[20] CSA GCR C001-2022 CSA 云应用安全技术规范
[21] CSA GCR C002-2022 CSA 云原生安全技术规范
[22] 数据出境安全评估办法
[23] 关键信息基础设施安全保护条例
[24] 国家网络安全事件应急预案
[25] 汽车数据安全管理若干规定（试行）
[26] 网络数据安全管理条例
[27] 工业和信息化部关于加强智能网联汽车生产企业及产品准入管理的意见