ICS 03.220.20
CCS R 85

团 体 标 准

T/ITS 0183—2022

车路协同云控基础平台 信息安全技术要求

Cloud control basic platform for vehicle-infrastructure cooperative system—
Technical requirements for cybersecurity

2022－12－05 发布 2022－12－05 实施

中国智能交通产业联盟 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。

本文件由中国智能交通产业联盟（C-ITS）提出并归口。

本文件起草单位：北京百度智行科技有限公司、中国汽车工程研究院股份有限公司、宁波吉利汽车研究开发有限公司、交通运输部公路科学研究院、博世汽车部件（苏州）有限公司、中兴通讯股份有限公司、威马汽车科技集团有限公司、东南大学、启明星辰信息技术集团股份有限公司、郑州信大捷安信息技术股份有限公司、北京信安世纪科技股份有限公司、杭州安恒信息技术股份有限公司、北京信长城科技发展有限公司、上海复旦微电子集团股份有限公司、南京国通智能交通科技有限公司、广州市德赛西威智慧交通技术有限公司、临沂城建建设集团有限公司、山东五棵松电气科技有限公司、西咸新区智慧城市发展集团有限公司、苏州未来智能交通产业研究院、浙江工业职业技术学院、舍弗勒智能驾驶科技（长沙）有限公司、广东盈峰智能环卫科技有限公司、北京航迹科技有限公司。

本文件主要起草人员：史波洋、贾元辉、刘健皓、彭伟、路宏、张杰、佘锋、金晨、焦伟赟、张云、陈增星、陈晓、王艳华、张健、于波、刘献伦、刘为华、付军、焦靖伟、李剑锋、宋娇、刘鹏、刘祎、钱公斌、段永刚、王小军、刘晓阳、张永合、孙文盛、粘凤菊、陈凯、吴作清、辛鲁超、李炳强、季心怡、邱登、万志平、黄志诚。

车路协同云控基础平台 信息安全技术要求

1 范围

本文件规定了车路协同云控基础平台的安全防护框架和安全技术要求。

本文件适用于指导车路协同云控基础平台的设计、开发和建设。

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 35273 信息安全技术 个人信息安全规范

GB/T 37988 信息安全技术 数据安全能力成熟度模型

GB/T 38636 信息安全技术 传输层密码协议（TLCP）

YD/T 3957 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

3 术语和定义、缩略语

3.1 术语和定义

T/ITS 0199.1所规定的及下列术语和定义适用于本文件。

3.1.1

路侧计算单元 road side computing unit

部署在道路、公路沿线或者场端，配合其他设施或系统完成交通信息汇聚、处理与决策的计算模块、设备或设施。

[来源：T/ITS 0180.1，3.1.3]

3.1.2

车载智能终端 onborad intelligent terminal

安装在车辆上，具有信息采集、处理、存储、传输、显示等功能，并提供人机交互操作与控制的智能化车载信息设备。

3.2 缩略语

以下缩略语适用于本文件。

CoAP：受限制的应用协议（Costrained Application Protocal）

CPU：中央处理器（Central Processing Unit）

HTTPS：超文本传输安全协议（Hyper Text Transfer Protocol Secure）

I/O：输入/输出（Input/Output）

MQTT：消息队列遥测传输（Message Queuing Telemetry Transport）

OAuth2.0：开放授权协议2.0（Open Authorization 2.0）

TLS：安全传输层协议（Transport Layer Security）

4 平台安全框架

4.1 安全防护范围

车路协同云控基础平台的信息安全防护范围应包括云基础设施安全、接入安全、应用安全和数据安全，如图1所示。

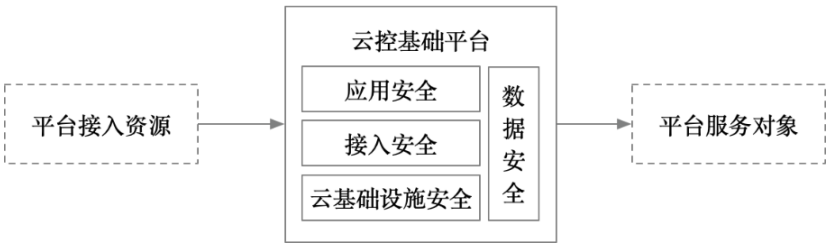

图 1 安全防护范围

4.2 安全防护框架

车路协同云控基础平台安全防护框架如图 2 所示，应包含以下内容：

a) 云基础设施安全：包括系统安全、网络安全、计算安全和虚拟化安全；
b) 接入安全：包括端侧设备接入安全和第三方平台接入安全；
c) 应用安全：包括接口安全、通信安全、访问控制和安全审计；
d) 数据安全：包括对数据收集、存储、加工、传输、提供和销毁的安全防护。

图 2 车路协同云控基础平台安全框架

5 平台安全技术要求

5.1 云基础设施安全

5.1.1 系统安全

云控基础平台在系统安全方面满足以下要求：

a) 应对系统登录的用户进行身份标识和鉴别：
   1) 身份标识具有唯一性；
   2) 身份鉴别应采用多因素认证，例如口令、密码技术、生物技术等两种以上组合的鉴别技术，且其中一种鉴别技术应至少使用密码技术来实现；
b) 应对系统端口、系统运行状态和系统性能进行实时监控，并具备异常事件检测能力，在检测到异常事件时及时上报和处理，确保系统的稳定性和可靠性；
c) 应对用户行为和安全事件进行分级，并对重要的用户行为和重要安全事件进行审计。

5.1.2 网络安全

云控基础平台在网络安全方面满足以下要求：

a) 应根据不同安全域的安全需求使用不同的安全域控制策略；
b) 应对接入用户进行访问控制，并对终端的安全状态进行检测和评估，防止非授权用户或终端连接至云控基础平台；

c) 应建立完善的网络应急响应机制，根据流量分析和规则匹配，及时对攻击做出响应，防止流量攻击破坏云控基础平台网络可靠性和可用性；
d) 应通过网络链路、关键网络设备的冗余机制的建设，实现网络的高可用性。

5.1.3 计算安全

云控基础平台在计算安全方面满足以下要求：
a) 应具备漏洞扫描功能及恶意代码防护机制，定期检测操作系统漏洞并识别安全隐患，评测安全风险，提供改进措施；
b) 应能检测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；
c) 应采用免受恶意代码攻击的技术措施或可信验证机制识别入侵和病毒行为；
d) 若采用可信验证机制，应基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警。

5.1.4 虚拟化安全

5.1.4.1 镜像安全满足以下要求：
a) 应支持虚拟机镜像、快照完整性校验功能，防止镜像被恶意篡改；
b) 应采取加密、漏洞扫描、病毒扫描或其他技术手段防止镜像、快照中可能存在的敏感资源被非法访问。

5.1.4.2 虚拟机安全满足以下要求：
a) 应支持虚拟化平台自身安全防护，抵抗面向虚拟化平台的入侵、篡改等攻击；
b) 应支持虚拟机之间的安全隔离，避免利用虚拟机之间的漏洞，发起针对虚拟机之间或者对外发起的攻击；
c) 应保证不同虚拟机之间 CPU 指令、内存、I/O 端口的隔离；
d) 应对虚拟机的运行状态等信息进行监控。如发生异常行为，宜采取阻断等方式处理。

5.1.4.3 容器安全满足以下要求：
a) 应支持容器编排、管理等组件本身的安全保护，保证容器安全；
b) 应支持容器之间的安全隔离，加强容器逃逸安全问题的防护。

5.1.4.4 宿主机安全满足以下要求：
a) 对登录宿主机的云控平台使用者应进行身份鉴别；
b) 应避免不必要的硬件、冗余软件和服务端口的暴露；
c) 应严格限制默认帐户的访问权限，并确保默认账户没有通用默认口令。

5.2 接入安全

5.2.1 端侧设备

云控基础平台可使用开放协议（HTTPS、MQTT、CoAP 等）自主接入路侧设备、车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。端侧设备接入云控基础平台满足以下要求：
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) 宜采用安全的 TLCP、TLS 加密传输协议确保通信安全，信息交互内容宜根据需要进行加密处理，如使用 TLCP 协议，应符合 GB/T 38636 的规定；
c) 应采用密码等技术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，在设备接入云控基础平台时，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。

5.2.2 第三方平台

第三方平台接入云控基础平台满足以下要求：

a) 云控基础平台与第三方平台使用 HTTPS 和 WebSocket 协议进行信息交互时，宜采用 OAuth 2.0、数字证书等方式进行认证；云控平台与第三方平台使用 MQTT 协议进行信息交互时，宜采用安全的 TLCP、TLS 的方式进行认证；
b) 宜采用安全的 TLCP、TLS 等加密传输协议确保通信数据保密性要求；信息交互内容宜根据需要进行加密处理；
c) 信息交互内容宜根据需要采用密码技术对通信数据进行完整性保护；
d) 云控基础平台应负责管理、维护对第三方平台的接入授权；接口在接入时应告知云控基础平台是否需要授权，若必须授权，则应告知接口的授权范围。

5.3 应用安全

5.3.1 接口安全

云控基础平台对外提供应用服务时，在接口安全方面满足以下要求：
a) 云控基础平台对应用服务接口的调用应进行鉴别，鉴别技术宜采用 OAuth2.0、数字证书、密钥、消息鉴别码等技术，只有鉴别成功后，其应用服务才可以被调用；
b) 若采用 OAuth 2.0 进行认证，应满足以下要求：
   1）第三方平台调用云控平台的认证接口；
   2）云控平台对第三方平台的身份进行验证，如合法则认证通过，否则身份认证失败；
   3）第三方平台的身份验证通过后，云控平台返回令牌信息给第三方平台；
   4）第三方平台调用云控平台数据或服务接口时，需在请求头的授权中加入令牌信息；
   5）云控平台校验令牌信息的有效性，并进行数据交互。

5.3.2 通信安全

云控基础平台对外提供应用服务时，在通信安全方面满足以下要求：
a) 云控基础平台应采用安全通信协议保证通信协议自身安全性，宜采用安全的 TLCP、TLS 等加密传输协议进行传输层安全保护；
b) 云控基础平台应采用密码等技术对通信数据进行保密性和完整性保护；
c) 云控基础平台面向车载智能终端以及其他智能交通参与终端提供 V2X 服务时，宜采用 V2X 的数字证书确保其通信安全，V2X 证书应符合 YD/T 3957 的规定。

5.3.3 访问控制

云控基础平台对外提供应用服务时应具备访问控制机制，且满足以下要求：
a) 云控基础平台应具备对其应用服务调用的访问控制能力，对应用服务调用范围、操作权限进行限定；
b) 支持对接口的访问频率进行限制，对超过正常请求范围的进行预警。

5.3.4 安全审计

云控基础平台对外提供应用服务时应具备安全审计机制，且满足以下要求：
a) 云控基础平台应对应用服务的调用过程进行审计并记录调用时间、类型和结果等内容；
b) 云控基础平台应能提供应用服务调用的审计记录查询、分类、分析和存储保护，确保审计记录不被破坏或非授权访问。

5.4 数据安全

5.4.1 通用要求

云控基础平台上的数据收集、存储、加工、传输、提供、销毁等数据安全应满足GB/T 37988的技术要求，涉及个人信息安全应满足GB/T 35273中的技术要求。

5.4.2 收集

云控基础平台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。云控基础平台在数据收集方面，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) 宜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所必要的安全管理策略和保障措施。

5.4.3 存储

云控基础平台在数据存储方面，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；
a) 应明确数据存储的有效期，支持对数据存储时效性配置；
b) 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；
c) 重要数据应存储在安全区域或以密文形式存储，宜具备对重要数据进行异地保护功能，确保重要数据的完整性和安全性。

5.4.4 加工

云控基础平台在数据加工方面,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。

5.4.5 传输

云控基础平台在数据传输安全方面，满足以下安全要求：

a) 应采用适当的加密保护措施，保证传输通道、传输节点和传输数据的安全，防止传输过程中数据被截取所引发的数据泄漏，宜采用安全的 TLCP、TLS 加密传输协议进行传输层安全保护；
b) 对传输的数据宜采用密码等技术进行保密性和完整性保护；
c) 传输的数据如涉及 V2X 通信数据，宜采用 V2X 的数字证书确保其数据安全，V2X 证书应符合 YD/T 3957 的规定。

5.4.6 提供

云控基础平台在数据提供方面，满足以下安全要求：

a) 应对数据提供的接口进行规范管理，管理内容包括但不限于数据提供接口类型、加密方式、传输周期、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。

5.4.7 销毁

云控基础平台提供者在数据销毁方面，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以再逆向恢复，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。

中国智能交通产业联盟

标准

车路协同云控基础平台 信息安全技术要求

T/ITS 0183-2022

北京市海淀区西土城路 8 号（100088）

中国智能交通产业联盟印刷

网址：http://www.c-its.org.cn

2022 年 12 月第一版　2022 年 12 月第一次印刷