ICS 03.220.20
CCS R 85

团 体 标 准

T/ITS XXXXX—XXXX

车路协同云控基础平台 信息安全技术要求

Technology requirements of cloud-control basic platform cybersecurity based on vehicle-road cooperative

（征求意见稿）

本稿完成时间：2022 年 8 月

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：

本文件主要起草人：

引　　言

本文件主要适用于车路协同云控基础平台安全建设，为车路协同云控基础平台开发、建设提供指导性建议，为车路协同云控基础平台开发者、建设者、使用者提供参考。

车路协同云控基础平台 信息安全技术要求

1 范围

本文件主要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 15852-2020 信息技术 安全技术 消息鉴别码

GB/T 20271-2006 信息安全技术 信息系统通用安全技术要求

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 25069-2010 信息安全技术 术语

GB/T 31168-2014 信息安全技术 云计算服务安全能力要求

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 35279-2017 信息安全技术 云计算安全参考架构

GB/T 37044-2018 信息安全技术 物联网安全参考模型及通用要求

GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型

GB/T 38636-2020 信息安全技术 传输层密码协议（TLCP）

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/ITS 0140-2020 智慧高速公路 车路协同系统框架及要求

T/ITS 0180.1-2021 车路协同信息交互技术要求 第1部分：路侧设施与云控平台

T/ITS 0180.2-2021 车路协同信息交互技术要求 第2部分：云控平台与第三方应用服务

T/ITS XXXX-2022 车路协同云控基础平台 第1部分：通用要求

3 术语和定义、缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

车路协同系统 vehicle infrastructure cooperative systems

采用无线通信和互联网技术，全方位实施车车、车路信息实时交互，并在全时空动态交通信息采集与融合的基础上开展车辆主动安全控制和道路协同管理，实现人、车、路的有效协同，从而形成安全、高效和环保的道路交通系统。

[来源：T/ITS 0140，3.1.1]

3.1.2

云控基础平台 cloud control basic platform

简称“云控平台”。指服务于车路协同业务的平台系统，具有实时信息融合与共享、实时计算编排、智能应用编排、大数据分析、信息安全等基础服务能力，可为智能汽车、管理及服务机构、终端用户提供辅助驾驶、自动驾驶、交通运输安全、交通管理等协同应用和数据服务。

[来源：T/ITS 0180.1，3.1.2]

3.1.3

云计算基础设施 cloud computing infrastructure

由硬件资源和资源抽象控制组件构成的支撑云计算的基础设施。硬件资源包括所有的物理计算资源，包括服务器（CPU、内存等）、存储组件（硬盘等）、网络组件（路由器、防火墙、交换机、网络链接和接口等）及其他物理计算基础元素。资源抽象控制组件对物理计算资源进行软件抽象，云服务商通过这些组件提供和管理对物理计算资源的访问。

[来源：GB/T 31168-2014，3.5]

3.1.4

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]

3.1.5

车载智能终端 vehicle 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。

API：应用程序接口（Application Programming Interface）
CoAP：受限制的应用协议（Costrained Application Protocal）
CPU：中央处理器（Central Processing Unit）
DTLS：数据包传输层安全协议（Datagram Transport Layer Security）
HTTP：超文本传输协议（Hyper Text Transfer Protocol）
HTTPS：超文本传输安全协议（Hyper Text Transfer Protocol Secure）
IP：网际互联协议（Internet Protocol）
I/O：输入/输出（Input/Output）
MQ：消息队列（Message Queue）
MQTT：消息队列遥测传输（Message Queuing Telemetry Transport）
OBU：车载单元（On board Unit）
OEM：原始设备制造商（Original Equipment Manufacture）
OAuth2.0：开放授权协议2.0（Open Authorization 2.0）
PC5：直连通信接口
RSCU：路侧计算单元（Road Side Computing Unit)
TLS：安全传输层协议（Transport Layer Security）
V2X：车载单元与其他设备通信（Vehicle to Everything）
V2N：车载单元与互联网通信（Vehicle to Network）
WebSocket：基于TCP的全双工通信协议

4 概述

4.1 平台架构

4.1.1 车路协同云控基础平台通常为V2X设备提供安全可靠的连接通信能力

4.1.2 车路协同云控基础平台向下连接海量V2X设备，支撑V2X设备数据采集上云

4.1.3 车路协同云控基础平台向上提供云端API，服务端通过调用云端API将指令下发至V2X设备端，实现设备管理、远程控制、监控运维等能力。

4.1.4 车路协同云控基础平台通常由云基础设施层、基础平台能力层、基础应用能力层和保障支撑体系组成，架构图可参考附录A.2。

4.2 平台介入资源

车路协同云控基础平台信息接入资源主要分为以下两类：

a） 端侧设备资源，包括路侧设备、车端设备以及及其他交通参与者携带的智能终端设备。路侧设备主要包括路侧计算单元（RSCU）、路侧感知单元、路侧通信单元以及其他交通设施资源；车端设备主要包括前装或后装的车载智能终端（如OBU）。

b） 第三方平台资源，包括车辆管理与服务平台（如车企OEM平台、公交车管理服务平台）、交通管理平台（如城市交通管理系统、高速公路管理服务平台等）、地图服务平台（如导航地图平台、高精度地图平台）、出行服务平台、气象服务平台以及其他第三方平台。

4.3 平台应用服务

车路协同云控基础平台对外提供的应用服务主要分为以下两类：

a） 面向车载智能终端以及其他智能交通参与终端的应用服务，主要包括辅助驾驶、自动驾驶等车路协同应用服务。

b） 面向第三方平台的应用服务，主要包括智能交通、智慧出行、公共安全等应用服务。

5 平台安全框架

5.1 安全防护范围

本文件所定义的车路协同云控基础平台的信息安全防护范围包括：平台安全、接入安全、数据安全、应用安全，如图1所示。

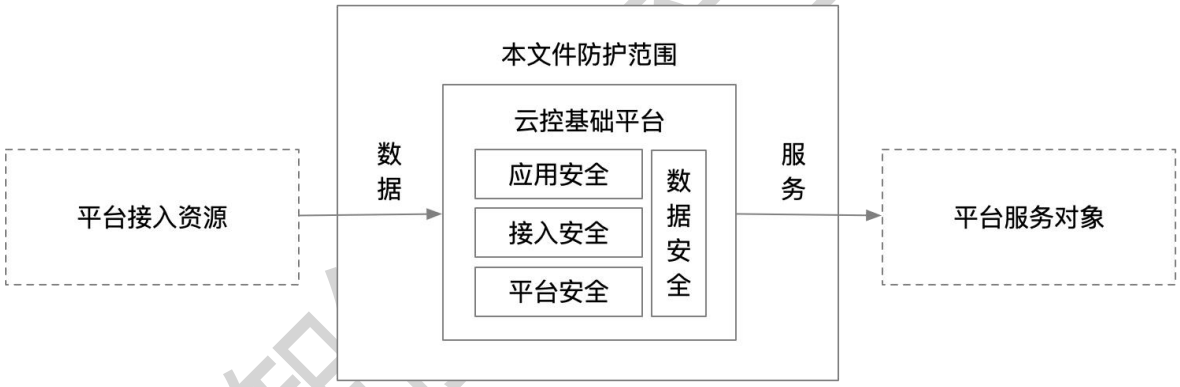

图 1 安全防护范围

5.2 安全防护框架

本文件所定义的车路协同云控基础平台安全防护框架包括：平台安全、接入安全、应用安全、数据安全，如图 2 所示。

a） 平台安全，主要包括部署云控基础平台的云基础设施安全，包括系统安全、网络安全、计算安全、虚拟化安全。

b） 接入安全，主要包括端侧设备接入安全、第三方平台接入安全，主要通过身份鉴别、通信安全、访问控制、安全审计等安全防护措施提升端侧设备、第三方平台等资源接入的安全可靠性。

c） 应用安全，是指通过接口安全、通信安全、访问控制、安全审计等安全防护措施，提升云控基础平台对外提供应用的安全可靠性。

d） 数据安全，是指对在云控基础平台中的数据收集、传输、存储、加工、提供、销毁等环节的数据安全防护。

图 2 车路协同云控基础平台安全框架

6 平台安全技术要求

6.1 平台本体安全

6.1.1 通用要求

云控基础平台的基础设施的通用安全要应符合 GB/T 22239 中的相应等级安全要求。

6.1.2 系统安全

云控基础平台在系统安全方面应满足以下要求：

a) 对系统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；
b) 采用口令、密码技术、生物技术等两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现；
c) 对系统端口、系统运行状态和系统性能等进行实时监控，在出现问题时及时上报和处理，确保系统的稳定性和可靠性；
d) 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。

6.1.3 网络安全

云控基础平台在网络安全方面应满足以下要求：

a) 根据不同安全域的安全需求，应用不同的安全域控制策略；
b) 采取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) 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) 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。

6.1.4 计算安全

云控基础平台在计算安全方面应满足以下要求：

a) 部署漏洞扫描系统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) 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；
c) 采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断；
d) 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。

6.1.5 虚拟化安全

6.1.5.1 镜像安全应满足以下要求：
a) 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) 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。

6.1.5.2 虚拟机安全应满足以下要求：
a) 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) 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) 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。

6.1.5.3 容器安全应满足以下要求：
a) 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) 支持容器之间的安全隔离，加强容器逃逸安全问题的防护。

6.1.5.4 宿主机安全应满足以下要求：
a) 对登录宿主机的云控平台使用者进行身份鉴别；
b) 避免不必要的硬件、冗余软件和服务端口的暴露；
c) 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。

6.2 接入安全

6.2.1 端侧设备

云控基础平台可使用开放协议（如 HTTP/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) 身份鉴别要求：设备接入云控基础平台之前，应通过身份鉴别，身份鉴别技术应采用设备密钥、X.509 证书等密码技术；
b) 通信加密要求：宜采用 TLCP、TLS1.2 等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 内容描述；
c) 数据完整性要求：应采用密码等技术对通信数据进行完整性保护，使用的密码技术应符合国家密码技术相关政策及规范；
d) 访问控制要求：云控基础平台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，在接入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) 安全审计要求：云控基础平台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。

6.2.2 第三方平台

云控基础平台可按需选择HTTP/HTTPS、WebSocket、MQ等通信协议接入第三方平台。其中，HTTP/HTTPS协议可用于低频类业务数据的交互，如登录认证或鉴权业务；WebSocket和MQ通信协议可用于高频类数据交互业务，如信号灯信息和高精地图信息等。第三方平台接入云控基础平台满足以下要求：

a) 身份鉴别要求：云控基础平台与第三方平台使用 HTTP/HTTPS 和 WebSocket 协议进行信息交互时，可采用 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 MQ 协议进行信息交互时，宜采用 TLS 的方式进行认证；
b) 通信保密性要求：应采用 TLCP、TLS1.2 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) 数据完整性要求：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，其中密码算法应使用符合国家密码技术相关政策及规范的密码技术；
d) 接入授权要求：云控基础平台应负责管理、维护对第三方平台的接入授权，只有将接口及及其提供的方法授权给第三方平台时，第三方平台才可调用该接口的方法。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。

6.3 应用安全

6.3.1 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权，鉴权技术宜采用 OAuth2.0、数字证书、密钥、消息鉴别码等技术，只有鉴权成功后，其应用服务才可以被调用。
b) 若使用消息鉴别码技术，应符合 GB/T 15852 要求。
c) 若采用 OAuth 2.0 进行认证，应满足以下要求：
——第三方平台调用云控平台的认证接口；
——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；
——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；
——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；
——云控平台校验令牌信息的有效性，并进行数据交互。

6.3.2 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 TLCP、TLS1.2 等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，使用的密码技术应符合国家密码技术相关政策及规范；
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应用服务时，通过路侧 RSU 与车端 OBU 以 PC5 通信的方式进行信息交互时，应采用 V2X 的数字证书确保其通信安全，V2X 证书应符合 YD/T 3957 内容描述；
d) 通过 V2N 以 Uu 通信的方式进行信息交互时，应采用 TLS1.2 等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和签名处理。

6.3.3 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。

6.3.4 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主体、客体、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。

6.4 数据安全

6.4.1 通用要求

云控基础平台上的数据收集、传输、存储、加工、提供和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。

6.4.2 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，确保数据收集的合规性、时效性和最少够用等原则要求；
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。

6.4.3 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 TLCP、TLS1.2 等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，密码算法应使用符合国家密码技术相关政策及规范的密码技术；
c） 传输的数据如涉及 V2X 通信数据，应采用 V2X 的数字证书确保其数据安全，V2X 证书应符合 YD/T 3957 内容描述。

6.4.4 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；
b） 应明确数据存储的有效期，支持对数据存储时效性配置；
c） 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；
d） 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。

6.4.5 加工

云控基础平台在数据加工方面,满足以下安全要求：

a） 加工重要数据，应在完成脱敏处理后再进行加工处理；
b） 加工个人信息，应在匿名化处理或去标识化处理后再进行加工处理；
c） 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；
d） 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；
e） 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。

6.4.6 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。

6.4.7 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、明确销毁对象和规范销毁流程，并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；

b) 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。

附 录 A
（资料性）
车路协同系统总体架构

A.1 车路协同系统逻辑架构

车路协同系统逻辑架构见图 A.1，由以下四个主要部分构成：

—— 出行者子系统：由出行者所携带的各类信息终端或其它信息处理设备构成；

—— 车载子系统：OBU或其他车载智能终端，也可以包括车载计算控制模块、车载网关、路由器等；

—— 路侧子系统：以RSCU、路侧通信设施、路侧感知设施为核心，也可包括交通安全与管理设施或其他附属设施等；

—— 中心子系统：包括云控平台和相关第三方平台，提供设备接入管理、数据汇聚共享、业务支撑和相关服务。

[来源：T/ITS 0180.1-2021，4.1.1]。

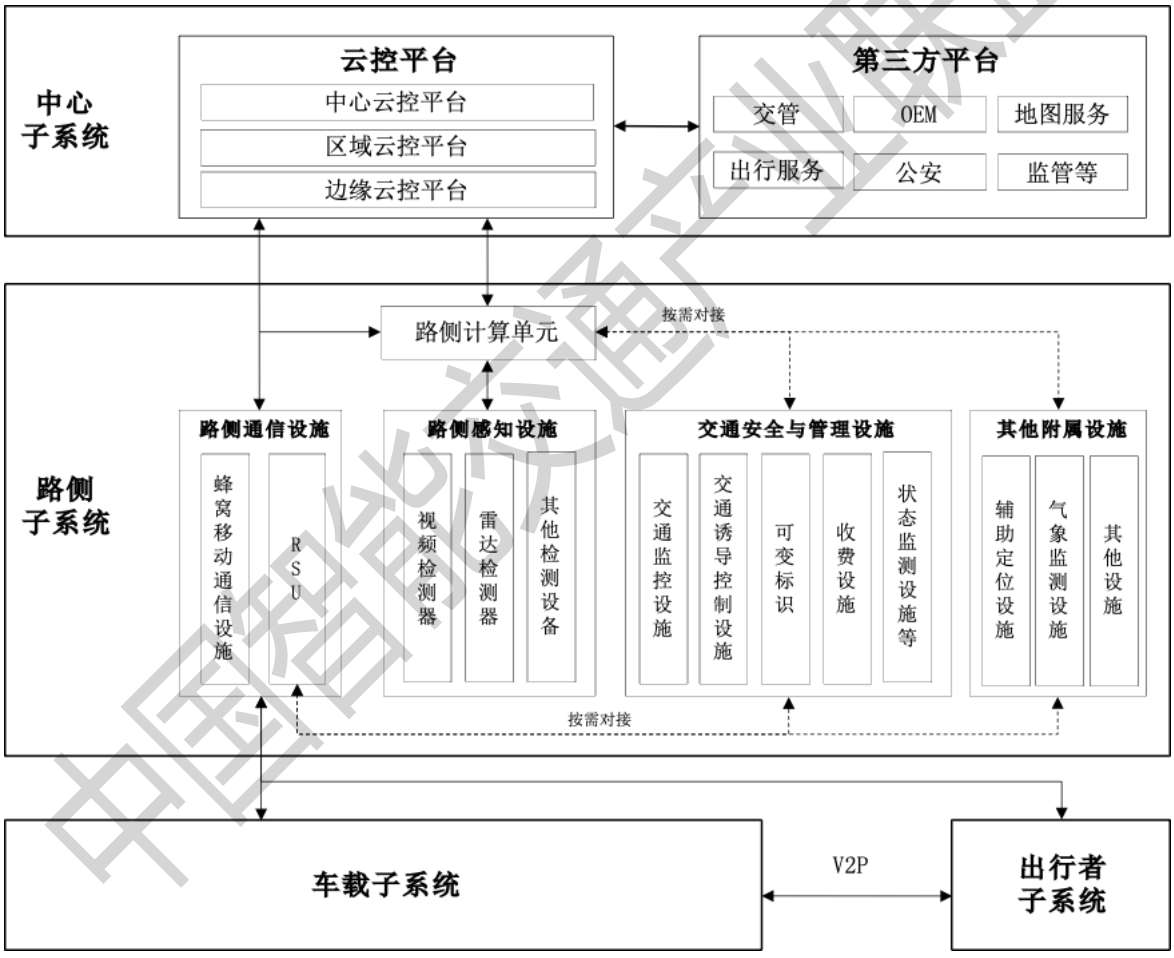

图 A.1 车路协同系统逻辑架构

A.2 云控基础平台架构

云控基础平台由云基础设施层、基础平台能力层、基础应用能力层和保障支撑体系组成，具体架构如图 A.2所示，其中：

a) 云基础设施提供云资源及云资源管理、运行和云服务调用相关的框架支撑；

b) 基础平台能力层提供以数据采集、处理和服务的通用基础功能；

c） 基础应用能力围绕产业链上下游协作，为用户提供可重用的微服务或行业服务；
d） 保障支撑体系提供平台运维管理和安全可信能力。

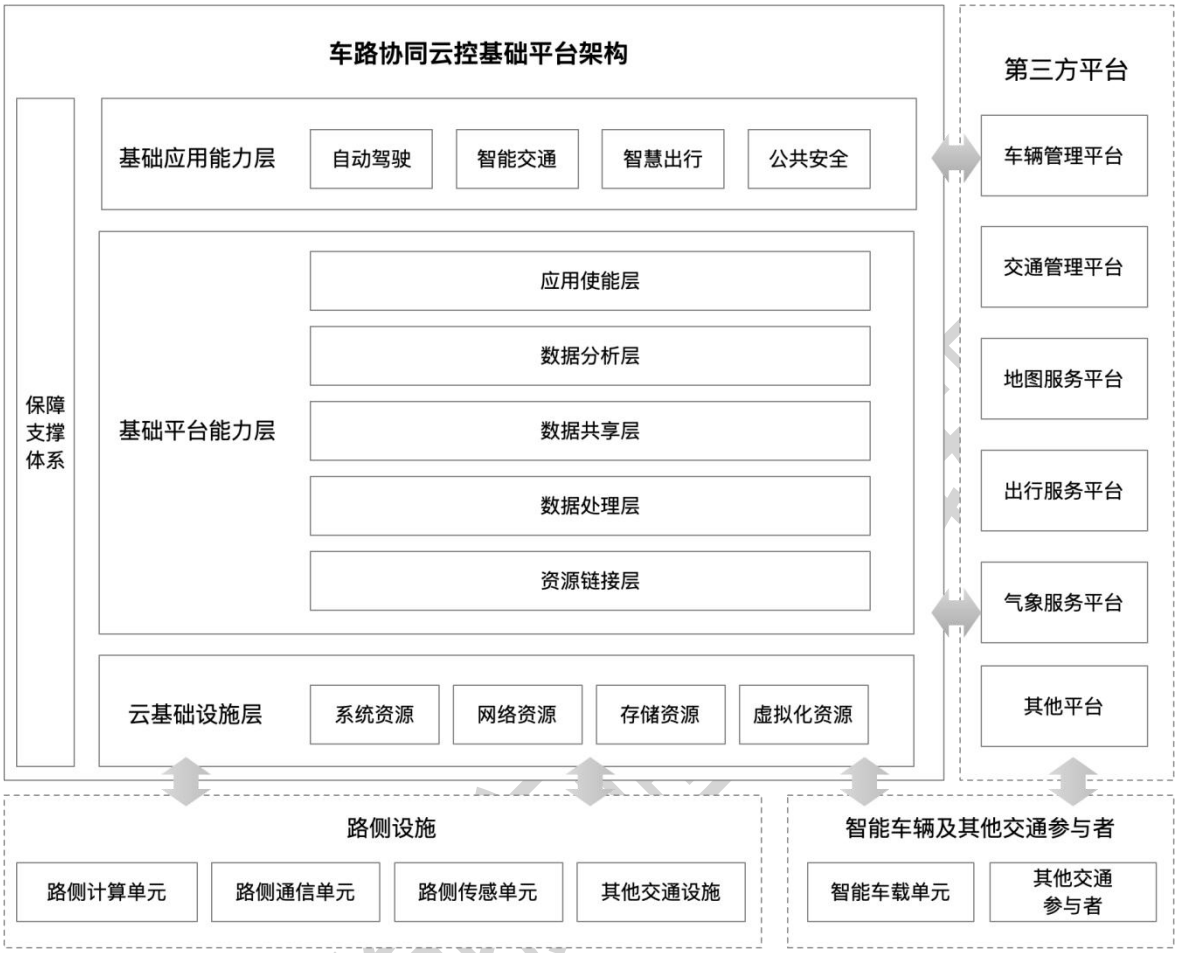

图 A.2 云控基础平台架构

A.3 云控基础平台对外应用服务架构

云控基础平台是中心子系统的组成部分之一，一般可分为边缘云控平台、区域云控平台和中心云控平台。云控基础平台对外提供应用服务的架构见图 A.3，可根据实际业务需要选择边缘云控平台、区域云控平台或中心云控平台进行对接。

[来源：T/ITS 0180.1-2021，4.1.1]。

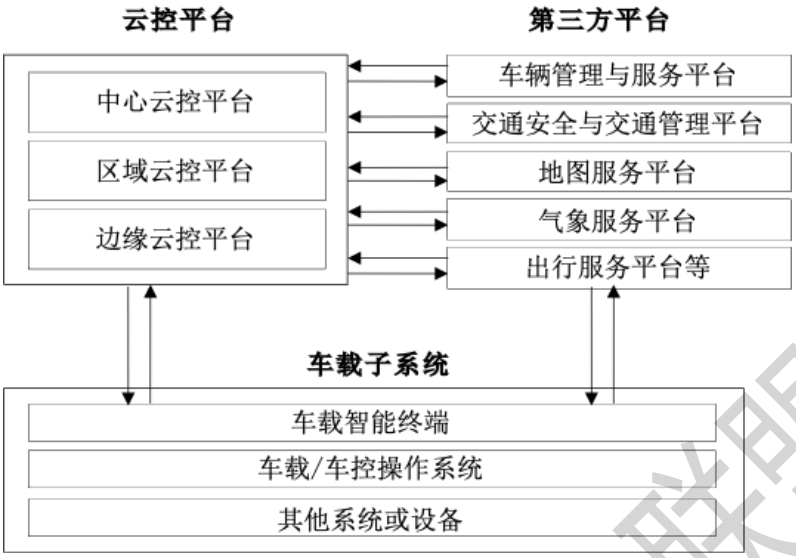

图 A.3 云控基础平台对外应用服务架构

T/ITS XXXX-XXXX

中国智能交通产业联盟

标准

自动驾驶公交车　第 1 部分：车辆运营技术要求

T/ITS XXXXX-202X

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

202X 年 XX 月第一版　202X 年 XX 月第一次印刷