ICS XX.XXX
X XX

团 体 标 准

T/ITS XXXX—2021

港口无人驾驶集装箱卡车性能和测试方法 第 2 部分：无线通讯和信息安全要求

Port unmanned container truck performance and test methods

Part 2: Wireless communication and information security requirements

（征求意见稿）

2017-XX-XX 发布 202X-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。

本文件由中国智能交通产业联盟提出并归口。

本文件起草单位：

本文件主要起草人：

引　　言

本文件规定了智能网联港口无人驾驶集装箱卡车的术语及定义，自动驾驶在智能网联港口的无线通讯和信息安全的技术和要求，提出了自动驾驶系统的无线通讯和信息安全特点及其重要性，适用于智能网联港口无人驾驶集装箱卡车自动驾驶系统的开发过程。

为使港口无人驾驶集装箱卡车能够按统一的标准进行说明和描述，特制定本文件。

为了保持标准的适用性与可操作性，各使用者在采标过程中，及时将对本文件规范的意见及建议函告中移（上海）信息通信科技有限公司，以便修订时研用。

港口无人驾驶集装箱卡车性能和测试方法
第 2 部分 无线通讯和信息安全要求

1 范围

本文件规定了港口无人驾驶集装箱卡车无线通讯和信息安全要求。

本文件适用于为实现基于蜂窝车联网技术的智能网联港口无人集装箱卡车运输系统所使用的通信设备。

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。

BD 420021-2019 北斗/全球卫星导航系统（GNSS）网络RTK中心数据处理软件要求与测试方法

BD 420023-2019 北斗/全球卫星导航系统（GNSS）RTK接收机通用规范

BD 420009-2015 北斗/全球卫星导航系统（GNSS）测量型接收机通用规范

GB/T 31024.1 合作式智能运输系统专用短程通信 第1部分：总体架构

GB/T 31024.2 合作式智能运输系统专用短程通信 第2部分：媒体访问控制层和物理层规范

GB/T 31024.3 合作式智能运输系统专用短程通信 第3部分：网络层和应用层规范

T/ITS 0058-2016 合作式智能运输系统车用通信系统应用层及应用数据交互标准

T/ITS 0097-2016合作式智能运输系统 通信架构

2018-0173T-YD_基于LTE的车联网通信安全技术要求

3 术语、定义和缩略语

下列术语和定义适用于本文件。

3.1 术语和定义

3.1.1

智能网联汽车 Intelligent & Connected Vehicle(ICV)

搭载先进的车载传感器、控制器、执行器等装置，并融合现代通信与网络技术，实现车与 X（人、车、路、云端等）智能信息交换、共享，具备复杂环境感知、智能决策、协同控制等功能，可实现“安全、高效、节能”行驶，并最终可实现替代人来操作的新一代汽车。

3.1.2

无线通信设备 radio communications equipment

包括一个或多个无线电发信机和/或收信机和/或固定使用、车载使用、便携使用的通信设备或其中的某

部分。无线通信设备可以与辅助设备一起使用，但基本功能不依赖辅助设备完成。

3.1.3

多接入边缘计算 Multi-access Edge Computing

多接入边缘计算（MEC）是一种基于移动通信网络的全新的分布式计算方式，构建在RAN（无线接入网）侧的云服务环境，通过使一定的网络服务和网络功能脱离核心网络，实现节省成本，降低时延和往返时间，优化流量，增强物理安全和缓存效率等目标。

3.1.4

辅助设备 ancillary equipment

与无线通信设备连接使用的设备。且满足与无线通信设备相连，以提供额外的操作和/或控制特性；就独立于无线通信设备之外使用就不能提供单独的用户功能；所连接的无线通信设备在无此辅助设备时仍能进行发射和/或接收等预定的操作（即辅助设备不是主设备基本功能的子单元）。

3.1.5

机箱端口 enclosure port

设备的物理边界，电磁场通过该边界辐射或照射。插件的物理边界由宿主单元定义。

3.1.6

主机设备 host equipment

不需要连接无线通信设备就可以完整运行功能的任何设备。无线通信设备只是提供额外功能。

3.1.7

端口 port

指定设备（装置）与外部电磁环境之间的特定接口。

3.1.8

信号/控制端口 signal and control

传送消息和控制信号的端口，不包含天线端口。

3.1.9

负载 load

终端在某一电路（如放大器）或电器输出端口，接收电功率的元器件、部件或装置统称为负载。

3.1.10

车载单元 On Board Unit(OBU)

安装在车辆上的可实现 V2X 通讯，支持 V2X 应用的硬件单元。

3.1.11

路侧单元 Road Side Unit(RSU)

安装在路边的可实现 V2X 通讯，支持 V2X 应用的硬件单元。

3.1.12

车用无线通信技术 Vehicle-to-Everything (V2X)

将车辆与一切事物相连接的新一代信息通信技术，其中V代表车辆，X代表任何与车交互信息的对象，当

前X主要包含车、人、交通路侧基础设施和网络。

3.1.13

自动驾驶系统 Autonomous Driving System

能够持续地执行部分或全部动态驾驶任务和/或执行动态驾驶任务接管的硬件和软件所共同组成的系统。

3.1.14

指令 Instruction

调度员输入信号和测试车辆通过感知、地图等信息自主发出的信号。例如变更车道场景， 测试车辆获得指令后执行变更车道动作,此时指令既可是调度员操纵转向指示灯发出的执行信号也可是测试车对车辆转向、加速、制动、灯光等系统的控制权。

3.1.15

智能车管平台 Intelligent vehicle management platform

智能车管平台负责和港口生产管理系统对接并将调度指令传递给港口无人驾驶集装箱卡车实现智能化业务运营，并将港口无人驾驶集装箱卡车的实时工作状态及智能驾驶信息回传给港口生产管理系统进行动态检查，智能车管平台能自动判断港口无人驾驶集装箱卡车异常状态，根据异常状态的紧急程度进行不同程度的预警和干预。

3.1.16

调度员 dispatcher

在港口车辆无驾驶员操作的条件下，通过激活驾驶自动化系统以实现车辆调度服务但不执行动态驾驶任务的用户。

注：装备有4级和5级驾驶自动化功能，且其ODD覆盖整个行程的车辆才可被调度。如果驾驶自动化系统未规划线路，调度员还需要指定目的地。

3.1.17

设计运行范围 Operational Design Domain (ODD)

设计时确定的驾驶自动化系统的运行条件，包括但不限于：道路、环境、交通、速度。

3.2 缩略语

以下缩略语适用于本文件：

LTE：长期演进（long Term Evolution）

5G：第五代移动通信技术（the 5th Generation mobile communication technology）

OBU：车载单元（On-Board Unit）

RSU：路侧单元（Road Side Unit）

MEC: 多接入边缘计算MEC（Multi-Access Edge Computing）

GNSS：全球导航卫星系统（Global Navigation Satellite System）

BDS：北斗卫星导航系统（BeiDou Navigation Satellite System）

GPS：全球定位系统（Global Positioning System）

RTK：载波相位差分技术（Real-time kinematic）

IVI：车载信息娱乐系统（In-Vehicle Infotainment）

ECU：电子控制单元（Electronic Control Unit）

APP：应用软件（Application）

T-BOX：远程信息处理器（Telematics BOX）

TSP：汽车远程服务提供商（Telematics Service Provider）

4 无线通讯技术要求

4.1 总则

港口无人驾驶集装箱卡车控制产品的物理结构是把技术逻辑结构所涉及的各种“信息感知”与“决策控制”功能落实到物理载体上。车辆控制系统、车载终端、交通设施、外接设备等按照不同的用途，通过不同的网络通道、软件或平台对采集或接收到的信息进行传输、处理和执行，从而实现了港口无人驾驶集装箱卡车控制产品的功能或应用（如图 1 所示）。

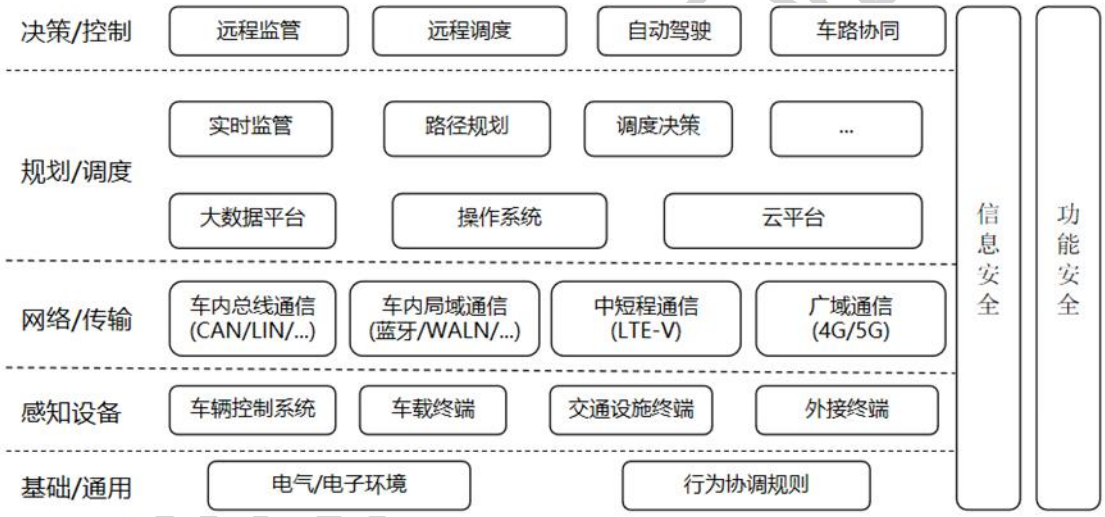

图 1 港口无人驾驶集装箱卡车控制产品物理结构

决策与控制层是根据智慧港口的应用场景需求设定的，包含远程监管、远程调度、自动驾驶、车路协调等功能，实现港口无人驾驶集装箱卡车的智慧监管、调度及运营。

规划与调度层主要涵盖车载计算平台和操作系统等基础平台产品，实时数据监管、诊断、路径规划、调度决策等应用服务，共同为港口无人驾驶集装箱卡车控制相关功能的实现提供平台级、系统级和应用级的服务。

网络与传输层根据通信的不同应用范围，分为车内总线通信、车内局域通信、中短程通信和广域通信，给信息传递提供智能的“通道”。

感知设备层按照不同的功能或用途，分为车辆控制系统、车载终端、交通设施终端、外接设备等，各类设备和终端是车辆与外界进行信息交互的载体，同时也作为人机交互界面，成为连接“人”和“系统”的载体。

基础和通用层涵盖电气/电子环境以及行为协调规则。安装在港口无人驾驶集装箱卡车上的设备、终端或系统需要利用汽车电源，在满足汽车特有的电气、电磁环境要求下实现其功能；设备、终端或系统间的信息交互和行为协调也应在统一的规则下进行。

4.2 功能要求

4.2.1 车路协同

港口基于车路协同的无人驾驶系统由车路协同平台子系统、路侧子系统、车辆子系统和网络子系统组成，见图 2。路侧子系统包含道路基础监控设施、智能路侧感知设施、港机设备通信设施、电子标志标线设施等。其中港机设备通信设施可以与路侧通信设施、车辆通信设施进行通信，实现港口作业相关信息的交互。

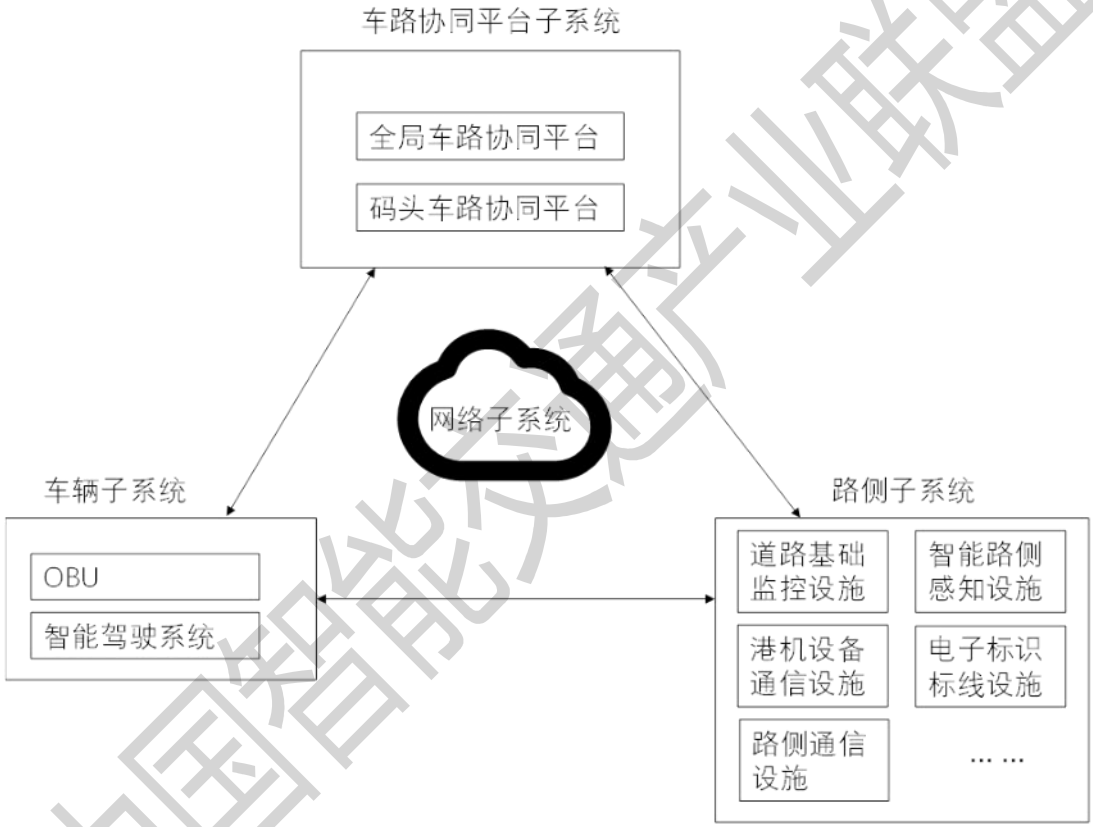

图 2 港口基于车路协同的无人驾驶系统

车辆子系统包含 OBU 和智能驾驶系统等。OBU 可以通过 V2X 通信方式将车辆信息传输给路侧子系统，也可以接收来自路侧子系统的数据。智能驾驶系统采用先进的通信、计算机、网络和控制技术，利用视频摄像头、雷达传感器等设备来了解周围的交通状况，对车辆实现实时、连续控制。要求如下：

a) 功能要求：

1) 港口无人驾驶集装箱卡车需支持车辆传感器采集数据的上报，采集数据类型如下：

- 车辆信息采集如车辆识别号、车辆类型、位置、速度、加速度、方向角等；
- 车载终端自主上传多接入边缘计算（MEC）的信息如紧急报警信息、事故信息等；

2) 港口无人驾驶集装箱卡车需支持接收路侧子系统数据，接收数据类型如下：

- 交通参与者信息，如港机设备、作业人员、临近车辆的位置、速度、运动方向信息；
- 路面障碍物分类与位置信息；

b) 车联网需求指标：

表 1 车联网无线网络需求指标

业务名称	整体需求描述	网络接入要求	通信需求		
			带宽	传输时延	可靠性
车联网	低延时，高可靠	支持多种无线和有线接入技术，包括 LTE、LTE-V、5G、蓝牙及 WIFI 等	10-20Mbps	≤50ms	≥99.9%

4.2.2 车载 GNSS 定位

高精度 GNSS 系统包含地基参考站网、数据处理与控制中心、数据播发平台、车载终端。通过建立永久性观测基准站，实时接收卫星系统观测数据并传输至解算平台，由解算平台将基准站定位结果与预存储的精确坐标比较形成差分改正数，并将其播发给相应终端以供其纠正定位结果，终端由此获得 GNSS 的高精度定位信息。

a) 港口无人驾驶集装箱卡车车载 GNSS 定位接收机的无线通讯功能应符合以下要求：

1) 接收卫星信号能力：车载 GNSS 接收机具备仅接收单卫星信号实现高精度测量的能力，也能支持 BDS（北斗卫星导航系统）、GPS（全球卫星导航系统）、GLONASS（格洛纳斯卫星导航系统）联合 RTK（载波相位差分技术）差分工作能力；

2) 通道数与跟踪能力：参考 BD 420009-2015 中 4.6.2 的规定，接收机通道数与跟踪能力的要求见表 2；

表2 接收机通道数与跟踪能力

接收机类别	频点数	最小系统组成	通道数
单模单频	≥1	BDS	≥12
多模单频	≥2	BDS、GPS/GLONASS	≥24
单模多频	≥2	BDS	≥24
多模多频	≥4	BDS、GPS/GLONASS	≥48

3) 定位数据输出能力：车载 GNSS 接收机支持通过 LTE、LTE-V、5G、蓝牙及 WIFI 等无线通信方式向外输出数据，输出频率可为 1Hz、2Hz 的频率；

4) RTK（载波相位差分技术）服务接收能力：车载 GNSS 接收机具备以 LTE、LTE-V、5G 等无线方式接收来自 RTK 数据处理中心的差分信号；

b) 车载 GNSS 定位需求指标：

表3　车载GNSS定位无线网络需求指标

业务名称	整体需求描述	网络接入要求	通信需求		
			带宽	定位数据上传到控制平台的传输时延	可靠性
车载 GNSS 定位	低延时，高可靠	支持多种无线和有线接入技术，包括 LTE、LTE-V、5G、蓝牙及 WIFI 等	>200Kbps	≤100ms	≥99.9%

表4　车载GNSS定位性能指标

应用场景分类	数据更新率		定位参数		信号跟踪时间	可靠性
	原始数据更新率	RTK定位数据更新	静态差分精度	RTK实时差分精度		
高精度定位	1Hz、2Hz	1Hz、2Hz	水平: $(\pm 2.5 + 1 \times 10^{-6} \times D)$mm D为被测点间距$Km$ 垂直: $(\pm 5 + 1 \times 10^{-6} \times D)$ mm	水平: $(\pm 10 + 1 \times 10^{-6} \times D)$ mm 垂直: $(\pm 20 + 1 \times 10^{-6} \times D)$ mm	信号重捕获 ＜2s	99.9%

4.2.3　远程控制

港口无人驾驶集装箱卡车感知设备的感知距离和传感器对周围环境检测的固定范围，并且感知范围还受到障碍物限制，如果车辆出现严重异常行为（车辆异常加速、爆胎、冲撞电子围栏等），调度员可在智能车管平台进行远程接管，通过摄像头查看周边环境、进行故障判断，远程操作港口无人驾驶集装箱卡车退出故障区。要实现远程控制，港口无人驾驶集装箱卡车需满足：

a)　功能要求：

1)　接收来自智能车管平台的指令；

2)　根据远程控制指令，执行操作；

3)　支持设备外置、内嵌多种方式采集数据。当启动远程控制后，共享其视频信息和传感器信息，为远程操作员提供足够的环境感知信息，港口无人驾驶集装箱卡车至少需要安装 4 路摄像头，对上行带宽的需求将达到 10-20Mbps/台。

b)　远程控制需求指标：

2)　表5　远程控制无线网络需求指标

业务名称	整体需求描述	网络接入要求	通信需求		
			带宽	传输时延	可靠性
远程控制	低延时，高可靠，大带宽	支持多种无线和有线接入技术，包括 LTE、LTE-V、5G、蓝牙及 WIFI 等	≥80Mbps	＜30ms	≥99.9%

5 信息安全技术要求

5.1 安全体系架

智能网联汽车信息安全架构如图3所示，整体安全由云端安全、通信安全、车辆安全等多个部分构成。其中车载端作为智能网联汽车内外通信的重要节点，是车辆安全的重要组成部分，保证汽车内部总线和子系统不因车辆具有联网功能而增加安全风险。

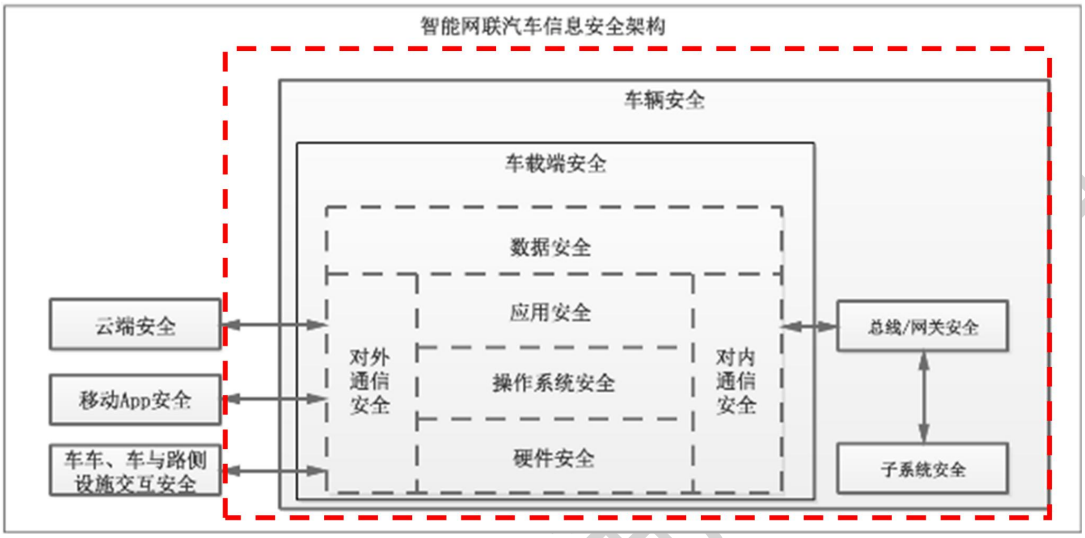

图3 智能网联汽车信息安全体系架构

5.2 安全威胁分析及技术要求

5.2.1 云服务平台

云服务平台可能存在安全漏洞，使得攻击者利用 Web 漏洞、数据库漏洞、接口 API 安全注入漏洞等攻击云平台，窃取敏感信息，以及面临拒绝服务攻击等问题。除了传统云服务平台漏洞外，云端与两端的传输安全、云端 OTA 升级整车零部件的安全问题也多次出现。

5.2.2 车载终端平台

车载终端包括IVI、T-box、汽车网关、其它 ECU 电子器件、传感器、外部接口等，IVI、T-Box 等组件一般包含操作系统、APP 应用和大量的第三方库，并且具有丰富的通信连接。一方面，操作系统、第三方库、协议栈可能含有大量的已知漏洞，攻击者可以通过已知漏洞攻入汽车内部网络，进而进行下一步渗透测试；另一方面，ECU 电子器件、车内 CAN 网络可能存在漏洞，攻击者可以通过 IVI 或 T-Box 进一步攻击网关或其它 ECU 电子器件（例如动力域 ECU），进而形成完全控车威胁。

5.2.3 设备终端

移动 APP 成为智能网联汽车的标配，由于获取成本极低，通过技术手段可以破解通信密钥、分析通信协议，并结合车联网远程控制功能干扰用户使用，同时也可协助对 IVI/T-BOX 进行渗透测试，通过攻击车联网关键部件影响车辆行驶安全。

5.2.4 通信网络

车与云、车与车和车内的通信存在被攻击风险，主要风险如下：一是认证安全，用户通信网络未验证发送者的身份信息，存在伪造身份、动态劫持等风险。二是传输安全，车辆信息没有加密或加密强度弱，或所有车型都使用相同的对称密钥，进而导致密钥信息暴露。三是协议安全，公众通信网络还面临协议伪装等风险。特别是在自动驾驶情况下，汽车根据 V2X 通信内容判断行驶路线，攻击者就有可能利用伪造消息来诱导车辆发生误判，进而影响车辆自动控制，导致交通事故的发生。

5.3 汽车信息安全威胁列表

参考《信息安全技术 信息系统安全等级保护基本要求》，使用 STRIDE 和 TVRA 分析方法建立威胁列见表6。

表6 汽车信息安全威胁列表

评估对象	威胁组件	威胁描述（举例）	影响范围
云服务平台	OTA 升级	OTA 升级过程面临升级包泄露、篡改风险， 从而攻击者可以获取敏感信息，或向升级包中置入后门。	TSP、T-Box
	管理平台登录	弱身份认证缺陷使得攻击者能通过伪造凭证的方式访问车联网管理平台，并进行网络攻击。	TSP
	服务端功能	后端服务中的管理错误，或者存储用于诊断车库数据时发生错误分享，导致信息泄露、共享。	TSP
	云端存储	敏感数据可能因第三方云服务提供商存储的攻击或事故，造成泄露或丢失	TSP
	服务端代码	代码可能存在 SQL 注入、跨站脚本、用户鉴权、账户口令等安全漏洞，使得攻击者利用漏洞窃取隐私、篡改等攻击。	TSP
车载终端	IVI	IVI 附属功能多、集成度高，因而攻击面大、风险多，所有接口都有可能成为黑客攻击的节点，攻击者可以通过攻击 IVI 作为跳板，进而控制车辆行驶，对整车系统造成篡改、拒绝服务、隐私泄露等安全威胁。	ECU、Gateway、T- BOX/IVI
	T-Box	攻击者通过逆向分析 T-BOX 固件，获取加密算法和密钥，从而解密通信协议，用于窃听隐私或伪造控车指令；或者通过 T-BOX 预留调试泄露内部信息用于攻击分析。	ECU、Gateway、T- BOX/IVI
	汽车网关	网关系统代码可能存在漏洞，攻击者利用车载以太网或 CAN 总线漏洞攻击网关，可以造成网关的篡改、拒绝服务、指令伪造等风险。	ECU、Gateway、T- BOX/IVI
	其它 ECU	车内各类 ECU 存在固件代码篡改、拒绝服务等威胁。	ECU、Gateway、T- BOX/IVI
	传感器	攻击者可以通过攻击胎压监测传感器漏洞进入汽车内部网络，对车内网络进行拒绝服务或进一步渗透攻击，进而影响车辆行驶安全。	ECU、Gateway、T- BOX/IVI
	OBD 接口	OBD 接口接入的外接设备可能存在攻击代码，接入后容易将安全威胁引入到汽车总线网络中，对汽车总线控制带来威胁。	ECU、Gateway、T- BOX/IVI
	充电接口	充电接口驱动存在漏洞，恶意攻击者通过在充电桩上置入病毒恶意代码，在汽车充电时“感染”汽车。	ECU、Gateway、T- BOX/IVI

表6 （续）

	板载硬件	板载硬件中暴露可用的调试连接接口，攻击者可以使用连接泄露硬件内部信息或泄露， 进而帮助攻击者进一步的车辆渗透。	ECU、Gateway、T- BOX/IVI
	固件	硬件 flash 中的固件未做防护，使得攻击者可提取、修改，造成代码、密钥等泄漏。	ECU、Gateway、T- BOX/IVI
	存储系统	攻击者可以使用侧信道攻击技术获取芯片中的隐私信息。	ECU、Gateway、T- BOX/IVI
手机终端	App	通过调试或者反编译应用来获取通信密钥、分析通信协议，并结合车联网远程控制功能伪造控制指令干扰用户使用，例如进行远程锁定、开启天窗等操作。	APP、TSP
	用户登录	可以伪造假的 TSP 骗取用户登录信息类似钓鱼网站的危害。	APP、TSP
	数据存储	私人或敏感数据（如付款信息，驾驶习惯 等）可能会在汽车出售给其他用户时泄露， 可能因交通事故或盗窃，敏感数据的泄漏造成人身伤害	APP
通信网络	TSP 通信网络	可以对 TSP 网络通信进行 dos 攻击，阻止其提供正常的服务	TSP、APP、T-Box
	蜂窝通信	攻击者通过伪基站、DNS 劫持等手段劫持T- BOX 会话，监听通信数据，一方面可以用于通信协议破解，另一方面可窃取汽车敏感数据，如汽车标识 VIN、用户账户信息等。	T-BOX/IVI
	LTE-V2X 通信	车车通信中存在恶意节点入侵，可通过阻断、伪造、篡改车-车通信或者通过重放攻击影响车- 车通信信息的真实性，破坏车- 车通信消息的真实性，影响路况信息的传递。	ECU、Gateway、T- BOX/IVI
	Wifi 通信	通过实现 WiFi 认证口令破解，攻击者可以接入到汽车内部网络，获取汽车内部数据信息或者进行渗透攻击。	T-BOX/IVI
	蓝牙通信	例如，蓝牙钥匙代码被篡改（例如固件篡 改，置入后门）、权限提升（例如可能进行除开车门的其它高级功能）风险或蓝牙信号泄露数字钥匙信息。	T-BOX/IVI
	车载以太网	Wifi 与车载以太网不做隔离，导致攻击者可以通过 wifi 破解接入 T-Box、网关等车载以太网节点，进而对整车进行渗透测试。	ECU、Gateway、T- BOX/IVI
	CAN 总线	在车内总线上、车内服务系统上持续发送模拟数据信号，导致驾驶系统发生意外或者通过远程诊断漏洞向T-Box 或IVI 等置入后门。	ECU、Gateway、T- BOX/IVI

5.4 汽车信息安全技术要求

5.4.1 硬件安全技术要求

汽车零部件应避免存在用以标注芯片、端口和管脚功能的可读丝印；禁用设计验证阶段所使用的调试接口，若必须保留，则必须采用一定的安全访问控制措施；通过硬件措施来防范对固件的提取与逆向。

车载终端系统采用HSM硬件加密芯片，且不能存在可以非法对芯片内存进行访问或者更改芯片功能的隐蔽接口。芯片在设计验证阶段使用的调试接口应在上市产品中禁用。

车载终端系统的电路板上不应标注芯片、端口和管脚功能的可读信息。

车载终端系统芯片之间敏感数据的通信线路应尽量隐蔽，对抗针对车载终端内部数据传输的窃听和伪造攻击。

车载终端所使用的关键芯片应尽量减少暴露管脚（例如：采用BGA/LGA封装的芯片）。

车载终端具备硬件实现的安全区域或安全模块， 能够有效地实现敏感数据安全存储和运算的物理隔离， 应使用必要的安全机制保障此区域的数据不被非授权访问。

车载终端具备硬件实现的安全区域或安全模块，实现车载终端设备重要数据安全存储与隔离。

在安全区域或安全模块中一次性写入的敏感信息，应不能非授权获取或者篡改。

安全区域或安全模块应具备检测与处置非授权访问的能力，对抗暴力破解。

使用必要的安全机制（例如：封装），防御针对芯片的电压、时钟、电磁、激光等方式的故障注入攻击。

使用必要的防护措施，对抗针对加密芯片的简单功耗分析、差分功耗分析、相关功耗分析，以及利用运行时间、温度等其它信息进行的侧信道攻击。

使用必要的防护机制，对抗针对车载终端设备内存的侵入和篡改攻击。

5.4.2 操作系统安全技术要求

汽车操作系统应及时进行补丁升级；提供安全调用控制与呈现能力；对必须保留的本地或远程管理功能，则要采取必要的安全访问控制措施；通过技术手段对整个系统进行必要的机密性、完整性和可用性防护。

应在安全存储区域存储操作系统签名。操作系统启动时应使用可信机制，在验证操作系统签名并判定通过后，再从可信存储区域加载车载终端操作系统，避免加载被篡改的操作系统。

如车载终端存在多个操作系统，应采用隔离机制，保障不同操作系统之间的安全防护。

应提供安全机制，保障操作系统只能加载启动可信的车载终端应用程序，能够验证应用的来源和完整性，避免运行恶意程序。应采用完整性校验手段，对关键代码或文件进行完整性保护。

车载终端系统不应存在国家漏洞管理机构发布了6个月及以上的高危安全漏洞。系统应具有能够及时进行漏洞修复的功能。

5.4.3 应用安全技术要求

应用安全要保证安装在汽车上的应用软件具备相应的来源标识和保密性、完整性和可用性的防护措施，可以对抗逆向分析、反编译、篡改、非授权访问等各种针对应用的安全威胁，并确保应用产 生、使用的数据得到安全的处理、车载端应用与相关服务器之间通信的安全性，保证应用为用户提供服务时，以及应用在启动、升级、登录、退出等各模式下的安全性。

应用软件不应存在国家漏洞管理机构发布了6个月及以上的高危安全漏洞。

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。

应用不以明文形式存储用户敏感信息（例如：用户口令、证件号、交易口令、私钥）。

应用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。

应用软件应采用代码签名认证机制，且代码签名机制符合相关标准要求。

关键应用程序在启动时应执行自检，检查程序运行时所必须的条件，确保程序自身和所处运行环境的安全性。

应用软件运行期间，应具备运行验证及编译混淆能力，防止运行数据被非法分析或代码被非法执行。

使用安全机制，防止和检测应用软件之间不必要的访问，避免数据泄漏、非法提权等安全问题。

具备识别、阻断恶意软件的能力，隔绝已经被感染的文件，拒绝软件的恶意访问。

5.4.4 通信安全技术要求

汽车敏感或重要信息通信过程，要对通信双方实施双向身份认证，对通信进行必要的加密处理； 要能够防范重放攻击和中间人攻击。

5.4.5 数据安全技术要求

车载终端所采集的与用户身份、位置信息等相关的敏感数据，应通过显式的方式告知用户并获得用户确认，应说明数据采集的依据。

车载终端对用户数据的采集应在提供相应服务的同时进行。若出于业务需要而必须事先采集相关数据，应向用户明示事先采集的目的和范围，并且只有在用户同意的情况下方可采集。

车载终端采集用户使用行为等用户数据时，应提示用户并向用户提供关闭数据采集的功能。在执行此类操作前，应首先对用户身份进行认证。

车载终端应具备支持国家监管部门依法进行数据采集工作的能力。

应符合以下要求：

a) 数据安全存储需求：

1) 车载终端在将用户敏感数据（例如：用户身份、位置信息）存储在车内系统时，应为保存数据的文件设置适当的权限，以防止未授权的访问和篡改；
2) 存储涉及用户生物特征的数据时，应采用加密形式保存；
3) 车载终端不应有未向用户明示且未经用户同意，擅自修改用户数据的行为；
4) 安全存储的文件应具备标识信息，无法在非授权设备中使用；

b） 数据安全传输：

1） 应使用防护措施，对所传输数据的完整性和可认证性进行保护；

2） 应使用国密算法对重要数据进行加密传输；

c） 数据安全删除：

1） 共享类应用，在当前用户退出后，该用户的敏感数据应被清空；

2） 通过车载终端采集的用户数据，在传送到后台服务器后，应具备相应的脱敏措施，防止用户隐私信息泄露；

3） 车载终端设备更换件后，换下的旧件所存放的数据需安全删除，相关用户数据需同步新件，以防止用户数据泄漏或丢失。

5.4.6 第三库安全技术要求

第三库安全技术要求使用安全的第三库，禁止使用安全漏洞频发、认证鉴权等明显不符合安全要求以及缺乏高效更新机制的第三库。

5.4.7 OTA 升级安全技术要求

OTA 升级安全技术要求 OTA 升级过程中车端与服务端采用安全的双向认证、建立安全通道以及对 OTA 升级包进行验证，确保 OTA 升级包的完整性、机密性和可用性。

5.4.8 总线安全技术要求

总线安全技术要求车内总线通信发送节点不被恶意应用调用从而向车内网络发送恶意数据，同时车内总线通信接收节点应对接收到车内数据信息进行合法性校验，必要时可以对关键的信息采用一定保护机制（例如：防重放机制、加密机制）。

在车内通信时，车载信息交互系统作为车内网络架构中的控制器节点，通过CAN或车载以太网等总线与车内其他控制器节点进行数据交互。在进行重要数据传输时，需使用安全机制对传输数据的可靠性、合法性及完整性进行保证。

5.5 港口通信安全威胁分析及技术要求

车联网具有无线通信网络所存在数据传输、认证等方面的安全风险。同时，车联网的互联网应用平台作为互联网上的服务，也面临互联网服务应用漏洞带来的安全威胁。数据安全包括数据的存储安全、数据备份和数据传输安全。数据安全通常与业务设计、技术实现有关，是车联网安全重点。

车联网网络安全防护技术主要从以下几个方面考虑：

a） 对传输信息实行安全保护策略，对传输信息进行分级保护，从技术角度出发实现对方案的设计管理，规范其中的安全性。

b） 实施网络加密技术，对传输数据进行加密。同时采用备份响应措施，根据实际需求采用冗余链路、冗余节点和冗余系统等方式，提供一定的网络恢复能力；关键数据如业务数据、设备配置数据、性能数据等应具有异地或本地数据备份。

c) 在采用无线通信技术传输消息时，可以通过使用数字证书的方式来有效地进行身份认证和数据完整性校验，实现安全通信，保证数据的不可篡改性和保密性。

港口通信安全要求如下：

1) 基于Uu接口通信，支持LTE、LTE-V、5G通信安全机制，包括基于EPS-AKA或5G-AKA的双向认证、空口加密和完整性保护，同时支持基于证书的应用层安全机制；

2) 基于PC5通信模式，可通过实现基于证书的应用层安全机制，进行双方身份识别和匿名信息交互，保证消息完整性和有效性。

中国智能交通产业联盟

标准

港口无人驾驶集装箱卡车性能和测试方法

第 2 部分：无线通讯和信息安全要求

T/ITS XXXX-20XX

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

2017 年 X 月第一版　2017 年 X 月第一次印刷