ICS 03.220.40;53.060
CCS R 46

团 体 标 准

T/ITS 0147.2—2021

港口无人驾驶集装箱车技术要求 第2部分 无线通讯和信息安全

Technical requirements for port driverless container vehicle
Part 2: wireless communication and information security

2021－12－07 发布　　2022－03－01 实施

中国智能交通产业联盟　发布

目　　次

前　言

本文件按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》给出的规则起草。

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提出并归口。

本文件起草单位：中国移动通信集团有限公司、东风商用车有限公司、中远海运港口有限公司、厦门远海集装箱码头有限公司、交通运输部公路科学研究所、招商局检测车辆技术研究院有限公司、阿里巴巴（中国）有限公司、宁波大榭招商国际码头有限公司、北汽福田汽车股份有限公司、上海机动车检测认证技术研究中心有限公司、北京经纬恒润科技股份有限公司、上研智联智能出行科技（上海）有限公司、招商局国际科技有限公司等。

本文件主要起草人： 蒋鑫、李阳、王敏、于海滨、闫名慧、王沈元、黄庭、余翔宇、祝绍嵩、董轩、杨志魁、林建喜、张锦阳、周炜、王戡、牛成勇、王琳、李飞、林麒、乐群凯、金大鹏、田俊涛、曹建永、费音、张林、吴临政、吴海飞、周安伍、汪沛。

港口无人驾驶集装箱车技术要求
第 2 部分 无线通讯和信息安全

1 范围

本文件规定了港口无人驾驶集装箱车无线通讯和信息安全。

本文件适用于为实现港口集装箱车无人驾驶的无线通讯系统建设。

注：本文件中港口无人驾驶集装箱车包括港口牵引车和半挂车组合形式，以及平板式无驾驶舱运输车形式等。

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 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

YD/T 3594-2019 基于LTE的车联网通信安全技术要求

T/CSAE 53-2020 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（第一阶段）

T/ITS 0097-2016 合作式智能运输系统 通信架构

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

港口无人驾驶集装箱车 port driverless container vehicle

搭载先进的车载传感器、控制器、执行器等装置，并融合现代通讯与网络技术，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，实现“安全、高效、节能”行驶，适应港口生产作业环境，承担港区内集装箱水平运输功能，能够持续地执行部分或全部动态自动驾驶任务的运输车辆。

3.1.2

自动驾驶系统 autonomous driving system

能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。

3.1.3

指令 instruction

调度员输入信号、码头生产管理系统调度任务下达、车管平台下达干预信息，测试车辆通过感知、地图等信息自主发出的信号。

3.1.4

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车实现智能化业务运营，并将港口无人驾驶集装箱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。

3.1.5

调度员 dispatcher

在港口无人驾驶集装箱车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，且其设计运行范围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。

3.2 缩略语

以下缩略语适用于本文件：

MEP：多接入边缘平台（Multi-access Edge Platform）

OBU：车载单元（On-Board Unit）

OTA：空中下载技术（Over-the-Air Technology）

RB：资源块（Resource Block）

S-NSSAI：单一网络切片选择辅助信息（Single Network Slice Selection Assistance Information）

UPF：用户面功能（User Plane Function）

V2X：车用无线通信技术（Vehicle to Everything）

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

4 无线通讯技术要求

4.1 无线网络技术要求

港口无线网络技术应符合以下要求：

a) 无线侧根据带宽需求和港区容量，采用单频段组网或者混合组网模式，4.9GHz 频段适合港区大带宽上行业务需求；2.6GHz 频段适合港区集装箱堆场密集、高度错落，无线环境复杂；采用 2.6GHz+4.9GHz 混合组网模式能降低基站间的干扰影响。港口无线通讯网络架构，见图 1。

b) 按不同业务所对应的网络服务类型规划行业专用切片 S-NSSAI，以满足业务隔离和网络性能保障要求。

c) 堆场无线网络信号覆盖 4-6 层箱高，以满足水平和垂直覆盖需求。

d) 通过无线侧 RB 资源预留，采用基于切片的 RB 资源预留，不同业务享有专有 RB，实现码头业务、公网业务的隔离。

e) 针对低时延高可靠不同需求，UPF 和 MEP 下沉至港口机房。

f) 使用双网冗余备份来保证数据传输可靠性。在有光缆的情况下，用 5G 网络作为备份，在光缆无法铺设的情况下，5G 和 WiFi 互为备份。

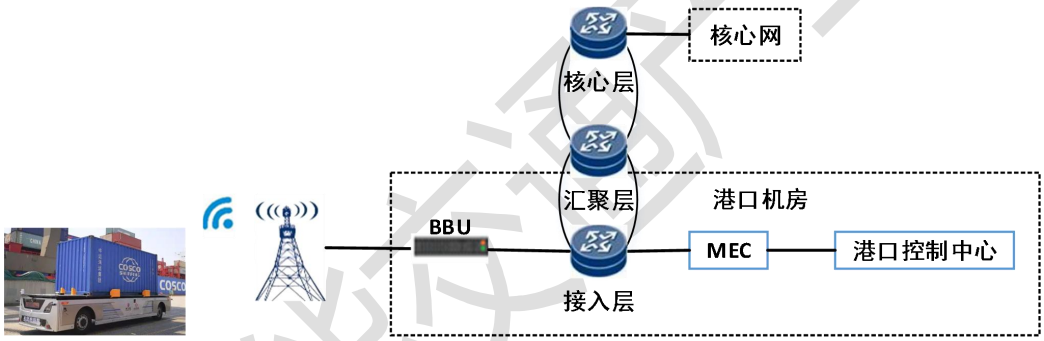

图 1 港口无线通讯网络架构

4.2 无线网络性能要求

4.2.1 自动驾驶场景

港口基于车路协同的自动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。车辆子系统包含OBU和智能驾驶系统，OBU通过V2X通讯方式将车辆信息传输给路侧子系统，同时接收来自路侧子系统的数据，智能驾驶系统利用视频摄像头、雷达传感器等设备来了解周围的交通状况。自动驾驶无线网络需求，见表1。

表 1 自动驾驶无线网络需求指标

业务名称	整体需求描述	通讯需求			
		带宽	传输时延	可靠性	小区切换时延
自动驾驶（控制部分）	低时延	50-100Kbps	≤30ms	≥99.99%	≤100ms
自动驾驶（视频部分）	大带宽	10-20Mbps	≤100ms	≥99.99%	≤200ms

4.2.2 远程控制场景

港口无人驾驶集装箱车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车退出故障区。远程控制无线网络需求，见表2。

表 2 远程控制无线网络需求指标

业务名称	整体需求描述	通讯需求		
		带宽	传输时延	可靠性
远程控制	低时延，大带宽	≥80Mbps	≤30ms	≥99.99%

5 信息安全技术要求

5.1 通讯安全技术要求

车辆敏感或重要信息通讯过程，对通讯双方实施双向身份认证，对通讯进行必要的加密处理，能够防范重放攻击和中间人攻击，应符合以下要求：

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。

b） 实施网络加密技术，对传输数据进行加密。通过使用数字证书的方式进行身份认证和数据完整性校验，保证数据的不可篡改性和保密性。

c） 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；业务数据、设备配置数据、性能数据等关键数据有异地或本地数据备份。

5.2 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。若出于业务需要而应事先采集相关数据，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） 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） 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，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。

5.3 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 总线安全技术要求

总线安全技术要求车内总线通讯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，同时车内总线通讯接收节点对接收到车内数据信息进行合法性校验，必要时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）。

在车内通讯时，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 操作系统安全技术要求

操作系统安全技术应符合以下要求：

a） 车辆操作系统及时进行补丁升级；提供安全调用控制与呈现能力；对应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。

b） 在安全存储区域存储操作系统签名。操作系统启动时使用可信机制，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。

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

d） 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。采用完整性校验手段，对关键代码或文件进行完整性保护。

e） 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。系统具有能够及时进行漏洞修复的功能。

中国智能交通产业联盟

标准

港口无人驾驶集装箱车技术要求 第2部分：无线通讯和信息安全

T/ITS 0147.2-2021

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

2021年12月第一版　2021年12月第一次印刷