|  |  |
| --- | --- |
| ICS | 点击此处添加ICS号 |
| CCS | |  | | --- | | D:\000000部门项目\09标准化插件开发\程序源代码\StandardEditor_ShanDongKeXieYuan\团标首页面字母T.pngD:\000000部门项目\09标准化插件开发\程序源代码\StandardEditor_ShanDongKeXieYuan\团标首页面字母T后面的反斜杠.png CPHA |   点击此处添加CCS号 |

中国港口协会团体标准

T/CPHA XXXX—XXXX

港口自动驾驶集装箱车辆远程监控系统

技术要求

Technical requirements for remote surveillance system of port autonomous container vehicles

XXXX - XX - XX发布

XXXX - XX - XX实施

中国港口协会  发布

1. 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。

本文件由中国港口协会提出/归口。

本文件起草单位：招商局港口集团股份有限公司、招商局国际科技有限公司、深圳海星港口发展有限公司、招商局检测车辆技术研究院有限公司、福建中科云杉信息技术有限公司、深圳海星智驾科技有限公司

本文件主要起草人：

港口自动驾驶集装箱车辆远程监控系统技术要求

* 1. 范围

本文件规定了港口自动驾驶集装箱车辆远程监控系统的系统构成、一般要求、信息采集、网络通信、应用服务器、数据存储、监控台和系统安全等要求。

本文件适用于港口自动驾驶集装箱车辆远程监控系统的设计、开发和使用。

* 1. 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 42811-2023港口集装箱作业系统技术要求

GB/T 42809-2023自动化集装箱码头操作系统技术要求

GB/T 40429-2021 汽车驾驶自动化分级

GB/T 4943.1-2011信息技术设备安全第1部分：通用要求标准

GB/T 32918.2 信息安全技术 SM2椭圆曲线公钥密码算法

GB/T 40861-2021 汽车信息安全通用技术要求

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 37933 信息安全技术 工业控制系统专用防火墙技术要求

GB/T 40855-2021 电动汽车远程服务与管理系统信息安全技术要求及试验方法

GB 50395-2007 视频安防监控系统工程设计规范

JTS-T 174-2019自动化集装箱码头设计规范

YD/T 3865 工业互联网数据安全保护要求

* 1. 术语和定义及缩略语
     1. 术语和定义

下列术语和定义适用于本文件。

港口自动驾驶集装箱车辆 port autonomous container vehicles

应用自动驾驶技术，在港口环境下进行自主导航、行驶和执行任务的集装箱运输车辆。它通过传感器、算法和通信技术实现对环境感知、路径规划、避障、货物装卸等功能，且支持平台远程控制。

远程监控系统 remote surveillance system

利用车载或路端传感器，实时监控安全员操作、驾驶舱环境、车外环境，检测危险及异常并上报监控台，且有智能提示功能与车辆接管功能的系统，用于港口自动驾驶集装箱车作业，保障车辆安全。

监控台 real time monitoring platform

对车辆运营关键指标、车辆线路运营状态、安全员、驾驶舱运行状态，进行实时监控的可视化监管平台。

被动接管 passive takeover

在自动驾驶系统出现某些状况（如系统故障、超出系统能力范围的复杂路况等）下，车辆控制权从自动驾驶系统自动转交到驾驶员手中，驾驶员需要被动地对车辆进行操作控制。

主动干预 Active Intervention

在自动驾驶系统正常运行过程中，驾驶员基于自己的判断，主动对车辆的行驶状态进行调整或者操作，改变自动驾驶系统原本的控制策略。

* + 1. 缩略语

下列缩略语适用本文件。

PACV：港口自动驾驶集装箱车辆（Port autonomous container vehicles）

RSS：远程监控系统（Remote surveillance system）

RTMP：监控台（Real time monitoring platform）

NTP：网络时间协议（Network Time Protocol）

TCP/UDP：传输控制协议 / 用户数据报协议（Transmission Control Protocol/User Datagram Protocol）

TLS：传输层安全协议（Transport Layer Security）

SSL：安全套接层协议（Secure Sockets Layer）

SM2：信息安全技术 SM2 椭圆曲线公钥密码算法

AES：高级加密标准（Advanced Encryption Standard）

RSA：Rivest-Shamir-Adleman加密算法

HSM：硬件安全模块（Hardware Security Module）

BCC：异或校验（Block Check Character）

* 1. 系统构成

港口自动驾驶车辆远程监控系统由信息采集、网络通信、应用服务器、数据存储、监控台和安全系统组成，系统构成见图1



1. 系统构成
   1. 一般要求
      1. 功能性要求
         1. 远程控制接管要求
            1. 被动接管

当港口自动驾驶车辆发生以下故障或自动驾驶系统出现以下异常情况时，应立即发出接管请求：

1. 车辆故障：转向系统故障、制动系统故障、动力系统故障、传感器故障、通信系统故障。
2. 自动驾驶系统异常：算法错误、数据处理异常、系统死机或崩溃。
3. 车辆通过专用通信通道向远程监控系统发送接管请求信号，信号应包含车辆故障或异常的详细信息。远程监控系统接收到请求后，以声光报警、弹窗提示、短信通知等多种方式提示操作员，操作员在确认身份后，允许远程控制车辆。接管过程中，车辆实时向远程监控系统反馈车辆状态信息，直至接管请求结束（如车辆故障修复或异常情况排除）。
   * + - 1. 主动干预

自动驾驶系统支持以下多种主动干预实现方式，操作员可根据实际情况进行操作：

1. 手动切换驾驶模式：在监控台上设置驾驶模式切换按钮，操作员可在自动驾驶模式和远程驾驶模式之间进行切换，切换时系统应进行身份验证，并确保切换过程平稳。
2. 调整车辆速度：通过监控台上的油门踏板或速度控制按钮，操作员可远程调整车辆行驶速度，速度调整范围应根据车辆性能和港口作业要求设定，调整过程中系统实时显示当前速度，并根据速度变化调整车辆动力输出和制动控制。
3. 改变行驶方向：利用监控台上的方向盘或方向控制按钮，操作员可远程控制车辆转向，转向操作应具备一定的手感反馈，同时系统实时显示车辆转向角度，并结合车辆速度和周围环境进行安全限制。
4. 操作员进行主动干预时，系统记录干预操作的详细信息，并实时反馈车辆状态信息，直至干预操作结束。
   * + 1. 作业保障要求
          1. 保障功能

系统作业保障功能应符合如下要求：

1. 车辆能以不低于每分钟一次的频率感知并上报电量信息及气泵气压信息，电量信息应包括电池总电量、剩余电量、充电状态等，气泵气压信息应涵盖各个气泵的工作气压。
2. 系统能进行详细的故障报警，将故障分为严重故障（如影响车辆行驶安全或作业关键功能的故障）和一般故障（如不影响车辆正常行驶但需及时维修的故障）。对于严重故障，采用紧急闪烁灯光、高分贝声音报警（音量不低于85分贝）；对于一般故障，采用屏幕弹窗提示、较低音量声音报警（音量不低于60分贝）等方式，同时在监控台上显示故障的详细信息（如故障类型、故障发生时间、故障位置等）。|
   * + - 1. 应急功能

无人集卡远程监控系统应符合如下要求：

1. 紧急情况下，远程控制系统操作者可通过按下监控台上的红色醒目紧停按钮，触发车辆的紧急停车指令。车辆接收到指令后，应在不超过 1 秒的时间内开始制动，并以最大制动力使车辆在最短距离内停止（根据车辆速度和载重情况确定最大制动距离标准），制动过程中车辆应保持稳定，避免侧滑或失控。
2. 远程控制系统操作者能通过监控台上的模式切换按钮在自动驾驶模式和远程驾驶模式之间进行切换，切换前系统应提示操作者再次确认操作，切换过程中车辆应限制速度，并保持转向稳定，同时监控台实时显示切换进度和车辆状态信息。
   * 1. 系统性要求
        1. 安全基本要求
           1. 系统安全

远程控制平台安全应满足如下基本要求：

1. 远控平台具有一定的安全策略，包括但不限于系统、应用、账户、权限、硬件、网络、升级和数据的安全；
2. 具备对远控平台攻击的监测能力，并能够将监测到的攻击行为展示给用户。
   * + - 1. 通讯安全

远控平台和无人集卡的以太网通信均应采用安全传输协议。

远控平台与车辆间的通信应采用双向认证，安全协议不低于TLS1.2，且应采取密码技术对车辆相关信息进行保密性和完整性防护。采用的密码应符合《GB/T 32918.2 信息安全技术 SM2椭圆曲线公钥密码算法》的要求。

* + - 1. 远控平台要求

远控平台至少包含远程驾驶、作业数据展示等系统。各个系统或模块间应确保相互协调，互不影响。单个模块异常不影响其他模块自身功能的运行。

远控平台远程驾驶的数据通信时延不大于50 ms。

远控平台服务器并发处理要求应能够同时处理大于或等于下辖车辆和设备总数1.5倍数量的通信请求，且响应时延不应大于300 ms。

* + - 1. 远程驾驶要求

远控平台应具备远程驾驶功能，并能覆盖所有具备自动驾驶能力的车辆。远程驾驶系统应具备控制车辆油门、档位和转向的基本能力，且能将车辆周围图像和感知信息回传到远控平台；远程驾驶系统的指令执行优先度应高于车辆自动驾驶系统，低于现场人工操作。

* + - 1. 设备接入要求

前端编码器设备（包括硬盘录像机，网络摄像机，NVR等平台需要接入的设备）应当能够接入应急指挥系统平台。尚未能接入的，应督促设备产商提供接口协议并由工程建设各相关责任主体负责接入各级应急指挥系统平台。

* + - 1. 设备保护要求

远程视频监控系统的设备设施应保护到位，非技术或工程要求，不得擅自调整、挪动、撤除，严禁遮栏摄像头，设备出现故障应当立即上报建设单位，作好书面记录并立即修复。

* 1. 信息采集要求
     1. 摄像头性能

远控平台视频显示系统的信息来源于安装在车辆上的摄像头，摄像头应满足以下要求：

1. 摄像头帧率不低于 30fps，以确保视频画面的流畅性，在车辆快速行驶或动态场景较多时能清晰捕捉画面。
2. 摄像头有效像素提升为 1920×1080 或更高（如 3840×2160），提高图像清晰度和细节捕捉能力。
3. 前视摄像头水平视场角≥120°，侧视或后视摄像头水平视场角≥100°，垂直视场角≥60°，扩大摄像头的视野范围，减少车辆周围盲区。
4. 防水等级≥IP67，增强摄像头在恶劣天气（如暴雨、积水等）和港口潮湿环境下的防护能力，确保其正常工作。
5. 图像清晰度应能清晰分辨车辆周围 100 米范围内的人员、车辆和物体轮廓；对比度应适中，确保不同亮度区域的细节可见；色彩还原度应接近真实场景，无明显偏色现象。摄像头应具备自动曝光、自动白平衡等功能，在不同光照条件（如强光直射、弱光环境、夜间无照明等）下能自动调整图像参数，保证画面质量稳定。|
   * 1. 摄像机数量与位置

根据车型和港口作业需求，摄像头的数量与位置应满足如下要求：

1. 标准集装箱卡车至少应安装前视摄像头2个（分别位于车头正前方和上方，用于不同角度的前方视野监测）、侧视摄像头4个（车辆两侧前后位置各1个，确保侧方视野无死角）、后视摄像头2个（车尾上方和下方，用于倒车和后方视野监测）、车内摄像头1个（用于监控驾驶舱内安全员状态）。
2. 摄像头应安装在车辆高处且视野不受遮挡的位置，确保能够有效覆盖车辆周围的关键区域，减少盲区，同时考虑安装位置对摄像头稳定性、防护性和图像采集效果的影响。网络通信要求
   1. 网络通信要求
      1. 网络接入与传输

网络接入根据视频监控传输带宽需要确定，应预留至少20%的带宽冗余，以应对网络高峰和突发数据流量，确保流畅传输。通过互联网加密传输的，应采用符合国密标准的加密设备（如加密路由器、加密网关等），加密设备应具备以下功能：支持TLS1.2或以上版本加密协议、密钥管理功能（包括密钥生成、存储、更新等）、对传输数据进行实时加密和解密处理，加密处理速度应满足系统最大数据传输需求。

各建设单位、施工现场的视频传输网络接入应采用固定网络地址（或能够对应每个前端设备的方式），网络地址分配应遵循统一规划原则，确保地址唯一性和可管理性。各接入点的网络配置应符合应急指挥系统平台的详细规范要求，包括子网掩码、网关、DNS服务器等配置参数。同时，建立网络地址管理数据库，记录硬盘录像机或视频服务器、前端监控点的网络地址配置情况及联系人信息，并实时更新，方便监督机构查询和管理。

远程驾驶系统的网络通信能力要求如下：

1. 网络设备应具备保障不低于8台车辆同时使用远程驾驶控制系统的业务处理能力及带宽，每辆车的最小带宽分配应不低于5Mbps（根据实际数据传输需求可调整）；
2. 应划分不同的网络区域，如控制区、数据区、视频区等，并为各网络区域分配独立的地址段，采用防火墙、VLAN（虚拟局域网）等技术进行隔离。重要网络区域（如控制区）应部署在具有多重防护措施（如入侵检测系统、防病毒网关等）的核心网络位置，避免直接暴露在网络边界；
3. 应提供通信线路和关键网络设备的冗余，采用双链路备份（如主备光纤线路）或负载均衡技术，保证系统的高可用性，主备链路切换时间应不超过50毫秒。
   * 1. 网络通信稳定性

云控平台、监控台与车端通信过程中，应保证各设备均能准确感知断开连接、丢包和延时等异常情况。设备应在 1 秒内检测到连接中断，丢包率超过 0.1% 时应能及时发出警报，延时超过 50 毫秒时应记录详细的延时数据。建立心跳机制，心跳数据包每 500 毫秒发送一次，心跳数据包应包含设备编号、时间标签、发送序号、数据包大小等信息。当接收方在 1 秒内未收到心跳数据包时，应判定为连接异常。

当检测到丢包时，系统应自动启动重传机制，根据丢包情况调整重传策略（如连续丢包时加大重传频率），重传次数不超过5次，若仍无法恢复数据，则记录丢包事件并通知相关人员。当延时超过阈值时，系统应自动降低数据传输频率（如减少视频帧率、暂停非关键数据传输等），同时分析延时原因（如网络拥塞、设备性能问题等），并采取相应优化措施（如调整网络路由、升级设备硬件等）

* + 1. 网络通信方式
       1. 网络通信方式要求

远程监控系统远控平台与自动驾驶车辆自动驾驶系统各部分通信方式如下：

1. 控制指令的下发采用TCP/UDP协议，时延不大于30ms;
2. 视频信号的传输采用TCP/UDP协议，时延不大于40ms;
3. 车辆状态和作业任务状态的传输采用TCP/UDP协议，时延不大于30ms。
   * + 1. 网络通信容错能力

云控平台、监控台与车端通信过程中，应保证各设备均能感知断开连接、丢包和延时等异常情况，当设备感知到断开连接时，应立即尝试重新连接，重新连接最多尝试5次，若仍无法连接则发出警报通知相关人员。当感知到丢包时，分析丢包原因（如网络故障、信号干扰等）并采取相应措施（如切换网络链路、调整信号发射功率等）。当感知到延时超过阈值时，暂停非关键数据传输，优先保证关键指令和状态信息的传输，并及时通知相关人员进行网络优化。

* + - 1. 网络通信感知链接异常

心跳数据包每300毫秒发送一次，心跳数据包应包含设备编号、时间标签、发送序号、设备状态信息。当接收方连续3次未收到心跳数据包时，判定为连接异常，立即采取相应措施（如尝试重新连接、切换备用链路等）。

* + - 1. 网络通信感知丢包和延时

应定时发送需要对方设备回复的请求数据包，并根据是否有响应数据包判断丢包概率，收到响应数据包后应根据发送时间和接受时间计算通信耗时，判断延时能否满足当前业务，不满足时需要做出应对措施。请求数据包和响应数据包至少应包含编号信息和时间标签，其中响应数据包中的编号信息和时间标签应和接收到的请求数据包相同。

* + 1. 网络通信灾备冗余能力

云控平台、监控台和车端通信过程中，应具备至少两种通信方式（如5G通信、有线网络通信等），并优先使用5G通信。当5G通信信号异常时，应立即无缝切换到有线网络通信。切换过程中，应确保数据不丢失，车辆和监控台之间的状态信息保持一致，切换时间不超过100毫秒。

建立通信链路状态监测系统，实时监测各通信链路的信号强度、丢包率、延时等参数，至少每10秒更新一次链路状态信息。当通信链路出现故障时，系统应自动记录故障时间、故障类型（如信号中断、硬件故障等）、故障链路等详细信息，并立即上报给监控台和相关维护人员。同时，定期对灾备冗余系统进行测试（如每月进行一次主备链路切换测试），确保其在需要时能够可靠运行，测试结果应记录并保存至少一年。

* 1. 数据存储要求
     1. 数据存储内容

数据存储内容应包含但不限于以下内容：

1. 存储车辆前方、车辆两侧、车辆后方以及车内的视频数据，视频分辨率不低于1920×1080，帧率不低于30fps，存储时间不少于30天。视频数据应按照时间、车辆编号、摄像头位置等维度进行分类存储，方便查询和检索。
2. 存储车辆底盘数据（如车速、转向角度、刹车状态、轮胎压力等）、自驾软件运行状态（如算法版本、决策逻辑、传感器数据融合结果等）、监控台运行状态（如操作员操作记录、系统报警信息、软件版本等），存储时间不少于30天。数据应进行结构化处理，建立合理的数据表结构和索引，便于数据分析和统计。
   * 1. 数据存储能力

数据存储能力应包含但不限于以下能力：

1. 存储数据能力应根据摄像头数量、视频分辨率、帧率、车辆运行数据更新频率等因素计算所需存储空间，确保存储设备容量满足至少30天的数据存储需求，并预留20%的空间用于临时数据缓存和系统扩展。
2. 提供多种检索条件，如按时间范围、车辆编号、事件类型、摄像头位置等进行检索。回放：支持视频数据的倍速播放、逐帧播放、画面缩放等功能，回放过程中应保证视频流畅性，不出现卡顿或跳帧现象。导出：支持将视频数据和车辆运行数据导出为常见格式，导出数据的完整性应得到保证。
3. 采用先进先出的循环存储策略，当存储空间达到设定阈值时，自动覆盖最早的数据。在覆盖数据之前，应对数据进行完整性校验，确保数据的准确性。同时，对重要数据应进行备份存储，备份存储时间不少于1年循环存储能力。
4. 支持在线扩容，扩容过程中应保证数据的正常存储和系统的不间断运行。提供容量扩展的规划和预测工具，根据数据增长趋势提前规划扩容方案，确保系统能够持续满足数据存储需求。
   1. 应用服务器要求
      1. 车辆管理服务
         1. 车辆的注册与注销

车辆注册时，需提交详细资料，包括车辆行驶证、保险证明、自动驾驶系统技术参数、车辆所有人信息等，资料审核由专人负责。注销车辆时，需提交注销申请，说明注销原因（如车辆报废、转售、系统升级后不再适用等），经审核通过后办理注销手续，同时更新车辆注册信息库。

* + - 1. 车辆登录管理

优化车辆上电与下电流程，确保车辆在上电过程中系统进行全面自检，自检通过后反馈上电成功信息。车辆登录港口任务调度系统时，系统应根据车辆类型、当前任务负载、港口作业优先级等因素进行智能调度，支持多任务并行处理。车辆登出时，系统应记录登出时间和相关信息，同时清理车辆在系统中的临时数据。反馈车辆登录情况时，应包括登录时间、登录结果、分配的任务信息等。

* + - 1. 用户管理服务

细化用户管理功能，将用户分为管理员、普通操作员、观察员等角色，为每个角色定义不同的权限范围。管理员可进行系统配置、用户管理、车辆调度等全面操作；普通操作员可进行车辆监控、远程控制、任务执行等操作；观察员仅可查看车辆状态和监控信息。用户登录时，系统进行身份验证。同时，支持用户权限的动态调整（如根据工作需要临时提升普通操作员权限），权限调整需经过审批流程并记录操作日志。

* + 1. 时间同步服务

时间同步精度应达到毫秒级，优先使用网络时间协议（NTP）服务器进行时间同步，如 NTP 服务器不可用，则采用本地高精度时钟源（如原子钟）。时间同步服务应在系统启动时自动启动，并每隔 10 分钟进行一次时间校准，校准过程中应记录时间偏差值。同时，系统应具备应对时钟漂移的补偿机制，确保系统中各设备的时间一致性。

* + 1. 流媒体服务器

负责车端远控摄像头视频数据的高效管理，包括视频流的采集、编码、传输和存储。支持同时处理至少10路高清视频流（1920×1080，30fps），确保视频数据的实时性和稳定性。优化视频流推送功能，支持自适应码率调整，确保视频在不同网络环境下的流畅播放。提供多种分辨率选择，用户可根据需求在监控台上进行切换。画面布局设计应支持多种模板，用户可根据实际监控需求灵活调整画面布局。

* + 1. 数据管理

负责收集车端运行数据与监控台运行数据，数据收集频率应根据数据类型和重要性进行合理设置。

* + - 1. 数据存储

选择合适的数据库类型，设计合理的数据表结构和索引，提高数据存储和查询效率。在存储数据之前，对数据进行清洗和预处理，确保数据的准确性和可用性。同时，建立数据备份机制，每天对数据进行全量备份，备份数据存储在异地灾备中心，保留至少1年的备份数据。

* + - 1. 数据分析支持

提供基本的数据分析功能，如数据统计、数据趋势分析，分析结果以图表形式在监控台上展示，为港口运营管理提供数据支持。

* + 1. 回放工具
       1. 视频回放

支持多画面同时回放，画面布局可自由调整。提供时间轴缩放功能，方便用户快速定位到特定时间点的视频内容。支持添加回放标记和注释功能，用户可对重要事件进行标注和说明，标记和注释信息应与视频数据一同存储。

* + - 1. 数据回放

以表格形式展示车端运行数据与监控台运行数据，支持数据筛选和排序。提供数据对比功能，用户可选择不同时间段或不同车辆的数据进行对比分析。回放工具应与数据分析功能紧密结合，用户可在回放过程中直接调用数据分析工具对选定的数据进行深入分析，分析结果在同一界面展示，方便用户进行数据挖掘和问题排查。

* 1. 监控台要求
     1. 硬件要求
        1. 显示设备要求

监控台应具备不少于一块高清显示屏，用于实时展示车辆远控视频画面、任务和车辆状态等信息，高清显示屏分辨率不低于2560×1440，屏幕刷新率不低于60Hz，具备防眩光处理，确保在强光环境下也能清晰显示画面。

具备不少于一块触摸屏，触摸屏触摸响应时间不超过50毫秒，触摸精度误差不超过2毫米，支持多点触控，用于查看无人驾驶车辆信息，实现客户端登录、远控、示忙等人机交互功能，触摸屏应支持可旋转和朝向调节。

指示灯应不少于3个，亮度应适中，在不同光照条件下均能清晰可见，颜色区分明显，用于显示警示、远控、示忙等状态。

* + - 1. 操控装置要求

监控台应具备方向盘、刹车踏板、油门踏板、档位控制杆（或档位切换按钮），实现对车辆转向、油门、刹车、档位的远程操控。

监控台应具备紧停按钮，安装在显眼且易于操作的位置，能够使操作员在紧急状态下使车辆快速进入紧停状态。

监控台应具备灯光控制设备，能够控制车辆的大灯、转向灯、雾灯等各类灯光，控制方式应简单直观。

监控台应具备喇叭控制设备，用于远程控制车辆喇叭提醒车辆周边行人与车辆注意。

* + - 1. 音频设备要求

监控台应具备语音输出设备，用于提示操作员关注车辆状态、监控台状态等一些重要信息。

* + - 1. 身份信息输入设备

监控台应具备身份信息输入设备，用于识别操作员是否为合格注册人员，支持多种身份验证方式，如密码键盘、指纹识别器、智能卡读卡器，可根据港口安全需求选择一种或多种组合使用。

* + - 1. 主机要求

监控台应具备一台主计算设备，用于运行监控台的主要软件。并支持接入章节10.1.1-10.1.4所述设备。

* + - 1. 座舱要求

监控台座舱应为整体式设计，座舱应具备电动可调节座椅；显示设备、操控装置、座舱整体设计应符合人体工学设计，减少操作员长时间工作造成的疲劳，座舱内配备通风和空调系统，保持温度在 22℃-26℃，湿度在40%-60%之间，提供舒适的工作环境。

* + 1. 软件要求
       1. 用户管理要求

监控台应支持用户管理，操作员需输入个人身份信息才能登录监控台进行操作，同时支持人员的添加、信息变更、权限设置与注销操作，将用户分为管理员、普通操作员、观察员等角色，为每个角色详细定义可操作的功能范围。管理员可进行系统配置、用户管理、车辆调度等全面操作；普通操作员可进行车辆监控、远程控制、任务执行等操作；观察员仅可查看车辆状态和监控信息。用户登录时，系统进行身份验证。支持用户权限的动态调整，权限调整需经过审批流程并记录操作日志。

* + 1. 监控台硬件冗余

同一作业场景应至少配备5台远控设备。当监控台故障时，云控系统应在10秒内自动检测到故障，并根据预设策略将故障监控台的数据和任务无缝转移到正常的监控台上，确保作业的连续性，转移过程中数据丢失率不超过0.01%。同时，对故障设备进行自动诊断和报警。

当其中一台远控设备出现故障时，系统应自动将其任务分配到其他正常设备上，其他设备的负载增加不应超过 20%，确保实际作业效率不受影响。定期对硬件冗余系统进行测试，测试结果应记录并保存至少一年，以便分析系统性能和优化配置。

* + 1. 监控台软件冗余

监控台软件采用微服务架构，将不同功能模块拆分为独立的服务，实现高内聚低耦合。对关键业务功能采用多种代码实现，并进行定期比对测试，确保不同代码实现的等效性。当某个模块发生故障时，系统应在1秒内自动检测到故障，并根据预设策略切换到其他正常代码运行，切换过程中数据不丢失，业务不中断。同时记录故障信息，通知开发人员进行修复。

* + 1. 监控台容错能力

云控平台应实时监控监控台设备的运行状态，包括硬件状态和软件状态，监控数据采集频率不低于每秒一次。当监控台出现故障时，云控平台应在1秒内启动报警程序，报警方式包括声光报警、短信通知、邮件通知等多种方式，通知对象包括监控台操作员、港口管理人员、维护人员等相关人员。

监控台故障时，应采用数据备份和恢复技术，确保数据丢失量不超过1分钟的数据量。云控平台应根据当前所有监控台的负载情况、网络状况等因素，在5秒内将车辆切换到最优的备用监控台上进行操作，切换过程中保持车辆控制指令的连续性，同步车端状态数据的时间不超过10秒，确保车辆运行不受影响，作业进度不中断。同时，对故障监控台进行隔离和诊断，记录详细的故障信息（如故障时间、故障现象、故障代码等），方便维护人员进行故障排查和修复，修复后的监控台应经过严格测试后重新投入使用。

* 1. 系统安全要求
     1. 硬件安全要求

港口自动驾驶集装箱车辆远程监控系统所使用的硬件满足以下要求:

1. 不应存在后门或隐蔽接口；
2. 调试接口应禁用或设置安全访问控制。

港口自动驾驶集装箱车辆远程监控系统所使用的处理器、存储模块、通信IC等用于处理、存储和传输个人信息的关键芯片及安全芯片，应减少暴露管脚。

若港口自动驾驶集装箱车辆远程监控系统和其他信息交互系统存在共用硬件的情况，则整个设备软硬件也应满足本文件的要求。

港口自动驾驶集装箱车辆远程监控系统应具备安全启动的功能，可通过可信根实体对安全启动所使用的可信根进行保护。

电路板及芯片不宜暴露用以标注端口和管脚功能的可读丝印。

* + 1. 通信安全要求

远程驾驶通信安全应符合如下要求：

1. 对源地址、目的地址、源端口和目的端口进行检查，防止外部数据攻击；
2. 在关键网络节点处对进出网络的内容进行有害信息过滤，并能提供实时报警

安全通信协议要求如下：

1. 应使用TLS1.2或以上版本；
2. 应不允许降级，例如降到TLS1.1、TLS1.0或SSL3.0、SSL2.0；
3. 应禁用TLS会话重协商；
4. 应禁用TLS压缩；
5. 若使用基于非对称密钥的身份认证机制，宜使用SM2、密钥长度不低于2048位的RSA或同级别以及更高级的密码算法，应具有对应的证书更新及撤销机制，证书的有效期宜不超过365天，证书更新过程应确保密钥安全性；
6. 若使用基于对称密钥的身份认证机制，宜使用SM4、密钥长度不低于128位的AES或同级别以及更高级的密码算法，应具有对应的密钥更新机制，更新过程中应确保密钥安全性。

加密要求如下:

1. 数据单元加密方式应采用SM4、密钥长度不低于128位的 AES或其他同级别以及更高级的密码算法;
2. 加密数据单元的密钥应与安全通信协议所使用的密钥不同。

网络端口传输安全要求如下：

1. 应通过对数据包的源地址、目的地址、源端口、目的端口和协议进行检查决定允许或拒绝数据包进出；
2. 应具备根据会话状态信息为进出数据流判定允许或拒绝访问的能力；
3. 应基于应用协议和应用内容对进出网络端口的数据流实现访问控制；
4. 应关闭非业务相关的网络服务端口，并对业务相关的网络服务端口进行访问控制；
5. 应对进入无人集卡车辆的带有攻击行为特征的网络数据进行识别，且识别率不低于95％；
6. 宜采用专用网络或者虚拟专用网络通信，与公网隔离；
7. 宜具备更新扩展安全规则的能力。
   * 1. 应用软件安全要求

软件系统安全要求如下：

1. 应具备判定和授予应用程序对系统资源的访问和操作权限的能力，同时建立权限审计机制，定期对用户权限使用情况进行审计，记录和分析权限操作日志，确保权限使用的合规性;
2. 宜进行可信验证，对于可信验证，明确验证的内容、验证方法和验证频率，确保应用软件的可信度和安全性。

数据存储安全要求如下：

1. 应用软件在存储远程服务与管理数据时，根据数据的重要性和敏感性选择合适的加密算法和存储方式。对于高度敏感数据采用 SM2、SM4 等国密算法进行加密存储，并存储在硬件安全模块（HSM）或加密文件系统中；对于一般数据可以选择AES、DES等国际算法进行加密，存储在普通文件系统中，并采取访问控制措施；
2. 安全重要参数在存储时进行加密处理，存储在受保护的存储区域，在使用过程中通过安全的 API 接口进行访问，并且只有授权的应用模块在经过严格的身份验证后才能读取和修改这些参数，防止参数被非法篡改或泄露。

应用软件应具备远程升级功能，升级包需要具备校验机制，校验升级包的完整性以及来源真实性。在升级过程中，采用安全的传输协议下载升级包，下载完成后先验证数字签名，再计算校验和与包内的校验和进行比对，若校验失败或签名验证不通过，则停止升级并提示用户。同时，制定升级失败的回滚策略，如在升级前备份原软件版本，升级失败时自动恢复到备份版本，确保系统的稳定性和可用性。

* + 1. 数据安全要求

建立数据分类分级制度，根据数据的重要性、敏感性和影响范围将数据分为不同级别（如机密级、秘密级、内部公开级等），针对不同级别数据制定相应的安全策略和防护措施。同时，明确数据所有者、管理者和使用者的职责，建立数据安全管理流程，确保数据在全生命周期（产生、存储、传输、使用、销毁等）内的安全。

报文加密

无人集卡车辆与云控平台、无人集卡车辆之间、无人集卡车辆与路侧设备、无人集卡车辆与协同作业设备、云控平台与路侧设备以及云控平台与协同作业设备之间的通信和涉及企业安全的数据均应采用校验码技术或安全芯片。采用密码技术保证通信过程中数据的完整性，并采用加密技术保证通信过程中敏感信息字段或整个报文的保密性。采用的安全芯片应同时支持国密算法及国际标准加密算法。加密密钥管理方面，建立密钥分层管理体系，根密钥存储在硬件安全模块中，会话密钥根据需要动态生成和更新，确保密钥的安全性和有效性。同时，加强对加密设备和安全芯片的管理，定期进行检测和维护，确保其正常运行和安全性。

* + - 1. 报文校验

采用BCC法，校验范围从命令单元的第一个字节开始，同后一字节异或，直到校验码前一字节为止，校验码占用一个字节，当数据单元存在加密时，应先加密后校验，先校验后解密。明确在数据单元加密情况下，加密、校验和解密的详细操作流程和顺序，确保数据的完整性和准确性。同时，建立报文校验失败的处理机制，如校验失败时自动重传数据、记录错误信息并通知相关人员进行排查等。

