ICS 53.020.20

J 80

|  |
| --- |
|  |

DB3202

无锡市地方标准

DB ××/T ××××—××××

|  |
| --- |
|  |

起重机械无线通信安全检测规范

|  |
| --- |
|  |
| （草稿） |

×××× - ×× - ××发布

×××× - ×× - ××实施

无锡市市场监督管理局   发布

目次

[前 言](#_Toc965) III

[1 范围 1](#_Toc4286)

[2 规范性引用文件 1](#_Toc29209)

3 [术语和定义 2](#_Toc31142)

[4 缩略语 4](#_Toc30778)

[5 概述 4](#_Toc17320)

[5.1 无线局域网系统 4](#_Toc31112)

[5.2 5G通信系统 5](#_Toc31112)

[6 起重机无线通信系统的安全要求 5](#_Toc17320)

[7 无线通信网络性能测试 6](#_Toc17320)

[7.1 测试条件 6](#_Toc31112)

[7.2 无线通信网络性能测试方法及判定准则 6](#_Toc27112)

[8 无线通信系统安全测试 9](#_Toc17320)

[8.1网络通道安全测试 9](#_Toc31112)

[8.2终端接入安全测试 1](#_Toc31112)0

[8.3控制信号与视频信号隔离测试 1](#_Toc31112)2

[8.4网络安全与防护检测 1](#_Toc31112)2

[8.5数据传输 1](#_Toc31112)2

[8.6操作、权限与维护检测 1](#_Toc31112)3

[8.7抗干扰与稳定性测试 1](#_Toc31112)3

[附录A（资料性） 起重机械无线局域网运行维护阶段工作要点 1](#_Toc10404)4

[附录B（规范性） 起重机械通信网络性能要求 1](#_Toc10404)5

[附录C（资料性） 多路视频终端汇集带宽计算经验公式 1](#_Toc19131)6

[附录D（资料性） 起重机械无线抗扰度测试要求 1](#_Toc19131)7

[附录E（资料性） 网络故障停机检测两种模式 1](#_Toc19131)8

[附录F（资料性） 视频与控制信号三种隔离方式](#_Toc19131) 20

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。

本文件由无锡市市场监督管理局提出并归口。

本文件起草单位：江苏省特种设备安全监督检验研究院江阴分院、江苏省电子信息产品质量监督检验研究院、江阴市市场监督管理局、金欧起重机有限公司、上海电机学院、中国移动通信集团江苏有限公司无锡分公司、金欧(海安)智能装备有限公司、上海科睿新机器人科技有限公司。

本文件主要起草人：沈刚、刁志锋、卢杰、唐晓白、张杰、姚海、季海军、郑斌、韩文芳、夏伟、赵永刚、俞强、蔡晓东、樊晟、彭建江、陈建武、黄付军、于小伟、王健、舒凯凯、陈凯、吴演哲、刘林、肖雪光、肖简军、刘佳、徐方强、田晓磊、韩运才、何智华、鲍池琛。

起重机械无线通信安全检测规范

1. 范围

本文件针对采用无线局域网或5G通信技术传输控制信号及视频信号的起重机械，规定了其通信安全基本要求和检测实施方法。

本文件适用于无锡市区域内纳入特种设备安全监督管理的起重机械，不适用于房屋建筑工地和市政工程工地所用的起重机械。

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 15629.11—2003 信息技术 系统间远程通信和信息交换局域网和城域网 特定要求 第11部分：无线局域网媒体访问控制和物理层规范

GB 15629.11—2003/XG1—2006 信息技术 系统间远程通信和信息交换局域网和城域网 特定要求 第11部分：无线局域网媒体访问控制和物理层规范 第1号修改单

GB 15629.1101—2006 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第11部分：无线局域网媒体访问控制和物理层规范：5.8GHz频段高速物理层扩展规范

GB 15629.1102—2003 信息技术 系统间远程通信和信息交换局域网和城域网 特定要求 第11部分：无线局域网媒体访问控制和物理层规范：2.4GHz频段较高速物理层扩展规范

GB/T 15629.1103—2006 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第11部分：无线局域网媒体访问控制和物理层规范：附加管理域操作规范

GB/T 22451—2024 无线通信设备电磁兼容性通用要求

GB/T 32420—2015 无线局域网测试规范

GB/T 50339—2013 智能建筑工程质量验收规范

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

T/ZJSEE 0030-2024 5G电力终端接入安全技术规范

YD/T 4970-2024 基于SIM卡的物联网安全服务技术要求

3GPP TS 33.220 GBA规范

GM/T 0021-2012 动态口令密码应用技术规范

ISO/IEC 15408 信息技术安全评估准则

1. 术语和定义

下列术语和定义适用于本文件。

**无线通信安全 wireless communication security**

通过加密、认证、抗干扰等技术保障通信数据的机密性、完整性与可用性。

**业务终端 business terminals**

起重机械上的数据采集与执行单元，包括传感器（如载荷传感器、倾角传感器）、摄像头（用于实时监控）、PLC控制器（执行控制指令）等，用于采集运行状态数据（如负载重量、设备位置）、接收并执行远程控制指令（如起吊、移动）。

**通信终端 communication terminals**

无线局域网中的STA以及集成5G模组的设备（如工业网关）。5G通信系统中，支持NSA/SA组网模式，用于将业务终端的数据封装为5G协议报文，通过空口（NR）发送至基站，同时接收下行指令并分发至业务终端。

**基站（gNB） generation nodeB**

5G无线接入节点，覆盖起重机作业区域，用于接收通信终端的无线信号，通过前传/中传网络将数据传输至核心网。

**传输设备 transmission device**

光纤、微波等物理传输媒介及交换机/路由器，用于连接基站与核心网，支持大容量数据传输。

**虚拟专用网 Virtual Private Network**

通过IPSec或SSL加密隧道保障数据传输安全。

**FLEXE（灵活以太网） Flexible Ethernet**

提供硬隔离的带宽通道，确保关键业务（如控制指令）的传输确定性。

**UPF（用户面功能） User Plane Function**

5G核心网的数据转发单元，路由数据至指定服务器，支持本地分流（如视频流直接送至监控中心）。共享UPF：多业务共用资源，适用于通用流量。专用UPF：为起重机械控制指令分配独立资源，降低时延和抖动。

**防火墙 firewall**

网络安全设备，用于过滤非法访问、抵御DOS/DDoS攻击，仅允许授权流量通过。

**系统服务器 system server**

远程控制平台、监控中心及云端服务器，用于解析控制指令并下发至起重机，存储与分析传感器数据，触发预警（如超载、设备故障），提供人机交互界面（HMI），支持远程操作与状态监控。

**WLAN维护类仪表 WLAN maintenance tool**

用于无线局域网规划、设计、验收、优化、排障、干扰分析的测试仪器或者测试软件工具。

**打点测试 inkersurvey**

在现场勘查测试过程中，使用特定工具，在测试区域的平面图上采用手动或基于GPS自动的方式进行点击并获取测试数据、计算测试结果的过程。

**网络切片 network slice**

5G通信系统中，提供特定网络能力和网络特征(如资源隔离、SLA保障特性等)、为客户提供多种业务属性的逻辑网络，分为通用切片和专用切片。

**二次认证(2FA) two-factor authentication**

通过结合两种不同形式的身份验证（如密码+动态令牌、生物特征+硬件密钥），显著提升系统安全性。在起重机械通信中，常用于以下场景：操作员登录：远程控制平台需输入密码+手机验证码。

**安全芯片(SE) secure element**

安全芯片是嵌入式硬件模块，用于安全存储密钥、执行加密运算及抵御物理攻击。在起重机械5G通信中的用于设备身份认证和数据加密。

**GBA Generic Bootstrapping Architecture**

3GPP定义的认证框架，基于共享密钥机制实现设备与网络的双向认证。在起重机械5G通信中用于设备接入认证和抵御中间人攻击。

**AKMA认证 Authentication and Key Management for Applications**

GBA的扩展，专为应用层设计，允许应用服务使用网络层生成的密钥进行加密和认证。在起重机械5G通信中用于远程控制指令保护和视频流安全传输。

1. 缩略语

下列缩略述语适用于本文件。

AP 无线接入点(Access Point)

ASU 鉴别服务单元(Authentication Service Unit)

QoS 服务质量(QualityofService)

SSID 服务集标识(Service Set IDentifier)

STA 站(点)(STAtion)

WLAN 无线局域网(Wireless Local Area Network)

WAPI 无线局域网鉴别与保密基础结构(WLAN Authentication and Privacy Infrastructure)

DoS 拒绝服务(Denial of Service)

DDoS 分布式拒绝服务(Distributed Denial of Service)

WPS WiFi保护设置(WiFi Protected Setup)

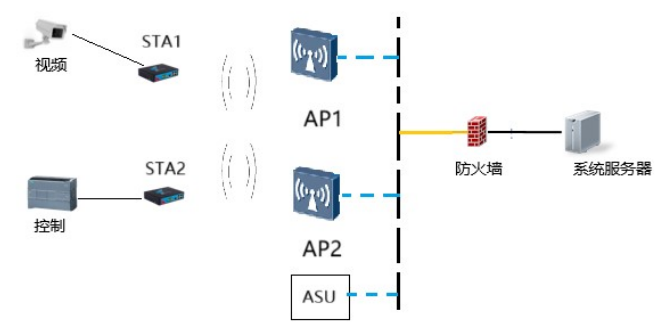
5G： 第5代移动通信技术（5th Generation Mobile Communication Technology）

NSA 非独立组网（Non-Standalone）

H.265 高效视频编码（High Efficiency Video Coding）

1. 概述
   1. 无线局域网系统

如图1所示，起重机械的无线局域网系统建立在已有的通用布缆系统基础之上，本标准所涉及的无线局域网系统为图1中实线框内的部分，该系统组成包括三种设备类型：与业务终端相连的STA、与系统服务器相连的AP和ASU，无线局域网设备的功能要求在GB 15629.11系列标准中给出，测试方法应符合GB/T 32420标准要求。本标准主要针对上述标准给出的功能要求，结合具体系统要求给出了起重机械无线局域网系统的工程测试方法。无线局域网系统工程测试将影响无线局域网运行维护阶段的工作，无线局域网运行维护阶段内容概要参见附录A。



**图1 起重机械的无线局域网系统组成**

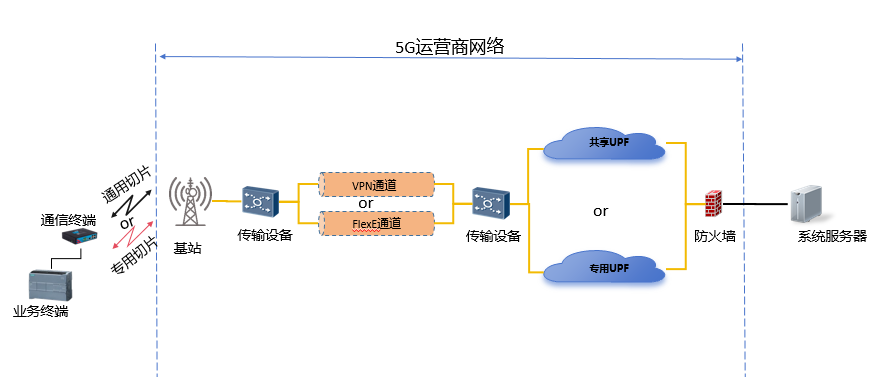
* 1. 5G通信系统

典型5G通信上行链路（数据采集与上传，见图2）：

PLC/传感器/摄像头数据→通信终端→基站→传输设备→VPN/FLEXE通道→UPF→防火墙→系统服务器。

典型5G通信下行链路（控制指令下发，见图2）：

远程操作指令→系统服务器→防火墙→UPF→传输设备→基站→通信终端→PLC执行动作。



**图2 起重机械的5G网络通信系统示意图**

1. 无线通信系统安全要求

起重机械无线通信系统应采用经过认证的无线通信协议（如IEEE 802.11ax及以上协议或3GPP 5G SA架构），支持强加密（如AES 128、SNOW3G 128、ZUC 128、AES-256、国密SM4等国家密码主管部门认可的算法），禁用弱加密协议（如WEP、WPA）。系统需采用安全的密钥管理机制，定期更换密钥（周期不超过24小时），并结合数据校验机制，确保数据传输的完整性和安全性。关于加密算法，目前5G网络无法配置AES-256 或国密 SM4，只支持AES 128(AES 128算法),SNOW3G 128(SNOW3G 128算法), ZUC 128(ZUC 128算法) 这个最好在里面加一下

系统需设置防火墙和入侵检测系统IDS，防止外部攻击与非法访问。定期开展网络安全审计、漏洞扫描及修复。记录无线通信操作日志，便于审计与排查。实时监控通信状态和数据，及时处理异常，定期备份关键数据，防止丢失。

对于具备5G功能的终端和网关，应支持3GPP标准认证机制，建议采用二次认证、安全芯片、GBA或AKMA认证。5G基站或核心网应支持终端访问控制，通过终端标识（IMSI/SUPI）、位置（CGI、TAI）、IMEI黑名单和流量限制等方式，仅允许特定终端接入5G专网。

系统应有自诊断和通讯故障保护功能，系统通电后，应能运行自检程序。自检或使用中，存在通讯信号中断或影响使用的故障，应立即发出报警信号并停止起重机械运行。

系统权限控制应采用基于角色的访问控制（RBAC），限制不同用户或设备的操作权限，如操作员（仅控制指令）、维护员（参数配置）、管理员（系统级操作），禁止越权访问。

网络传输带宽设计应满足视频传输、通信的要求，留有余量。

通信网络系统传输时延、抖动、丢包率应符合要求。

起重机械远程控控制系统监控中心应具备针对起重机械的紧急停止功能。

控制信号与视频信号应分开传输，可采用业务隔离或网关隔离或切片隔离等方式实现，QoS实现优先级保障，控制信号赋予更高优先级，保障时延。

系统应具备抗干扰能力，能够在复杂的工业环境中稳定运行，使用跳频技术或其他抗干扰措施，减少信号干扰对通信的影响。通信设备电磁兼容安全性能及测试方法应符合GB/T 22451要求。

非正常停机可能引发重大安全事故的起重机械，通信系统应具备冗余设计，确保在主通信链路失效时能够切换到备用链路。

视频系统分辨率应不低于1080P，视频帧率不低于25帧/s，视频存储时间不低于72h。

起重机械通信网络总体安全应符合GB/T 22239要求。

5G SIM卡安全参照行业标准YD/T 4970要求执行。

1. 无线通信网络性能测试
   1. 测试条件

网络工程性能测试需在满足以下条件的前提下进行：

a) 开始检测前，应根据设计、验收文件制定工程测试计划和测试文档；

b) 被测方应至少提供相关设备的进网许可证（含进网试用批文）、产品合格证、无线电发射设备

型号核准证等资质文件；

c) 检测所使用的仪器仪表应通过相应的计量和校准；

d) 无线局域网抽样测试AP的比例应不低于10%，被抽测AP的数量应不小于10个，如果总的AP数量小于10个，应全部测试。

* 1. 无线通信网络性能测试方法及判定准则
     1. 信号强度测试
        1. 边缘场强

测试步骤和判定准则：

a) 采用专业的 WLAN或5G维护类测试仪表或维护类测试仪表；

b) 在目标覆盖区域内进行打点测试；

c) 以热图形式得出测试区域的场强覆盖情况；

d) 测试路径的设计应合理，覆盖起重机接收装置的运行线路；

e) 边缘场强应符合系统设计、验收的要求。无线局域网和5G通信时，接收信号强度分别不低于-70dBm和-96dBm。

* + - 1. 信噪比

测试步骤和判定准则：

a) 使用WLAN或5G维护类测试仪表进行测试；

b) 在测试目标区域内进行打点测试；

c) 以热图形式显示测试区域内全面的信噪比测试结果；

d) 信噪比应符合系统设计、验收的要求。无线局域网和5G通信时，信噪比在设计目标覆盖区域内95%以上的位置，接收到的下行信号信噪比分别大于10dB和3dB。

* + - 1. QoS

测试步骤和判定准则：

a) 采用专业的WLAN或5G维护类测试仪表；

b) 检测队列调度机制；

c) 边缘场强符合系统设计、验收的要求，能够区分业务流，保障控制业务数据优先发送。

* + 1. 传输性能测试
       1. 网络连通性

测试步骤和判定准则：

a) 测试终端通过认证后，接入指定无线局域网络或5G网络；

b) 利用ping命令测试网络连通性；

c) 连续测试不小于50次，统计测试成功率；

d) 连通成功率应符合系统设计、验收要求，成功率大于97%。

* + - 1. 传输速率与吞吐量

测试步骤和判定准则：

a) 使用 WLAN维护类测试仪表关联到目标AP/SSID或采用5G测试终端接入5G通信网络；

b) 在起重机械运行区域内，采用网络性能测试工具，如Iperf，测试AP与模拟成STA的测试仪表之间的上传/下载速率，并对此AP/SSID进行系统吞吐量和带宽的测试，测试5G终端与服务器之间的上传/下载速率并对此5G通信链接进行系统吞吐量和带宽的测试；

c) 传输速率、系统吞吐量和带宽值应符合系统设计、验收的要求，传输速率宜满足上行不低于10Mbit/s，下行不低于30Mbit/s，并符合附录B要求。多视频终端时，带宽计算经验公式见附录C。

* + - 1. 丢包率

测试步骤和判定准则：

a) 将WLAN或5G维护类测试仪表接入网络；

b) 测试数据包应采用不少于100个ICMP64Byte帧长；

c) 记录丢包率等参数，丢包率计算公式：

d) 丢包率宜满足不少于95%路径，控制类数据包丢失率小于0.1%，视频类数据包丢失率小于0.3%。

* + - 1. 抖动

测试步骤和判定准则：

a) 将WLAN或5G维护类测试仪表接入网络；

b) 成功接入网络后，ping指定测试网络地址的时延；

c) 测试数据包应采用不少于100个ICMP 64Byte帧长；

d) 记录每次测试时延，平均抖动时延公式：；

e) 平均抖动宜小于20ms。

* + - 1. 往返时延
         1. 控制信号时延

测试步骤和判定准则：

a) 将测试终端接入无线局域网或5G网络；

b) 成功接入网络后，ping指定测试网络地址的时延；

c) 测试数据包应采用不少于100个ICMP 64Byte帧长；

d) 记录时延时间，精确到毫秒，往返时延计算公式：；

e) 往返时延应符合系统设计、验收要求，平均时延不大于30ms。

* + - * 1. 视频信号时延

测试步骤和判定准则：

a) 将测试终端接入无线网络或5G网络；

b) 成功接入网络后，ping指定测试网络地址的时延；

c) 测试数据包应采用不少于100个ICMP 1400 Byte帧长；

d) 记录时延时间，精确到毫秒，往返时延计算公式：；

e) 往返时延应符合系统设计、验收要求，平均时延小于100ms。

* + - 1. 网络故障停机检测

测试步骤和判定准则：

触发网络通信故障，远程操作站关闭网络连接，可采用点对点非应答模式（接收包间隔）或点对点应答模式（RTT往返时延），统计失败包的个数，起重机端控制信号触发停机状态为止，失败包个数与程序设计一致。（两种测试模式参见附录D）

1. 无线通信系统安全测试

测试可通过采用仪器仪表或测试工具进行或由5G网络提供商出具相关检测报告，包括但不限于接口和信令安全、5G终端接入安全、SIM卡安全、数据完整性保护等，测试环境见图1和图2。

测试工具及准备基本要求：

1. 测试方应使用不存在法律风险或合规风险的工具进行测试

b) 测试方应使用获得网络安全主管部门认可的漏洞扫描工具进行测试

c) 对于测试工具应确保不存在木马后门程序或严重的软件缺陷，应重点关注测试工具本身的安全性，及时针对测试工具进行补丁修复和版本升级；

d) 严禁使用公开的平台进行存在数据外发的漏洞利用测试，如采用公开的平台测试远程命令执行、XSS和SQL注入等漏洞；

e) 禁止向任何未经授权的第三方泄露测试相关的任何信息。

* 1. 网络通道安全测试
     1. 通信协议与加密检测
        1. 协议合规性测试

测试步骤及判定准则:

使用网络分析工具抓取无线通信数据包，结果显示采用符合要求的协议，且协议支持加密（如WPA3、AES-256）和认证机制（如EAP-TLS）。

* + - 1. 加密强度验证

测试步骤及判定准则：

通过渗透测试工具模拟攻击，测试加密算法的抗破解能力，记录破解所需时间，AES-256/SM4抗破解时间≥72小时。

验证密钥管理机制应安全，密钥生成、分发、更新流程合规。

* + 1. 网络安全防护检测
       1. 防火墙与入侵检测测试

测试步骤及判定准则：

模拟DOS/DDoS攻击或恶意流量，防火墙应能有效拦截，入侵检测系统（IDS）及时报警并阻断攻击。

* + - 1. 网络漏洞扫描

测试步骤及判定准则：

使用漏洞扫描工具对网络进行扫描，结果显示应无潜在漏洞。

* 1. 终端接入安全测试
     1. 无线局域网终端接入安全测试
        1. 假冒MAC地址

测试步骤和判定准则：

使用WLAN安全监测仪表，通过厂商OUI、无线媒体类型等进行假冒MAC地址测试。所获得的厂商OUI应符合厂商规范中的规定，AP设备具备MAC地址相关管理功能。

* + - 1. 射频扫描

测试步骤和判定准则：

使用相应测试工具对空SSID(NullSSID)探测帧进行检测。测试结果应符合系统安全功能设计、验收要求，AP设备具备射频相关管理功能。空SSID探测帧数宜小于50帧/s。

* + - 1. 接入认证

测试步骤和判定准则：

a) 在AP覆盖区域内不同地点使用“用户名+密码”方式进行20次DHCP+页面认证，记录是否认证成功；

b) 用户使用相应的测试终端，在网络覆盖区域内的不同地点进行20次MAC认证，记录是否认证成功；

c) 接入认证的控制策略应符合设计要求。认证失败次数宜小于或等于1次。

* + - 1. 非法接入测试
         1. 未授权AP

测试步骤和判定准则：

使用WLAN安全监测仪表通过MAC地址、生产商ID、SSID、无线媒体类型、射频信道等参数检测未授权AP。测试结果应符合系统防攻击设计、验收的要求。检测到的未授权AP的信号强度宜低于80dBm，或者其发送帧数小于50帧/s。

* + - * 1. 未授权STA

测试步骤和判定准则：

WLAN安全监测仪表与测未授权AP使用相同的机制，对未授权STA进行检测。测试结果应符合系统防攻击设计、验收的要求。检测到的未授权STA的信号强度宜低于80dBm，或者其发送帧数小于50帧/s。

注:这些检测机制是通过MAC地址、生产商ID、SSID、无线媒体类型、射频信道来实现的。另外，关联到未授权AP的终端同样会触发一个未授权终端告警。

* + 1. 5G终端安全接入测试
       1. 本体安全
          1. 通信唯一标识

测试步骤和判定准则：

a）审查配置文件，查看唯一标识生成方式

b）重启5G终端，抓包分析标识应无变化

c）更改终端配置，终端标识应无改变

* + - * 1. 终端漏洞检测

测试步骤及判定准则：

采用漏洞扫描工具对终端进行漏洞扫描，结果应未发现漏洞。

* + - * 1. 进程控制

测试步骤及判定准则：

启动未经配置允许的程序，结果应不能正常启动。

* + - 1. 访问控制

测试步骤及判定准则：

a）使用白名单外的IP地址访问终端的IP地址和端口，访问应不能成功。

b）5G基站或核心网开启任一限定条件验证，终端应不能正常上网。

* + - 1. 登录失败处理

测试步骤及判定准则：

使用错误密码尝试多次登录，检查账户应被锁定。闲置会话一段时间，会话应结束。

* + - 1. 认证与鉴权
         1. 机卡绑定

测试步骤及判定准则：

将SIM卡插入其他终端，应不能正常获取IP地址，机卡分离后约5分钟SIM卡停机。

* + - * 1. 身份认证

测试步骤及判定准则：

a）终端认证过程中应使用数字证书，并验证数字标识；

b）只有在认证通过后，业务数据才能接入；

c）手动篡改证书、密钥后，认证应不能成功。

* + - * 1. 双向认证

测试步骤及判定准则：

a）身份认证过程中终端证书应被主站验证；

b）身份认证过程中主站证书应被终端验证。

* + - 1. 终端信令和数据安全

测试步骤及判定准则：

通过5G路测工具测试或审查运营商提交的配置文件，测试结果或文件显示开启加密和完整性保护。

* 1. 控制信号与视频信号隔离测试

测试步骤及判定准则：

视频和控制数据隔离，可分为业务隔离、网关隔离、切片隔离（仅5G）三种(见附录F)，满足其中

一种方式即可。通过5G路测工具测试或审查运营商提交的配置文件，检查采用隔离的方式。

a）业务隔离采用网络侧抓包，解析视频和控制数据的目的IP应不同；

b) 网关（物理）隔离采用查看配置文件和现场目测检查，控制信号和视频信号采用不同网关进行传输；

c）切片隔离采用5G核心网抓捕或通过核心网日志验证切片隔离有效性，或审查运营商提交的配置文件，解析视频和控制数据应接入不同的5G网络切片。

* 1. 数据传输
     1. 完整性

测试步骤及判定准则：

1. 通过抓包工具，查看数据包中是否具有校验码、消息摘要、数字签名。
2. 篡改传输中的数据包（如修改CRC校验值），验证接收端是否能检测到异常。检查是否使用HMAC（哈希消息认证码）等机制确保数据完整性。
   * 1. 实时监控

测试步骤及判定准则：

部署日志分析工具监控数据传输过程，应识别异常行为（如重复请求、数据篡改）。

* + 1. 保密性
       1. 国密算法

测试步骤及判定准则：

通过抓包工具查看传输数据，应用国家密码主管部门认可的密码算法。

* + - 1. 数字证书分发

测试步骤及判定准则：

通过抓包工具验证，数据传输过程中应使用数字证书进行公钥分发。

* 1. 操作、权限与维护检测
     1. 权限控制验证

测试步骤及判定准则：

a）检查RBAC（基于角色的访问控制）配置，不同角色的操作权限严格隔离；

b）测试越权操作（如普通用户尝试管理员功能）,系统应进行拦截。

* + 1. 日志审计

测试步骤及判定准则：

检查系统，应记录完整的操作日志（如设备接入、密钥更新、异常事件）。

验证日志，应加密存储且不可篡改。

* + - 1. 人员培训验证

测试步骤及判定准则：

通过现场考核或模拟演练，确认操作人员熟悉安全规程和应急措施。

* + 1. 长期运行监测

测试步骤及判定准则：

连续运行系统72小时以上，监测通信稳定性、设备发热量等指标应符合设计要求。

* 1. 抗干扰与稳定性测试
     1. 频谱分析

测试步骤及判定准则：

使用频谱分析仪检测无线频段是否存在干扰源，并验证采用跳频技术（FHSS）或扩频技术（DSSS）或正交频分复用技术（OFDM）来增强抗干扰能力。

* + 1. 环境模拟测试

测试步骤及判定准则：

在复杂电磁环境（如工厂车间）中测试通信稳定性。在30dBm强干扰源下（模拟工厂电焊机干扰），持续通信10分钟，丢包率≤2%，时延波动≤20%。

模拟高负载场景，100台终端同时传输控制指令，监测网络吞吐量≥50Mbps时，时延≤80ms。

* + 1. 冗余与应急功能验证

测试步骤及判定准则：

a）通信系统如采用冗余设计，应人工切断主链路，记录切换时间及数据连续性，切换时间≤1秒，零数据丢失。

b）急停指令可靠性，在90dB噪声环境中发送急停信号，重复测试100次，成功率100%，响应时间≤100ms。

起重机无线局域网运行维护阶段工作要点

* 1. 运行维护工作内容

起重机无线局域网系统运行维护工作主要包括以下内容：

a) 检测无线局域网是否能在运行中实时管理以下性能问题；

1) 误包率过高；

2) 信源干扰；

3) 过低的传输速率；

b) 评估无线局域网的运行日志、维护记录等文档的记录、保存情况；

c) 检测无线局域网能否管理所有AP；

d) 检测无线局域网对于突发故障的处理能力；

e) 检测无线局域网的远程故障处理能力；

f) 对无线局域网环境的变化进行比较；

g) 检测无线局域网的隐藏终端；

h) 评估无线局域网多径干扰对性能的影响；

i) 进行无线局域网带内干扰源和带外干扰源的定位和规避。

* 1. 运行维护工作建议

起重机无线局域网系统运行维护工作建议包括：

a) 无线局域网的性能管理系统包括对以下情况进行实时报警:误包率过高、信源干扰及过低的传输速率。如果可以实时报警,则本项合格,否则不合格；

b) 无线局域网保存文档包括:日常运行的日志、故障处理记录、网络设备变更记录。否则本项不合格；

c) 无线局域网配备的AP管理工具功能如下:

1) 远程实时管理AP；

2) 当同一信道内的AP过多时的自动报警；

d) 无线局域网的故障检测诊断工具,在出现通讯故障时,可通过物理层检查、链路测试、协议分析做出处理。

表B.1 起重机械通信网络性能要求

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 业务大类 | 终端型 | 单终端需求速率-上行（Mbps） | 单终端需求速率-下行（Mbps） | 网络往返时延（ms） | 抖动（ms） | 丢包率 |
| 视频监控类 | 4K摄像头 | 4 | 不敏感 | 100 | 30 | <0.3% |
| 2.5K摄像头 | 4 | 不敏感 | 100 | 30 | <0.3% |
| 2K摄像头 | 2 | 不敏感 | 100 | 30 | <0.3% |
| 1080P摄像头 | 1 | 不敏感 | 100 | 30 | <0.3% |
| 控制类 | PLC | 1 | 1 | 30 | 20 | <0.1% |

多路视频终端汇集带宽计算经验公式

* 1. 方法1：

I帧码速=码率 × 6倍（6倍为一般配置值）

监控基线= I帧码速 × 碰撞个数 + 码率 ×（摄像头汇聚总路数 - 碰撞个数）

附录C.1 摄像头汇集后I帧碰撞概率

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 摄像头个数 | 非碰撞概率 | 2个I帧碰撞概率 | 3个I帧碰撞概率 | 4个I帧碰撞概率 | 5个I帧碰撞概率 | 6个I帧碰撞概率 |
| 1 | 100% | 0 | 0 | 0 | 0 | 0 |
| 5 | 65% | 34% | 2% | 0% | 0% | 0 |
| 10 | 13% | 72% | 14% | 1% | 0% | 0 |
| 15 | 0% | 56% | 38% | 6% | 1% | 0% |
| 20 | 0% | 25% | 57% | 15.60% | 0.20% | 0.02% |

* 1. 方法2：

如果I帧有发送时机协商机制，计算方式如下：

计算公式为：总带宽 = 单个摄像头码率 × 摄像头数量 ×（1 + 冗余系数）。

其中冗余系数一般取 10% - 20%，以应对网络波动等情况。例如，有 20 个 1080P 的摄像头，采用 H.264 编码，取 15% 的冗余系数，则总带宽 = 4Mbps×20×(1 + 15%)=92Mbps。

附录C.2 总带宽计算选择参数

|  |  |  |  |
| --- | --- | --- | --- |
| 分辨率 | 像素 | 编码格式 | 码率 |
| 720P | 100 万像素 | H.264 编码 | 2Mbps |
| H.265 编码 | 1.2Mbps |
| 1080P | 200 万像素 | H.264 编码 | 4Mbps |
| H.265 编码 | 2Mbps |
| 2K | 300 万像素 | H.264 编码 | 6Mbps |
| H.265 编码 | 3Mbps |
| 4K | 400 万像素 | H.264 编码 | 8Mbps |
| H.265 编码 | 4Mbps |

起重机械通信设备抗扰度测试要求

* 1. 静电放电抗扰度

通信终端应符合GB/T17626.2-2018中等级4的规定。接触放电试验电压8kV，空气放电试验电压15kV，试验期间通信终端不应出现损坏，数据不应出现长时间中断或丢失。试验结束后，电力5G通信终端应能正常工作和通信。

* 1. 射频电磁场辐射抗扰度

通信终端应符合GB/T17626.3-2016中等级3的规定。在磁场强度10Vm，频率范围80MHZ~1000MHZ，调幅80%AM(1KHz)，持续60s的试验环境中，通信终端应处于正常工作状态，不应出现数据丢失。

* 1. 工频磁场抗扰度

通信终端应符合GB/T17626.8-2006中等级4的规定。在场强度30A/m，持续60s的实验环境下，通信终端应处于正常工作状态，不应出现数据丢失。

* 1. 电快速瞬变脉冲群抗扰度

通信终端应符合GB/T17626.4-2018中等级4的规定。在电源端口试验电压+4kV，重复率SkIz，持续时间60s的试验环境中，ping包不应长时间中断，实验结束后，通信终端应能正常工作和通信。

* 1. 浪涌(冲击)抗扰度

通信终端应符合GB/T17626.5-2019中等级4的规定。在直流电源端口试验电压公模+4kV、差模+2kV、持续时间150s的试验过程中，通信终端应不应出现损坏，数据不应出现长时间中断或丢失。

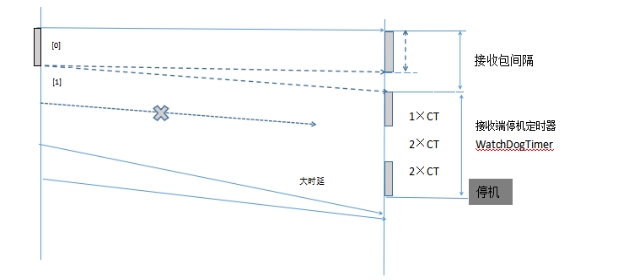
* 1. 阻尼振荡波抗扰度

通信终端应符合GB/T17626.18-2006中等级3的规定。在磁场强度30Am、持续时间60s的测试期间，通信终端应处于正常工作状态，数据不应出现丢失。

网络故障停机检测两种模式

* 1. 点对点非应答模式（接收包间隔）

点对点非应答模式业务逻辑见图E.1



图E.1 点对点非应答模式示意图

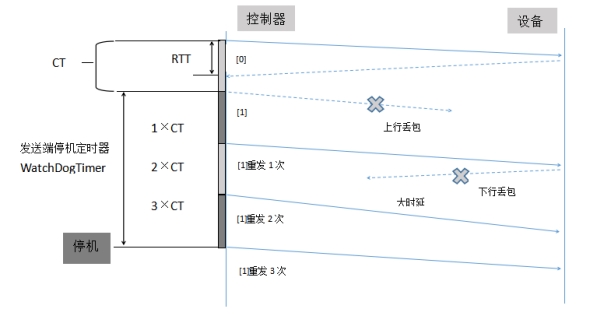
1) 发送端按照设定周期发送数据/控制指令；

2) 接收端接收到指令后进行相应动作；

3) 接收端连续一段时间没有收到控制指令则认为链路故障，停机。

* 1. 点对点应答模式（RTT往返时延）

点对点应答模式业务逻辑见图E.2



图E.2 点对点应答模式示意图

1) 发送端按照设定周期CT发送数据/指令；

2) 发送端在一定时间内没有收到应答，则重新发送；

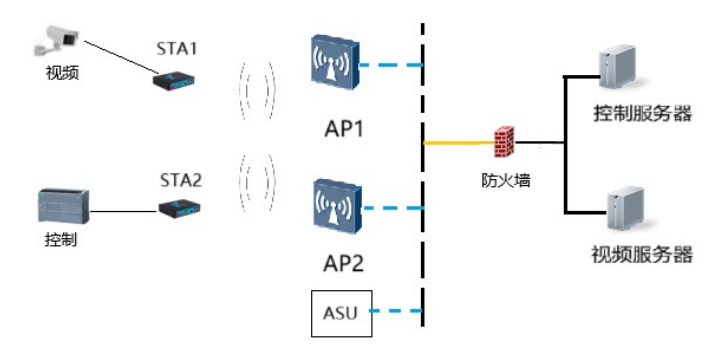
3) 发送端连续N次没有收到应答则认为链路故障，停机。

视频与控制信号三种隔离方式

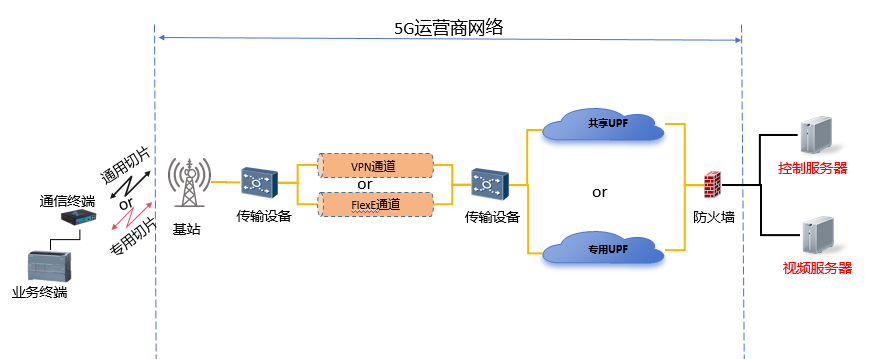
* 1. 业务隔离

1) 视频和控制数据对接不通的服务器，目的IP的不同，数据间隔离；

2) 在网络传输过程中，根据IP地址将视频和控制数据导向不同的路径。



图F.1 无线局域网业务隔离传输示意图



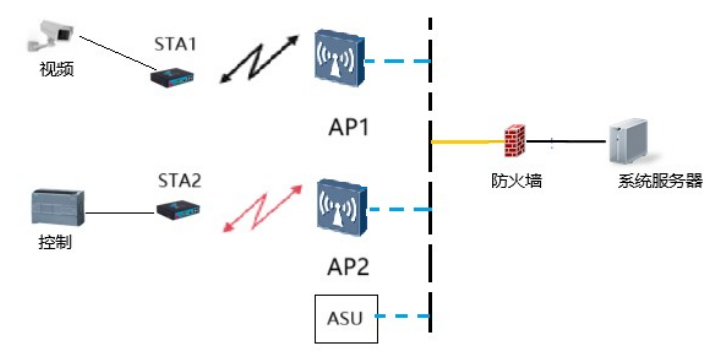
图F.2 5G业务隔离传输示意图

* 1. 网关（物理）隔离

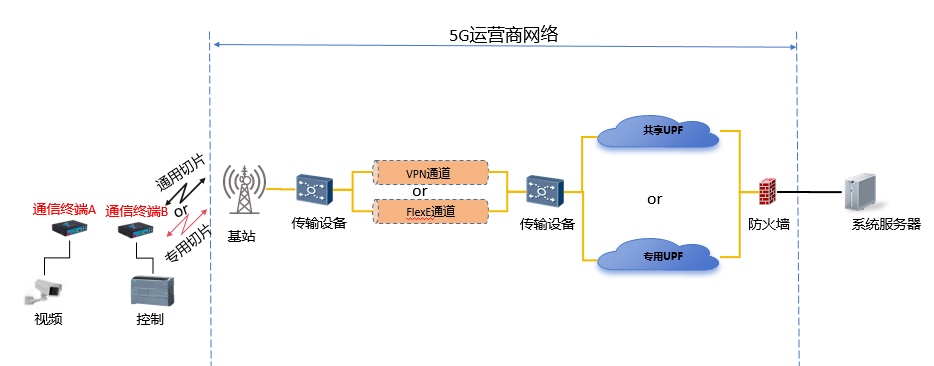
1) 视频和控制数据分别搭建独立的物理网络；

2) 5G通信终端A接视频业务，5G通信终端B接控制业务；

3) 5G通信终端A与5G通信终端B互不影响。



图F.3 无线局域网网关（物理）隔离传输示意图



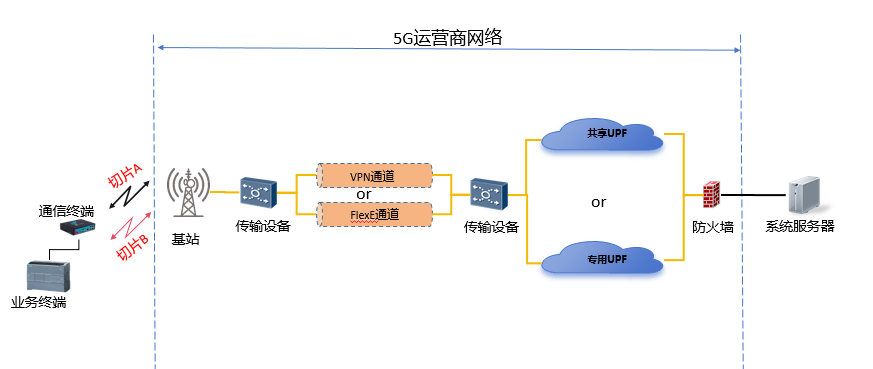
图F.4 5G网关（物理）隔离传输示意图

* 1. 切片隔离（仅针对5G通信）

1) 视频和控制数据配置不同的5G切片进行业务隔离；

2) 通过端口、ip、传输协议等，区分视频和控制数据；

3) 视频数据接5G切片A，控制数据接5G切片B。



图F.5 切片隔离传输示意图