# 智慧工地平台

# 塔式起重机设备要求及安全管理系统通讯协议

# （第二版）

成都市住房和城乡建设局制

# 目 录


1. 功能要求.....1
1.1. 必备功能.....1
1.2. 其他功能.....1
2. 系统要求.....2
2.1. 系统结构.....2
2.2. 通信方式.....2
2.3. 基本功能要求.....2
3. 平台接入协议.....4
3.1. 适用范围.....4
3.2. 协议说明.....4
3.3. 信息段说明.....5
3.3.1. 身份验证.....5
3.3.2. 实时数据上传.....6
3.3.3. 设备指令下发.....8
3.3.4. 信息传输.....8
3.3.5. 基本信息.....8
3.3.6. 保护区信息.....9
3.3.7. 限位信息.....11
3.3.8. 工作循环上报.....11
3.3.9. 远程升级.....12
3.3.10. 远程配置.....13
3.3.11. 心跳帧.....14
3.3.12. 指纹模板下发（取消使用）.....15
3.3.13. 照片上传.....16
3.3.14. 事件上报.....17
3.3.15. 顶升状态确认帧.....20
3.3.16. 登录状态确认帧.....20
3.3.17. 顶升数据传输帧.....21
3.3.18. 照片抓取指令请求.....21
4. CRC16 计算代码.....23

# 1. 功能要求

## 1.1. 必备功能

1、实时采集塔机吊钩当前高度
2、实时采集塔机小车当前位置
3、实时采集塔机当前吊重
4、实时采集塔机当前转角位置
5、实时采集塔机上方当前风速
6、实时采集相干涉塔机信息，做塔机防碰撞预警、报警
7、塔机与障碍物、禁行区之间的预警、报警检测
8、显示屏上对塔机各传感器的基本参数进行标定
9、显示屏上实时显示各传感器采集到的数据
10、显示屏上绘制塔机二维图形，供塔机操作人员观看
11、显示屏上绘制相干涉塔机俯视图
12、显示屏上对各传感器限位值的预警、报警做颜色闪烁处理，提醒塔机操作人员
13、语音提示预警、报警相关信息
14、对各传感器及设备自身故障进行自检
15、支持通过“成都市塔式起重机安全管理系统”对操作人员身份进行确认。
16、本地数据存储功能，缓存未上报成功等数据
17、工作循环检测
18、支持实时采集信息、预警等上传“成都市塔式起重机安全管理系统”。
19、设备自带电池包（能支持设备自主工作不小于 48 小时），并能实现电池电量检测

## 1.2. 其他功能

20、驾驶室照片抓取功能
21、设备远程升级功能（设备能自动下载服务器端提供固件，完成设备程序升级）
22、设备远程配置功能（可通过手机端远程配置设备相关参数）
23、顶升检测功能

# 2. 系统要求

## 2.1. 系统结构

塔机安全监控系统按照结构划分为塔机部分、工地部分、服务器部分和远程客户端四部分，系统结构如图 1 所示。

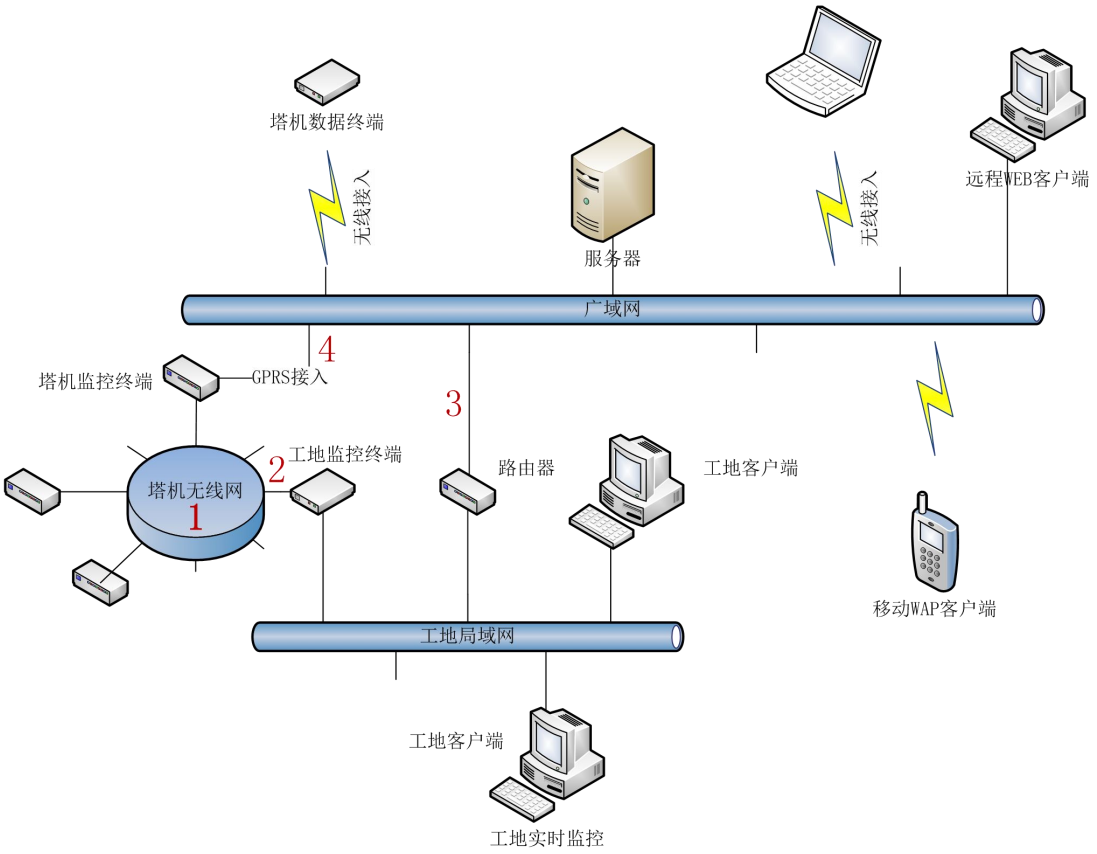



图 1 塔机安全监控系统结构图

## 2.2. 通信方式

各塔机监控终端以及工地监控终端之间采用微功率数传模块相互连接。塔机监控终端通过移动网络接入服务器平台。工地监控终端接入工地局域网供工地客户端实时监控，并可通过工地有线网络或者 3G 网络接入服务器平台。

## 2.3. 基本功能要求

塔机部分：功能至少包含塔机间碰撞保护，敏感区域保护，障碍物碰撞保护，超重力矩

保护，倾角、风速报警，人机管理，数据存储，故障诊断，数据上报功能。其中数据存储按照 1 秒为周期存储塔机运行状态，可追溯 30 天内的数据；记录塔机工作循环，报警，违章，故障诊断以及人员验证信息，存储容量不小于一百万条。

工地部分：功能至少包含局域网实时监控，参数设置，数据记录，报警、违章、故障数据统计与查看，数据上报。工地监控终端使用移动网络模式接入服务器。设备工作实时数据上传周期为 0.5-5 秒。

# 3. 平台接入协议

## 3.1. 适用范围

此标准适用于塔机安全监控系统中塔机监控终端与服务器平台、远程配置终端与服务器平台间的通信。

## 3.2. 协议说明

协议基于用户数据报协议（UDP），接入方式包含各种有线和无线的互联网接入方法。通信帧包含包括上行帧和下行帧两类。帧结构如下：

表 3-1　下行帧同步方式

| 帧同步方式 | 字节填充同步方式 |
|---|---|
| 帧同步字 | 用 DLE STX 标示帧的开始<br>用 DLE ETX 标示帧的结束<br>用 DLE DLE 标示传送数据信息中的 DLE<br>DLE = 0xFE　STX = 0xFB　ETX = 0xFA |

表 3-2 上、下行帧格式

| 字段 | 协议版本/厂商代码 | | 帧类型/信息段长 | | 设备代码 | 信息段 | 校验 |
|---|---|---|---|---|---|---|---|
| | 协议版本 | 厂商代码 | 帧类型 | 信息段长 | | | |
| 长度 | [7:4]4Bits | [3:0]4Bits | [15:11]5Bits | [10:0]11Bits | {3,16} Bytes | ≤ 1024Bytes | 2Bytes |

注：字节传输顺序采用网络字节序，由高字节到低字节依次发送。

表 3-3　协议版本

| 内容 | 此版本固定为：0x04 |
|---|---|
| 用途 | 用于前后协议兼容，便于后续升级 |

表 3-4 帧校验方式

| 校验方式 | CRC（16 位） |
|---|---|
| 多项式 | X16+X15+X2+1 |

注：CRC 参考代码见附录 1

表 3-5 厂商代码

| 内容 | 0-3 保留，4-15 用于区分不同厂商 |
|---|---|
| 定义 | 由监管部门统一分配 |

表 3-6 设备代码

| 内容 | 用于区分每台设备，各设备互不相同，（建议采用设备中网络模块的 IMEI 移 |
|---|---|

| | |
|---|---|
| | 动设备国际身份码 15 位+1 位自定义区分码）<br>16Bytes 在身份验证请求时使用，其余情况下使用 3Bytes |
| 定义 | 16Bytes，对于 GPRS 和 3G 接入方式，使用 IMEI；<br>对于有线接入方式，使用 MAC 地址。<br>3Bytes 登录后由服务器分配，作为通信 ID |

表 3-7 帧类型说明

| 帧类型值 | 说明 |
|---|---|
| 0x00 | 身份验证请求帧 |
| 0x01 | 身份验证回应帧 |
| 0x02 | 实时数据上传请求帧 |
| 0x03 | 实时数据上传回应帧 |
| 0x04 | 信息传输帧 |
| 0x05 | 信息回应帧 |
| 0x06 | 事件上报帧 |
| 0x07 | 事件回应帧 |
| 0x08 | 指纹帧 |
| 0x09 | 工作循环 |
| 0x0A | 设备指令确认回应帧 |
| 0x0B | 远程升级帧 |
| 0x0C | 远程配置帧 |
| 0x0D | 心跳帧 |
| 0x0E | 照片上传 |
| 0x10 | 远程配置客户端使用 |
| 0x11 | 顶升确认状态帧 |
| 0x12 | 登录状态确认帧 |
| 0x13 | 顶升数据传输帧（设备直接传给平台） |
| 0x14 | 照片抓取指令请求 |
| 0x1B | 安卓远程升级帧类型 |

表 3-8 发送顺序

| | |
|---|---|
| 字段顺序 | 表中各字段自左向右顺序依次发送 |
| 字节顺序 | 网络字节序（各字段由高字节到低字节依次发送） |

**注：为保证信息安全，设备应不接收非平台服务器 IP 地址发送的数据**

# 3.3.信息段说明

## 3.3.1. 身份验证

表 3-9 验证流程

| | |
|---|---|
| 验证方式 | 向服务器发送验证帧，直至验证成功。未收到回应每隔 20 秒后重发。 |

| | |
|---|---|
| 验证时机 | 开机或者持续 120 秒未收到服务器回应<br>（如网络状态很差 120 秒超时时间可调大，但不大于 600s） |

表 3-10 请求帧格式如下

| 字段 | 密码 |
|---|---|
| 内容 | 设备唯一 ID(32Bytes) |
| 内容 | 密码(32Bytes) 保留信息 |
| 长度 | 64bytes |

表 3-11 回应帧格式如下

| 字段 | 说明 | 字段长度 |
|---|---|---|
| 验证结果 | 验证结果 | 1Byte |
| 设备 ID | 验证成功后服务器分配的通信 ID | 3Bytes |
| 时间 | 当前时间，用于同步。<br>格式说明如下，后续的时间均以此为标准：<br>[31:26] 年，6bits，0-63(以 2010 为基数)<br>[25:22] 月，4bits，1-12<br>[21:17] 日，5bits，1-31<br>[16:12] 小时，5bits，0-23<br>[11:6] 分，6bits，0-59<br>[5:0] 秒，6bits，0-59 | 4Bytes |

表 3-12 验证结果说明

| 验证结果 | 说明 |
|---|---|
| 0x00 | 验证成功 |
| 0x01 | 不支持的厂商代码 |
| 0x02 | 设备代码未注册 |
| 0x03 | 密码错误 |
| 0x04 | 设备已禁用 |

### 3.3.2. 实时数据上传

表 3-13 发送方式

| | |
|---|---|
| 发送方式 | 持续循环发送，发送内容为塔机状态，不需要重发 |
| 上报时间 | 自定义间隔，间隔在 0.5 秒-20 秒之间 |

表 3-14 上报帧格式

| 字段 | 说明 | 字段长度 |
|---|---|---|
| 时间 | 状态采集时间 | 4Bytes |
| 回转（逻辑坐标） | 回转角度值，以 0.1 度为单位，范围-3276.8° － 3276.7° | 2Bytes |
| 幅度 | 幅度值，以 0.1 米为单位，范围 0 米 － 6553.5 米 | 2Bytes |
| 高度 | 吊钩离地面的距离，以 0.1 米为单位，范围-3276.8 米 － | 2Bytes |

| | | |
|---|---|---|
| | 3276.7 米 | |
| 称重 | 吊钩所掉重物的重量，以 0.01 吨为单位，范围 0 吨 － 655.35 吨 | 2Bytes |
| 力矩 | 当前力矩所占最大力矩的百分比，范围为 0 － 255 | 1Byte |
| 电池电量 | 0-100 | 1Byte |
| 风速 | 风速，以 0.1 米/秒为单位，范围为 0 米/秒 － 6553.5 米/秒 | 2Bytes |
| 塔身倾斜度 X 向 | 塔身倾斜角度，以 0.1 度为单位，范围为-12.8°- 12.7°<br>X 向与塔机坐标 X 轴向一致，如安装方向不一致请转换 | 1Byte |
| 塔身倾斜度 Y 向 | 塔身倾斜角度，以 0.1 度为单位，范围为-12.8°- 12.7°<br>Y 向与塔机坐标 Y 轴向一致，如安装方向不一致请转换 | 1Byte |
| 限位报警编码 | [3:0]左限位, [7:4]右限位, [11:8]远限位, [15:12]近限位, [19:16]高限位, [23:20]低限位<br>以上各值，0000 无，0001 预警，0010 报警，0100 故障，<br>bit25: 0-正常，1-回转机械左限位故障<br>bit26: 0-正常，1-回转机械右限位故障<br>bit27 : 0-正常，1-变幅机械远限位故障<br>bit28 : 0-正常，1-变幅机械近限位故障<br>bit29 : 0-正常，1-高度机械限位故障<br>bit30 : 0-正常，1-起重机械限位故障<br>bit31 : 0-正常，1-力矩机械限位故障<br>其余保留 | 4Bytes |
| 其他报警编码 | [3:0]起重<br>0000 无，0001 重载，0010 超载，0011 违章，0100 故障，其余保留<br>[7:4]力矩<br>0000 无，0001 重载，0010 超载，0011 违章，0100 故障，其余保留<br>[11:8]风速<br>0000 无，0001 预警，0010 报警，0100 故障，其余保留<br>[15:12]保留, [19:16]塔身倾角<br>0000 无，0010 报警，其余保留 | 4Bytes |
| 塔机碰撞报警编码 | [3:0]左碰撞, [7:4]右碰撞, [11:8]远碰撞, [15:12]近碰撞, [19:16]低碰撞<br>0000 无，0001 预警，0010 报警，其余保留<br>[BIT31]0-前臂，1-后壁 | 4Bytes |
| 禁行区碰撞报警编码 | [3:0]左侧禁行, [7:4]右侧禁行<br>0000 无，0001 预警，0010 报警，0011 违章，其余保留<br>[BIT31]0-前臂，1-后壁 | 4Bytes |
| 障碍物碰撞报警编码 | [3:0]左侧障碍, [7:4]右侧障碍, [11:8]远方障碍, [15:12]近方障碍, [19:16]低障碍<br>0000 无，0001 预警，0010 报警，其余保留<br>[BIT31]0-前臂，1-后壁 | 4Bytes |
| 继电输出编码 | 如果不支持，可填为全 0.<br>[3:0]左, [7:4]右, [11:8]远, [15:12]近, [19:16]高, [23:20]低 | 4Bytes |

| | | |
|---|---|---|
| | 0000 无，0001 截断低速，0010 截断高速，其余保留 | |

实时数据上传回应帧见 2.3.3 设备指令下发：

## 3.3.3. 设备指令下发

设备指令由服务器在实时数据上传回应帧中附加指令信息，返回终端，终端回应设备指令确认帧后，执行指令。

注意服务器指令通知下发后，在收到终端回应执行帧前，会在后续回应帧中保持指令下发状态。终端应及时回应，防止指令重复执行。或者回应指令后延时后执行。

表 3-15 实时数据上传回应帧格式

| 字段 | 说明 | 字段长度 |
|---|---|---|
| 服务器更新时间 | 服务器信息更新时间 | 4Bytes |
| 设备指令下发 | 0x00: 空指令，设备应无动作<br>0x01：主供电断电后 10 分钟关闭 3G 及传感器供电（一直发）<br>0x04: 设备重启<br>…… | 1Bytes |

## 3.3.4. 信息传输

表 3-19 发送方式

| | |
|---|---|
| 发送方式 | 带有确认帧的发送，失败则重发直到收到确认帧，重发超时时间 2 秒 |
| 发送时间 | 端口登录后发送 |

表 3-20 信息格式

| 字段 | 说明 | 字段长度 |
|---|---|---|
| 信息类别 | 0x01：基本信息<br>0x02：保护区信息<br>0x03：限位信息 | 1Byte |
| 信息内容 | 见具体定义 | 见具体定义 |

## 3.3.5. 基本信息

表 3-21 基本信息请求帧格式

| 字段 | 说明 | 字段长度 |
|---|---|---|

| | | |
|---|---|---|
| 信息版本 | 基本信息的版本号，范围 0-65535 | 2Bytes |
| 塔机名称 | 塔机的名称（支持显示中文 GB2312）为塔机现场编号 | 16Bytes |
| 塔机 ID | 塔机在当前塔群中的编号，范围 0-62，63 用于地面 | 1Bye |
| 塔群 ID | 塔机所在塔群的编号，范围 0-63（2km 区域的塔群 ID 必须不同） | 1Byte |
| 塔机类型 | 0x00，保留（固定式塔机、移动式塔机和自升式塔机） | 4bits |
| 吊绳倍率 | 2, 4, 6, 8 倍 | 4bits |
| 坐标 X | 以 0.1 米为单位，范围-3276.8-3276.7 米 | 2Bytes |
| 坐标 Y | 以 0.1 米为单位，范围-3276.8-3276.7 米 | 2Bytes |
| 前臂长度 | 前臂长度，0.1 米为单位，范围 0 米−6553.5 米 | 2Bytes |
| 后臂长度 | 后臂长度，0.1 米为单位，范围 0 米−6553.5 米 | 2Bytes |
| 塔臂高度 | 塔臂相对基础高度，0.1 米为单位，范围 0 米−6553.5 米 | 2Bytes |
| 塔帽高度 | 塔帽顶点相对于塔臂的高度，0.1 米为单位，范围 0 米-25.5 米 | 1Byte |
| 顶升位置角度 | 塔机转到不绞电缆的顶升方向时的逻辑角度读数。（以 0.1 度单位） | 2Byte |
| 安装经度 | 塔机经度 double 类型 | 8Byte |
| 安装纬度 | 塔机纬度 double 类型 | 8Byte |
| 指北角度 | 塔机从顶升位置转到指北方向时的逻辑角度读数。（以 0.1 度单位） | 2Byte |
| 版本号 | 0-255 | 1Byte |
| 版本子号 | 0-255 | 1Byte |
| APK 版本号 | 0-255 | 1Byte |
| APK 版本子号 | 0-255 | 1Byte |

表 3-22 基本信息回应帧格式

| 字段 | 说明 | 长度 |
|---|---|---|
| 信息类别 | 0x01：基本信息 | 1Byte |
| 信息版本 | 基本信息的版本号，范围 0-65535 | 2Bytes |

## 3.3.6. 保护区信息

获取时不区分保护区序号，一个工地固定一个保护区序号，所有保护区内的禁行区,障碍物，只发送一次(都是相对与 0 号塔机，不针对不同塔机重复发送同一障碍物)

表 3-23 保护区信息请求帧格式

| 字段 | 说明 | 字段长度 |
|---|---|---|
| 信息版本 | 保护区信息的版本号，范围 0-65535 | 2Bytes |
| 保护区个数 | 本塔机相关的保护区个数，范围 0-5 | 1Byte |
| 保护区信息 | 每个保护区的信息，见具体定义 | 见具体定义 |

所有保护区信息的保护区序号为 1

表 3-24 保护区信息格式

| 字段 | 说明 | 字段长度 |
|---|---|---|

| | | | |
|---|---|---|---|
| 保护区类型<br>保护区元素个数 | 保护区类型 | 0 禁行区，1 障碍物 | [7]1bit |
| | 保护区序号 | 每个保护区单独发送，则该字段对应于第几个保护区（1~6） | [6:4]3bits |
| | 保护区元素个数 | 保护区元素的个数，3-10 | [3:0]4bits |
| 保护区名称 | 保护区名称 | | 16Bytes |
| 保护区 id 号 | 保护区的 id 号，同一工地，每个保护区 id 号唯一 | | 1Byte |
| 保护区建筑类别 | 0 其他,1 医院,2 学校,3 广场,4 道路,5 居民区,6 办公区,7 高压线；其余类型待定（保留，只对禁行区有效） | | 1Byte |
| 保护区高度 | 只对障碍物有效 | | 2Bytes |
| 保护区元素信息 | 每个保护区元素的信息，见具体定义 | | 见具体定义 |

表 3-25 保护区元素信息格式

| 字段 | 说明 | 字段长度 |
|---|---|---|
| 保护区元素类型 | 0x00：点<br>0x01：圆弧（保留） | 1Byte |
| 保护区元素位置 | 每个保护区元素的位置信息，见具体定义 | 见具体定义 |

位置信息 X,Y 坐标都是相对与 0 号塔机的相对位置

表 3-26 保护区点位置信息格式

| 字段 | 说明 | 字段长度 |
|---|---|---|
| X 坐标 | 相对于塔机中心的 X 坐标，以 0.1 米为单位，范围 -3276.8 米−3276.7 米 | 2Bytes |
| Y 坐标 | 相对于塔机中心的 Y 坐标，以 0.1 米为单位，范围 -3276.8 米−3276.7 米 | 2Bytes |

表 3-27 保护区圆弧位置信息格式

| 字段 | 说明 | 字段长度 |
|---|---|---|
| 圆心 X 坐标 | 相对于塔机中心的 X 坐标，以 0.1 米为单位，范围 -3276.8 米−3276.7 米 | 2Bytes |
| 圆心 Y 坐标 | 相对于塔机中心的 Y 坐标，以 0.1 米为单位，范围 -3276.8 米−3276.7 米 | 2Bytes |
| 圆半径 | 圆弧所在圆的半径，,以 0.1 米为单位，范围 0 米−6553.5 米 | 2Bytes |
| 起点角度 | 圆弧所在圆起点角度，以 0.1° 为单位，范围 0° −359.9° | 2Bytes |
| 终点角度 | 圆弧所在圆终点点角度，以 0.1° 为单位，范围 0° −359.9° | 2Bytes |

表 3-28 保护区信息回应帧格式

| 字段 | 说明 | 长度 |
|---|---|---|
| 信息类别 | 0x02：保护区信息 | 1Byte |

| | | |
|---|---|---|
| 信息版本 | 基本信息的版本号，范围 0-65535 | 2Bytes |
| 保护区序号 | 对应于保护区数据编号（保留） | 1Byte |

## 3.3.7. 限位信息

表 3-29 限位信息请求帧格式

| 字段 | 说明 | 字段长度 |
|---|---|---|
| 信息版本 | 限位信息的版本号，范围 0 - 65535 | 2Bytes |
| 左限位 | 左转最大角度，以 0.1 度为单位，范围-3276.8° – 3276.7° | 2Bytes |
| 右限位 | 右转最大角度，以 0.1 度为单位，范围-3276.8° – 3276.7° | 2Bytes |
| 远限位 | 小车前行最远点离塔臂前端的距离，以 0.1 米为单位，范围 0 米 – 25.5 米 | 1Bytes |
| 近限位 | 小车回收最近点离塔身中心的距离，以 0.1 米为单位，范围 0 米 – 25.5 米 | 1Bytes |
| 高限位 | 吊钩起升的最高点离塔臂的距离，以 0.1 米为单位，范围 0 米 – 25.5 米 | 1Bytes |
| 起重量限位 | 塔机支持的最大起重量，以 0.01 吨为单位，范围 0 吨 – 655.35 吨 | 2Bytes |
| 最大幅度起重量限位 | 塔机最大幅度支持的最大起重量，以 0.01 吨为单位，范围 0 吨– 655.35 吨 | 2Bytes |
| 力矩限位 | 力矩限位百分比，单位为 1% | 2Bytes |
| 传感器使能标志（保留） | bit0：回转传感器使能标志；<br>bit1：幅度传感器使能标志；<br>bit2：高度传感器使能标志；<br>bit3：称重传感器使能标志；<br>bit4：行走传感器使能标志；<br>bit5：风速传感器使能标志；<br>bit6：塔身倾斜传感器使能标志； | 1Byte |

表 3-30 限位信息回应帧格式

| 字段 | 说明 | 长度 |
|---|---|---|
| 信息类别 | 0x03：限位信息 | 1Byte |
| 信息版本 | 限位信息的版本号 | 2Bytes |

## 3.3.8. 工作循环上报

设备 >> 服务器：

| 字段 | 说明 | 字段长度 |
|---|---|---|
| 起始时间 | 工作循环开始时间 | 4Bytes |
| 结束时间 | 工作循环结束时间 | 4Byte |

| | | |
|---|---|---|
| 吊重 | 工作循环最大吊重 | 2 Bytes |
| 登录状态 | 操作人是否打卡（0：未打卡，1：打卡） | 1 Bytes |
| 最大力矩 | 单位:0.1 kNm | 2Bytes |
| 最大高度 | 单位：0.1m | 2Byte |
| 最小高度 | 单位：0.1m | 2 Bytes |
| 最大变幅 | 单位：0.1m | 2 Bytes |
| 最小变幅 | 单位：0.1m | 2 Bytes |
| 起吊点转角 | 单位：0.1 度 | 2 Bytes |
| 起吊点变幅 | 单位：0.1m | 2 Bytes |
| 起吊点高度 | 单位：0.1m | 2 Bytes |
| 卸吊点转角 | 单位：0.1 度 | 2 Bytes |
| 卸吊点变幅 | 单位：0.1m | 2 Bytes |
| 卸吊点高度 | 单位：0.1m | 2 Bytes |

设备 >> 服务器（使用相同帧类型）：

| 字段 | 说明 | 字段长度 |
|---|---|---|
| 当前时间 | | 4Bytes |

## 3.3.9. 远程升级

远程升级的数据包采用第二 UDP 端口传输，包头中的帧类型字段值为 0x0B。

a. 查询心跳包

该包用于设备向服务器查询是否有新版本固件，数据包格式：

设备->服务器：

| 字段 | 会话序号（0-255） | 会话类型（0x051） |
|---|---|---|
| 长度 (byte) | 1 | 1 |

注：会话序号用于同步设备与服务器的每次对话，发起方在本地对其计数，一次对话成功后对该计数加 1， 应答方发送数据时直接复制发送该字段。

服务器->设备：

| 字段 | 会话序号（0-255） | 会话类型（0x051） | 版本号（为 0 表示服务器端无固件） | 版本子号 | 固件长度（byte） | 文件 MD5 值（无固件时该字段不存在） |
|---|---|---|---|---|---|---|
| 长度 | 1 | 1 | 1 | 1 | 4 | 16 |

b. 固件获取包

该包用于设备向服务器请求固件数据，当设备查询到固件版本号比自身固件版本更新之后，便进入远程升级状态，发送该包获取固件数据，一直到固件下载完成，或者下载失败。

数据包格式：

设备->服务器：

| 字段 | 会话序号（0-255） | 会话类型（0x052） | 数据在固件文件中的偏移地址 | 本次获取数据的长度 |
|---|---|---|---|---|
| 长度(byte) | 1 | 1 | 4 | 4 |

服务器->设备：

| 字段 | 会话序号（0-255） | 会话类型（0x052） | 实际可用数据长度 | 数据 |
|---|---|---|---|---|
| 长度 | 1 | 1 | 4 | … |

单个固件数据获取包的数据长度推荐使用 512，设备在发送获取包 500ms 后如果还未收到对应会话的服务器应答，则应重新发起该会话，即用同样会话序号再发送获取包，服务器连续超过 10 次无应答，设备应视为升级失败，退回到空闲状态。

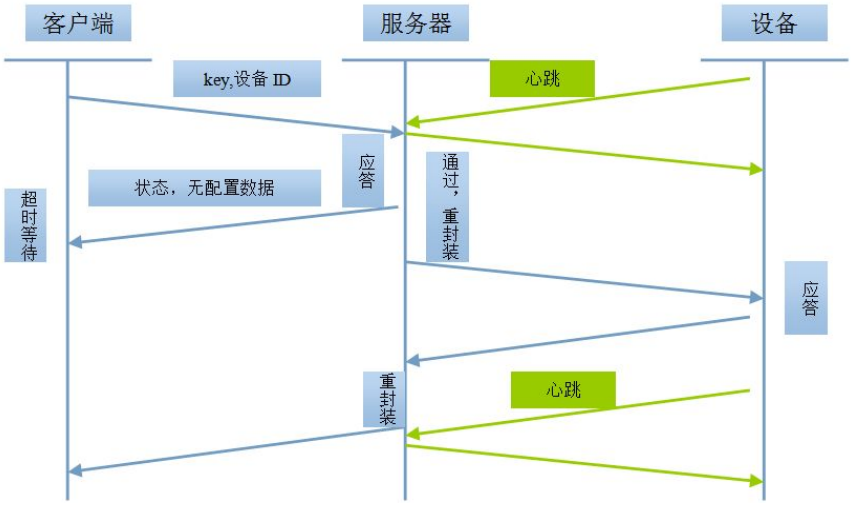
设备根据查询到的固件数据长度来判断整个固件数据是否获取完成，完成后需要对固件文件进行 MD5 计算，如果计算出的 MD5 值和查询到的 MD5 值相等，则固件成功下载，保存固件文件，否则放弃保存固件文件。最后退出固件升级状态，让该通信的端口回到空闲状态。

**安卓远程升级帧类型：0x1B**

**安卓升级包下载时，会话序号长度改为 2 字节无符号数，其它与设备升级保持一致**

## 3.3.10. 远程配置

远程配置的数据包采用第二 UDP 端口传输，包头中的帧类型字段值为 0x0C，设备的通信流程如下：




a. 远程配置客户端与服务器通信数据包头协议与塔机大致相同，省去了登录过程，包头格式如下。

| 字段 | 协议版本/厂商代码 | | 帧类型/信息段长 | | 客户端 ID（MAC 后三字节） | 信息段 | 校验 |
|---|---|---|---|---|---|---|---|
| | 协议版本 | 厂商代码 | 帧类型（10H） | 信息段长 | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 长度 | [7:4]4Bits | [3:0]4Bits | [15:11]5Bits | [10:0]11Bits | 3bytes | ≤1024B | 2B |

信息段格式如下：

客户端->服务器：

| 字段 | 口令 | 设备 ID | 配置数据包 |
|---|---|---|---|
| 长度 (byte) | 8 | 12 | (变长） |

服务器->客户端：

| 字段 | 状态 | 设备 ID | 配置数据包 |
|---|---|---|---|
| 长度 (byte) | 1 | 12 | (变长） |

状态字段值解释：

0x00: 数据成功到达服务器端

0x01：表该帧含设备回发的配置数据包字段

0x02：key 未通过

0x03：设备无响应

0x04：设备不在线 （服务器根据是该设备是否处于活跃状态(5s 内有数据通信)判断设备在线状态）

b. 远程配置设备端数据格式。

远程配置数据包包头中的帧类型值使用 0x0C，信息段里存放对应客户端 ID 和配置数据包。

服务器->设备：

| 字段 | 客户端 ID | 配置数据包 |
|---|---|---|
| 长度 (byte) | 3 | (变长） |

设备->服务器：

| 字段 | 客户端 ID | 配置数据包 |
|---|---|---|
| 长度 (byte) | 3 | (变长） |

## 3.3.11. 心跳帧

心跳帧 5s 发送一次，在端口处于空闲状态时发送。心跳帧类型值为 0xD，第一端口需要发送心跳帧， 以维持端口活跃状态。 第二端口由于有新固件请求帧一直在发送，所以不需要再单独发送心跳帧。心跳帧信息段内容格式：

| 字段 | 说明 | 字段长度 |
|---|---|---|
| 时间 | 当前设备时间 | 4 |
| 风速 | 0.1m/s | 2 |

| | | |
|---|---|---|
| 电量 | 0-100，百分点 | 1 |
| 风速报警 | Bit[0-3] | 1 |

心跳帧服务器回应格式:

| 字段 | 说明 | 字段长度 |
|---|---|---|
| 时间 | 当前服务器时间 | 4 |
| 设备指令下发 | 0x00: 空指令，设备应无动作，主供电断电后不关闭 3G 供电<br>0x01：主供电断电后 10 分钟关闭 3G 及传感器供电（一直发）<br>0x04: 设备重启<br>0x05: 设备关机<br>… | 1Bytes |

## 3.3.12. 指纹模板下发（取消使用）

指纹模板下发通信使用第二 UDP 端口，帧类型为 0x08，采用一次性全发的方式，设备定时(1 分钟)查询一次服务器是否有模板更新。如果是，则下载模板存入高速 flash。

a. 指纹模板文件

服务器的模板文件不能大于 64k，其中模板文件数据格式如下：

| 字段 | 说明 | 长度 |
|---|---|---|
| 模板版本 | 用于区分是否有模板更新，可以时间戳表示 | 4 byte |
| 人员个数 | | 4 byte |
| 人员 1 证书编号 | GB2312 编码，空余字节补 0 | 24byte |
| 人员 1 姓名 | GB2312 编码，空余字节补 0 | 8 byte |
| 人员 1 指头 1 模板 | 包含 3 个 512 字节的模板数据 | 1536 byte |
| 人员 1 指头 2 模板 | 包含 3 个 512 字节的模板数据 | 1536 byte |
| 人员 2 证书编号 | GB2312 编码，空余字节补 0 | 24byte |
| 人员 2 姓名 | GB2312 编码，空余字节补 0 | 8 byte |
| 人员 2 指头 1 模板 | 包含 3 个 512 字节的模板数据 | 1536 byte |
| … | … | … |

b. 设备查询指纹模板数据包格式

该包用于设备向服务器查询是否有新版本指纹模板，发送间隔为 60s 一次，服务器对其作出响应，会话应答超时为 500ms。

设备->服务器：

| 字段 | 会话序号<br>（0-255） | 会话类型<br>（0x051） |
|---|---|---|
| 长度<br>(byte) | 1 | 1 |

注：会话序号用于同步设备与服务器的每次对话，发起方在本地对其计数，一次对话成功后

对该计数加 1， 应答方发送数据时直接复制发送该字段。

服务器->设备：

| 字段 | 会话序号（0-255） | 会话类型（0x051） | 版本号（为 0 表示服务器端无指纹模板） | 文件长度（byte） |
|---|---|---|---|---|
| 长度 | 1 | 1 | 4 | 4 |

c. 设备获取指纹模板文件包格式

该包用于设备向服务器请求指纹模板数据，当设备查询到固件版本号比本地现有指纹模板版本新之后，便进入下载更新状态，发送该包获取指纹模板数据，一直到文件下载完成，或者下载失败。只有当下载成功之后，设备才更新指纹模板到指纹头。数据包格式：

设备->服务器：

| 字段 | 会话序号（0-255） | 会话类型（0x052） | 数据在固件文件中的偏移地址 | 本次获取数据的长度 |
|---|---|---|---|---|
| 长度 (byte) | 1 | 1 | 4 | 4 |

服务器->设备：

| 字段 | 会话序号（0-255） | 会话类型（0x052） | 实际可用数据长度 | 数据 |
|---|---|---|---|---|
| 长度 | 1 | 1 | 4 | … |

数据获取包的数据长度推荐使用 512，设备在发送获取包 500ms 后如果还未收到对应会话的服务器应答，则应重新发起该会话，即用同样会话序号再发送获取包，服务器连续超过 10 次无应答，设备应视为下载败，退回到空闲状态。

## 3.3.13. 照片上传

照片上传通信使用第二 UDP 端口，帧类型为 0x0E，设备主动发起，服务器做出响应。

设备->服务器：

| 字段 | 人员登录时间 00h | 人员证书编号 | 文件总长度 | 文件偏移地址 | 数据段长度 | 数据段 |
|---|---|---|---|---|---|---|
| 长度 | 4 | 24 | 4 | 4 | 4 | 变长（<=512） |

服务器->设备：

| 字段 | 照片文件偏移地址 00h |
|---|---|
| 长度 | 4 |

## 3.3.14. 事件上报

事件上报计入平台统计，必须确保每帧均正确上报，如未收到正确回应帧在 2 秒后重发。

表 3-41 事件上报帧格式

| 字段 | 说明 | 字段长度 |
|---|---|---|
| 发生时间 | 事件发生时间 | 4Bytes |
| 事件类型 | 0x03：故障诊断<br>0x05：人员登录上报<br>0x07：升降上报<br>0x09: 关机上报<br>0x0A: 报警上报<br>0x0B: 更换钢绳事件<br>0x0C: 机械限位故障上报 | 1Byte |
| 事件信息 | 事件的具体信息 | N Bytes |

表 3-42 事件回应帧格式

| 字段 | 说明 | 字段长度 |
|---|---|---|
| 最后收到上报时间 | 服务器收到的最后一个上报事件的发生时间 | 4Bytes |
| 事件类型 | 0x03：故障诊断<br>0x05：人员登录上报<br>0x07：升降上报<br>0x09: 关机上报<br>0x0A: 报警上报<br>0x0B: 更换钢绳事件<br>0x0C: 机械限位故障上报 | 1Byte |
| 指令下发 | 0x00 不操作，0x01 主供电断电后 10 分钟关闭 3G 及传感器供电;0x04 设备重启;0x05 设备关机<br>只针对掉电故障有效，其他默认 0x00 | 1Byte |

### 1) 故障诊断信息上报

***故障信息描述：***

表 3-43 监控系统故障

| 字段 | 说明 | 字段长度 |
|---|---|---|
| 故障掩码 | 0-正常, 1-故障<br>Bit[0]:变幅传感器故障<br>Bit[1]:高度传感器故障<br>Bit[2]:转角传感器故障<br>Bit[3]:吊重传感器故障<br>Bit[4]:风速传感器故障<br>Bit[5]:海拔传感器故障（暂不用）<br>Bit[6]:倾角传感器故障（暂不用） | 2 |

| | | |
|---|---|---|
| | Bit[7]:语音电路故障<br>Bit[8]:无线模块故障<br>Bit[9]:存储系统故障<br>Bit[10]:主供电掉电<br>Bit[11]: 参数设置故障<br>Bit[12]: 时钟故障<br>Bit[13]: 3G 模块故障<br>Bit[14]: 显示屏通讯故障<br>Bit[15]：保留 | |

## 2) 人员登录上报

| 字段 | 说明 | 字段长度 |
|---|---|---|
| 打卡状态 | 0x10：打卡成功，0x00:未打卡，0x01:打卡失败 | 1Bytes |
| 操作人员 ID | 操作人员证书编号（此字段只存在于打卡状态为成功时） | 24Bytes |

## 3) 自动关机上报

表 3-61 关机上报信息格式

| 字段 | 内容 | 长度 |
|---|---|---|
| 电池电压 | 关机前一刻电池的电压，单位 0.1V | 2Bytes |
| 电量百分比 | 关机前一刻电池电量的百分比，单位 1% | 1Bytes |

## 4) 报警上报

表 3-62 报警上报信息格式

| 字段 | 内容 | 长度 |
|---|---|---|
| 动作时间 | | 4bytes |
| 动作类型 | 1-产生，2-解除 | 1bytes |
| 报警级别 | 1-预警，2-报警，3-违章 | 1bytes |
| 报警类型 | 0x11:左限位，0x12:右限位，0x13:近限位，0x14:远限位，0x15:高限位。<br>0x21:左碰撞，0x22:右碰撞，0x23:近碰撞，0x24:远碰撞，0x25:低碰撞<br>0x31:左障碍，0x32:右障碍，0x33: 近障碍，0x34:远障碍，0x35:低障碍 | 1bytes |

| | | |
|---|---|---|
| | 0x41:左禁行，0x42:右禁行<br>0x51：吊重 ，0x52:力矩<br>0x61：风速<br>0x71: 未打卡操作设备 | |
| 力矩 | uint8_t 当前力矩所占最大力矩的百分比，范围为 0 － 255 | 1byte |
| 转角 | int16_t 当前转角（相对于塔机自身角度）0 0.1 度为单位 | 2bytes |
| 变幅 | int16_t 小车当前位置，以 dm 为单位 | 2bytes |
| 高度 | int16_t 吊钩当前高度，以 dm 为单位 | 2bytes |
| 吊重 | int16_t 吊钩所掉重物的重量，以 0.01 吨为单位 | 2bytes |
| Vlue | 各类型值 | 2bytes |
| resverse | 保留 | 2bytes |
| uint32_t state_alarm_upload 记录报警上报状态<br>1-报警状态已上报 0-报警状态未上报<br>bit0:左限位报警上报<br>bit1:右限位报警上报<br>bit2:近限位报警上报<br>bit3:远限位报警上报<br>bit4:高限位报警上报<br>bit5:吊重报警上报（已使用）<br>bit6:吊重违章上报（已使用）<br>bit7:力矩报警上报（已使用）<br>bit8:力矩违章上报（已使用）<br>bit9:风速报警上报<br>bit10:打卡违章上报 | | |

**注：碰撞和障碍物无展示数据，可选择勾选的方式**

## 5) 更换钢绳上报

表 3-63 更换钢绳上报信息格式

| 字段 | 内容 | 长度 |
|---|---|---|
| | | 1bytes |

## 6) 机械限位故障上报

表 3-64 机械限位故障上报信息格式

| 字段 | 内容 | 长度 |
|---|---|---|

| | | |
|---|---|---|
| 动作时间 | | 4bytes |
| 动作类型 | 1-产生，2-解除 | 1bytes |
| 故障类型 | 0x11:回转机械限位故障（单位：0.1 度） 阀值：<br>0x12:变幅机械限位故障（单位：dm）<br>0x13:高度机械限位故障（单位：dm）<br>0x14:起重机械限位故障（单位：10kg）<br>0x15:力矩机械限位故障（单位：百分比） | 1bytes |
| | 故障产生时，上报故障产生起始点的值<br>故障解除时，上报由故障产生到解除的过程中最大（最小）的值<br>注：力矩值为百分比 | 2bytes |

## 3.3.15. 顶升状态确认帧

顶升状态确认请求帧

| 字段 | 说明 | 字段长度 |
|---|---|---|
| 设备 ID | 当前设备唯一标识 | 16bytes |
| 顶升开始时间 | | 4bytes |
| 等待超时 | 生成顶升二维码后等待是否超时（暂定半小时）<br>0x00：等待未超时<br>0x01：等待超时 | 1byte |

顶升状态确认回复帧

| 字段 | 说明 | 字段长度 |
|---|---|---|
| 顶升信息提交状态 | 0x00:未收到顶升信息提交状态<br>0x01:收到顶升记录状态且测量值和实际值一致<br>0x02:收到顶升记录状态但测量值和实际值不一致<br>0x03:收到设备端等待超时状态 | 1byte |
| 错误代码 | | 1byte |

## 3.3.16. 登录状态确认帧

登录状态确认请求帧

| 字段 | 说明 | 字段长度 |
|---|---|---|
| 设备 ID | 当前设备唯一标识 | 16bytes |
| 状态 | 等待用户登录时间（暂定 5 分钟）<br>0x00：正常请求<br>0x01：收到平台已登录状态 | 1byte |

| | | |
|---|---|---|
| | 0x10：退出登录 | |

登录状态确认回复帧

| 字段 | 说明 | 字段长度 |
|---|---|---|
| 登录状态 | 0x00：未登录<br>0x01：已登录<br>0x02：确认设备端收到登录状态（设备端收到该状态后不再发请求）<br><br>0x11：收到设备端退出登录状态 | 1byte |
| 操作员姓名 | 状态为已登录时解析 | 8bytes |

## 3.3.17. 顶升数据传输帧

表 3-60 顶升数据传输帧

| 字段 | 内容 | 长度 |
|---|---|---|
| 顶升开始时间 | | 4Bytes |
| 顶升结束时间 | | 4Bytes |
| 顶升状态 | 0x00:未开始顶升<br>0x01:顶升开始<br>0x02:顶升正常结束<br>0x03:顶升非正常结束 | 1byte |
| 错误代码 | 0x00: 顶升循环正常完成<br>0x01: 顶升循环超时 | 1byte |
| 标准节数量 | | 1Byte |
| 保留 | | 1Byte |
| 顶升前塔臂高度 | 以 0.1 米为单位，范围-3276.8 米 － 3276.7 米 | 2Bytes |
| 顶升后塔臂高度 | 以 0.1 米为单位，范围-3276.8 米 － 3276.7 米 | 2Bytes |

表 3-60 顶升数据传输帧

| | | |
|---|---|---|
| 顶升开始时间 | | 4Bytes |

## 3.3.18. 照片抓取指令请求

照片抓取指令请求帧

| 字段 | 说明 | 字段长度 |
|---|---|---|
| 状态 | 0x00：正常请求<br>0x01：显示端正在抓拍照片 | 1byte |

| | | |
|---|---|---|
| | 0x02:　照片上传成功<br>0x03:　照片上传失败<br>0x04:　显示端抓拍照片失败<br>注：平台收到 0x02、0x03、0x04 后回复 0x03 | |

照片抓取指令回复帧

| 字段 | 说明 | 字段长度 |
|---|---|---|
| 登录状态 | 0x00：未下发抓取指令<br>0x01：抓取照片<br>0x02：设备正在抓拍照片<br>0x03:　此次通讯结束 | 1byte |

2.4 部分国家（建议）参考标准（gbt28264-2017）

1、pg_10: 操作指令做监控（宜监控）

2、Pg_10: 抗风防滑做监控（宜监控）

3、Pg_10: 视频监视点

4、Pg_11: 信息采集源做控制功能

5、Pg_11: 系统检测出起重机械发生故障时，除发出报警外还应具备按要求预设的止停控制功能

6、Pg_11: 在关闭电源或者供电中断时，系统的信息存储单元应保留已采集的所有信息

7、Pg_11: 系统应能存储不少于 30 个连续工作日的监控数据，应能存储不少于连续 72h 的视频数据

8、Pg_12: 系统的检测应对司机的操作指令进行实时监控、记录、及历史回放

# 4. CRC16 计算代码

```
unsigned short crc16_calculate(unsigned char* pucSendBuf, unsigned short
usLen)
{
    unsigned short i, j;
    unsigned short usCrc = 0xFFFF;
    for (i = 0; i < usLen; i++)
    {
        usCrc ^= (unsigned short)pucSendBuf[i];
        for (j = 0; j < 8; j++)
        {
            if (usCrc & 1)
            {
                usCrc >>= 1;
                usCrc ^= 0xA001;
            }
            else
            {
                usCrc >>= 1;
            }
        }
    }

    return usCrc;
}
```