

F-C-03-01: RS232/RS485 通讯乱码或无数据

典型现象

- 上位机或 PLC 接收到的数据为乱码（如 ??、00 等）。
- 通讯完全无响应，发送指令后无任何返回。
- 部分数据正确，但偶尔夹杂错误字节。

可能原因

- 串口参数不匹配**：波特率、数据位、停止位、校验位（None/Even/Odd）在主从设备间不一致。
- 接线错误**：
 - RS-232: TX 接 RX（交叉），GND 必须连接。
 - RS-485: A(+) 接 A(+), B(-) 接 B(-)，若反接则无数据。
- 电平不匹配**：RS-232 设备与 RS-485 设备直接连接，未使用转换器。
- 硬件故障**：串口芯片损坏、USB 转串口驱动异常。
- 终端电阻缺失**：长距离 RS-485 无终端电阻，信号反射导致乱码。

排查思路

- 核对通讯参数**：使用串口调试助手（如 CommTool），尝试常见组合（9600,8,N,1；19200,8,E,1 等），直到能收到正确数据。
- 检查接线**：
 - RS-232: 用万用表测量 TX→RX 引脚对地电压，正常应在 $\pm 5\sim\pm 12V$ 之间。交叉接线（2-3，3-2，5-5）。
 - RS-485: 确认 A 接 A、B 接 B。对调两根线后测试。
- 测试回路**：短接 RS-232 的 2-3 脚，发送数据应自收自回。若无，串口硬件可能故障。
- 检查转换器**：若使用了 USB 转 RS-485，更换品牌转换器测试。
- 增加终端电阻**：对于 RS-485 超过 100 米或悬挂多个节点，在两端加 120 Ω 电阻。

保养提示

- 在设备台账中记录每个串口的通讯参数（波特率、奇偶校验等），避免遗忘。
- 定期紧固接线端子，防止氧化松动。
- 为长距离 RS-485 使用屏蔽双绞线，并单端接地。

F-C-03-02：无线 AP 信号不稳定

典型现象

- 移动设备（AGV、手持终端）在不同位置时信号强度变化剧烈。
- 通讯时断时续，任务因掉线而失败。
- AP 指示灯异常（如橙灯常亮、绿灯慢闪）。

可能原因

- 天线遮挡或安装不当**：金属货架、立柱遮挡信号；天线极化方向不一致。
- 同频干扰**：附近其他 AP 或微波设备使用相同信道。
- 功率不足**：AP 发射功率过低，或移动端天线增益不足。
- AP 漫游切换延迟**：多个 AP 覆盖边界重叠不足，切换不及时。
- WiFi 频段选择错误**：2.4 GHz 干扰多；5 GHz 穿墙能力弱。

排查思路

- 使用信号测试工具**：手机安装 WiFi Analyzer，现场走动测量 RSSI 值。理想值 > -65 dBm。
- 调整天线**：将天线竖直向上，避开金属遮挡；若货架高，采用吸顶天线或定向天线。
- 更改信道**：扫描周围 AP 使用的信道，选择干扰最小的（1、6、11 或自动信道选择）。
- 检查 AP 功率设置**：登录 AP 管理界面，将发射功率调整到最大（但需符合法规），逐步降低找到平衡点。
- 优化漫游**：开启 AP 的“快速漫游”（802.11r）或调整漫游阈值（-70 dBm 触发切换）。
- 切换频段**：若 2.4 GHz 干扰严重，强制使用 5 GHz（需设备支持）。

保养提示

- 定期使用热力图软件（如 Ekahau）评估无线覆盖，补点或调整 AP 位置。
- 每季度检查 AP 固件版本，升级修复已知的漫游 bug。
- 在 AGV 路径上设置关键点位，监控丢包率，一旦恶化通知维护。

F-C-03-03：扫码枪偶发漏读

典型现象

- 扫码枪触发后，界面未显示条码或提示“读取失败”。
- 同一个条码有时能读有时不能读。
- 其他扫码枪在同一位置可正常读取。

可能原因

- 条码质量差**：脏污、破损、打印模糊、对比度低。
- 景深不合适**：扫码枪与条码之间的距离不在有效焦距范围内。
- 通讯干扰**：RS-232 或 USB 线缆过长、附近电磁干扰。
- 解码设置错误**：扫码枪禁用了当前条码类型（如 Code128、QR）。
- 瞄准光斑偏移**：激光线或 LED 十字线未对准条码中心。

排查思路

- 更换条码测试**：打印一张新的高对比度条码，若可读则原条码质量差。清洁或重新打印。
- 调整距离**：移动扫码枪（从 5cm 到 30cm）逐步测试，找到最佳读取距离。
- 检查通讯线缆**：更换短 USB 线或 RS-232 线。若为无线扫码枪，检查电池电量及无线干扰。
- 恢复出厂设置**：扫描恢复默认配置码（参见说明书），启用所有常用码制。
- 观察瞄准光斑**：确保光线对准条码中央。若偏移，使用设置码调整。
- 测试其他位置**：若仅在特定工位漏读，检查环境光（强光直射）或振动。

保养提示

- 定期清洁扫码枪窗口镜片，避免灰尘积垢。
- 设置扫码成功后蜂鸣或振动反馈，操作员可立即发现漏读。
- 每半年验证一次扫描景深，记录最佳位置。

F-C-03-04: OPC UA 连接中断

典型现象

- OPC 客户端与服务器之间的连接无故断开，需重新连接。
- 数据订阅停顿，变量值不更新。
- 日志报错：“Secure channel closed”、“Certificate validation failed”。

可能原因

- 证书过期或不受信任**：服务器或客户端证书有效期结束，或未加入信任列表。
- Endpoint URL 错误**：配置的地址（如 `opc.tcp://192.168.1.10:4840`）与服务器实际监听地址不符。
- 安全策略不匹配**：客户端与服务器所选的安全策略（如 Basic256Sha256、None）不一致。
- 心跳超时**：网络短暂中断导致未收到 keep-alive 消息，连接被服务端关闭。
- 用户认证失败**：用户名/密码错误，或匿名访问被禁用。

排查思路

- 检查证书状态**：
 - 在 OPC 服务器中查看证书有效期，若过期则重新颁发。
 - 将客户端证书添加到服务器的“信任证书”列表中。
- 验证 Endpoint**：使用 UaExpert 客户端连接到服务器，查看可用的 Endpoint 列表，选择正确的 URL。
- 降低安全策略测试**：临时将安全策略设为“None”，如能连接则说明是安全配置问题。
- 调整会话超时**：在客户端增大 Session Timeout（如从 60 秒改为 300 秒）和 Keep-Alive 间隔。
- 检查用户权限**：确认使用的用户名具有连接权限，且密码未过期。
- 抓取网络包**：使用 Wireshark 捕获 OPC UA 报文（端口4840），观察断开前的错误代码。

保养提示

- 为 OPC UA 证书设置自动续期（如 Let's Encrypt）或使用更长的有效期（10 年）。
- 采用高可用 OPC 服务器集群，避免单点故障。
- 部署 OPC 隧道或代理，对不稳定网络进行缓冲。