

# 华芯智科 安全白皮书

端·边·云·管：工业物联网与端侧智能的安全架构、机制与边界

华芯智科 Huaxin Core · 2026-09 · 本文档描述架构与机制，具体参数与配置基线通过资料对接环节提供

## 第一章 威胁模型与安全架构总纲



图 5 · 应急响应六步与不承诺项



图 4 · 数据生命周期与三条边界



本章定义资产范围、四层信任边界、威胁模型与设计原则，并写明不承诺的边界。威胁模型采用 STRIDE，逐条给出攻击者前提与缓解机制；能力按「已支持 / 按项目适配 / 规划中」三态标注。「端」指设备层，「边」指网关与端侧推理，「管」指网络层，「云」指平台层与应用层。

## 1.1 资产与信任边界

### 被保护的资产

| 资产                 | 失陷后果        | 保护机制                          |
|--------------------|-------------|-------------------------------|
| 设备身份：一机一密密钥、设备证书   | 冒名上线、伪造上报   | 密钥不以明文出片；按设备维度校验；换板即重注册并吊销旧密钥 |
| 原始数据：遥测原始值、图像、工艺参数 | 工艺泄露与合规风险   | 端云分级；原始遥测可设「永不出厂」标签，端侧只回传决策结论 |
| 控制指令：下行控制、配置与围栏    | 误动作、人身伤害、停产 | 指令签名与防重放；沙箱限定执行边界；关键指令二次确认    |
| 固件与模型：镜像、权重与配置     | 后门植入、模型被调包  | 启动链验签；加密存储；A/B 双槽原子切换与失败回滚    |
| 密钥与凭据：签名私钥、租户密钥    | 批量伪造、跨租户泄露  | 分层密钥体系与托管；最小权限；敏感操作两人复核       |

### 四层信任边界

| 边界                    | 默认不信任什么         | 边界上的强制机制                        |
|-----------------------|-----------------|---------------------------------|
| B1 端 ↔ 边（本地总线、串口、园区网） | 设备侧软件栈与本地链路     | 采集侧鉴权与测点白名单；明文老设备不直接暴露公网        |
| B2 边 ↔ 管（网关出口、承载网络）   | 弱网、共享链路、可被劫持的网络 | MQTT/HTTPS 强制开启；TLS 双向校验；证书周期轮换 |
| B3 管 ↔ 云（平台接入层）       | 任何入站连接与凭据       | 一机一密与双向认证；接入限流；注册需授权与工单         |
| B4 云内与运维通道            | 本租户外的服务与运维终端    | 多租户隔离（可物理隔离）；细粒度 RBAC；服务间鉴权     |

1.2 威胁模型（STRIDE）

按 STRIDE 六类（仿冒、篡改、抵赖、信息泄露、拒绝服务、权限提升）逐层建清单。前提取最低假设：A1 可物理接触；A2 可控制链路一跳；A3 持有低权限云侧账号；A4 可接触供应链某一环节；A5 可记录并重发报文。长时间持有设备并做实验室级拆解与侧信道分析者不在模型内，理由见 1.4。

端（设备）

| 编号   | STRIDE    | 攻击面                           | 前提           | 缓解机制                               | 状态    |
|------|-----------|-------------------------------|--------------|------------------------------------|-------|
| T-01 | 篡改 / 信息泄露 | 物理拆解：开箱取板、短接、替换探头             | A1           | 防拆开关与 Tamper Mesh 触发即清零 TEE 内密钥并留痕 | 按项目适配 |
| T-02 | 权限提升      | 调试口暴露：UART / JTAG / SWD 可读写内存 | A1 且会接线调试    | 量产固件关闭调试通道并烧断调试位；授权调试需专用凭证         | 已支持   |
| T-03 | 篡改 / 信息泄露 | 固件提取与回滚：读镜像或下发旧版              | 能读取存储或投递 OTA | 加密存储并验签后写非活跃分区；计数器拒收更低版本           | 已支持   |

边（网关与端侧推理）

| 编号   | STRIDE    | 攻击面                    | 前提           | 缓解机制                              | 状态           |
|------|-----------|------------------------|--------------|-----------------------------------|--------------|
| T-04 | 权限提升      | 网关越权并向内网横向，以网关跳板访问产线网  | 已取得网关普通权限    | 测点白名单与只读边界；策略沙箱在 TEE 内执行；内网不开放管理面 | 已支持          |
| T-05 | 信息泄露 / 篡改 | 模型窃取与投毒：拷走权重、替换模型、污染样本 | 可读取网关存储或影响回传 | 模型加密存储、TEE 内解密并验签，外部注入拒载；样本回传验签名  | 已支持，训练侧审计规划中 |

管（传输）

| 编号   | STRIDE    | 攻击面                  | 前提           | 缓解机制                                                               | 状态  |
|------|-----------|----------------------|--------------|--------------------------------------------------------------------|-----|
| T-06 | 仿冒 / 信息泄露 | 中间人：恶意接入点、链路一跳被劫持    | A2           | MQTTs/HTTPS 强制开启，TLS 1.2 及以上，禁用 SSLv3 与 TLS 1.0/1.1 及弱套件；证书双向校验并轮换 | 已支持 |
| T-07 | 仿冒        | 伪造设备接入：泄露凭据上线、重复身份同登 | 已获凭据或能触达注册接口 | 一机一密按设备维度校验；换板即重注、旧密钥即时吊销；同密钥异地登录即拒绝并告警                            | 已支持 |

| 编号   | STRIDE | 攻击面                   | 前提         | 缓解机制                                  | 状态  |
|------|--------|-----------------------|------------|---------------------------------------|-----|
| T-08 | 篡改     | 重放与指令篡改：录制报文重发或改写下行指令 | A5         | 指令签名并带时间戳与随机数，端侧以可信时钟与计数器验重；沙箱强制执行边界  | 已支持 |
| T-09 | 拒绝服务   | 流量压制：大量伪造连接或链路长时间中断   | 具备带宽或能切断链路 | 接入限流、DDoS 防护与 WAF；断网自治与缓存补传；链路中断作告警上报 | 已支持 |

云（平台）

| 编号   | STRIDE      | 攻击面                      | 前提            | 缓解机制                                           | 状态    |
|------|-------------|--------------------------|---------------|------------------------------------------------|-------|
| T-10 | 权限提升 / 信息泄露 | 越权与横向：低权限提权、跨租户访问、运维终端跳板 | A3 或运维终端已被入侵  | 多租户隔离（可物理隔离）；RBAC 分只读、运维、管理员；OTA 两人复核；服务间鉴权与分段 | 已支持   |
| T-11 | 篡改          | 供应链植入：芯片、模组、外包生产或物流环节    | A4            | 供应商准入与来料核验、关键器件渠道管控、产线密钥注入审计、依赖清单跟踪            | 按项目适配 |
| T-12 | 抵赖 / 篡改     | 审计抵赖与日志篡改：删改记录掩盖路径       | 已取得日志或运维通道写权限 | 日志全量留存，哈希链与可信时钟保证完整与顺序；查看与写权限分离                | 已支持   |

十二条威胁覆盖 STRIDE 六类：端与边多以物理可达为前提，管以链路可控为前提，云以凭据或终端失陷为前提。

1.3 设计原则

- 最小权限：**只授予任务所需权限并带有效期；因为横向移动依赖上一步多给的权限。
- 默认拒绝：**白名单外的连接、测点、指令与模型一律拒绝；因为黑名单滞后于新攻击面。
- 纵深防御：**端、边、管、云各自独立守住底线；因为单层机制都可能被绕过。
- 密钥不落盘明文：**根密钥在可信根内生成或注入，不出安全边界；因为拿到密钥即拿到身份。
- 原始数据不出厂可选项：**原始遥测可设「永不出厂」标签，端侧只回传结论；因为现场多数要求数据不出物理边界。
- 可审计可追溯：**策略命中、模型加载、越界拦截与开箱写入哈希链封存日志；因为不能回放的事故无法定责。
- 失败安全 (fail-safe)：**断链、策略超时或校验失败时转入保守状态（限速、限区、人工确认、回滚）；因为可用性压力最易压低底线。

**升级必须可回滚：**写入非活跃分区并原子切换、失败自动回滚，并以计数器阻止降级绕过修复；因为可回滚与防降级须同时成立。

1.4 不做什么 / 不承诺什么

**不承诺物理不可提取：**不承诺设备在攻击者具备物理拆解能力且长时间接触时仍不可提取密钥；防拆与清零的目标是提高成本、留下痕迹、使后果可追溯。

**不承诺侧信道与故障注入防护：**功耗、电磁、时序侧信道与电压、时钟毛刺不在设计与验证范围内。

**不承诺存量设备同等能力：**无安全启动或只跑明文的老设备，安全等级取决于网关后的边界防护，须在验收单注明。

**不承诺尚未取得的合规结论：**等保 2.0 三级为测评推进中，ISO/IEC 27001 为体系建设中；证书出具前不声明「已通过」「已认证」。

**不承诺 GDPR 合规结论：**GDPR 为就绪设计，面向出海客户场景；未承接欧盟个人数据业务前不做合规承诺。

**不承诺国密之外的通用密码合规结论：**国密 SM2/SM3/SM4 已支持且为可选套件，属平台能力而非认证证书。

**不承诺「永不出厂」在被自行改配后仍成立：**客户自行开启外发通道后结论随之变化，需重新核对数据流。

**不承诺绝对不被入侵：**风险收敛程度取决于部署方式、运维水平与客户侧管控。

**不公开测试细节：**红队与渗透测试结论可在保密协议下查阅，攻击路径与绕过细节不公开。

1.5 适用范围与读者

本文面向客户 CISO 与安全负责人、总工与架构师、集成商技术负责人、采购与合规人员。本文描述架构与机制，不含具体参数与配置基线；密码套件清单、端口开通清单、加固配置基线样例、证书轮换周期、审计字段定义等，通过资料对接环节按项目提供。

| 读者                 | 关注点                     | 建议读法              |
|--------------------|-------------------------|-------------------|
| CISO / 安全负责人、采购与合规 | 威胁是否被识别、边界是否成立、承诺边界是否清晰 | 1.2 至 1.4，重点看不承诺项 |
| 总工 / 架构师           | 信任边界画在哪、原则能否落地          | 1.1、1.3           |
| 集成商技术负责人           | 边界上的强制机制与三态能力           | 1.1、1.5           |

涉及本方的资质与能力状态以下表为准。

| 事项                 | 状态    | 说明                             |
|--------------------|-------|--------------------------------|
| 等保 2.0 三级          | 测评推进中 | 计划 2027 Q1 完成测评与备案，时间随测评机构排期调整 |
| ISO/IEC 27001      | 体系建设中 | 计划 2027 Q2 完成认证审核，证书编号通过后公布    |
| GDPR 数据处理设计        | 就绪设计  | 面向出海客户场景；未承接欧盟个人数据业务前不做合规承诺    |
| 国密 SM2 / SM3 / SM4 | 已支持   | 可选套件，按交付项目启用；属平台能力，不是第三方认证证书   |
| 退租数据擦除             | 已支持   | 退租数据 30 日内彻底擦除并出具报告            |
| 端侧模型 FP16 回退       | 已支持   | 关键任务支持 FP16 回退，精度损失按逐层比对判定     |

本章要点

- 需保护的资产为设备身份、原始数据、控制指令、固件与模型、密钥与凭据五类；四层之间共四条信任边界，每层对相邻层默认不信任。
- 威胁清单共 12 条，覆盖 STRIDE 六类，逐条给出攻击者前提条件与缓解机制，缓解按三态标注。
- 八条设计原则中，默认拒绝、失败安全与可回滚最易被可用性压力侵蚀，需在交付与运维环节单独立项守住。
- 明确不承诺物理长时间接触下的密钥不可提取、不承诺侧信道防护、不承诺等保三级与 ISO/IEC 27001 的既得结论、不承诺 GDPR 合规结论。
- 本文只描述架构与机制；参数、配置基线与资质证据通过资料对接环节提供，合规状态以《可信与合规中心》台账为准。

第二章 设备与端侧安全：从芯片到应用的信任链与现场边界

设备交付现场后，物理可达、网络不可信是常态。本章说明端侧安全边界如何建立，并列出不在于防护假设内的能力。能力按三态标注：已支持、按项目适配、规划中。

2.1 安全启动与信任链

信任自片内不可改写的 BootROM 开始，每级只校验下一级。

| 校验级            | 校验对象             | 信任根                 | 失败动作              |
|----------------|------------------|---------------------|-------------------|
| BootROM → 一级引导 | 引导头与签名           | ROM 固化公钥哈希（一次性可编程位） | 不跳转，进 SoC 恢复模式    |
| 引导 → 内核        | 内核、设备树、initramfs | 同层级密钥逐级派生           | 回退 A/B 可用分区，失败进恢复 |
| 内核准入 → 根文件系统   | 只读根、系统分区         | 哈希树摘要随镜像签名          | 不挂可写根，重启进恢复       |
| 系统 → 应用与容器     | 应用包、容器镜像         | 发布密钥签名的镜像清单         | 拒绝加载，其余服务继续       |

**熔丝与失败动作。**产线在整机测试通过后逐台写入安全启动使能位、根密钥哈希、单调计数器初值与调试生命周期位，写入不可逆。任一级校验失败即进恢复模式：恢复镜像只支持刷写、诊断与日志导出，不运行业务，无"跳过校验"开关，不降级放行。

2.2 一机一密与设备身份

**生成在哪里。**私钥在安全芯片内生成且不离开芯片，或由产线密钥管理服务在硬件安全模块内生成后封装下发；不用 MAC、SN 等可枚举标识充当凭据。

**产线注入流程。**① SN 与设备内公钥请求绑定；② 产线 CA 或客户 CA 签发设备证书；③ 写入安全芯片密钥槽、TEE 安全区或加密分区；④ 挑战值验签回读；⑤ 证书指纹与批次入台账，出厂前断外网完成接入与吊销自检。

**不出厂区的约束。**密钥环节在独立网段完成，签名服务与 CA 无公网出口；私钥不以文件、标签、包装或工单形式离开该网段，不落盘明文；注入失败的设备按废品处理密钥槽。

| 存储载体    | 私钥可导出性     | 说明                |
|---------|------------|-------------------|
| 安全芯片    | 不可导出，签名在片内 | 已支持，带安全单元的网关与 DTU |
| TEE 安全区 | 不可导出至普通世界  | 按项目适配，依赖主控平台      |
| 加密分区    | 密文可读、明文不可得 | 密钥由设备唯一密钥封装       |

**吊销与换新。**吊销状态由平台维护并周期性下发，证书按短周期自动轮换；返修换板或失窃时提交书面吊销，旧证书立即失效，换新设备重走注入流程并记入台账。

2.3 固件与模型的可信更新

**签名与密钥层级。**国密 SM2/SM3 为可选套件（已支持），默认 ECDSA P-256 与 SHA-256。根密钥离线保管、不联网，仅用于签发发布密钥；发布密钥在签名服务内外包；镜像与模型签名密钥随批次轮换，根密钥按门限使用。

**版本防回滚。**单调计数器位于熔丝或受保护存储，只增不减；发布清单声明最低版本号，设备拒绝低于下限的镜像，含版本号更低的回放镜像。

**A/B 双分区与断电续传。**更新写入非活动分区，分片下载、支持断电续传，写完校验整包哈希与签名，再以原子槽位标志切换启动项。首次启动为试运行，服务、自检与心跳正常才确认，否则自动回滚；槽位标志与版本双副本写入，掉电后可判定启动项。

**灰度与熔断判据。**灰度按内场样机、种子现场、按区域与批次逐步放开，是否继续由下列字段判定；阈值在升级单中按型号与现场基线书面约定，不给固定数值。

| 判据字段       | 含义               | 触发动作         |
|------------|------------------|--------------|
| 升级成功率      | 成功确认台数占本批下发台数之比  | 低于批次阈值即暂停本批  |
| 回滚率        | 试运行未确认而回滚的占比     | 超阈值即暂停并冻结版本  |
| 启动失败与看门狗复位 | 升级后单位时间的启动异常计数   | 超阈值即熔断停发     |
| 离线率偏移      | 与升级前同型设备基线的偏离    | 正向偏离超阈值即熔断   |
| 关键业务错误码    | 指定错误码在升级后设备的出现次数 | 出现即人工介入      |
| 人工熔断       | 值班与交付负责人可随时停止灰度  | 立即生效，按回滚策略运行 |

**模型更新。**模型与固件同一链路；支持 FP16 回退，精度由逐层比对判定，偏差超约定范围即不发布。

2.4 端侧数据边界

**原始数据本地处理，只回传决策结论。**端侧推理在设备内完成，上行内容为结论、事件与统计量，不含原始遥测、图像与音频；传输强制开启 MQTTS/HTTPS。

**「永不出厂」标签在端侧如何生效。**它不是云端过滤规则，而是设备内的数据分流：

- 标签随签名配置下发，端侧保存策略表；
- 采集侧在写入上行队列前判定，命中数据只写本地加密库，不进上行路径；
- 报文按白名单字段构造，集合外字段丢弃并计数；
- 补传与实时路径共用同一过滤，缓存分区按标签隔离；

标签变更与丢弃计数留痕上报，经鉴权可现场核验生效策略。

**本地缓存的加密与保留。**落盘数据写入加密分区，密钥由设备唯一密钥封装；保留策略按保留时长与容量上限配置，超限按时间顺序覆盖。

**72h 弱网缓存补传的完整性。**断网期间按队列本地缓存，恢复后按序补传：每条记录带单调序号，批次附 SM3 摘要或 HMAC；平台按设备标识与序号去重幂等；补传前后核对摘要，不一致记录进隔离区并上报，不静默丢弃。

**退租与回收。**退租数据 30 日内擦除并出具报告；设备回收或转租时，端侧销毁封装密钥使密文不可解读并记录动作。

2.5 物理与接口防护

现场设备默认物理可达，防护目标是可发现、可收敛、可追溯。

| 威胁             | 机制                                 | 边界                   |
|----------------|------------------------------------|----------------------|
| 调试口被用于读内存或改写引导 | 量产态关闭 UART 控制台与 JTAG，生命周期位与引导器共同禁止 | 熔丝已闭合的整机不可恢复开启，需换主控板 |
| 需重新开启调试口       | 客户书面授权加服务端一次性令牌与时效窗口，到期自动关闭        | 单人无工单不可开启，令牌不可复用     |
| 拆壳读取存储介质       | 存储加密，密钥置于安全芯片或 TEE                 | 具拆焊能力者可读到密文，对抗见 2.6  |
| 固件被提取与仿制       | 安全启动，镜像加密按项目适配                     | 不对合法获得设备者的复制作承诺      |
| 现场维护越权         | 维护需客户授权与服务端令牌，临时账号设有效期             | 不接受共享口令与长期有效账号       |

**外壳防拆与审计。**防拆开关、螺丝封胶与易碎标触发的事件本地记录并上报，可配置告警或清除密钥；作用是让拆解被发现，而非不可能。设备记录安全启动结果、镜像与模型版本、熔丝摘要、恢复模式进入、调试口开关与升级回滚事件并上报；日志带完整性摘要，重写或截断可被发现。

2.6 明确不承诺的边界

下表能力**不在本产品标准防护假设内**；确有此类威胁模型时按项目单独评估并形成书面结论。

| 攻击能力                        | 是否在防护假设内 | 说明              |
|-----------------------------|----------|-----------------|
| 长时间物理接触、拆焊、芯片解封、显微探测与聚焦离子束  | 不在假设内    | 属实验室级攻击能力       |
| 侧信道分析（功耗、电磁、时序）与故障注入（毛刺、激光） | 不在假设内    | 按项目单独评估，不承诺对抗等级 |
| 冷启动与内存残留读取                  | 不在假设内    | 密钥不驻留普通内存属尽力而为  |
| 供应链与代工环节的芯片级植入              | 不在假设内    | 依赖器件厂商与代工厂流程    |
| 设备不可被破解的一般性承诺               | 不承诺      | 只承诺提高成本与可发现性    |

## 2.7 能力状态与合规口径

| 项目                           | 状态                   | 说明           |
|------------------------------|----------------------|--------------|
| 国密 SM2/SM3/SM4               | 已支持，可选套件             | 传输与签名链路按项目启用 |
| MQTT/HTTPS                   | 已支持，强制开启             | 端侧不启用明文端口    |
| 原始遥测「永不出厂」                   | 已支持                  | 点位级标签，端侧生效   |
| 断网 72h 缓存补传                  | 已支持                  | 序号与摘要校验，去重幂等 |
| FP16 回退与逐层比对                 | 已支持                  | 精度由逐层比对判定    |
| 安全启动、A/B 回滚与调试口授权            | 已支持，部分按项目适配          | 视主控平台与生命周期位  |
| 等保 2.0 三级 / ISO 27001 / GDPR | 测评推进中 / 体系建设中 / 就绪设计 | 平台侧与出海场景     |
| 退租数据擦除                       | 已支持                  | 30 日内擦除并出具报告 |

### 本章要点

- 信任链自 BootROM 起逐级校验，失败即进恢复模式，不降级放行；熔丝与一次性可编程位是物理锚点。
- 一机一密在产线完成，私钥在安全芯片或硬件安全模块内生成且不可导出，吊销与换新记入台账。

- 固件与模型共用签名、A/B 分区、自动回滚与单调计数器；灰度判据字段明示，阈值按批次约定。
- 「永不出厂」在采集侧生效；72h 补传带序号与摘要校验；退租数据 30 日内擦除并出具报告。
- 长时间物理接触、拆焊、侧信道、故障注入、冷启动与芯片级植入不在防护假设内。

## 第三章 传输安全与身份体系

本章说明设备从出厂到退役的全过程里，"谁在跟谁说话、说的话有没有被改过、断网时数据还算不算数"这三件事。默认立场是：网络不可信、明文不可接受、离线不等于失去控制。MQTT/HTTPS 强制开启，明文端口不作为生产接入方式；国密 SM2/SM3/SM4 作为可选套件已支持。

### 3.1 双向认证：设备与平台互验证书

设备接入使用 mTLS（TLS 1.3 优先，TLS 1.2 及以上兜底），链路两端都出示 X.509 证书。

| 握手阶段           | 设备侧动作              | 平台侧动作             | 失败处理          |
|----------------|--------------------|-------------------|---------------|
| 版本与套件协商        | 提交支持的协议版本与套件       | 协商版本与套件           | 版本或套件不合规即中止   |
| 平台证书           | 校验证书链、有效期、域名       | 下发服务器证书链          | 校验失败即断链，不退明文  |
| 设备证书           | 从安全存储区取私钥签名后提交证书   | 校验证书链、注册状态与 SN 绑定 | 未注册或绑定不符则拒绝接入 |
| 密钥交换与 Finished | 派生会话密钥，校验 Finished | 同样派生并校验           | 校验失败即中止       |

为什么不用单向认证：单向认证只证明"服务器是真的"，不证明"连上来的是哪台设备"。任何持有合法服务器证书的冒充者都能与设备建立加密链路，而平台无法分辨接入的是现场那台网关还是一台复制出来的影子设备。双向认证把设备身份从"口令或密钥字符串"变成"证书加私钥"，密钥不落在明文配置文件里。

证书与设备 SN 的绑定：证书主体（CN/SAN）在出厂注册环节与设备唯一标识、产品型号绑定，一台设备一份证书，同型号不同 SN 不可互换。更换板卡必须重新注册，旧密钥立即吊销；同一密钥出现两地同时在线会直接拒绝并告警。

### 3.2 密码套件与国密

套件选择遵循"先禁用、再择优"。

| 类别   | 条目                                                      | 处理             |
|------|---------------------------------------------------------|----------------|
| 禁用协议 | SSLv3、TLS 1.0/1.1                                       | 全链路禁用          |
| 禁用套件 | NULL、EXPORT、匿名套件（无证书）、RC4、3DES 及弱 CBC 组合                | 全链路禁用          |
| 推荐套件 | ECDHE 前向保密 + AES-GCM 或 ChaCha20-Poly1305，摘要 SHA-256 及以上 | 默认优先           |
| 国密套件 | SM2 证书与密钥交换 + SM3 摘要 + SM4 对称加密                         | 已支持，可选套件，按项目启用 |

国密的适用场景与切换方式：适用于有商用密码合规要求的政企、能源、水务项目，或客户明确要求国密算法的场景。切换时在网关与平台两侧同时配置国密套件，设备侧不需要更换硬件；算力受限的终端是否启用按项目适配——SM2、SM4 的运算开销高于同等强度的 ECC 与 AES，建议在网关或带密码模块的终端上启用。

密钥长度与算法取舍：对称加密以 128 位（SM4、AES-128）覆盖多数场景，256 位用于长周期敏感数据；非对称加密中 ECC P-256 与 SM2 在安全强度上与 RSA-2048 及以上等效，但密钥更短、运算开销更小，更适合设备侧。国密与通用算法不在同一条链路上混用，避免套件协商被降级利用。

### 3.3 证书与密钥全生命周期

| 环节 | 内部 CA 签发                  | 客户自带 CA 签发                    |
|----|---------------------------|-------------------------------|
| 签发 | 平台 CA 签发设备证书，与 SN 绑定后写入设备 | 客户提供 CA 或中间 CA，按其规范生成 CSR     |
| 轮换 | 证书生命周期自动轮换，支持在线换发         | 周期与流程按客户 PKI 规范执行             |
| 吊销 | 平台侧吊销列表即时生效               | 客户提供 CRL 或 OCSP 端点，生效时效由客户侧决定 |

轮换触发条件：证书到期（到期前 30 天告警）、疑似泄露（私钥外泄、固件被篡改、设备被物理接管）、设备转让（所有权变更后重新注册）、算法与套件策略变更（例如由通用套件切至国密）。

吊销的取舍：CRL 实现简单、可离线分发，但列表体积随吊销量增长、刷新存在延迟；OCSP 实时性好，但要求设备在线且能访问响应器，弱网与内网隔离场景下容易失败。工程上采用短有效期、在线吊销与网关缓存三者组合：证书有效期越短，吊销窗口越小；网关缓存已下发的吊销状态，供子设备在离

线时查询。

离线设备的宽限期：长期离线设备无法及时获知吊销决定。设计上给出宽限期，期内允许设备继续本地采集与缓存，但限制其上行写入与控制类指令，网络恢复后优先完成证书校验与状态同步。宽限期时长按项目适配，与客户的风险容忍度共同确定。

3.4 工业协议场景的完整性

| 协议             | 原生安全性          | 我们的处理方式                                                                    | 边界                              |
|----------------|----------------|----------------------------------------------------------------------------|---------------------------------|
| MQTT / MQTTS   | 明文或 TLS        | MQTTS 强制开启，明文端口不作为生产接入                                                     | 设备无法改造时改由网关终结                   |
| Modbus RTU/TCP | 无加密、无认证、无完整性保护 | 网关侧终结，上行统一加密；寄存器白名单；写操作二次确认                                                | 网关到设备这一段仍是明文                    |
| OPC UA         | 内建安全模型         | 生产环境用 Basic256Sha256 + Sign&Encrypt，端口 4840，客户端证书由平台侧签发、有效期 1 年，到期前 30 天告警 | 物理隔离且无法升级的老设备才允许 None，且须在验收单上注明 |
| 串口 / 现场总线      | 无              | 视为可信物理域，边界收敛到网关机柜                                                          | 不承诺对已被物理接管的现场总线内部通信提供机密性        |
| ROS / ROS2     | 话题与服务默认不加密     | 经网关桥接至 MQTT/MQTTS 上行                                                       | 机器人本体内部总线安全由本体侧负责               |

不改设备的前提下，保护落在网关：Modbus 等协议本身没有加密能力，网关在协议侧终结后按点表映射，上行通过 MQTTS 加密。点表在进场前逐点核对，通信方式、寄存器地址、数据类型与字节序、只读还是可写、通信异常时的设备行为都写入点位表，可写点逐条确认后才进白名单。控制类指令（写寄存器、下发任务、执行回滚）默认关闭，需租户管理员审批后按角色开放，并记录在审计日志中。

3.5 防重放与指令可信

| 机制  | 作用            | 说明                |
|-----|---------------|-------------------|
| 时间戳 | 限定指令的有效窗口     | 超出窗口即拒绝，窗口长度按项目适配 |
| 随机数 | 保证单次有效，防止原样重放 | 每次会话独立生成          |
| 序列号 | 保证顺序、支撑去重     | 与缓存补传共用同一套序号      |

签名与二次确认：关键控制指令（合闸、下发策略、执行回滚）需携带签名，网关或终端验签通过后才执行；同时要求二次确认，下发与执行分两步，执行前由现场侧或管理员确认。对时方面，平台与设备通过 NTP 或平台侧授时对齐；长期离线设备存在时钟漂移，处置方式是以序列号为准、时间戳仅作参考，漂移超出阈值时把该批数据标记为待复核，而不是直接丢弃。

### 3.6 弱网与缓存补传的完整性

断网 72h 离线缓存：网关内置 SQLite 环形缓冲区，掉电不丢数，网络恢复后增量补传。

| 字段  | 作用                       |
|-----|--------------------------|
| 序号  | 全局单调递增，用于去重与顺序恢复         |
| 时间戳 | 记录采集时刻，供离线时钟漂移判断         |
| 校验值 | 采集时计算，读取与补传时复核，防止存储介质位翻转 |
| 签名  | 对批量数据签名，证明来源与未被篡改        |

补传时按序号去重，平台侧只接受未出现过的序号；顺序上按序号归并，允许乱序到达，但按采集时刻落库。断点续传以已确认序号为断点，续传完成后校验整体校验值；若不一致，回退到上一个已确认断点重传，不做部分采信。

### 3.7 明确边界与不承诺项

客户自建 CA 时，吊销链路的时效由客户侧决定，平台不承诺即时生效。

不承诺对已被物理接管的现场总线内部通信提供机密性；设备被拆解、探针接入后，串口与总线上的明文仍然存在。

无法启用 TLS 的老设备经网关接入时，网关到设备一段为明文，仅在边界收敛与点表白名单范围内可控。

离线宽限期内设备可继续采集与缓存，但不承诺此时控制类指令实时生效。

合规状态以公开口径为准：等保 2.0 三级测评推进中，ISO/IEC 27001 体系建设中，GDPR 就绪设计；国密 SM2/SM3/SM4 为已支持的可选套件。

能力标注沿用三态：已支持、按项目适配、规划中；本章未列出的能力项不视为已交付。

#### 本章要点

- 设备与平台双向持证，mTLS 之外不做降级；证书与 SN 一对一绑定，换板即重注册、旧密钥即吊销。

- 套件先禁用再择优：SSLv3、TLS 1.0/1.1、NULL 与 EXPORT 等弱项全链路禁用；国密 SM2/SM3/SM4 已支持，作为可选套件按项目启用。
- 证书生命周期覆盖签发、轮换、吊销与离线宽限；客户自带 CA 时，吊销时效由客户侧决定。
- Modbus 等无加密能力的老协议在网关侧终结，靠白名单与写操作二次确认兜住完整性；现场总线内部通信不在机密性承诺范围内。
- 离线 72h 数据以序号、校验、签名保证可信，补传按序号去重并按断点校验，不做部分采信。

## 第四章 平台与数据安全

本章说明平台在租户隔离、身份与权限、数据分级与驻留、生命周期、审计追溯与接口层面的口径。能力以「已支持 / 按项目适配 / 规划中」三态标注；服务水平相关量化承诺按合同附件约定，不给脱离合同的数字。

### 4.1 多租户隔离：租户边界画在哪里

平台以租户为最高隔离单元，边界覆盖四个平面。

**账号平面：**租户是账号体系根节点，用户、角色、组织树与登录策略在租户内定义，账号不可跨租户复用；运营与客户账号分属不同认证域。

**数据平面：**遥测、决策结论、业务元数据与审计日志写入时即携带租户标识，存储按租户分区或分库；查询由数据访问层统一注入租户过滤条件，业务代码不得自行拼接。

**设备平面：**设备接入时一机一密注册并绑定唯一租户，证书与租户标识关联；归属变更须审批并重新注册，历史数据不随设备迁移。

**消息平面：**MQTT 主题按租户划分命名空间，Broker 以 ACL 限制客户端仅能收发本租户主题；规则引擎、告警通道与出站 Webhook 目标同样限定在租户内。

| 隔离方式     | 实现方式            | 适用条件         |
|----------|-----------------|--------------|
| 逻辑隔离（默认） | 共享集群、租户标识分区、ACL | 多数项目，资源利用率高  |
| 资源池隔离    | 独立数据库实例或命名空间    | 客户有合规或性能隔离要求 |
| 物理隔离     | 专有实例、客户机房或私有云   | 强监管行业或合同约定   |

跨租户访问默认拒绝：跨租户的数据读取、设备控制与配置变更均被阻断。确需跨租户的场景须逐项审批：客户书面授权、明确数据范围与有效期、开通独立受托通道，留痕并纳入审计，到期自动回收。已支持。

### 4.2 身份、权限与最小特权

**人员账号：**可与企业身份源对接（LDAP / OIDC / 企业微信等，按项目适配）；强制口令复杂度与登录失败锁定；运维人员、平台运营人员及具备导出权限的角色强制启用 MFA（已支持）；普通操作员按项目策略开启。

**角色模型：**权限按「角色—资源—操作」三元组授予，遵循最小特权与职责分离。

| 角色      | 典型人员      | 可做什么              | 不可做什么            |
|---------|-----------|-------------------|------------------|
| 租户管理员   | 客户 IT 负责人 | 管理本租户用户、角色与配额     | 跨租户操作、查看平台运维日志   |
| 运维工程师   | 客户现场运维    | 查看设备状态、诊断、下发授权内指令 | 改账号与权限、导出全量数据    |
| 数据分析师   | 客户业务分析岗   | 查询导出授权内数据、建看板     | 下发控制指令、改设备配置     |
| 应用开发者   | 客户或集成方开发  | 创建管理 API 凭据、调试沙箱  | 访问生产原始遥测（除非单独授权） |
| 平台支持工程师 | 华芯智科技术支持  | 经授权在受控通道排障        | 无授权时不可见客户数据      |

**服务账号与密钥：**服务账号与人员账号分离，一服务一凭据；密钥由平台密钥管理服务托管，支持轮换与吊销，禁止明文写入代码或配置；泄露可按租户即时吊销。

**运维人员访问客户数据：**默认无客户数据访问权。需要介入时执行「申请—客户授权—限时开通—留痕—到期回收」流程，明确申请人、事由、工单号、数据范围与时段；授权以客户确认为前提，紧急故障按合同例外流程执行并补授权；会话记录操作人、时间、对象与动作，客户可在审计模块查询。已支持。

### 4.3 数据分级与驻留

数据分四级，默认位置、加密方式、保留期与访问范围如下，保留期以合同约定为准。



图 6 · 合规进度三态

| 数据分级    | 默认存储位置                 | 加密方式（传输中 / 静态）                    | 默认保留期               | 谁可访问               |
|---------|------------------------|-----------------------------------|---------------------|--------------------|
| 原始遥测    | 客户指定地域的时序库；「永不出厂」时不入平台 | MQTTS / HTTPS 强制，存储卷加密，可选 SM4 字段级 | 按项目合同约定             | 租户内被授权角色；平台运维默认不可见 |
| 决策结论    | 平台时序库（与遥测同地域）          | MQTTS / HTTPS 强制，存储卷加密            | 按项目合同约定             | 租户内全体授权用户          |
| 业务元数据   | 平台业务库（与租户同地域）          | HTTPS 强制，静态加密，敏感字段 SM4            | 随租户存续               | 租户管理员与对应角色         |
| 账号与审计日志 | 平台审计库（与租户同地域）          | HTTPS 强制，静态加密与哈希链                 | 按合同与合规要求，默认不少于 6 个月 | 租户管理员可查本租户；平台安全审计岗 |

传输层强制 MQTTS 与 HTTPS，禁用明文端口；国密 SM2/SM3/SM4 已支持，可按项目启用。

**客户指定存储地域：**租户创建时确定驻留地域，写入与备份路径绑定该地域，跨地域复制默认关闭；跨境传输须客户书面同意。已支持。

**「永不出厂」的平台侧强制点：**客户可选择端侧只回传决策结论（合格与不合格、异常等级、计数与时间戳），原始遥测在客户侧留存。强制点有三处：接入层拒绝该租户原始遥测主题的订阅与写入；存储层不落盘、不建索引；导出与开放 API 无对应数据可返回。已支持；确需回传原始数据的项目单独约定并写入合同。

4.4 数据生命周期

**保留期：**默认见上表，时长按项目合同约定；到期自动归档或删除并记入审计。

**备份与恢复：**执行定期全量与增量备份，备份加密存储，恢复演练按计划开展。RTO 与 RPO 的口径及取值按合同附件约定，本章不单独承诺。

**退租擦除：**退租后 30 日内完成彻底擦除并出具报告。

退租确认与冻结：客户确认退租，租户转只读并停止写入。

导出窗口：客户如需留存，冻结期内提供一次完整导出。

擦除执行：业务库、时序库、对象存储、缓存、消息队列与备份按序擦除，密钥作废。

出具凭证：《数据擦除报告》载明擦除范围、时间、执行人与校验方式。

客户确认归档：作为退租完成凭证留存。

## 4.5 审计与可追溯

审计日志覆盖：登录与登出（含失败尝试）、权限与角色变更、设备与平台配置变更、数据导出、指令下发、跨租户授权与运维受托访问、密钥操作、退租与擦除。

留存期按合同与合规要求设定，默认不少于 6 个月。防篡改改为只追加写入，关键字段以哈希链串联并定期校验；存储账号无删除权限。客户可在控制台自助查询并导出本租户记录。已支持。

## 4.6 应用与接口安全

**开放 API：**调用方须使用租户级凭据，凭据与角色权限绑定；按租户与凭据限流，超限返回错误码；调用纳入审计。

**越权测试：**发布前执行越权检查，覆盖 IDOR / BOLA（直接对象引用与对象级授权缺失）、横向越权（同租户跨用户）、纵向越权（低权限调用高权限接口）与批量接口的租户过滤遗漏，检查项纳入发布门禁，修复后放行；自助检查报告为规划中。

**文件上传与导出：**上传限制类型与大小并做内容校验，文件独立存储与扫描；导出须具备对应权限，记录导出人、范围与时间，大批量导出二次确认。

**第三方集成：**按最小授权发放独立凭据，限定数据范围与接口集合，可随时吊销、不得转授。

## 4.7 合规口径与责任边界

合规状态：等保 2.0 三级测评推进中；ISO/IEC 27001 体系建设中；GDPR 就绪设计；国密 SM2/SM3/SM4 已支持。上述状态不代表已取得认证结论，进展以正式证明文件为准。

边界如下。

客户自行导出的数据脱离平台管控后，存储、传输与使用安全由客户负责。

客户侧账号因弱口令、凭据外借或终端被控而失窃，平台不承担该情形责任，但提供登录异常检测与凭据吊销。

客户未按合同启用 MFA、未及时回收离职人员权限的后果，由客户承担。

客户在端侧自行留存处理的原始数据，安全由客户负责。

平台不就客户自行接入的第三方系统缺陷负责，仅对其接口调用提供凭据与审计管控。

超出约定范围的驻留与跨境需求，须客户书面确认后适配。

本章要点

- 租户边界覆盖账号、数据、设备、消息四个平面；跨租户访问默认拒绝，例外须书面授权、限期开通、全程留痕。
- 运维人员默认无客户数据访问权，介入须走「申请—客户授权—限时开通—留痕—回收」流程。
- 数据分四级，传输强制 MQTTS / HTTPS，静态加密与国密 SM2/SM3/SM4 按项目启用；原始遥测可设「永不出厂」，平台侧在接入、存储、导出三处阻断。
- 退租后 30 日内完成彻底擦除并出具《数据擦除报告》；保留期与 RTO / RPO 口径按合同附件约定。
- 审计日志只追加并以哈希链防篡改，覆盖登录、权限变更、配置变更、数据导出与指令下发，客户可自助查询。

第五章 合规进展、供应链可信与安全运营

本章写三件事：合规走到哪一步、物料与固件从哪里来、出问题怎么处理。口径与站内一致：我们不悬挂未取得的资质，以下为当前真实状态；证书编号与时限不预先撰写。

5.1 合规进度台账

台账用三态：**已取得**（可核验）、**进行中**（在做，给出目标季度，不写"即将通过"）、**不适用**（不做通用声明，按项目、按型号办理）。进行中条目的时间随机构排期调整，以书面确认为准。

| 条目                     | 三态  | 当前状态  | 说明                          | 下一步                         | 责任角色  |
|------------------------|-----|-------|-----------------------------|-----------------------------|-------|
| 网络安全等级保护 2.0 三级        | 进行中 | 测评推进中 | 测评尚未完成，不写「已通过」              | 计划 2027 Q1 完成测评与备案          | 安全负责人 |
| ISO/IEC 27001 信息安全管理体系 | 进行中 | 体系建设中 | 尚未接受认证审核                    | 计划 2027 Q2 完成认证审核；证书编号通过后公布 | 安全负责人 |
| GDPR 数据处理设计            | 进行中 | 就绪设计  | 面向出海客户场景，未承接欧盟个人数据业务前不做合规承诺 | 计划 2026 Q4 完成数据映射与数据处理协议模板  | 法务与安全 |

| 条目                           | 三态  | 当前状态 | 说明                                                  | 下一步         | 责任角色    |
|------------------------------|-----|------|-----------------------------------------------------|-------------|---------|
| 国密算法套件<br>SM2 / SM3 /<br>SM4 | 已取得 | 已支持  | 传输与签名链路已支持，可按项目启用；是平台能力，不是第三方认证证书                   | 随项目提供启用配置说明 | 平台研发负责人 |
| ICP 备案与公安联网备案                | 已取得 | 已备案  | 陕ICP备2026021314号-2、陕公网安备61010202000543号，页脚可跳转查询系统核对 | 信息变更时同步更新   | 法务与行政   |

台账每季度复核，状态变化当季更新；书面证明文件按项目在保密协议下提供。

## 5.2 供应链与物料可信

**元器件来源与替代料评审。** 按项目提供整机物料清单，标注关键器件的品牌、型号与第二供应来源。替代料导入前评审电气参数与封装、工作温度、停产风险、驱动适配与是否需重新认证，通过后先在样机与小批量产线验证再量产。客户如需限制特定品牌或物质，可在下单前提出。

**固件第三方组件。** 每个第三方组件登记组件名、版本、来源与许可证类型，按 SBOM 思路维护固件物料清单并随版本更新。许可证逐项确认与闭源分发的边界；其安全公告纳入统一漏洞台账，与自研代码同一路径。

**代工厂与产线的信息安全要求。** 代工厂签署保密与信息安全条款；工装（治具、烧录器、测试程序）按工单授权，烧录密钥不以明文落地，用完回收权限；测试数据（设备标识、测试日志、不良品图像）归项目所有，禁止外带；驻厂与远程支持按最小权限管理并留痕。

**来料检验与批次可追溯。** 关键器件按批次入库并保留来料检验记录，整机出厂带批次号；出现问题时回溯到来料批与生产工单，缩小排查范围。

## 5.3 安全开发流程

**需求阶段的安全评审。** 新需求进入开发前先过评审：数据分类（个人信息、客户工艺数据、视频原始流）、是否需要国密套件、是否涉及出海与跨境、是否引入第三方组件。评审输出安全需求条目，未通过不排期。

**代码评审与静态检查。** 合并前执行人工评审与静态检查；密钥不得硬编码，命中即阻断合并，凭据走密钥管理；对外接口的鉴权、限流与输入校验列为评审要点。

**依赖漏洞扫描。** 每次构建对依赖做已知漏洞比对并定期复扫，命中项建单，按 5.4 分级处理；许可证变更同步登记。

**发布前安全检查清单。** 逐条核查，结果与核查角色记入发布记录：

| 检查项              | 核查方式      |
|------------------|-----------|
| 默认口令已修改，调试口关闭    | 配置基线比对    |
| 安全启动与固件签名校验开启    | 启动日志核对    |
| 调试串口与 JTAG 关闭或加锁 | 实机连接验证    |
| 依赖扫描无未处置的高级别命中   | 扫描报告与工单   |
| 日志不含明文凭据与个人信息    | 抽样检查      |
| OTA 包签名与版本校验通过   | 签名验证与回滚演练 |
| 第三方组件与许可证清单已更新   | 清单比对      |
| 回滚包与回滚步骤就绪       | 回滚演练记录    |

**变更与回滚纪律。** 变更提交时须附回滚方案；平台侧灰度分批发布，固件侧保留可回退版本；记录与审批人留存，紧急变更事后补评审。

### 5.4 漏洞管理与渗透测试

**接收渠道。** 外部报告走站内联系入口与技术与商务邮箱，标题注明「安全漏洞」；内部来源含自测、代码扫描与客户反馈。收到后登记报告人、复现步骤与受影响版本。

**响应分级。** 分级只看两点：能否被远程利用，以及影响的是数据、设备还是业务连续性。时限**按合同附件约定**，本文不给通用小时数。

| 级别 | 判定                          | 响应路径                     | 时限      |
|----|-----------------------------|--------------------------|---------|
| P0 | 可远程未授权利用，或已造成客户数据泄露、设备被批量控制 | 通报安全负责人，启动应急响应（5.5），通知客户 | 按合同附件约定 |
| P1 | 可远程利用但需特定条件，或影响鉴权与签名链路      | 安全负责人牵头定修复计划，评估临时缓解      | 按合同附件约定 |
| P2 | 需本地权限或客户侧配置不当才能触发           | 排入常规修复版本，评估配置加固          | 按合同附件约定 |
| P3 | 低风险问题与加固建议                  | 记录归档，随版本处理               | 按合同附件约定 |

**修复与披露。** 修复走变更流程：修复、验证、回归，再发布修复版本并通知报告方与受影响客户。披露时间与报告方约定；涉及客户数据的内容以客户同意为前提。

**渗透测试。** 自测：大版本发布前测试设备接入、鉴权、升级链路与对外接口。第三方：按年度或按项目委托外部机构，范围与授权书提前书面确认。**报告可按项目提供**，在保密协议下交付，含测试范围、方法、发现项与修复验证结论。

## 5.5 应急响应

**事件分级。** 四级：Ⅰ级（客户数据泄露或大范围业务中断）、Ⅱ级（部分客户业务受影响或关键链路不可用）、Ⅲ级（单客户或有限设备受影响）、Ⅳ级（未造成实际影响的告警）。定级在事件确认后完成并留痕。

**处置流程。**

| 阶段 | 关键动作                 | 产出物       |
|----|----------------------|-----------|
| 发现 | 告警、客户反馈与外部报告统一登记     | 事件工单与时间线  |
| 定级 | 确认影响范围与数据性质          | 定级结论与响应名单 |
| 遏制 | 隔离受影响设备或节点，冻结凭据，阻断路径 | 遏制记录与影响边界 |
| 根因 | 复现分析，定位根因与受影响版本      | 根因分析记录    |
| 恢复 | 修复加固、分批恢复、验证无残留      | 恢复验证记录    |
| 复盘 | 复盘会议，整改项与责任人         | 事后报告      |

**客户通知与配合项。** 触发条件：确认事件涉及客户数据，或已影响客户业务运行。通知对象为合同约定联系人，内容包括已知事实、影响范围、已采取措施与客户配合项（隔离设备、更换凭据、提供日志）。事实未确认前先做初步通报并说明不确定性。节奏按合同附件约定。

**事后报告。** 包含时间线、影响范围与受影响设备或数据清单、根因分析、处置动作与遏制效果、数据影响判断依据、整改项与责任人、验证方式与复测结论。

## 5.6 边界与不承诺项

本文不构成合规证书、审计结论或法律意见，也不替代客户自身的合规判断与监管沟通。

等保 2.0 三级测评与 ISO/IEC 27001 认证仍在进行中；资质证书编号与测评结论在取得后公布，此前不提供编号，也不以「已通过」表述。

响应时限、通知时限与服务等级以合同附件约定为准，本文不给出通用小时数承诺。

不承诺对客户侧自建系统、自行部署环境与自有账号负责，包括弱口令、客户侧网络与主机配置、客户自建应用漏洞；责任边界在合同与交付文档中写明。

无线电型号核准、入网许可与物料合规声明（RoHS / REACH 类）按目标市场、型号、频段与项目逐项办理，本文不做通用声明。渗透测试报告、删除记录与固件物料清单按项目在保密协议下提供。

#### 本章要点

- 合规台账三态公开：等保 2.0 三级测评推进中、ISO/IEC 27001 体系建设中、GDPR 就绪设计、国密 SM2/SM3/SM4 已支持，逐条有下一步与责任角色。
- 供应链可信覆盖替代料评审、固件第三方组件清单（SBOM 思路）、代工厂工装与测试数据管控、批次可追溯。
- 发布前检查清单逐条可核查，变更必须带回滚方案；漏洞按 P0-P3 分级，时限按合同附件约定，测试报告可按项目提供。
- 应急响应按发现、定级、遏制、根因、恢复、复盘六步执行，通知与事后报告内容明确。