

T/JXEA

江西省工程师联合会团体标准

T/JXEA 372—2026

电子信息工程智能化系统设计规范

Design specification for intelligent system in electronic information engineering

（征求意见稿）

2026—XX—XX 发布

2026 - XX- XX 实施

目 次

前 言 II

引 言 III

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 智能化系统总体原则与架构要求 2

5 感知与数据采集子系统设计要求 2

6 传输网络与通信子系统设计要求 4

7 智能处理与控制平台要求 4

8 信息安全与网络防护要求 5

9 系统集成测试与验收 6

10 运行维护与管理 7

附 录 A 9

前 言

本文件依据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***提出。

本文件由***归口。

本文件起草单位：

本文件主要起草人：

引 言

随着人工智能、物联网、通信技术的深度融合，电子信息工程智能化系统已广泛应用于工业园区、智慧楼宇等多个领域，成为提升基础设施运行效率、保障安全、实现节能降耗的核心支撑。当前，智能化系统建设存在设计标准不统一、子系统兼容性差、安全防护薄弱等问题，影响系统稳定运行与功能发挥。为规范系统规划、设计、施工及运维全流程，统一技术要求与管理标准，保障系统建设质量与安全可靠运行，特制定本规范。本规范明确了系统架构、各子系统设计及验收运维等核心要求，为相关单位提供权威遵循，助力推动电子信息工程智能化行业规范化、高质量发展。

电子信息工程智能化系统设计规范

1 范围

本文件规定了电子信息工程智能化系统设计的总体原则与架构要求、感知与数据采集 subsystem 设计要求、传输网络与通信 subsystem 设计要求、智能处理与控制平台要求、信息安全与网络防护要求、系统集成测试与验收，以及运行维护与管理等内容。

本文件适用于工业园区、智慧楼宇、公共基础设施及政务服务等领域电子信息工程智能化系统的规划、设计、施工、验收和运行维护活动。综合布线系统、楼宇自动化控制系统、智能安防与视频监控系统、智慧照明与能源管理系统等各类 subsystem 的设计均适用本文件。其他电子信息工程项目可参照执行。

2 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 50057 建筑物防雷设计规范

GB 50348 安全防范工程技术标准

GB/T 14285 继电保护和安全自动装置技术规程

GB/T 20269 信息安全技术 信息系统安全管理要求

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 50311 综合布线系统工程设计规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

电子信息工程智能化系统 intelligent system for electronic information engineering

以计算机技术、通信技术、自动控制技术、传感技术为核心，融合人工智能算法，实现对建筑或基础设施各功能 subsystem 自动感知、智能处理、协同控制和信息共享的综合电子系统。

3.2

感知层 perception layer

智能化系统中负责采集物理世界信息的最底层，由各类传感器、执行器、射频识别（RFID）标签、摄像机等感知设备及其接口协议构成，是整个系统获取原始数据的基础。

[来源：GB/T 22239, 3.2]

3.3

网络层 network layer

智能化系统中负责感知数据传输的中间层，承担将感知层设备采集的数据可靠传输至平台层的职责，包括有线局域网（LAN）、工业以太网、PoE 供电网络、无线传感器网络（WSN）及 4G/5G 蜂窝网络等。

[来源：GB/T 22239, 3.3]

3.4

平台层 platform layer

智能化系统中负责数据汇聚、存储、计算分析和业务应用的核心层，通常由云计算平台、边缘计算节点、数据库集群和应用服务器组成，为上层应用提供统一的数据服务接口和智能分析能力。

3.5

信息安全等级保护 **classified security protection of information**

依据信息系统在国家安全、经济建设、社会生活中的重要程度及遭到破坏后的危害程度，将信息系统划分为不同安全等级，并实施相应级别安全保护措施的一种信息安全管理制度的。

[来源：GB/T 22239, 3.5]

3.6

边缘计算节点 **edge computing node**

部署在靠近感知设备侧（现场或接入层）的计算资源节点，具备数据预处理、协议转换、本地控制决策等功能，能够在网络不稳定或延迟敏感场景下实现低时延的本地智能处理，降低向云端传输的数据量。

4 智能化系统总体原则与架构要求

统一规划原则。电子信息工程智能化系统应在项目建设初期进行整体规划，统筹考虑各子系统的功能需求、技术路线、接口标准和扩展空间，避免各子系统独立建设形成“信息孤岛”。系统架构设计应预留不低于30%的系统容量冗余，以适应未来业务扩展需要。系统规划应同步考虑综合布线的路由预留，依据GB/T 50311进行综合布线工程的专项规划设计。

分层解耦原则。智能化系统应采用“感知层—网络层—平台层—应用层”的四层分层架构，各层之间通过标准化接口协议解耦，允许各层技术独立演进和替换，避免因底层设备更换导致上层应用的大规模改造。感知层设备宜采用支持MQTT、OPC-UA或Modbus等标准协议的产品，以确保设备级互操作性。

安全可信原则。智能化系统的信息安全设计应依据GB/T 22239的网络安全等级保护要求，根据系统承载业务的重要程度确定安全保护等级（二级及以上），从物理安全、网络安全、主机安全、应用安全和数据安全五个维度构建纵深防御体系。系统设计阶段应同步开展安全风险评估，识别主要威胁并制定相应的安全控制措施，形成安全需求规格说明书作为后续安全测评的基准文件。

可靠性原则。系统关键节点（核心交换机、中央管理服务器、UPS电源等）应采用冗余配置，确保系统整体可用性满足设计目标。对于安全防范类子系统，参考GB 50348的要求，视频监控核心设备的平均无故障时间（MTBF）应不低于30000 h；核心数据存储设备宜采用RAID-5及以上级别的磁盘冗余方案；消防联动、应急广播等涉及人身安全的子系统还应配置独立的不间断电源（UPS），在市电断电后维持正常运行时间不少于30 min。

绿色节能原则。智能化系统设计应充分考虑建筑能源管理需求，通过智能照明调节、空调联动优化、能耗数据实时监测等功能降低建筑整体能耗。系统能耗数据采集应覆盖主要用能设备，采样周期不大于15 min，数据存储周期不少于1年，以支持能源审计和节能改造决策。楼宇自动化系统的设计应符合公共建筑节能设计标准的相关规定，照明控制回路宜与人员感知传感器联动。

标准开放原则。系统集成宜采用国家或行业标准接口协议，优先选择支持RESTful API、WebSocket等开放式接口标准的平台产品，避免采用私有封闭接口导致系统长期被单一厂商锁定。对外数据共享接口应实施身份认证和访问授权控制，防止数据泄露或未授权访问。

智能化系统设计的技术依据主要包括：

- a) 现行国家标准：GB/T 50311、GB 50348、GB/T 22239、GB 50057、GB/T 20269、GB/T 14285；
- b) 行业技术标准：建设项目所在地适用的地方性智能化工程建设规范及行业主管部门发布的技术要求；
- c) 建设方需求文件：业主方提出的功能需求书、性能指标要求及项目建设标准；
- d) 设计文件体系：系统总体设计方案、各子系统深化设计图纸、综合布线系统图及设备选型清单。

5 感知与数据采集子系统设计要求

5.1 传感器与终端设备选型原则

智能化系统中各类传感器和感知终端设备的选型应符合以下基本要求：

- a) 传感器精度等级应依据应用场景确定，环境监测类传感器（温湿度、CO₂、PM2.5等）精度应满足建筑环境测量的行业要求；工业过程控制类传感器精度应不低于量程的0.5%；
- b) 室外安装的传感器和摄像机防护等级应不低于IP66，依据GB 50348对应场景的环境要求选取，沿海或化工区域安装时还应选用具备防盐雾和防腐蚀能力的型号；
- c) 视频监控摄像机应依据监控区域特征选型，出入口控制摄像机宜选用支持人脸识别的高清摄像机（分辨率不低于1080P），停车场监控宜选用支持车牌识别的低照度摄像机，重要区域宜选用支持热成像或星光级夜视的摄像机；
- d) 感知终端设备应优先选用具备国家相关认证（如3C认证、无线电型号核准等）且支持主流通信协议（Zigbee、Z-Wave、Wi-Fi 6、LoRa等）的产品，以确保感知层的互操作性和可维护性；
- e) 用于安全防范的入侵探测器、门禁读卡器等安全级感知设备，应符合GB 50348关于主要设备技术要求的规定，并由具备相应资质的产品供应商提供。

5.2 视频监控系统设计

视频监控系统应依据GB 50348进行整体设计，系统设计方案应包含监控点位布置图、存储容量计算书和网络带宽评估报告。主要设计要求如下：

点位布置：覆盖项目主要出入口、公共通道、停车场、重要功能区域及设备机房；摄像机安装高度应确保人脸有效采集（距地2.5 m~4 m，仰角不超过15°）；室内走廊摄像机间距应保证监控无盲区，相邻摄像机视野应有不少于5%的画面重叠。

录像存储：视频录像资料的保存时间应满足GB 50348的最低要求（重要场所不少于30天），存储设备应采用NVR网络录像机或集中式IP-SAN存储系统；存储容量应按照“摄像机路数×码率×录像天数×保险系数（1.1）”公式计算，高清摄像机单路码流宜按4 Mbit/s估算；重要系统应配置热备存储以防止单点故障导致录像丢失。

网络传输：视频监控专网应与办公管理网络物理隔离或通过防火墙逻辑隔离；监控专网交换机应支持PoE供电（符合IEEE 802.3af/at标准），每个PoE端口供电功率应依据终端设备功耗留有不低于20%的余量；骨干网络链路应采用光纤连接，带宽应满足峰值并发视频流的传输需求并预留50%余量。

智能分析：视频监控平台宜集成人员越界报警、遗留物检测、人员聚集预警等视频智能分析功能；智能分析算法误报率应不高于5%，漏报率应不高于3%（以系统验收测试结果为准）；人脸识别比对准准确率不应低于98%（标准光照、正面角度下）。

设备供电与防雷：室外摄像机及相关控制设备应依据GB 50057做好防雷接地设计，信号线路和电源线路均应安装相应防雷器（SPD）；安防系统设备应由专用UPS供电，UPS额定功率应按所有接入设备满载功耗总和乘以1.25的系数配置。

5.3 门禁与出入口控制系统设计

门禁与出入口控制系统设计应遵循GB 50348的相关规定，系统拓扑应采用前端控制器加中央管理服务器的分布式架构，主要技术要求如下：

门禁控制器的处理能力：单台门禁控制器最大管理的门数不应超过其设计额定容量的80%；控制器应具备离线运行能力，在与服务器断开通信后仍能独立执行已下载的通行权限和时间表，离线模式下的存储记录容量应不少于10000条；

身份识别技术：出入口识别方式宜采用多因素认证（如IC卡+密码、人脸识别+IC卡等），重要区域（机房、财务室等）应采用双因素及以上认证；读卡器应支持13.56 MHz的ISO 14443标准，密码键盘应具备防窥设计；人脸识别模块的活体检测性能应满足金融级以上安全要求；

联动功能：门禁系统应与视频监控系统、入侵报警系统、消防系统实现联动，报警触发后应自动关联调取对应区域摄像机实时画面；消防报警信号触发后门禁控制器应自动切换为疏散模式，解锁疏散通道上的电磁锁，以保障人员安全疏散；

数据安全与审计：门禁系统服务器应与中央管理平台连接，所有刷卡记录、报警记录和操作日志应实时上传并按GB/T 20269的要求进行安全存储，记录保存期限不少于6个月；敏感权限变更应进行双人复核制度，形成不可篡改的操作审计日志。

5.4 环境与能耗数据采集设计

建筑环境及能耗数据采集系统（含温湿度、CO₂、照度、PM2.5、电能、水耗等）的设计应符合以下要求：

- a) 采集点位布置应覆盖各楼层主要功能区域、机电设备机房及配电间；室内环境传感器应避免安装在空调出风口正下方、直射阳光照射处及门窗附近等干扰位置；能耗采集电能表应具备通信接口（RS-485 Modbus或以太网），支持有功功率、无功功率、电能累计值和电流电压的实时读取；
- b) 环境传感器通信协议宜统一采用Zigbee Pro或RS-485 Modbus协议，以便接入统一的楼宇自动化系统（BAS）；采集网关设备应具备数据本地缓存能力，网络中断时缓存数据量不少于24 h，网络恢复后自动上传缺失数据；
- c) 能耗数据应分项计量（照明用电、动力用电、空调用电、特殊用电分项独立计量），支持按日、周、月和年度生成能耗报告；能耗异常分析功能应能自动识别高于历史同期30%的用能异常并推送告警；
- d) 所有采集数据应统一汇入智能化系统平台层数据库，时序数据采用专用时序数据库（如InfluxDB）存储，保存周期不少于3年；历史数据应支持图表化趋势展示和数据导出功能，以满足能源审计需求。

6 传输网络与通信子系统设计要求

智能化系统的传输网络设计应以GB/T 50311综合布线系统工程设计规范为基础，同时满足以下各子系统的差异化传输需求，形成统一的网络基础设施：

综合布线规划：水平子系统宜采用超六类（Cat 6A）非屏蔽双绞线或6类屏蔽双绞线，最大水平布线长度不超过90 m，并应在设计文件中说明每条链路的余量（链路损耗余量应不小于3 dB）；垂直主干子系统应依据系统容量采用光纤（宜选用OM4及以上级别多模光纤）；综合布线管线路由应避开强电线路，与强电桥架平行敷设时最小间距不应小于0.3 m，依据GB/T 50311的相关规定执行。

网络安全区域划分：智能化系统网络应依据承载业务的安全级别划分不同安全域（感知接入域、运营管理域、核心数据域等），各域之间通过防火墙或具备访问控制功能的交换机实现逻辑隔离；互联网出口处应部署防火墙、入侵防御系统（IPS）和上网行为管理设备；无线网络覆盖应独立规划AP部署方案，访客无线网络应与内网严格隔离。

带宽规划：网络带宽规划应基于各子系统并发数据量计算，视频监控为带宽消耗最大的子系统，应按最大并发路数计算接入层和汇聚层带宽；物联网设备（传感器、门禁、能耗采集等）的并发数据量较小，但数量众多，宜单独规划接入子网并通过边缘计算网关进行数据汇聚，降低核心网络压力。

时钟同步：时间敏感型应用（门禁记录、视频录像时间戳、能耗计量等）所依赖的设备应通过NTP协议（GB/T 14285对时序准确性有相关要求）与系统时钟服务器同步，时钟同步精度应优于100 ms；系统时钟服务器宜通过GPS或北斗卫星授时与标准时间同步，确保各子系统时间一致性。

无线通信规划：室内无线覆盖应依据楼层平面布局规划Wi-Fi AP点位，信号覆盖区域接收信号强度（RSSI）应不低于-70 dBm，相邻AP之间信道应交错分配（2.4 GHz频段采用1/6/11信道交错），避免同频干扰；对于地下停车场、机房等特殊区域应进行现场勘测并采用定向天线或泄漏电缆方案保障覆盖效果。

通信设备的防雷接地：所有网络设备机柜及机架应可靠接地，接地电阻应依据GB 50057的规定满足电子设备机房接地要求（通常不大于1 Ω），信号线路入楼处应安装信号线路浪涌保护器。

7 智能处理与控制平台要求

7.1 集成管理平台基本要求

电子信息工程智能化系统应部署统一的集成管理平台（IMS），实现各子系统的信息汇聚、统一展示、跨系统联动控制和综合数据分析。集成管理平台的基本功能要求如下：

统一数据接入：平台应支持主流工业协议（Modbus TCP/RTU、BACnet/IP、OPC-UA、MQTT等）的设备数据接入，支持同时接入不少于50个不同品牌子系统；新增子系统或设备类型时无需修改平台核心代码，通过配置或插件方式完成适配，确保平台的可扩展性；数据接入延迟应不超过1 s（设备状态数据）。

可视化展示：平台宜提供基于BIM（建筑信息模型）或二维GIS地图的三维可视化界面，支持各子系统的空间定位展示；告警事件应在地图/模型上以不同颜色标注并自动弹出处置工单；平台应支持多屏显示，大屏展示模式应具备态势感知和实时汇总功能。

7.2 边缘计算与本地控制要求

对于时延敏感型控制场景（如消防联动、入侵报警响应等），系统应部署边缘计算节点实现本地闭环控制，边缘节点的主要技术要求如下：

实时响应：边缘计算节点从接收到报警触发信号到完成联动控制指令的端到端时延应不超过200 ms；本地控制逻辑应固化为标准化的联动场景脚本，并在边缘节点本地存储，网络断线期间仍可正常执行预设联动动作；

可靠性设计：边缘计算节点应具备软件看门狗和硬件看门狗双重保障，发生软件异常时应在30 s内自动重启并恢复控制功能；边缘节点操作系统宜采用实时操作系统（RTOS）或经过加固的Linux，禁止安装与控制功能无关的应用软件；

数据同步：边缘节点应与云端平台保持增量数据实时同步，同步延迟应不超过5 s；在离线状态下，边缘节点应本地缓存控制记录、报警记录和传感器数据（缓存容量应支持至少72 h的数据），待恢复联网后自动上传补传，确保数据不丢失。

7.3 数据存储与分析要求

集成管理平台的数据存储与分析功能应满足以下规定：

数据库架构：关系型数据（设备台账、人员权限、系统配置等）应采用关系数据库（MySQL或等效产品）存储；时序型数据（传感器采集数据、能耗数据等）应采用时序数据库存储；视频录像和图片等非结构化数据应采用对象存储；不同类型数据库应统一纳入平台数据管理层，提供标准化数据访问接口。

数据安全：平台数据库应满足GB/T 22239等级保护二级以上要求；重要数据（权限数据、审计日志、告警记录）应加密存储；数据库管理账号应分级设置权限，禁止使用默认密码；数据库操作日志应完整记录并保存不少于6个月；生产数据库应每日进行增量备份、每周进行全量备份，备份数据应异地存储。

智能分析：平台应具备以下智能分析功能：人员异常行为分析（人员滞留、徘徊、周界入侵）；设备状态预测性维护（基于历史运行数据预测设备故障时间）；能耗优化建议（基于室外气象数据和室内环境数据自动优化空调和照明控制策略）。智能分析模型应支持在线更新，更新操作须经过测试验证后方可部署至生产环境。

告警管理：平台告警应依据严重程度分级（紧急/重要/一般/提示四级），不同级别告警应通过不同渠道通知（大屏弹窗、短信、App推送等）相关责任人；告警处置应流程化管理，每条告警记录应包含告警时间、处置人员、处置措施和关闭时间，告警处置响应时间应在SLA中明确约定。

系统对接：平台应提供标准化RESTful API供第三方系统调用，API文档应随系统版本同步更新；对外接口应实施OAuth 2.0或等效的访问令牌认证机制，所有API调用应记录访问日志，防止接口被滥用；平台应支持向上级主管部门或城市级智慧平台输出标准化数据，接口格式应符合相关行业数据交换规范。

8 信息安全与网络防护要求

8.1 安全等级保护建设要求

电子信息工程智能化系统的信息安全建设应依据GB/T 22239的规定，在系统上线前完成安全等级保护定级、备案和建设整改工作，满足相应级别的安全保护能力要求：

安全等级保护建设内容主要包括：

- a) 物理与环境安全：服务器机房应满足GB/T 22239二级（或更高）物理安全要求，包括门禁管控、视频监控（24 h录像保存不少于90天）、防雷、防火、防水、温湿度控制（温度18℃～27℃，相对湿度40%～70%）及电磁屏蔽等；
- b) 网络与通信安全：互联网出口应部署防火墙（访问控制策略应遵循最小权限原则）、入侵检测/防御系统（IDS/IPS）；内部网络应进行VLAN划分，不同安全域之间的访问应经过访问控

制设备审查；重要网络设备（核心交换机、防火墙）管理通道应采用SSH加密，禁止使用Telnet明文管理；

- c) 主机与应用安全：服务器操作系统应及时安装安全补丁，关闭非必要端口和服务；应用系统应进行输入验证、SQL注入防护和跨站脚本（XSS）防护；应用层应部署Web应用防火墙（WAF）。

8.2 密码技术应用要求

智能化系统中密码技术的应用应符合国家密码管理相关规定，主要技术要求如下：

数据传输加密：系统管理平台与前端设备之间的控制指令传输，以及平台与用户终端之间的Web访问，应采用TLS 1.2及以上版本加密传输；不应使用已知存在安全漏洞的SSL 3.0、TLS 1.0等旧版本协议；移动App与服务端通信应采用HTTPS，并实施证书绑定（Certificate Pinning）防止中间人攻击。

身份认证：系统管理员账号应实施多因素认证（MFA），认证因素应至少包含密码和动态口令（TOTP）或生物特征中的一种；账号密码应满足复杂度要求（长度不少于8位，包含大小写字母、数字和特殊字符），密码有效期不超过90天；连续输入错误密码5次后账号应自动锁定，需管理员手动解锁。

访问控制：系统应实施基于角色的访问控制（RBAC），不同岗位人员仅能访问其工作所需的最小权限；特权操作（权限变更、系统配置修改等）应进行二次确认并留有操作审计日志；依据GB/T 20269的规定，访问控制策略应形成文件并定期审查。

安全审计：系统应对所有用户登录、权限变更、重要配置修改、告警处置等操作进行完整审计记录；审计日志应独立存储，防止被系统管理员删除；审计日志保存周期不少于6个月；系统应配置统一的安全信息与事件管理平台（SIEM），对审计日志进行自动化分析，识别异常访问行为并触发告警。

安全漏洞管理：系统上线前应委托具备资质的第三方机构进行渗透测试和安全评估；系统运行期间应定期（建议不超过每6个月）进行漏洞扫描；发现高危漏洞应在48 h内完成补丁评估，10个工作日内完成修复或采取临时缓解措施并记录处置过程。

9 系统集成测试与验收

9.1 系统集成测试要求

电子信息工程智能化系统在竣工验收前应完成系统集成测试，测试应覆盖以下内容，测试结果应形成书面测试报告，作为验收的技术依据：

- a) 子系统功能测试：对每个子系统（视频监控、门禁、入侵报警、楼宇自动化、能耗监测等）分别进行功能符合性测试，验证功能实现与设计文件的一致性，每项功能测试应记录测试步骤、预期结果和实际结果，通过率应达到100%方可进入联调测试；
- b) 子系统联动测试：模拟各类触发场景（如消防报警触发门禁疏散、入侵报警联动摄像机预置位等），验证跨子系统联动的正确性和响应时间；联动响应时间应满足设计文件规定的指标，且测试次数不少于3次，每次测试均应达标；
- c) 性能与负载测试：模拟系统在设计最大并发用户数和最大数据吞吐量条件下的运行状态，验证系统资源占用率（CPU使用率应不超过70%，内存使用率应不超过80%）和响应时间指标；视频实时预览延迟应不超过2 s，设备状态刷新延迟应不超过3 s。

9.2 安全测试要求

系统竣工验收前应对信息安全进行专项测试，安全测试应委托具有CNAS资质认可的信息安全测评机构承担，主要测试内容包括：

漏洞扫描：对系统所有服务器、网络设备和应用系统进行自动化漏洞扫描，发现的高危漏洞应在验收前完成修复；中危漏洞应制定整改计划，原则上在系统上线后1个月内完成整改；

渗透测试：对系统互联网暴露面（如远程访问接口、移动App）进行黑盒渗透测试，模拟外部攻击者视角验证系统安全边界的有效性；渗透测试报告应明确测试范围、发现的安全问题及修复建议，所有高危和中危渗透测试发现均应在验收前完成整改；

等级测评：按照GB/T 22239的要求，委托具备等级测评资质的测评机构对系统进行等级保护测评，测评结论应为“符合”方可通过安全验收，测评存在不符合项时应按测评报告完成整改后重新测评。

9.3 竣工验收程序

系统竣工验收应按照以下程序组织实施，验收资料应完整归档：

- a) 预验收：由施工单位自行组织，对照设计文件和合同技术要求逐项检查，形成预验收报告并提交建设单位，预验收发现的问题应在正式验收前完成整改；
- b) 正式验收：建设单位组织设计单位、监理单位、施工单位及最终用户代表共同参与；验收组成员应对系统功能、性能指标、文档资料、培训记录逐项验收；验收结论分为“通过”“有条件通过”和“不通过”；
- c) 竣工资料移交：验收通过后，施工单位应向建设单位移交完整的竣工资料，包括竣工图纸、设备清单（含序列号）、系统配置文件备份、软件安装包及授权证书、操作维护手册、培训资料及验收测试报告；
- d) 系统档案建立：建设单位应依据移交的竣工资料建立智能化系统电子档案，档案应覆盖系统全生命周期，包含规划设计文件、施工过程记录、验收报告、日常维护记录和系统变更记录，档案保存期限应不少于系统使用年限。

用户接受测试（UAT）：最终用户应在系统正式上线前完成用户接受测试，验证系统操作流程的易用性和业务功能的完整性；UAT测试用例应由用户方自行设计，测试结果填入本规范附录A规定的验收记录表，并由用户代表和系统集成商代表双方签字确认；验收合格后，系统集成商应向用户方移交系统管理员账号和全套技术文档。

10 运行维护与管理

10.1 运行维护组织要求

电子信息工程智能化系统运行维护应建立专职或兼职的运维团队，运维人员应满足以下要求：

- a) 运维人员技能：系统管理员应熟悉所管理子系统的操作规程，掌握基本网络排查技能（使用ping、tracert等工具进行网络故障初步判断），了解信息安全基础知识；涉及安防系统的运维人员宜取得GB 50348相关的安防系统施工维保资质；
- b) 运维制度：应建立覆盖日常巡检、定期保养、故障响应、变更管理和应急预案的完整运维管理制度；运维工作应留有完整的操作记录（含巡检记录、维修记录、配置变更记录），记录应至少保存2年；
- c) 运维外包管理：当部分运维工作委托第三方服务商承担时，应签订服务级别协议（SLA），明确故障响应时间（高优先级故障4 h内响应，24 h内解决；一般故障8 h内响应，48 h内解决）、定期保养频次和数据保密要求；运维服务商操作人员的账号权限应单独管理，离场后应及时撤销。
- d) 应急预案：应针对主要故障场景（核心交换机故障、服务器宕机、视频监控全面断线、安防系统主机故障等）制定专项应急处置预案，预案应明确故障判断步骤、临时替代措施和恢复流程；应急预案应至少每年演练一次并根据演练结果修订完善。

10.2 日常巡检与定期保养

智能化系统的运行维护应制定年度保养计划，维护内容及周期如下：

日常巡检（每天）：查看集成管理平台告警信息，对新产生的未处置告警进行确认和处置；检查视频监控系统各摄像机实时画面是否正常（无遮挡、无黑屏、无画面冻结）；确认机房环境温湿度在规定范围内；巡检记录应录入系统运维管理模块，异常情况应在24 h内形成处置报告。

月度保养（每月）：检查网络核心设备（核心交换机、路由器、防火墙）运行状态和日志告警；清理服务器机柜灰尘，检查UPS电池健康状态（放电测试）；核查系统安全补丁更新情况，对尚未修复的已知漏洞进行风险评估；月度保养完成后出具月度运维报告，提交建设单位存档。

季度保养（每季度）：对门禁、入侵报警系统进行功能性测试（模拟报警触发，验证联动效果）；对视频监控存储系统进行存储空间核查和录像资料抽查；对综合布线系统进行抽检测试（随机抽测不少于5%的链路），依据GB/T 50311的验收指标核查链路性能是否仍满足要求。

10.3 系统变更与版本管理

智能化系统在运行期间的变更（包括软件升级、配置修改、设备替换等）应遵循以下变更管理规范：

- a) 变更申请：任何变更应提前提交书面变更申请，说明变更内容、变更原因、影响范围评估和回退方案；变更申请须经系统管理员和建设单位负责人审批后方可实施；涉及信息安全配置的变更应同时通知安全管理员进行安全影响评估；
- b) 变更实施：变更应在非业务高峰期执行，实施前应对关键配置进行备份；变更实施过程应有技术人员全程在场并实时监控系统状态；变更完成后应进行功能验证测试，测试通过后方可关闭变更任务；
- c) 版本管理：系统软件和配置文件应纳入版本控制管理，每次变更后应更新版本记录；版本记录应包含版本号、变更日期、变更内容摘要和变更人员；历史版本的配置文件应保留不少于3个历史版本，以便在变更失败时快速回退。
- d) 变更归档：变更完成后应将变更申请单、审批记录、实施记录、测试报告一并归入系统档案；重大变更（系统架构调整、核心设备更换等）应及时更新系统竣工图纸和技术文档，确保档案记录与系统实际状态保持一致。

10.4 故障处置与应急响应

系统运行期间发生故障时，运维人员应参照故障处置手册按照以下规范进行响应，重大故障应启动应急响应程序：

故障分级响应：依据故障影响范围和业务影响程度，将故障分为一级（全系统瘫痪或重要安防系统失效）、二级（主要功能模块故障或多个子系统受影响）和三级（单个设备或功能点故障）；一级故障应立即启动应急预案，30 min内通知相关责任人，2 h内提出临时解决方案；二级故障4 h内响应，24 h内解决；三级故障48 h内解决，不影响系统整体运行。

故障记录与分析：每次故障处置完成后应填写故障处置报告，内容包括故障发生时间、影响范围、故障根本原因分析（RCA）、处置措施、恢复时间及预防复发的改进建议；对于重复性故障应特别关注根本原因，制定针对性改进措施并跟踪落实；故障数据应纳入月度运维报告统计分析，持续改善系统可靠性。服务商应对变更造成的故障承担责任，并及时协助系统恢复，相关记录应归入系统档案。

附 录 A
(规范性)
电子信息工程智能化系统验收检查记录表

表A.1 电子信息工程智能化系统验收检查记录表

验收类别	检验项目	检验内容与判定标准	备注
A 综合布线与网络	A1 布线系统	水平链路测试 (Cat 6A) : 插入损耗: <input type="checkbox"/> 合格 <input type="checkbox"/> 不合格 近端串扰 (NEXT) : <input type="checkbox"/> 合格 <input type="checkbox"/> 不合格 回波损耗 (RL) : <input type="checkbox"/> 合格 <input type="checkbox"/> 不合格 抽测比例: _____% 不合格点数: _____ 综合布线验收结论: <input type="checkbox"/> 合格 <input type="checkbox"/> 不合格	依据GB/T 50311
	A2 网络设备	核心交换机状态: <input type="checkbox"/> 正常 <input type="checkbox"/> 异常 VLAN划分正确性: <input type="checkbox"/> 已验证 <input type="checkbox"/> 有偏差 防火墙策略: <input type="checkbox"/> 已配置 <input type="checkbox"/> 未配置 带宽压力测试: 核心链路利用率_____ % 网络验收结论: <input type="checkbox"/> 合格 <input type="checkbox"/> 不合格	记录设备型号和序列号
B 视频监控系统	B1 摄像机与录像	在线摄像机数量: _____路 离线: _____路 图像质量 (随机抽查10路) : <input type="checkbox"/> 全部合格 <input type="checkbox"/> _____路不合格 录像存储正常: <input type="checkbox"/> 是 <input type="checkbox"/> 否 录像保存天数: _____天 (要求≥30天) 视频系统结论: <input type="checkbox"/> 合格 <input type="checkbox"/> 不合格	依据GB 50348
	B2 视频智能分析	越界报警测试 (各区域各测1次) : <input type="checkbox"/> 全部触发 <input type="checkbox"/> _____处未触发 人脸识别准确率测试 (100次) : _____% (要求≥98%) 误报率测试: _____% (要求≤5%) 智能分析结论: <input type="checkbox"/> 合格 <input type="checkbox"/> 不合格	记录测试样本数量
C 门禁与安防	C1 门禁系统	门禁点总数: _____ 在线: _____ 离线: _____ 刷卡响应时间 (抽测5处) : _____ms (要求≤500ms) 离线模式功能验证: <input type="checkbox"/> 合格 <input type="checkbox"/> 不合格 与消防联动解锁测试: <input type="checkbox"/> 合格 <input type="checkbox"/> 不合格 门禁系统结论: <input type="checkbox"/> 合格 <input type="checkbox"/> 不合格	依据GB 50348
	C2 入侵报警	探测器在线率: _____% (要求100%) 触发报警响应时间: _____s (要求≤30s) 防破坏报警测试: <input type="checkbox"/> 合格 <input type="checkbox"/> 不合格 报警联动摄像机: <input type="checkbox"/> 合格 <input type="checkbox"/> 不合格 报警系统结论: <input type="checkbox"/> 合格 <input type="checkbox"/> 不合格	记录报警处置流程
D 信息安全	D1 等级保护	GB/T 22239保护等级: _____级 等保测评机构: _____ 测评时间: _____年____月____ 测评结论: <input type="checkbox"/> 符合 <input type="checkbox"/> 基本符合 <input type="checkbox"/> 不符合 不符合项整改完成: <input type="checkbox"/> 是 <input type="checkbox"/> 否	附测评报告
	D2 安全配置	默认密码修改: <input type="checkbox"/> 已全部修改 <input type="checkbox"/> 存在未修改 账号权限审查: <input type="checkbox"/> 合格 <input type="checkbox"/> 需整改 高危漏洞修复: <input type="checkbox"/> 已全部修复 <input type="checkbox"/> 存在_____个未修复 数据加密传输 (HTTPS) : <input type="checkbox"/> 已启用 <input type="checkbox"/> 未启用 安全配置结论: <input type="checkbox"/> 合格 <input type="checkbox"/> 不合格	依据GB/T 20269
E 防雷与接地	E1 防雷接地	机房等电位接地电阻: _____Ω (要求≤1Ω) 室外设备防雷器安装: <input type="checkbox"/> 全部安装 <input type="checkbox"/> 缺_____处 信号线SPD: <input type="checkbox"/> 已安装 <input type="checkbox"/> 未安装 防雷验收结论: <input type="checkbox"/> 合格 <input type="checkbox"/> 不合格	依据GB 50057
F 集成平台	F1 平台功能	子系统接入数量: _____个 (设计数量: _____) 设备在线率: _____% (要求≥98%) 平台响应时间 (设备状态) : _____s (要求≤3s) BIM/地图可视化: <input type="checkbox"/> 正常 <input type="checkbox"/> 异常 平台功能结论: <input type="checkbox"/> 合格 <input type="checkbox"/> 不合格	记录平台版本号

验收类别	检验项目	检验内容与判定标准	备注
	F2 综合验收	竣工资料完整性: <input type="checkbox"/> 完整 <input type="checkbox"/> 缺__项 操作培训完成: <input type="checkbox"/> 已完成 <input type="checkbox"/> 未完成 系统档案建立: <input type="checkbox"/> 已建立 <input type="checkbox"/> 未建立 综合验收结论: <input type="checkbox"/> 通过 <input type="checkbox"/> 有条件通过 <input type="checkbox"/> 不通过 验收日期: ____年____月____日	归档期限≥系统使用年限
	F2 签字存档	制造商代表签字: _____ 用户方代表签字: _____ 检验日期: ____年____月____日 归档编号: _____	档案保存期限≥5年

注: 本表适用于电子信息工程智能化系统竣工验收、阶段性验收及年度巡检, 由检验人员逐项填写, 所有项目检验合格后由建设单位和施工单位代表双方签字确认, 作为系统档案的重要组成部分归档保存。