

广州北江引水工程（花都水厂及配水管道 工程部分）施工总承包（标段二）

技术需求书

智能化系统工程分册

招标人：广州市花都自来水有限公司

编制人：广东省建筑设计研究院有限公司

2023 年 10 月

一、用户需求书	1
二、技术规格书	9
1 综合布线系统	10
1.1 系统概况及架构	10
1.2 设计界面	10
1.3 系统总体技术要求	10
1.4 主要设备技术参数要求	11
2 信息网络系统	15
2.1 系统概况	15
2.2 系统构成	15
2.3 系统总体技术要求	15
2.4 主要设备技术参数要求	15
3 统一时钟系统	46
3.1 系统概述	46
3.2 系统结构及功能要求	46
3.3 主要设备技术要求	46
4 公共广播系统	48
4.1 系统概述	48
4.2 系统结构及功能要求	48
4.3 系统总体技术要求	48
4.4 主要设备技术要求	49
5 安防集成应用综合管理（平台）系统	51
5.1 系统概况	51
5.2 视频安防监控系统模块	51
5.2.1 系统概况	51
5.2.2 系统构成	51
5.2.3 系统总体技术要求	51
5.2.4 主要设备技术参数要求	52
5.3 出入口控制系统模块	63
5.3.1 系统概况及构成	63
5.3.2 系统基本要求	63
5.3.3 主要设备基本技术要求	64

一、用户需求书

1 工程概况

花都水厂选址定于狮岭镇集贤村北面，芙蓉嶂水库以东，山前旅游大道北侧，总占地面积约 650 亩。花都水厂首期设计规模为 48 万 m^3/d ，首期占地面积为 407 亩，远期设计规模为 100 万 m^3/d 。应急备用取水泵房选址定于芙蓉嶂水库主坝东侧的山坡边，距离大坝东侧约 160 米。项目主要建设内容与规模如下：花都水厂：总设计规模为 100 万 m^3/d ，首期设计规模为 48 万 m^3/d 。主要包括混合槽、絮凝池、平流沉淀池、V 型滤池、清水池、吸水井、二级泵房、投药间、泥水调节池、污泥浓缩池、污泥脱水车间、机修间、仓库、供电及配电、综合楼、候工楼等附属设施，并预留预处理及深度处理用地。

2 总则

2.1 工程范围

2.1.1 本智能化工程范围为智能化设计图纸中所反映的广州北江引水工程（花都水厂及配水管道工程部分）智能化系统工程建设标段二。标段二建设内容与一阶段共用系统后台设备。关于工作范围的详细说明，详本文件和图纸。

2.1.2 工程范围内主要工程内容包括（但不限于）：

1、基础设施

- （1）综合布线系统
- （2）信息网络系统
- （3）统一时钟系统
- （4）公共广播系统

2、安防集成应用综合管理（平台）系统

- （1）视频安防监控系统模块
- （2）出入口控制系统模块

3、其他

- （1）智能化系统配电、防雷和接地

2.2 工程界面

2.2.1 与土建工程界面

1、土建专业负责弱电机房、弱电间、弱电竖井、弱电孔洞的基本建设与预留。智能化专业负责因建筑智能化工程管线敷设或设备安装需要而作的开孔、墙面开槽等工程（包括因土建单位未预留或不完整的部分），并负责修复。

2、弱电竖井、孔洞在施工完成后的防火封堵，由智能化专业负责，且施工方法、材料必须满足消防要求，确保通过消防验收。

2.2.2 智能化系统机房工程、配电工程、接地工程与其它系统的工程界面

1、智能化系统配电工程以弱电主机房的强电配电箱进线端子为界，端子外侧进线电缆、管线的供货和安装由电气或自控专业负责。智能化系统的配电箱、UPS 电源装置及智能化配电箱之间、配电箱至智能化系统设备段的配电线路的供货和安装属智能化施工单位负责范围。

2、综合楼厂级集控室、网络机房、弱电间的总接地引出线电气专业负责。智能化专业负责各弱电机房、弱电间房间内部以及机房之间、机房至大楼接地端子的弱电接地汇流网、弱电接地干线、弱电接地端子排的供货和安装；并负责将智能化系统的设备、机柜等与弱电接地端子连通。

2.3 项目目标

利用先进的工业技术和信息化手段，实现信息化和工业化的深度融合，使得水厂的运营更加科学高效化、生产更加智能化、运营作业过程更加移动简单化、服务更加个性化，从而实现智慧化。

1) 减少人力：结合水厂生产工艺要求，设置适配的 PLC 和 SCADA，并制定优化方案，实现工艺控制过程自动化、智慧化。

2) 提高能效：在保障水质、供水量的前提下，配置数据分析和辅助决策应用，实现生产精细化，提高能效减少药耗。

3) 保障厂区安全：设置完善的安全防范系统。

4) 保障支撑能力：设置完善的信息设施。

5) 实现水厂智慧化运行：生产、安防与运营管理融合交互，通过可视化监控、预警报警、分析决策、协同管理等综合应用。

6) 预警联动，调度可视化，应急预案执行。

7) 预留接口：在开发和建设中，对其它以后预测到想要的东西，现阶段必要性不强，或者尚未成熟的，给其留有端口。

3 系统总体技术要求

3.1 现场环境条件

3.1.1 地理位置、气候条件

- 1、“花都水厂”位于广东省广州市。
- 2、气候条件：亚热带海洋性气候，年平均气温 22.3℃。
 - 1) 室外温度：0℃～50℃
 - 2) 室内温度：0℃～40℃
 - 3) 相对湿度：5～95%
- 3、腐蚀性：有轻度盐雾影响

3.1.2 电力供应

- 1、厂级集控室、弱电机房及弱电末端设备由 UPS 集中供电。
- 2、电压：AC 380V/220V
- 3、频率：50 Hz
- 4、波形失真：20%
- 5、频率波动：±1Hz
- 6、电压波动：±10%

3.1.3 设备工作时间

- 1、年工作时间：365 天
- 2、日工作时间：24 小时

3.2 标准和规范

- 《建筑设计防火规范》（GB 50016-2014）
- 《民用建筑电气设计标准》（GB51348-2019）
- 《火灾自动报警系统设计规范》（GB 50116-2013）
- 《智能建筑设计标准》（GB 50314-2015）
- 《综合布线系统工程设计规范》（GB 50311-2016）
- 《安全防范工程技术标准》（GB 50348-2018）
- 《入侵报警系统工程技术规范》（GB 50394-2007）
- 《视频安防监控系统工程技术规范》（GB 50395-2007）
- 《出入口控制系统工程技术规范》（GB 50396-2007）
- 《公共广播系统工程技术规范》（GB/T 50526-2021）
- 《数据中心设计规范》（GB 50174-2017）
- 《低压配电设计规范》（GB50054-2011）
- 《供配电系统设计规范》（GB50052-2009）

- 《通用用电设备配电设计规范》(GB50055-2011)
- 《建筑照明设计标准》（GB50034-2013）
- 《建筑物防雷设计规范》（GB50057-2010）
- 《建筑物电子信息系统防雷设计技术规范》（GB 50343-2012）
- 《综合布线系统工程验收规范》（GB/T 50312—2016）
- 《建筑电气工程质量验收规范》（GB50303—2015）
- 《智能建筑工程施工规范》（GB 50606-2010）
- 《智能建筑工程质量验收规范》（GB50339—2013）
- 《安全防范系统验收规则》（GA308—2001）
- 《建筑物防雷工程施工与质量验收规范》（GB50601—2010）
- 《自动化仪表工程施工及质量验收规范》（GB50093—2013）
- 《城镇供水厂运行、维护及安全技术规程》（GJJ 58-2009）
- 《反恐怖防范管理第 1 部分通则》DB4401T 10.1-2018
- 《反恐怖防范管理 第 25 部分：水务系统》DB4401/T 10.25-2019
- 《公共供水安全防范设施技术规范》DBJ 440100 T 123—2012

3.3 线缆、配线及设备端口的标签

- 3.3.1 所有使用的标签均应为机器打印，手写标签不予接受。标签上的编号应同时支持简体汉字、英文字母、数字、标点。标签上字体应清晰可辨。
- 3.3.2 标签应具有永久的防脱落、防水、耐温（ $\geq 500^{\circ}\text{C}$ ）特性。
- 3.3.3 所有线缆必须单独标签，线缆的两端及中途可为人接触的地方须加上标签。
- 3.3.4 所有设备端口都应使用标签予以标识。
- 3.3.5 所有前端设备须以标签加以标识，并清楚地表明其位置。
- 3.3.6 所有的配线及跳线都应采用标签予以标识，并单独编号。
- 3.3.7 所有的线槽应有明显的标识。

3.4 线缆端接

- 3.4.1 光纤的接续和端接须采用产品供应商认可的方法和工具设备。
- 3.4.2 光纤接续点必须在接续工作完成后进行现场测试。
- 3.4.3 光纤接续点的衰减损耗应小于 0.2dB。
- 3.4.4 除非与设备端接，所有线缆不允许续接。

3.5 线槽与线管

3.5.1 系统布线所需敷设的线槽及线管应采用经防腐、防锈处理的金属材料。

3.5.2 除非已进入设备机壳内，所有线缆必须放置于线槽、线管内，不得外露。

3.5.3 所有相互连接的线槽、线管必须使用裸铜线做电气导通，并接入弱电设备间的接地端子排，以保证接地电势的一致。导通用的铜线不得焊接在线管或线槽上，必须使用压接方式。

3.6 线缆敷设

3.6.1 所有线缆的敷设应按相关规范和标准施工，应确认有足够空间敷设线缆。

3.6.2 所有的线缆应敷设在指定的线槽或线管内，线缆的敷设应平直，不得产生扭绞、打圈等现象，不应受到外力的挤压和损伤。

3.6.3 在安排线缆路线时，必须考虑线缆的最小弯曲半径，并提供参数给监理或业主审核。

3.6.4 敷设多条电缆的位置应用扎线带绑扎，并做出标识，扎线带应保持相应间距，线缆扎线带的绑扎不能太紧以免影响线缆的使用。

3.6.5 线缆的排列应避免交叉。

3.6.6 线缆布放时长度应有冗余。在前端设备安装位置、设备间的铜缆的预留长度一般为 1 米至 2 米，光缆在设备端预留长度为 2 米至 3 米。有特殊要求的应按设计要求预留长度。

3.6.6 控制台、机柜内的线缆应排列整齐，并绑扎在机柜内的布线槽内，同时做出标识。线缆的敷设应便于机柜门的开启或关闭、设备的维护与更换。

3.7 接地

3.7.1 智能化施工单位负责本工程各弱电机房或弱电间的弱电专用干线及接地端子排（箱）的安装，以及与该接地端子排的端接及楼内接地线的敷设。所有接地要求符合国家相关标准。

3.7.2 智能化施工单位保证所提供的设备都能可靠接地，并负责实施，所有接地线应采用多股铜芯导线或铜带，截面应满足国家有关规范的要求。

3.7.3 其他专业提供的联合接地装置的接地电阻不大于 1 欧姆。

3.8 技术培训及售后服务

3.8.1 智能化施工单位需对各个子系统设备进行操作手册编制，并对物业维护人员进行系统性培训，确保维护人员能熟练操作各个子系统以及能进行简单日常维护。

3.9 设计及施工资质要求

3.9.1 智能系统是水厂关键设施，承包人中标后应委派一名持有计算机技术与软件专业技

术及相关专业资格证和具备工业系统智能化施工经验的工程师作为该系统施工管理的负责人，对智能化系统施工进行专业管理。同时，应配备不少于两名计算机相关专业人员负责日常现场施工管理和协调工作。

3.10 各子系统拓展性要求

3.10.1 智能化各子系统软件需提供二次开发条件，后期可根据需求进行功能拓展。

3.11 承包人保证

3.11.1 智能化各子系统软件应采用永久授权。

3.11.2 承包人应提供原厂安装服务、原厂维保、原厂软件及硬件固件版本升级服务、原厂技术支持。

3.11.3 本项目质保期：硬件提供工程完工验收通过之后的 2 年原厂质保服务；软件提供自工程完工验收通过之日起 2 年免费维保服务。在质量保证期内，若系统发生故障，承包人需免费调查故障原因并修复直至满足验收指标和性能的要求，包括且不限于更换整个或部分有缺陷的设备、修补系统漏洞或缺陷等。承包人收到通知后应在规定的售后服务时间内免费维修。如果承包人收到通知后在规定的售后服务时间内没有弥补缺陷，发包人可采取必要的补救措施，但其风险和费用应由承包人承担，发包人根据合同规定对承包人行使的其它权力不受影响。

3.11.4 质量保证期内，承包人应按以下方式提供免费服务：

3.11.4.1 服务人员：承包人至少派遣 1 名跟踪服务人员，对系统提供的业务中断、业务问题或功能提升予以支持。

3.11.4.2 现场服务：当系统提供的业务中断、业务问题或功能提升复杂等级高时且远程登录无法解决问题时，承包人须按照合同约定在规定时限内派遣工程师赴现场解决问题，确保发包人系统在规定时限内恢复正常运行。

3.11.4.3 远程登录：当系统提供的业务中断、业务问题或功能提升复杂等级高时，需要提供远端登录支持。

3.11.5 在质量保证期内，如果发包人为适应新的标准和工作要求，须对系统做小范围改进或增加新功能等，承包人应免费、及时进行修改或提供相关软件给发包人单位使用。

3.11.6 系统正常运行后，由于承包人对系统软件进行版本升级，承包人应向发包人提供免费升级服务。

3.11.7 对于测试、阶段性验收、整体上线试运行验收、项目竣工验收未发现的系统漏洞、缺陷，并不免除承包人的修复责任，承包人应免费予以修复以满足系统正常运行及

技术文件的要求。

- 3.11.8 在合同确定的质保期内，如发包人需要对系统继续进行二次开发（不在项目建设目标范围内），可委托承包人提供相应服务，包括但不限于技术咨询、开发实施等，承包人应积极配合工作；由此产生增加的费用，应首先参考本合同类似基础价格，如合同中无类似基础价格参考，则由甲乙双方另行协商。
- 3.11.9 承包人须将本项目合同质保期外运维及升级的相关服务（包括硬件设备、软件的费用）列入实施方案中，并需经发包人同意。
- 3.11.10 承包人保证向发包人提供的全部服务和交付的全部工作成果不侵犯任何第三方的知识产权及其他合法权益。
- 3.11.11 系统软件、通用软件必须是具有在中国境内的合法使用权或版权的正版软件，如任何第三方指控发包人使用本合同成果或服务侵犯其知识产权或其他权益，承包人应自费为发包人协助发包人进行答辩。如最终由司法机关或仲裁机关判决或裁定发包人构成侵权并需要赔偿，或在承包人同意前提下发包人与指控方进行和解，由此给发包人造成的一切损失（包括但不限于答辩费用、律师费、赔偿费等）均由承包人承担。
- 3.11.12 本合同总价中包含承包人所有应向所有权人支付的专利权、商标权或其它知识产权的一切相关费用。承包人需对所有成果、产品的知识产权负有瑕疵担保责任，因使用未被授权使用技术、组件、系统软件、通用软件等知识产权问题引起的纠纷所产生的所有责任及费用由承包人自行承担。
- 3.11.13 本项目的成果及其技术文档等所有权由发包人享有，技术文档资料包括完备的系统设计文档、功能模块说明、程序源代码、执行代码、使用手册等，发包人对本项目的成果具有所有权。项目所交付的应用系统软件环境包括生产环境（正式环境）、测试环境、开发环境，所有环境均要求能正常使用，未经发包人许可，承包人不得将相关发包人资料提供给第三方。
- 3.12 承包人中标后，应向发包人提交花都水厂智能化整体实施方案，其内容包括不限于：总体架构设计、基础设施建设、智能系统建设、智能化各子系统的功能、梳理业务流程及操作规程、业务流程优化、UI 设计、施工方案、二次深化设计、测试及试运行方案、培训方案、数据处理和维护、质保期内服务方案、质保期外运维及升级的相关服务方案（包括硬件设备、软件的费用）等。

3.13 标段二实施的智能化系统的软件系统应能融合到项目首期一阶段（标段一）已建成的系统或花都自来水公司现有信息化系统中，在对接原有系统过程中所必须增加的系统配置软件、数据接口或硬件均由承包人负责，且其费用已包括在投标报价中综合考虑，发包人不另外计价。

3.14 标段二实施的智能化系统的软件和硬件必须与项目首期一阶段（标段一）已建成的相兼容，且配置不得低于标段一，承包人应无条件采取措施达到数据对接顺畅、系统稳定、软硬件匹配等目标，否则，发包人有权对对应施工内容不予验收。上述工作的费用已包括在投标报价中综合考虑，发包人不另外计价。

二、技术规格书

1 综合布线系统

1.1 系统概况及架构

具体详见各图纸及其设计说明。

1.2 设计界面

具体详见各图纸及其设计说明。

1.3 系统总体技术要求

1) 系统必须符合国际标准 TIA/EIA-568B.2-1, EN50173 和 ISO11801: 2002 对六类铜缆布线及各子系统的规定。

2) 除机柜外, 系统的其余所有铜缆、模块、配线架、跳线管理器、跳线、面板、标签夹、接插件、工具等设备材料必须为端对端同一厂家的布线产品。系统的所有光缆、耦合器、光纤配线架、光纤跳线管理器、光纤跳线、尾纤、光纤面板、接插件、工具等设备材料也必须为端对端同一厂家的布线产品。生产商应具备 ISO9001 或 ISO14001 体系认证证书, 并提供相关证明文件。

3) 综合布线系统的六类产品及组成的永久链路必须通过如 3P、UL、Delta 等国际或国内第三方实验室的基于 TIA/EIA-568B.2-1 或 ISO11801 (2002) 六类标准的认证测试, 并提供证明文件。系统产品应取得信息产业部数据通信产品质量监督检验中心的认证。项目竣工时必须针对本次项目提供详细的测试报告和技术文档。

4) 系统非屏蔽铜缆必须符合 EMC 标准的电磁兼容性要求。

5) 所有网线及室内光缆要求采用符合 IEC60754 标准的阻燃材料, 满足防火等级 不低于 IEC60332-3A 标准, 并提供同等级的相关防火检验报告。

6) 综合布线系统的所有线缆在敷设过程中必须一根线缆敷设到位, 中间不得有断点。所有机架/机柜内各配线架的摆放及线缆的走向必须合理, 接插件、模块及跳线的标志齐全, 线缆终端必须有编号和标签, 以标明线号、线位、区号和房号。

7) 工程完成后, 系统永久链路的回波损耗 (RL)、插入损耗 (IL)、近端串音 (NEXT)、近端串音功率和 (PS NEXT)、衰减串音比 (ACR)、衰减串音比功率和 (PS ACR)、等电平远端串音 (ELFEXT)、等电平远端串音功率和 (PS ELFEXT)、直流环路电阻、传播时

延、传播时延偏差、非平衡衰减等指标应满足或高于 《综合布线系统工程设计规范》（GB 50311-2016）系统指标中的 E 级标准，并提供检测报告。（测试设备应使用第三方厂商生产国际测试设备，如：美国 Fluke 公司的 Fluke-DSP4000 或 OmnisScanner2）

8）承包人需提供生产厂商 30 年以上质量保证及系统应用保证，包括产品、链路/通道和应用三部分。

1.4 主要设备技术参数要求

1.4.1 六类非屏蔽信息模块

- 1) 电气性能达到六类标准 TIA/EIA568B.2-1 CAT6 的要求, 传输参数测试应达到 250MHz。
- 2) 匹配线规：23~24AWG
- 3) 组成：RJ45 插座，排线块
- 4) 规格：支持 1U24 口高密度管理
- 5) 端接方式：免打线工具，可重复端接
- 6) 打线方式：T568A 或 T568B

1.4.2 工作区面板

- 1) 白色 86 方形单口/双口面板，自带防尘盖。
- 2) 阻燃级别：94V-0
- 3) 强度要求：耐抗击强冲击
- 4) 模块安装方式：90 度（垂直）或 45 度（斜角）安装
- 5) 应带有标签、色标及明显的标识以区分数据点或语音点，并留有可填写编号的空间。

1.4.3 六类 4 对非屏蔽双绞线（UTP）

- 1) 线规：23AWG
- 2) 规格：100 欧姆，250 MHz
- 3) 芯线对数：4 对，每芯带有彩色护套
- 4) 线缆结构：线缆内部带十字支撑架结构
- 5) 阻燃级别：低烟无卤阻燃，并符合 IEC60332-3A 标准
- 6) 标准：ISO 11801、TIA/EIA-568B.2-1

1.4.4 室内多模光纤

- 1) 规格：50/125um，满足 ISO 的 OM4 多模光缆标准，支持 10G 以太网应用 400 米，1G 以太网应用 1000 米
- 2) 衰减： $\leq 3.0\text{dB}/1.0\text{dB}@850/1300\text{nm}$
- 3) 带宽： $\geq 1500/500\text{MHz-Km}@850/1300\text{nm}$
- 4) 芯数：按图纸要求配置。
- 5) 阻燃级别：低烟无卤阻燃，并符合 IEC60332-3A 标准
- 6) 标准：ISO11801、TIA/EIA-568B
- 7) 室外型应带金属铠装、防潮

1.4.5 室内单模光纤

- 1) 规格：9/125um，满足 ITU-T 的 G652D 关于 OS2 单模光缆标准
- 2) 衰减： $\leq 0.36\text{dB/km}@1310\text{nm}$ ； $\leq 0.22\text{dB/km}@1550\text{nm}$ 。
- 3) 芯数：按图纸要求配置。
- 4) 阻燃级别：低烟无卤阻燃，并符合 IEC60332-3A 标准
- 5) 标准：ISO11801、TIA/EIA-568-C.3
- 6) 应采用干式+非延燃外护层结构。

1.4.6 室外单模光纤

- 1) 规格：8.3/125um，满足 ITU-T 的 G652D 关于 OS2 单模光缆标准，支持 10G 以太网应用 10km。
- 2) 衰减： $\leq 0.36\text{dB/km}@1310\text{nm}$ ； $\leq 0.22\text{dB/km}@1550\text{nm}$ 。
- 3) 芯数：按照图纸要求。
- 4) 标准：ISO 11801、TIA/EIA-568B。
- 5) 室外型应带金属铠装、防潮。

1.4.7 RJ45 标准模块式配线架（包括面板、六类模块、理线器、标签等）

- 1) 金属箱体，1U 高度
- 2) 面板端口：配 24 口六类 RJ45 屏蔽信息模块
- 3) 卡接线规范范围：23~24AWG
- 4) 打线方式：T568-A/B

5) 配原厂线缆管理器、标签夹、打印标签纸

6) 安装方式：19 英寸机柜式安装

7) 标准：符合 TIA/EIA-568-B

1.4.8 光纤配线架（包括面板、耦合器、尾纤、理线器、标签等）

1) 金属箱体，后端进线，内置绕线盘，面板可前端取下

2) 面板端口：配 6/12/24 口单模 LC 耦合器

3) 面板端口密度：24 口单模 LC/1U

4) 尾签：与连接光纤、耦合器匹配

5) 连接衰减：0.2dB

6) 安装方式：19 英寸机柜式安装，可前端施工和维护管理

1.4.9 六类数据跳线

1) 类别：原厂正品，六类非屏蔽

2) 接口类型：4 对 RJ45/RJ45

3) 芯数：8 芯

4) 长度：2/3 米可选

5) 阻燃级别：低烟无卤阻燃

6) 标准：ISO 11801、TIA/EIA-568B

1.4.10 双芯单模光纤跳线

1) 类别：原厂正品

2) 规格：单模光纤，9/125 μ m

3) 标准：符合 EN60794-1-1 规范

4) 典型插入损耗： ≤ 0.3 dB，最小反射系数：35 dB

5) 芯数：2 芯

6) 长度：2/3 米可选

7) 阻燃级别：低烟无卤阻燃

8) 接口类型：LC，并与各配线架、面板、设备的连接器相匹配。

1.4.11 楼层弱电机柜

- 1) 19"标准机柜，落地安装
- 2) 2.0mm 厚高强度冷轧板，表面防静电喷涂
- 3) 机柜内备有竖向跳线管理器、风扇、PDU 电源插座及门锁
- 3) 配置 16 位 16A PDU（总容量 16A）。
- 4) 尺寸：42U，600x600x2000mm（弱电间）。
- 5) 机柜颜色、样式、外观等应在承包人提供的采购方案或实施方案中说明，并在承包人中标后由发包人最终确定。

2 信息网络系统

2.1 系统概况

具体详见各图纸及其设计说明。

2.2 系统构成

详见各图纸及其设计说明。

2.3 系统总体技术要求

- 1) 所有交换设备、网管软件必须是同一品牌的产品，以方便维护和管理。
- 2) 核心交换机应采用万兆交换机。
- 3) 网络设备应支持 SNMP、Web、RMON 等网管协议，可与网管中心配合完成故障管理、配置管理、性能管理和安全管理。
- 4) 系统设备应满足的标准如下：
 - IEEE 802.1d：介质存取控制标准
 - IEEE 802.3x：以太网标准（包括 802.3ab、802.3u、802.3z 等）
 - IEEE 802.1Q/P
 - 组播协议支持：PIM（松散模式和密集模式）、DVMRP、IGMP
 - 若投标人的产品还满足其它标准或专用标准，应详细说明
- 5) 网络管理应选用当前主流网络管理平台，对网络设备运行状态实行实时监控，提供对网络故障检测、网络性能分析、设备配置、网络安全控制等有效地管理。
- 6) 投标人应根据用户的实际需求，提交在网内划分 VLAN，通过交换机的第三层交换中设置访问列表（Access Lists），控制相互通讯部门之间的数据来往方向。

2.4 主要设备技术参数要求

2.4.1 核心层交换机（办公网）

- 交换容量：≥76.8Tbps。
- 包转发率：≥8640Mpps（双参数以较小参数为准）。

- 业务板插槽：≥6 个。
- 硬件：支持交换网数量≥2,支持 GE 光、GE 电接口板。全宽主控，关键部件热插拔，电源模块冗余。
- 二层功能：支持基于端口、协议、子网和 MAC 的 VLAN 划分。
- 三层功能：支持 RIP、OSPF、ISIS、BGP 等 IPv4 动态路由协议,支持 RIPng、OSPFv3、ISISv6、BGP4+等 IPv6 动态路由协议。
- QoS：支持 Remark 等动作,支持多种队列调度方式,支持拥塞避免机制,支持流量整形。
- 实配：万兆光端口≥3 个；千兆电端口≥24 个，千兆光端口≥24 个，交换网板≥2，主控单元≥2 块，电源≥4 块；支持扩展千兆电口，千兆光口，10GE、40GE、100G 等接口。
- 堆叠：通过单台配置不少于 2 个 10GE 端口实现双机二虚一。
- 可靠性：主要部件主控板、交换网板、电源、风扇支持冗余备份，并支持热插拔。
- 本设备所配置功能应满足本项目整体竣工验收前所需业务需求。

2.4.2 智能网核心层交换机（智能网）

- 交换容量：≥38.4Tbps。
- 包转发率：≥7200Mpps（双参数以较小参数为准）。
- 业务板插槽数：≥3 个。
- 网络协议：支持 IEEE 802.1d(STP)、802.1w(RSTP)、802.1s(MSTP)，支持 Jumbo Frame，支持跨版端口镜像，支持流镜像，支持远程端口镜像。
- 路由：支持静态路由和动态路由 RIP、RIPng、OSPF、OSPFv3，支持策略路由。
- QoS：支持 SP、WRR、WFQ、SP+WRR 等调度方式，支持双向 CAR，支持 WRED。
- 万兆光端口≥3 个；千兆光端口≥24 个，≥24 个千兆电接口，支持扩展千兆电口，千兆光口，10GE 等接口，配置主控单元≥2 块，电源≥2 块；
- 可靠性：主要部件主控板、电源、风扇支持冗余备份，并支持热插拔。
- 本设备所配置功能应满足本项目整体竣工验收前所需业务需求。

2.4.3 生产网核心层交换机（生产网）

- 交换容量：≥38.4Tbps。
- 包转发率：≥7200Mpps（双参数以较小参数为准）。
- 业务板插槽数：≥3 个。

- 网络协议：支持 IEEE 802.1d(STP)、802.1w(RSTP)、802.1s(MSTP)，支持 Jumbo Frame，支持跨版端口镜像，支持流镜像，支持远程端口镜像。
- 路由：支持静态路由和动态路由 RIP、RIPng、OSPF、OSPFv3，支持策略路由。
- QoS：支持 SP、WRR、WFQ、SP+WRR 等调度方式，支持双向 CAR，支持 WRED。
- 万兆光端口 ≥ 3 个；千兆光端口 ≥ 24 个， ≥ 24 个千兆电接口，支持扩展千兆电口，千兆光口，10GE 等接口，配置主控单元 ≥ 2 块，电源 ≥ 2 块；
- 可靠性：主要部件主控板、电源、风扇支持冗余备份，并支持热插拔。
- 本设备所配置功能应满足本项目整体竣工验收前所需业务需求。

2.4.4 接入层交换机（办公网）

- 交换容量： $\geq 336\text{Gbps}$ 。
- 包转发率： $\geq 108\text{Mpps}$ 。
- 端口配置：非 POE 交换机：千兆光口 ≥ 2 个，千兆\百兆自适应电口 ≥ 24 个。
- 二层功能：支持 MAC 地址 $\geq 16\text{K}$ 。
- 三层功能：支持静态路由、RIP、RIPng、OSPF 等。
- 堆叠功能：接入层交换机采用可堆叠功能交换机，每个堆叠单元不超过 4 台。
- 本设备所配置功能应满足本项目整体竣工验收前所需业务需求。

2.4.5 接入层交换机（办公网，无线 AP 接入用）

- 交换容量： $\geq 336\text{Gbps}$ 。
- 包转发率： $\geq 108\text{Mpps}$ 。
- 端口配置：POE+交换机：千兆光口 ≥ 2 个，千兆\百兆自适应电口 ≥ 24 个。
- 二层功能：支持 MAC 地址 $\geq 16\text{K}$ 。
- 三层功能：支持静态路由、RIP、RIPng、OSPF 等。
- 堆叠功能：接入层交换机采用可堆叠功能交换机，每个堆叠单元不超过 4 台。
- 本设备所配置功能应满足本项目整体竣工验收前所需业务需求。

2.4.6 接入层交换机（办公网，生产区域使用）

- 交换容量： $\geq 336\text{Gbps}$ 。
- 包转发率： $\geq 51\text{Mpps}$ 。
- 端口配置：非 POE 交换机：千兆光口 ≥ 2 个，千兆\百兆自适应电口 ≥ 24 个。

- 二层功能：支持 MAC 地址 $\geq 16K$ 。
- 三层功能：支持静态路由、RIP、RIPng、OSPF 等。
- 堆叠功能：接入层交换机采用可堆叠功能交换机，每个堆叠单元不超过 4 台。
- 本设备所配置功能应满足本项目整体竣工验收前所需业务需求。
- 采用工业级以太网交换机。

2.4.7 接入层交换机（办公网，生产区域使用）

- 交换容量： $\geq 336Gbps$ 。
- 包转发率： $\geq 51Mpps$ 。
- 端口配置：POE+交换机：千兆光口 ≥ 2 个，千兆\百兆自适应电口 ≥ 24 个。
- 二层功能：支持 MAC 地址 $\geq 16K$ 。
- 三层功能：支持静态路由、RIP、RIPng、OSPF 等。
- 堆叠功能：接入层交换机采用可堆叠功能交换机，每个堆叠单元不超过 4 台。
- 本设备所配置功能应满足本项目整体竣工验收前所需业务需求。
- 采用工业级以太网交换机。

2.4.8 接入交换机（智能网）

- 交换容量： $\geq 336Gbps$ 。
- 包转发率： $\geq 51Mpps$ 。
- 端口配置：非 POE 交换机：千兆光口 ≥ 2 个，百兆\十兆自适应电口 ≥ 24 个。
- 二层功能：支持 MAC 地址 $\geq 16K$ 。
- 三层功能：支持静态路由、RIP、RIPng、OSPF 等。
- 堆叠功能：接入层交换机采用可堆叠功能交换机，每个堆叠单元不超过 4 台。
- 本设备所配置功能应满足本项目整体竣工验收前所需业务需求。

2.4.9 接入交换机（智能网）

- 交换容量： $\geq 336Gbps$ 。
- 包转发率： $\geq 51Mpps$ 。
- 端口配置：POE 交换机：千兆光口 ≥ 2 个，百兆\十兆自适应电口 ≥ 24 个。
- 二层功能：支持 MAC 地址 $\geq 16K$ 。
- 三层功能：支持静态路由、RIP、RIPng、OSPF 等。

- 堆叠功能：接入层交换机采用可堆叠功能交换机，每个堆叠单元不超过 4 台。
- 本设备所配置功能应满足本项目整体竣工验收前所需业务需求。

2.4.10 接入层交换机（智能网）

- 交换容量： $\geq 336\text{Gbps}$ 。
- 包转发率： $\geq 51\text{Mpps}$ 。
- 端口配置：非 POE 交换机：千兆光口 ≥ 2 个，千兆\百兆自适应电口 ≥ 24 个。
- 二层功能：支持 MAC 地址 $\geq 16\text{K}$ 。
- 三层功能：支持静态路由、RIP、RIPng、OSPF 等。
- 堆叠功能：接入层交换机采用可堆叠功能交换机，每个堆叠单元不超过 4 台。
- 本设备所配置功能应满足本项目整体竣工验收前所需业务需求。
- 采用工业级以太网交换机。

2.4.11 接入层交换机（智能网）

- 交换容量： $\geq 336\text{Gbps}$ 。
- 包转发率： $\geq 51\text{Mpps}$ 。
- 端口配置：POE+交换机：千兆光口 ≥ 2 个，千兆\百兆自适应电口 ≥ 24 个。
- 二层功能：支持 MAC 地址 $\geq 16\text{K}$ 。
- 三层功能：支持静态路由、RIP、RIPng、OSPF 等。
- 堆叠功能：接入层交换机采用可堆叠功能交换机，每个堆叠单元不超过 4 台。
- 本设备所配置功能应满足本项目整体竣工验收前所需业务需求。
- 采用工业级以太网交换机。

2.4.12 防火墙

- 性能要求：本次配置吞吐量 $\geq 40\text{Gbps}$ ，配置最大并发连接数 ≥ 1000 万，配置每秒新建连接数 ≥ 40 万。
- 负载均衡：支持并配置负载均衡功能，包括链路智能选路负载均衡、服务器负载均衡等功能，负载均衡算法包括但不限于简单轮询、加权轮询、最小连接、加权最小连接等。
- 安全功能：支持不少于 4000 种漏洞特征的攻击检测和防御。支持 Web 攻击识别和防护，如跨站脚本攻击、SQL 注入攻击，DDOS 攻击等。

- 实配：≥6 个万兆光口和 2 千兆光口，≥4 千兆电口；配置双电源。配置入侵检测系统功能授权≥3 年、网络防病毒安全功能授权≥3 年。
- 扩展：支持 10GE 接口，便于平滑扩展需要。
- 本设备所配置功能应满足本项目整体竣工验收前所需业务需求。

2.4.13 网管系统

- 系统管理规模：系统支持大规模网络管理能力，单套最多可以管理 20,000 台设备。
- 系统安全性：系统提供用户的分权分域功能，为不同的用户分配不同的设备管理范围和操作权限；提供用户账号和密码的设置策略；提供登录 IP 地址段和登录时间的设置；支持在线用户查询，并能够强制在线用户退出。
- 拓扑管理：系统需要提供拓扑管理，能够以拓扑方式显示设备以及设备间的连接关系，拓扑上能够提供设备、链路的状态显示和刷新，能够提供设备和链路的信息，如：设备名称、设备 IP、接口速率、带宽利用率等。
- 故障管理：系统需要支持 7*24 小时对全网设备告警的实时监控，并支持 Email、SMS 形式的告警通知，通知内容可以自定义。
- 性能管理：系统支持基于任务的性能监控，7*24 监控网络性能。通过设置不同的性能阈值，可生成 4 级不同阈值告警：紧急、重要、次要、提示。支持历史性能的比较查看。
- 资源管理：系统提供多种设备资源发现方式，支持单台设备添加、按 IP 段添加、通过文件导入方式添加等。
- WLAN 网络管理：系统支持 7*24 小时 WLAN 网络监控能力，支持基于区域维度的拓扑可视化监控。
- 移动运维 APP：系统提供基于 Android 和 IOS 的移动运维 APP，实现 WLAN 网络的移动化管理，支持区域维度的无线网络质量监控和一键式故障诊断。
- 要求提供网管软件配套硬件（硬件性能应支持软件功能实现），并配置对应网元管理 license。
- 本软件所配置功能应满足本项目整体竣工验收前所需业务需求。

2.4.14 上网行为管理

- 网络层吞吐量（大包）：4.8Gb，应用层吞吐量：600Mb，带宽性能：400Mb，IPSEC VPN 加密性能（最高性能）：120Mb；支持用户数：3000；

- 规格：1U，内存大小：4GB，硬盘容量：64G SSD+960G SSD，电源：单电源，接口：4 千兆电口，4 千兆光口 SFP；
- 支持网关模式，支持 NAT、路由转发、DHCP、GRE、OSPF 等功能；
- 支持网桥模式，以透明方式串接在网络中；支持电口 bypass；
- 必须支持多路桥接功能，最多可支持 32 组网桥模式；
- 支持旁路模式，无需更改网络配置，实现上网行为审计；
- 旁路支持主主、主备模式部署；
- 支持部署在 IPv6 环境中，设备接口及部署模式均支持 ipv6 配置，所有核心功能（上网认证、应用控制、流量控制、内容审计、日志报表等）都支持 IPv6
- 可针对内网用户的 web 访问质量进行检测，对整体网络提供清晰的整体网络质量评级，支持以列表形式展示访问质量差的用户名单，支持对单用户进行定向 web 访问质量检测。
- 支持通过 OAuth 认证协议对接，支持阿里钉钉，口袋助理，企业微信第三方账号授权认证；
- 支持企业微信、MOA、钉钉 这三个平台支持同步组织结构，用户通过企业微信、MOA、钉钉认证上线，本地会创建与认证服务器上对应的用户组，用户会上线到对应创建的组；
- 支持基于 802.1x 的外部 CA 证书认证，同时支持在线证书状态查询（OCSP）；
- 支持哑终端通过 MAC 认证的方式接入网络，必须支持在终端管理列表批量绑定设备 IP/MAC 快捷放通入网；
- 支持图形化查看当前内网 IP 使用情况，帮助管理员减少人工维护 IP 表的工作量；
- 对网络接入的终端进行可视化管理，展示终端详细信息、异常状态等 2.支持查看终端类型，以及终端详细信息（厂商，系统，端口等）；3.支持查看终端类型分布；
- 设备必须支持能自动发现网络中通过无线上网的热点和移动终端的 IP 和终端类型，支持移动终端型号识别，至少识别不少于 10 种移动终端型号；
- 支持终端调用管理员指定脚本/程序以满足个性化检查要求，比如检测系统更新是否开启、开放端口、已安装程序列表、终端发通知等对不满足检查要求的终端可弹窗提示、禁止上网；
- 基于“流量”、“流速”、“时长”设置配额，当配额耗尽后，将用户加入到指定的流控黑名单惩罚通道中

- 支持统一平台设备下发升级包，一次下发，2 台设备连续同时升级成功。升级过程中会进行双机切换来保证业务不中断
- 支持攻击、双机切换告警、移动终端管理告警、风险终端发现告警、web 关键字过滤告警、杀毒告警、设备流量超限告警、磁盘/CPU/内存异常告警等
- 支持首页分析显示接入用户人数、终端类型、认证方式资产类型分布、新设备发现趋势、终端违规检查项排行、终端违规用户排行带宽质量分析、实时流量排名泄密风险、违规访问、共享上网等行为风险情况
- 实时提供用户流量排名、应用流量排名、所有线路应用流速趋势、流量管理状态、连接监控信息
- 支持 PPS 异常、丢包异常、ARP 异常、内网 DOS 攻击等异常情况实时监测，显示每日异常事件个数及情况
- 支持针对上网权限策略进行检测分析，查看各个应用是否匹配相关策略
- 支持对加密 HTTPS、SMTP-SSL、SMTP 的邮件进行关键字过滤；
- 必须能基于关键字、发件人地址等识别和过滤使用邮件客户端外发 SSL 加密邮件的行为；
- 必须能够基于关键字识别和过滤使用 SSL 加密的 Webmail 邮箱外发邮件的行为，比如 QQ 邮箱；
- 支持从本地导入和扫描导入，支持以 CSV 格式文件导入帐户/分组/IP/MAC/描述/密码等信息
- 支持为用户添加自定义属性（职位、临时项目组、邮件组等），能够根据用户属性自动归类并可以针对用户属性配置上网权限策略、流控策略，审计策略等；
- 支持智能负载均衡，负载策略可配置：优先使用优先级最高的线路、按运营商负载、剩余带宽、带宽比例、平均分配以及禁用默认负载策略；
- 支持根据 IP、协议、带宽、于用户、域名、应用、DSCP 设置选路策略；
- 支持对移动应用的细分权限控制，微信：微信网页版、微信传文件、微信朋友圈、微信游戏。移动 QQ：QQ 传文件、QQ 视频语音等；

2.4.15 出口路由器

- 基本参数：整机高度 $\leq 2U$ ，业务插槽 ≥ 4 个；非堆叠架构； ≥ 6 个 10GE 光口， ≥ 10 个 GE 电口

- 性能参数：包转发能力 $\geq 60\text{Mpps}$ ，内存 $\geq 8\text{GB}$ ；
- 基础功能：DHCP server/client/relay，PPPoE server/client，NAT，子接口管理
- 路由协议（IPV4）：路由策略，静态路由，RIP，OSPF，IS-IS，BGP
- 路由协议（IPV6）及功能：静态路由，路由策略，RIPng，OSPFv3，IS-ISv6，BGP4+，IPv6 ND，IPv6 PMTU，IPv6 FIB，IPv6 ACL，ICMPv6，DNSv6，DHCPv6
- MPLS：LDP，MPLS L3 VPN，VLL，PWE3，静态 LSP，动态 LSP，MPLS TE，IP FRR，LDP FRR，TE FRR
- 安全：ACLv4/v6，基于域的状态防火墙，802.1x 认证，MAC 认证，Portal 认证，AAA，RADIUS，HWTACACS，PKI，广播风暴抑制，ARP 安全，ICMP 防攻击，URPF，CPCAR，黑名单，攻击源追踪，国密算法，上网行为管理，IPS，URL 过滤
- 本设备所配置功能应满足本项目整体竣工验收前所需业务需求。

2.4.16 堡垒机

- 软硬件一体化产品，2U、硬盘 2T*2、硬盘须配置 RAID1、至少配备 6 个 100/1000M 自适应电口和 4 个 1000M 光口（并配 2 个 SFP 多模模块），1+1 冗余电源
- 可管理设备数量 ≥ 500 个，运维用户无限制
- 单台堡垒机字符类并发会话 ≥ 500 、图形类并发会话 ≥ 200
- 设备采用旁路部署，不得影响业务环境；须支持 HA 主备模式，管理口和心跳口须支持多链路端口绑定功能，防止单网卡或单线故障。
- 支持多台堡垒机异地备份部署，每台设备都能提供运维和审计服务，配置数据自动同步
- 支持集群部署模式，中心采用 HA，节点可以横向扩展，实现统一登录入口、统一配置同步、审计日志集中查询、实时会话集中监控，以满足业务增长需求。
- 支持用户多角色划分功能，如系统管理员、部门管理员、运维员、审计管理员、密码管理员等，对各类角色需要进行细粒度的权限管理
- 支持用户的批量导入/导出，按用户类型等分组方式；支持用户安全策略功能，如密码锁定次数、密码有效期、密码复杂度、用户有效期、用户登录时间限制、用户登录 IP 范围等
- 支持按部门组织架构（至少 5 个层级的部门）管理用户数据、资产数据、授权数据、审计数据。

- 每个部门可以管理本部门及下级部门的用户角色：部门管理员、运维管理员、审计管理员、运维员。
- 每个部门的部门管理员可以管理本部门及下级部门的主机、授权关系、策略。
- 每个部门的审计管理员可以管理本部门及下级部门的运维会话日志
- 产品内置 VPN 模块，无需与其他 VPN 设备联动，实现运维入口安全接入
- 支持与 AD、LDAP、RADIUS、吉大正元、北京 CA 认证系统联动登录堡垒机，支持自动同步 AD/LDAP 用户
- 支持与 get、post、soap 发送方式的 http 短信网关平台进行联动
- 支持手机 APP 动态口令认证方式登录堡垒机，且新用户首次登录后需强制绑定 APP 动态口令。
- 堡垒机须内嵌动态令牌和 usbkey 认证引擎，可同时使用动态令牌和 USBkey。
- 支持基于国密算法的动态令牌进行双因子认证
- 支持采用国密加密算法进行核心敏感数据加密存储
- 基于不同的用户设置不同的双因子认证模式，如 user1 用动态令牌、user2 用 USBkey、user3 手机 APP 动态口令认证
- 支持域认证与双因子认证结合使用，如同时使用 AD/LDAP 用户名+AD/LDAP 密码+手机 APP 动态口令登录堡垒机、同时使用 AD/LDAP 用户名+AD/LDAP 密码+短信口令登录堡垒机
- 可设置用户密码错误达到一定次数后的锁定时长及登录失败次数的重置时间
- 可以设置用户密码的长度、复杂度、相关度，其中相关度可以设置密码与用户名的关系，可以选择是否检查历史密码。并可支持密码过期前告警。
- 支持认证窗口的全局设置：可以选择启用哪种或者哪几种认证登录窗口
- 支持常用的运维协议：SSH、TELNET、RDP、VNC、FTP、SFTP、rlogin；可通过应用发布的方式进行协议扩展，如数据库 Oracle、MSSQL、MySQL、VMware vSphere Client、浏览器等客户端工具
- 支持 DB2、oracle、mysql、sqlserver 主流数据库协议代理运维
- IE/Chrom 代填应用发布：HTTP/HTTPS 协议的 web 设备，且可以直接代填账号和密码
- 可以通过 socks5/http/ssh 等代理协议连接管理异地云资源区中私有网络的云主机
- 支持对设备进行按设备类型分组、按部门分组，支持设备批量导入/导出

- 支持设备帐户和密码的自动登录、手工登录、二次自动登录模式
- 支持设置共享账户，用于不同主机拥有相同账户名及密码的场景。
- 支持自动收集设备 IP、运维协议、端口号、账号、密码、与用户的权限关系，甚至可自动完成授权
- 导出的设备信息文件加密存储，解密时须由 2 个管理员同时解密才能查看到设备信息文件内容。
- 运维人员可以向管理员申请需要访问的设备，申请时可以选择：设备 IP、设备账户、运维有效期、备注事由等，并且运维工单以邮件方式通知管理员。
- 管理员对运维工单进行审核之后以邮件方式通知给运维人员；如果允许，则运维人员才可访问；否则就无法访问。
- 支持定期自动修改 windows 服务器、网络设备、linux/unix 等目标设备密码功能。
- 可以通过编写改密脚本的方式进行改密操作。
- 支持完善的自动改密安全保护机制，包括：改密前备份、备份失败不改密、改密后备份、密码文件加密；
- 支持发送方式，包括邮件、FTP、SFTP 等
- 支持自动密码恢复、手工验证密码、密码强度控制等
- Web 访问方式：至少支持使用 IE、谷歌、火狐三种浏览器打开堡垒机的 Web 页面直接调用 mstsc、VNC、Xshell、SecureCRT、Putty、winscp、flashFXP、FileZilla、SecureFX 等运维客户端工具
- H5 运维方式：支持 ssh、telnet、rlogin、rdp、vnc 协议的 H5 运维，无需本地运维客户端工具
- 支持对主机联通性、账号有效性进行周期性检测。并可设置是否开启检测连通性、有效性功能。
- 支持通过堡垒机页面直接调用本地 Windows 系统里的 plsql、sqlplus、toad、sqlwb、ssms、mysql.exe 等数据库客户端工具。
- 客户端访问方式：支持使用本地的 mstsc/Xshell/SecureCRT/Putty 等客户端工具登录堡垒机访问图形或字符设备，视图界面一致性、搜索能力
- 支持使用本地的 winscp/flashFXP/SecureFX 等客户端工具登录堡垒机访问 SFTP/FTP 设备
- 支持使用本地的 SecurCRT/Xshell/OpenSSH 工具通过 SSH 网关代理方式直接登录字

符设备

- 可以使用 SSH-agent-forwarding 登录到 ssh 服务器，用于登录堡垒机和登录 ssh 主机使用相同私钥的场景。
- 可以使用密码或公钥的方式登录到 SSH 资产，并且可以发送运维用户信息、运维来源 IP 等环境变量到资产上。
- 支持在 mac 电脑里使用 navicat 工具通过堡垒机登录 mysql、oracle 等数据库服务器
- 支持批量登录字符设备功能：能自动生成 SecurCRT/Xshell 工具的批量登录文件，实现在工具中批量自动登录多台设备。
- 可一键批量登录不同协议的主机资产。
- 可记录最近运维的主机，用于快速对主机进行运维。
- AD/LDAP 环境，支持直接使用登录堡垒机的 AD/LDAP 用户及密码可以直接自动登录到服务器里
- 可进行用户会话数量限制，允许自定义每个用户最多可以同时开启多少个会话。
- 支持通过多个维度筛选待运维资产，可包括主机 IP/主机名、操作系统、主机编码、主机组等。其中涉及到需要手动输入进行筛选的选项，需支持选择模糊搜索或精准搜索。
- 支持对运维操作会话的在线监控、实时阻断、日志回放、起止时间、来源用户、来源 IP、目标设备、协议/应用类型、命令记录、操作内容（如对文件的上传、下载、删除、修改等操作等）的详细行为日志。
- 支持保存 SSH 的 sz/rz 命令（zmodem）传输的原始文件
- 支持保存 SFTP/FTP 传输的原始文件
- 支持保存 RDP 粘贴板（桌面之间复制-粘贴）传输的原始文件
- 支持保存 RDP 磁盘映射传输的原始文件
- 支持对 RDP 屏幕文字内容、标题窗口、键盘输入的记录和搜索定位。
- 支持审计主流数据库（如 DB2、oracle、mysql、sql server）运维中的 SQL 语句，可进行关键信息定位查询
- 支持全局搜索审计日志，无需区分图形/字符/文件/应用类型，只需通过关键信息直接搜索定位。
- 可针对审计操作进行规则设置，自定义用户与资产的审计关系，即可选择用户有权限审计指定设备的操作行为。

- 审计数据支持通过 SFTP/FTP 方式自动归档，并在页面中可以查询哪些数据是否归档。归档过程时，可以设置自动执行归档的时间以及归档传输的速度限制并可设置归档成功之后自动删除数据，归档后的数据可以用专用播放器离线查看。
- 支持通过基于时间、IP/IP 段、用户/用户组、设备/设备组、设备账号、命令关键字、控制动作、黑白名单等组合访问控制策略，授权用户可访问的目标设备。
- 对重要设备启用登录审核功能，运维人员须向管理员申请登录，管理员允许之后才可登录；否则无法登录
- 支持对重要命令进行审核：运维人员执行命令后，须等到管理员审批通过后才可执行成功。
- 对于审批操作，可以设置审批人及该审批人有权限审批的资产
- 支持自动推送命令任务，如可自动备份交换机/路由器的配置信息、可自动执行周期任务；并将结果以邮件/FTP/SFTP 的方式发送给相关管理员
- 支持运维空闲会话时间全局设置限制功能
- 内置丰富的报表统计模板，可点击柱状图、或曲线图进行数据钻取分析，且支持 PDF、doc、html 格式导出
- 内置根据运维人员和组生成各种维度的分析报表，维度包含总为运维次数、时长、活动时长、会话起止时间、会话大小、命令数、上传下载文件数，分别从全局及平均值、最大值、最小值、单次运维、单个会话等角度提供非常有价值有意义的报表。
- 支持运维报表自动定期发送，提供一键导出符合等级保护、SOX 法案要求的综合分析报告。
- 支持配置 DNS 服务器，且可配置首选、备选 DNS
- 支持自定义堡垒机代理协议的端口。
- 支持配置静态路由
- 支持对登录堡垒机的来源 IP 进行限制。可采用黑白名单两种模式
- 支持自身审计，包括但不限于：系统状态检测、登录日志、用户配置日志、设备配置日志、授权配置日志、策略配置日志、运维访问日志、系统配置日志等
- 支持系统日志报表统计功能，包括但不限于登录日志统计、配置日志统计、运维访问日志统计等，可以导出报表。
- 支持中文、英文、繁体中文，并可配置是否允许用户进行语言切换。
- 支持自定义 WEB 管理界面的 LOGO

- 支持邮件/syslog 方式输出告警日志
- 支持 SNMP 方式输出系统信息
- 提供排错工具：ping、TCP 端口检测、UDP 端口检测、路由跟踪等
- 需提供用户、资产、授权的增删改查等 API 接口，允许第三方平台调用堡垒机的 API 接口，实现用户、资产、权限自动同步到堡垒机，简化堡垒机配置工作量

2.4.17 综合日志审计

- ≥ 6 个工作管理口（千兆电口）；
- 内存 $\geq 64\text{GB}$ ，磁盘 $\geq 4\text{T} \times 4$ raid5（支持 raid1、raid5）；
- 双电源；
- 启动：默认硬盘启动；
- 支持审计 ≥ 500 个日志源；
- 平均处理能力（每秒日志解析能力 EPS） ≥ 10000 EPS；
- 峰值处理能力（每秒日志解析能力 EPS） ≥ 14000 EPS。
- 独立完成审计日志采集，不依赖于设备或系统自身的日志系统；
- 审计工作不影响被审计对象的性能、稳定性或日常管理流程；
- 审计结果存储于独立存储空间；
- 自身用户管理与设备或主机的管理、使用、权限无关联；
- 提供全中文 WEB 管理界面，无需安装任意客户端软件或插件；
- 采用解决方案包上传对产品进行功能扩展，无需要代码开发；
- 支持 kafka 日志接收转发、大数据安全域同步、APT 沙箱报告转发等大数据联调功能，Kafka 收发支持 SSL 加密。
- 支持手动或按周期自动备份系统配置，可随时对系统资产等配置进行还原操作，且自动备份周期与备份包个数可配；支持系统配置备份自动备份至远程服务器。
- 支持通过界面自定义字段方式实现与第三方平台的数据共享，快速满足第三方平台个性化分析和对接需求。
- 支持配置平台信息，包括 logo、名称及版权信息。
- 支持 Syslog、SNMP Trap、HTTP、ODBC/JDBC、WMI、FTP、SFTP 协议日志收集；支持阿里云 SLS 日志的采集。
- 可通过接收协议限制日志接收速率，包括 Http 接收、syslog 接收、SNMPtrap 接收、TCP 接收、WMI 接收、aliyun 接收。

- 支持使用代理(Agent)方式提取日志并收集，安装包支持界面下载，且安装支持可视化向导。
- 支持对 Agent 进行统一管控，包括卸载、升级、启动及停止操作，支持将日志收集策略统一分发。
- 支持目前主流的网络安全设备、交换设备、路由设备、操作系统、应用系统等；
- 支持常见的虚拟机环境日志收集，包括 Xen、VMWare、Hyper-V 等。
- 可以基于日志等级进行过滤；
- 可以通过自定义配置过滤掉用户不关心的日志；
- 支持对收集到的重复日志进行自动聚合归并，减少日志量；
- 支持可由用户定义和修改的日志聚合归并逻辑规则；
- 支持将收集到的日志转发，当原始日志设备无法设置多个日志服务器时，可以通过本系统的日志转发功能将日志转发到其他日志存储设备；
- 日志支持文本方式输出给第三方平台，进行数据共享；
- 内置 5000+解析规则，支持对收集的 5000+设备类型日志进行解析（标准化、归一化），解析维度多达 200+，解析规则可以根据客户要求定制扩展；
- 可对日志进行细粒度解析
- 支持基于跨设备的多事件关联分析；
- 具备安全评估模型，评估模型基于设备故障、认证登录、攻击威胁、可用性、系统脆弱性等纬度加权平均计算总体安全指数。安全评估模型可以显示总体评分、历史评分趋势。安全评估模型各项指标可钻取具体的评分扣分事件。；
- 内置设备异常、漏洞利用、横向渗透、权限提升、命令执行、可疑行为 6 大类 50+子类的安全分析场景；
- 进行关联分析的规则可定制；三维关联分析；支持通过资产、安全知识库、弱点库三个维度分析事件是否存在威胁，并形成关联事件。
- 可设置日志存储备份策略。包括系统日志保存期（天）、磁盘使用率百分比等策略；
- 支持日志本地备份及恢复；
- 支持日志备份自动传送到远程服务器；
- 支持从远程仓库恢复数据；
- 支持 FTP、SAMBA、NFS 和 FILE，4 种方式的远程服务器。
- 支持 B/S 模式管理，支持 SSL 加密模式访问；

- 支持按日期、时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、操作对象、技术方式、技术动作、技术效果、攻击类型、地理城市等参数进行过滤查询；
- 支持用任意关键字对所有事件进行高性能全文检索；
- 支持可指定多个查询条件进行组合查询；
- 支持将查询的条件存储为查询模版，方便再次使用；
- 支持亿级的日志里根据做任意的关键字及其它的检索条件，在秒级里返回查询结果。
- 支持监控设备自身 CPU、内存、磁盘等工作运行状况；
- 通过在目标主机上安装 Agent 程序，支持监测目标主机的 CPU 利用率、内存使用率、磁盘使用率、磁盘使用情况、流量等信息；
- 支持以下对象的性能监控：
 - 操作系统 - Windows、Linux、Aix、FreeBSD、HP-UX/Tru64、Max OS、Sun Solaris
 - 数据库 - MySQL、Oracle
 - 应用服务器 - Weblogic、Tomcat
 - Web 服务器 - Apache
- 支持应用性能历史详情回溯查看；
- 支持监控 LINUX/Windows 操作系统,MySQL、Oracle、Apache 数据库的，监控应用服务器（Tomcat、Weblogic）等所有参数
- 支持从 IBM Rational AppScan 导入资产弱点漏洞信息；
- 内置 73000+条 CVE 漏洞数据知识库；
- 内置数十项符合 OWASP 的 Web 漏洞数据知识库。
- 内置 GeoSec 地理安全子系统，内置世界以及中国安全 GIS 地图；
- 支持用地理地图展示来源威胁的趋势；
- 支持用地理地图展示目的威胁的趋势；
- 支持在地理地图上标注威胁事件的发生分布；
- 内置 IP 地址到经纬度的转换库；
- 支持以地理信息类进行统计的数据报表；
- 可预设置安全告警策略；
- 支持数据阈值设置，超过阈值将产生告警；
- 可以通过邮件、短信和屏幕显示进行告警；

- 自动防止在短时间内大量发送报警信息(告警抑制);
- 具备报警合并和在一个时间段内抑制报警次数的能力;
- 支持磁盘空间阈值告警, 资产性能监控异常告警, 远程仓库状态监测可告警。
- 内置合规性报表 1000+种;
- 内置 SOX、ISO27001、WEB 安全等解决方案包;
- 内置完善的等级保护合规报表;
- 内置综合性自动化审计报告;
- 支持用户自定义报表;
- 自定义的报表支持多个统计维度的数据集合;
- 支持报表导出为 PDF 和 Word 格式文件。
- 根据三权分立的原则和要求进行职、权分离, 对系统本身进行分角色定义, 如管理员只负责完成设备的初始配置, 规则配置员只负责审计规则的建立, 审计员只负责查看相关的审计结果及告警内容; 日志员只负责完成对系统本身的用户操作日志管理;
- 系统自带自身管理日志;
- 用户支持双因子认证登录, 双因子认证令牌支持绑定至具体用户;
- 提供一键式故障排除功能;
- 提供自助式的升级接口, 支持对产品升级、规则升级。
- 注册用户资产时, 提供自动发现识别能力;
- 资产拓扑支持按照实际的用户环境进行编辑发布并可以和资产进行绑定, 拓扑可以显示资产采集的事件数量被采集资产的状态等信息。
- 支持分布式部署, 支持页面一键添加子节点, 自动进行绑定添加, 采集器可以选择同步日志范围, 按需转发数据;
- 支持集中式管理和升级模式;
- 支持分级管理模式;
- 采用 B/S 架构操作方式, 无需客户端安装。

2.4.18 数据库审计

- 产品采用专用工控机硬件架构, 非普通 PC 服务器, MTBF(平均故障间隔时间) ≥ 65000 小时;
- 处理器采用 Intel 高性能 CPU, 内存 $\geq 16\text{GB}$ DDR3 1600Mhz, 硬盘 $\geq 4\text{TB}$ (2T*2),

支持 RAID1，最大支持扩展到 4T*4 硬盘；

- 网络端口：
- 支持监听接口扩展，配备至少 6 个千兆电口管理口；
- 支持千兆网络环境下的监听能力，标配至少 4 个千兆电口和 4 个千兆光口；
- 支持最大扩展至 8 电 8 光或 16 电或 16 光共 16 个千兆以太网口。
- 支持的数据库实例个数：12
- 审计性能：峰值 SQL 处理能力 ≥ 20000 条/秒；
- 硬件最大吞吐量 2000Mbps，最大纯数据库流量 200Mbps，标配日志存储数 20 亿条；
- 审计日志检索能力 ≥ 1500 万条/秒。
- 旁路部署模式下无须在被审计数据库系统上安装任何代理即可实现审计；
- 可在云环境操作系统中安装软件代理
- 在目标数据库安装 agent 解决云环境、虚拟化环境内部流量无法镜像场景下数据库的审计；
- 支持分布式部署，管理中心可实现统一配置、统一报表生成、统一查询、一键批量升级所有节点；
- 管理中心和探测器都可存储审计数据，实现大数据环境下磁盘空间的有效利用和扩展；
- 支持 IPv4/IPv6 双栈审计；
- 支持和 ES 平台对接，将审计日志和告警日志存储在 ES 系统中，并支持通过页面查询日志。
- 支持 Oracle、PostgreSQL、SQLServer、DB2、Informix、Sybase、MySQL、MariaDB、SybaseIQ 等主流数据库的审计；
- 支持 GuassDB、Teradata、人大金仓（Kingbase）、达梦（DM）、南大通用数据库（Gbase）、Oscar、K-DB 等国产数据库的审计；
- 支持 MongoDB、Hbase、Hive、impala、ElasticSearch、HDFS、Cassandra、greenplum、LibrA、graphbase、cache、Redis、HANA、ArangoDB、Neo4j、OrientDB 等非关系型数据库的审计
- 支持主流业务协议 HTTP、HTTPS、Telnet、FTP 的审计；
- 可以通过导入证书的方式实现审计和防护，支持对 SQLServer（2005 及以上版本）数据库；

- 可以通过导入证书的方式实现 MySQL5.7 及以上版本采用了加密协议通讯的审计；
- 支持对各种协议自动识别编码及在 web 界面手工配置特定编码。
- 支持数据库操作表、视图、索引、存储过程等各种对象的所有 SQL 操作审计；
- 审计信息能够记录执行时长，影响行数、执行结果描述与返回结果集
- 支持数据库请求和返回的双向审计，特别是返回字段和结果集、执行状态、返回行数、执行时长、客户端工具、主机名等内容，支持通过返回行数控制返回结果集大小
- 支持跨语句、跨多包的绑定变量名及绑定变量值审计；
- 支持超长 SQL 语句（最长 4M）审计
- 支持自动发现流量中的数据库信息，简化配置。
- 支持审计记录中敏感数据的模糊化处理，内置常见敏感数据掩码规则，支持自定义；
- 产品具有内置规则，规则类型有 sql 注入、账号安全、数据泄露和违规操作等，并可依据规则进行邮件告警
- 内置安全特征库不少于 900 条，如 SQL 注入、缓冲区溢出等
- 可自定义审计规则，审计规则至少支持 18 个条件；
- 规则各条件之间支持与或非逻辑关系；
- 支持内置安全规则单独升级
- 支持信任规则，信任规则至少支持 18 个匹配条件。
- 具有高效的查询性能，后台采用全文检索引擎检索；
- 查询条件易于使用，审计查询条件均为非正则表达式形式进行；
- 支持基于数据库访问日期、时间、源/目的 IP、来源、数据库名、数据库表名、字段值、数据库登录账号、SQL 关键词、数据库返回码、SQL 响应时间、数据库操作类型、影响行数等条件的审计查询；
- 支持在审计日志中一键添加过滤规则，支持在告警规则中一键添加信任规则和规则白名单
- 设置日志检索条件时，检索条件可根据历史信息自动弹出，检索条件支持源 IP、目的 IP、客户端工具、数据库名、数据库账号等，输入检索条件时支持智能联想
- 支持告警分析功能
- 系统内置多种报表模板库，报表不少于 20 种；
- 报表支持严格按照塞班斯（SOX）法案、等级保护标准要求生成多维度综合报告；
- 支持按照时间曲线统计流量、在线用户数、并发会话、DDL 操作数、DML 操作数、

执行量最多的 SQL 语句等报表；

- 支持性能分析，准确提炼出 SQL 语句执行频率和执行时间异常的报表；
- 支持基于表维度的报表分析，表分析报表支持通过桑基图展示对该表的访问情况；
- 支持 HTML、PDF、PNG、Word 等格式的报表导出；
- 支持报表页面信息钻取。
- 可依据客户端工具名、数据库用户名、客户端 IP、操作系统用户名、客户端主机名、数据库名、操作类型、服务器 IP 等配置行为模型，并可查看相应告警日志；
- 可通过桑基图展示访问数据库的路径，路径包括数据库账号、IP 地址、客户端工具、数据库名、表明等；
- 支持根据在线数据最小保留天数和在线数据的磁盘空间占比自动清理早期数据；
- 支持对在线数据的备份，支持调整备份压缩级别，支持展示数据备份进度；
- 支持将审计日志通过 FTP/SFTP 的方式外送，支持自定义在线数据备份时间周期，支持从 FTP/SFTP 上恢复数据，恢复数据支持进度展示；
- 提供审计策略和系统配置信息的单独导入、导出功能。
- 支持用户界面告警、邮件、短信、钉钉、SYSLOG、微信方式告警；
- 采用 B/S 架构管理；
- 支持系统安全配置（登录超时、用户登录失败锁定策略、密码强弱策略、密码有效时间）；
- 支持 NTP 时间同步，客户端浏览器时间同步、SNMP（V1、V2、V3）网络管理协议；
- 支持系统资源使用率触发式系统告警，且告警支持通过页面、SYSLOG、邮件、短信、钉钉、微信方式输出。
- 支持在审计管理端批量安装、卸载、重新安装审计代理；
- 支持在审计管理端启动、停止、挂起 Agent；
- Agent 支持设置 CPU 亲和性、最大资源使用率限制（CPU、内存）
- 支持根据系统 CPU 使用率、系统内存使用率、系统 I/O 使用率自动熔断；
- Agent 支持按照客户端工具、数据库账号过滤审计日志；
- Agent 支持在 RDP 或 SSH 登录数据库服务器运维时，审计原始登录人员的 IP 地址；
- Agent 支持设置抓包过滤串、回环网口抓包；
- 支持在审计页面直接升级或回退已安装在数据库服务器上的 Agent
- 功能全面 API 化，支持第三方调用（需要提供 API 功能列表）。

- 支持在管理节点上管理数据库资产、审计规则、报表订阅、告警通知等；
- 支持在管理节点查询所有审计节点的日志信息；
- 支持在管理节点上监控所有审计节点的状态信息，包括 CPU 使用率、内存使用率、数据库流量、磁盘使用率、审计日志数、告警日志数等信息；
- 支持管理中心和审计节点手工同步配置信息；
- 支持在管理中心直接升级审计节点；
- 管理中心和审计节点统一 license。
- 可提供客户端访问 Web 服务器的 URL 和应用服务器访问数据库的 SQL 语句关联功能；
- 支持通过部署 agent 实现 javaweb 环境 100%准确关联。
- 支持对 SQL 语句进行业务化翻译
- 支持资产组管理；
- 支持分组管理，分组管理包含 IP 组、应用用户组、对象组、时间组、数据库账号组；
- 支持一键取证；
- 支持区分历史会话和在线会话；
- 支持 LDAP 用户认证；
- 支持配置过滤规则，过滤规则包含 IP 过滤、SQL 模板过滤和自定义过滤，自定义过滤条件不少于 28 个条件；
- 在页面支持 ping、traceroute、nc 命令测试连通性；
- 支持路由配置。
- 支持英文界面
- 内置排错平台，支持一键检测系统的关键信息
- 内置运维终端，可实现日志查看、设备状态检查、执行 SQL 语句、执行常用命令、特权运维等能力
- 支持系统引擎管理，支持租户化管理

2.4.19 主机安全防护系统与终端防病毒系统（服务器）

- 具备防护系统 1 套，主机安全防护系统 50 套，终端防病毒系统（2500 套）
- 支持当前待处理高危风险展示，包括弱口令、待处理病毒、待处理漏洞数据，并支持一键跳转到对应处理页面

- 支持控制台动态更新显示全网终端安全状态分布，包括：终端总数、在线终端数、防护中终端数、异常设备数；
- 支持查看当前安全防护信息数据，包括渗透追踪防护、勒索防护数据、病毒防护数据、系统登录防护数据、web 请求防护数据
- 支持查看当前 top 5 风险资产、top 5 威胁 ip、top 5 威胁区域
- 支持实时查看当前安全动态
- 只支持自定义安全策略、安全策略可继承，内置多个初始策略模板，包括防护模板、审计模板
- 支持通过对终端制定模板的方式做到一键策略下发
- 支持对 CPU 使用率监控、内存占用率监控、磁盘读写监控、上下行流量监控。
- 支持对 CPU、内存、磁盘读写、网络上下行流量达到配置阈值时告警。支持对 CPU、内存达到一定阈值时客户端进行熔断。
- 支持网络通信全时监控。
- 支持自动收集终端资产信息，包括：计算机名称、内核版本、操作系统、处理器、主板、内存、硬盘、显卡、终端版本、病毒库版本、最近更新时间
- 支持自动收集终端资产：监听端口、运行程序、账号、软件、启动项等信息，并支持从资产的维度和信息的维度去查看数据，支持数据的导出
- 支持对本机的扩展行为（信息收集、权限提升）进行监测，防止提权行为和信息泄露。
- 识别渗透过程中的隧道代理（端口映射、端口转发、内网代理），可阻断隧道代理搭建行为。
- 对失陷后主机远控持久化行为进行检测（反弹 shell、远程控制），可阻断远控。
- 对内网的恶意攻击行为进行识别（漏洞利用、横向移动），可阻断恶意探测行为。
- 可对渗透的收尾阶段的数据清除行为进行识别和阻断。
- 支持防端口扫描，锁定恶意的端口扫描，并记录告警。
- 支持扫描后对高危漏洞进行自动修复。
- 支持设置对修复完成后的补丁文件进行删除。
- 支持对系统登录行为进行一定的限制，可设置单个 IP 请求时间、登录失败次数、IP 临时锁定时间。
- 违规外联支持黑、白名单双模式，白名单模式可配置是否允许访问特定的网站和地址；黑名单模式可自定义恶意 IP，支持黑名单告警和阻断。

- 支持反渗透监控，包括横向渗透的危险操作等。
- 支持网站漏洞防护，防护内容包括 SQL 注入、XSS、应用程序漏洞及自定义规则。
- 支持智能检测防御 CC 攻击，并可进行高、中、低三档设置。
- 内核级防火墙（业务间流量东西向隔离）功能，包括 IP、端口、协议、流向等细粒度权限控制。
- 支持流量画像，支持全网流量可视化。
- 支持登录防护，包括以系统账号为粒度的异常登录防护、支持五个任意维度（任意 IP，任意域名，任意计算机名，任意时间）的系统登录访问策略设置。
- 支持显示隐藏的系统账户。
- 具有系统漏洞扫描和修复功能，提供真实漏洞补丁：
 - 1.在补丁依赖关系上支持重启验证机制（保证补丁安装的稳定性）。
 - 2.管理中心可作为补丁服务器，支持管理中心可上网和不可上网两种情况。提供离线补丁下载器，按需智能获取内网所需补丁。
- 具备为用户提供 Windows 漏洞修复的热补丁列表能力。
- 支持扫描的漏洞类型包括但不限于操作系统漏洞（Windows、Linux 等）、数据库漏洞（MySQL 等）、Web 容器漏洞（Tomcat、Apache、Ngnix 等）及其他组件漏洞。
- 支持对文件变化的审计。
- 移动存储介质管理：
 - 1.支持管理员对入网的移动存储介质进行注册，可以对已注册的移动介质进行管理，包括授权、启用、停用、删除、导出注册列表、行为监控及审计等。
 - 2.支持客户端自主申请移动存储介质注册，管理员统一对申请进行审批。
 - 3.支持管理员设置自动审批客户端注册请求。
 - 4.支持从资产维度、设备维度对存储介质的权限进行精细化设置，同一设备可针对不同的资产设置不同的读写权限，有效控制不明来历的移动存储可能带来的病毒传播等隐患。
 - 5.支持设置 U 盘的使用时间。
- 支持对无线网卡、光驱、软驱、打印机、调制解调器、红外设备、蓝牙设备、摄像头、鼠标、键盘、手机/数码设备的权限管理。
- 支持对 USB 接口、串口/并口、1394 控制器、PCMCIA 等接口的控制。
- 支持开启进程黑名单，阻止不受信任的程序启动和生成，同时支持路径和 MD5 两种

形式。

- 支持开启白名单，对白名单内的文件的操作进行放行。
- 支持对资产的远程端口进行修改，并支持自动添加本机系统防火墙策略。
- 支持对文件 HASH、IP、域名、邮箱等 IOC 指标进行动静态鉴定，通过和云端威胁情报进行碰撞，实时返回威胁结果。
- 联动威胁情报，支持对外联 IP、DNS 解析、可疑文件进行实时情报鉴定，实现风险一站式实时监测。
- 支持文件实时监控，在文件执行、文件修改、存储介质连接时自动触发。
- 支持多种扫描模式包括极速模式、低资源占用模式设置，且低资源占用模式可自定义 CPU 使用率。
- 支持多引擎设置，包括默认引擎、深度扫描引擎。
- 支持对压缩包扫描及深度进行设置，默认 9 层深度。
- 支持对文件扫描进行跳过，默认 50M 以上文件进行跳过。
- 支持自定义病毒处理方式，包括自动处理、记录、删除。优先对病毒文件进行修复，并将修复前的病毒文件进行备份。
- 支持对顽固流行病毒进行智能拦截。
- 针对 Windows 系统，提供内核级的数据防护能力，保护文件不被恶意修改、加密等，可自定义配置保护的文件及目录，支持设置例外进程。
- 提供专门的勒索风险评估功能。
- 提供专门的针对未知勒索病毒的防御引擎，并提供功能开关项。对于未知勒索病毒确保无法加密。同时支持白名单设置。
- 提供专门的挖矿风险评估工具。
- 提供专门的挖矿实时防御工具，并提供功能开关。
- 支持病毒立即处理，对于无法普通隔离的病毒文件进行处理并加入隔离区，或动态移动到信任区。
- 支持部分病毒感染文件的修复功能，对于二进制文件可剥离感染部分，保证应用正常使用。
- 支持查杀映像劫持类型的病毒。
- 支持查杀防范网页中的恶意代码。
- 支持对压缩文件、打包文件进行查杀病毒（默认支持 9 层压缩扫描，可根据用户需求

增加扫描层数）。

- 支持运行文件的病毒查杀。
- 支持支持图片、视频等多媒体文件的病毒查杀。
- 支持查杀各类 Office 文档中的宏病毒、夹带型木马。
- 支持对扫描发现的网马进行自动查杀设置。
- 支持在线、离线病毒库升级。
- 支持下发文件、安装应用程序、远程执行命令。
- 支持对屏幕拍照泄密数据的行为进行溯源。
- 支持在客户端自定义设置需要拦截的弹窗。
- 告警类型包括：护网高级威胁、系统防护、网络防护、Web 应用防护。
- 告警内容至少包括：资产名称、IP 地址、日志类型、风险概况、风险评级、事件发生时间等详细内容。
- 告警方式包括：邮件告警、Syslog、短信告警及 SNMP trap。
- 支持病毒库、补丁库的离线升级及在线升级；支持管理平台、终端软件安装包、终端软件更新包、系统漏洞库、弱口令库的离线升级。
- 客户端程序支持在线热升级，升级之后旧版本驱动等程序无残留。
- 管理平台支持一键设置客户端卸载密码、一键卸载监控端、一键解除绑定、一键停止/恢复所有防护、一键关闭/重启主机、一键重启客户端、一键迁移资产。
- 支持导出已安装客户端程序的资产清单。
- 支持导出日志。
- 能够通过统一的管理中心对多个服务器或主机进行监控。
- 能实时检测工作组件的工作状态以及系统关键资源的运行状态。
- 能对服务器或主机节点进行分组管理。
- 支持多级中心部署，查看所有下级控制中心的资产部署情况以及风险数据。
- 支持通过 web 页面进行客户端推广部署，推广页面支持自定义
- 支持生成报表并且导出，包括 PDF、HTML、DOC。
- 支持采集多种日志，包括防护日志、操作日志、运维日志。
- 支持自定义日志保存路径，自定义设置日志保留时间。
- 支持多级用户管理：租户管理员、租户。
- 支持自定义创建用户角色以及权限。

- 至少支持以下帐号管理功能：帐号创建、帐号授权、帐号属性修改和帐号删除。
- 进行身份认证，用户切换角色时，必须进行重新认证。
- 支持超时重新认证机制，并能够定义用户认证尝试的最大允许失败次数。
- 支持 SSL 的 Web 界面。
- 管理中心支持支持 Windows 系统部署及 Linux 系统部署。
- Linux 客户端支持批量安装。
- Windows 客户端支持静默安装。
- Windows 支持在 cmd 命令下进行在线安装。
- 能展示各个服务器或主机节点的信息。
- 能监测节点遭受网络攻击的趋势信息。
- 支持监控用户和应用实时流速，包括用户名、应用名、用户组、上行速率、下行速率、总速率、会话数等信息，帮助管理员快速甄别网络异常行为；支持提供重大事件应急响应预案。
- 提供 3 年的病毒库、程序升级服务。
- 对于新发现的病毒、零日漏洞，厂商能够于 24 小时内作出响应，及时通知用户，并提供专门应急预案、处置工具或专杀工具。
- 支持 7*24 小时威胁溯源服务。

2.4.20 工业监测审计系统

- 标准 2U 机架式，冗余双电源，配置于 4 个千兆电口、6 个千兆 SFP 光口，1 个 MGMT 以太网管理端口，1 个 EXT 以太网扩展端口。

2.4.21 漏洞扫描系统

- 标准 1U 机架式，标配 6 千兆电口+2 千兆光口+2 万兆光口，支持 2 个接口扩展槽，2T 企业级硬盘，系统扫描范围：256；系统扫描任务并发：2；系统扫描 IP 并发：100
- Web 网站扫描：30 个；Web 扫描任务并发：1
- 数据扫描任务并发：1
- 口令猜解任务并发：1。

2.4.22 网闸

- 2U, 4 个万兆光口, 4 个千兆电口, 2 串口, 内外网单元各配置不少于 4 个 USB 2.0 端口、 1 个 RJ45 MGMT 网络管理端口、1 个 RJ45 HA 专用接口, 内外网单元各配置不少于 1 个 RJ45 Console 管理端口, 双机热备。
- 吞吐量 $\geq 900\text{Mbps}$, 带宽 $\geq 6\text{G}$, 最大并发连接数 ≥ 20 万, 满负荷运行的时延时间 $\leq 1\text{ms}$ 。
- 系统内部剥离 TCP/IP 协议, 数据还原成文件, 采用私有协议实现内部数据传输。
- 采用经安全加固的 LINUX 系统。
- 系统透明支持 TCP/IP 以上的应用层协议, 网页浏览、数据库复制、文件交换、数据库访问、邮件、消息服务等无需二次开发。
- SQLServer、Oracle 等的单、双向数据交换; 支持周期复制、实时复制、增量更新等多种同步方式; 支持设定同步时间和同步周期; 支持复杂网络部署, 不需改变用户网络环境
- 支持 SQLServer、Oracle、Sybase、DB2 等常见数据库应用
- 支持客户端、samba、NFS、ftp、有客户端等多种文件交换方式; 支持文件复制、移动、增量等多种传输方式; 支持断点续传
- 文件特征检查: 具备自有非第三方的文件特征检查功能, 能够对 EXE、DOC、DOCX、XLS、XLSX、TXT、BMP、MP3、S48、AVI-divx、AVI-JPEG、WMV 等文件格式进行检查, 防止伪造后缀名或增加二进制执行代码的恶意文件传输。
- 支持安全文件上传下载, 安全 Cookie 保护
- 支持多种方式的访问控制, 包括源, 目的 IP、子网、时间、时间端口、内容过滤;
- 可实现基于 IP+MAC 绑定的客户端访问控制;
- 支持 MAC 认证用户: 应用于 DHCP 网络环境下
- 防止多个 DOS 攻击源一起攻击某台服务器
- 支持单、双向可选的访问控制
- 具备多网络接口端口聚合功能;
- 具备双机热备功能和负载均衡功能。
- 支持 SAT 和透明应用代理两种工作模式, 支持混合工作模式; 支持将多个网络接口网桥方式
- 设备具备黑白名单功能, 能够通过黑白名单实现数据交换安全访问控制策略。
- 系统可存储和审计包含: 系统日志; 管理日志;

- 网络活动日志；入侵报警及处理日志；
- 访问控制日志；
- 支持日志信息输出到 SysLog、WebTrends 外部日志系统；
- 采用 B/S 结构或串口管理
- GUI 图形管理界面
- 集中设备管理系统
- 基于角色管理员分级管理
- 提供液晶面板显示系统工作状态
- 管理平台采用图形化的网络行为监控；可实时监控网络流量、并发连接数、违反规则尝试次数等统计信息。

2.4.23 室内、室外无线 AP（802.11ac）

- 支持 802.11a/b/g/n/ac/ax Wave 2 标准
- 支持 2.4GHz/5GHz 双频段工作
- 支持最大接入用户数 ≥ 512 个
- 支持 2×2 MIMO，4 条空间流
- 整机速率 ≥ 1.775 Gbps
- 支持 1 个 GE 电接口
- 内置智能天线，提供官网链接和截图证明
- 资质要求：必须持有国家无线电委员会入网核准证

2.4.24 机房防腐防爆无线 AP（802.11ac）

- 支持 802.11a/b/g/n/ac/ax Wave 2 标准
- 支持 2.4GHz/5GHz 双频段工作
- 支持最大接入用户数 ≥ 512 个
- 支持 2×2 MIMO，4 条空间流
- 整机速率 ≥ 1.775 Gbps
- 支持 1 个 GE 电接口
- 内置智能天线，提供官网链接和截图证明
- 资质要求：必须持有国家无线电委员会入网核准证
- 采用聚碳酸酯等防腐防爆材料，符合生产机房的抗打击要求及耐腐蚀要求。

2.4.25 无线控制器

- 转发性能：≥10 Gbps
- 最大管理 AP 数：≥512，配置 license，满足可管理 AP 需求
- 端口要求：提供 2 个 10GE SFP+接口，20 个千兆 RJ45 电口和 4 个千兆 Combo 口
- 无线漫游：支持 AC 内漫游，支持跨 AC 间漫游，支持跨 VLAN 的三层漫游
- 可靠性：支持设备冗余备份功能，可支持 1+1 或 N+1 备份，并支持主备 AC 间配置同步
- 本设备所配置功能应满足本项目整体竣工验收前所需业务需求

2.4.26 4G/5G 上网路由器

- 支持 5G NR，兼容 FDD/TDD-LTE，具备宽温工作能力，满足不同应用场景要求
- 转发性能≥2Mpps；防火墙性能：800Mbps；加密性能：100Mbps；NAT 会话数：25 万；WAN 以太口：1*GE（电）+ 2*GE（光）；LAN 以太口：4*GE（电）；内置单 5G 模组，支持 5G NR、TDD/FDD-LTE、WCDMA
- 全面支持 AD-WAN 能力，包括：SR/SRv6, Openflow, Telemetry, Netconf、零配置等
- 丰富的 VPN 互联技术，包括：IPSec、L2TP、ADVPN 等，支持国密办加密算法，提供各种应用场景下的 VPN 安全接入
- 支持千种以上 PC 和手机常见应用的识别和控制，对网络流量进行精细化控制；支持上网日志审计，满足无线非经审计要求
- 支持 Openflow、Telemetry, Netconf 等管理控制协议，可被 H3C AD-WAN 控制器和第三方控制器管理控制 支持 Segment Routing、VxLAN、EVPN 等转发业务，可定义多种转发模型，满足不同业务组网需求
- 支持 URL、U 盘、DHCP 零配置部署，满足批量、低成本、快速开局要求
- 支持 DPI 应用识别能力，对网络流量进行精准识别，实现网络流量可视化、自定义和灵活调度
- 支持 SRv6 功能，具备 EVPN L2VPN over SRv6 Policy/BE, EVPN L3VPN over SRv6 Policy/BE 组网能力

- 支持基于报文五元组过滤，ASPF 状态过滤、MAC 地址过滤、URL 过滤、基于域防火墙、IPS 等
- 多样化的 VPN 技术，包括：IPsec、L2TP、GRE、ADVPN、MPLS VPN，以及多种 VPN 技术的叠加使用
- 终端接入安全：支持 802.1X/Portal 认证，EAD 安全检查认证、终端 MAC 地址认证等
- DDoS 攻击防范：支持防 SYN 泛洪、ACK 泛洪、RST 泛洪、UDP 泛洪等攻击
- 设备管理安全：支持基于角色权限管理，能够基于角色进行资源分配、用户与角色的对应，灵活安全控制权限 支持控制平面流量限制：支持基于已知协议类型、自定义协议报文进行流量控制和过滤
- 专业的防火墙功能：支持包过滤防火墙、状态防火墙、基于域的防火墙等安全过滤功能
- 内置高速稳定的 5G/4G 接口，支持所有运营商的 TDD/FDD 4G LTE 网络 支持 SIM/USIM 卡与设备绑定的功能
- 支持 GPS 定位功能
- 支持短信开局和管理维护
- 支持 Telnet/SSH、SNMP、TR069、Netconf 等多种网络管理方式
- 支持 EAA（内嵌自动化架构）功能，具备 TCL 和 Python 脚本自编程能力，可对系统软硬件部件的内部事件、状态进行监控，出现特定事件时自动执行预先定义的脚本

2.4.27 网络准入控制管理系统

- 标准机架式硬件服务器，标配 6 个千兆电口，可扩展支持 4 个端口千兆光纤扩展卡或 2 个万兆光口扩展卡，支持≥1TB 存储空间，提供断电保护机制，如心跳、Bypass。
- 服务器采用 Linux 操作系统，支持 B/S，C/S 双重管理架构，便利易操作管理设计。
- 支持旁路部署方式，产品兼容多网段、有线\无线 AP、跨 NAT 等复杂网络环境，设备部署过程中不改变原有网络结构。

- 支持独立部署准入控制服务器，单独管理特定网段。
- 支持与终端安全管理系统采用统一平台进行管理，不得使用两个客户端程序。
- 支持 802.1X、端口流镜像准入、DHCP、MAB、SNMP、VLAN 和 portal 认证等多种常用准入控制技术，同时必须提供 VARP 端口级准入控制技术。
- 支持对合法入网设备建立授信画像，同时可以针对特殊设备和服务器设置白名单放行，白名单设备访问特定服务器地址不进行网络阻断处理。
- 支持无客户端模式下终端注册，通过 web 页面引导填写注册信息，支持管理员审批/自动审批入网。
- 系统支持客户端和无客户端双部署模式，移动设备支持安装 APP 后自动入网。支持独立或并行使用多种准入方式，搭建网络边界级、端口级、应用级网络阻断控制功能。
- 支持自动拨号认证、设备绑定 VLAN 组功能等准入技术。
- 支持资产识别、设备防伪冒、关键设备管理、安全风险分析、资产管理等功能。
- 支持禁止终端计算机连接非可信网络及非可信计算机，终端计算机只允许与授权计算机进行网络通信，非法接入或未授权计算机无法与终端计算机通信。终端计算机脱网后禁止连接除准入服务器外的所有网络。
- 具备公安部计算机信息系统安全专用产品销售许可证、信息技术产品安全测试证书。

2.4.28 网络安全二、三级系统等保测评与评估

- 取得公安主管部门颁发的信息系统安全等级保护备案证明：办公网、智能网取得网络安全等级保护二级证明，生产网取得网络安全等级保护三级证明。

3 统一时钟系统

3.1 系统概述

具体详见各图纸及其设计说明。

3.2 系统结构及功能要求

具体详见各图纸及其设计说明。

3.3 主要设备技术要求

3.3.1 NTP 网络时钟服务器

- (1) 1. 网络协议: NTPv1. v2. v3&v4 (RFC1119&1305)、SNTP (RFC2030) Telnet (RFC854)、TIME (RFC868) DAYTIME (RFC867)
- (2) 服务器性能: GPS 时钟参考模式, 一级网络时间服务器, 同步精度 $10\mu\text{s}$;
用户终端同步授时精度: $1\text{--}10\text{ms}$ (局域网典型值);
- (3) 用户容量: 可支持数万台客户端
- (4) NTP 请求量: 14000 次/秒
- (5) 可作为从服务器同步于其他 NTP 网络时间服务器

3.4.2 网络中心母钟

- (1) 类型: 支持 NTP 协议, 支持网络校时, 当 GPS 信号中断时, 采用内置原子钟守时; 可手动或软件设置时区和地址码; 手动北斗/GPS 信号源设置; 备冗余电源设计, 支持双机热备份, 无需主备切换器, 无需人工干预, 自动切换时间 $\leq 10\text{ms}$, 系统具有更高的可靠性, 支持远程操作维护; 内置高性能铷振荡器, 守时精度: $\leq 1\text{ms}/\text{年}$ 。
- (2) 授时精度: 1PPS 秒脉冲输出精度: $\leq 100\text{nsec}$ (平均);
- (3) LCD 显示: 卫星接收与锁定状态, 当前位置的经纬度, 海拔高度参数及内部主控设备电压参数;

3.4.3 GPS (北斗)接收装置

- (1) 授时精度: 卫星信号锁定时优于 $\pm 1 \times 10^{-10}$ 秒; 卫星信号失锁 2 小时内优于 $\pm 1 \times 10^{-9}$ 秒
- (2) 频率稳定度: 卫星信号锁定时优于 10^{-10} 秒 (24 小时); 卫星信号失锁时优于 10^{-9}

秒（24 小时）

- （3） 对标准时间的同步误差： $\leq 1 \mu s$
- （4） 信号传输距离 ≤ 1200 米
- （5） 工作温度： $-15^{\circ}\text{C} \sim 60^{\circ}\text{C}$ ；湿度：30%~85%（不结露）
- （6） MTBF：7 万小时

3.4.4 GPS（北斗接收天线）

- （1） 电压驻波比应满足:1.5:1
- （2） 带宽应满足： $< \pm 5 \text{ MHz}$
- （3） 阻抗应满足： $< 50 \text{ ohm}$
- （4） 最高增益应满足： $> 3\text{dBic}$ ，基于 $7 \times 7\text{cm}$ 地平面 % Volum
- （5） 增益范围应满足： $> -4\text{dBic}$ ， $-90^{\circ} < 0 < +90^{\circ}$ ，over 75B

3.4.5 单面数字子钟

- （1） 接口:RJ45 或 RS422，可接受外部 NTP 时码；
- （2） 功能:自动消除机械累积误差，连续运行无累积误差；无校信号自动切换到内部时钟状态。
- （3） 独立计时精度： $\leq \pm 0.5$ 秒/天
- （4） 力距:800 克/厘米
- （5） 环境要求:工作温度 $0 \sim +50^{\circ}\text{C}$ ，20%~85%（不结露）
- （6） 电源电压:220V $\pm 10\%$ 电源频率：50Hz $\pm 5\%$

4 公共广播系统

4.1 系统概述

具体详见各图纸及其设计说明。

4.2 系统结构及功能要求

具体详见各图纸及其设计说明。

4.3 系统总体技术要求

1) 系统设备必须按《强制性产品认证管理规定》的要求，通过国家 3C 认证。兼做消防广播，必须要有 3CF 认证。

2) 系统应具有公共广播及背景音乐广播的功能。

3) 系统主机热备份状态，应具备对设备、线路、功放故障自动检测功能，且所有的检测工作均以不中断正常广播为前提，系统还应具有故障信息提示功能。

4) 功率放大设备是对输入信号进行处理和放大的设备，要求具有很好的信噪比和频率响应，当主功率放大器发生故障时，能自动切换到备用功率放大器工作。

5) 功率放大器的额定输出功率至少应按不少于回路负载功率的 1.5 倍配置。同时，每组功率放大器组须配备备用功率放大器，备用功率放大器按不小于该功率放大器组的最大回路的功率放大器容量配置。

7) 设置背景音乐工作站，可根据需要检测功放的工作状态。功放的工作状态均在系统界面直观显示，同时也可以通过通道选择开关及监听扬声器监听功放输出的内容。

8) 系统应能实时发布语音广播，且传声器优先。

9) 系统单台广播功率放大器失效不应导致整个广播系统失效。系统单个扬声器失效不应导致整个广播分区失效。

11) 系统应具备对设备、线路、功放等的工作及故障进行自动检测提示功能，且所有的检测工作均以不中断正常广播为前提。

12) 系统应可灵活地对广播呼叫站信号、本地音源和广播分区进行编组，任何一个广播音源信号均可自由地分配至任一广播分区或多个广播分区。

13) 系统电声性能指标满足以下要求：应备声压级 ≥ 85 dB，声场不均匀度 ≤ 10 dB，漏出

声衰减 $\geq 15\text{dB}$ ，设备信噪比 $\geq 70\text{dB}$ ，语言清晰度 $\geq 85\%$ ，传声增益 $\geq -10\text{dB}$ 。

14) 公共广播区域声场内播放的声压级比广播区域的背景噪声高出 10~15dB。

15) 广播主机支持消防强切功能，消防时强制切换公共广播系统静音。

4.4 主要设备技术要求

4.4.1 服务器及工作站

服务器、工作站要求采用专业服务器、工作站（计算机），具体技术参数要求统一按第 14 章“服务器、工作站通用技术要求”中要求。

4.4.2 CD/MP3 播放器

- 1) 应具有 CD 及 MP3 播放功能。
- 2) 应具有动态 VFD 显示功能。
- 3) 应具有曲目直选功能。
- 4) 应具有通电自动播放功能。
- 5) 应具有远程控制功能，能够实现定时播放。

4.4.3 广播控制主机

- 1) X86 架构，支持千兆网口上联。
- 2) 可管理音频输入及音频输路数详系统图要求。
- 3) 主机应内置数码播放器，播放器容量不少于 2G，播放内容可根据用户需求配置。
- 4) 主机可在 19 寸标准机柜内安装。
- 5) 主机应配置音频优先输入模块，确保消防强切功能。
- 6) 主机应配置远程遥控寻呼话筒、CD/MP3 播放器、调谐器等的音频输入模块。
- 7) 主机应具有诊断系统，可定时检测监视系统及功放的工作状况，并具有事件日志纪录功能。
- 8) 主机应具有密码保护功能，确保系统安全稳定操作、运行。
- 9) 系统应配置管理工作站及管理软件，实现对系统的编程及监测。系统脱离它所连接的电脑而独立工作。
- 10) 投标人应根据系统容量及功能要求，并结合设计图纸，配置相应的模块。

4.4.4 功率放大器

- 1) 通道数量：四通道、双通道

- 2) 功率：以图纸要求为准
- 3) 每通道的音量、音调可独立调节。
- 4) 定压输出：200V，100V，70V 可切换。
- 5) 应具有工作状态显示功能。
- 6) 应具有强插控制输入口。
- 7) 应可与广播矩阵主机通信，交换控制信号和状态信息
- 8) 主要技术指标：
 - (1) 频宽：40Hz 至 16KHz（ $\pm 3\text{dB}$ ）。
 - (2) 失真度：小于 1%（1KHz）。
 - (3) 信噪比： $>80\text{dB}$ 。
 - (4) 输入阻抗： $100\text{K}\Omega$ 。

4.4.5 室内喇叭

- 1) 功率：3W/6W
- 2) 工作电压 100/70V
- 3) 灵敏度高： $91\pm 2\text{dB}$
- 4) 最大声压级：97dB
- 5) 频宽：100Hz ~16kHz
- 6) 安装方式：壁挂、吸顶、嵌入

4.4.6 室外音柱

- 1) 额定功率：30W
- 2) 标称阻抗： 6Ω
- 3) 频率响应：80Hz-20KHz@-10dB
- 4) 灵敏度：90dB(1M/1W)
- 5) 覆盖角度：水平:45°；垂直:20°
- 6) 喇叭单元：2.5"中低音 \times 8+1" \times 2 高音

5 安防集成应用综合管理（平台）系统

5.1 系统概况

采用安全防范综合管理（平台）系统（以下简称安综平台），通过一个平台整合视频安防监控、出入口控制、停车场管理、电子围栏等系统模块功能，综合管控，统一管理。

5.2 视频安防监控系统模块

5.2.1 系统概况

详见各图纸及其设计说明。

5.2.2 系统构成

详见各图纸及其设计说明。

5.2.3 系统总体技术要求

- 1) 系统中使用的设备必须符合国家法律法规和现行强制性标准的要求，并经法定机构检验或认证合格。
- 2) 系统的制式应与我国的电视制式一致。图像质量的性能指标应符合《视频安防监控系统工程设计规范》（GB50395-2007）第 5.0.10 的规定。
- 3) 系统画面显示应能任意编程，并可自动或手动切换；同时应可对视频输入进行编组，用以对各组不同视频的显示及操作进行组别限制。
- 4) 系统的显示画面及录像图像画面应有摄像机的编号、部位、记录时间和日期显示，文字显示应采用简体中文。
- 5) 磁盘中录像图像资料应保存不少于 31 天，建筑出入口以及室外的监控图像信号应以全高清质量保存。
- 6) 系统应具有与其他系统联动的接口，当其他系统向视频系统给出联动信号时，系统应能按照预订工作模式，切换出相应部位的图像至指定监视器上，并能启动视频记录设备，其联动响应时间不大于 3 秒。
- 7) 系统录像设备应可记忆多个同时到达的报警，并按报警的优先级别进行排序。用于报警处理的监视器最先显示最高优先级的报警，并可逐个显示直到清空。当有多台监视器用于显示报警图像时，则监视器可按设置依次同时显示多路报警图像。
- 8) 系统应配置独立的工作站及管理软件控制，实现软件对系统的控制和视频画面调用显

示。

- 9) 系统应具备独立的软件控制功能，实现软件对管理、存储、显示设备的控制和视频画面调用显示；并可通过键盘和鼠标应可对各摄像机、云台、镜头、监视器进行控制。
- 10) 系统应设置操作员权限，被授权的操作员具有不同的操作权限、监控范围和系统参数。
- 11) 系统应支持用户群组、用户权限、系统权限、设备操作权限的分级细致管理，满足系统用户、角色、权限的复杂管理需求；权限管理最少达到 6 级以上。
- 12) 系统应具有对主要设备的自检功能，故障报警。
- 13) 管理服务器软件功能要求：
 - 应自动实现自动容错功能，无须人工干预。
 - 所有命令均可通过鼠标点击菜单或图标的方式来完成。
 - 应可对云台、镜头、辅助开关、显示设备进行控制。
 - 应具备完整的电子地图显示功能，支持包括 AutoCAD 在内的多种图形文件格式，并具有图标编辑功能。
 - 可管理的前端摄像机数量应大于 10000 台。
 - 控制信号以纯 IP 的方式传输，与数据流、视频流分开。
- 14) 系统应具有系统信息存储功能，在供电中断或关机后，对所有编程信息和时间信息均应保持。
- 15) 系统软件应具备标签功能，可手动添加、根据报警事件自动生成视频标签，标签与视频录像同步保存，方便事后检索。
- 16) 系统应具有对设备的自检功能，故障报警。
- 17) 图像切换时间小于 0.5 秒，不同监控点的图像切换时间小于等于 0.5 秒。
- 18) 系统响应时间：小于等于 2 秒（从控制中心的图像工作站或键盘发出控制指令开始，直到视频监视屏的摄像机画面开始变化所需的时间）。
- 19) 系统应具备视频移动侦测与视频信号丢失报警功能，可根据用户的使用要求增加该功能设置。

5.2.4 主要设备技术参数要求

5.2.4.1 摄像机

- (1) 投标人应按照招标图纸要求，并根据摄像机安装的位置及现场条件选配摄像机，保证系统清晰稳定。一般情况下摄像机采用定焦距、定方向的固定安装方式，选用日/夜型自动光圈镜头并配置防护罩

- (2) 采用日/夜转换型彩色摄像机。
- (3) 背光强烈的出入口采用超宽动态彩色摄像机。
- (4) 摄像机灵敏度应能适应防护目标光照度的变化，适应防护目标的最低照度条件。
- (5) 摄像机应采用外同步、内同步、电源同步或其他形式的同步方式，以保证在图像切换时不产生明显的画面跳动。
- (6) 室外安装的摄像机应做相应的防雷措施。
- (7) 所有摄像机不低于 1080P（1920x1080）（200 万像素）。

5.2.4.2 人脸识别电梯 200 万半球摄像机性能参数要求

- (1) 传感器：≥1/3 英寸 CMOS 传感器，星光级
- (2) 有效像素：200 万像素
- (3) 最大分辨率：≥1920×1080（1080P），25 帧
- (4) 压缩标准：H. 265/H. 264/M-JPEG 等编码格式，支持不同压缩格式下的双码流
- (5) 最低照度：彩色≤0.001Lux，黑白≤0.0001Lux
- (6) 自动曝光，自动白平衡，AGC 增益，背光补偿
- (7) 支持 ONVIF、GB/T28181 标准
- (8) 镜头：2.8/4.0/6.0mm 定焦
- (9) 前端支持智能分析功能
- (10) 网络接口：RJ45 10/100 自适应以太网口
- (11) 电源：POE 供电或 12VDC/24VAC，50Hz（在电梯轿厢顶现场取 AC220V 电源，设备应自带变压整流装置）
- (12) 防电场或磁场干扰，电磁兼容性符合国家标准。
- (13) 环境条件：工作温度：-10℃~50℃，工作湿度：10%~95%RH（无冷凝）
- (14) 支持 3 种深度智能功能：人脸检测、行为分析

5.2.4.3 人脸识别日夜型 200 万半球 IP 摄像机性能参数要求

- (1) 传感器：≥1/3 英寸 CMOS 传感器，星光级
- (2) 有效像素：≥1920×1080（200 万像素）
- (3) 最大分辨率：≥1920×1080（1080P），25 帧
- (4) 压缩标准：H. 265/H. 264/M-JPEG 等编码格式，支持不同压缩格式下的双码流
- (5) 最低照度：彩色≤0.001Lux，黑白≤0.0001Lux
- (6) 自动曝光，自动白平衡，AGC 增益，背光补偿

- (7) 支持 ONVIF、GB/T28181 标准
- (8) 镜头：2.8/4.0/6.0mm 定焦
- (9) 前端支持智能分析功能
- (10) 网络接口：RJ45 10/100 自适应以太网口
- (11) 电源：POE 供电或 12VDC/24VAC，50Hz
- (12) 防电场或磁场干扰，电磁兼容性符合国家标准。
- (13) 环境条件：工作温度：-10℃~50℃，工作湿度：10%~95%RH（无冷凝）
- (14) 支持 3 种深度智能功能：人脸检测、行为分析

5.2.4.4 人脸识别日夜型 200 万枪式 IP 摄像机性能参数要求

- (1) 传感器：≥1/3 英寸 CMOS 传感器，星光级
- (2) 有效像素：≥1920×1080（200 万像素）
- (3) 最大分辨率：≥1920×1080（1080P），25 帧
- (4) 压缩标准：H.265/H.264/ M-JPEG 等编码格式，支持不同压缩格式下的双码流
- (5) 宽动态：≥105dB（室外摄像机要求）
- (6) 支持 ONVIF、GB/T28181 标准
- (7) 彩色：≤0.001Lux，黑白：≤0.0001Lux
- (8) 自动曝光，自动白平衡，AGC 增益，背光补偿，走廊模式可选
- (9) 镜头：4.0/6.0/8.0/10.0mm 定焦
- (10) 红外功能：红外距离≥50 米
- (11) 前端支持智能分析功能
- (12) 网络接口：RJ45 10/100 自适应以太网口
- (13) 电源：POE 供电或 12VDC/24VAC，50Hz
- (14) 无电场或磁场干扰
- (15) 防护等级：≥IP67（室外摄像机要求）
- (16) 环境条件：工作温度：-10℃~50℃，工作湿度：10%~95%RH（无冷凝）
- (17) 支持 2 种深度智能功能：人脸检测、行为分析

5.2.4.5 室内人脸识别日夜型 200 万快球 IP 摄像机性能参数要求

- (1) 摄像元件：CMOS 传感器（要求≥1.8”英寸 CMOS 传感器）星光级
- (2) 有效像素：≥1920×1080（200 万像素）
- (3) 最大分辨率：≥1920×1080（1080P），25 帧

- (4) 自动变焦： ≥ 33 倍光学变焦
- (5) 压缩标准：H. 265/H. 264/M-JPEG 等编码格式，支持不同压缩格式下的双码流
- (6) 宽动态： $\geq 105\text{dB}$
- (7) 支持 ONVIF、GB/T28181 标准
- (8) 最低照度：彩色： $\leq 0.001\text{Lux}$ ，黑白： $\leq 0.0001\text{Lux}$
- (9) 自动光圈、背光补偿，自动增益控制
- (10) 手动速度： $1\sim 90^\circ/\text{秒}$ ，预置位速度： $\geq 360^\circ/\text{秒}$
- (11) 水平扫描角度： 360° 连续，垂直扫描角度 $0^\circ \sim 90^\circ$
- (12) 水平旋转速度 $0.5^\circ \sim 250^\circ/\text{秒}$ ，垂直旋转速度 $0.05^\circ \sim 200^\circ/\text{秒}$ ；
- (13) 编程预置点不少于 128 个，预置点水平移动速度不低于 $230^\circ/\text{秒}$ ，垂直移动速度不低于 $180^\circ/\text{秒}$ ，设置的数据断电不丢失；
- (14) 功能：巡航路线、预置位、自动翻转、自动归位、密码保护、隐私区域设定、2 组报警输入、2 组继电器输出。
- (15) 支持前端智能分析功能
- (16) 接口：RJ45 10/100 自适应以太网口
- (17) 电源：12VDC/24VAC，50Hz（系统提供 AC220V 电源，设备应自带变压整流装置）
- (18) 无电场或磁场干扰
- (19) 环境条件：工作温度： $-10^\circ\text{C} \sim 50^\circ\text{C}$ ，工作湿度： $0\% \sim 95\%\text{RH}$ （无冷凝）
- (20) 防护等级： $\geq \text{IP67}$ 。（室外摄像机要求）
- (21) 支持吊架、天花内嵌（半球）、立杆安装的安装方式。
- (22) 支持 2 种深度智能功能：人脸检测、行为分析

5.2.4.6 室外日夜型 400 万快球 IP 摄像机性能参数要求

- (1) 摄像元件：CMOS 传感器（要求 $\geq 1.8''$ 英寸 CMOS 传感器）星光级
- (2) 有效像素： $\geq 2560 \times 1440$ （400 万像素）
- (3) 图像分辨率： $\geq 2560 \times 1440$ （1440P），25 帧
- (4) 自动变焦： ≥ 33 倍光学变焦
- (5) 压缩标准：H. 265/H. 264/M-JPEG 等编码格式，支持不同压缩格式下的双码流
- (6) 宽动态： $\geq 105\text{dB}$
- (7) 支持 ONVIF、GB/T28181 标准
- (8) 最低照度：彩色： $\leq 0.001\text{Lux}$ ，黑白： $\leq 0.0001\text{Lux}$

- (9) 自动光圈、背光补偿，自动增益控制
- (10) 手动速度：1-90° /秒，预置位速度：≥360° /秒
- (11) 水平扫描角度：360° 连续，垂直扫描角度 0° ~90°
- (12) 水平旋转速度 0.5° —250° /秒，垂直旋转速度 0.05° —200° /秒；
- (13) 编程预置点不少于 128 个，预置点水平移动速度不低于 230° /秒，垂直移动速度不低于 180° /秒，设置的数据断电不丢失；
- (14) 功能：巡航路线、预置位、自动翻转、自动归位、密码保护、隐私区域设定、2 组报警输入、2 组继电器输出。
- (15) 支持前端智能分析功能
- (16) 接口：RJ45 10/100 自适应以太网口
- (17) 电源：12VDC/24VAC，50Hz（系统提供 AC220V 电源，设备应自带变压整流装置）
- (18) 无电场或磁场干扰
- (19) 环境条件：工作温度：-10℃~50℃，工作湿度：0%~95%RH（无冷凝）
- (20) 防护等级：≥IP67。（室外摄像机要求）
- (21) 支持吊架、天花内嵌（半球）、立杆安装的安装方式。
- (22) 支持 2 种深度智能功能：人脸检测、行为分析

5.2.4.7 室外星光级 800 万全景 IP 摄像机性能参数要求

- (1) 摄像元件：CMOS 传感器（要求≥1.8”英寸 CMOS 传感器）星光级
- (2) 有效像素：800 万像素
- (3) 图像分辨率：≥3840*2160，25 帧
- (4) 自动变焦：≥33 倍光学变焦
- (5) 压缩标准：H.265/H.264/M-JPEG 等编码格式，支持不同压缩格式下的双码流
- (6) 宽动态：≥120dB
- (7) 支持 ONVIF、GB/T28181 标准
- (8) 最低照度：彩色：≤0.001Lux，黑白：≤0.0001Lux
- (9) 自动光圈、背光补偿，自动增益控制
- (10) 手动速度：1-90° /秒，预置位速度：≥360° /秒
- (11) 水平扫描角度：360° 连续，垂直扫描角度 0° ~90°
- (12) 水平旋转速度 0.5° —250° /秒，垂直旋转速度 0.05° —200° /秒；
- (13) 编程预置点不少于 128 个，预置点水平移动速度不低于 230° /秒，垂直移动速度

不低于 180° /秒，设置的数据断电不丢失；

- (14) 功能：巡航路线、预置位、自动翻转、自动归位、密码保护、隐私区域设定、2 组报警输入、2 组继电器输出。
- (15) 支持前端智能分析功能
- (16) 接口：RJ45 10/100 自适应以太网口
- (17) 电源：12VDC/24VAC，50Hz（系统提供 AC220V 电源，设备应自带变压整流装置）
- (18) 无电场或磁场干扰
- (19) 环境条件：工作温度：-10℃~50℃，工作湿度：0%~95%RH（无冷凝）
- (20) 防护等级：≥IP67。（室外摄像机要求）
- (21) 支持吊架、天花内嵌（半球）、立杆安装的安装方式。
- (22) 支持 4 种深度智能功能：人脸检测、人脸比对、周界布防、人数统计

5.2.4.8 热成像双光谱筒型网络摄像机性能参数要求

- (1) 热成像像素：分辨率：256×192；焦距：10mm；视场角：18° ×13.5°
- (2) 可见光像素：分辨率：2688×1520；焦距 8mm；视场角：39.4° ×22.1° 最大分辨率：≥1920×1080（1080P），25 帧
- (3) 压缩标准：H. 265/H. 264/ M-JPEG 等编码格式，支持不同压缩格式下的双码流
- (4) 支持 ONVIF、GB/T28181 标准
- (5) 测温精度：±2℃或量程的±2% ℃ （取最大值）
- (6) 测温范围：-20℃~550℃自动曝光，自动白平衡，AGC 增益，背光补偿，走廊模式可选
- (7) 车辆周界最远报警距离（以 4 米*1.4 米为准）：300m；目标物最远测温距离（以 0.1 米*0.1 米为准）：17m
- (8) 支持 15 米红外补光
- (9) 网络接口：RJ45 10/100 自适应以太网口
- (10) 电源：POE 供电
- (11) 无电场或磁场干扰
- (12) 防护等级：≥IP67（室外摄像机要求）
- (13) 环境条件：工作温度：-40℃~70℃，工作湿度：10%~95%RH（无冷凝）
- (14) 支持 3 种深度智能功能：越界入侵、区域入侵、进入/离开区域

5.2.4.9 室内人脸识别防腐防爆日夜型 200 万快球 IP 摄像机性能参数要求（生产房间）

- （1）摄像元件：CMOS 传感器（要求 ≥ 1.8 英寸 CMOS 传感器）星光级
- （2）有效像素： $\geq 1920 \times 1080$ （200 万像素）
- （3）最大分辨率： $\geq 1920 \times 1080$ （1080P），25 帧
- （4）自动变焦： ≥ 33 倍光学变焦
- （5）压缩标准：H.265/H.264/M-JPEG 等编码格式，支持不同压缩格式下的双码流
- （6）宽动态： $\geq 105\text{dB}$
- （7）支持 ONVIF、GB/T28181 标准
- （8）最低照度：彩色： $\leq 0.001\text{Lux}$ ，黑白： $\leq 0.0001\text{Lux}$
- （9）自动光圈、背光补偿，自动增益控制
- （10）手动速度： $1\text{--}90^\circ/\text{秒}$ ，预置位速度： $\geq 360^\circ/\text{秒}$
- （11）水平扫描角度： 360° 连续，垂直扫描角度 $0^\circ \sim 90^\circ$
- （12）水平旋转速度 $0.5^\circ \text{--} 250^\circ/\text{秒}$ ，垂直旋转速度 $0.05^\circ \text{--} 200^\circ/\text{秒}$ ；
- （13）编程预置点不少于 128 个，预置点水平移动速度不低于 $230^\circ/\text{秒}$ ，垂直移动速度不低于 $180^\circ/\text{秒}$ ，设置的数据断电不丢失；
- （14）功能：巡航路线、预置位、自动翻转、自动归位、密码保护、隐私区域设定、2 组报警输入、2 组继电器输出。
- （15）支持前端智能分析功能
- （16）接口：RJ45 10/100 自适应以太网口
- （17）电源：12VDC/24VAC，50Hz（系统提供 AC220V 电源，设备应自带变压整流装置）
- （18）无电场或磁场干扰
- （19）环境条件：工作温度： $-10^\circ\text{C} \sim 50^\circ\text{C}$ ，工作湿度： $0\% \sim 95\text{RH}$ （无冷凝）
- （20）支持吊架、天花内嵌（半球）、立杆安装的安装方式。
- （21）支持 2 种深度智能功能：人脸检测、行为分析
- （22）防爆相关认证：Ex d IIC T6 Gb /Ex tD A21 IP68 T80 $^\circ\text{C}$
- （23）支持 IP68 防护等级，IK10 防暴等级。

5.2.4.10 室内外人脸识别防腐防爆日夜型 200 万枪式 IP 摄像机性能参数要求

- （1）传感器： $\geq 1/3$ 英寸 CMOS 传感器，星光级
- （2）有效像素： $\geq 1920 \times 1080$ （200 万像素）
- （3）最大分辨率： $\geq 1920 \times 1080$ （1080P），25 帧

- (4) 压缩标准：H. 265/H. 264/ M-JPEG 等编码格式，支持不同压缩格式下的双码流
- (5) 宽动态： $\geq 105\text{dB}$ （室外摄像机要求）
- (6) 支持 ONVIF、GB/T28181 标准
- (7) 彩色： $\leq 0.001\text{Lux}$ ，黑白： $\leq 0.0001\text{Lux}$
- (8) 自动曝光，自动白平衡，AGC 增益，背光补偿，走廊模式可选
- (9) 镜头：4.0/6.0/8.0/10.0mm 定焦
- (10) 红外功能：红外距离 ≥ 50 米
- (11) 前端支持智能分析功能
- (12) 网络接口：RJ45 10/100 自适应以太网口
- (13) 电源：POE 供电或 12VDC/24VAC，50Hz
- (14) 无电场或磁场干扰
- (15) 防护等级： $\geq \text{IP67}$ （室外摄像机要求）
- (16) 环境条件：工作温度： $-10^{\circ}\text{C}\sim 50^{\circ}\text{C}$ ，工作湿度：10%~95%RH（无冷凝）
- (17) 支持 2 种深度智能功能：人脸检测、行为分析
- (18) 防爆相关认证：Ex d IIC T6 Gb /Ex tD A21 IP68 T80 $^{\circ}\text{C}$
- (19) 支持 IP68 防护等级，IK10 防暴等级。

5.2.4.11 镜头性能参数要求

- (1) 按使用环境要求配置定焦镜头、自动光圈定焦镜头、自动光圈变焦镜头。如无特别说明，一般镜头均配自动光圈。
- (2) 定焦镜头之焦距应根据镜头所处位置，视场高度，目标距离及像场高度等参数进行具体计算与选型。
- (3) 变焦镜头之变焦范围应根据镜头所处位置，视场范围等因素决定。
- (4) 手动光圈、直流驱动光圈可选。

5.2.4.12 摄像机防护罩、支架

- (1) 防护罩及其支架须坚固、防锈，应足以承受摄像机及其附件之重量，并具备相当的抗机械性创伤强度。
- (2) 防护罩不应影响摄像机任何性能，包括图面质量及自由运转。
- (3) 防护罩、支架应与装饰效果相协调，并尽可能地隐蔽安装。球形玻璃（或有机玻璃）型防护罩应可隐蔽摄像机的视角。
- (4) 室外护罩应具有降温、除雾、除霜功能，防护等级：IP67。

5.2.4.14 视频管理软件

- 最大支持用户 10000 个，最大支持并发登陆 500 个用户
- 支持用户权限管理；支持用户密码有效时间段进行设置管理，支持用户 IP 绑定，指定 IP 地址用户才能登陆平台
- 支持软授权方式，可以部署在服务器或虚拟机上；
- 支持 BS、CS 客户端以及 IOS、Android 移动端应用；
- 具有高兼容性，支持 ONVIF、国标协议设备接入；
- 支持多网域访问，支持 AD 域
- 支持对监控点、编码设备、门禁设备的在线状态进行设备巡检，并以统计图方式展示巡检结果；
- 支持对监控的图像进行视频质量诊断，图像异常项包括图像偏色、噪声干扰、图像过暗、图像过亮、画面冻结、视频抖动、对比度异常、条纹干扰、视频遮挡、信号丢失、图像黑白、图像模糊、场景变换、视频剧变；
- 能按照指定设备、指定通道进行图像的实时点播，支持点播图像的显示、缩放、抓拍和录像，支持多用户对同一图像资源的同时点播，宜支持基于 GIS 地图的图像点播
- 监控点最多管理容量为 100000 路
- 系统支持国标协议上下级平台级联，支持流媒体集群配置
- 支持对平台内管理的视频设备的在线状态进行检查
- 客户端支持自动在 1/4/6/7/9/16/24 画面分隔模式间进行监控点轮巡预览，轮巡时间可设置，支持全屏显示
- 支持电视墙场景管理和场景切换
- 可对大屏进行 1/4/9/16/25 分屏、拼接、开窗、窗口漫游的操作，通过客户端支持电视墙开窗后支持分割，并可将大屏分屏配置另保存为场景

5.2.4.15 存储设备

- （1）采用 IP SAN 网络存储方式，支持 iSCSI 主机 GE 接口；
- （2）单机柜最大支持磁盘数量 ≥ 72 ，加扩展柜 ≥ 3 （本次建设不考虑扩展柜，用于后期增加存储天数时扩展磁盘）；磁盘：SATAII、8TB、7200rpm、企业级。
- （3）录像存储时间需保证不少于 90 天，容量详见图纸。
- （4）SAN 环境中最大主机连接数 ≥ 256 ，并配置所有连接许可；
- （5）存储设备应具备两个以上千兆 RJ45 端口和 1 个 SFP 千兆光端口；

- （6）支持磁盘热插拔及在线更换故障磁盘，支持启动时磁盘顺序加电和磁盘电源短路保护；
- （7）支持系统内部磁盘可以任意的更换位置；
- （8）支持数据保险箱功能，异常停电时可以继续供电以便把写缓存数据保存到数据保险箱中，完全保证用户数据的完整性；
- （9）支持 RAID 0、1、5、6、10 等 RAID 级别；
- （10）支持流媒体软件模块，支持循环录像的功能，可通过视频存储设备实现视频数据的直接录像、点播、回放和下载。
- （11）客户端图像检索延迟为秒级；
- （12）应适应 5-40 度的工作环境温度；
- （13）必须有 CE/ FCC 认证，并提供认证证书（电子件）；
- （14）MTBF \geq 15 年。

5.2.4.16 流媒体服务器

- 2U 单路标准机架式服务器
- CPU：1 颗 x86 架构 HYGON 处理器，核数 \geq 16 核，频率 \geq 2.4GHz
- 内存：64G DDR4，16 根内存插槽，最大支持扩展至 2TB 内存
- 硬盘：2 块 600G 10K 2.5 英寸 SAS 盘，最高可支持 12 块 3.5 寸(兼容 2.5 寸)热插拔 SAS/SATA 硬盘
- 支持 1 个 M.2 插槽
- 支持 1 个 TF 插槽"
- 阵列卡：标配 SAS_HBA 卡，支持 RAID0/1/10
- 可选 RAID_2G 卡，支持 0/1/5/6/10/50/60，可选支持断电保护
- 网口：4 个千兆电口
- 电源：标配 550W（1+1）白金冗余电源
- 操作系统：正版操作系统

5.2.4.17 智能视频分析服务器

- 支持不少于 20 万张人脸图片，30 个人脸名单库
- 支持不少于 20 万张车牌名单，30 个车牌库,支持黑名单/白名单
- 用于人脸识别分析：支持同时不少于 12 路人脸识别（1080p 视频流）或 20 张/秒图片

流比对报警；

- 用于视频结构化分析：支持同时不少于 12 路视频结构化分析（1080P 视频流），单模块 30 个目标属性提取(无特征向量)；
- 支持前 FR，前 FD+后 FR，前 FR+后 FR，后 FD+后 FR，前结构化+后人脸 FR，前 ITC+后人脸 FR
- 支持不少于 16 路周界防范，每路支持 10 条规则
- 支持前智 ITC 摄像机接入并进行车牌比对
- 支持不少于 800 万条人脸历史抓拍库
- 支持不少于 400 万条周界防范历史抓拍库
- 支持不少于 800 万人体检测历史抓拍库
- 支持不少于 800 万机动车检测历史抓拍库
- 支持不少于 800 万非机动车检测历史抓拍库
- 支持联动录像，抓图，日志，蜂鸣，邮件，预置点，本地报警输出，IPC 报警输出，门禁，语音播报
- 支持不少于硬盘接口 6 个，SATA3.0，单盘最大 10T；
- 网络接口 4 个 RJ-45，10/100/1000Mbps 自适应以太网口（千兆电口）；

5.2.4.18 操作键盘

- 三维遥杆控制，带显示功能，带宏命令按键。
- 它能控制不少于 128 台 PTZ 解码器。
- 应具有保密访问码，允许授权者对键盘进行编程。
- 网络端口：RJ45。

5.2.4.19 光纤收发器

- 遵循 IEEE802.3，IEEE802.3u，IEEE802.3/ab 协议。
- 一个 10/100/1000 自适应 RJ45 接口；1 个 SC 多模光纤接口。
- 自动检测半/全双工模式，光纤传输波长 1310nm（最长可达 2km）。
- LED 指示灯显示电源、链接和数据接。
- 工作温度：-10~70℃，5~90%的湿度（无凝结）。

5.2.4.20 其它设备

投标人认为有必要提供且有利于系统优化的设备或装置，如操作台、电视墙、打印机等。操作台、电视墙规格、尺寸、样式应配合机房装修进行配置，并满足各弱电系统的使用要求。操作台、电视墙具体要求详本技术需求书机房工程章节。

5.3 出入口控制系统模块

5.3.1 系统概况及构成

详见各图纸及其设计说明。

5.3.2 系统基本要求

- 1) 系统中使用的设备必须符合国家法律法规和现行强制性标准的要求，并经法定机构检验或认证合格。
- 2) 系统采取二层分布式网络组网结构，管理层遵循 TCP/IP 协议，区域管理器与系统服务器之间建立双向数据通道。现场层采用标准现场总线协议，并接受系统服务器的管理。
- 3) 系统可储存和管理出入卡的数量不低于 10000 张，卡的使用和进出历史记录系统至少能存储 1 年。
- 4) 系统响应时间：从读卡识别至执行部分开始启闭出入口动作的时间不应大于 0.5 秒；系统报警信息传送至管理中心的响应时间应不大于 2 秒；管理员从管理中心发出启闭指令始至执行部分开始启闭入口动作的时间不应大于 2 秒。
- 5) 系统允许同时登录的管理工作站不得少于 20 台，授权的操作人员数量大于 200 个，登录密码长度不小于 6 位数字或字符。
- 6) 系统对门状态的检测应具有防仿伪（采取如：剪线、短路、并接、串接等手段仿效或模拟门关闭的状态）和防破坏的能力。
- 7) 系统可以在线更新数据库信息并使修改后的数据库生效，控制器不得中断正常工作。
- 8) 系统的信息处理装置应能对系统中的有关信息自动记录、打印、存储，并有防篡改和防销毁等措施。应有防止同类设备非法复制的密码系统，密码系统应能修改。
- 9) 系统应根据门的配置情况，除双向玻璃门采用阳极锁外，电控锁均采用磁力锁，设于消防疏散门的电控锁应采用电控功能的消防专用通道锁。
- 10) 系统与事件记录、显示及识别信息有关的计时部件、管理软件应有校时功能。
- 11) 系统应具有防破坏及故障报警功能，触发报警内容包括：无效卡读卡操作；未使用授权的卡强行通过出入口；未经正常操作使出入口开启；开门时间过长报警；强行打开现场识别装置；主电源中断或短路；系统通信传输发生故障等。

- 12) 报警反应：无效卡刷卡时，读卡器发出报警提示音；无效卡连续 3 次以上刷卡及其他触发报警事件，读卡器发出报警提示音，管理中心主机发出警报声，同时显示该报警的相关信息和相应的控制操作与处理措施，服务器记录该报警事件。
- 13) 系统应具有报警、故障、被破坏、操作等信息的显示记录功能。记录信息应包括事件发生时间、地点、性质等。记录的信息应不可更改。
- 14) 系统应可在线更新数据库信息并使修改后的数据库生效，控制器不应中断正常工作。
- 15) 系统控制器、工作站、服务器之间的网络数据传输应使用加密技术。
- 16) 当供电中断时，系统的密钥信息及各记录信息不得丢失。
- 17) 系统应具有与其他系统联动或集成的输入/输出接口。

5.3.3 主要设备基本技术要求

5.3.3.1 门禁控制器

- (1) 支持 RS485、TCP/IP 有线网络双通信接口，通讯数据采用特殊加密处理，更安全，无泄密之忧
- (2) 支持长度为 20 位的卡号识别和存储
- (3) 支持多门互锁功能、反潜回功能、多重卡开门功能、首卡开门功能、超级卡和超级密码开门、在线升级功能、中心远程开门功能
- (4) 支持读卡器防拆报警、门未关妥报警、门被外力开起报警、开门等待超时报警、胁迫卡和胁迫码报警、限制名单报警、非法卡超次刷卡报警
- (5) 支持防区报警输入，具有防短、防剪功能
- (6) 同时支持 RS485 接口和韦根接口读卡器的接入
- (7) 支持 IC 卡、CPU 卡、二代身份证等多种卡片类型
- (8) 支持脱机记录保持功能和纪录储存空间不足警告功能
- (9) 备用电池设计、主机断电后数据可以保存

5.3.3.2 非接触式感应 IC 卡

- (1) 识别卡为非接触式感应智能卡或 CPU 卡，该卡同时作为员工进出工作区的识别证件。
- (2) 识别卡应能提供不小于 130 亿个唯一的识别码，并采用被动工作方式无需电池，永久使用。
- (3) 识别卡应能接收读卡器发出的写入信息，写入用户需要的相关信息并存储。
- (4) 识别卡应采用 Desfire Ev1 或具有国密算法的卡片类型，卡片内部含多个分区，每

个分区数据可独立应用在一个系统中，实现一卡通用。

- (5) 卡片制成材料应具有很好的韧性、强度、及耐磨性。

5.3.3.3 门禁读卡器

- (1) 读卡器为非接触式感应读卡器。
- (2) 读卡器要求能支持 Mifare 卡片类型，读卡时间： $\leq 1\text{msec}$ 。
- (3) 读卡器支持 IC 卡+密码按键、手机 NFC 识别功能。
- (4) 通讯接口：支持 Wiegand34 以上算法或 RS485 通信。
- (5) 读卡器须做到外型美观，提供多种款式供选择。
- (6) 刷卡后读卡器应对应发出确认音或拒绝音，并在音调上有显著区别。
- (7) 当出现门开启时间过长的情况，读卡器须产生报警提示音。
- (8) 读卡器感应读卡距离不小于 50mm。
- (9) 读卡器至控制器最远距离不应小于 100 米。
- (10) 面板应有 LED 状态指示灯，并带有声音提示，可通过指示灯和声音区分待机、正确刷卡、错误刷卡等信息。
- (11) 读卡器具有防拆报警功能，正常拆卸应使用特殊工具。

5.3.3.4 门禁读卡器（人脸）

- (1) 读卡器为非接触式感应读卡器。
- (2) 读卡器要求能支持 Mifare 卡片类型，读卡时间： $\leq 1\text{msec}$ 。
- (3) 读卡器支持人脸、IC 卡、手机 NFC 及二维码识别。
- (4) 通讯接口：支持 Wiegand34 以上算法或 RS485 通信。
- (5) 读卡器须做到外型美观，提供多种款式供选择。
- (6) 刷卡后读卡器应对应发出确认音或拒绝音，并在音调上有显著区别。
- (7) 当出现门开启时间过长的情况，读卡器须产生报警提示音。
- (8) 读卡器感应读卡距离不小于 50mm。
- (9) 读卡器至控制器最远距离不应小于 100 米。
- (10) 读卡器具有防拆报警功能，正常拆卸应使用特殊工具。

5.3.3.4 防腐防爆门禁读卡器（人脸）

- (1) 读卡器为非接触式感应读卡器。

- (2) 读卡器要求能支持 Mifare 卡片类型，读卡时间： $\leq 1\text{msec}$ 。
- (3) 读卡器支持人脸、IC 卡、手机 NFC 及二维码识别。
- (4) 通讯接口：支持 Wiegand34 以上算法或 RS485 通信。
- (5) 读卡器须做到外型美观，提供多种款式供选择。
- (6) 刷卡后读卡器应对应发出确认音或拒绝音，并在音调上有显著区别。
- (7) 当出现门开启时间过长的情况，读卡器须产生报警提示音。
- (8) 读卡器感应读卡距离不小于 50mm。
- (9) 读卡器至控制器最远距离不应小于 100 米。
- (10) 读卡器具有防拆报警功能，正常拆卸应使用特殊工具。
- (11) 采用聚碳酸酯等防腐防爆材料，符合生产机房的抗打击要求及耐腐蚀要求。

5.3.3.5 门禁读卡器（闸机）

- (1) 读卡器为非接触式感应读卡器。
- (2) 读卡器要求能支持 Mifare 卡片类型，读卡时间： $\leq 1\text{msec}$ 。
- (3) 读卡器支持人脸、IC 卡、手机 NFC 及二维码识别。
- (4) 通讯接口：支持 Wiegand34 以上算法或 RS485 通信。
- (5) 读卡器须做到外型美观，提供多种款式供选择。
- (6) 刷卡后读卡器应对应发出确认音或拒绝音，并在音调上有显著区别。
- (7) 当出现门开启时间过长的情况，读卡器须产生报警提示音。
- (8) 读卡器感应读卡距离不小于 50mm。
- (9) 读卡器至控制器最远距离不应小于 100 米。
- (10) 读卡器具有防拆报警功能，正常拆卸应使用特殊工具。

5.3.3.6 电控锁

- (1) 采用电磁锁，应具有门磁、锁状态信号。
- (2) 承受力应不少于 300 公斤。
- (3) 具有掉电开锁功能。

5.3.3.7 速通闸机人脸识别

- (1) 设备外观：采用 8 英寸 LCD 显示屏，200 万像素双目摄像头，面部识别距离 0.3m-1.5m，支持照片视频防假。

- （2） 设备容量：支持 50000 张人脸白名单，1：N 人脸比对时间 $\leq 0.2\text{S}/\text{人}$ ，支持 50000 张卡片，250000 条记录。
- （3） 认证方式：支持人脸、刷卡的认证方式；支持二维码识别（与访客机可识别二维码类型保持一致）。
- （4） 人脸识别验证速度：不大于 1 秒。
- （5） 支持防假体攻击功能，对视频、电子照片、打印照片中的人脸应不能进行人脸识别。
- （6） 输出接口：电锁*1 个，报警输出*1 个。
- （7） 工作电压： DC 12V/3A，不自带电源。
- （8） 支持支持 IP65 防水等级。