

**T/CECS ×××－20××**

中国工程建设标准化协会标准

智慧园区设计标准

Design standard for intelligent campus

（征求意见稿）

**中国工程建设标准化协会标准**

**智慧园区设计标准**

Design standard for intelligent campus

**T/CECS XXX－20 XX**

主编单位：华为技术有限公司

中国建筑科学研究院有限公司

批准单位：中国工程建设标准化协会

施行日期：20××年××月××日

20××　北　　京

**前　　言**

根据中国工程建设标准化协会《关于印发<2019年第二批协会标准制定、修订计划》的通知》（建标协字[2019]22号）的要求，由华为技术有限公司、中国建筑科学研究院有限公司会同有关单位共同编制而成。标准编制组经过深入调查研究，总结了我国智慧园区工程实践经验，参考国内外有关标准，并在广泛征求意见的基础上，制定本标准。

本标准的主要技术内容是：1.总则；2.术语和符号；3.基本规定；4.感知执行层；5.通信传输层；6.数字平台层；7.智慧应用层；8.安全体系。

请注意本标准的某些内容可能直接或间接涉及专利，本标准的发布机构不承担识别这些专利的责任。

本标准由中国工程建设标准化协会归口管理，由华为技术有限公司负责技术内容的解释。执行过程中如有意见或建议，请寄送华为技术有限公司（地址：广东省深圳市龙岗区坂田华为基地H2，邮编：518129；电子邮箱：designstandard@huawei.com），以供修订时参考。

主 编 单 位：华为技术有限公司

中国建筑科学研究院有限公司

参 编 单 位：

主要起草人员：

主要审查人员：

**目　　次**

[1 **总　　则** 6](#_Toc52304001)

[2 **术语和符号** 7](#_Toc52304002)

[2.1 术语 7](#_Toc52304003)

[2.2 符号与缩略语 8](#_Toc52304004)

[3 **基本规定** 11](#_Toc52304005)

[4 **感知执行层** 12](#_Toc52304006)

[4.1 一般规定 12](#_Toc52304007)

[4.2 设备管理类 12](#_Toc52304008)

[4.3 消防类 13](#_Toc52304009)

[4.4 安全技术防范类 14](#_Toc52304010)

[4.5 信息设施类 16](#_Toc52304011)

[4.6 物联网设备设施类 16](#_Toc52304012)

[4.7 机房工程 17](#_Toc52304013)

[5 **通信传输层** 20](#_Toc52304014)

[5.1 一般规定 20](#_Toc52304015)

[5.2 通信网络设施 21](#_Toc52304016)

[5.3 边缘节点 24](#_Toc52304017)

[6 **数字平台层** 27](#_Toc52304018)

[6.1 一般规定 27](#_Toc52304019)

[6.2 云平台层 27](#_Toc52304020)

[6.3 ICT能力层 28](#_Toc52304021)

[6.4 业务服务层 29](#_Toc52304022)

[7 **智慧应用层** 31](#_Toc52304023)

[7.1 一般规定 31](#_Toc52304024)

[7.2 企业事业服务 32](#_Toc52304025)

[7.3 公共信息服务 32](#_Toc52304026)

[7.4 智慧通行服务 33](#_Toc52304027)

[7.5 公共设施管理 34](#_Toc52304028)

[7.6 绿色健康管理 34](#_Toc52304029)

[7.7 公共安全管理 35](#_Toc52304030)

[7.8 智慧运营中心 36](#_Toc52304031)

[8 **安全体系** 37](#_Toc52304032)

[8.1 一般规定 37](#_Toc52304033)

[8.2 感知执行层安全 37](#_Toc52304034)

[8.3 通信网络安全 38](#_Toc52304035)

[8.4 区域边界安全 38](#_Toc52304036)

[8.5 计算安全 38](#_Toc52304037)

[8.6 网络安全管理中心 39](#_Toc52304038)

[本标准用词说明 40](#_Toc52304039)

[引用标准名录 41](#_Toc52304040)

[条文说明 43](#_Toc52304041)

Contents

**1　General provisions……………………………………………………6**

**2　Terms and symbols…………………………………………………………7**

2.1　Terminology………………………..………………………………7

2.2　Symbols and Abbreviations…..…….……………………………8

**3　Basic requirements……….……………………………………………11**

**4　Sensor & execution layer………………………………………………12**

4.1　General requirements……………………………………………12

4.2　Building automation system……………………………………12

4.3　Automatic Fire alarm system……………………………………13

4.4　Security Technology Protection Systems.………………………14

4.5　Information facility system……..……………………………16

4.6　Device of IoT …………….…………………………………16

4.7　Engineering of electronic equipment plant….……………17

**5　Communication transport layer……………………………………20**

5.1　General requirements……………………………………………20

5.2　Communication network facilities……..………………………21

5.3　Edge node…….………………………….……………………24

**6　Digital platform layer …………………………………………27**

6.1　General requirements…....………………………………………27

6.2　Cloud platform layer…….………………………………………27

6.3　ICT Capability layer……………………….……………………28

6.4　Business service layer……………………….……………………29

**7　Intelligent application layer……………………………………………31**

7.1　General requirements……………..………………………………31

7.2　Service for Enterprise and Public institution………………………32

7.3　Information service for Public…………….……………………32

7.4　Service for Intelligent transport…………….……………………33

7.5　Communal facility management...……………………………………34

7.6　Green management and Managed care….…………………………34

7.7　Public security management…….…………….……………………35

7.8　Control center of Intelligent campus………….……………………36

**8　Security system…………..………………………………………37**

8.1　General requirements……………..………………………………37

8.2　Security of sensor & execution layer………………………………37

8.3　Security of communication network……………….…………………38

8.4　Security of regional border…………………….……………………38

8.5　Computing security.................……………………………………38

8.6　Security operations center……….………………………………39

**Explanation of wording in this standard………………………………40**

**List of quoted standards…………………………………………………41**

**Addition：Explanation of provisions……………………………………43**

1. 总　　则

1.0.1　为了规范智慧园区工程规划、设计，提高智慧园区工程设计及建设质量，制定本标准。

1.0.2　本标准适用于新建、改建和扩建的园区数字化转型的整体规划及具体项目设计，满足园区的智慧化、信息化、绿色健康的设计要求以及经济活动的需求。

1.0.3　智慧园区设计应遵循智慧城市的总体规划，并与总体规划协调一致。

1.0.4　智慧园区设计除应符合本标准外，尚应符合国家现行有关标准的规定。

1. **术语和缩略语**
	1. 术语

2.1.1　智慧园区　intelligent campus

人、物、事、空间、环境等互联互通、数据融合、可持续发展的统一规划区域及其建筑空间，充分利用云计算、5G、物联网、大数据、人工智能等技术，为园区用户和经营管理者提供高效、便捷、舒适、安全、环保的体验，促进业务增值和效率提升。

2.1.2　人工智能 artificial intelligence(AI)

研究、开发用于模拟、延伸和扩展人的智能的理论、方法、技术及应用系统的一门新的技术科学。

2.1.3　新能源　new energy

指传统能源之外的各种能源形式，即刚开始开发利用或正在积极研究、有待推广的能源，如太阳能、地热能、风能、海洋能、生物质能和核聚变能等。

2.1.4　智慧运营中心 intelligent operation center

智慧园区的报告中心、指挥中心、管理中心，应用云计算、大数据、建筑信息模型、数字平台等技术，通过业务分析、辅助决策、风险预警、协同作业、调度指挥等智慧化场景应用，实现园区的可感、可视、可管、可控，实现高效的园区运行、维护、管理、服务。

2.1.5　数字平台 digital platform

融合技术、聚合数据、赋能应用、迭代演进的数字化服务中枢，能够借助物联和信息系统的联接，通过开放、解耦、功能复用、可配置的理念，实现人、机、物、事、环境、空间深入融合，提供贴近场景的可调用、松耦合、弹性的标准化数字服务，使能智慧业务创新和高效运营。

2.1.6　通信网络设施 communication network facilities

用于建立园区信息传输通道，提供高速的信息传输网络，实现感知层数据信息在各种网络的汇总、传输、交换，进而将相关信息进行各系统间整合的设施。

2.1.7　信息管网 information pipeline network

用于敷设信息通信线缆的一种通道，由管道、人（手）孔和建筑物引入管等组成。

2.1.8　光缆线路 optical fiber line

通过光纤将通信信号从一个地点传送到另外一个地点的传输媒介。

2.1.9　边缘计算节点 edge computing node

在网络边缘处或靠近用户侧提供计算能力、存储能力及应用服务的新型计算节点。

2.1.10 边缘网关节点 edge gateway node

在网络边缘处或靠近终端侧提供接入能力、回传能力及计算服务的新型网关节点。

* 1. 缩略语

API（Application Programming Interface）[应用程序](https://baike.baidu.com/item/%E5%BA%94%E7%94%A8%E7%A8%8B%E5%BA%8F)接口

APT（Advanced Persistent Threat）防未知高级威胁

AQI（Air Quality Index）空气质量指数

ATSE （Automatic Transfer Switching Equipment）自动转换开关电器

BAS（Building Automation System ）建筑设备自动化系统

BLE（Bluetooth Low Energy）蓝牙低能耗

DDoS（Distributed Denial of Service） 反分布式拒绝服务攻击

DLP（Digital Light Processing）数字光处理显示屏

DNS（Domain Name System）域名系统

EPS（Emergency power supply）应急电源

ERP（Enterprise Resource Planning）企业资源计划

F5G（Fifth Generation Fixed Network ）第五代固定网络

GIS（Geographic Information System）地理信息系统

HA（Highly Available）高可用性集群

HTTPS（ Hyper Text Transfer Protocol over SecureSocket Layer）超文本传输安全协议

IAM（Identity and Access Management ）身份识别与访问管理

ICT（ Information and Communications Technology）信息与通信技术

IDE（Integrated Development Environment）集成开发环境

IEEE（ Institute of Electrical and Electronics Engineers）电气和电子工程师协会

IGP（Interior Gateway Protocol）内部网关协议

IoT（Internet of Things）物联网

IP（Internet Protocol）互联网协议

IPv6（Internet Protocol Version 6）互联网协议第6版

ITU-T（ ITU-Telecommunication Standardization Sector）国际电信联盟电信标准分局

LoRa（Long Range Radio）远距离无线电

NB-IoT（Narrow Band Internet of Things ）窄带物联网

PKI-CA （Public Key Infrastructure-Certificate Of Authority）公钥基础设施-认证中心

PLC（Power Line Communication）电力线通信

POL（Passive optical LAN）无源光接入局域网

QoS（Quality of Service）服务质量

RFID（Radio Frequency Identification）射频识别技术

SFTP（Secret File Transfer Protocol）安全文件传送协议

SSID（Service Set Identifier）多服务集标识

SSL（Secure Sockets Layer）安全套接字协议

UI（User Interface）用户界面

UPS（Uninterruptible Power Supply）不间断电源

UWB（Ultra-Wide Band）超宽带无线载波通信技术

VLAN（Virtual Local Area Network）虚拟局域网

VPC（Virtual Private Cloud）虚拟私有云

VPN（Virtual Private Network）虚拟专用网络

WAF（Web Application Firewall） 网站应用级入侵防御系统

5G（5th Generation Mobile Networks） 第五代移动通信技术

1. **基本规定**

3.0.1　智慧园区设计应体现以人为本、以服务为中心，以实现园区功能需求为目标，满足园区规划科学、建设有序、运营高效、通行快捷、安全绿色、生活健康的需求。

3.0.2　智慧园区整体架构规划应与园区的整体规划相匹配，应满足本地生态园区、绿色园区、园区区域能源规划和海绵城市的要求。智慧园区技术架构（图3.0.2）应根据园区的部署设施、功能特点、基础条件和应用方式等进行层次化结构设计，包括感知执行层、通信传输层、数字平台层、智慧应用层等。



**图3.0.2 智慧园区技术架构图**

3.0.3　智慧园区的系统配置应根据园区架构长期规划，结合智慧应用需要选择配置平台和系统能力。

3.0.4　智慧园区应通过安全接入、通道加密、数据加密、授权秘钥、隐私保护、日志审计、防攻击等多种技术手段构建园区整体安全体系。

1. **感知执行层**
	1. 一般规定
		1. 感知执行层应对智慧园区的交通、安全、绿色、健康、设备、设施等园区信息进行全面感知，并及时、准确地执行相关指令或展示相关内容，满足智慧园区应用场景需求。
		2. 感知执行层设备应具有唯一设备信息，具有开放、通用的通信接口和协议，满足与通信传输层快捷对接的技术要求。
		3. 感知执行层应选用低误报、低功耗、符合精度及时延要求的设备，应适应传输网络少线化、无线化的发展趋势，应满足物理安全及信息安全的要求。
		4. 感知执行层在通信传输层中断状态下应能够维持基本功能持续运行、进行必要联动，保证消防及各类公共安全系统设施正常运转，宜根据使用需要选用具备相应存储和计算能力的设备。
		5. 感知执行层的设计范围应包括设备管理、消防、安全技术防范、信息设施、物联网设备设施、信息机房六大类子系统或设备设施，各子系统的设计应符合国家现行有关标准的规定。
	2. 设备管理类
		1. 感知执行层宜采集下列设备设施的相关信息：
2. 电气设备：配电柜、变压器、柴油发电机组、UPS、EPS；
3. 空调设备：制冷机组、热泵机组、锅炉、换热机组、换热器、新风机组、热回收机组、空调机组、精密空调、变风量末端、风机盘管、空调水系统水泵、冷却塔；
4. 通风设备：普通送/排风机、排风兼排烟风机；
5. 给排水设备：变频调速给水设备、生活水泵组、生活水转输泵组、排污泵；
6. 新能源设备：太阳能光伏发电、风力发电、充电桩等；
7. 其他设备：电梯、照明、加热器、电动门窗、电动遮阳设施及与工艺相关设备等。
	* 1. 感知执行层宜根据功能需求配置下列感知设备：
8. 感知建筑结构应变、变形和裂缝等的传感器；
9. 水流开关、防冻开关、液位开关、压差开关、高压进线柜开关、低压出线柜开关、母联柜开关、门窗磁开关等；
10. 液体流量计、风流量计、能量表、电表、水表、气表等；
11. 水管温度传感器、水管压力传感器、水管流量变送器、风管温度传感器、风管湿度传感器、风管压力传感器、CO传感器、CO2传感器、风速传感器、环境温度传感器、环境湿度传感器、环境照度传感器、PM2.5/PM10传感器、空气质量传感器、电压变送器、电流变送器、功率变送器、功率因数变送器、室外风力风向变送器、有害气体探测器、有毒气体探测器、环境噪声探测器、漏水探测器等。
	* 1. 感知执行层宜根据功能需求配置下列执行设备：
12. 风阀、开关型风阀执行器、调节型风阀执行器、蝶阀、球阀、水力平衡阀、动态平衡阀、开关型水阀执行器、调节型水阀执行器等；
13. 水泵变频器、风机变频器等。
	1. 消防类
		1. 感知执行层宜采集下列消防信息：
14. 环境信息：烟雾浓度、温度、可燃气体浓度、火焰、电弧；
15. 设备设施信息：配电系统剩余电流、线缆温度、配电箱内温度、消防设备电源的电压、电流、消防水池（箱）的水位、消防水系统的管网水压、气体灭火钢瓶压力、泡沫灭火系统状态、气体灭火系统状态、干粉灭火系统状态、防火门启闭、防火卷帘启闭等信息。
	* 1. 感知执行层应根据消防规范及园区消防安全要求选用下列探测器、传感器：
16. 火灾自动报警类：感烟火灾探测器、感温火灾探测器、火焰探测器、图像型火灾探测器、光束感烟火灾探测器、手动火灾报警按钮、输入模块等；
17. 可燃气体报警类：甲烷探测器、丙烷探测器、一氧化碳探测器等；
18. 电气火灾监控类：剩余电流式电气火灾监控探测器、测温式电气火灾监控探测器、故障电弧探测器、测量热解粒子式电气火灾监控探测器、探测绝缘性能式电气火灾监控探测器、防火限流式保护器等；
19. 消防设备电源监控类：电压传感器、电流传感器、电压/电流传感器、蓄电池状态等；
20. 消防给水监控类：消防水池（箱）温度探测器、消防水池（箱）水位探测器、消防管网压力探测器、消防泵的状态监测设备等；
21. 防烟排烟类：消防应急疏散防烟系统余压探测器、排烟专用探测器、送（补）风空气质量探测器等；
22. 防火门、防火卷帘监控类：门磁开关、防火分隔系统状态监测设备；
23. 气体灭火类：钢瓶压力探测器、消防钢瓶爆裂预警探测器等；
24. 无线传输类：无线感烟火灾探测器、无线感温火灾探测器、无线液位传感器、无线液压传感器、无线手动报警按钮、无线可燃气体报警探测器、用户信息传输装置，无线状态监测仪，无线电气火灾、传统消防接入网关等。
	1. 安全技术防范类
		1. 安全技术防范设计应符合下列要求：
25. 根据防护对象的风险等级及安全管理要求设置感知执行层设备；
26. 有效感知、清晰记录园区内的非法入侵、群体伤害、社会治安等事件，及时准确地反馈至园区运营中心；
27. 设备采集的信息应包括绝对时间，并与智慧园区管理平台进行时钟同步；
28. 设备应可不依赖系统集成平台独立实现基本的报警、联动、记录功能，宜具有依据本地的简单逻辑判断触发执行机构的能力；
29. 对建筑物、园区的主要公共活动场所、通道、重要部位和区域、重要目标等进行有效的图像、声音信息采集，前端设备所采集的图像、声音信息的应满足国家现行有关标准的要求及智能分析的要求；
30. 能支持系统实现图像的结构化数据提取，根据园区安全防范需求对采集的图像、信息数据进行人脸识别、车牌识别、人员/车辆的定位与轨迹追踪、逆行/测速/违停、滞留、越界、物品遗留或丢失、人员热力图、客流统计等智能分析；
31. 设备、设施的安全等级的设计应符合国家现行有关标准的规定。
	* 1. 感知执行层宜根据园区安全防范要求采集下列信息：
	1. 入侵探测和紧急报警类：入侵探测信号、紧急报警信号、求助信号等；
	2. 图像、声音拾取类：图像信号、声音信号、声强信号等；
	3. 目标识别类：人员身份、生物特征、行为、车牌、车型、物品标签、危险品等；
	4. 人体健康信息类：体温；
	5. 人员及物品定位类：人员及物品位置；
	6. 设备状态及控制类：控制指令、设备状态、异常告警等。
		1. 感知执行层宜根据园区安全防范要求采用下列设备：
32. 入侵探测和紧急报警类：各类入侵探测传感器、报警主机及附件、紧急/求助报警设备、声音探测器及复核装置、对讲设备等；
33. 图像、声音拾取类：各类摄像机、声强探测器、拾音器、编码器、处理器等；
34. 目标识别类：出入口控制系统的各类认证介质、识读设备、控制器、执行器，电子巡查系统的各类巡检器、巡更点、识读设备，停车库(场)安全管理系统的各类出入口识读、检测设备、车位占位检测设备、用户端设备，防爆安全检查系统的固定及手持式安检设备等；
35. 人体健康信息类：红外热成像体温监测设备、红外体温检测设备等；
36. 人员及物品定位类：基于Wi-Fi、5G、蓝牙、RFID、UWB、北斗卫星导航等技术的各类设备；
37. 设备状态及控制类：包括各类一体化设备及控制器。
	1. 信息设施类
		1. 信息设施类感知设备主要包括对语音、图像和多媒体信息数据进行采集和输入的设备；执行设备主要包括对语音、图像和多媒体等信息进行呈现的设备。
		2. 信息设施类感知设备包括信息查询机、互动触摸屏、平板电脑、话筒、拾音器等。
		3. 信息设施类执行设备包括扬声器、声/光报警器、LED屏、LCD屏、DLP屏、投影仪、时钟显示器、Wi-Fi智能终端、5G智能终端、交通信号灯、交通诱导牌等。
	2. 物联网设备设施类
		1. 园区宜运用物联网技术实现空间的智慧场景应用。
		2. 园区宜运用物联网技术将相关公共设施智能化，并符合下列要求：
38. 综合杆：宜支持智能照明、智能安防、智能交通、智能监测、新能源、5G基站、园区公共服务等感知与执行设备；
39. 公厕：宜采集空气质量及异味、厕位状态、皂液/厕纸/擦手纸余量、垃圾桶满溢、马桶堵塞、地面浸水、各类机电装置工作状态、耗水量、耗电量、紧急求助信号、客流量、用户评价等信息；宜具备入口导引显示、厕位状态指示、紧急求助声光警报、各类机电装置控制等功能；
40. 垃圾桶：采集垃圾桶位置、满溢程度、倾斜程度，宜包括桶内温度、氨硫有害气体、可燃气体浓度等信息；
41. 井盖：采集井盖位置、倾斜、振动，宜包括井盖开裂状态、井下水位、井下温湿度、井下气体浓度等信息；
42. 消火栓：采集消火栓位置、出水口压力、水流状态、闷盖开/闭状态、倾斜角度等信息。
	* 1. 园区可根据功能需要设置相应类型的机器人，并确定其定位精度、越障高度、移动方式与速度、承载能力、续航时间等参数，机器人宜具有环境识别、定位和地图构建能力，自主导航、运动、自主充电功能，防撞、防跌落设计，设置急停按钮。
	1. 机房工程
		1. 机房工程设计应与智慧园区总体规划相结合，满足用户接入、汇聚和转接服务的需求，应预留通信机房面积，满足各信息业务经营者对设备安装和维护的要求。
		2. 信息机房的位置应符合现行国家标准《智能建筑设计标准》GB50314的要求，不应与变电室、电梯机房、水泵房、厕所、浴室等贴临布置，不得布置在有水房间的正下方。
		3. 应根据园区产业特点和规模，设置消防、安防、运营等类型的集中监控中心及分控室。
		4. 机房工程的设计应符合下列要求：
43. 可采用机柜、布线、供电、制冷、监控等模块化集成方案，满足快速部署，分期扩容、即插即用；
44. 应采用高效供电、制冷部件，宜遵循“先冷设备、后冷环境”的原则，实现冷热通道密闭/隔离，宜采用“园区核心机房、各功能分区分支机房、楼层接入机房”架构；
45. 园区核心机房、各功能分区/部门分支机房、楼层接入机房所采用解决方案宜同时支持本地管理、统一平台集中运维管理。
	* 1. 机房工程设计应根据使用功能、建筑布局、业务性质、管理要求设置信息接入机房（进线间）、信息网络机房、用户电话交换机机房、消防控制室、安防监控中心、弱电间（电信间）、有线电视前端机房、应急响应中心、运营管理中心等智能化系统机房，也可视需求使用园区统一提供的机房设施。
		2. 园区的信息机房应符合现行国家标准《数据中心设计规范》GB50174的规定，楼层设备间布局应满足机柜数量和维护需要，并预留可扩展的面积。
		3. 园区机房工程应结合不同业务的需求，设计不同标准的机房类型满足其对信息机房的使用需求。
46. 核心机房设计宜参考现行国家标准《数据中心设计规范》GB50174中机房标准，可靠性等级不低于B级；
47. 各功能分区/部门分支机房设计宜参考现行国家标准《数据中心设计规范》GB50174中的B级机房标准，部分可参照C级机房标准；
48. 各建筑物的楼层接入机房设计宜参考现行国家标准《数据中心设计规范》GB50174中的C级机房标准。
	* 1. 机房工程包括建筑装饰、供配电、照明、防雷、接地、UPS不间断电源、空调、动力与环境监测、火灾报警及灭火、出入口控制、入侵报警、视频监控、综合布线、系统集成和电磁防护等设计内容。
		2. 机房工程设计应与智能化、电气、空调、给水排水、机房装饰等专业对接，并根据工程施工标段划分情况，明确各方设计界面。
		3. 园区信息机房正常照明度应不低于500lx，事故照明照度应不低于50lx。
		4. 园区信息机房的防雷和接地设计应满足人身安全及电子信息系统正常运行要求，并符合现行国家标准《建筑物防雷设计规范》GB50057和《建筑电子信息系统防雷技术规范》GB50343的相关规定，核心机房宜采用三级防雷保护，通讯专线应进行防雷保护，机房要求采用综合接地方式，接地电阻应≤1Ω。
49. **通信传输层**
	1. 一般规定
		1. 通信传输层应联接物联感知执行层和数据平台层，并实现各类数据的传输、存储等，包括通信网络设施、边缘节点等。
		2. 通信传输层设计应遵循“统一规划、集约建设、资源共享、适度超前”的原则，满足园区信息化、智能化需求。
		3. 信息管网应适应城市建设与信息通信发展的需要，应明确接入园区的通信线路在城市地下空间的位置，协调与城市其它工程管线之间的关系。
		4. 园区的信息管网、光缆线路的设计应符合网络接入的技术与安全要求、保留一定余量并预留相关数据接口。
		5. 园区内管道宜配置物理双路由接入城市主干信息管道。园区内的地下信息管道设计应根据通信业务需求及发展趋势确定管道的总容量，结合园区内综合管道的设置及地理环境条件设计敷设方式和路由。
		6. 园区应建设光纤通信网、4G/5G移动通信网、无线局域网等通信网络设施以保障通信质量，宜按F5G、POL等新技术构架实施通信方案。
		7. 园区接入网应统筹配置，应具有多种类信息业务经营者平等接入的条件，同时满足接入网使用方灵活选择不同经营者的要求。
		8. 园区网络带宽应能支持高清视频数据、图片数据、结构化数据等多维数据的高质量、低延时、高速率传输。
		9. 园区内边缘节点应结合实际业务需求，具备一定的计算、存储能力，以满足用户对边缘智能的远程管控、数据处理、分析决策、就近智能化的诉求。
	2. 通信网络设施
		1. 通信网络设施应包括信息管网、布线系统、园区物联接入网、固定通信网、移动通信网、无线局域网等。
		2. 信息管网设计应符合以下要求：
50. 应以城市发展规划和通信建设总体规划为依据；
51. 对于新建、改扩建的建筑物，楼外预埋通信管道应与建筑物的建设同步进行，并应与共用通信管道相连接；
52. 在终期管孔容量较大的宽阔道路上，宜在道路两侧修建通信管道或通道，并预留过街管道，或根据具体情况建设；
53. 应选择地下、地上障碍物较少、易于维护管道的路由，不宜选在埋设较深的其它管线附近；
54. 不宜与燃气管道、高压电力电缆在道路同侧建设。
	* 1. 布线系统设计应符合以下要求：
55. 应设置布线系统，布线系统包括光纤、光缆、综合布线等；
56. 光纤的选择应符合现行有关国家标准的要求；
57. 光缆中光纤数量的配置应充分考虑到网络冗余要求、未来预期系统制式、传输系统数量、网络可靠性、新业务发展、光缆结构和光纤资源共享等因素；
58. 光缆宜采用G.652光纤；当需要抗微弯光纤光缆时，宜采用G.657光纤；
59. 综合布线设计应满足信息化、智能化发展要求，力求资源共享，避免重复开挖地面，且不应与楼内其他系统产生冲突；
60. 综合布线应满足各种通信与信息业务服务接入的需求，且与建筑智能化同步设计，避免建筑物内管网的重复建设；
61. 宽带网络设计应以F5G、POL建设为主，满足园区信息通信服务需求。
	* 1. 园区物联接入网设计应符合以下要求：
62. 应根据区域内的业务需求，构建园区物联接入网；
63. 应把园区感知子系统通过有线网络、电力线载波网络、Wi-Fi、4G/5G、NB-IoT等接入方式连接起来，进行信息交换和通讯，以实现智能化识别、定位、跟踪、监控和管理；
64. 应具备感知终端的自动发现、设备类型自动识别、终端设备零配置自动入网，满足感知终端即插即用快速联网要求；
65. 应满足在网络中传输物联协议数据无丢失和低网络传输时延的要求；
66. 应基于物联安全要求，对感知终端进行身份认证，实现对认证报文和物联协议报文的加密；以访问业务实施访问权限最小化为原则，园区物联接入网应与办公、生产等网络数据进行隔离；
67. 应具备感知终端接入与管理能力，宜实现感知终端的可视化运维、在线监测、故障预测告警等连接管理；
68. 应具备边缘网关的接入与云化管理能力，宜实现设备认证接入、设备统一升级、在线监测、故障预测告警等管理。
	* 1. 固定通信网设计应符合下列规定：
69. 应满足园区近期与远期业务需求，选择适合的接入设备；
70. 核心交换机设备应满足可靠性要求，并采用双节点冗余设计，关键链路应采用Trunk方式冗余备份或负载分担；
71. 接入层设备宜采用POL设备或框式交换设备，应满足可安装及日常维护要求；
72. 接入层网络设备应具备满足不同终端带宽需求，接入设备应具备基础电信运营企业端口接入能力。
	* 1. 移动通信网设计应符合下列规定：
73. 网络覆盖应结合室外、办公区、室内公共区、出入口区等场景实际需求进行设计，并应满足移动通信信号的覆盖要求；
74. 园区及建筑应预留移动通信基站和室内覆盖系统所需的屋面杆塔设施、机房、管道、供电电源及防雷接地等；
75. 园区应配合基础电信运营企业建设和优化移动网络，其建设应符合现行行业标准《移动通信基站工程技术规范》YD/T 5230的规定；
76. 绿地、灯杆等园内设施宜用于移动通信网络建设使用，并具备设备安装、光纤传输和电源供电等条件；
77. 移动通信网络服务在网络覆盖区内无线可通率应满足移动台在无线覆盖区内90%的位置、99%的时间可接入网络；
78. 移动通信网应能同时提供移动通信和物联接入服务。
	* 1. 无线局域网设计应符合下列规定：
79. 应设计园区的无线局域网，满足园区公共区域和主要办公楼宇无线网络热点覆盖；
80. 宜基于最新的Wi-Fi技术标准进行设计，其建设应符合现行国家标准《无线局域网工程设计标准》GB/T 51419的规定；
81. 应基于同一个无线网络、采用SSID方案，为园区内办公网、物联网、园区管理等分配独立的服务集标识；
82. 应具备无线干扰检测与避让能力，具备独立的干扰扫描射频，识别检测RFID、BLE等其他无线协议并采取有效的抗干扰机制，保证无线局域网承载业务稳定；
83. 无线流量应基于内外网隔离设计，确保不同无线业务的隔离与安全；
84. 应基于云化管理架构设计，满足云化统一管理要求。
	* 1. 园区网络、网管系统、网络出口设计应符合下列规定：
85. 园区网络架构应采用分层级进行设计，可采用两级（接入/核心两层）或三级架构（接入/汇聚/核心三层）设计；
86. 园区网络应对设备接入带宽、接入层至汇聚层、汇聚层至核心层以及出口带宽进行详细设计；
87. 园区网络应根据功能分区域设计，宜含接入区、核心区、应用区、管理区、出口区；
88. 园区网络内部协议应采用IGP协议或静态路由进行设计，出口对接应采用BGP路由或静态路由方式进行设计；
89. 园区网络业务应该根据重要性进行优先级划分，并按照不同优先级进行QoS业务保障设计；
90. 网管系统应包含有线及无线等各类网络，具备统一的网管、资源管理等功能；
91. 园区网络出口与基础电信运营企业互联链路应不少于两条，且避免单点线路故障；
92. 园区网络出口区设备应采用虚拟化设计，避免设备单点故障；
93. 园区网络出口应建立边界防护体系，保证外网流量进入园区网络安全可靠。
	1. 边缘节点
		1. 园区宜根据业务需求设置边缘节点，边缘节点包括边缘计算节点及边缘网关节点。
		2. 边缘计算节点应具备以下功能：
94. 应具备标准化网络接口，支持与多种网络进行数据传送的能力，数据可以从有线网络、无线网络等多类网络进行传送；
95. 应具备与云计算的协同能力，支持处理云计算中心下发的计算任务，也可向云计算中心发出请求；
96. 应根据部署的上层应用，实现本地大流量计算能力、本地存储能力及数据分析能力，并支持计算、存储的扩展；
97. 应具备对第三方应用的管理能力；
98. 应支持节点的网络容灾能力及数据容灾能力。
	* 1. 边缘计算节点的设计应符合以下要求：
99. 应明确节点的业务覆盖范围、应用类型、对数据的要求及对网络带宽的要求；
100. 硬件资源应根据业务覆盖范围、对应用处理能力及存储能力的需求设计；
101. 网络架构应能从时延、带宽等方面满足数据传送要求；
102. 硬件资源应包括计算资源、存储资源及网络资源，各类硬件资源应能满足业务量及应用处理的需求，应能满足不同应用场景的QoS要求，并根据不同场景对硬件资源进行合理配置。
103. 功能模块应基于硬件资源的能力及容量，根据边缘应用对计算资源、存储资源及网络资源的不同需求形成不同逻辑上的功能单元；
104. 网络架构应能满足多种网络及应用的对接需求，网络带宽及时延应满足边缘节点所部署应用的业务质量要求；
105. 应具备设备的容灾能力、网络容灾能力及数据容灾能力，并具备外部网络对边缘计算节点攻击的防护能力；
	* 1. 边缘网关节点注重于接入功能应具备以下功能：
106. 具备标准化、多样化的接入接口对各类终端提供接入能力，接口应包括固定以太网口、固定串口，宜能支持PLC通信能力，宜具备告警接口；
107. 支持与多种上层网络进行数据回传的能力，应能支持固定以太接口、PON接口及无线网络等多类网络的回传能力；
108. 支持节点的本地计算能力、网络容灾能力、数据加密能力；
109. 支持接入园区网管平台，具备远程管理、维护升级的能力。
	* 1. 边缘网关节点的设计应符合以下要求：
110. 设计应明确节点的业务覆盖范围、终端接入类型、对数据传送质量的要求及对网络带宽的要求；
111. 处理能力应根据接入覆盖范围、终端接入数量、数据传送能力及数据加密能力的需求设计；
112. 硬件资源应包括接口资源、计算资源及网络资源，各类硬件资源的能力应能满足终端接入需求、数据传送需求及本地计算的需求；
113. 网络架构应能满足终端的接入需求、与上层网络的对接需求；
114. 宜具备设备的容灾能力、网络容灾能力及数据容灾能力，并具备外部网络对边缘网关节点攻击的防护能力。
115. **数字平台层**
	1. 一般规定
		1. 数字平台层应通过通信传输层采集或接收感知执行层及园区信息化系统的数据信息，进行融合、分析、处理、加工，打破信息孤岛，以服务和工具的形式支撑园区智慧应用层，并将智慧应用对设备的操控转化为对感知执行层的设备操作指令。数字平台应从云平台层、ICT能力层和业务服务层三个层面进行建设。
		2. 数字平台层应按照模块化、积木化原则建设，统一建模，具备解耦能力，实现数据管用分离，支持智慧应用灵活、按需组装，满足多业态的解决方案，实现平台的生态化。
		3. 数字平台层应遵循统一性原则建立数据湖、物联标准，统一安全管控、运维、门户、运营，提升智慧应用的融合效率。
	2. 云平台层
		1. 云平台层应提供承载数字平台的云基础设施和基础云服务，可根据实际需求体现为公有云、混合云、私有云、边云协同等一种或多种部署形态。
		2. 云平台层宜保持云的弹性伸缩，可自动适配业务，自动调整计算资源，满足平台软件的应用，保证业务平稳健康运行。
		3. 云平台层宜提供云容器引擎服务，支持多种异构服务器设施的使用，支持自动化部署、大规模可伸缩、应用容器化管理，满足全生命周期的运维需要。
		4. 云平台层可提供可靠、规格丰富并且可弹性扩展的云硬盘服务，支持系统备份策略，支持多种性能规格的云硬盘，满足不同业务场景需求。
		5. 云平台层可提供弹性文件服务，通过多级可靠性架构，提供按需扩展的文件存储，并提供云安全技术保障。
		6. 云平台层可提供对象存储服务，为视频、图片等非结构化对象提供存储策略，通过大带宽和低时延满足视频分析应用的数据需求。
		7. 云平台层可提供弹性负载均衡服务，支持异地容灾、同城双活容灾、园区内容灾等各种场景，无缝实时切换，支持快速部署、实时生效、调整分发等策略，满足海量业务访问需求。
		8. 云平台层可提供分布式缓存服务，支持集群部署、在线扩容、多规格存储、高速存取等功能，满足读写要求高及弹性调整的场景。
		9. 云平台层宜提供云关系型数据库服务，实现即开即用、稳定可靠、弹性伸缩、便捷管理等功能，在高并发情况下，业务稳定运行、低时延，保证数据不丢失。
		10. 云平台层宜支持云解析服务，提供高可用、高扩展的权威DNS服务和DNS管理服务，要求时延低、安全性高，防劫持、防DDoS。
		11. 云平台层应具备安全服务，应提供网络层和应用层的DDoS攻击防护，提供资产管理、漏洞管理、入侵检测、基线检查等功能，支持安全编码检查、主机、数据库、WEB漏洞、业务逻辑漏洞扫描等能力，支持SSL证书管理、堡垒机等服务。
	3. ICT能力层
		1. ICT能力层应进行合理规划，采用成熟技术对平台进行能力支撑，ICT部件应具有标准化协议接口，支持引入技术生态，实现部件可替换。
		2. ICT能力层宜引入人工智能技术，支持平台组件及智慧应用的智能化，应支持可插拔、可替换、可升级。
		3. ICT能力层应引入大数据技术，支持园区海量数据信息处理，对数据信息进行实时和非实时的分析和挖掘，获取数据价值。
		4. ICT能力层应引入音视频处理能力，支持统一存储、安全使用各类音视频资源，支持视频存储、分析、播控、检索、转码等服务。
		5. ICT能力层宜引入地理信息技术、建筑信息模型、定位技术等，供上层智慧应用集成，实现基于二/三维地图的可视化的园区管理，并对接智慧城市建设。
		6. 智慧园区应协同边缘网关，对感知执行层的设备或系统进行管理和控制，针对园区的环境、设备、系统等提供统一的物模型定义，实现物联网管理功能。
	4. 业务服务层
		1. 业务服务层应包括应用服务、数据服务、集成服务、开发服务，通过不同服务沉淀和积累园区数字资产，支撑多业态智慧园区的应用需要。
		2. 应用服务宜提供智慧应用的服务支撑，按标准的WEB服务协议暴露服务，向智慧应用层提供实时的业务交互能力，并将智慧应用层发布的指令传导给下层；应支持引入和集成生态伙伴的业务服务，共同为应用提供服务能力。
		3. 数据服务宜提供一站式的数据开发环境，具有全托管的数据调度能力，实现数据建模、数据集成、数据处理脚本开发、批量任务调度、运维监控等数据处理与分析流程，提供标准化的数据主题库、专题库及数据服务，便于智慧应用层便捷、准确、高效地获取数据信息，进行趋势判断、数据运营、辅助决策、智能分析等。
		4. 集成服务宜提供一站式的集成编排环境，实现系统间数据、服务、消息、多云等集成全场景覆盖，并沉淀设备/系统的标准化集成对接的能力，提升项目集成效率，降低项目交付成本。
		5. 开发服务宜提供在线开发IDE平台，通过界面可视化拖拽式UI开发、元数据引擎、流程引擎、工作流引擎、服务编排等技术手段，方便智慧应用的软件编制。
		6. 业务服务层应提供接入网络的设备或设备子系统的物模型，采集和汇聚通信传输层、感知执行层的物联数据，在获取环境、设备、系统等的物理属性和状态数据的基础上，叠加设备的实际空间信息、维护信息等信息模型的数据，为智慧应用对设备的访问和控制提供服务，并支持设备从物理世界到数字世界的全方位映射能力。
116. **智慧应用层**
	1. 一般规定
		1. 智慧应用层宜提供以下智慧园区场景的服务、管理，适应职住平衡、区企一体、产城融合等园区发展需要。智慧应用层应包含但不限于以下内容：
117. 企业事业服务；
118. 公共信息服务；
119. 智慧通行服务；
120. 公共设施管理；
121. 绿色健康管理；
122. 公共安全管理；
123. 智慧运营中心。
	* 1. 智慧应用层宜配合社区网格化管理，针对园区内的人、地、事、物、组织等，实施全覆盖、全时空、全响应、数字化、精细化、动态化的管理，形成智慧园区的各种场景应用，并对接智慧城市（社区）平台。
		2. 智慧应用层应构建于数字平台层之上，应用数字平台层提供的业务服务工具，全方位融合、分析、处理智慧园区的各种数据，协调、组织各个智能化系统与设施的运转。
		3. 智慧应用层做出的各种决策指令，必须得到园区相关责任人的审核、确认，方可下达到数字平台层，并通过智慧园区系统落实、执行。
		4. 智慧应用层宜应用人工智能、云计算、大数据、数字平台、语音交互、无人机与机器人等新技术，增强智慧园区的科技体验感。
		5. 智慧应用层的软件编制，应满足数字平台层的接入要求，并应采用标准化结构、接口、界面，便于操作、使用、维护。
		6. 智慧应用层的软件产品投入使用，应满足以下规定：
	1. 具有合法著作权；
	2. 通过国家授权的第三方检测机构的测试；
	3. 通过所使用数字平台层厂家的授权、认证、测试。
	4. 企业事业服务
		1. 企业事业服务应面向入驻园区的政务、企业、事业单位，包括法人、自然人等，提供全产业链条、全生命周期、全过程的企业信息服务。
		2. 园区宜面向招商、入驻、产业对接、仓储物流、人才服务、知识产权、咨询等园区业务，提供信息化服务。
		3. 园区可链接电子政务、电子金融、电子商务等公共服务，丰富园区的公共信息服务资源，满足企业运行与办公需要。
		4. 园区可配套信息化系统，筛选有前景的创新企业，提供创业辅导、项目路演、天使对接等社会服务，以及资金、管理、场地等多种便利服务，构建企业孵化器。
		5. 园区可向入驻企业提供云服务资源、网络信息安全服务，以及信息化规划、咨询、设计、建设、运维等专业化服务和培训，支持创新企业入住。
		6. 企业事业服务可部署数字化工厂，借助虚拟现实技术，对新产品的生产过程进行仿真、评估、优化，进而组织产品全生命周期的生产活动。
	5. 公共信息服务
		1. 园区宜提供各种为民、便民、利民等信息服务，包括城市、社区、园区、建筑环节的各种公共服务信息。
		2. 园区宜部署电子政务系统，并链接智慧城市（社区）的公共信息服务平台，在线办理各项市政、园区等业务。
		3. 园区宜部署电子商务系统，提供线上购买、线下配送等服务，组织调度物流仓储，统一监管物流柜。
		4. 园区宜设置园区门户网站，构建数字园区，共享园区的公共信息与文化资源，提供各项智慧园区的场景应用业务，配套必要的搜索引擎、移动终端软件。
		5. 园区必须设置信息发布的认证、审查、签发机制，满足国家相关规定与要求。
	6. 智慧通行服务
		1. 园区宜采用物联网、视频监控、大数据分析、可视化辅助决策等技术，针对园区的行人、车辆、道路、交通等提供电子警察、交通诱导、便捷通行等管理与服务，维护通行秩序，提高通行效率。
		2. 园区可研判管沟、井盖、路面等道路设施的完整性，识别道路障碍、违规停车、交通事故等事件。根据园区的应急预案，疏导道路交通，引导排障。
		3. 园区宜提供区域内的访客预约管理、自助登记业务、无感通行服务、电梯自动调度、智慧电子导航等智慧场景应用。
		4. 园区宜针对道路、广场、场馆等公共场所，实施人群密度分析。根据园区的应急预案，及时疏导、分流密集人群。
		5. 园区可综合分析行人、车辆、道路、交通、车位等信息，协调管理道路照明、交通红绿灯，实时发布园区道路、停车等信息，提供车位引导与反向寻车服务。
		6. 园区可自动识别与追踪校车、特种车辆、危险品运输车辆，协调组织道路交通，给予此类车辆优先通行等便利。
		7. 园区宜对接道路交通执法部门，协助甄别套、假车牌，识别与追踪涉事、嫌疑、超重车辆，联动卡口动作，及时阻止该类车辆在园区通行，并上报有关执法部门。
		8. 园区宜构建交通档案库，登记出入园区的机动车、非机动车、行人等，记录交通违规行为，补充当事人的诚信档案。
	7. 公共设施管理
		1. 园区应综合分析数字平台层提供的各类数据，组织、管理各类设施与设备，协调多种自动化系统与智能机电设备，实现能源与资源等综合利用，满足各类活动需要。
		2. 园区应能及时发现停水、停电、断网等供给故障，联动感知执行层的相关设备。并根据园区应急预案，组织抢修。
		3. 园区宜响应绿色健康管理、公共安全管理等相关指令，根据事件的轻重缓急，调度、组织、协调园区的设施与设备。
		4. 园区宜集中监管各类机房，自动调阅机房的监控图像、设备信息、综合环境数据，分析、评估机房工作状态，保障园区机电系统正常运行。
		5. 园区宜自动采集信报箱、物流箱的使用信息，提醒收取积压物件，并评估快递公司的服务质量。
		6. 园区可支持智能家居、智能办公等系统托管服务，为合约用户提供智能家居系统的运行、维护作业，满足智慧家居、办公等服务需要。
		7. 园区应构建设施与设备档案，登记设施与设备的购置信息、运行数据，自动生成设施与设备报表，及时组织运行、维护。
	8. 绿色健康管理
		1. 园区宜从卫生、健康、节能、服务、人文等维度，评价绿色、健康环境，制定绿色园区运维策略，满足园区健康生活与产业绿色发展需要。
		2. 园区宜实时监管风热环境、噪声环境、用水水质、空气质量、室内环境、污染物排放、以及海绵城市的相关数据，具备超标预警、分析处置、控制管理等功能。
		3. 园区宜分项、分级、分区统计建筑能耗，重点监控大型办公与公共建筑、充电桩等能耗，集中监管园区的电力、天然气、冷热量等能源供给，并审计、调度、优化能源结构。
		4. 园区宜监测、分析并评估可再生能源利用情况，对太阳能、风能等分布式能源系统进行统一协调管理与调度。
		5. 园区宜计算分析碳排放，评估单位GDP碳排放量、人均碳排放量和单位面积碳排放量等指标是否达标。
		6. 园区应按照绿色健康的相关规定，指导设施与设备管理、以及车辆与交通管理，落实绿色健康目标。
	9. 公共安全管理
		1. 园区应针对发生的公共安全事件，实施快速反应、统一指挥、联合行动，并预留接入上一级指挥系统的接口。
		2. 园区应具备公共安全事件的监控、预测、报警功能，并触发园区管理单位预先设置的应急与救援预案，满足安全生产和生活的需要。
		3. 园区应监控管理安全生产，监督企业生产、科研、经营活动的安全性，落实安全生产责任制度。
		4. 园区应部署智慧消防系统，评估判断火灾风险，根据应急预案，实施逃生、扑救、警戒、交通管制。
		5. 园区应配合社区防疫网格化管理，部署信息化系统。针对疫情的采集、上报、审核、发布等环节，实施全过程跟踪管理。
		6. 园区应针对治安及其他公共安全事件，联动、协调、控制各个安全防范子系统，并组织、疏导、管制交通。
		7. 园区可采用数字孪生技术，依托数字平台，实现三维可视化操控，调度各类设施、资源、人力，实现“事前预防、事发应对、事中处置、善后管理”。
		8. 园区应设置应急联勤通讯录，采取多种通信方式，实现就地和异地报警，实施呼叫、引导、调度、指挥。
	10. 智慧运营中心
		1. 园区应设置智慧运营中心，提供办公场地，配套相应的监控、指挥、调度设施，协同相关业务部门，高效管控各项事务。
		2. 智慧运营中心宜配套物业运行管理系统，实现网络办公、线上调度、行政管理、资产管理，并能实现物业部门全员绩效考核。
		3. 智慧运营中心宜配套工程建设监管信息管理系统，针对项目的规划、立项、设计、建设、验收、移交等过程，提供项目审批、参建单位、现场施工、业务流程等业务管理。
		4. 智慧运营中心可与社会征信机构合作，合法采集经济活动的信用信息、并加工整理信用产品，构建企业与自然人的诚信档案。
		5. 智慧运营中心宜构建居民的健康档案卡，提供餐饮、营养、健身、康养、医疗等信息化服务，协助园区组织实施卫生防疫工作。
		6. 智慧运营中心应设置呼叫中心，受理并响应客户投诉、报修、建议等业务，定期实施满意度网络调查，不断改善与提升物业服务水平。
124. **安全体系**
	1. 一般规定
		1. 园区安全体系设计应从物理环境、计算环境、区域边界、通信网络、感知终端和管理中心等方面落实安全保护技术要求，能够为园区网络安全提供有力保障。
		2. 园区安全体系设计应遵循总体网络安全规划。感知执行层、通信传输层、数字平台层和智慧应用层中应根据各层的特点分别设置网络安全保障体系，各层与总体规划协调一致。
		3. 园区网络安全应为园区的空间数据、环境数据、建筑数据、组织数据、用户数据等的检测、传输、存储和应用提供安全保证。
		4. 园区网络安全的建设必须维护园区管理者和使用者的数字主权需要和园区隐私安全的需要。
		5. 园区客户应采取配套的管理措施、管理流程，建立安全管理团队并授予相应的权限；安全管理人员应定期进行系统日志检查，数据备份，系统安全巡检并及时对发现问题及时修复和解决。
		6. 园区网络安全设计除应符合本标准外，还应符合现行国家标准《信息安全技术网络安全等级保护实施指南》GB/T25058的规定。
	2. 感知执行层安全
		1. 感知执行层应根据设备及感知层中各类感知设备和传输方式多样化特点，总体制定本层信息安全规划，满足实用性、机密性、完整性、可用性、可追溯性等需要。
		2. 感知执行层中具备计算能力的主机或智能终端，宜具备主机安全与应用安全防护能力，包括：身份鉴别、访问控制、入侵防范、恶意代码防范、数据完整性与保密性、安全审计、可信验证、备份与恢复、个人信息保护等。
	3. 通信网络安全
		1. 通信网络安全应保证网络架构安全、通信完整性与保密性。
		2. 通信网络架构应具备关键节点冗余设计保证通信稳定、分区分域合理要求。
		3. 通信网络应保证信息传输与存储过程中的一致性、完整性、机密性要求。
		4. 通信网络设备应满足可信验证要求，保证网络设备身份可信，防止假冒网络通信设备。
	4. 区域边界安全
		1. 园区应根据需求划分安全域并确定安全等级保护定级要求，在安全域之间通过部署区域边界安全设备，实现对定级系统的安全计算环境边界，以及安全计算环境与安全通信网络之间安全防护策略。
		2. 区域边界的安全设备应根据园区要求满足边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计、可信验证等要求。
	5. 计算安全
		1. 园区应通过设备、主机、移动终端、应用服务器和数据库的安全机制服务，保障应用业务处理全过程以及数据的计算环境安全。
		2. 平台系统安全应满足如下要求：
125. 应通过操作系统安全扫描、安全加固、安全补丁等措施加强操作系统安全性；
126. 应通过数据库安全扫描、数据库安全补丁、数据库安全加固等措施及加强数据库安全性；
127. 应通过WEB应用防护、WEB容器安全加固等措施加强WEB安全性。
	* 1. 数据安全安全应满足以下要求：
128. 敏感数据的安全：对敏感数据应从采集、存储、传输、使用、删除/销毁等数据全生命周期考虑端到端的数据安全性；
129. 数据的隐私防护安全：对隐私数据应遵从当地的隐私保护相关法律和政策；
130. 数据备份：对数据应提供定期的备份机制，保证数据备份的安全性，并保证数据安全恢复，恢复的数据需要提供生产数据同样的安全防护策略。
	* 1. 应用安全应满足以下要求：
131. 系统应提供权限与用户管理机制，应采用最小授权原则；
132. 应用系统对文件和数据包括客户资料应提供访问控制机制；
133. 应支持输入检查、上传下载控制、防越权等手段防范应用攻击；
134. 宜支持日志审计、应用数据稽核等手段发现业务活动异常，如非法篡改等。
	1. 网络安全管理中心
		1. 网络安全管理中心应对系统的安全策略及安全计算环境、安全区域边界和安全通信网络三个部分的安全机制，形成一个统一的安全管理中心，实现统一管理、统一监控、统一审计等功能。

本标准用词说明

1　为便于在执行本标准条文时区别对待，对要求严格程度不同的用词说明如下：

1）表示很严格，非这样做不可的：

正面词采用“必须”，反面词采用“严禁”；

2）表示严格，在正常情况下均应这样做的：

正面词采用“应”，反面词采用“不应”或“不得”；

3）表示允许稍有选择，在条件许可时首先应这样做的：

正面词采用“宜”，反面词采用“不宜”；

4）表示有选择，在一定条件下可以这样做的，采用“可”。

2　条文中指明应按其他有关标准执行时的写法为：“应符合……的规定”或“应按……执行”。

引用标准名录

《建筑设计防火规范》GB 50016

《人民防空地下室设计规范》GB 50038

《火灾自动报警系统设计规范》GB 50116

《火灾自动报警系统施工及验收标准》GB 50166

《数据中心设计规范》GB 50174

《公共建筑节能设计标准》GB 50189

《电力工程电缆设计标准》GB 50217

《综合布线系统工程设计规范》GB 50311

《智能建筑设计标准》GB 50314

《消防应急照明和疏散指示系统技术标准》GB 51309

《建筑物电子信息系统防雷技术规范》GB 50343

《安全防范工程技术规范》GB 50348

《通信管道与通道工程设计标准》GB 50373

《入侵报警系统工程设计规范》GB 50394

《视频安防监控系统工程设计规范》GB 50395

《出入口控制系统工程设计规范》GB 50396

《公共广播系统工程技术规范》GB 50526

《无障碍设计规范》GB 50763

《城市综合管廊工程技术规范》GB 50838

《住宅区和住宅建筑内光纤到户通信设施工程设计规范》GB 50846

《信息安全技术网络安全等级保护基本要求》GB/T 22239

《信息安全技术网络安全等级保护实施指南》GB/T 25058

《绿色建筑评价标准》GB/T 50378

《无线通信室内覆盖系统工程技术标准》GB/T 51292

《宽带光纤接入工程技术标准》GB/T 51380；

《电子巡查系统技术要求》GA/T 644

《智慧住区建设评价标准》T/CECS 526-2018

**中国工程建设标准化协会标准**

**智慧园区设计标准**

CECS XXX-20XX

条文说明

**目　　录**

[1  **总　　则** 46](#_Toc52358425)

[**3 基本规定** 47](#_Toc52358426)

[4 **感知执行层** 52](#_Toc52358427)

[4.1 一般规定 52](#_Toc52358428)

[4.2 设备管理类 52](#_Toc52358429)

[4.3 消防类 53](#_Toc52358430)

[4.4 安全技术防范类 54](#_Toc52358431)

[4.5 信息设施类 55](#_Toc52358432)

[4.6 物联网设备设施类 55](#_Toc52358433)

[**5 通信传输层** 57](#_Toc52358434)

[5.1 一般规定 57](#_Toc52358435)

[5.2 通信网络设施 57](#_Toc52358436)

[5.3 边缘节点 61](#_Toc52358437)

[**6 数字平台层** 62](#_Toc52358438)

[6.1 一般规定 62](#_Toc52358439)

[6.2 云平台层 63](#_Toc52358440)

[6.3 ICT能力层 68](#_Toc52358441)

[6.4 业务服务层 72](#_Toc52358442)

[**7 智慧应用层** 75](#_Toc52358443)

[7.1 一般规定 75](#_Toc52358444)

[7.2 企业事业服务 77](#_Toc52358445)

[7.3 公共信息服务 78](#_Toc52358446)

[7.4 智慧通行服务 80](#_Toc52358447)

[7.5 公共设施管理 81](#_Toc52358448)

[7.6 绿色健康管理 82](#_Toc52358449)

[7.7 公共安全管理 84](#_Toc52358450)

[7.8 智慧运营中心 86](#_Toc52358451)

[**8 安全体系** 88](#_Toc52358452)

[8.2 设备及感知层安全 88](#_Toc52358453)

[8.3 通信网络安全 88](#_Toc52358454)

[8.4 区域边界安全 89](#_Toc52358455)

[8.5 计算安全 90](#_Toc52358456)

[8.6 网络安全管理中心 92](#_Toc52358457)

1  **总　　则**

1. 0.1　为适应国家智慧园区工程建设的需要，使本标准具有适时性、适用性和可指导性而制定。

1.0.2　本标准具备普适性，适用于新建、扩建和改建的产业园区、住宅、办公、教育、金融、交通、医疗、体育、文化、展馆等民用建筑及通用工业园区的智慧化设计。本标准规定了智慧园区建设应通过智慧化、信息化技术与园区融合，有效提升园区综合性能，实现节约资源、保护环境为主题的绿色建设要求，支撑园区全生命周期内不断提升和挖掘智慧化综合技术功效。

1.0.4　本标准所引用的国家现行相关标准，是本标准在实施中应遵守的基础技术依据。在本标准中未注明该标准发布年号所被使用的标准，应是该标准实施中的有效版本。

**3 基本规定**

3.0.2 智慧园区架构要求如下：

1. 架构规划要求

智慧园区技术架构应满足智慧建设的功能要求、基础条件和应用方式，采用层次化的架构设计，其核心是数字平台，将各子系统统一接入、汇聚、建模，形成综合分析展示、集成联动和统一服务的能力。

2. 通用技术架构图

智慧园区体系架构是针对智慧园区的标准的信息系统部分的总体架构，采用开放平台面向服务的架构。

3. 架构各层重要技术指标

园区在实际应用中，需要接入园区中多种类型的设备与子系统，使用园区中5G、WI-FI6、以太网络、PLC等多种类型网络连接技术，集成协调多样化的园区已有IT系统和互联网服务，并支撑和应对园区物业管理、生产生活、社会治理等多样化的创新应用，所涉及的业务、技术均具有多样性、复杂性、多变性、灵活性等特征。

方案应采用水平分层架构，应对不同层间的技术复杂性，对水平能力和功能进行抽象与标准化，简化水平层次间的调用关系，实现水平层内技术和业务复杂度的高内聚，以及层间的有序依赖；同时，统一构建贯穿多个水平层的公共能力，如安全、运维、运营等。

智慧园区架构从水平和垂直分别包括（如下①~⑥序号与正文图3.0.2 智慧园区技术架构图对应）：

① 感知执行层：

本层包括园区常见的物理设备、感知设备与设备子系统，例如摄像头、电梯、传感器、控制器以及梯控子系统等，提供对园区人、机、物、事、环境的感知能力和控制能力，也会包括进行贴近设备控制的边缘设备。

园区的设备及感知层的各类设备主要面临的挑战在于园区设备的多样化，厂商的多样化、技术多样化，本层是规范设备快速接入、控制、升级、维护等接入技术要求。本层主要包括存量设备/子系统体系以及体系之上的设备接入能力、设备数字化描述能力、接受升级及维护的能力、安全能力。

本层需要提供如下技术和标准化能力：

a 设备IP化能力：主要是指设备本身对外交换数据是基于IP的通信方式，如PLC（电力线通信，Power Line Communication）,Wi-Fi, Ethernet, 5G, Bluetooth等各项接入能力，具备能与网络传输层设备/设施进行数据交换的能力；

b 联接无线化能力：主要是指设备采用的互联方式，需要根据设备的运行要求和运行环境，选择合适的无线技术来联接，减少园区布线和线管铺设方面的安装成本和维护成本；

c 设备数字化描述能力：主要是指设备本身能够进行自描述，包括设备的规格、地址、状态上报等；

d 接受升级及维护的能力：指设备可以被纳管，接受纳管系统对设备的升级、维护设备的请求及响应；

e 安全能力：主要指设备本身有机自认证能力，安全防护能力，防篡改能力等。

一般来说，基础设施层是属于园区物理范围内的基础设施、设备及附属系统，但其中部分体系受到园区边缘节点或者云服务的管理与控制。

② 通信传输层：

本层用于连接应用、服务与设备和子系统，包括有线网络、无线网络、边缘节点、信息机房等所组成的网络传输基础设施，实现设施与感知层数据与数据平台数据的双向传输以及边缘计算能力。有线网络包括骨干交换网络、通信公网、各类专网以及网络交换设备；无线网络包括蓝牙、RFID（无线射频识别技术，Radio Frequency Identification）、Wi-Fi、NB-IoT（窄带物联网，Narrow Band Internet of Things）等；边缘节点包括具有边缘计算能力的本地控制器、服务器等侧重实现数据的就地加工处理；信息机房承载本地的边缘设备及汇聚网络节点等能力，以及为了支持这些网络运行的安全体系，网元维护管理体系等。

本层需要提供如下技术和标准化能力：

a 智能网络能力：网络本身能够智能动态调整，选择最佳路径发挥最优性能，使得网络状况即使是在单点故障时，依然可以提供网络服务；

b 智能网络策略配置能力：网络本身提供网络策略智能、快速的配置能力，基于用户组实现权限、带宽、QoS等网络策略的自动化配置，以满足大量感知终端的快速的入网与权限调整；

c 设备的边缘控制能力：指边缘处贴近设备的发现、管理、接入、鉴权、本地控制和基于本地策略的联控、群控、升级、运维等能力，包括对数字化设备的物理投影建模，非数字化设备的数字化描述，并尽可能实现设备的建模和标准化；

d 边缘智能技术：进一步从园区业务的成本、可靠性、时效性、智能化要求出发，实现边缘智能，包括人工智能、策略与规则、联控与群控逻辑等；

e 视频管理能力：本地进行视频汇聚、视频管理的能力，提供外部通过特定视频协议访问视频、播控视频流、控制视频设备的能力。

**③ 数字平台层：**

本层是构建水平化智慧园区方案实现的关键核心。数字平台层应包含成熟的服务化组件，针对园区的服务能力，以及业务快速开发、部署的工具性设施。

数字平台划分为三个层次：云平台层、ICT能力层、业务服务层。云平台层提供高可靠的云基础设施及基础云服务；ICT能力层支持业界ICT成熟技术能力，或在平台内构建ICT核心能力，提供技术核心，包括人工智能、大数据、视频分析、IOT技术、定位技术、GIS平台、BIM平台等；业务服务层包括数据服务、应用服务、集成服务和开发服务，数据服务包括各类基础系统的数据接入、汇聚、加工、分析、存储、访问规则等，应用服务是以园区业务视角的定义和沉淀各领域各业务活动的公共能力，为应用开发提供共享的服务能力集合，以服务化/微服务化形式对外暴露，集成服务是联接物理世界和数字世界的桥梁，驱动系统间数据、服务、消息流通与融合，是云时代的应用和数据集成平台，开发服务是提供在线开发工具IDE，支持可视化编程，支持将各类服务进行元数据化信息访问，实现服务的快速编排，快速构建智慧应用的能力。

智慧园区面临业务、技术和系统的多样性、复杂性、易变性等特征，数字平台层应对以下技术进行抽象和标准化，支持业务的发展：

a 部署形态多样化：支持云、本地一体化设备等多种部署形态；

b 设备模型的标准化：在下层解决了设备模型的抽象问题后，需要在本层对设备模型进行标准化定义，确保整个方案中使用相同的设备描述语言来描述设备/子系统的能力和属性，提供的设备服务等；

c 协议标准化：应采用业界或国际国内标准的访问协议方式（如REST协议、消息协议、SOAP协议等），暴露所有的平台能力供外部访问；

d 服务标准化：包括服务的接口标准化，服务生命周期的管理，服务响应级别的统一管理，服务日志的格式统一，服务调用链的统一，服务的治理等。

**④ 智慧应用层：**

本层包括了应用的运行和运行环境，运行环境可能来自于数字平台层的支持，可是原生的APP，虚拟机或者容器环境。

智慧应用层上的业务包括基于数字平台的开发能力构建的应用，或来自于其他应用构建技术，通过服务访问的方式与园区数字平台和设施交互的松耦合应用。

园区应用的创新多变，推荐应用能够基于一定的园区行业知识沉底基础进行构建，并在容器等技术上实现多租能力。

本层需要提供如下技术和标准化能力：

前后端解耦技术：智慧应用的前端界面和后端服务采用解耦的方式，前端注重体验、页面流、交互的建设，主要特点是多变，后端的服务着重于抽象、固化、可配置化，主要特点是稳定。

**⑤ 安全体系：**

智慧园区建设应构建统一的端到端的安全体系，实现系统的统一入口、统一认证、统一授权、运行跟踪、系统安全应急响应等安全机制，涉及各横向建设层次。

智慧园区的安全体系应包括面向人员的安全性和面向设备的安全性两方面，建立面向人和物的统一标识体系，实现访问安全、数据安全、存储安全、安全事件可跟踪、可稽核、可审计等能力。

**⑥ 运维体系：**

智慧园区的运维体系机制，涉及各横向建设层次应确保智慧园区整体系统的建设管理和高效运维。

智慧园区运维体系应包括设备基础设施的运维、通信网络的运维、数字平台和应用的运维等不同层次，应基于不同的技术进行运维信息的获取和展现以及对应的行动。

智慧园区运维体系应包括了面对不同水平层次或领域的运维子系统和园区统一的运维呈现、指控能力，应体现在整体架构中，但不属于设计标准范畴，不在本标准中体现。

4 **感知执行层**

4.1 一般规定

4.1.1感知与执行层是智慧园区感知外部状态、获取外部信息的基本来源，是落实智慧园区智慧应用层指令的执行设备、执行机构或子系统,是位于智慧园区总体框架内的物理基础层，本层的功能应用由园区智慧应用层定义。

4.1.2宜采用满足IPv6物联网的Ethernet、光纤、Wi-Fi、NB-IoT等一系列有线、无线标准传输方式。

4.1.3在可靠性以及其他性能要求适用的情况下，优选采用无线化的接入方式。考虑物联网安全，所有TCP/IP协议的智能终端和设备应支持X.509证书，支持基于证书的802.1x接入认证。

4.1.4一般将数据挖掘与决策能力配置在数字平台层，本层只配备基本管理功能，如联动、视频智能分析等。

4.1.5本层涉及各子系统可配备独立运行能力，也可将感知与执行设备直接纳入数字平台层控制、管理，各子系统的设计要求不再在本标准中重复规定，设计应符合既有标准、规范的相关要求。

4.2 设备管理类

4.2.1设备管理类子系统负责建筑设备监控、智能照明监控、建筑能效监管、电梯运行监控、环境监测等园区、建筑内各类设备、环境的感知与执行。

4.2.2设备管理配置有本地控制器的接入，应采用二线制无源干接点接口传输方式；建筑设备管理配置无本地控制器的接入，应采用无线传输方式，宜采用有线物联网、LoRa、Wi-Fi协议无差别接入系统；感知表计类（传感器及变送器）设备有本地控制器或有本地显示需求的接入，宜采用有线传输方式，应满足多种接口协议；智能能量表、智能水表、燃气表等可选用4~20mA二线制接口、脉冲二线制接口、应支持TCP/IP、BACnet MS/TP或 Modbus RTU协议的RS485等通用多种通讯接口形式；感知表计类（传感器及变送器）设备无本地控制器和无本地显示需求的接入，宜采用无线传输方式，须满足采用物联网、Wi-Fi协议无差别接入系统；电能计量表具的设置应满足节能及分项计量要求。宜设置智能电表可以高精度的测量所有常用的电力参数，如三相电压、三相电流、有功功率、无功功率、频率、功率因数、四象限电能等，采用可视度高的LCD来显示仪表测量参数和电网系统的运行信息；电能计量采集器宜采用满足多种通用开放通讯协议的设备，并满足电力规约要求；应对变压器、直流屏、ATSE、EPS、UPS进行监测，宜选择支持多种通用开放通讯协议的设备。

4.2.3阀体型号、材质应符合设计要求，阀芯泄漏应满足相关规范的规定，宜由第三方检测机构进行检测；执行机构输入电压、输出信号和接线方式应符合设计要求；执行机构行程、压力和最大关闭力应符合设计要求，宜由第三方检测机构进行检测；变频器功率配置及基本功能应满足园区电机变频速度调节控制的需求；变频器有本地控制需求的接入，应采用有线传输方式，须满足多种输入控制方式要求；变频器应具有0~10VDC三线制、4~20mA二线制反馈信号接口。

4.3 消防类

4.3.1 各类消防信息可通过用户信息传输装置、具有传输功能的火灾报警控制器、消防控制室图形显示装置、LoRa网关等设备上传至园区智慧应用层，这些设备与园区智慧应用层之间可采用以太网、4G、5G等多种通信方式进行数据交互。

4.3.2 各类消防信息宜在信息产生后宜10s内上传至园区智慧应用层。对于仅电池供电的感知设备的消防运行状态信息，两次上传时间间隔不大于24h。消防感知类设备完成开机、复位等操作后，宜在30s内把当前运行状态信息上传至园区智慧应用层。

4.3.3 火灾探测器、电压传感器、可燃气体探测器等感知设备应具有唯一的身份信息标识，有利于对大量的各类消防信息进行梳理分类、分发、共享等管理操作。

4.4 安全技术防范类

4.4.1安全技术防范类感知与执行层设备的设计和选用应符合下列要求：

1 入侵探测和紧急报警类

1）应按照防护对象纵深防护体系的周界、监视区、防护区、禁区的要求结合风险防范要求和现场环境条件等因素，选择适当类型的探测设备，确定适当的安装位置，构成点、线、面、空间或其组合的综合防护体系。

2）应能准确、及时地探测入侵行为或触发紧急报警装置，并发出入侵报警信号或紧急报警信号，应能准确、及时地发出防拆信号及设备、线路、电源、传输链路的故障信号，并发出声、光报警信号。

2 图像、声音拾取类

应能对建筑物、园区的主要公共活动场所、通道、重要部位和区域等进行有效的图像、声音信息采集，以实现报警、控制、图像显示、分析、记录与回放，设备的灵敏度和动态范围应与现场环境相适应，所采集信息应满足不同场景和目标特征识别的要求，可选用具备目标探测、识别、跟踪，行为分析、客流统计、人流量密度检测、人数统计、周界越界探测等功能的智能摄像机或智能设备。

3 目标识别及控制类

1）应能对进出园区、建筑、受控区域的人员、车辆进行信息采集、身份识别、权限判断及放行控制。认证介质可采用智能卡及生物识别技术如CPU卡、ID卡、Mifare、ID/ Mifare双频卡、身份证、人脸、人证比对、指纹、掌纹、指静脉、虹膜、二维码等不同形式或其组合。

2）出入口控制可集电子门禁、身份识别、考勤、电梯控制、停车场出入口管理、内部消费、巡更、签到等功能为一体，通过不同类型的现场认证设备实现“一卡通”。

3）应能对规定的爆炸物、武器及其他违禁品进行实时、有效的探测、显示、记录和报警，同时确保被检人员、物品的安全。

4 设备状态及控制类

应满足各系统报警、联动、控制、记录、存储要求，应能实时传递各类报警、设备状态、事件信息及控制指令，应支持与集成平台之间的通讯，实现信息交互与共享。

4.4.2安全技术防范类感知与执行层所应采集的信息包括智慧园区内的环境、建筑、人员、车辆、物品、设备安全状况信息及异常报警信号，包括各类被动入侵探测、主动报警信息，现场音频、视频信息，生物、身份识别信息，危险品探测信息，人员、物品位置信息，控制执行指令及设备状态反馈等信息，用于支持智慧园区的风险识别和判断、安全管理及应急指挥调度。

4.5 信息设施类

4.5.1智慧园区应根据功能需求设置有线电视、数字会议、时钟、卫星电视、公共广播、信息导引及发布等信息设施类子系统；其中信息导引及发布可直接由数字平台层直接控制和管理，其他各子系统相对独立运行，并在系统端与数字平台层对接，接受统一管理。

4.5.2 信息查询机等宜设置在大厅、服务台等处；手持PAD等移动终端宜设置在方便拾取的地方，如服务台、客房床头柜等处。

4.5.3 LED 大屏宜设置在室外、室内大厅、大型会议室、报告厅、监控及指挥中心等处；LCD显示器宜设置在普通会议室、电梯厅、会议室门口处；投影仪宜设置在会议室；DLP、LCD拼接屏宜设置在监控及指挥中心。

4.6 物联网设备设施类

4.6.2

a)园区的道路对各类设备的需求不断增加，将道路照明、视频安防摄像机、交通摄像机、气象监测、5G基站等综合到灯杆上安装，提升园区美观度，同时节能节材、方便智慧感知设备的接入和管理。

b)智慧园区可运用物联网技术使能相关公共设施，并符合下列要求：

* 1. 空气质量及异味检测范围一般包括NH3、H2S、CH2O、CO2、TVOC、PM2.5、PM10浓度及温度、湿度等；
	2. 厕位状态包括一般包括占用、空闲和维修三种状态；
	3. 各类机电装置例如暖通空调设备、照明器具、消毒设备、开水机、吹地机等；
	4. 入口导引显示内容一般包括公厕使用/维护状态、各种厕格的空余数量、空余厕格位置、预计等待时间、空气质量参数等。

c)智慧垃圾桶可由垃圾桶本体和检测设备两部分组成，也可采用集成检测设备的一体式垃圾桶。

d)智慧井盖可由本体和检测设备两部分组成，也可采用集成检测设备的一体式井盖，井盖的类型及设置部位由给排水、电力、通信、燃气等专业设计确定。

e)智能消火栓包括消火栓本体和监控设备两部分，监控设备可作为闷盖使用。

4.6.3机器人的用途包括引导、巡逻、物流、清洁等等。

**5 通信传输层**

5.1 一般规定

5.1.1 通信传输层是智慧园区建设的基础，指为园区生产和居民服务提供公共服务的网络设施或虚拟的系统和资产。

5.2 通信网络设施

5.2.2 信息管网

1. 管道管孔容量，应符合以下要求：

表5.2.2 管道管孔容量表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 园区用户规模（信息点） | 主干管道（孔） | 配线管道（孔） | 建筑物接入管道（孔） | 机房接入管道（孔） |
| 建筑物集中分布 | 建筑物分散分布 | 建筑物集中分布 | 建筑物分散分布 | 建筑物集中分布 | 建筑物分散分布 | 建筑物集中分布 | 建筑物分散分布 |
| 0-1000 | 4 | 4 | 5 | 6 | 3 | 3 | 6 | 6 |
| 1000-2000 | 4 | 5 | 6 | 10 | 3 | 3 | 12 | 12 |
| 2000-5000 | 6 | 7 | 12 | 18 | 5 | 4 | 15 | 22 |
| 5000-10000 | 8 | 12 | 18 | 24 | 5 | 4 | 22 | 30 |
| 10000以上 | 应根据建筑物分布情况，适当增加管道容量。 |

注： 1） 表中主干、配线管道容量是指每一方向的容量。

2） 表中孔数按9子孔栅格管计算，管材变化时应根据管材进行调整。

3） 表中建筑物接入管道指建筑每一处接入的管道容量。

4） 建筑物集中分布是指单栋建筑用户规模在100个信息点以上的建筑，建筑物分散分布是指单栋建筑用户规模在100个信息点以下的建筑。

1. 管道管孔容量，应符合以下要求：

1）标准孔指内径不小于90mm的水泥管、波纹管、单孔实壁管及钢管等管材。每标准孔可布放3孔子管。

2）采用栅格管时，栅格管根数管孔按标准孔数量的三分之二取定。

3）栅格管种类繁多，目前一般采用内径50mm 的4孔栅格管和内径33.5mm 的9孔栅格管。

4）计算公式

A-信息点总容量；

B-出局总芯数，B=A\*1.2（1.2为信息点数与配线比，光缆冗余一般为1.1～1.3）；

C-平均每孔含线容量，主干光缆一般按照48-288芯计算；配线光缆一般按照24-144芯计算；

D-主干管孔总容量:光缆计算公式D=B/32\*3/C，其中光缆按照1比32分光比计算；3家运营商。

E-配线管孔总容量:光缆计算公式E=B/C；

5）管孔容量的计算示例

1000信息点的主干管孔容量计算如下：

D＝1000×1.2/32\*3/324(432) ＝0.347(0.260)≈1孔(1孔)

1000信息点的配线管孔容量计算如下：

D＝1000×1.2/432(648) ＝2.778(1.852)≈3孔(2孔)

设计人员须考虑备用孔（一般不小于1－2孔）等因素进行适当预留。

6）表XXX 管道容量表的说明

0～1000信息点，主干管道（集中分布）管孔容量4孔中，智能接入线缆占用不少于2孔，通信占用1孔,备份1孔。1000～2000信息点，主干管道（集中分布）管孔容量4孔中，智能接入线缆占用不少于2孔，通信占用1孔，备份1孔。2000～5000信息点，主干管道（集中分布）管孔容量6孔中，智能接入线缆占用不少于3孔，通信占用2孔，备份1孔。5000～1万信息点，主干管道管孔容量8孔中，智能接入线缆占用不少于4孔，通信占用3孔，备份1孔。1万信息点以上，应根据建筑物分布情况，适当增加管道容量。

0～1000信息点，主干管道（分散分布）管孔容量4孔中，智能接入线缆占用不少于2孔，通信占用1孔,备份1孔。1000～2000信息点，主干管道（分散分布）管孔容量5孔中，智能接入线缆占用不少于3孔，通信占用1孔,备份1孔。2000～5000信息点，主干管道（分散分布）管孔容量7孔中，智能接入线缆占用不少于4孔，通信占用2孔,备份1孔。5000～1万信息点，主干管道管孔容量12孔中，智能接入线缆占用不少于6孔，通信占用5孔,备份1孔。1万信息点以上，应根据建筑物分布情况，适当增加管道容量。

0～1000信息点，配线管道（集中分布）管孔容量5孔中，智能接入线缆占用不少于2孔，通信占用2孔,备份1孔。1000～2000信息点，配线管道（集中分布）管孔容量6孔中，智能接入线缆占用不少于2孔，通信占用3孔,备份1孔。2000～5000信息点，配线管道（集中分布）管孔容量12孔中，智能接入线缆占用3孔，通信占用9孔。5000～1万信息点，配线管道（集中分布）管孔容量18孔中, 智能接入线缆占用4孔，通信占用14孔。

0～1000信息点，配线管道（分散分布）管孔容量6孔中，智能接入线缆占用不少于2孔，通信占用3孔,备份1孔。1000～2000信息点，配线管道（分散分布）管孔容量10孔中，智能接入线缆占用不少于3孔，通信占用6孔,备份1孔。2000～5000信息点，配线管道（分散分布）管孔容量18孔中，智能接入线缆占用4孔，通信占用14孔。5000～1万信息点，配线管道（分散分布）管孔容量24孔中，智能接入线缆占用6孔，通信占用18孔。1万信息点以上，应根据建筑物分布情况，适当增加管道容量。

0～2000信息点，建筑物的接入管道管孔容量3孔中，智能接入线缆占用不少于1孔，通信占用1孔，备用1孔。2000～1万信息点，建筑物的接入管道（集中分布）管孔容量5孔中，智能接入线缆占用不少于1孔，通信占用3孔，备用1孔；（分散分布）管孔容量4孔中，智能接入线缆占用不少于1孔，通信占用2孔，备用1孔。1万信息点以上，应根据建筑物分布情况，适当增加管道容量。

2000～5000信息点，机房在民用建筑群（集中分布）的配套建筑内的接入管道管孔容量15孔中，智能接入线缆占用4孔,通信占用11孔。5000～1万信息点，机房在民用建筑群（集中分布）的配套建筑内的接入管道管孔容量22孔中，智能接入线缆占用4孔，通信占用18孔。2000～5000信息点，机房在民用建筑群（分散分布）的配套建筑内的接入管道管孔容量22孔中，智能接入线缆占用4孔，通信占用18孔。5000～1万信息点，机房在民用建筑群（分散分布）的配套建筑内的接入管道管孔容量30孔中，智能接入线缆占用6孔，通信占用24孔。1万信息点以上，应根据建筑物分布情况，适当增加管道容量。

若固定通信机房与有线电视机房分开建设时，主干及接入管道按各自管孔数量需求分开设计。

5.2.4 园区物联接入网

1. 园区物联接入网用于园区感知终端的接入，应基于业务需求选用数字化、标准的通信网络。根据不同感知终端部署环境，宜选用合适的联接技术。
2. 新建园区的物联接入网宜采用满足IPv6协议的Ethernet、光纤、宽带PLC、Wi-Fi 6、NB-IoT有线无线标准的传输方式， 扩建或改建园区的物联接入网综合考虑原有IPv4系统的兼容，联接感知执行终端。
3. 园区物联接入网应考虑安全可信，支持感知终端基于证书的IEEE802.1x与ITU-T X.509数字证书的方式认证接入到园区网络中。

5.2.7 移动通信网

依据工信部通信〔2020〕49号《工业和信息化部关于推动5G加快发展的通知》的一（二）加大基站站址资源支持中提到的“鼓励地方政府将5G网络建设所需站址等配套设施纳入各级国土空间规划，并在控制性详细规划中严格落实；在新建、改扩建公共交通、公共场所、园区、建筑物等工程时，统筹考虑5G站址部署需求”制定。

5.2.8 无线局域网

无线局域网应基于Wi-Fi 6（802.11ax无线局域网标准）及以上技术标准进行设计。

5.2.9 其他要求

1. 网管系统应具备基于AI能力自动进行网络故障分析及定位功能。
2. 网管系统应具备安全性风险分析能力，可以对加密及非加密流量进行分析，识别威胁。
3. 网管系统应具备终端访问追溯功能，识别出终端类型、用户名、连接的AP、交换机端口、连接问题的能力。

5.3 边缘节点

5.3.1 边缘计算节点注重于计算功能，为满足园区对特定应用计算的需求而设置。边缘网关节点注重于接入功能，是为满足园区内各类终端及用户提供各类接入方式并回传至上级网络。

5.3.2 边缘计算节点设置的目标是为满足低时延、高带宽的应用需求，实现在网络边缘或用户侧提供应用所需及计算、存储能力，减少对核心网络的资源占用，降低网络时延。

5.3.3 边缘网关节点设置的目标是为满足多样性终端的接入并上传数据的需求，实现在网络边缘侧提供多样化接口满足各类终端的接入，并向上提供多种回传接口的能力。

5.3.4 边缘计算节点注重于计算功能，在网络边缘或用户侧提供应用所需的计算、存储能力，以减少对核心网络的资源占用，降低网络时延。

5.3.5 边缘网关节点注重于接入功能，在网络边缘侧提供多样化接口满足各类终端的接入，并向上提供多种回传接口的能力.

**6 数字平台层**

6.1 一般规定

6.1.1 通过数字平台的构建，可以与智慧园区各层级进行协同：

对感知执行层，主要体现为设备/系统应具备设备接入能力、设备数字化描述能力、被管理的能力、安全能力等，宜支持将各类总线信号转化为IP网络信息，应支持无线化、少线化的趋势。

对通信传输层，具备边缘计算能力、边缘存储能力、边缘视频分析能力、边缘物联节点等一个或多个能力，数字平台层通过通信传输层进行前置计算、存储功能到网络边缘、或用户侧，减少对核心网络的资源占用，降低网络时延。提供信息通信的管道设施,具备标准化网络接口，支持与多种网络进行数据传送的能力，满足数据传输的时延、带宽等要求。

对数字平台层，汇聚除了感知执行层的数据，还应采集和汇聚智慧园区各个信息化应用系统的信息，实现园区全方位数据的综合处理，并封装感知执行层的设备的所有查询、操控、升级等指令，提供数据和业务服务供智慧应用使用。

对智慧应用层，基于数字平台提供的数据和业务服务，实现各类创新智慧应用。

数字平台层包括以下三层：



图6.1.1 数字平台分层架构图

6.1.2数字平台的建设，满足模块化、积木化原则，达到实现平台生态化的目标：

模块化：在一个复杂系统中，把功能分解为特定的子功能，这些完成特定的子功能的部件可以称为模块，所有模块组装起来后整体完成系统的功能；

积木化：在复杂大型系统中，进行模块拆分时，定义模块间的统一对接标准，降低平台能力的耦合程度，使得模块可以像积木一样按需选取、任意组合，也能够满足特定的功能。

通过模块化和积木化的架构设计原则，达成平台生态化应用的目的。平台的ICT能力和承载的应用都可以引入生态能力进行替换，按需组装形成满足多业态需要的解决方案：

1. 通过对智慧园区业务实体对象的统一建模和对象固有属性和能力的抽象，形成业务资产的沉淀和封装，数据统一在业务资产内部进行管理，园区不同的业务逻辑使用业务资产进行编排，形成复杂的智慧应用，实现数据与逻辑解耦。
2. 通过平台和应用的分工，平台负责主数据的管理，应用负责数据的使用，实现管用分离；平台按照标准服务的形式提供业务服务，实现平台和应用的解耦；除了主框架之外，应用之间也进行解耦，来满足应用的可替代性。
3. 通过在ICT能力层的积木化设计，将ICT能力和平台解耦，平台可以按需引入平台生态中的ICT能力，也可以按需裁剪ICT能力。

6.1.3 数字平台按照统一性原则构建数据湖和物联标准，通过统一数据湖定义规范数据的描述，通过统一定义不同的设备的物模型规范设备的描述、属性和操作，满足帮助智慧应用基于统一业务语言进行快速的构建和交互；数字平台还定义应用的门户入口一致，界面风格一致，服务接口协议一致，运维统一，安全标准一致，最终表现为系统整体体验一致，多个不同的智慧应用天然可以融为一体，避免系统割裂。

6.2 云平台层

6.2.1 智慧园区数字平台部署的主要形态应包含公有云、私有云、混合云、边云协同等一种或多种。其中：

1. 混合云一般指私有云和公有云结合，由于当地法律法规要求，或者用户在私有数据中心内已经建设云等原因，综合考虑成本、效率等多种因素，用户可能不会将所有业务应用和信息放置到公有云上，会根据实际需要选择混合部署组网模式。
2. 边云协同部署是一种新型部署形态，属于混合云的一种特例，其主要特点在于业务在客户机房运行，管理在公有云上进行，可以实现本地资源最小化的前提下获得更大程度的数据掌控度。

云平台层可以根据需要部署在客户的本地机房。

6.2.2 云平台层宜提供弹性云服务器服务，用于部署平台软件及应用系统。为了自动适配业务的弹性伸缩，提升使用效率，降低成本，从而配置弹性伸缩服务，自动调整计算资源，使云服务器数量自动随业务负载增长而增加，随业务负载降低而减少，保证业务平稳健康运行。

1. 弹性云服务器支持自助开通、按需使用、灵活计费。
2. 弹性云服务器支持多种规格类型、支持规格变更、多种镜像类型、多种不同性能速率的磁盘种类。
3. 弹性云服务器具备数据高可靠、弹性调整、安全防护、高效运维等特点。
4. 弹性云服务器支持负载均衡将访问流量自动分发到多台云服务器，扩展应用系统对外的服务能力，实现更高水平的应用程序容错性能。

6.2.3 云平台层宜提供云容器引擎服务，提供高度可扩展的、高性能的企业级容器编排集群，支持运行容器。借助云容器引擎，客户可以在云上轻松部署、管理和扩展容器化应用程序。

1. 云容器引擎服务支持自动化部署、大规模可伸缩、应用容器化管理。
2. 在生产环境中部署一个应用程序时，通常要部署该应用的多个实例以便对应用请求进行负载均衡。
3. 云容器引擎服务支持通过云容器引擎创建容器集群，支持通过云容器引擎自动化部署和一站式运维容器应用，使得应用的整个生命周期都在云容器引擎内高效完成。
4. 云容器引擎服务支持直接使用高性能的弹性云服务器、裸金属服务器、GPU加速云服务器等多种异构基础设施，根据业务需要在云容器引擎中快速创建混合集群、鲲鹏集群、裸金属集群和GPU容器集群等业界常见集群，并通过云容器引擎对创建的集群进行统一管理。
5. 云容器引擎服务支持多种网络访问方式，支持四层、七层负载均衡，满足不同场景下的访问诉求。
6. 云容器引擎服务支持多种持久化存储卷，如本地磁盘存储、云硬盘存储卷、云文件存储卷、云对象存储卷和云极速文件存储卷。
7. 云容器引擎服务提供工作负载和可用区、工作负载和节点以及工作负载间的亲和性/反亲和调度。可根据业务需求设置亲和性，实现工作负载的就近部署，容器间通信就近路由，减少网络消耗；也可对同个工作负载的多个实例设置反亲和部署，减少宕机影响，对互相干扰的应用反亲和部署，避免干扰。
8. 云容器引擎服务支持集群节点、工作负载的弹性伸缩，支持手动伸缩和自动弹性伸缩，并可以自由组合多种弹性策略以应对业务高峰期的突发流量浪涌。
9. 云容器引擎服务支持非侵入式的微服务治理生态支持，应支持常见生态应用服务网格和标准模板。应通过应用服务网格支持非侵入式的微服务治理解决方案，支持完整的生命周期管理和流量治理能力。

6.2.4 云平台层可提供云硬盘服务,为云服务器提供高可靠、高性能、规格丰富并且可弹性扩展的块存储服务，可满足不同场景的业务需求，适用于分布式文件系统、开发测试、数据仓库以及高性能计算等场景。

1. 云硬盘服务支持多种性能规格云硬盘，满足不同业务场景需求。
2. 云硬盘服务支持弹性扩展、备份恢复、数据共享等关键特性。
3. 云硬盘服务确保安全可靠，应支持分布式多副本技术，能够保证任何一个副本故障时快速进行数据迁移恢复，数据可靠性高，避免单一硬件故障造成数据丢失；应支持数据加密，且加密过程应用无感知，安全便捷。

6.2.5 云平台层可提供弹性文件服务，能够采用多级可靠性架构，提供按需扩展的高性能文件存储，为云上多个弹性云服务器，容器，裸金属服务器提供共享访问文件，支持通过秘钥方式加密文件，支持通过标准协议访问数据，无缝适配主流应用程序进行数据读写。

1. 弹性文件服务通过多级可靠性架构，保障数据持久性和服务可用性。
2. 弹性文件服务提供多种文件存储服务，应支持高读写、低时延或高带宽等不同性能特点的业务场景。
3. 弹性文件服务提供托管的文件存储服务，无须关心底层硬件基础设施，避免了部署、维护硬件带来的复杂性。
4. 弹性文件服务提供云安全技术保障，保护用户数据安全，应确保用户间数据隔离。

6.2.6 云平台层可提供对象存储服务，为视频、图片等非结构化对象提供低成本、高可靠性的存储系统，满足原始视频或图片的存储，并且通过高性能的带宽和时延满足视频分析应用的数据需求。对永久保存的数据提供归档存储大幅降低数据存储成本。

1. 对象存储服务通过多级可靠性架构，保障数据持久性和服务可用性；
2. 对象存储服务通过可信云认证，应支持服务端加密、防盗链、IP黑白名单、VPC网络隔离、日志审计、细粒度权限控制，保障数据安全可信；
3. 对象存储服务支持智能调度，辅以传输加速、大数据垂直优化等技术，致力于为用户提供高并发、大带宽、稳定低时延的数据访问体验；
4. 对象存储服务支持管理控制台和API两种管理方式，提供多种语言的SDK，兼容主流的客户端工具。

6.2.7 云平台层可提供弹性负载均衡服务，将访问流量根据转发策略分发到后端多台弹性云服务器的流量分发控制服务，可以通过流量分发扩展应用系统对外的服务能力，提高应用程序的容错能力。

1. 弹性负载均衡服务支持集群、双机、本地多机房甚至异地机房、同城双活容灾等各种场景下的负载均衡：
2. 弹性负载均衡服务支持应用流量自动进行分发，与弹性伸缩服务无缝集成，灵活扩展应用对外服务能力；
3. 弹性负载均衡服务支持快速部署、实时生效，支持多种协议，支持多种调度算法，支持高效管理和调整分发策略。

6.2.8 云平台层可提供分布式缓存服务，支持双机热备的HA架构，提供单机、主备、集群等多种部署方式，满足高读写性能场景及弹性变配的业务需求。

1. 分布式缓存服务支持双机热备或者集群部署，主机故障时秒级切换，应用无感知；
2. 分布式缓存服务支持多种规格的缓存服务，例如主备、集群、单机等，支持不同硬件配置规格；
3. 分布式缓存服务支持在线扩容能力，支持在线一键式完成扩容，应用无感知；
4. 分布式缓存服务支持数据的持久化机制，缓存数据可高速写到物理磁盘，避免数据丢失；同时支持数据备份机制；
5. 分布式缓存服务支持网络和租户的隔离、流量过滤、访问授权、身份认证、安全审计等安全措施；
6. 分布式缓存服务提供监控运维能力，可提供常见运维监控指标和统计接口、可触发告警；

6.2.9云平台层宜提供即开即用、稳定可靠、弹性伸缩、便捷管理的在线云关系型数据库服务，支持业界主流的关系型数据库。

1. 云关系型数据库服务支持即开即用，服务应具备软硬件部署、弹性扩容、自动备份、补丁升级、监控告警、故障转移等功能，用户免运维；
2. 云关系型数据库服务支持高并发情况下，业务稳定运行、低时延，保证数据不丢失；
3. 云关系型数据库服务支持业务数据量突增时，快速完成实例扩展；
4. 云关系型数据库服务提供业界主流的关系型数据库，兼容开源主流产品。

6.2.10 云平台层宜支持云解析服务，提供高可用、高性能、高扩展的权威DNS解析服务和DNS管理服务，把常用的域名或应用资源转换成用于计算机连接的IP地址，从而将最终用户路由到相应的应用资源上。要求时延低、安全性高，防劫持、防DDoS。

1. 云解析服务支持高性能的内网域名解析服务，要求时延低、安全性高，防劫持、防DDoS；
2. 云解析服务支持从IP到域名的反向解析能力，用于用户特定需要场景；
3. 云解析服务提供高效稳定的解析能力，单节点支持千万级并发能力。

6.2.11 云平台层应具备安全服务，确保业务无忧、数据无忧：

1. 安全服务宜支持网络层和应用层的DDoS攻击防护，并提供攻击拦截实时告警，有效提升用户带宽利用率，保障业务稳定可靠；应支持配置高防IP，将攻击流量引流到高防IP，确保源站稳定可靠，确保用户在遭受大流量DDoS攻击下业务平稳运行；
2. 安全服务宜提升主机整体性安全能力，提供资产管理、漏洞管理、入侵检测、基线检查等功能，降低主机安全风险；应能够扫描容器镜像中的漏洞，以及提供容器安全策略设置和防逃逸功能；
3. 安全服务宜支持安全编码检查、主机、数据库、WEB漏洞、业务逻辑漏洞扫描等能力，提高弱密码扫描、安全基线检测、定期巡检等能力；支持恶意请求和未知威胁的智能识别和防御；
4. 安全服务宜支持数据脱敏、数据库审计和防注入攻击等功能，保证数据存储安全；支持数据加密服务；
5. 安全服务宜支持SSL证书管理、堡垒机等服务，提供多种安全管理手段；应支持智能防护，对安全攻击进行感知、预测、处置等强大的安全态势管理能力；支持安全专家服务。

6.3 ICT能力层

6.3.1 ICT能力作为数字平台内部技术部件，提供给平台本身及智慧应用可重用的服务能力，明确系统边界和对接标准，实现能力共享，达到能力价值最大化的目的。

1. 常见的ICT技术能力宜包括人工智能技术、大数据技术、视频分析技术、物联网管理平台、定位技术、地理信息技术、建筑信息管理技术等。
2. 技术能力在数字平台进行统一封装，封装后的服务以标准WEB服务协议的形式进行暴露，采取相同标准服务接口的技术部件可以进行替换，以满足多样化的园区场景，避免各个应用单独引入ICT能力造成的成本浪费和重复建设。
3. ICT技术能力的引入，基于相同的标准打造ICT技术生态，所有经认证满足标准的ICT技术可引入到数字平台，避免对某个特定产品和技术的依赖。

6.3.2人工智能技术应满足平台及应用的需要，支持业界主流算法框架，支持多内核、多框架的模型训练、推理和服务调用，支持可插拔、可替换、可升级。

1. 支持多种业界主流算法框架、主流内核处理器、主流计算芯片的模型训练和推理。
2. 支持边云协同部署架构，支持云上训练云下推理、云上训练云上推理、云下训练云下推理等多种方式。
3. 支持园区常见的视频类分析、图片类分析，如视频周界、人脸识别、车辆识别等算法推理；支持推理结果上发至云端，最终产生业务告警。
4. 支持插拔人工智能技术，实现平台的轻量化。
5. 支持新的训练数据训练优化后的算法模型，进行算法模型升级，应支持废弃旧的算法模型，升级安装新的算法模型。

6.3.3 大数据技术提供企业级大数据存储、查询、分析的能力，支持存储大容量数据仓库，支持对流式数据进行实时在线运算处理，支持数据集成、数据建模、数据分析、数据治理等系列化工具；大数据技术应支持独立部署及能力裁剪。

1. 支持非结构化/半结构化/结构化大容量数据仓库，支持各类海量数据的存储和管理；
2. 在智慧园区的引用上应具有更多的灵活度，支持中小型园区场景下使用轻量化的关系型数据库；
3. 支持流式数据处理引擎，应具有高吞吐、低时延、高可靠等特性，性能要求达到毫秒水平，处理的可靠性可以达到精确一次，同时支持多租户资源隔离，更适合企业级流处理场景；
4. 支持独立部署，对平台及智慧应用进行支撑，在不需要的场景下，支持对大数据能力进行裁剪。

6.3.4 视频技术应以服务方式提供视频资源共享和视频处理分析能力开放，支持对视频流的接入管理、存储、分析、播控、检索、转码等能力，支持功能组合和拆分部署和使用，支持边云协同部署、单台部署、集群部署、级联部署等多种部署形态。

1. 支持视频监控、视频分析、视频检索能力。视频监控功能应包含视频的接入管理、摄像头的管理、视频的调阅、视频的实时监控等；视频分析功能应对视频流进行视频分析，如人脸识别、车牌识别等；视频检索功能应支持对视频进行检索，查找特定的特征体，常用于布控，如人脸布控、车辆布控等，也包括以图搜图能力。
2. 视频存储，考虑到大带宽的要求，宜部署在园区的边缘节点，提供边云协同的能力，支持云上播放和控制。
3. 视频分析，考虑到大带宽的要求，宜部署在园区边缘计算节点，支持边云协同能力，支持云上算法推送到边缘计算节点，丰富视频算法的引入，灵活扩展视频分析的能力。
4. 支持实时监控、视频流转发、录像、备份、告警、语音对讲、语音广播，支持运营管理，大幅提高视频监控效率。
5. 支持人脸识别、人体特性识别、活体识别、车辆特征识别、以图搜图、视频摘要、视频搜索等功能；
6. 支持多种功能的组合和拆分，支持边云协同部署、单台部署、集群部署、级联部署等多种部署形态。
7. 支持通过数字水印和媒体安全传输，保证视频文件的可靠性和安全保密性，支持国标GB35114双向认证。
8. 支持独立部署，对平台部件及智慧应用进行支撑，在不需要的场景下，支持对视频技术能力进行裁剪。

6.3.5智慧园区管理应是一个立体空间的管理，既涉及建筑内多楼层的管理，也有园区内建筑分布的管理，还有市政道路及市政基础设施的管理。在这个立体空间中，管理着众多与空间有关的相对静态数据和动态变化的数据，包括：园区的建筑基础信息，水电管网等设施基础信息，公共道路及管道，空调、水暖、消防等BA楼控信息，资产、人员、车辆管理等物业信息，人、车、物的位置信息，园区设施的安全运行状态信息，ICT基础设施分布和使用信息等。

1. 宜支持二三维一体化的地理信息系统，实现对园区空间静动态数据的采集、储存、管理、运算、分析、显示，并支持与位置服务系统集成，实现室内的人员定位与导航基本功能。
2. 宜引入建筑信息模型技术，对园区的规划、设计、施工、维护、运营等生命周期环节，利用信息化数据，对建筑模型、内部结构、建筑内对象参数、空间几何体系、对象关系等能力进行可视化呈现和管理。
3. 宜支持定位技术，基于蓝牙、Wi-Fi、基站、惯性导航等融合定位技术，实现高精度终端定位能力，并在地图上进行呈现。
4. 宜引入城市信息模型技术，对建筑信息技术、地理信息技术甚至物联技术进行结合，形成三维立体的园区信息模型，实现各类空间数据和物信息的统一管理和可视化呈现，并可结合物联控制技术，实现可视化的操作。
5. 园区内的市政道路及市政基础设施，是城市规划发展的一部分，也作为园区信息模型的一部分进行管理。
6. 相关技术应支持独立部署，在园区不需要该技术的场景下，平台可以对该技术进行裁剪。

6.3.6 物联网管理平台，需要跟边侧物联网关、端侧设备/系统配合协调作用，实现对端侧设备/系统的信息采集上报，主动管理和控制端侧设备/系统；应通过标准物模型来定义园区的环境、设备、系统等，实现物的标准化操作，并支持模型快速适配能力。

1. 物联网管理需要云、边、端进行协同完成，云端统一定义物的数字标准化描述及运用，边侧物联网关实现设备的管控、策略及标准化，端侧感知执行层体现设备/系统接入能力、设备/系统数字化描述能力、被管理的能力。
2. 智慧园区应支持对接多个物联网厂商，提供统一的标准物模型定义，供智慧应用遵循标准接口进行调度和控制。
3. 智慧园区的物联对接能力应提供标准的接口定义，支持遵循标准接口的生态物联厂商直接对接，减少对单一厂商的依赖；
4. 智慧园区的物联模型的对接适配，应提供轻量化的适配对接工具，帮助不同的设备/系统快速对接；

6.4 业务服务层

6.4.1 数字平台的业务服务包含四个方面：

1. 应用服务：主要提供实体对象的建模和应用资产；应用实时业务的服务。
2. 数据服务：主要提供主题库的建模和数据资产；应用分析或统计的服务。
3. 集成服务：主要提供设备/系统的集成对接资产；设备查询、操作、控制的服务。
4. 开发服务：主要提供在线开发IDE平台、界面组件资产及敏捷开发运维一体化系列流程工具；运行态分布式服务框架。

数字平台的资产沉淀包含两层含义，一层是指提供数字资产的沉淀，包括公共服务资产、行业知识资产、数字孪生资产、框架应用资产等；一层是指积累数字资产的能力，本质上是一系列工具。

6.4.2 应用服务主要提供的是实时交互的服务能力，比如实时查询设备状态、实时处理告警信息、实时控制门禁、实时记录日志、实时处理工单等；支持复用伙伴或客户已有服务，在平台托管伙伴生态的服务能力，共同支撑智慧应用创新。

1. 应用服务提供的服务应包含公共服务资产、行业知识服务资产、数字孪生资产。
2. 应用服务应支持生态伙伴的服务能力或客户原有系统服务，托管至平台进行服务编排提供更多的服务能力。

6.4.3 数据服务提供数据从建模、采集、清洗、加工、聚合等端到端的数据处理分析流程，并按照智慧园区的典型对象构建和沉淀主题库和专题库等数据资产，以标准化WEB服务的协议提供服务，便于智慧应用进行趋势判断、数据运营、辅助决策、智能分析，是智慧园区通过数据驱动运营获取数字化转型能力的必要手段。

6.4.4 集成服务是一站式的集成编排工具及基于工具开发的系列化集成资产，集成资产的目的是预集成和认证各类设备/系统，构建生态标准接口，实现项目中认证设备/系统即插即用即开通，减少项目集成活动，提升集成效率，降低交付成本。

1. 集成编排工具提供的能力包括：数据集成、API集成、消息集成等；
2. 数据集成支持从各种异构数据源提供数据同步功能，支持跨云、跨网络、跨数据中心的数据同步，支持根据数据源插件化扩展能力；
3. API集成提供API接入开放网关，支持API的注册、发布、路由、流控、升降级和接入认证等能力；
4. 消息集成支持跨云、跨网络、跨数据中心消息中间件，支持消息的发布与订阅，多集群部署，支持消息轨迹跟踪。消息集成模块提供消息的发布、订阅、存储、跨中心路由和跨云传输，并支持安全接入和轨迹跟踪；
5. 系统标准集成接口按照生态模式提供集成标准接口，生态符合标准的设备/系统均支持直接对接，降低项目集成工作量，降低交付及更成本。

6.4.5 开发服务宜提供在线可视化开发IDE，采用元数据建模、流程引擎、服务编排、可视化UI开发等工具技术，实现智慧应用软件快速开发；提供的工具包括：

1. 提供UI展示单元与交互的描述与封装工具，支持界面开发；
2. 提供元数据定义模型的界面和元数据引擎机制，支持数据库模型开发；
3. 提供脚本开发机制，支持后台服务开发；
4. 提供不同IT系统的适配工具；
5. 提供业务开发、测试、发布、集成、部署、升级、运维等工具。

6.4.6 业务服务层的物联服务，是典型的设备的抽象服务，提供以下功能：

1. 设备在系统中的增删改查等基本的生命周期管理、安全鉴权等；
2. 设备静态信息的维护，包括品牌、型号、归属、位置、标签等信息；
3. 设备的运维信息，设备的特殊状态管理；
4. 设备升级包版本，升级通知，升级操作等；
5. 设备健康度管理：设备诊断，设备调试，设备唤醒等；
6. 设备与业务关联信息：组合、聚合关系、时间维度、空间维度、业务归属、规则属性等；
7. 设备仿真信息：维护保养、仿真模拟、设备损耗计算、复现故障等；
8. 设备的人工智能运用：结合人工智能技术，实现自动辨识、趋势判断、预判异常、预测未来等高级数字孪生特性。

**7 智慧应用层**

7.1 一般规定

7.1.1 智慧园区应围绕现代园区的经济活动，适应职住平衡、区企一体、产城融合等现代园区的发展需要，提供以下智慧化的应用、服务、管理：

1. 园区有别于住区、社区，应聚焦于生产、科研、服务等经济活动，提供智慧化的服务与支撑。
2. 现代园区要求职住平衡，提升园区的生活配套设施，提高园区生活的便利度、体验感、科技性，满足科技人才的生活需要。
3. 伴随现代园区的发展，呈现为区企一体的特征，融入了物业管理、社区活动、医教文体等社区服务功能，需要通过智慧化来实现。
4. 随着现代园区的规模化发展，加快了产城融合，园区成为城市的重要构成，并承担着园区内的城市公共服务职能，需要与智慧城市对接。

7.1.2 智慧园区宜对接智慧城市（社区），上报园区管理信息，满足智慧城市（社区）的管理与服务等需要。

1. 智慧园区需要配合智慧社区的网格化管理系统，对接智慧城市（社区），协调管理园区的人口、户籍、卫生、治安、防疫等相关事务；
2. 智慧园区宜链接智慧城市系统，获取园区周边的道路交通、公共交通、共享交通等信息，为园区内用户提供智慧出行等信息服务；
3. 在有条件的城市、社区，智慧园区应能接入城市（区）能源管理平台，提供园区、以及园区公共建筑等能耗数据，满足智慧城市的绿色可持续发展需要。

7.1.3 智慧应用层所提供的各种智慧场景应用，构建于数字平台层的云生态系统之上，从数字平台层获取各种数据，借助数字平台层提供的各种信息处理工具，完成大数据分析，剔除错误的信息，获得精准的研判，做出系统性、协同化的决策，组织、协调各类园区机电设施的运行。

7.1.4考虑到数字软件还需要经过长期实证检验，智慧应用技术并不能承担行为人的责任，需要将园区管理的职责落实到人，特设置此项规定。

1. 智慧应用管理层应用各种算法，形成一项或多项决策的建议，存在信息错误、算法错误等风险，还需要经过人的判断、甄别，化解决策风险；
2. 在园区管理体系中，各种职责落实到人，责任人承担了本级管理的责任、风险，智慧应用层无替代人的职责。

7.1.5 智慧园区鼓励采用成熟、先进的技术，可采用以下高新技术提高体验感：

1. 通过园区网站、公众号、APP应用程序等数字化系统，实现移动化的园区消费、服务、管理、办公等业务，改善智慧园区的获得感。
2. 采用成熟的三维可视化技术，构建园区的数字孪生平台，部署数据仓与仪表盘，集成联动各个弱电子系统，实现园区的全景可视、全息感知、全域可控，满足智慧园区的运维、操作、指挥、调度等管理需要。
3. 数字孪生平台融合园区企业分布、道路分布、人口分布、建筑物三维模型、全景图，结合传感器实时监测和预警全要素数据，构建园区监测预警一张图，直观操控环境监控、设备管理、应急响应、绿色园区等园区业务。
4. 具备多种语音交互能力，通过人与平台、机器、建筑、园区等语音对话，触发各类应用服务，改善园区服务的体验感。
5. 部署无人机、机器人等机动设施，提高监控盲点、突发事件等信息的采集能力，创新园区的科技体验感。

7.1.6 智慧应用层的软件编制，应满足以下编制要求：

1. 应提供简体中文图形界面，具有可视化、图形化、简单化等特点，便于操作、使用；
2. 应采用标准化、结构化、模块化的数据结构，具有开放性的数据格式、传输协议、系统接口，支持虚拟化业务；
3. 应符合数字平台层的应用统一体验、统一业务访问、统一业务权限认证等相关规定；
4. 软件的功能性、可靠性、易用性、效率、维护性、可移植性等，以及软件的有效性、生产率、安全性、满意度，应满足软件工程产品质量标准；
5. 软件产品中涉及的中文代码、中文字型、中文输入法等，均应符合相关的国家标准；
6. 软件应提供安装、使用、维护说明书，提供产品标识和运行环境说明。

7.1.7由于软件产品应用所存在的极大不确定性，一旦发生意外可能导致较大的损失，需要通过专业化测试。对软件产品的测试与认定又具有极强的专业性，为了确保智慧应用管理层能够顺利实现设计场景，故要求核心软件产品、核心技术在使用前必须通过第三方检测机构测试。

7.2 企业事业服务

7.2.1智慧园区应服务于政、产、学、研、资、介、贸等企事业单位的经济活动，提供必要的信息化平台，满足入驻单位的信息化业务需求。

7.2.2 智慧园区提供信息化服务，包括以下内容：

1. 招商业务宜包括招商范围、招商政策、产品类型、产业配套、数字园区等信息服务；
2. 入驻业务宜支持企业入驻、装修、开业、运行、扩张、退出等提供全过程服务，可满足客户入住的需要；
3. 产业对接业务宜支持产品的研发、小批量生产、检测测试、大规模生产、市场拓展等上下游产业对接服务；
4. 园区仓储物流服务平台宜具备仓储实时监控、物流车辆监管、智慧物流系统等信息化功能；
5. 人才服务平台宜提供线上人才交流、人力资源服务、协助人才引进落户等信息化服务；
6. 知识产权业务宜满足园区企业在专利申报、专利展示、专利交易等方面的需求，有助于促进知识产权创造、保护和交易转化；
7. 政策咨询业务宜提供政策发布、政策解读、政策咨询、政策申报指导、政策代办等业务信息；
8. 专业咨询业务宜包括法律、财务、税务、管理等专业性咨询服务。

7.2.3 智慧园区应能获取以下公共信息服务：

1. 链接城市（社区）的电子政务平台，获取工商注册、安全生产、政策查询、项目申报、人才引进、税务等公共服务；
2. 链接社会的金融服务平台，获取融资产品、优惠政策、典型案例等金融服务，满足线上、线下融资的对接需要；
3. 链接社会的电子商务服务平台，获取电子货币交易、电子数据交换、供应链管理、市场网络营销、在线事务处理等服务，附带园区外的物流配送服务。

7.2.4智慧园区可基于自身的市场、经济、资本等优势，联合社会投融资企业，以多种形式扶持科创企业，孵化科技创新企业，满足园区可持续发展需要。

7.2.5进入信息化时代，企业无法脱离网络而发展，却又往往缺乏网络建设、运维的专业技术人员与资金，需要智慧园区提供相关的技术服务、租用业务、支撑业务。智慧园区统一建设运维园区信息、网络、云服务体系，可以降低入驻企业的开业成本，扶持创新企业发展壮大，增强智慧园区的客户黏性。

7.2.6 产、学、研相结合，是智慧园区的重要经济活动。通过数字化工厂，模拟生产过程，发现、解除从研到产过程的各种不确定性，有助于提高成果转化的周期、质量，快速形成园区经济的生产力。

7.3 公共信息服务

7.3.1 智慧园区宜提供以下公共信息服务：

1. 信息服务包括市政业务、社区服务、园区管理、建筑环境；
2. 满足社区服务站、警务室、卫生防疫站、劳动保护站、社区图书馆、志愿者之家等信息化服务的需要；
3. 支持园区的政务公开、社团活动、社情共享、民情互动；
4. 提供园区的衣、食、住、行、娱、购、游、健等生活便利。

7.3.2 智慧园区可提供以下市政、园区等信息化业务

1. 链接智慧城市公共服务平台，提供户籍、就业、社保、城管、交通、公安、环境、卫生、气象、基建等相关业务，涉及位置服务、业务预约、网络办理、线上支付、进度查询、投诉评价等服务；
2. 在线办理园区内的供电、供水、供气、广电、通信等市政业务，在线办理租赁、入住、办卡、出入、报装、报修、报事、缴费等园区事务，具备电子缴费、账单查询、电子票据等功能；
3. 提供园区的其他便民服务，包括但不限于公交、教育、健康、医疗、养老、托育、家政、文旅、公益、科普、法律等社会服务。

7.3.3 智慧园区可提供以下电子商务：

1. 可提供商户位置查询、在线预约、网上购物、送货上门、家政中介服务、健康保健业务、汽车租赁、求职招聘等服务；
2. 可具备电子数据交易、电子货币交易、在线事务处理、供应链管理、区块链应用等信息化功能；
3. 可提供网页管理、电子账户、网上订购与支付、电子账户、用户管理、商品管理、交易管理、物流管理等信息化服务。

7.3.4 智慧园区可通过门户网站，提供以下公共信息服务：

1. 为企业提供线上线下宣传、展厅展览、纸媒电视、新媒体等网络服务，满足企业品牌与成果展示等需要；
2. 构建网络交互空间，提供沙龙论坛、文体活动、知识分享、技能培训等网络服务，满足企业文化生活的需要；
3. 提供动态新闻发布、招商就业信息、便民服务指南、重大信息公布、园区发展论坛等信息服务；
4. 发布园区防疫、康养、托养、医护、健康、家政等公共信息。
5. 发布园区的道路、交通、停车等信息，提供园区内外交通引导信息。
6. 提供园区的水电、物业、公共安全、信报与物流箱等相关信息。
7. 构建社团建设、居民自治、邻里交流、关爱帮扶、服务热线等信息化平台，提供在线咨询服务，共享园区文化资源；
8. 为园区社团建设、居民自治等，提供信息化服务，实现园区政务公开、社情共享、民情互动；
9. 提供个人网页建设，包括个人主页、个人相册、个人活动、我的日志、我的群组、我的一家、个人信息、留言墙等网络空间；
10. 开通社区网络论坛，方便社团、个人发表意见，为持续改进园区服务收集信息；
11. 提供其他传媒、资讯、咨询等信息化服务。

7.3.5 智慧园区不得发布违规、反党、低俗、封建、迷信等信息，避免发布未经审查的广告与资讯，需要建立相应的认证、审查、签发机制。

7.4 智慧通行服务

7.4.1 智慧园区采取以下技术措施：

1. 智慧园区能监管道路、交通、车辆，动态规划出行路线，及时疏导道路交通、管制事故现场，保障园区的交通秩序；
2. 智慧园区具备智能搜索、流量统计、情报分析、行为判断、布控预警、违章报警等功能；
3. 智慧园区自动追踪入园车辆，识别车辆违规、违章、超时现象，智慧调度、管理进入园区的车辆。

7.4.2 通过物联网、视频监控、大数据分析、可视化辅助决策等技术，及时发现垃圾堆积、道路障碍、道路照明、违章占道、交通事故等问题，监控防护与警示设施的完整性，管制事故现场，清运道路障碍，疏导道路交通，保障交通秩序。

7.4.3社区网格化管理、以及园区防疫工作，需要园区实施出入园区的登记管理。智慧园区宜应用信息化、大数据技术，优化相关流程管理，方便人员出入、通行，提供人员在园区内的通行效率。

7.4.4智慧园区可采用采用物联网、视频监控、大数据分析、可视化辅助决策等技术，分析园区交通轨迹，及时发现人群聚集事件，智慧引导行人避让通行，阻止人群聚集，疏导聚集人群，避免发生意外。

7.4.5 智慧园区应具备以下行人、车辆、道路、交通、车位等信息化服务

1. 综合分析道路交通信息，显示交通热力图、态势图、轨迹图，辅助道路交通决策。
2. 协调各个路口的红绿灯状态，组织道路照明，提高道路交通的效率。
3. 根据驾驶员的指令，结合车辆的历史行驶规律，为驾驶员提供园区导航服务，并提供车位引导与反向寻车服务。

7.4.6 针对进入园区的校车、特种车辆、危险品运输车辆，可以加以识别与跟踪，给予优先通行的便利，降低此类车辆引发的风险几率。

7.4.7针对涉事、嫌疑、超重车辆，宜及时识别、追踪、布控，阻止其在园区通行，规避此类车辆引发的交通风险。

7.4.8 园区需要对出入园区的车辆、行人实施登记管理，并结合城市车辆主管部门提供的信息、园区采集的各种交通违规信息等，构建交通黑白名单，满足园区道路、交通管理等需要。

7.5 公共设施管理

7.5.1 园区的公共设施包括，但不限于：

1. 楼控、安防、消防等弱电系统，以及感知执行层的各种设备；
2. 信息设施系统、以及传输层的线路与设备；
3. 弱电机房内的工作站、服务器、存储器；
4. 配电、供电、变电、馈电系统设备；
5. 建筑电气、家用电气、办公电气、智能机电；
6. 信报箱、物流柜；
7. 室外管井与立杆、路灯、自动旗杆；
8. 红绿灯与道路交通设施。

7.5.2 停水、停电、断网等事件发生，将严重影响园区的正常经济、生活活动，必须及时识别与发现，联动有关的园区设施与设备，最大限度地保障园区供给，并组织人员抢修。

7.5.3 园区绿色健康管理需要联动相关的建筑、道路、交通等设施，园区公共安全 管理也需要调度相应的建筑、道路、交通等设备，应由公共设施管理系统协调、统一，避免不同智能场景系统各自为政，导致智慧园区运行混乱。

7.5.4 园区机房包括：弱电进线机房，消防、安防、楼控等监控中心，网络与数据机房，高低压与变配电机房，电梯机房、制冷机房、锅炉房、水泵房等。

7.5.5 针对信报箱、物流箱缺乏信息化管理，是传统园区普遍存在的问题，智慧园区宜建设智慧信报箱、智慧物流箱，提高园区的服务水平。

7.5.6 随着越来越多的人使用智能家居、智能办公等系统，需要园区提供系统托管、运维等专业化服务，智慧园区系统可响应此类用户需求，提升园区的服务品质。

7.5.7智慧园区应构建园区设施与设备档案，自动收集与分析设备、环境、资源等数据，具备信息查询、故障报警、检修提示、工单派发、检修报告等功能，包括设施与设备的采购、安装、运行、故障、检修、维护等信息。

7.6 绿色健康管理

7.6.1 智慧园区应满足以下健康、绿色等建设要求：

1. 节约资源和保护环境是我国的一项基本国策，智慧园区应能够充分融合感知层数据，对园区环境、交通、废弃物资源化、非传统水源利用、能源利用等方面进行展示、分析和指导，积极引导建设绿色生态园区。
2. 智慧园区应满足国家或地区对绿色建筑、健康建筑等要求，基于园区的全生命周期，建立完善的管理机制，保障园区整体环境质量。

7.6.2 智慧园区应根据现行国家规范与标准，实现以下绿色园区功能：

1. 绿色园区依据现行的国家标准，对室外环境进行监测和预警，监测园区内关键空气质量指标，公开区域空气质量指数AQI；
2. 绿色园区对园区内的垃圾站、锅炉房或废气排放建筑等主要污染源进行重点监测，定期公示园区环境监测结果，对异常环境监测进行警报、分析，提供处理指导意见；
3. 绿色园区对园区风热环境进行监测，具备对区域风热环境的预测分析能力，有效指导园区作业，采取措施缓解园区热岛效应，保障园区人员安全健康；
4. 绿色园区依据现行的国家标准，对发变电站、交通干道和其他园区噪声源进行监测和有效控制。对园区内医院、学校、机关、科研单位和住宅等噪声敏感建筑物（群），进行声环境监测和预测预警，防治园区噪声污染；
5. 绿色园区对园区建筑室内环境进行监测并公示，根据现行的国家标准，对温湿度、颗粒物、有害气体等主要空气质量异常进行报警，实时联动楼宇自控设备，改善室内环境参数；
6. 绿色园区对园区生活用水、非传统水源、采暖空调系统用水、景观水体等各类水质进行监测或定期检测。若水质未达到现行的国家及行业标准，应予以报警；
7. 绿色园区综合管理园区用水，按用水来源、用途、用水区域等实现用水分项计量；并对园区供水管网进行监测，及时发现供水管网的损漏现象；
8. 绿色园区监测并分析园区污染物排放情况，跟踪生产、生活产生的废水、废气、废渣等排放与处理，并针对超标准排放等现象实时报警；
9. 绿色园区提供海绵城市建设运行效果监测和评估数据，提供年雨水径流总量控制率计算，并判断是否满足现行《海绵城市建设技术指南》要求。

7.6.3 智慧园区应能提供以下能源管理功能：

1. 智慧园区应能定期收集园区建筑、公用设施的能耗数据，根据智慧园区的能源规划，采用动态逐时分析技术，与现行标准规定的引导值进行比较，合理降低园区能耗；
2. 预留与上级能耗监测平台的信息接口。

7.6.4 智慧园区应能提供以下能源应用功能：

1. 智慧园区设计应对场地及周边可获得的太阳能、风能、生物质能等可再生能源进行合理规划和充分利用。
2. 智慧园区设应着眼园区实际能源需求，分布式产能设施、区域能源输送网络、可再生能源产能与输配网络等，对传统能源规划进行补充，兼顾产能、储能、节能、用能，结合综合能源管理技术，推进多形式能源综合利用。

7.6.5本条旨在通过三个碳排放主要指标的计算和分析，对智慧园区的节能减排情况进行科学监测，指导后续园区节能减排措施制定，从而达到所在地和城区的减碳要求。

7.6.6 本章节所制定的运行策略，需要通过公共设施管理系统落实执行，避免多头管理引起系统混乱。

7.7 公共安全管理

7.7.1园区的公共安全事件，应包括火灾、自然与次生灾害、重大安全生产事故、社会治安与公共卫生事件等。

7.7.2 智慧园区应对以下公共安全事件实施响应：

1. 应与城市地质、防洪、消防、生物、海洋、气象等部门联网并实时获取灾害警示信息；
2. 自动响应断水、断电、断网、道路交通事故等突发事件，启动灾害应急处理与救援预案；
3. 及时地公示、通知、预警各种自然灾害，协调园区的设施设备、交通组织，落实灾害应急与救援预案；
4. 模拟分析自然灾害，评估风险程度，定期进行灾害防护模拟演练，提高园区灾害防护能力。

7.7.3 智慧园区应具备以下安全生产管理功能：

1. 配合安全生产监管部门，针对涉及安全生产的事项实施批准、核准、许可、注册、认证，实施安全生产标准化等级评定，并记录相关信息；
2. 针对园区生产、科研、经营单位，登记、报备、核验其消防员、安全员、特种作业的从业资格证与上岗证，定期收集上述人员的安全生产培训信息；
3. 备案储运重大危险品的仓库、车辆、司乘人员，全过程监控出入园区的危险品运输、装卸、仓储，登录涉及重大安全生产设备的维护、保养、维修信息；
4. 采集生产安全设施的运行数据，融合分析厂区各类数据，发现安全生产风险并警示，触发安全生产应急与救援预案，联动园区的公共安全系统，实施应急响应。

7.7.4 智慧园区应能提供以下智慧消防功能：

1. 应用大数据技术与智能算法，融合分析各个弱电系统采集的数据，及时发现火灾隐患，指导园区物业人员排查。
2. 融合分析火灾现场的数据，以及园区设施与设备、道路与交通等信息，规划最佳消防措施，协调各个部门的消防作业。

7.7.5 智慧园区应能应对卫生防疫工作，实现以下信息化服务：

1. 融合分析园区公共卫生基础信息，实时监控疫情防控对象的健康状况，支持公众进行疫情线索采集和投诉举报，对信息缓报、隐瞒、谎报等行为进行信息提示和警告。
2. 基于园区企业基本信息和卫生防控动态采集信息，建立疫情评估量化指标，利用大数据和地理信息系统技术，实时分析园区疫情发展趋势，绘制疫情变化态势图，为疫情防控提供可视化工作平台。

7.7.6 智慧园区应实施以下园区交通治安管理，保障园区的生活与工作活动秩序：

1. 使用视频大数据分析技术，识别、追踪危险性、或攻击性行为，预防、或及时阻止公共安全事件的发生。
2. 围绕人、房、车、警情事件等要素，通过人像比对、轨迹刻画、数据挖掘等，实时监控被关注的人员、车辆，实现异常告警、风险防控。
3. 利用信息化技术，实现警情类事件的报警响应、实时推送、快速处置、信息反馈，满足园区精细化管理的需要。

7.7.7 智慧园区应具备以下公共安全功能：

1. 通过一体化操作界面，针对园区各类安全事件，实施实时报警、联动响应、调度指挥。
2. 具备集成管理、信息管理、用户管理、设备管理、日志管理、预案管理、统计分析、人机交互、联网共享、系统运维等功能，实施动态巡防、日常勤务、警情研判、模拟演练、预案流转、警力布控、联动控制、快速处理、调度指挥等管控。
3. 与各类应急通信、移动通信等设施互联互通，支持智能语音交互、APP应用等功能，具备设备接入、触发报警、信息存储、图像显示、操作权限、系统时间、网络安全等管理措施。

7.7.8 智慧园区应提供以下通信服务，满足应急响应管理的需要。

1. 智慧园区应构建应急联勤通信录，可通过智慧指挥系统呼叫各级联勤、备勤人员，为疫情快速响应提供人员保障。
2. 智慧园区应具备多种通信机制，方便群众、员工及时报告园区风险，并组织调度工作人员，及时排险。
3. 智慧园区可提供OA、ERP、邮件、多媒体等业务，具备应急呼应、移动办公、IP云会议等应用功能。

7.8 智慧运营中心

7.8.1 智慧园区应集中调度、指挥、管理园区的各项活动，需要在运营中心配套以下设施：

1. 应部署大屏幕监控装置与操作台，满足统一调度、指挥的需要。
2. 应显示设施与设备位置、运行状态、报警信息，可模拟故障场景，满足应急演练的需要。
3. 应支持移动应用终端，提供微信公众号，邮件、短信，电话留言等多种方式，实现应急呼叫。
4. 配套装修、空调、照明、配电、中控、动环、布线、防雷、接地等机房工程。

7.8.2 智慧园区宜具备以下物业信息管理功能，满足物业办公与园区管理的需要：

1. 实现人口、访客、房屋、车辆、资产、交通、租赁、运维、仓储、档案等管理数字化。
2. 具备合同管理、财务管理、资产管理、收费管理、人事管理、行政管理、后勤管理、协同办公、公文流转、电子桌面、即时通讯等信息化功能。
3. 具备工单任务、告警类、流程提醒、到期/超期提醒等多种类别消息推送，可量化考核员工绩效。

7.8.3 围绕园区经济活动，存在新建、改建、扩建、装饰等基本工程建设需要。为了确保园区建设与运转互不干扰，智慧园区宜能够全过程监管基本工程建设。

7.8.4 智慧园区以经济活动为核心，园区经济活动又依赖于行为人的诚信。智慧园区宜与社会征信机构合作，建立企业与个人的诚信档案，满足园区经济活动的需要。

7.8.5智慧园区为配合智慧城市的建设，宜构建居民健康档案，打通园区与医院、营养膳食、文体机构的信息通道，为居民的健康生活提供便利。

7.8.6 智慧园区应建立园区与居民的信息联系通道，及时响应与处理了解居民的需求，具备完善智慧园区的应用场景能力。

**8 安全体系**

8.2 设备及感知层安全

8.2.1 感知层设备传输安全宜具备如下要求：

1. 具备数据安全的传输能力，保证数据传输过程中的机密性、完整性；
2. 具备安全接入能力，防止终端被仿冒接入通信网络。如：TCP/IP协议的智能终端或设备可采用ITU X.509证书、IEEE 802.1x技术实现安全入网；
3. 具备网络侦测与网络重建能力。

8.2.2 感知层设备主机与应用安全宜具备如下要求：

1. 具备系统可信启动、安全升级能力；
2. 具备重要信息的安全保存能力；
3. 具备对本地调试或远程访问权限控制能力；
4. 具备对系统入侵、设备损毁检测检测与防护能力；
5. 系统授权认证和数字留痕功能；
6. 感知数据的自动校对和地址绑定功能；
7. 数据加密解密和自我修复功能。

8.3 通信网络安全

8.3.2 网络架构安全，应考虑如下设计要求：

1. 关键节点的硬件冗余建设要求，包括通信线路（包括业务数据链路和带外管理链路）、网络设备、安全设备、计算设备，并部署链路负载均衡设备。
2. 网络负载可靠性要求，平均值带宽建议40%利用率，峰值带宽不高于70%，以保障通信网自身的健壮性稳定性。
3. 应分区分域合理规划路由，业务终端与业务服务器之间建立安全路径。根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的网段或VLAN。保存有重要业务系统及数据的重要网段不能直接与外部系统连接，需要和其他网段隔离，单独划分区域。
4. 智慧园区网络一般分为：内网办公区、外网办公区、物联接入区、互联网区、数据中心区、管理运维区、互联网区等。各区域之间按业务需求部署网闸或者防火墙等隔离设备，关键节点的硬件冗余设计，并启用ACL进行访问控制。

8.3.3通信完整性和保密性应满足如下功能要求：

1. 对于信息传输的完整性校验应由传输加密系统完成，通过识别传输协议类型对网络数据进行隧道封装，为用户认证提供安全加密传输，并实现全业务数据在复杂网络环境下的传输。对于信息存储的完整性校验应由应用系统和数据库系统完成。宜部署SSL/IPSec安全接入网关或防火墙来实现。
2. 对于信息传输的通信保密性应由传输加密系统完成。宜部署SSL VPN系统或防火墙保证远程数据传输的数据保密性。

8.3.4 通信网络设备可信芯片要求：具有唯一芯片号、公私钥对，可参与通信过程身份认证及加密。可信网络通信设备以密码芯片为可信根，通过散列算法实现完整性度量，通过非对称算法提供身份认证，通过对称算法提供数据加密，为密码算法、密钥、度量值、密码运算等提供更单纯、安全的安全芯片环境。

8.4 区域边界安全

8.4.2区域边界安全设备，应满足如下要求：

1. 边界安全防护设备应具备：网络准入控制、非授权用户外联行为监控、无线网络访问管理能力。宜部署网络准入控制系统，实现对内部网络中出现的内部用户未通过准许私自联到外部网络的行为进行检查，维护网络边界完整性。
2. 边界访问控制应具备：强化网络安全策略、对网络存取和访问进行监控审计、防止内部信息的外泄、精确流量管理、基于WEB应用的协议及内容控制等能力。宜部署边界防火墙及WEB应用防火墙设备实现相关功能。
3. 边界入侵防范应具备：入侵防护系统IPS、防DDoS泛洪攻击、防未知高级威胁（APT）、主动防御（诱捕）等能力。宜部署部署诱捕系统提升内网安全。
4. 边界恶意代码和垃圾邮件防范，应在办公外网边界部署防病毒网关或防火墙（开启防病毒功能、防垃圾邮件功能），并保证病毒库和垃圾邮件规则库需及时升级至最新版本。
5. 安全审计应具备：全网日志管理、精准到用户级行为分析、安全事件分析等功能。在各主要边界（重要服务器区域、外部连接边界）需要设置必要的审计机制，进行数据监视并记录各类操作，通过审计分析能够发现跨区域的安全威胁，实时地综合分析出网络中发生的安全事件。
6. 边界安全设备应具备可信验证能力。应基于可信根设计，提供如下能力，基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性收到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

8.5 计算安全

8.5.1 计算安全，宜根据园区安全需求，具备如下能力：

1. 根据等级保护规范要求，应包括如下安全能力；
2. 身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性和保密性、数据备份与恢复、剩余信息保护、个人信息保护等。
3. 宜在安全管理中心部署双因子认证系统、PKI-CA系统，实现身份鉴别（身份唯一性标识、登录保护、登录失效、多因子认证）、访问控制（用户账号与权限、访问控制策略及力度）功能。
4. 宜在管理中心部署IAM访问控制系统，提供集中统一访问管理功能，针对应用系统和用户进行统一访问方式、访问准入、访问控制等功能。

8.5.2平台应配备AntiDDoS、WAF、数据库防火墙、漏洞扫描工具、系统加固等措施，加强系统安全性：

1. 应提升主机安全能力，提供系统漏洞扫描、入侵检测等功能，降低主机安全风险；应能够扫描容器镜像中的漏洞，以及提供容器安全策略设置和防逃逸功能。
2. 应支持主机、数据库、WEB漏洞扫描等能力，支持恶意请求和未知威胁的智能识别和防御。
3. 应支持主机、数据库定期更新安全补丁，修补系统安全漏洞，从而提升系统抵御外部非法入侵的能力。
4. 应支持对主机、数据库、WEB容器、WEB应用等进行安全加固，裁剪不安全的组件、封闭不必要的端口、增加安全配置，屏蔽和消除缺陷和漏洞，使系统保持在一个相对更安全的状态。

8.5.3数据安全涉及应用、数据库、主机、网络、存储、管理等多方面的安全防护，应包括：

1. 数据采集应遵循最小化和必要性原则，对隐私数据的采集必须获得数据主体的许可；在数据主体未授权的情况下，将不采集、不保存、不处理数据主体的数据。
2. 对敏感数据和隐私数据的存储应进行加密存储，对于涉及的密钥通常也需要进行加密保存，以确保密钥的安全性。
3. 敏感数据的传输，应加密传输或采用加密通道进行传输，如HTTPS、SFTP等，尤其对于口令、银行帐号等信息，支持加密并且利用加密通道传输，确保数据在传输过程安全。
4. 敏感数据的展示，应采用匿名化的方式处理，在WEB界面、日志文件、配置文件中都不明文显示。在WEB界面或输入框宜用星号屏蔽，在日志文件或配置文件中，显示为加密后的密文。
5. 敏感数据的生命周期结束时，应删除或销毁数据以保护数据安全。对于数据，应设定一定的保存期限，到期进行删除或销毁；对于隐私数据，在数据主体要求的情况下，如与法律法规不冲突，也应进行删除和销毁。
6. 数据应定期进行备份，可采用本地备份、容灾备份等多种备份方式，避免意外情况下的数据丢失；在备份数据进行恢复时，应采取措施保证数据安全恢复，对于恢复的数据应采取与生产数据同样的防护措施。

8.4.4智慧园区系统应提供完善的权限与用户管理，可采用基于角色的授权模型，并按照最小授权原则进行用户授权：

1. 操作员和互联系统应被认证才可以访问系统。
2. 操作员应采用基于密码或手机验证码的认证策略，密码策略宜使用强密码策略。
3. 应用系统对文件和数据包括客户资料应实行访问控制，对敏感数据采用二次密码等措施进行控制。
4. 应通过输入检查、输出编码、上传下载控制、异常处理等手段，防范了WEB应用攻击。
5. 宜结合日志审计、应用数据稽核，发现业务活动异常，包括非法篡改等操作。

8.6 网络安全管理中心

8.6.1 网络安全管理中心宜部署以下系统，实现统一安全管理：

1. 部署统一网络管理系统，实现对通信网络设备的系统的资源和运行进行配置、控制和管理
2. 部署日志审计系统，实现安全审计：网络设备、安全设备、主机、终端、服务器日志审计，以及入侵防范：威胁溯源、网络溯源等功能。
3. 部署安全管理平台系统，实现对安全设备进行统一管理、状态监控、策略下发、集中审计。
4. 部署网络安全态势感知系统，实现对整网安全态势做感知，分析，预警等。
5. 部署运维审计系统，实现对网络系统、应用服务器、业务系统、数据库进行状态监测和监控，实时发现故障并报警，快速定位故障点，为恢复环境提供依据。

8.6.2智慧园区管理单位宜建立安全管理团队，并发布相关的安全维护管理流程，并授予安全管理团队相应的权限对系统进行监管：

1. 安全管理团队应包括能够维护系统并处理紧急问题的重要人员，建议设立安全管理员、系统管理员、系统操作员、报表操作员等角色，操作员和管理员应具备必要的安全知识或者接受必要的安全培训。
2. 安全部门应建立日志检查、日志备份、日志审计等制度，以便及时发现可能存在的操作异常。
3. 安全部门应建立数据定期备份机制，备份的间隔周期应参考恢复的时间指标，在生产环境数据损坏乃至物理损坏等场景下，应保证系统和数据恢复时间满足客户的预期。
4. 安全管理员应定期检查系统是否已被攻击或存在明显的安全隐患，能对巡检问题及时修复和解决，减少安全问题的进一步扩大和规避潜在损失。