

ICS 35.03
CCS A91

T/FJAF

团体标准

T/FJAF 005—2025

博物馆和文物保护单位
综合电子防范技术规范

Technical Specifications for Integrated Electronic Security in Museums
and Cultural Heritage Protection Sites

(征求意见稿)

202X-XX-XX 发

202X-XX-XX 实施

福建省公共安全防范行业协会 发布

目 次

前言..... II

引言..... III

1 范围..... 1

2 规范性引用文件..... 1

3 术语和定义..... 2

4 缩略语..... 3

5 总体要求..... 4

6 系统构成..... 4

7 技术要求..... 5

8 重要部位防护要求..... 14

9 系统建设要求..... 19

参考文献..... 22

前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由福建省公共安全防范行业协会提出并归口。

本文件起草单位：

本文件主要起草人：

引 言

目前，大数据在安防领域的应用已从辅助工具升级为核心驱动力，从风险预警、安防管理到运营维护，形成了全域化、智能化的保护网络。大数据技术正在深刻重塑博物馆和文物保护单位的综合防护体系，它通过全方位的数据采集、深度分析和智能应用，推动安防从“事后追溯”转向“事前预警+事中干预”，全面提升博物馆和文物保护单位对各类风险的感知、预警、防范和处置能力，为守护人类宝贵的文化遗产提供了强大的技术支撑。将来，随着物联网、多模态人工智能、云计算等技术的进一步发展，大数据在文博防护领域的应用将更加深入和成熟。

本文件根据现阶段安全防范技术、产品和管理方式的发展状况，在GB/T 16571-2012《博物馆和文物保护单位安全防范系统要求》技术防范措施的基础上，针对供电、防火等薄弱环节，进一步强化风险预警、管控等应对措施。同时，将大数据技术融入博物馆和文物保护单位的综合防范体系，借助人工智能、物联网、云计算、无人机应用、预防性保护和数字化保护等技术手段，通过数据挖掘与跨领域协作，提升文物保护能力和安全管理效率，为文化遗产的可持续传承提供多样化的技术保障。

本文件可作为GB/T 16571-2012《博物馆和文物保护单位安全防范系统要求》等标准技术防范措施的补充内容。博物馆和文物保护单位的人力防范和实体防范应按现行相关标准执行。

博物馆和文物保护单位综合电子防范技术规范

1 范围

本文件规定了博物馆和文物保护单位综合电子防范系统（以下简称“系统”）的总体要求、系统构成、技术要求、重要部位防范要求和系统建设要求，是博物馆和文物保护单位系统设计、施工、监理、检验、验收的依据。

本文件适用于新建、扩建和改建的博物馆和古文化遗址、古墓葬、古建筑、石窟寺、古石刻、古壁画、近代现代重要史迹和代表性建筑等文物保护单位。纪念馆、考古研究所、考古发掘工地、文物商店和其他收藏、临时展出文物场所可参照执行。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

- GB 12663—2019 入侵和紧急报警系统 控制指示设备
- GB/T 15408—2011 安全防范系统供电技术要求
- GB/T 16571—2012 博物馆和文物保护单位安全防范系统要求
- GB 1679—62022 安全防范报警设备 安全要求和试验方法
- GB/T 20270 信息安全技术 网络基础安全技术要求
- GB/T 21431—2015 建筑物防雷装置检测技术规范
- GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
- GB/T 23863—2024 博物馆照明设计规范
- GB/T 28181 公共安全视频监控联网系统信息传输、交换、控制技术要求
- GB/T 28448—2019 信息安全技术 网络安全等级保护测评要求
- GB/T 28827.1 信息技术服务 运行维护 第1部分：通用要求
- GB/T 28827.3 信息技术服务 运行维护 第3部分：应急响应规范
- GB/T 30147—2013 安防监控视频实时智能分析设备技术要求
- GB/T 30235—2013 古代壁画保护修复档案规范
- GB/T 31132—2014 入侵报警系统 无线（射频）设备互联要求
- GB/T 32581—2016 入侵和报警系统技术要求
- GB 35114—2017 公共安全视频监控联网信息安全技术要求
- GB/T 37078—2018 出入口控制系统技术要求
- GB/T 37732—2019 信息技术 云计算 云储存系统服务接口功能
- GB 40050—2021 网络关键设备安全通用要求

GB 42590—2023 民用无人驾驶航空器系统安全要求
GB 50343—2012 建筑物电子信息系统防雷技术规范
GB 50348—2018 安全防范工程技术标准
GB 55029—2022 安全防范工程通用规范
GA/T 644 电子巡查系统技术要求
GA/T 670 安全防范系统雷电浪涌防护技术要求
GA/T 678 联网型可视对讲系统技术要求
GA/T 751—2024 公安视频图像屏幕显示信息叠加规范
GA/T 761—2024 停车库（场）安全管理系统技术要求
GA/T 833 机动车号牌自动识别技术规范
GA/T 1081—2020 安全防范系统维护保养规范
GA/T 1185 安全防范工程技术文件编制深度要求
GA/T 1708—2020 安全防范视频监控红外热成像设备
QX 189—2013 文物建筑防雷技术规范
WW/T 0082—2017 古建筑壁画数字化测绘技术规程
WW/T 0116—2023 石窟寺二维数字化采集与加工
WW/T 0117—2023 石窟寺三维数字化采集与加工

3 术语和定义

GB/T 16571、GB/T 32581—2016、GB/T 37078—2018、GB 50343—2012、GB 50348—2018界定的以及下列术语和定义适用于本文件。

3.1 藏品库房 Storage for Collections

博物馆等建筑中专门用于存放、保护和管理文物、标本及其他藏品的区域，具备防火、防盗、防潮、防虫、防尘、防光（紫外线）、防震、防空气污染等功能（或其中某些功能）。

3.2 综合电子防范系统 Integrated Electronic Security System

运用电子、计算机、物联网等技术、产品和其他相关产品构成的入侵和紧急报警、视频监控、出入口控制、防爆安全检查、停车库（场）管理、声音复核、专用通讯、应急广播、可视对讲、防火预警、智慧供电、雷电防范、无人机应用、大数据人工智能应用、预防性保护和数字化保护等系统，以及由这些系统组合或集成的电子系统或网络。

3.3 数字化保护 Digital conservation

通过采用三维激光扫描、近景摄影测量、倾斜摄影、遥感测绘、数据复原等先进技术手段，对文物进行全息记录，建立高精度的数字档案，实现文物信息的永久保存与活化利用。

3.4 预防性保护 Preventive Preservation/Protection

通过系统性和科学性的手段，在文物尚未发生显著损坏或劣化之前，采取主动干预措施，消除或降低人为因素、气象因素、环境因素等对文物构成的安全威胁，延缓或阻止文物的物理和化学性质劣化的措施。

3.5 边缘服务器 Edge Server

部署在物联网边缘侧，具有数据处理、网络通信、数据存储能力的设备，是文物数字化保护和云端协同的关键技术节点和核心基础设施。

[来源：GB/T 41780.1—2022, 3.2, 有修改]

3.6 大数据采集装置 Big Data Collection Device

基于物联网和云计算等技术的传感、识别和追踪装置，包括但不限于温度、湿度、压力、流量、光强、气体、速度、光学、红外、NFC、RFID、GPS、Mac 地址等信息采集装置。

3.7 应急广播 Emergency Broadcasting

利用公共广播、专用通讯、网络视听等信息传输方式，向公众或特定区域、特定人群发布应急信息的系统。

3.8 系统管理平台 system management platform

对综合电子防范系统的各子系统及相关信息系统进行集成，实现实体防范、电子防范和人力防范资源的有机联动、信息的集中处理与共享应用、风险事件的综合研判、事件处置的指挥调度、系统和设备的统一管理与运维等功能的硬件和软件组合。

[来源：GB 50348—2018, 2.0.16, 有修改]

3.9 设备间 Equipment Room

博物馆和文物保护单位集中放置电子防范设备、网络设备、供电设备和其他电子、电气设备的物理区域。

[来源：GA 38—2021, 3.20, 有修改]

4 缩略语

下列缩略语适用于本文件：

BDS：北斗卫星导航系统 (BeiDou Navigation Satellite System)

CDMA：码分多址 (Code division multiplexing access)

LoRa：一种低功耗广域网无线标准 (Long Range Radio)

LPZ：雷电防护区 (lightning electromagnetic impulse)

OCR：光学字符识别 (Optical Character Recognition)

SPD：浪涌保护器 (surge protective device)

VR/AR：虚拟现实和增强现实 (Virtual Reality/Augmented Reality)

5 总体要求

- 5.1 系统的建设，应按照相关管理要求，严格安全准入机制，选用符合要求的专业设计、施工和服务队伍，建立完善的保密制度。
- 5.2 应预先进行风险防范规划，通过风险评估明确需要防范的风险，统筹考虑实体防护状况和人力防护的能力，合理运用适宜的技术手段，构建安全可控的综合电子防范体系。
- 5.3 根据防护对象的分布情况和环境条件，合理划分周界、监视区、防护区、禁区，实现纵深防护的均衡性；不具备建立整体纵深防护体系的，应建立局部纵深防护体系。
- 5.4 系统应以规范化、结构化、模块化、集成化的方式实现，适应系统运维和技术发展的需要，采用成熟而先进的技术和可靠而适用的设备。
- 5.5 涉及网络信息安全的核心设备应选用符合 GB 35114—2017 和国密相关标准的国产化产品，实现信息传输、转发、存储、下载等阶段端到端全程保密。
- 5.6 文物保护单位的系统建设应坚持对文物本体最小干预和与环境相协调的原则，充分考虑保护对象的特殊性，科学规划、合理设计、规范施工、有效使用。
- 5.7 系统的运维应符合 GB 50348—2018 第 11 章和 GB/T 28827 及 GA/T 1081 等标准的规定。

6 系统构成

- 6.1 系统由入侵和紧急报警、视频监控、出入口控制、声音复核、电子巡查、防爆安全检查、停车库（场）管理、专用通讯、应急广播、可视对讲、火灾预警、智慧供电、雷电防范、大数据人工智能应用、无人机应用、预防性保护和数字化保护等子系统及系统管理平台组成。实际应用中，可根据安全防范需要，由上述某个子系统构成，也可由某些子系统的组合或集成。系统完整的技术架构如图 1 所示：

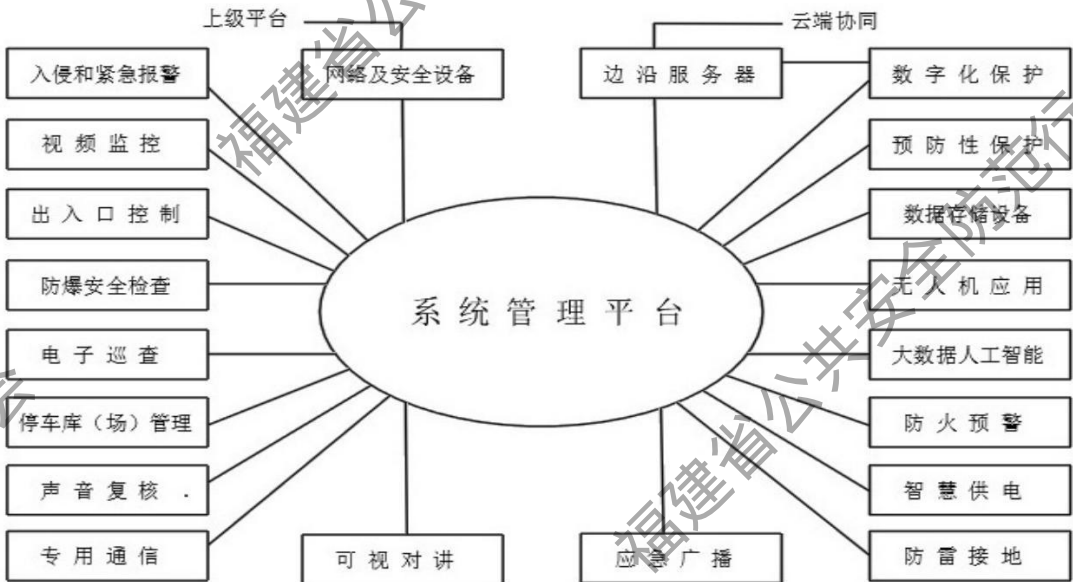


图 1 综合电子防范系统示意图

6.2 系统管理平台具备预案联动功能,可根据应用需求加载各类应急预案数据库,当接收到预警、报警、运维等信息时,可同步联动相应的处置预案投屏显示,必要时可分发至处置人员移动终端。

6.3 可通过部署运维服务平台或在系统管理平台设置运维模块,开展运维服务工作。

7 技术要求

7.1 入侵和紧急报警系统

7.1.1 应综合考虑防区分布、环境特点等因素,合理选择不同探测原理、不同技术性能的入侵探测装置,结合防护要求构成点、线、面、空间或其组合的综合防护体系。

7.1.2 应具备对隐蔽进入、强行闯入以及撬、挖、凿等入侵行为的探测与报警功能,单控制器系统报警响应时间不应超过 2s。

7.1.3 探测传感器和控制传输设备应具备防拆、防破坏和故障检测报警等功能;传输管线应落实刚性防护措施;紧急报警装置应有防误触发措施,触发后应自锁。

7.1.4 室外设备(包括但不限于探测器、控制器、设备箱)的防护等级应不低于 IP55。

7.1.5 报警控制防区的规划应满足以下要求:

——不同技术原理的入侵探测器不应接入同一防区;不同功能物理区域的入侵探测器不应接入同一防区;

——紧急报警防区应设置不少于 2 路的独立防区,且 24h 不可撤防,每路防区安装的紧急报警装置不应多于 4 个;

——周界入侵探测防区划分应有利于报警时的准确定位,单个防区不宜大于 100m,不应有盲区。

7.1.6 系统应有两种及以上联网报警传输方式,联网报警的主传输通道应优先使用有线网络,主通道故障时应能自动切换到备用报警通道。

7.1.7 系统的布防、撤防、预警等信息的存储时间应不小于 180d,重要预警和报警信息应长期保存。

7.1.8 系统应具备与视频监控、出入口控制、声音复核、辅助照明等设备联动的功能,支持大数据信息采集。

7.1.9 其他要求应符合 GB/T 32581-2016 的规定。

7.2 视频监控系统

7.2.1 应能对监控区域和目标进行实时视频采集、监视、记录与回放,对视频采集设备及其信息进行控制;应保持图像和声音记录信息的原始完整性,并具备防篡改、防销毁、防窃取以及视频信号丢失、画面遮挡等报警等功能。

7.2.2 视频图像的分辨率应不小于 1920×1080(1080P),帧率不小于 25fps,要害部位和重要保护目标的视频图像应支持 4K 录像和回放;视频图像的文字标注应符合 GA/T 751 的规定。视频图像记录信息保存时间应不小于 30d,要害部位、重要保护目标及防范恐怖袭击重点目标的视频图像信息保存期限应不小于 90d。

7.2.3 出入口设置的视频监控装置,应能清楚地显示出入人员面部特征、机动车号牌等信息;宜具备 AI 识别和大数据应用等功能。

7.2.4 视频监控区域设有声音复核装置的，应对相应的音频信号进行同步记录和同步回放。

7.2.5 具有智能视频识别分析功能的视频监控装置，应符合 GB/T 30147—2013 的规定，能根据使用和管理需要设置视频警戒区域和报警触发条件，并具备智能化和大数据应用功能。

7.2.6 前端视频采集设备所处的环境照度不能满足视频监控需要时，应配置辅助照明装置，辅助照明光源不得对防护对象造成损伤（使用 LED 冷光源、限制光照强度不大于 50 lux 等）；辅助照明装置宜采用监控中心集中供电，采用现场供电时，应配置备用电源装置。

7.2.7 视频/音频采集、传输、切换、远程控制、视频显示和声音展示、存储/回放/检索、视频/音频分析、多摄像机协同、系统管理、独立运行、集成与联网等，应符合 GB 50348—2018 中 6.4.5 的规定。

7.2.8 其他要求应符合 GB 50348—2018、GB 55029—2022 及 GB/T 16571 的相关规定。

7.3 出入口控制系统

7.3.1 系统应能满足目标识别、出入管理的要求，具有防拆卸、防技术开启等防护能力。出现出入口非授权开启、胁迫开启、断电、控制主机被破坏等异常情况时，应能及时将异常信息报送联网监控中心。

7.3.2 出入口控制装置的设置应满足紧急情况下人员疏散的要求，通向疏散通道方向为防护面时，系统必须与火灾报警系统及其他紧急疏散系统联动，当发生火警或需紧急疏散时，人员不使用密钥应能迅速安全通过。

7.3.3 系统应符合 GB/T 37078—2018 中 3 级及以上安全等级的要求，具备复合识别、强防重入、胁迫报警、凭证防拷贝等功能。

7.3.4 当出入口控制系统与其他非安防业务系统共用凭证或凭证为“一卡通”应用模式时，出入口控制系统应独立管理。

7.3.5 采用非编码信号控制的驱动执行部分和控制设备，必须设置于该出入口的对应受控区、同级别受控区或高级别受控区内。执行部分的输入电缆在该出入口的对应受控区、同级别受控区或高级别受控区外的部分，应刚性封闭保护，其保护结构的抗拉伸、抗弯折强度应不低于壁厚 2.0mm 的镀锌钢管。

7.3.6 其他要求应符合 GB/T 37078—2018 的规定。

7.4 停车库（场）安全管理系统

7.4.1 应根据车辆进出停车库（场）的安全管理要求，选择适当类型的识读、控制与执行装置，具备进出车辆识别、信息提示、通行控制和数据记录等功能。

7.4.2 系统应符合 GA/T 761—2024 中 3 级及以上安全等级的要求。

7.4.3 防砸区的车辆检测宜首选雷达探测器或超声波探测器，具备完善的防误砸功能。

7.4.4 采用车牌识别识读方式时，应具有防车牌照片和车牌视频攻击的能力。

7.4.5 车辆号牌识别准确率应符合 GA/T 833 的要求。

7.4.6 应具备远程联网管理和支持黑名单布控及大数据应用功能；

7.4.7 其他要求应符合 GA/T 761—2024 的规定。

7.5 声音复核系统

7.5.1 应能清晰地探测现场内人员走动、语音和撬、挖、凿、锯、砸等动作发出的声音，声音探测的有效性应满足入侵报警和视频监控复核的要求。

7.5.2 系统采集的音频信息应与对应区域的视频图像同步记录，同步回放，时间偏差应不大于 1s。

7.5.3 音频信号谐波失真应不大于 5%，信噪比不小于 50dB，通频带不小于 100Hz~12kHz。

7.5.4 使用数字声音复核系统时，应保证声音信息的原始完整性和时效性。

7.5.5 系统应支持 AI 识别和大数据应用。

7.6 电子巡查系统

7.6.1 系统设备器材的选型和应用模式，应与博物馆和文物保护单位的具体需求相适应，可实现与上级文物保护管理平台联网管理。

7.6.2 应优先选用在线式电子巡查系统。可综合利用 RFID、NFC、GIS、BDS 等技术及出入口控制、视频监控及其他电子系统的前端设备构建巡查路线，实现实时可视化巡查。

7.6.3 应根据建筑物、环境、保护对象及安全管理要求，合理规划巡查路线和设置巡查点，确保安保人员巡查时不会误触发设防区域产生报警。

7.6.4 其他要求应符合 GA/T 644 的规定；宜支持大数据人工智能应用。

7.7 防爆安全检查系统

7.7.1 应根据博物馆和文物保护单位的特点和出入口管理要求，在适当区域部署防爆安全检查系统，设立身份验证区和安检通道，配置符合 GB 15208、GB 15210、GB 12899 标准、具备智能识别和联网报警功能的 X 射线违禁品安检设备、通过式金属探测门、手持式金属探测器和防爆毯及围栏等安检设备器材。

7.7.2 应能对易燃易爆、枪支弹药、管制器具、腐蚀有毒、放射性、毒品等禁带限带物品进行有效探测识别、显示记录和分析报警。

7.7.3 应与监控中心联网，安全检查设备应能向系统管理平台实时发送检测数据和设备状态等信息，并能与安检区的相关视频图像关联存储，支持大数据采集和应用。

7.8 专用通讯系统

7.8.1 可根据现场情况，选择有线传输与无线传输相结合的通讯方式，并综合考虑信号覆盖范围、可靠性、安全性及与其他系统的集成等因素，建立由专用传输线或公共电话网构成的有线传输系统，并配置无线对讲系统，确保通信手段的多样性。

7.8.2 支持多方实时通话，系统管理平台应能与各要害部位和重要保护目标实现双向实时对讲，确保紧急情况下的快速响应。

7.8.3 无线系统应支持分组独立呼叫和语音无缝切换，避免沟通延迟；信号应覆盖建筑内外所有区域，地下停车库、消防通道、电梯轿厢等弱信号区，可采用中继台、同轴电缆和玻璃钢天线等技术实现信号无盲区覆盖。

7.8.4 无线通信内容应采用数字加密技术，防止窃听；设置分级权限管理，区分安保、导览等不同部门的通信权限。

7.8.5 系统宜内置紧急报警、紧急广播等功能，并能与视频监控、消防报警等系统联动或统一管理，遇紧急情况时可自动触发对讲系统通知相关人员。

7.9 可视对讲系统

7.9.1 系统可独立运行，并具备与入侵和紧急报警、视频监控，出入口控制等系统集成管理、组合管理或联动管理等功能。

7.9.2 主机（管理机）与分机（门口机及室内机）可实现双向通话，支持免提操作。

7.9.3 支持 IC 卡、密码、生物特征识别及远程开锁等功能。

7.9.4 分机最低照度不大于 0.1Lux（彩色），分辨率不小于 420TVL，支持红外补光以适应低照度环境。

7.9.5 宜支持 AI 识别和大数据应用。

7.9.6 其他要求应符合 GA/T 678 的规定。

7.10 信号传输系统

7.10.1 应根据安全管理要求和 GA/T669 的相关规定，对系统的网络结构、组网模式等进行统筹规划。

7.10.2 网络关键设备应符合 GB 40050-2021 的要求，视频流的联网传输、交换、控制的接口应符合 GB/T 28181 的规定。

7.10.3 信号传输与管线敷设除应符合 GB 50348-2018 中 6.13 的规定外，还应满足下列要求：

——本地传输网络宜采用以监控中心为汇接点的星形/树形传输网络拓扑结构，传输通信链路应满足系统的信息传输、交换和共享应用的需要。当有线传输不具备条件时，可采用具有安全措施的无线传输方式，并保证传输信息的有效性和抗干扰性能；

——远程联网传输系统，可采用专线方式或公共传输网络基础上的 VPN 方式，通过多级管理平台的互联，实现大范围、跨区域的系统级联。同时，可实现与其他业务系统的联网集成和综合应用。

7.10.4 IP 传输网络应符合以下要求：

——网络传输时延应不大于 300 ms，传输时延抖动应不大于 50 ms，传输丢包率应不大于 1×10^{-3} ；

——单路图像采集设备接入监控中心的网络传输带宽不小于 4 Mbps；

——图像采集设备端到端的信息延迟时间应 $\leq 2s$ ；图像采集设备与用户终端设备端到端的信息延迟时间应 $\leq 4s$ 。

7.10.5 云端协同传输应符合以下要求：

——视频传输：4K 直播不小于 15Mbps/路，VR/AR 不小于 200Mbps，抖动不大于 5ms；时延不大于 20ms；

——双向时延不大于 20ms，帧同步抖动不大于 2ms。

7.10.6 物联网（IoT）传输应符合以下要求：

——窄带传输：不大于 100Kbps/设备，时延容忍不大于 5s；

——协议效率：CoAP/UDP 头部压缩率不小于 50%。

7.11 数据存储系统

7.11.1 宜采用前端存储和监控中心存储相结合的分布式存储策略，重要数据应进行后端集中备份，备份链路应具备断点续传功能。

7.11.2 视频监控图像信息宜采用 NVR、NAS 等网络存储设备进行存储与管理，存储设备的资源配置应符合 GA/T 1211 的规定。

7.11.3 可利用边缘服务器辅助存储大数据应用信息和云端协同数据信息。边缘计算节点与云端协同的接口协议应符合 GB/T 37732-2019 的要求。

7.11.4 必须对存储数据库的完整性进行定期检测，建立数据防丢失、防篡改、溯源和保密的安全机制：

- 数据库备份机制：应能实现数据的主从备份和实时备份，发生故障时自动切换；
- 数据保障和数据库恢复机制：应具备应急恢复、版本恢复、前滚恢复等数据恢复手段；
- 数据库监控管理机制：应具备面向安全性的用户管理、权限管理和密码管理等功能。

7.11.5 视频监控图像信息的保存时间应符合 7.2.2 的规定，其他数据的保存时间应符合相关规定和满足应用需求，重要预警和报警信息应做到永久性保存，有标记的数据应实施保护。

7.11.6 应通过自动或手动方式定期（不大于 180d）对存储信息进行整理，清除过期和失效的信息。

7.12 系统管理平台

7.12.1 系统管理平台的功能、性能及应用模式，必须和系统的规模及保护对象的安全管理要求相适应。

7.12.2 可对各子系统进行集成管理，实现子系统间的高效协同工作；具备完善的系统管理（用户管理、权限管理、设备管理、安全认证等）、数据库服务（储存、分发）、多层电子地图联动等功能。

7.12.3 支持 LAN、LoRa、ZigBee（基于 IEEE 802.15.4 标准的低功耗、近距离无线通信技术）等全域协议接入和统一管理，管理范围应覆盖本地电子防范设备、移动终端、物联网传感和大数据应用及其他异构设备。

7.12.4 可通过物联传感器实现文物信息、人员行为、环境监测、社交媒体等数据的实时采集和应用；支持多源数据整合、数据清洗、敏感数据加密和海量数据存储。

7.12.5 支持数据融合与跨网协同，可对设备端或边缘节点进行初步数据分析，生成结构化数据；可将物联数据转化为信息网可理解的语义数据。

7.12.6 支持“边缘节点-边缘域-云中心”架构；可利用大数据技术和部署边缘服务器与其他信息平台（如国家文物局数据中心等）对接，实现云端协同。

7.12.7 可实时检测各子系统和物联传感器的工作状态（包括但不限于供电、防拆、干扰、自然环境等），并对异常情况进行预警和自动启动运维程序。

7.12.8 可针对不同的事件编制、执行不同的应急处置预案，并对事件的处置过程进行记录。

7.12.9 可为经授权的远程用户登录系统、访问数据信息和控制前端设备等操作提供 C/S、B/S 等方式的服务。

7.12.10 支持 BDS、CDMA、B 码等时间源，内嵌网络时间协议，可对系统中所接入的设备进行网络授时。系统内的时间误差应不大于 10s，授时设备的主时钟与北京时间偏差不大于 1s。

7.13 网络安全系统

7.13.1 系统的网络安全设计应符合 GB/T 20270 的规定，安全等级保护应不低于 GB/T 22239-2019 中“二级安全保护能力”的要求，核心数据交换区域（藏品库房、监控中心等），宜提升至三级安全保护能力。

7.13.2 需要与不同安全保护等级的网络环境进行信息交换的，应落实适宜的安全隔离措施（如：部署网闸、防火墙、UTM、VPN 等）。

7.13.3 系统中的 IP 摄像机、客户端、移动终端及各种信息采集传感设备应进行 IP/MAC 绑定，核心设

备（服务器、数据库、边缘节点等）应启用多因素认证，密码策略更换周期不大于 90d。

7.13.4 边缘服务器、应用服务器和数据库服务器宜采用双机热备份或集群部署设计。

7.13.5 系统联网视频信息和控制指令信息应采用 GB 35114 规定的国密认证协议，禁止使用未加密的 RTSP、HTTP 等协议传输视频数据。

7.14 防火预警系统

7.14.1 系统可通过部署温度传感器、多模态融合算法热成像摄像机、光纤测温等技术装置，实现火灾的早期探测、预警及报警；支持预警温度和报警温度设定。

7.14.2 热成像摄像机应支持烟火识别、区域入侵侦测等 AI 算法。热成像分辨率不小于 384×288 像素，可见光分辨率不小于 1920×1080 像素，支持双光路融合显示（热成像叠加可见光画面）。

7.14.3 测温范围不小于 -20°C — 550°C ，测温精度 $\pm 1^{\circ}\text{C}$ 或 $\pm 1\%$ 。支持定温预警和温升速率预警，预警响应不大于 2s；支持动态灵敏度调整，过滤蒸汽、高温设备等干扰源。

7.14.4 光纤测温系统激光安全等级应满足文物保护要求，测温范围应不小于 -40°C — 150°C ，测温精度不低于 $\pm 0.5^{\circ}\text{C}$ ，空间分辨率不低于 0.5m，响应时间不大于 2s，测温距离不小于 2km。

7.14.5 支持多系统协同和电子地图可视化，可与 GIS 系统结合实现热源定位；支持预警信息自动推送至本地和远程管理平台，支持干节点报警输出，可联动消防水炮、排烟机和其他消防设备。

7.14.6 支持火情蔓延模拟及数字孪生应用；支持温度变化曲线分析和后期复盘等功能。

7.14.7 热成像设备的其他要求应符合 GA/T 1780-2020 的规定。

7.15 智慧供电系统

7.15.1 系统的构建应以高可靠性、智能化管理和文物保护优先为核心，结合多电源冗余、负荷分级、节能环保为原则，通过部署电力监控模块和智慧配电箱等手段，实现用电环境状态和供电系统参数实时监测、故障诊断和预警等功能。

7.15.2 具备学习、分析、诊断和自适应能力，能够实时监测各供电回路电压、电流的变化，以及传输线、断路器、接线排、插座等节点和用电设备设施的温度参数，并自动与历史统计数据比对分析，对异常情况进行预警；遇电压、电流瞬间异常升高、漏电、过载、缺相等情况，立即执行保护动作并发出报警信息。

7.15.3 支持主备系统自动切换，当主系统发生故障时可自动/手动切换到备用系统，自动切换时间应不大于 30s，手动切换时间应不大于 1s。备用电源在市电中断后的持续工作时间应满足以下要求：

——支持视频监控系统正常工作时间不小于 2h；

——支持入侵和紧急报警系统正常工作时间不小于 8h；

——支持锁具采用断电开启方式的出入口控制系统正常工作时间不小于 48h（执行设备能正常开启 50 次以上），同时配置有机机械锁具，且无需执行远程授权控制的出入口控制系统，正常工作时间不小于 8h；

——支持信息传输链路相关设备（路由器、交换机、光端机和无线传输设备等）正常工作时间应不小于 48h。

7.15.4 具备规约扩展能力，能够兼容未来可能出现的新协议和标准，便于融入建筑管理系统或工业物联网平台，实现更高层次的智能化管理。

7.15.5 系统主要技术参数应满足以下要求：

- 稳态电压偏移不大于 $\pm 2\%$ ；
- 稳态频率偏移不大于 $\pm 0.2\text{Hz}$ ；
- 电压波形畸变率不大于 5% ；
- 允许断电持续时间 $0\sim 4\text{ms}$ ；

7.15.6 具备远程控制和运维功能，能够将故障信息和告警信息推送到管理端桌面和移动终端，并可实现AR远程协助功能，帮助运维人员快速定位和解决问题。

7.15.7 电子系统的前端设备和分布式中间设备应由监控中心集中供电。不具备市电供电条件的前端设备和文物保护单位，可采用风能、光伏以及发电机组等供电方式。

7.15.8 无人值守文物保护单位的电子系统，当市电断电后，应能向上级联网管理平台发送断电报警信息，备用电源应能自动切换，切换时不应改变系统核心设备工作状态。

7.15.9 其他要求应符合GB/T 15408-2011、GB/T 23863-2024和GB 50348—2018 6.12的规定。

7.16 防雷接地系统

7.16.1 系统必须落实等电位连接和保护接地措施，等电位连接网络宜选择GB 50343—2012中5.2的星形结构单点接地模式，并通过合理规划防雷接地路由和采取必要的隔离措施，防止地环流引入干扰。

7.16.2 接地装置应优先利用建筑物的自然接地体，当自然接地体的接地电阻值达不到要求时，应增加人工接地体，并将自然接地体、人工接地体和市电PE线的汇集点作为系统总接地端，尽可能避免多点接地，以减小雷电反击电压的影响。

7.16.3 供电回路各级SPD的配置，应符合GB 50343—2012中5.4的规定，必要时可预先进行模拟实验，确保防浪涌保护回路的有效保护水平与被保护设备的耐冲击性能相适应。

7.16.4 SPD的等电位连接应采用铜质线缆，截面积不小于 16mm^2 ；监控中心接地汇流环或汇流排采用裸铜线，截面积不小于 35mm^2 。

7.16.5 分布于室外的前端设备，应充分利用建筑物防雷功能，引入建筑物传输线路（跨越不同LPZ）的防雷接地措施应符合GB 50343—2012中5.5的要求。

7.16.6 防雷接地系统应依照GB 50343—2012中8.1和8.2的规定进行维护和管理。

7.16.7 文物建筑雷电防护应符合QX 189-2013的规定。其他要求应符合GB 50348-2018中6.11和GB 50343—2012及GA/T 670的相关规定。

7.17 大数据人工智能应用系统

7.17.1 应因地制宜，统筹规划，围绕风险防控需求，结合成本效益和实施可行性等因素，选择成熟和适用的大数据和人工智能技术和产品，搭建大数据人工智能应用平台或部署相应的管理模块。

7.17.2 应支持人流管控。可通过分布于公众服务区出入口的AI摄像机及各陈列展厅的NFC、RFID等物联传感装置采集人流信息；对于大型博物馆和文物保护单位，可结合无人机、机器人巡查追踪等手段，整合多源数据资源，预测各区域人流趋势和识别异常行为，实现实时人流信息发布和预设情景预警，以

便预先优化导览路线和限流策略。

7.17.3 支持环境监测预警。可通过物联网传感装置实时监测陈列展厅、藏品库房、修复室等文物保存环境和不可移动文物所处区域的温度、湿度、光照、污染物浓度等参数，结合历史数据建立预测模型，提前识别环境异常并自动预警。

7.17.4 支持文物高精度数字化存档。可通过三维激光扫描、无人机测绘、高清照相、多光谱成像等技术进行三维场景基础数据采集和建模，实现重要文物数字孪生和永久性数字化保存及云端数字化文物的虚拟展示。

7.17.5 支持虚拟展厅演示。可通过边缘服务器的“本地计算+云端协同”模式，实现数字化文物的异地交互式展览展示，有效解决珍贵、脆弱文物在运输和展览过程中受损的风险。

7.17.6 支持VR/AR技术集成。可实现AR安防信息叠加、构建高精度VR数字孪生模型、沉浸式VR应急演练、AR辅助现场操作和辅助设备巡检及维修等应用。

7.18 无人机应用系统

7.18.1 地面控制单元可通过4G/5G/低轨道星链等通信手段对无人机实施超视距远程操控，并可通过BDS/GPS等系统实现厘米级定位，定位误差不大于2m。

7.18.2 无人机可搭载热成像摄像机、激光雷达、高分辨率相机、红外传感器、气象探测器等技术装备采集目标信息；具备高清视频与图像信息实时回传、实时AI分析、地形测绘、气象监测、跟踪巡查、火灾预警等功能。

7.18.3 视频采集单元所采集视频图像分辨率应不小于1920×1080，帧率应不小于25fps；实时数据传输速率不低于10Mbps。

7.18.4 支持多机自主集群协同、信息共享和AI辅助决策，具备一键返航、自动巡航、断点续航、定点悬停和链路中断/低电量/非致命故障自动返航等功能。返航的实际落点与预定返航点偏差半径应 $\leq 1\text{m}$ 。

7.18.5 支持自主决策、远程调度、环境感知和多样化任务设定，可规划航迹、航点、巡查和监测目标；可通过视觉识别、激光雷达、超声波等传感技术，实现自动避障和图像识别降落等功能，落点精度应不低于 $\pm 3\text{cm}$ 。

7.18.6 应具备飞行参数限制和保护能力，包括最大飞行高度、最大平均飞行速度和飞行区域限制等功能。

7.18.7 在环境风速 $\leq 3\text{m/s}$ ，无人机悬停期间应保持稳定的飞行状态，水平最大偏差应 $\leq 1.5\text{m}$ ，高度最大偏差应 $\leq 0.5\text{m}$ 。

7.18.8 其他要求应符合GB 42590-2023的相关规定。

7.19 预防性保护系统

7.19.1 针对文物保护单位建筑结构、附属设施及周边环境特点，利用物联网传感等技术手段，实现实时状态监测、数据采集与风险预警；通过与入侵报警、视频监控等系统联动，形成预防性防护体系。

7.19.2 设备选型应满足对文物最小干预的原则，优先选用低功耗、非接触式监测设备，安装方式不得对文物本体造成损伤，可采用表面贴装、非接触式传感等工艺。

7.19.3 支持建筑结构和构筑物安全监测（位移、沉降、倾斜、裂缝、振幅、加速度、频率、动态平衡、人体舒适度、温湿度、地震烈度等）、环境及效应监测（大气温湿度、风速、降雨量、光照度、紫外辐

射、二氧化硫、地下水位、振动干扰等)。

7.19.4 技术设备应满足以下要求：

——支持北斗 BDS 卫星定位，搜星数不小于 20 颗，定位精度不大于毫米级，支持 4G/5G 等通信方式，下行速率不小于 150Mbps，具备 OTA 远程升级与断点续传功能；

——支持三轴 (XYZ) 智能倾斜监测，测量范围不小于 $\pm 90^\circ$ ，精度不低于 $\pm 0.1^\circ$ ，振动阈值可根据实际需要配置，具备非接触式水浸检测与磁激活功能，支持 4G/5G、NB-IoT 等通信方式和 NFC 终端配置参数；

——支持北斗微基站全球导航，实时定位精度不低于厘米级，天文授时精度不低于 10 纳秒，接收灵敏度不低于 -142dBm (分贝毫瓦)，防护等级大于 IP68；

——温度传感器量程范围不小于 $-20^\circ\text{C} \sim 80^\circ\text{C}$ ，湿度传感器量程不小于 $0\% \sim 100\% \text{ RH}$ ，精度分别不低于 $\pm 0.2^\circ\text{C}$ 、 $\pm 1.8\% \text{ RH}$ ，有害气体传感器响应时间不大于 30s，检测精度不低于 ppm 级，具备自动校准功能。

——预防性保护装备应具备防电击、防机械危险和耐环境应力，对文物不会造成损害，并符合 WW/T 0100-2020 的规定。

7.19.5 数据处理与传输应满足以下要求：

——采用边缘服务器与云端协同存储策略，前端数据存储不小于 7d，核心数据 (如结构位移、沉降) 云端备份不小于 90d；

——支持时序数据库和海量时间序列数据处理，存储效率大于 10 万条/秒，支持数据加密与防篡改；

——本地传输应采用星形拓扑结构，有线网络带宽不小于 100Mbps，无线网络支持 4G/5G，传输时延不大于 300ms。

7.19.6 分级预警响应机制应满足以下要求：

——一级预警 (紧急)：结构位移超阈值 20%、沉降速率大于 1mm / 日、突发振动大 1G，触发声光报警并联动视频监控锁定区域，同步推送短信至应急团队；

——二级预警 (警告)：环境参数异常 (温度大于 35°C 或湿度大于 80% RH，持续 24 小时)、缓慢变形超阈值 10%，平台弹窗提醒并生成维护工单。

7.19.7 联动处置应满足以下要求：

——预警触发后，系统自动关联文物位置信息、历史监测数据及应急预案，联动出入口控制装置限制区域进入，启动辅助照明及平台端二次信息备份存储。

——应急响应时间：一级预警不大于 10min，二级预警不大于 2h，必须在 48h 内完成现场核查和处置工作。

7.19.8 其他要求应符合 WW/T 0117—2023、WW/T 0116—2023 和 WW/T 0082—2017 等标准的相关规定。

7.20 数字化保护系统

7.20.1 应预先对数字化保护措施和文物安全进行风险评估，优先采用本文件 7.17.4 等方式为重要文物建立数字化分身，确保数字化信息可逆、可溯、可再生。

7.20.2 数字化信息采集范围宜包括文物本体、保护范围及建设控制地带。

7.20.3 可通过数字孪生平台三维模型分析，结合物联网传感数据，识别建筑物、构筑物和其他不可移

动文物形变、位移、沉降、倾斜等病害，作为数字化保护的延伸，为预防性保护提供数据支撑。

7.20.4 数字化点云数据应满足以下要求：

- 点云规格和精度：ply、ptx、e57 等通用三维彩色点云格式，数据拼接精度误差不大于 8mm；
- 点云噪点和拼接指标：文物本体外无噪点，点云拼接无分层；
- 采集点云数据完整率大于 90%，高透光材质除外。

7.20.5 纹理采集设备应满足以下要求：

- 在保证文物安全的前提下选择标准光源进行图像数据、图像颜色和纹理的采集工作；
- 首选全画幅照相机，像素不小于 5000 万；纹理清晰度不低于 150dpi。

7.20.6 现场数据采集应使用非接触方式工具和工艺，不扰动文物本体，保证文物安全。

7.20.7 三维模型建模精度与点云误差不超过 2cm；贴图分辨率不小于 8192*8192 像素。

7.20.8 数据格式/存档数据的类别应满足以下要求：

- 原始数据：扫描仪采集的未经任何处理的原始格式；
- 复制级数据：经过简单点云优化、补洞处理的完整模型数据；
- 研究级数据（高模）：保持模型细节，并进行点云简化与贴图的完整模型数据；
- 浏览级数据（低模）：支持浏览器展示的完整模型数据。

7.20.9 成果格式应满足以下要求：

- 原始扫描点云数据，格式：扫描仪工程文件格式；
- 优化后点云数据（复制级数据），格式：ply、ptx、e57、obj；
- 模型提交格式：obj 或 ply；
- 纹理提交格式：TIFF、JPG、JPEG 等；
- 正射影像成果应保存为 TIFF、PSB、PSD 等通用存储格式。

7.20.10 成果提交要求

- 标准通用格式点云原始数据资料，包括标准通用格式未配准原始点云数据；
- 标准通用格式三维数据成果文件（含高清贴图纹理模型）；文件格式 obj、ply 等；
- 标准通用格式二维数据成果文件（不含贴图纹理模型）；文件格式 obj、stl 等；
- 标准通用格式多角度高清二维图片；文件格式 RAW，分辨率不低于 300dpi；
- 标准通用格式视频成果文件；文件格式 mp4、avi、mov 等；
- 原始数据和成果精度应能服务于文物保护和监测工作，支持文物数字化展示和数字化管理。

7.20.11 其他要求应符合 WW/T 0082—2017、WW/T 0116—2023 和 WW/T 0117—2023 等标准的相关规定。

8. 重要部位防范要求

8.1 博物馆

8.1.1 外周界的防护应满足下列要求：

- 外周界有物理隔离防护的，应设置防翻越的入侵探测、视频监控、声音复核等装置，可设置电子巡查装置和应急广播装置；
- 只划定区域无实体外周界的，应设置视频监控和电子巡查装置，可设置声音复核和应急广播等

装置；

——外周界出入口应设置视频监控、声音复核等装置，可设置出入口控制和大数据采集装置。

8.1.2 公众服务区（包括公共活动区、服务设施区域、教育用房、停车场所等）的防护应满足下列要求：

——应设置视频监控和声音复核装置，对人流、物流、车流进行有效的视频监控，可设置入侵和紧急报警、应急广播和大数据采集等装置；

——对外开放的入口应设置视频监控和声音复核装置；可设置防爆安全检查、应急广播和大数据采集装置；

——停车库（场）应设置视频监控、声音复核、紧急报警装置和停车库（场）安全管理系统，对进出车辆进行监控和管理；可设置应急广播、电子巡查和大数据采集装置；

——主要通道及其他重要部位应设置视频监控、声音复核、紧急报警、应急广播和电子巡查等装置。

8.1.3 陈列展览区（常设展厅、临时展厅及室外展区等）的防护应满足下列要求：

——应分配独立供电回路，部署智慧供电和防火预警装置，设置紧急报警、专用通信等装置。

——陈列展厅、藏品库房、修复室出入口和安检通道及其他重要区域应设置具有 AI 功能的视频监控装置和大数据采集装置；

——外周界或室内周界应设置入侵探测、视频监控、声音复核和电子巡查等装置；建筑物的门、窗、管道口、布展通道等应设置入侵探测装置；

——参观通道应设置视频监控装置，对人员的活动情况进行视频监控，视频图像应能辨识人员的体貌特征；出入口应设置出入口控制和大数据采集装置；内部区域应设置入侵探测、紧急报警、视频监控、应急广播和声音复核装置；

——珍贵文物展柜内应设置入侵探测和位移报警装置及大数据采集装置；展柜的布置区域应设置视频监控和声音复核装置；无展柜保护的重要展品，应设置位移探测、压力传感等传感装置，并具备现场声光警示功能；

——室外展区应设置入侵探测、紧急报警、视频监控和声音复核装置，宜具备现场声光警示功能；

——室外重要展品应设置入侵探测、位移探测、视频监控装置和声音复核装置。

8.1.4 文物卸运交接区的防护应满足下列要求：

——文物卸运交接区应设为禁区；可设置大数据采集装置；

——应设置出入口控制装置、周界入侵探测装置，以及紧急报警、可视对讲等装置；

——应设置视频监控和声音复核装置，视频图像应无死角清晰显示文物装卸、交接的全过程，并可辨识人员的体貌特征和车辆号牌；

——运输通道应设置视频监控和声音复核装置，对文物的运输过程进行全程跟踪监控；

8.1.5 文物保护技术区（包括文物整理、清洗、消毒、干燥、试验、修复、交接、摄影、鉴赏等区域和部位）的防护应满足下列要求：

——出入口应设置出入口控制、视频监控和声音复核装置；可设置大数据采集装置；

——门、窗和管道口应设置入侵探测装置；

——室内应设置入侵探测、紧急报警、视频监控、声音复核和专用通讯装置；

8.1.6 藏品库区和库房的防护应满足下列要求：

——藏品库区和库房均应设为禁区。应分配符合 GB/T15408 规定的独立供电回路，部署智慧供电和

防火预警装置；

——外周界、室内周界应设置入侵报警、紧急报警、视频监控和声音复核装置；门、窗和管道口应设置入侵探测装置；

——通道内应设置视频监控和声音复核装置，对文物的搬运过程进行全跟踪监控，视频图像应能辨识人员的脸部特征和车辆号牌；

——库房内应设置入侵报警、紧急报警、视频监控、声音复核、专用通讯和大数据应用装置，落实预防性保护措施；与外界（包括内部公共区域）相邻的墙体、天花板、地板等应设置入侵探测装置。

——出入口应设置出入口控制、视频监控、声音复核、可视对讲等装置；出入口控制系统宜具备防尾随、双向验证及关门提示等功能。

8.1.7 业务与科研区、行政管理区的防护应设置视频监控、声音复核、入侵报警、紧急报警和专用通讯装置；重要场所应设置出入口控制装置和可视对讲装置；可设置大数据采集装置；

8.1.8 监控中心、设备间应满足下列要求：

——监控中心和设备间均应设为禁区。应配备专用的有线和无线通讯设备，设置紧急报警装置和声光警报装置；

——应设置出入口控制装置和可视对讲装置，出入口控制系统宜具备防尾随、双向验证及关门提示等功能；

——监控中心和设备间室内、室外通道应设置视频监控装置和声音复核装置；

——无人值守的设备间应设置入侵探测装置和防火预警装置；

——应分配符合 GB/T15408 规定的独立供电回路，部署智慧供电和防火预警装置；防雷和接地装置应满足人身安全和电子信息系统正常运行的要求，并符合 GB 50343 和 GA/T 670 的规定。

8.2 古文化遗址和古墓葬

8.2.1 建设有封闭实体防护设施的外围周界应设置入侵报警、视频监控、电子巡查、应急广播等装置。

8.2.2 周界主要车辆出入口应设置具有车辆抓拍和车牌识别功能的视频监控装置，能够对车辆的进出情况进行实时监控和抓拍，视频图像和抓拍图片应能清晰显示车辆号牌、驾驶员脸部特征等信息；人员出入口应安装视频监控和声音复核装置，可设置防爆安全检查和大数据采集设备。

8.2.3 地面遗存文物建筑及建筑基址外围应设置视频监控和声音复核装置；文物建筑内设有文物展览的，应参照 8.1.3 的要求进行防护。

8.2.4 地面遗存的石雕、石刻等附属文物区域，应设置入侵报警、视频监控及声音复核装置，视频监控装置应具备 AI 功能；可落实预防性保护和数字化保护措施。

8.2.5 已探明地下遗存文物的区域，应设置入侵报警、视频监控和声音复核装置。入侵报警装置应对入侵、监控及各种破坏行为进行有效探测。

8.2.6 对外开放的公共活动区和主要通道应设置视频监控、声音复核和应急广播等装置，视频图像应能清晰显示人员活动情况和体貌特征。

8.2.7 藏品库房可参照 8.1.6 的相关要求进行防护；监控中心应符合 8.1.8 的规定。

8.2.8 不具备设置电子巡查条件的或安保人员巡查困难的区域和部位，可部署无人机或机器人巡视系统。

8.2.9 重要文物宜落实数字化保护和预防性保护措施。

8.3 古建筑

8.3.1 古建筑外周界防护应满足下列要求：

——应根据现场条件和安全管理要求设置入侵探测、视频监控、声音复核、电子巡查、紧急报警和应急广播等装置；

——出入口应设置视频监控、声音复核和专用通讯装置；可设置防爆安全检查和大数据采集装置；

8.3.2 古建筑本体防护应满足下列要求：

——应根据环境条件和建筑格局合理设置视频监控装置，对古建筑本体、防护范围和建设控制地带进行全方位监控；

——古建筑对外的门、窗、管道口应设置入侵探测装置，可设置视频监控和声音复核装置；

——可设置专用通讯、应急广播和大数据采集装置；

8.3.3 区域、部位的防护应满足下列要求：

——古建筑作为博物馆使用时，应符合本文件 8.1 的要求；

——有点灯、燃香等活动的区域，应设置视频监控、声音复核、防火预警和电子巡查等装置；可设置大数据采集装置；

——保存有壁画、塑像、碑刻及其他重要文物的区域，应设置入侵报警、紧急报警、视频监控和声音复核装置；宜设置大数据采集装置；

——古建筑作为配套服务用房使用时，应设置视频监控装置，对古建筑本体和人员活动情况进行有效监控；宜设置声音复核、紧急报警和专用通讯装置。

8.3.4 重要文物宜落实数字化保护和预防性保护措施。

8.3.5 监控中心应结合现场情况就近设立，并符合 8.1.8 的规定。通过远程控制中心进行管理时，应保证信号传输的有效性、安全性和抗干扰等性能符合相关要求。

8.4 石窟寺和古石刻

8.4.1 应根据环境条件合理规划防护区域。周界应设置入侵探测装置和视频监控装置，视频图像应能清晰显示周界区域人员行为特征和活动情况。

8.4.2 周界出入口应设置视频监控和声音复核装置，视频图像应能清晰显示进出人员的体貌特征和进出车辆的号牌；可设置防爆安全检查装置和大数据采集装置。

8.4.3 设有出入口安全检查区的，应设置视频监控、声音复核、紧急报警和专用通讯装置，视频图像应能清晰显示安全检查过程、携带物品和人员脸部特征。

8.4.4 设有值班室的，内部应设置紧急报警、专用通信、视频监控和声音复核装置，视频图像应能清晰显示室内人员活动情况。

8.4.5 石（洞）窟（龕）、摩崖石刻、摩崖造像、岩画等集中分布的崖面（壁）应设置视频监控装置，视频图像应能清晰显示崖面（壁）全貌和洞窟（龕）出入口状态，以及沿栈道上人员活动和进出洞窟（龕）情况，能辨识人员的体貌特征。

8.4.6 经幢、碑刻、石雕等石刻文物集中分布的区域，应根据道路和隔离情况设置视频监控装置，视频图像应能清晰显示人员体貌特征和活动情况。

8.4.7 公众集中活动区域、游客聚集区域、售票和检票区域应设置应急广播、视频监控和声音复核装置，

视频图像应能清晰显示人流、人群聚集及人员活动等情况，能辨别人员的行为特征。

8.4.8 售检票室、存包处、检票通道应设置视频监控、声音复核、紧急报警、专用通讯等装置，视频图像应能清晰显示区域内人员和体貌特征和活动情况。

8.4.9 保存有重要石刻、壁画、造像等文物的洞窟，以及摩崖石刻、摩崖造像的内侧通道，应设置入侵和紧急报警装置；对公众开放的，应设置视频监控和声音复核装置，视频图像应能清晰显示人员体貌特征和活动等情况。

8.4.10 散落分布的碑刻、雕刻、佛塔、经幢等石刻（群）、摩崖石刻、摩崖造像、岩画等文物，应设置视频监控装置、声音复核装置、应急广播等装置，视频图像应能清晰显示文物全貌，以及人员体貌特征和活动情况。

8.4.11 具备安保巡查条件的，应合理规划巡查路线，设置电子巡查装置；重要文物宜落实数字化保护和预防性保护措施。

8.4.12 不具备落实电子防范措施的，可使用无人机采集文物和周边现场图像，巡视间隔应不大于 8h。

8.4.13 监控中心的设置，应符合 8.3.5 的规定。

8.5 古壁画

8.5.1 应合理规划管控区域，设置周界入侵和紧急报警、视频监控、声音复核、应急广播装置，视频监控图像应能显示文物的全貌，能辨认管控区域人员的体貌特征和活动情况。

8.5.2 位于封闭式区域的古壁画，应在出入口设置视频监控装置，可设置出入口控制装置和安全检查装置，视频监控图像应能辨认人员的脸部特征和携带物品。

8.5.3 应采用物联网传感、人工智能等技术手段和产品，落实微环境监测和调控措施：

——温湿度控制：通过部署恒温恒湿设备（如空调系统、调湿机）维持稳定环境；

——有害气体过滤：安装空气净化装置，减少二氧化硫、氮氧化物等污染物侵蚀；

——光照管理：采用低紫外线照明（如 LED 冷光源），限制光照强度（通常不大于 50 lux）；

8.5.4 根据现场环境条件，采用符合 7.19.4 要求的技术设备，落实预防性保护措施；对于资产价值较高的古壁画，应落实数字化保护措施。

8.5.5 古壁画有缺损的，应及时保护和修复，并建立符合 GB/T 30235—2013 规定的修复档案。

8.5.6 监控中心的设置，应符合 8.3.5 的规定。

8.6 近代现代重要史迹和代表性建筑

8.6.1 应根据保护对象所处的环境条件、资产价值和日常人流、车流状况等具体情况，针对建筑结构、构件、历史风貌、人为破坏、盗窃、事故和自然灾害受损等风险因素，合理规划电子防范系统的架构、规模和应用模式及防护区域。

8.6.2 应根据保护对象周界、监视区、防护区和禁区等重点防护区域的特点，构建整体纵深防护和（或）局部纵深防护体系。

——外周界应设置视频监控、入侵和紧急报警、电子巡查、应急广播、声音复核、大数据采集和无人机应用等装置；视频监控图像回放应能辨别人员的行为特征和车辆的型号与颜色。

——监视区应设置视频监控、紧急报警、电子巡查、应急广播、声音复核、大数据采集等装置；视频监控图像回放应能辨别人员的体貌特征和车辆的号牌。可选择具有智能分析功能的设备，实现人流统

计、越界探测、动态预警、黑名单布控等防范效果。

——防护区应设置视频监控、入侵和紧急报警、电子巡查、专用通讯、应急广播、声音复核、大数据采集等装置；视频监控应无死角监视人员的活动情况，图像回放应能辨别人员的体貌特征。有博物馆功能的防护区和禁区（包括监控中心），应满足 8.1.3、8.1.4、8.1.5、8.1.6 和 8.1.8 的要求。

8.6.3 涉及消防安全的区域和建筑本体，宜落实防火预警和智慧供电等措施。

8.6.4 管控区出入口宜设置出入口控制、AI 视频监控、声音复核、专用通讯和大数据采集等装置，视频监控图像回放应能辨别出入人员的脸部特征。AI 摄像机应具备人流统计、黑名单布控等功能。

8.6.5 设有停车库（场）的单位，宜设置停车库（场）管理系统，可设置视频监控、紧急报警、电子巡查、应急广播、声音复核、防火预警和大数据采集等装置。

8.6.6 应根据重要史迹和代表性建筑的劣化和病害等情况，落实预防性保护措施；重要文物应落实数字化保护措施。

9 系统建设要求

9.1 系统的建设程序必须符合 GB 50348—2018 第 5 章的规定。

9.2 方案设计

9.2.1 设计单位在完成现场勘查和实施风险评估的基础上，应遵循 GB 50348—2018 第 6 章和 GB 55029—2022 第 3 章及其他相关标准的规定及《设计任务书》的要求进行技术方案设计。

9.2.2 应根据博物馆和文物保护单位的规模和环境条件及技术要求的不同，合理规划系统功能和性能指标及电子防范设备的组合方式，选择适宜的数据传输方式和路由。

9.2.3 系统管理平台应首选自主的信息技术应用创新产品，支持全域协议（包括 ZigBee、LoRa、LAN 等）接入；网络交换设备、服务器、存储设备、路由设备、安全隔离设备的资源配置应符合 GB 35114—2017（C 级）和国密相关标准；无线设备应支持 IEEE 802.11/a/b/g/n、4G/5G 和窄带物联网（NB-IoT）等无线通信网络协议。

9.2.4 应根据网络安全要求，规划系统管理平台的安全策略，选择适宜的接入设备、数据与网络传输安全措施及不同网络环境的安全隔离措施。

9.2.5 应依照 GB 50348—2018 中 6.6、6.7、6.8、6.10 的规定，对系统的安全性、电磁兼容性、可靠性、环境适应性进行整体设计。

9.2.6 设计文件应符合 GA/T 1185 和 GB/T 16571—2012 附录 A 及其他相关规定。

9.3 施工

9.3.1 应针对博物馆和文物保护单位的特点及文物保护要求，组建施工项目管理团队，编制施工组织方案，对保护性施工工艺进行整体规划，明确施工程序，特殊岗位的施工人员应具备相应的资质和能力。

9.3.2 施工过程应遵循 GB 50348—2018 第 7 章和 GB 55029—2022 第 4 章及其他相关标准的规定，落实安全施工、文明施工和环境保护等措施。

9.3.3 设备器材的安装和管线的敷设及其他施工措施，均必须严格依照保护性施工方案的工艺要求实施，不得对文物本体和其他保护对象造成损伤或破坏（包括化学影响）。

9.3.4 需要在文物本体上敷设管线和安装设备器材时，应征求文物专家的意见，选择低烟无卤阻燃型电缆穿金属管暗敷，尽可能减少对文物本体和环境的影响。

9.3.5 涉及珍贵文物本体的数据采集和各种数字化保护措施的施工，必须符合WW/T 0082—2017、WW/T 0116—2023、WW/T 0117—2023和其他相关标准的规定。

9.4 监理

9.4.1 建设单位可委托具有相应能力的监理单位对系统建设进行监督管理，并依照相关规定对监理单位及监理人进行保密审查和签订《保密协议》。

9.4.2 监理范围、程序和要求应符合 GB 50348—2018 第 8 章和 GB/T 50319 的规定。

9.4.3 陈列展厅、藏品库房、修复室、监控中心、设备间设备器材的安装调试、接地装置的施工、系统的功能调试、数字化保护施工等关键节点和工序，监理单位应安排监理工程师进行旁站。

9.4.5 数字化保护施工现场的监理工程师，必须熟悉文物的数字化信息采集流程和工艺要求，预先对现场设备实施的安全性进行监督管理。

9.4.6 监理单位应如实编制监理文件，并按约定的时间节点交付建设单位。

9.5 检验

9.5.1 系统竣工验收前，建设单位可委托具备安全防范工程检验资质且检验能力在资质能力授权范围内的机构进行检验，并提供检验报告；高风险系统交付使用后，可定期进行运行检验。

9.5.2 检验所使用的仪器仪表必须经有资质的机构鉴定或校准合格，满足检验项目的精度要求，且在有效期内。

9.5.3 系统应依照 GB 50348—2018 第 9 章的规定的的方法、程序、内容进行检验。

9.5.4 防雷接地系统可依照 GB 50343—2012 7.1 和 GB/T 21431—2015 的规定进行检测。

9.5.5 无人机系统可按 GB 42590—2023 第 5 章的要求进行实验。

9.5.6 网络安全可按 GB/T 28448—2019 的规定进行测评。

9.5.7 主要设备器材的检验应符合相关标准：

- 入侵和紧急报警系统可依照 GB 12663—2019 和 GB 16796—2022 的相关规定进行试验；
- 热成像摄像机可依照 GA/T 1708—2020 的规定进行检测；
- AI 设备可依照 GB/T 3014—2013 第 9 章的规定进行试验。

9.6 验收

9.6.1 系统软硬件安装调试结束，经初验、试运行和检验合格，并完成技术培训后，由文物主管部门会同相关单位依照 GB 50348—2018 第 10 章的规定组织竣工验收，并出具验收报告。

9.6.2 竣工验收文件可参照 GB 50348—2018 中 5.6 的要求进行收集与编制。

参 考 文 献

- [1] GB/T 21431—2015 建筑物防雷装置检测技术规范
 - [2] GB/T 25724 公共安全视频监控数字视音频编解码技术要求
 - [3] GB/T 31132—2014 入侵报警系统 无线（射频）设备互联要求
 - [4] GB 37300—2018 公共安全重点区域视频图像信息采集规范
 - [5] GB 50174 数据中心设计规范
 - [6] GB 50198—2011 民用闭路监视电视系统工程技术规范
 - [7] GB 51348—2019 民用建筑电气设计标准
 - [8] GB 55024—2022 建筑电气与智能化通用规范
 - [9] GA/T 70 安全防范工程建设和维护保养费用预算编制办法
 - [10] GA/T 600 报警传输系统的要求（系列）
 - [11] GA/T 669（所有部分） 城市监控报警联网系统技术标准
 - [12] GA/T 1211 安全防范高清视频监控系统技术要求
 - [13] GA 1394—2017 信息安全技术 运维安全管理产品安全技术要求
 - [14] JGJ 66—2015 博物馆建筑设计规范
 - [15] WW/T 0066—2015 馆藏文物预防性保护方案编写规范
 - [16] WW/T 0114—2023 可移动文物二维数字化采集与加工
 - [17] WW/T 0115—2023 可移动文物三维数字化采集与加工
 - [18] WW/T 0125—2025 文物建筑防火设计规范
 - [19] WW/T 0126—2025 文物建筑电气火灾防控技术规范
-