ICS 35.020
CCS L 70

团　体　标　准

T/HSPA 0001—2023

文物安全综合信息应用平台
总体要求

Integrated information application platform for cultural relics security—General requirements

2023－09－25 发布　　2024－01－01 实施

湖北省安全技术防范行业协会　　发　布

目　　次

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。

本文件与T/HSPA 0002—2023《文物安全综合信息应用平台　功能要求》、T/HSPA 0003—2023《文物安全综合信息应用平台　数据接口要求》、T/HSPA 0004—2023《文物安全综合信息应用平台　数据资源分类及编码》共同构成支撑文物安全综合信息应用平台建设的标准体系。

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。

本文件由湖北省安全技术防范行业协会归口。

本标准主要起草单位：中国文物信息咨询中心、中南民族大学、中国人民公安大学、武汉旗云高科工程技术有限公司、重庆声光电智联电子有限公司、湖北省智能识别产品质量监督检验中心。

本标准主要起草人：张学文、刘为军、李成华、石鸿凌、江小平、刘晓栋、王奎、张伟、夏天、喻光超、侯建华、张楠、吴祥林。

引　言

从2017年的国务院办公厅《关于进一步加强文物安全工作的实施意见》（2017年81号文），到2018年中共中央办公厅、国务院办公厅的《关于加强文物保护利用改革的若干意见》（2018年10月发文），再到2022年4月国家文物局的《文物安全防控“十四五”专项规划》（2022年第12号文），这些文件都指出服务于文物安全保护的信息化系统建设刻不容缓。2020年7月针对目前文物安全保护领域信息化系统建设存在缺乏顶层设计、规范和标准长期缺位的问题，国家文物局发布了《文物安全监管平台建设指南(2020)》(文物督发〔2020〕24号)。该文件对文物安全监管平台建设起到了一定的指导作用，但未对建设全国互联的平台提供整体规范性指导，导致相关平台建设仍然各自为政、效益不高。2022年5月国家文物局印发《文物安全防控“十四五”专项规划》的通知（文物督发〔2022〕12号），进一步提出“出台文物安全监管平台建设技术指导标准，实现文物安全防护智能化和标准化”等要求。可见，指导信息化建设的相关标准规范迫在眉睫，亟需出台。

本文件以文物安全综合信息应用平台为标准化对象，目标是以科技手段辅助文物行政管理部门落实监管责任以及文物保护单位落实直接管理责任，提升防范和化解不可移动文物的盗掘、盗窃、火灾以及法人违法等文物安全风险的能力。本文件提出了总体要求，且与《文物安全综合信息应用平台　功能要求》、《文物安全综合信息应用平台　数据接口要求》以及《文物安全综合信息应用平台　数据资源分类及编码》等共同构成支撑文物安全综合信息应用平台建设的系列文件，涵盖了平台构成、技术框架、性能要求、安全要求、功能要求、数据接口要求以及数据资源分类和编码等内容，为服务于文物安全监督管理信息化平台的建设提供了较为完整的指导。文件的制定将促进相关系统的建设，使得文物安全监督管理高效有力，更好地服务于国家文物安全战略。

文物安全综合信息应用平台　总体要求

1　范围

本文件界定了文物安全综合信息应用平台的术语和定义，规定了文物安全综合信息应用平台的平台架构、性能要求以及安全要求。

本文件适用于文物保护单位开展文物安全综合信息应用平台的设计、建设以及验收。博物馆单位可参考本文件开展相关信息系统的设计和建设。

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，仅注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/T 16571 博物馆和文物保护单位安全防范系统要求

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 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 28827.1 信息技术服务 运行维护 第1部分：通用要求

GB/T 32922 信息安全技术 IPSec VPN安全接入基本要求与实施指南

GB/T 37931 信息安全技术 Web应用安全检测系统安全技术要求和测试评价方法

GB 50348 安全防范工程技术规范

T/HSPA 0002 文物安全综合信息应用平台 功能要求

T/HSPA 0003 文物安全综合信息应用平台 数据接口要求

T/HSPA 0004 文物安全综合信息应用平台 数据资源分类及编码

3　术语和定义

GB 50348、GB/T 16571界定的以及下列术语和定义适用于本文件。

3.1

文物安全综合信息应用平台　integrated information application platform for cultural relics security

以信息化数字化为驱动，综合利用文物保护单位内部安防、消防等信息系统数据以及文物保护单位外部的其他数据等多种数据资源，为各级文物行政管理部门落实文物安全监管责任以及为文物保护单位落实文物安全直接责任提供服务，提升对不可移动文物的盗掘、盗窃、火灾以及法人违法等文物安全风险防控能力的信息系统。

3.2

边缘数据接入系统　edge data access system

获取文物保护单位安防、消防等信息系统的报警类、故障类等数据，消除信息孤岛，为上层应用提供统一格式数据服务的信息系统。

3.3

文物安全事件　event of cultural relics security

指危害文物安全的事件，分为突发事件和异常事件两类。文物安全突发事件是指已造成文物损失和文

物保护工作失序的人为或非人为的事件。文物安全异常事件是指有可能造成文物损失和文物保护工作失序的人为或非人为的事件。

4 缩略语

以下缩略语适用于本文件：

AI：人工智能（Artificial Intelligence）

GIS：地理信息系统（Geographic Information System）

HTTP：超文本传输协议（Hypertext Transfer Protocol）

HTTPS：超文本传输安全协议（Hypertext Transfer Protocol over Secure Socket Layer）

MQTT：消息队列遥测传输（Message Queuing Telemetry Transport）

OPC：对象连接和嵌入技术在过程控制规范(Object Linking and Embedding for Process Control)

REST：表述性状态传递(Representational State Transfer)

VPN：虚拟专用网络（Virtual Private Network）

5 平台构成

5.1 文物安全综合信息应用平台（以下简称“平台”）由文物安全综合信息应用系统以及边缘数据接入系统构成，见图1。

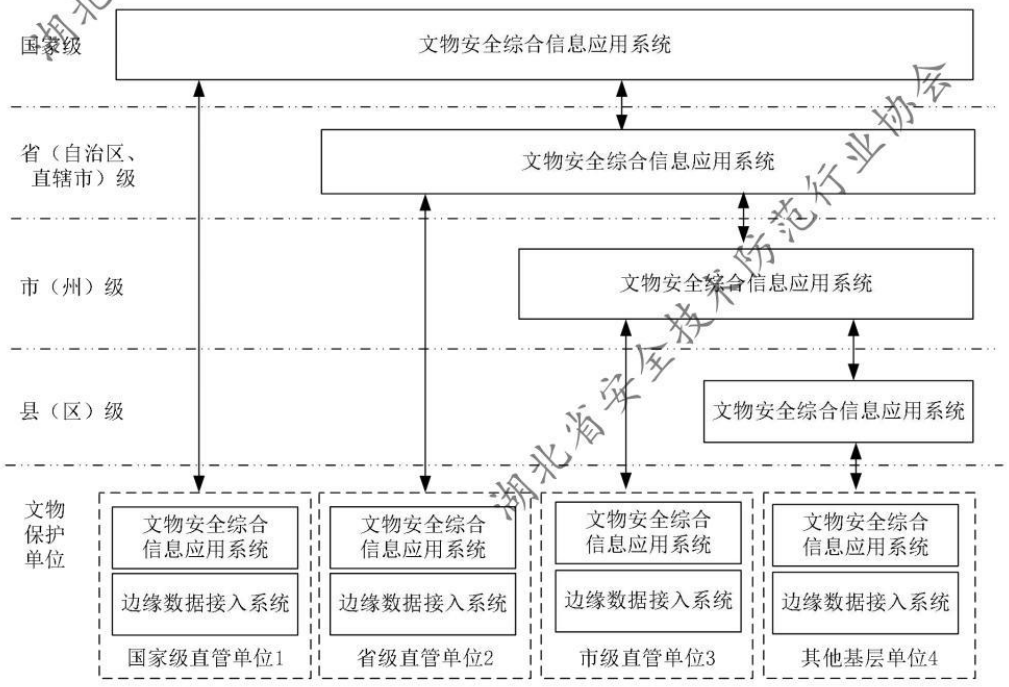

图 1 平台构成

5.2 平台用户类型分部门用户和单位用户两类，部门用户来自文物行政管理部门，可分为国家级用户、省级用户、市级用户以及县级用户四个等级，主要对本级所直接管辖的文物保护单位履行文物安全监管责任。单位用户来自文物保护单位，主要履行文物安全直接责任。

5.3 不同等级部门用户的应用层具有相同的应用层功能模块，区别在于所管辖文物保护单位和下级行政区域不同。上级用户拥有对下级系统的数据访问权限以及访问应用的权限。

5.4 边缘数据接入系统设置在文物保护单位，其主要应用功能目标是屏蔽底层不同厂商提供的安防、消防等信息系统之间的技术架构和数据差异，以统一格式协议提供数据服务。

6 技术框架

6.1 文物安全综合信息应用系统技术框架

文物安全综合信息应用系统技术框架见图 2，由数据服务层、应用支撑层和应用层构成。

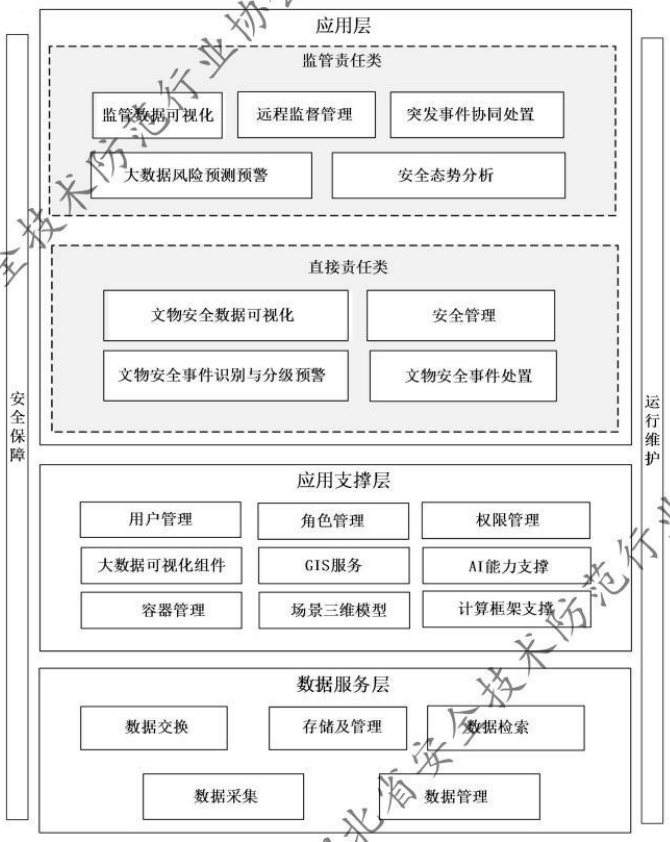

图 2 文物安全综合信息应用系统技术框架

6.1.1 数据服务层

6.1.1.1 数据采集

包括但不限于以下要求：

a）应支持获取边缘数据接入系统的提供数据，其数据接口应符合T/HSPA 0003 附录A的A接口的A.1-A.10要求；

b）宜支持采集社会数据，包括但不限于以下要求：

——文物拍卖交易数据；

——网络舆情数据；
——涉及文物安全违法犯罪的数据。

c）宜支持采集横向部门的公共数据，包括但不限于以下要求：
——气象部门的天气数据；
——公共安全部门的公共安全数据；
——应急部门的公共数据；
——医疗部门的疫情数据；
——地震部门的公共数据。

6.1.1.2 数据交换

包括但不限于以下要求：

a）应支持下级单位的系统向上级部门系统开放数据访问权限；

b）宜具备向公安、海关、应急、医疗卫生等部门提供数据服务接口的功能。

6.1.1.3 数据管理

应包括但不限于以下要求：

a）支持元数据管理功能，实现数据定义、数据类型和数据格式的统一管理；

b）提供数据资源目录管理功能；

c）具备数据访问权限管理功能。

6.1.1.4 存储及管理

包括但不限于以下要求：

a）应支持对结构化数据及非结构化数据的存储能力；

b）应建立数据的容错和高可用机制,包括数据的备份和快速恢复；

c）应支持设置数据存储策略,并自动执行存储策略；。

d）系统业务数据存储应留有一定容量，存储设备应性能可靠；

e）应提供包括但不限于基础数据库、主题数据库以及专题数据库等服务；

f）建立基础数据库、主题数据库以及专题数据库的数据表宜符合T/HSPA 0004 的描述。

6.1.1.5 数据检索

包括但不限于以下要求：

a）应支持结构化数据的精确检索和模糊检索；

b）应支持全文检索能力；

c）应具备多用户并发检索能力；

d）应具备海量数据的快速检索能力。

6.1.2 应用支撑层

6.1.2.1 AI 能力支撑

宜包括但不限于以下要求：

a）统计分析能力：提供多维度数据统计分析算法；

b）大数据风险预测能力，包括以下内容：
——提供基于大数据分析算法的文物安全风险预测模型服务；
——提供模型管理服务，包括模型训练与评估、模型发布、版本管理、部署情况等；
——预测的风险类型宜涵盖盗掘、盗窃、火灾以及法人违法等。

c）基于视频数据的文物安全事件识别能力，包括以下内容：

——提供基于深度学习的文物安全事件识别模型服务；

——提供模型管理服务，包括模型训练与评估、模型发布、版本管理、部署情况等；

——采用容器化部署技术，将模型和其依赖项打包为独立的容器；

——文物安全事件类型涵盖盗掘、盗窃、火灾以及法人违法等。

6.1.2.2 场景三维模型

宜包括但不限于以下要求：

a）支持采用三维建模技术对重点文物防护对象实景进行建模；

b）支持对三维模型文件的存储与管理。

6.1.2.3 容器管理

宜包括但不限于以下要求：

a）采用容器化技术部署基于视频数据的文物安全事件识别模型；

b）提供包括容器启动、容器运行状态监控、容器关闭以及镜像文件管理等功能。

6.1.2.4 GIS服务支撑

应提供GIS服务，以支持基于GIS的信息可视化呈现。

6.1.2.5 大数据可视化组件

应支持折线图、饼图、柱状图、雷达图以及热力图等多种形式的数据展示方式。

6.1.2.6 计算框架支撑

宜提供流式计算、批量计算、图计算以及内存计算等多种计算框架。

6.1.2.7 用户管理

应包括但不限于以下要求：

a）支持对系统用户进行增加、删除、修改、查询的操作；

b）新增用户信息包括用户账号、登录口令、用户姓名、电话号码、有效期、超时时间、最大登录次数、用户角色等信息项；

c）支持按用户账号、用户姓名等条件检索用户信息；

d）支持对用户登录口令重置。

6.1.2.8 角色管理

应包括但不限于以下要求：

a）支持系统管理员对角色的自定义管理,支持角色信息的增加、删除、修改、查询操作；

b）支持系统管理员添加角色名称、角色描述等信息。

6.1.2.9 权限管理

应包括但不限于以下要求：

a）支持对不同角色分配不同的功能权限；

b）支持对不同角色分配不同的数据资源权限；

c）支持对不同角色分配不同的表单操作权限。

6.1.3 应用层

包括但不限于以下要求：

a）应用层应包括监管责任类应用和直接责任类应用两个部分。监管责任类应用的服务对象是文物行政管理部门用户，直接责任类应用的服务对象是文物保护单位；

b）监管责任类应用宜包括“监管数据可视化、远程监督管理、大数据风险预测预警、安全态势分析以及突发事件协同处置”等功能。其功能目标是实现监管责任清晰化、监督管理业务规范化以及事件处置协同化，促进文物安全监管责任得到高效落实，提升文物监管效能；

c）直接责任类应用宜包括“文物安全数据可视化、文物安全事件识别与分级预警，事件处置以及安全管理”等功能。其功能目标是实现直接管理责任清晰化、安全管理信息化以及风险防控主动化，促进文物安全直接管理措施得到有效落实，提升推动文物保护单位风险防控能力；

d）应用层功能建设宜满足T/HSPA 0002 的要求。

6.2 边缘数据接入系统技术框架

边缘数据接入系统技术架构见图3，由数据接入层、数据缓存层、数据服务层和应用层构成。

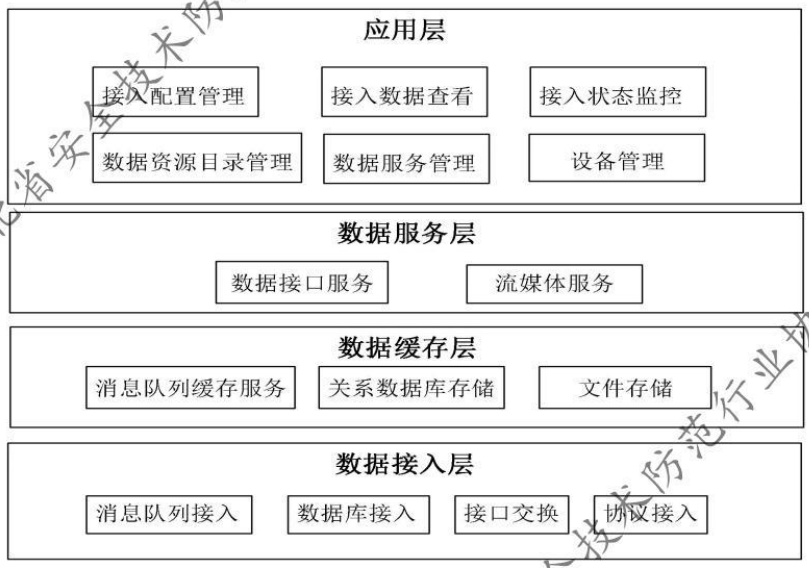

图 3 边缘数据接入系统技术架构

6.2.1 数据接入层

应包括但不限于以下要求：

a）被接入的数据源应包括但不限于文物保护单位的安防、消防类信息系统；

b）接入的数据类型包括但不限于安全事件报警类和故障报警类数据；

c）应具备从数据库管理系统获取数据库数据的能力；

d）应具备通过Web Service、REST接口获取数据的能力；

e）应提供开放接口供第三方开展数据对接；

f）开放接口宜符合T/HSPA 0003 附录B的要求；

g）应具备从消息队列中消费数据的能力，以消息订阅的方式获取数据；

h）应具备以协议解析数据方式获取结构化数据的能力；

i）应具备以协议转换、编解码等技术获取监控视频数据和音频数据的能力。

6.2.2 数据缓存层

应包括但不限于以下要求：

a）提供消息队列缓存服务；

b）提供关系数据库存储服务；

c）支持面向视频数据的文件存储服务。

6.2.3 数据服务层

包括但不限于以下要求：

a）应以数据接口服务方式向文物安全综合信息应用系统提供结构化数据服务；

b）数据接口要求宜符合T/HSPA 0003附录AA的A接口描述；

c）应提供流媒体服务。

6.2.4 应用层

应用层提供包括接入配置管理、接入数据查看、接入状态监控、数据资源目录管理、数据服务管理和设备管理，具体功能要求宜符合T/HSPA 0002的描述。

7 安全保障要求

7.1 设备安全

包括但不限于以下要求：

a）文物安全综合信息应用系统的信息安全等级宜达到GB/T 22239 规定的第二级标准及以上；

b）边缘数据接入系统的信息安全等级宜达到GB/T 22239 规定的第三级标准及以上；

c）文物安全综合信息应用系统宜提供设备注册和认证管理功能，支持边缘数据接入系统进行注册，并进行合法性认证；

d）边缘数据接入系统应具有双物理网卡，并使得内部网络与外部互联网隔离；

e）平台宜部署在已获得安全许可认证的服务器设备上；

f）平台的服务器宜使用已获得安全许可认证的国产操作系统；

g）平台宜使用已获得安全许可认证的国产数据库管理系统。

7.2 传输安全

宜包括但不限于以下要求：

a）文物安全综合信息应用系统与边缘接入系统之间，以及文物安全综合信息应用系统之间采用专线网络连接；

b）文物安全综合信息应用系统与边缘数据接入系统之间，以及文物安全综合信息应用系统之间采用互联网连接时，按照GB/T 32922要求实施VPN安全接入，以建立起安全网络隧道。

7.3 数据安全

包括但不限于以下要求：

a）访问控制应满足GB/T 22239的8.1.3.2要求；

b）安全审计应满足GB/T 22239的8.1.3.5要求；

c）宜支持多种数据容灾备份方式，关键数据存储采用高安全性的数据备份保护机制；

d）文物安全综合信息应用系统与边缘数据接入系统之间，以及文物安全综合信息应用系统之间进行数据传输时，宜采用数字证书对上传的所有数据进行签名与加密；

e）文物安全综合信息应用系统宜提供统一的密钥管理功能，包括数字证书的申请、注册、获取、更新或销毁等。

7.4 应用安全

平台的Web应用应符合GB/T 37931中的基本级要求。

8 运行维护要求

8.1 资产管理

应包括但不限于以下要求：

a）所有硬件资产建立统一标识；

b）所有资产建立管理台账，覆盖设备使用的生存周期；

c）针对重点平台资产实现维保提示和故障预警。

8.2 日志管理

应包括但不限于以下要求：

a）建立完备的运维日志体系；

b）运维日志包括操作时间、操作者和操作类型等信息。

8.3 运维策略

应包括但不限于以下要求：

a）平台建立完整和统一的运维策略体系，并符合GB/T 28827.1的规定；

b）平台建立统一的运维策略标识。

9 性能要求

9.1 文物安全综合信息应用系统性能要求

包括但不限于以下要求：

a）文物安全综合信息应用系统应提供统一时钟服务；

b）数据吞吐量宜不低于100万笔/s；

c）处置策略推理计算延迟宜不高于1s；

d）网页页面加载响应时间宜不超过2s；

e）资源利用率指标，宜满足以下要求：

——峰值内存保持在 80%以下；

——峰值 CPU 占有率保持在 75%以下。

9.2 边缘数据接入系统性能要求

包括但不限于以下要求：

a）获取数据时，误码率宜低于为10^{-6}；

b）支持接入的协议类型应包括但不限于：WEBSOCKET、HTTPS、HTTP、MQTT、MODBUS、OPC等；

c）支持接入的数据库管理系统类型应包括但不限于GaussDB和mysql等；

d）视频数据流媒体服务应符合 GB/T 28181的要求。

参 考 文 献

[1] 关于进一步加强文物安全工作的实施意见,国办,[2017]第81号.
[2] 关于加强文物保护利用改革的若干意见,中办、国办,2018年10月.
[3] 文物安全监管平台建设指南,国家文物局文物督发,[2020]第24号.
[4] 文物安全防控“十四五”专项规划,国家文物局文物督发,[2022]第12号.
[5] T/HSPA 0005—2023 文物保护单位安全管理风险评估指南.