ICS 35.240.99
UNSPSC 43.23.15
CCS L 77

团 体 标 准

T/UNP 555—2025

灭白蚁用设备控制系统技术规范

Technical specification for equipment control systems for termite extermination

2025－04－02 发布　　2025－04－02 实施

中国联合国采购促进会　　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。

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。

本文件由中国联合国采购促进会提出并归口。

本文件起草单位：武汉猫头鹰生物技术有限公司、湖北逸昂环保科技有限公司、武汉朗夏环保科技有限公司、湖北楚慧环保科技有限公司、上海蒂锦特环保科技有限公司。

本文件主要起草人：李永明、张盼、李支祥、李琳琳、刘海波。

引　言

为助力中国企业参与国际贸易，推动企业高质量发展，中国联合国采购促进会依托联合国采购体系，制定服务于国际贸易的系列标准，这些标准在国际贸易过程中发挥了越来越重要的作用，对促进贸易效率提升，减少交易成本和不确定性，保证产品质量与安全，增强消费者信心具有重要的意义。

联合国标准产品与服务分类代码（UNSPSC，United Nations Standard Products and Services Code）是联合国制定的标准，用于高效、准确地对产品和服务进行分类。在全球国际化采购中发挥着至关重要的作用，它为采购商和供应商提供了一个共同的语言和平台，促进了全球贸易的高效、有序发展。

围绕UNSPSC进行相关产品、技术和服务团体标准的制定，对助力企业融入国际采购，提升国际竞争力具有十分重要的作用和意义。

本文件采用UNSPSC分类代码由6位组成，对应原分类中的大类、中类和小类并用小数点分割。

本文件UNSPSC代码为“43.23.15”，由3段组成。其中：第1段为大类，“43”表示“信息技术广播与电信”，第2段为中类，“23”表示“软件”，第3段为小类，“15”表示“特定于业务功能的软件”。

灭白蚁用设备控制系统技术规范

1 范围

本文件规定了灭白蚁用设备控制系统的系统架构、功能要求、性能要求、安全要求、接口要求、运行维护及评价改进。

本文件适用于灭白蚁用设备控制系统的设计、建设与运维。

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/T 20270 信息安全技术 网络基础安全技术要求

3 术语、定义和缩略语

3.1 术语和定义

本文件没有需要界定的术语和定义。

3.2 缩略语

下列缩略语适用于本文件。

AES：高级加密标准（Advanced Encryption Standard）

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

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

JSON：对象表示法（JavaScript Object Notation）

SSL/TLS：安全套接层/传输层安全协议（Secure Sockets Layer/Transport Layer Security）

TCP/IP：传输控制协议/网际协议（Transmission Control Protocol/Internet Protocol）

UDP：用户数据报协议（User Datagram Protocol）

XML：可扩展标记语言（eXtensible Markup Language）

4 系统架构

灭白蚁用设备控制系统架构见图1，分为硬件层、网络层、支撑层、运维层、应用层、安全层、接口层，其中：

a) 硬件层：包含检测白蚁活动迹象的传感器、执行灭白蚁操作的设备、负责数据传输的通信设备以及具备数据处理和存储能力的计算设备；

b) 网络层：负责网络拓扑规划配置、设备管理监控及安全防护。依最小权限设访问策略，用防火墙等保障数据安全传输至上层，保证组件无缝通信；

c) 支撑层：包含数据库管理系统和操作系统。负责存储和管理系统运行过程中产生的数据，为系统软件和应用程序提供运行环境；

d) 运维层：包含日常运行维护任务、故障处理流程、性能优化策略以及系统更新管理。运维层保证系统保持良好的运行状态；

e) 应用层：包含数据管理模块、设备控制模块、预警与报警模块以及用户管理与权限控制模块，提供操作与管理功能；

f） 安全层：包括网络与系统安全保障。网络安全限制访问、加密传输等；系统安全控制用户访问、认证授权等，抵御安全威胁；
g） 接口层：包含设计原则、类型与规范、接口安全以及接口管理。实现系统与外部的有效交互。

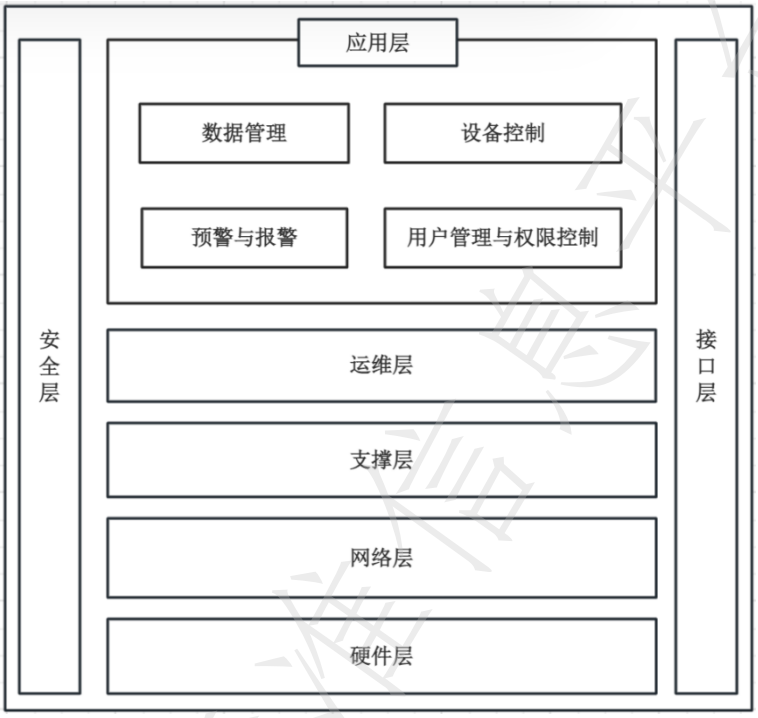

图1　灭白蚁用设备控制系统架构图

5　功能要求

5.1　数据管理

5.1.1　数据采集

数据采集模块的要求包括但不限于：
a） 应支持通过湿度传感器、温度传感器等采集白蚁活动相关的物理参数，如白蚁活动产生的振动幅度、活动区域的温湿度变化、白蚁释放的特殊气味浓度等；
b） 应支持实时获取设备运行状态信息，包括设备的工作温度、电量或功率消耗、通信信号强度等；
c） 应根据实际需求调整传感器数据采集的频率；
d） 采集的数据应附带时间戳和位置信息；
e） 应兼容不同型号和规格的传感器及设备，具备自动识别和适配功能。

5.1.2　数据共享

数据共享模块的要求包括但不限于：
a） 应支持数据共享功能，支持在授权范围内与其他相关系统或人员共享数据；
b） 应建立数据共享安全审计机制，对数据共享操作进行详细记录，包括共享时间、共享对象、共享数据内容摘要等信息；
c） 应支持数据共享权限的动态管理，根据不同用户或系统的实时需求和信用评级等因素，灵活调整数据共享的范围和权限级别。

5.1.3　数据存储

数据存储模块的要求包括但不限于：
a） 应具备数据分类功能，将白蚁活动数据、设备运行数据、环境数据等按照不同的类别和时间序列进行存储和管理；

b） 应具备数据编辑功能，支持数据标记、注释和修正；
c） 应定期自动备份数据到外部存储设备或云端；
d） 应支持存储监测数据、设备运行日志、操作记录等信息；
e） 应具备数据存储容量的动态扩展能力；
f） 存储的数据应具备高可用性，在部分硬件故障或网络异常情况下仍保证数据的正常访问和使用；
g） 应采用分层存储和索引技术，优化数据存储结构；
h） 应具备数据存储完整性校验功能，定期对存储的数据进行哈希值计算和比对；
i） 应支持多版本数据存储，对重要数据的修改和更新操作进行版本记录，可回溯历史数据版本；
j） 应支持数据的压缩存储和加密存储。

5.1.4 数据处理与分析

数据处理与分析模块的要求包括但不限于：
a） 应对采集到的原始数据进行数据清洗、数据校准和数据转换等实时预处理；
b） 应运用智能算法对处理后的数据进行深度分析，如采用模式识别技术判断白蚁活动类型（觅食、筑巢、迁徙等），运用趋势分析算法预测白蚁活动的发展趋势；
c） 应具备自动学习和优化分析模型的能力；
d） 应支持白蚁活动数据、环境数据和设备状态数据等融合分析，挖掘数据的内在关联。

5.2 设备控制

5.2.1 手动控制

手动控制模块的要求包括但不限于：
a） 操作界面应支持用户通过图形化界面或快捷键等方式手动启动、停止和调整各类灭白蚁设备的运行状态和参数；
b） 应实时反馈设备的执行情况和当前状态；
c） 应支持临时保存当前设备参数设置；
d） 应支持对设备进行分组控制和单独控制，支持用户根据实际需求灵活选择控制对象。

5.2.2 自动控制

自动控制模块的要求包括但不限于：
a） 应具备预设多种智能控制策略的能力，如根据白蚁活动的高峰期和低谷期自动调整设备的工作模式和强度，在白蚁活动频繁时自动增加防治力度，在活动较少时进入节能或低强度监测模式；
b） 应适应温度、湿度、光照等因素的环境变化，自动优化设备控制参数；
c） 应根据设备运行时长、累计工作量等因素自动安排设备维护计划并提示用户；
d） 应根据历史数据和实时监测数据自动评估控制策略的有效性，并进行自我优化调整；
e） 应支持对现场设备的实时监控和远程管理。

5.3 预警与报警

5.3.1 监测预警

监测预警的要求包括但不限于：
a） 应支持实时监测系统运行状态和数据变化，检测到白蚁活动异常、设备故障或环境参数异常等情况时，立即触发报警信号；
b） 应支持用户自定义报警条件和阈值，根据不同的应用场景和需求设置个性化的报警规则；
c） 应具备报警事件的关联分析能力，多个相关异常同时发生时能综合判断报警级别和处理优先级；
d） 应根据历史报警数据自动优化报警阈值和规则，减少误报和漏报；
e） 应根据报警事件的严重程度和紧急程度进行分级。

5.3.2 报警推送

报警推送模块的要求包括但不限于：

a) 应提供短信通知、电子邮件通知、系统弹窗等多种报警通知方式，并增加智能过滤功能；
b) 应支持报警通知的个性化设置，用户可根据自己的偏好选择接收报警的方式和时间间隔；
c) 应支持报警通知的推送优先级设置，保证重要报警优先推送；
d) 应具备报警通知发送状态的反馈和记录功能；
e) 报警通知应包含报警时间、报警地点、报警原因、报警级别等信息。

5.4 用户管理与权限控制

5.4.1 用户管理

用户管理模块的要求包括但不限于：

a) 应支持用户账户的创建、修改、删除和查询操作，用户信息应包括用户名、密码、联系方式、所属部门、角色等；
b) 应具备用户账号锁定和解锁功能，在用户密码多次错误或账号存在安全风险时自动锁定，经授权后可解锁；
c) 应支持用户信息的批量导入和导出功能；
d) 应支持密码强度设置、密码修改提醒、密码找回等操作；
e) 应根据用户的职责和权限将用户划分为不同的用户组，如管理员组、操作人员组、数据分析人员组等。

5.4.2 权限控制

权限控制模块的要求包括但不限于：

a) 应基于用户角色和用户组进行细粒度的权限管理，不同权限的用户对系统功能和数据具有不同的访问和操作权限；
b) 应根据业务需求和用户职责的变化及时调整权限配置；
c) 应具备权限申请和审批流程，用户可根据工作需要申请额外权限，经审批后生效；
d) 系统应记录用户的操作日志，包括登录时间、操作内容、操作结果等信息。

6 性能要求

6.1 响应时间

系统的响应时间宜控制在1.5 s以内。

6.2 并发用户数

系统应稳定支持至少150个并发用户，在用户访问高峰时段，系统能高效、稳定地提供服务。

6.3 数据容量

系统应具备强大的数据存储能力，能存储至少15万条数据记录。

6.4 系统稳定性

系统应设计故障转移和灾难恢复机制，在发生故障后，宜在45 min内恢复正常运行。

6.5 网络带宽占用

正常数据传输时网络带宽占用率不应超过30%，大数据量传输（如批量数据同步）不应超过80%。

7 安全要求

7.1 用户安全

7.1.1 应对灭白蚁用设备控制系统的用户进行访问控制，基于角色和权限限制对系统功能和数据的访

问。

7.1.2 应采用多因素认证身份验证和授权机制，防止非授权人员操作。

7.1.3 应定期进行系统漏洞扫描，并密切关注系统补丁，及时更新，防范黑客攻击。

7.1.4 应建立系统安全审计机制，记录用户登录、操作记录等操作日志，日志应不可篡改。

7.1.5 应定期审计分析，至少每月一次。

7.1.6 宜建立系统用户行为分析模型，如数据大量异常下载、非法修改系统关键配置等，监测用户操作行为模式，及时发现异常行为并进行预警和干预。

7.2 网络安全

7.2.1 应依据最小权限原则建立网络访问控制策略，限制对灭白蚁用设备控制系统的网络访问，仅允许授权用户和设备访问。

7.2.2 应设置防火墙，配置合理的访问控制策略，应允许授权的网络流量通过，网络安全防护应符合GB/T 20270 的相关要求。

7.2.3 宜采用 AES、SSL/TLS 等加密算法对传输的重要信息进行加密。

7.2.4 加密算法应定期更新，防止数据在传输中被窃取或篡改。

7.2.5 应至少每周一次进行网络漏洞扫描，及时发现并修复灭白蚁用设备控制系统网络中的漏洞。

7.2.6 应建立网络备份策略，定期备份网络设备和系统，保障白蚁防治工作的连续性。

7.2.7 应建立网络安全态势感知系统，实时收集、分析网络安全相关信息，如网络攻击趋势、漏洞分布等。

8 接口要求

8.1 设计原则

接口设计原则包括但不限于以下方面：

a) 通用性：遵循行业通用标准与规范，保证接口在不同系统间具备广泛的兼容性与通用性；
b) 开放性：采用开放架构设计，积极接纳第三方系统接入，为系统的扩展与融合创造有利条件；
c) 安全性：重视数据安全，通过加密算法、身份认证、授权管理等多重安全手段，防范各类安全威胁；
d) 稳定性：在复杂多变的运行环境中，能持续稳定地提供服务。

8.2 类型与规范

接口类型与规范要求包括但不限于以下方面：

a) 数据接口：应支持 XML、JSON 等常用数据格式，通过 HTTP/HTTPS 协议实现高效、安全的数据通信；
b) 控制接口：采用高强度加密协议保障指令安全，并配备身份验证机制；
c) 通信接口：支持 TCP/IP、UDP 等多种通信方式，依据实际需求灵活选择；
d) 监测接口：实时采集并反馈设备运行状态及环境数据。

8.3 接口安全

接口安全要求包括但不限于以下方面：

a) 加密传输：对数据传输实施全程加密策略，运用 AES、SSL/TLS 等先进加密算法；
b) 身份认证：建立身份认证体系，运用用户名/密码、数字证书等多种认证方式，验证访问者身份；
c) 访问授权：基于精细的角色管理实施访问授权策略，根据用户角色精准分配接口操作权限，有效限制非法操作；
d) 日志记录：记录接口访问的全过程日志，涵盖访问时间、操作内容、访问 IP 等关键信息。

8.4 接口管理

接口管理要求包括但不限于：

a) 接口文档管理：构建接口文档库，及时更新接口的详细说明、参数信息、使用示例等内容；
b) 版本管理：实施接口版本管理策略，保证不同版本之间具备良好的兼容性，在进行版本更新时，提前向用户发布通知；
c) 故障处理：配备专业技术团队负责接口日常维护工作，及时响应并处理各类故障，并积极收集用户反馈，优化接口功能与性能。

9 运行维护

9.1 日常维护

9.1.1 应定期检查各类硬件设备，如传感器、服务器、存储设备等，检查软件界面的显示准确性和功能完整性。
9.1.2 应定期核对工艺参数、喷雾环境参数等各类参数的设置。
9.1.3 应定期对系统中的重要数据进行备份，防止数据丢失。
9.1.4 应及时更新系统架构文档、用户手册等，记录系统的设计和配置信息。
9.1.5 应记录系统维护操作和变更，保证维护活动的可追溯性。
9.1.6 应维护系统配置文档，保证系统配置的准确性和一致性。

9.2 系统监控

9.2.1 应实时监控系统的稳定性、工艺参数的准确性、喷雾环境参数的实时性等。
9.2.2 应检查服务器的负载情况、内存使用量、磁盘空间剩余量等关键指标，以及喷雾数据的采集频率和准确性。
9.2.3 应监控喷雾检测控制、喷雾量分布图、喷雾数据采集等模块的运行数据。

9.3 性能优化

9.3.1 应分析系统中数据处理算法，对工艺参数计算、喷雾数据统计等算法进行优化。
9.3.2 应优化系统界面的响应速度，保证用户操作的流畅性。
9.3.3 应合理管理系统资源，如内存、CPU 等。

9.4 应急管理

9.4.1 应建立应急处置机构，建立预防预警机制，定期进行测试、培训和演练。
9.4.2 发生系统故障、数据丢失等突发事件，应立即启动应急响应计划，采取相关措施抑制事件的不良影响。
9.4.3 应制定针对灭白蚁用设备控制系统的安全应急预案，明确安全事件分类、应急响应级别和处理流程。
9.4.4 应对灭白蚁用设备控制系统的安全事件总结评估，分析原因和教训，总结应急经验教训，提出改进措施。

10 评价改进

依据第 5 章～9 章规定的要求，定期开展灭白蚁用设备控制系统的功能、性能、安全、接口和运维方面的评价，审查不合格项，并有针对性地采取纠偏措施并持续改进。

参 考 文 献

[1] GB/T 50768—2012 白蚁防治工程基本术语标准