ICS
CCS 点击此处添加 CCS 号

团　　体　　标　　准

T/XXX XXXX—XXXX

智能商品资产盘查管控平台技术规范

Technical Specifications for the Intelligent Commodity Asset Inventory Control Platform

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

全国城市工业品贸易中心联合会　　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　　提出。

本文件由全国城市工业品贸易中心联合会归口。

本文件主要起草单位：

本文件主要起草人：

智能商品资产盘查管控平台技术规范

1 范围

本文件规定了智能商品资产盘查管控平台技术规范的术语和定义、运行环境、功能要求、平台性能及安全要求、平台验收测试。

本文件适用于智能商品资产盘查管控平台。

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 25000.51 系统与软件工程 系统与软件质量要求和评价（SQuaRE） 第51部分：就绪可用软件产品（RUSP）的质量要求和测试细则

3 术语和定义

下列术语和定义适用于本文件。

3.1

商品资产盘查管控 Commodity assets inventory control

商品资产盘查管控是指对企业或组织所持有的商品资产进行全面的清查、核实、记录、管理和控制的过程。

4 运行环境

4.1 硬件环境

4.1.1 CPU:I3 以上。

4.1.2 内存:1G 以上。

4.1.3 硬盘:500 G 以上。

4.2 软件环境

WINDOWS XP、WINDOWS 7、8、10、WINDOWS 2008 操作系统环境。

5 功能要求

5.1 资产信息管理

5.1.1 资产录入与编辑

系统应支持快速、准确地录入和编辑商品资产信息，包括资产名称、编码、类型、数量、位置、状态等。

5.1.2 资产分类与标签

根据企业需求，系统应支持自定义资产分类和标签，以便于资产的快速查找和分类管理。

5.1.3 资产查询与搜索

系统应提供灵活的查询和搜索功能，允许用户根据多种条件（如资产名称、编码、位置等）快速找到所需资产。

5.1.4 资产报表生成

系统应能够自动生成各类资产报表，如资产清单、资产折旧表、资产变动表等，并支持导出和打印功能。

5.2 资产盘查管理

5.2.1 实时盘查

系统应支持通过物联网技术（如RFID、二维码等）进行实时盘查，确保资产信息的实时性和准确性。

5.2.2 定期盘查

系统应支持设置定期盘查计划，自动提醒并记录盘查结果，便于跟踪和管理。

5.2.3 盘查结果记录

系统应详细记录每次盘查的时间、地点、参与人员、盘查结果等信息，便于后续分析和审计。

5.2.4 异常预警

系统应能够在盘查过程中发现异常情况时自动触发预警机制，提醒相关人员及时处理。

5.3 资产变动管理

5.3.1 资产入库与出库

系统应支持资产的入库和出库操作，记录相关信息并更新资产状态。

5.3.2 资产调拨与转移

系统应支持资产的调拨和转移操作，确保资产在企业内部合理流动。

5.3.3 资产维修与报废

系统应支持资产的维修和报废管理，记录维修信息和报废原因，确保资产得到合理处理。

5.4 数据管控

5.4.1 数据统计与分析

系统应对资产数据进行统计和分析，包括资产数量、分布、使用状况等，为管理决策提供数据支持。

5.4.2 趋势预测

系统应基于历史数据预测未来资产变化趋势，为企业制定采购、库存等策略提供参考。

5.4.3 决策支持

系统应提供可视化的数据分析结果，帮助企业管理层快速了解资产状况，制定有效的管理策略。

6 平台性能及安全要求

6.1 性能要求

系统的性能要求应符合 GB/T 25000.51的要求。

6.2 安全要求

6.2.1 物理安全

6.2.1.1 确保服务器和数据中心位于安全的环境中，有适当的访问控制和物理防护措施。

6.2.1.2 使用防盗报警系统、视频监控和门禁系统来监控和记录物理访问。

6.2.2 网络安全

6.2.2.1 实施防火墙、入侵检测系统（IDS）和入侵防御系统（IPS）来抵御网络攻击。
6.2.2.2 定期更新和修补网络设备和应用程序的安全漏洞。
6.2.2.3 部署网络隔离和访问控制策略，限制对系统的非法访问。

6.2.3 系统安全

6.2.3.1 使用强密码策略，并定期更换系统密码。
6.2.3.2 限制系统管理员的访问权限，并遵循最小权限原则。
6.2.3.3 实施定期的安全审计和日志审查，以检测异常行为。

6.2.4 数据安全

6.2.4.1 使用加密技术（如 TLS/SSL）来保护数据传输过程中的机密性。
6.2.4.2 在数据库中实施数据加密，保护敏感信息的存储。
6.2.4.3 遵循数据备份和恢复策略，确保数据的可靠性和可恢复性。

6.2.5 应用程序安全

6.2.5.1 对应用程序进行安全编码和测试，以防止 SQL 注入、跨站脚本（XSS）等常见漏洞。
6.2.5.2 实施输入验证和输出编码，以减少应用程序层面的安全风险。
6.2.5.3 定期更新和修补应用程序的安全漏洞。

6.2.6 访问控制

6.2.6.1 实施基于角色的访问控制（RBAC），确保用户只能访问其所需的数据和功能。
6.2.6.2 使用多因素身份验证（MFA）来提高用户登录的安全性。
6.2.6.3 定期审计和审查用户账户和权限，删除不再需要的账户和权限。

6.2.7 审计和合规性

6.2.7.1 实施全面的日志记录和监控策略，以跟踪和检测异常行为。
6.2.7.2 定期进行安全审计和渗透测试，以评估系统的安全性并发现潜在的安全风险。

6.2.8 灾难恢复和业务连续性

6.2.8.1 部署灾难恢复计划，确保在发生灾难时能够迅速恢复系统的正常运行。
6.2.8.2 实施备份和恢复策略，包括定期备份数据和关键系统组件。
6.2.8.3 测试灾难恢复计划的有效性，并定期进行更新和修订。

6.2.9 安全漏洞管理

6.2.9.1 建立漏洞管理流程，及时识别和响应系统中的安全漏洞。
6.2.9.2 与安全供应商和社区保持联系，获取最新的安全信息和补丁。

7 平台验收测试

按照GB/T 25000.51的要求进行验收测试。