ICS 点击此处添加 ICS 号
CCS 点击此处添加 CCS 号

团　　体　　标　　准

T/QGCML XXXX—XXXX

供应链信息跟踪管理平台技术规范

Technical specifications for supply chain information tracking and management 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。

本文件起草单位：

本文件主要起草人：

本文件为首次发布。

供应链信息跟踪管理平台技术规范

1 范围

本文件规定了供应链信息跟踪管理平台技术规范的术语和定义、系统架构、功能要求、安全要求以及测试与维护。

本文件适用于供应链信息跟踪管理平台技术的设计和检验。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

供应链信息跟踪管理平台 Supply chain information tracking and management platform

指通过信息技术手段，实现供应链各环节信息实时采集、存储、处理、分析和展示的综合性管理平台。

4 系统架构

4.1 模块化设计

将系统划分为多个模块，每个模块负责特定的功能，以降低模块间的耦合度，提高系统的可维护性和可扩展性。

4.2 分布式部署

采用分布式架构，将系统部署在多个服务器上，实现负载均衡和故障转移，提高系统的稳定性和可用性。

4.3 接口设计

定义清晰的接口规范,确保各模块之间的数据交换和通信顺畅。同时,提供与外部系统的标准接口，如RESTful API，以便于与其他系统的集成和互操作。

5 功能要求

5.1 信息采集与录入

5.1.1 多源数据采集

平台应支持从各种设备和系统（如RFID、条形码扫描器、GPS跟踪器、传感器等）中自动采集供应链数据，包括但不限于产品标识、位置信息、温度湿度数据、运输状态等。

5.1.2 手动录入

对于无法自动采集的数据，平台应提供用户友好的界面，允许用户手动输入相关信息，并确保数据的准确性和完整性。

5.1.3 数据校验

平台应对采集和录入的数据进行校验，以确保数据的有效性，并减少错误和冗余数据。

5.2 数据存储与管理

5.2.1 数据仓库

建立统一的数据仓库，对采集和录入的供应链数据进行集中存储和管理，确保数据的一致性和安全性。

5.2.2 数据分类与索引

根据业务需求，对存储的数据进行分类和索引，以便于后续的查询和分析。

5.2.3 数据备份与恢复

实施定期的数据备份策略，确保在发生数据丢失或损坏时能够迅速恢复数据。

5.2.4 数据安全性

采用数据加密、访问控制等技术手段，确保存储数据的安全性和保密性。

5.3 信息查询与展示

5.3.1 灵活查询

提供多种查询方式，如关键词搜索、条件筛选、时间范围选择等，使用户能够根据自己的需求快速找到所需的信息。

5.3.2 可视化展示

利用图表、地图等可视化工具，将复杂的供应链数据以直观的方式呈现出来，帮助用户更好地理解数据和发现潜在问题。

5.3.3 报表生成

支持自定义报表生成功能,用户可以根据自己的需求生成各种形式的报表,如销售报表、库存报表、运输报表等。

5.4 用户权限管理

5.4.1 角色划分

根据业务需求，将用户划分为不同的角色，并为每个角色分配相应的权限。

5.4.2 权限管理

实现精细化的权限管理功能，确保用户只能访问和操作自己有权访问的数据和功能。

5.4.3 日志记录

记录用户的操作日志，以便于后续的审计和追踪。

6 安全要求

6.1 数据安全

6.1.1 数据加密

6.1.1.1 所有在平台中存储的敏感数据（如供应商和客户的个人信息、财务数据、商业机密等）应使用强加密算法进行加密，确保数据的机密性。

6.1.1.2 数据在传输过程中，特别是在公共网络环境中，应采用安全传输协议（如 HTTPS）进行加密传输，防止数据被截获和篡改。

6.1.2 数据备份与恢复

6.1.2.1 平台应实施定期的数据备份策略，确保数据的完整性和可用性。

6.1.2.2 备份数据应存储在安全的地方，以防止物理损坏或非法访问。

6.1.2.3 在数据丢失或损坏的情况下，应能够快速、准确地恢复数据。

6.1.3 数据访问控制

6.1.3.1 平台应实施严格的访问控制策略，确保只有授权用户才能访问敏感数据。

6.1.3.2 用户访问权限应根据其角色和职责进行划分，避免权限过大或过小导致的数据泄露或误操作。

6.1.3.3 应对用户访问进行审计和监控，记录访问日志以便后续审计和追查。

6.2 系统安全

6.2.1 防火墙与入侵检测

6.2.1.1 平台应部署防火墙和入侵检测系统，防止非法访问和恶意攻击。

6.2.1.2 防火墙应配置合理的安全策略，限制不必要的端口和服务，防止潜在的安全风险。

6.2.1.3 入侵检测系统应实时监控平台的安全事件，发现异常行为及时报警并采取相应措施。

6.2.2 漏洞管理

6.2.2.1 定期对平台进行安全漏洞扫描和评估，发现潜在的安全漏洞并及时修复。

6.2.2.2 对于已知的安全漏洞，应尽快发布补丁或升级版本，确保平台的安全性。

6.2.3 安全审计与日志记录

6.2.3.1 平台应实施安全审计机制，对系统的安全事件和异常行为进行记录和审计。

6.2.3.2 审计日志应详细记录用户操作、系统事件、安全事件等关键信息，以便后续追查和审计。

6.2.3.3 审计日志应妥善保存，防止被篡改或删除。

6.3 应用安全

6.3.1 身份验证与授权

6.3.1.1 平台应采用强密码策略，要求用户设置复杂且不易被猜测的密码。

6.3.1.2 用户登录平台时应进行身份验证，确保登录用户的合法性。

6.3.1.3 对于关键操作（如修改数据、删除数据等），应进行二次验证或授权确认，防止误操作或恶意操作。

6.3.2 安全更新与补丁管理

6.3.2.1 定期对平台的应用软件、中间件、操作系统等进行安全更新和补丁安装，确保软件的安全性。

6.3.2.2 在更新和补丁安装前应进行充分的测试和验证，确保更新过程不会对系统的稳定性和可用性造成影响。

6.3.3 应用安全测试

6.3.3.1 在平台开发完成后应进行全面的安全测试，包括渗透测试、漏洞扫描等，确保平台的安全性和稳定性。

6.3.3.2 对于发现的安全漏洞和问题应及时修复并重新进行测试验证。

7 测试与维护

7.1 功能测试

7.1.1 根据需求文档和设计文档，设计覆盖所有功能的测试用例，确保每个功能都得到充分测试。

7.1.2 按照测试用例执行测试，记录测试结果，包括成功、失败、阻塞等情况，并编写测试报告。

7.2 性能测试

7.2.1 结合实际业务场景，设计性能测试场景，包括并发用户数、响应时间、吞吐量等指标。

7.2.2 按照性能测试场景执行测试，并使用性能监控工具对系统进行实时监控，记录性能指标数据。

7.3 安全测试

7.3.1 使用安全扫描工具对系统进行扫描，发现潜在的安全漏洞。

7.3.2 模拟黑客攻击，测试系统的安全防护能力。

7.4 日常维护

7.4.1 使用系统监控工具对系统进行实时监控，包括服务器状态、网络状态、数据库状态等，确保系统稳定运行。

7.4.2 定期查看和分析系统日志，发现潜在的问题和异常，并及时处理。

7.5 故障处理

7.5.1 通过系统监控、用户反馈、日志分析等方式发现系统故障。

7.5.2 使用调试工具和技术手段对故障进行定位，找到故障的原因和位置。

7.5.3 根据故障定位结果，修复故障并验证修复效果。

7.6 升级与维护

7.6.1 根据业务需求和技术发展，对系统进行升级和优化，提高系统的性能和稳定性。

7.6.2 制定长期和短期的维护计划，包括定期巡检、系统优化、安全加固等，确保系统的持续稳定运行。