# 范围

## 标识

注释：本条应描述本文档所适用的系统和软件的完整标识，适用时，包括其标识号、名称、缩略名、版本号和发布号。

注释：本条应概述本文档所适用的系统和软件的用途，描述系统与软件的一般特性（如规模、安全性、可靠性、实时性、技术风险等特性），概述系统开发、运行和维护的历史，标识项目的需方、用户、开发方和保障机构等，标识当前和计划的运行现场，列出其他有关文档。

注释：本条应概述本文档的用途和内容，并描述与它的使用有关的保密性方面的要求。

## 系统概述

注释：本章应列出引用文档的编号、标题、编写单位、修订版及日期，还应给出不能通过正常渠道得到的文档的来源。

## 文档概述

注释：本章应分为如下小条规定软件需求，即作为软件验收条件的软件配置项特征。软件需求是为满足分配给该软件配置项的系统需求而形成的软件需求。每条需求应指定项目唯一的标识符以便于测试和追踪，而且应以一种能为其定义具体测试对象的方式来描述。每条需求应注明所采用的合格性方法（见第4章），还应注明与系统或子系统需求的可追溯性（或在第5章给出）。

# 引用文档

# 需求

## 要求的状态和方式

注释：如果要求软件在多种状态或方式下运行，并且不同的状态或方式具有不同的需求，则应标识和定义每一状态和方式，例如分析、训练、降级、紧急情况、后备、战时和平时等。以仅用方式、用方式中的状态、状态中的方式、或其他有效的方式描述软件。如果不需要多种状态和方式，应如实陈述，而不需要进行人为的区分；如果需要多种状态和/或方式，应使本规格说明中的每个需求或每组需求与这些状态和方式相对应，对应关系可以在本条或本条所引用的附录中，通过表格或其他方式加以指明，也可以在该需求出现的章条中加以说明。

## CSCI能力需求

注释：为详细说明与软件各个能力相关的需求，本条可分为若干子条。“软件能力需求”中的“能力”为一组相关需求，可用“功能”、“主题”、“对象”、或其他适合表示需求的词替代。

注释：本条应标识必需的每一个软件能力，并详细说明与该能力有关的需求。能力可以更清晰地分解成若干子能力，则应分条对子能力进行说明。需求应详细说明所需的软件行为，包括适用的参数，如响应时间、吞吐时间、其他时限约束、时序、精度、容量、优先级、连续运行需求和在基本运行条件下允许的偏差；适当时，需求还应包括在异常条件、非许可条件或超限条件下所需的行为，错误处理需求和任何为保证在紧急时刻运行的连续性而引入到软件中的规定。输出有关的需求时，应考虑在3.3.X给出的要考虑的主题列表。

### 用户身份验证功能

a) 标识号：REQ-1.1

b) 说明：用户登录时必须通过多因素身份验证（MFA）确保安全性。

c) 进入条件：用户尝试访问系统受限资源。

d) 输入：

- 用户名

- 密码

- 动态验证码（如短信/邮件/认证器App）

e) 输出：

- 访问令牌（JWT）

- 错误提示（如认证失败）

f) 处理：

1. 验证用户名和密码是否匹配数据库记录。

2. 向用户注册设备发送动态验证码。

3. 比对用户输入的验证码与服务端生成的验证码。

4. 生成并返回JWT令牌（有效期2小时）。

g) 性能：

- 认证响应时间 ≤ 2秒（95%请求）。

- 支持每秒50次并发认证请求。

h) 约束与限制：

- 仅支持TOTP（时间型动态令牌）和短信验证码。

- 密码复杂度要求：至少8字符，包含大小写字母、数字及特殊符号。

---

### 数据批量导入功能

#### 实时通知推送功能

a) 标识号：REQ-3.1

b) 说明：向用户推送系统通知（站内信、邮件、短信）。

c) 进入条件：系统事件触发（如订单状态变更）。

d) 输入：

- 事件类型（如“订单发货”）

- 用户ID

- 动态模板参数（如订单号、物流单号）

e) 输出：

- 通知发送状态（成功/失败）

- 用户侧通知展示

f) 处理：

1. 根据事件类型选择通知模板。

2. 替换模板中的动态参数。

3. 异步调用第三方服务（邮件服务器/SMS网关）。

4. 记录通知状态及失败重试（最多3次）。

g) 性能：

- 推送延迟 ≤ 5秒（从事件触发到用户接收）。

- 支持每秒2000条通知。

h) 约束与限制：

- 短信通道仅支持国内运营商。

- 邮件模板需预审，禁止包含外部链接。

---

#### 数据分析报告生成功能

a) 标识号：REQ-4.1

b) 说明：自动生成用户行为分析PDF报告。

c) 进入条件：用户选择时间范围并提交生成请求。

d) 输入：

- 时间范围（开始日期-结束日期）

- 分析维度（如地域、设备类型）

e) 输出：

- PDF报告文件（含图表）

- 生成进度状态

f) 处理：

1. 从数据仓库提取指定时间范围内的原始数据。

2. 执行聚合计算（如UV、PV、转化率）。

3. 调用图表引擎生成可视化图表。

4. 使用LaTeX引擎渲染PDF。

g) 性能：

- 10万条数据生成时间 ≤ 30秒。

- 支持同时处理5个并发生成任务。

h) 约束与限制：

- 最大时间范围：3个月。

- 仅支持英文/中文报告。

---

#### 系统日志归档功能

a) 标识号：REQ-5.1

b) 说明：每天凌晨自动压缩并归档3个月前的日志文件。

c) 进入条件：系统时间到达预设调度时间（00:00）。

d) 输入：

- 原始日志文件（路径：`/var/log/app/\*.log`）

e) 输出：

- 压缩后的日志包（格式：`.tar.gz`）

- 归档记录（写入数据库）

f) 处理：

1. 扫描日志目录，筛选满足时间条件的文件。

2. 使用GZIP算法压缩文件。

3. 上传至云存储（如AWS S3）。

4. 删除本地原始日志文件。

g) 性能：

- 压缩比 ≥ 70%。

- 100GB日志处理时间 ≤ 1小时。

h) 约束与限制：

- 仅保留最近6个月的归档文件。

- 单次压缩文件数 ≤ 5000个。

#### 用户权限管理功能

##### 数据可视化仪表盘功能

a) 标识号：REQ-7.1

b) 说明：提供可配置的实时数据仪表盘，支持动态图表交互。

c) 进入条件：用户访问仪表盘页面或刷新数据。

d) 输入：

- 数据源配置（如数据库表、API端点）

- 可视化模板（折线图/柱状图/热力图）

e) 输出：

- 动态渲染的图表组件

- 数据刷新时间戳

f) 处理：

1. 解析用户选择的图表配置参数。

2. 从指定数据源拉取最新数据集。

3. 执行数据聚合（如按小时/天/月统计）。

4. 调用ECharts引擎生成交互式图表。

g) 性能：

- 10万条数据渲染时间 ≤ 3秒。

- 支持每秒5次动态数据更新。

h) 约束与限制：

- 单图表最多展示5个数据维度。

- 实时数据流仅保留最近30天的历史记录。

---

##### 多语言国际化支持功能

a) 标识号：REQ-8.1

b) 说明：实现系统界面与内容的动态多语言切换。

c) 进入条件：用户修改语言偏好或首次访问系统。

d) 输入：

- 用户语言选择（如zh-CN、en-US）

- 翻译资源文件（JSON格式）

e) 输出：

- 本地化渲染的界面元素

- 缺失翻译项的警告日志

f) 处理：

1. 加载对应语言的翻译资源文件。

2. 替换界面组件中的文本占位符。

3. 动态格式化数字/日期（如货币符号、时区）。

4. 记录未翻译词条并通知运维团队。

g) 性能：

- 语言切换响应时间 ≤ 1秒。

- 支持50种语言包并行加载。

h) 约束与限制：

- 翻译文件需符合i18next标准格式。

- 默认语言为英语，缺失翻译项自动回退。

---

##### 自动化测试调度功能

a) 标识号：REQ-9.1

b) 说明：支持定时执行测试用例并生成覆盖率报告。

c) 进入条件：到达预设时间或代码库触发变更事件。

d) 输入：

- 测试用例集（JUnit/TestNG格式）

- 测试环境配置（如DEV/UAT/PROD）

e) 输出：

- 测试结果摘要（通过率/失败详情）

- HTML格式的代码覆盖率报告

f) 处理：

1. 根据优先级排序测试用例执行队列。

2. 动态分配测试资源（如浏览器实例/移动设备）。

3. 使用Jacoco收集代码执行路径。

4. 失败用例自动重试（最多3次）。

g) 性能：

- 1000个测试用例执行时间 ≤ 15分钟。

- 支持10个并发的测试任务执行。

h) 约束与限制：

- 仅支持Java/Python语言的测试框架。

- 单次测试任务最多包含5000个用例。

---

##### 安全漏洞扫描功能

a) 标识号：REQ-10.1

b) 说明：定期扫描代码库与依赖库的已知安全漏洞。

c) 进入条件：代码提交至版本库或手动触发扫描。

d) 输入：

- 代码仓库地址（Git/SVN路径）

- 漏洞数据库（如NVD、CVE列表）

e) 输出：

- 漏洞风险等级报告（CRITICAL/HIGH/MEDIUM/LOW）

- 修复建议文档（含补丁链接）

f) 处理：

1. 克隆代码库至隔离沙箱环境。

2. 解析依赖关系树（如Maven/npm）。

3. 匹配组件版本与CVE数据库条目。

4. 生成风险评分（CVSS 3.0标准）。

g) 性能：

- 100MB代码库扫描时间 ≤ 5分钟。

- 支持每周同步最新漏洞数据库。

h) 约束与限制：

- 仅识别公开披露的漏洞。

- 无法检测逻辑漏洞与业务风险。