目录

[1. 总体设计说明书 1](#_Toc143851484)

[1.1. 系统目标 2](#_Toc143851485)

[1.2. 系统描述 2](#_Toc143851486)

[1.3. 系统上下文 2](#_Toc143851487)

[1.4. 参考资料 2](#_Toc143851488)

[1.5. 系统功能 3](#_Toc143851489)

[1.6. 技术架构 15](#_Toc143851490)

[1.7. 逻辑模型 16](#_Toc143851491)

[1.8. 非功能设计 17](#_Toc143851492)

[1.9. 应用系统设计 20](#_Toc143851493)

# 总体设计说明书

## 系统目标

项目主要目标是开发和维护一套界面软件系统，系统通过python语言实现，可部署于Windows和Linux操作系统。系统可以单独部署、通过浏览器进行访问，最终呈现的是一个小而美的工具型应用。可应用于电能质量的电网数据，对数据进行维护、处理、分析、计算。系统具备部署简单、使用快捷、迁移方便、数据复用、安全性强等特点。

## 系统描述

该项目基于系统预置参数及用户输入电网相关参数进行数据处理，潮流计算，理论模型处理。最终将项目中的数据、通过使用的模型（即算法）进行计算，最终导出所需类型的数据报告。

## 系统上下文

系统功能建设包括四部分内容：

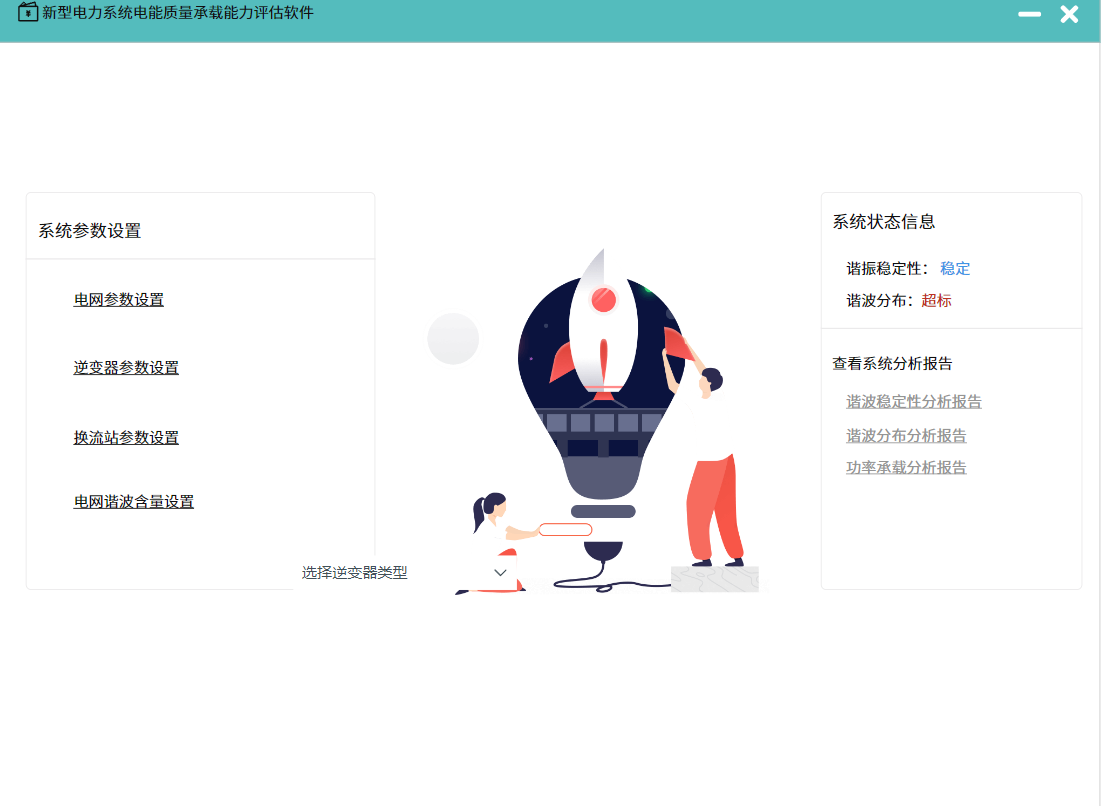
* 第一部分是主页面，包括系统参数设置，系统拓扑结构展示，信息导航卡。
* 第二部分是谐波稳定性分析报告：包含dq阻抗，正负序阻抗，SISO正负序阻抗。
* 第三部分是谐波分析报告：包括节点1，节点2，节点3，节点4的谐波电压和谐波电流。
* 第四部分是功率承载分析报告：包含谐波电压承载，谐波电流承载，稳定性承载。

## 参考资料

|  |  |
| --- | --- |
| **文档名** | **说明** |
|  |  |
|  |  |
|  |  |

## 系统功能

### 主页面



本模块主要实现了系统参数设置、系统拓扑图展示，信息导航卡三个模块。

### 1.5.1.1 系统参数设置

该模块主要用于设置系统参数，包含了：电网参数设置、逆变器参数设置、环流站参数设置、电网谐波含量参数设置。

#### **电网参数设置**

点击链接进行操作

* **输入**



系统电压等级: 必填。

逆变器功率额定值：必填。

换流站功率额定值：必填。

电网强度：必填。

换流站 (标幺值)：必填。

逆变器(标幺值）：必填。

* **重置按钮**

点击重置按钮后讲数据重置为预设值

* **保存按钮**

点击保存按钮，保存当前参数并进行算法计算

* **输出**

保存状态提示

* **处理**

保存数据成功后进行数据计算

#### **逆变器参数**

点击链接进行操作

* **输入**



逆变器直流电压：必填。

滤波电感：必填。

滤波电容：必填。

滤波电感内阻：必填。

连接线路单位电阻：必填。

连接线路单位电感：必填。

连接线路长度：必填。

内环电流控制带宽：必填。

外环有功功率控制带宽：必填。

PLL带宽：必填。

* **重置按钮**

点击重置按钮后讲数据重置为预设值

* **保存按钮**

点击保存按钮，保存当前参数并进行算法计算

* **输出**

保存状态提示

* **处理**

保存成功后进行参数处理

#### **环流站参数设置**

点击链接进行操作

* **输入**



换流站直流电压：必填。

换流站直流侧等效电阻：必填。

换流站直流侧等效电感：必填。

换流站直流侧电容：必填。

滤波电感：必填。

滤波电容：必填。

滤波电感内阻：必填。

PLL带宽：必填。

连接线路单位电阻：必填。

连接线路单位电感：必填。

连接线路长度：必填。

内环电流控制带宽：必填。

外环有功功率控制带宽：必填。

PLL带宽：必填。

* **重置按钮**

点击重置按钮后讲数据重置为预设值

* **保存按钮**

点击保存按钮，保存当前参数并进行算法计算

* **输出**

保存成功提示

* **处理**

数据保存后进行参数处理

#### **电网谐波含量设置**

点击链接进行操作

* **输入**



3次谐波幅值(标幺值)：必填。

5次谐波幅值(标幺值)：必填。

7次谐波幅值(标幺值)：必填。

11次谐波幅值(标幺值)：必填。

* **重置按钮**

点击重置按钮后讲数据重置为预设值

* **保存按钮**

点击保存按钮，保存当前参数并进行算法计算

* **输出**

保存状态提示

* **处理**

保存成功后进行参数处理

### 1.5.1.2 系统信息导航卡

该模块主要展示系统状态信息及系统分析报告跳转链接。

#### **系统状态信息**

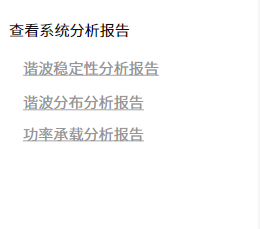
展示当前输入系统参数计算的状态信息

* **输出**



输出展示：谐振稳定性、谐波分布。

#### **查看系统分析报告**



展示三个报告页面跳转链接

* **处理**

谐波稳定性分析报告链接

谐波分布报告链接

功率承载分析报告链接

### 1.5.1.3 谐波稳定性分析报告

模块用于展示通过数据处理计算获取到的谐波稳定性分析报告数据。

#### **风力**

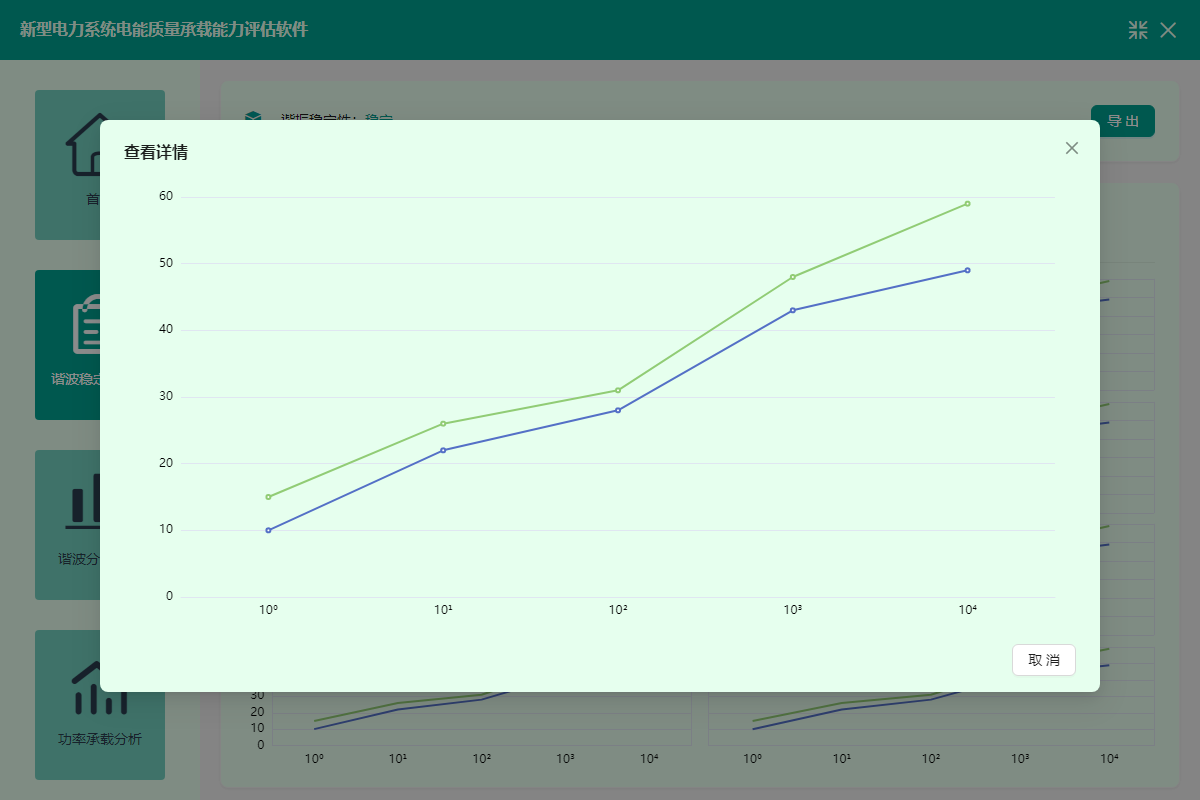
展示风力计算的dq阻抗、正负序阻抗、SISO正负序阻抗报告信息

* **输出**



* **处理**

点击图形内容可查看详情，放大展示图标详细信息



#### **直流**

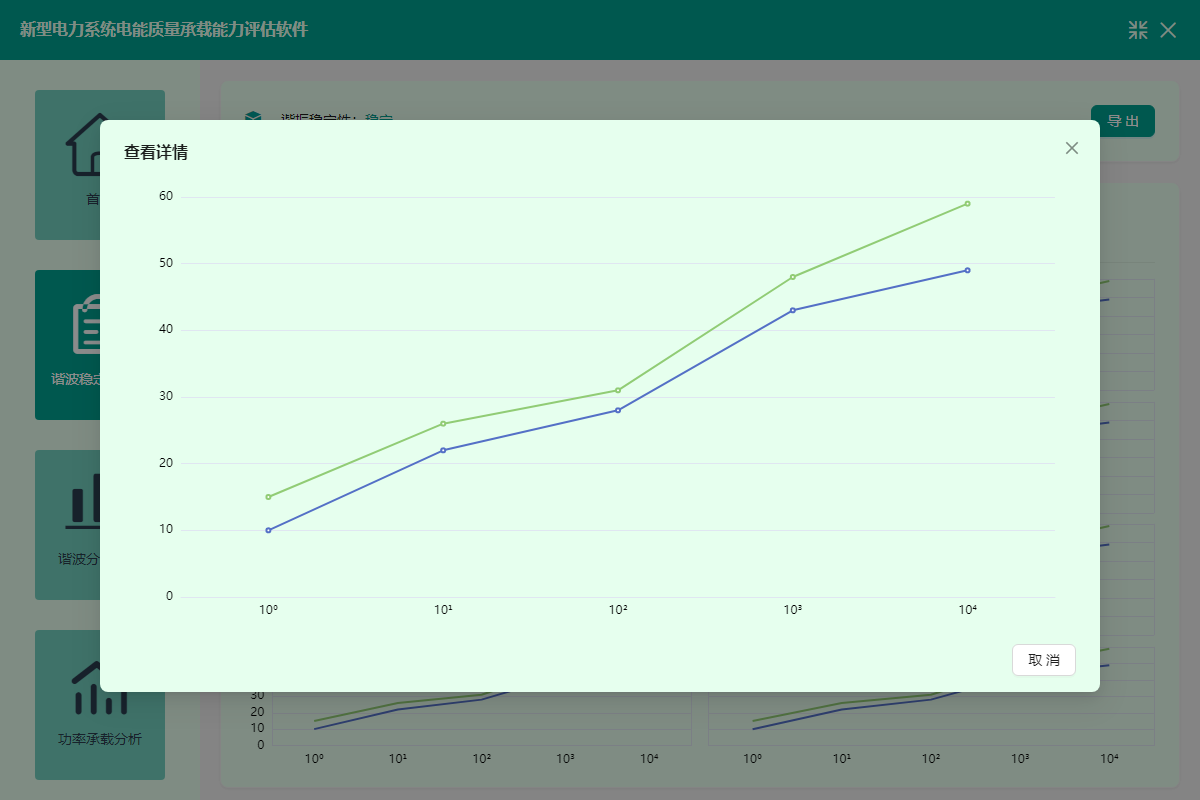
展示直流计算的dq阻抗、正负序阻抗、SISO正负序阻抗报告信息

* **输出**



* **处理**

点击图形内容可查看详情，放大展示图标详细信息



#### **交流**

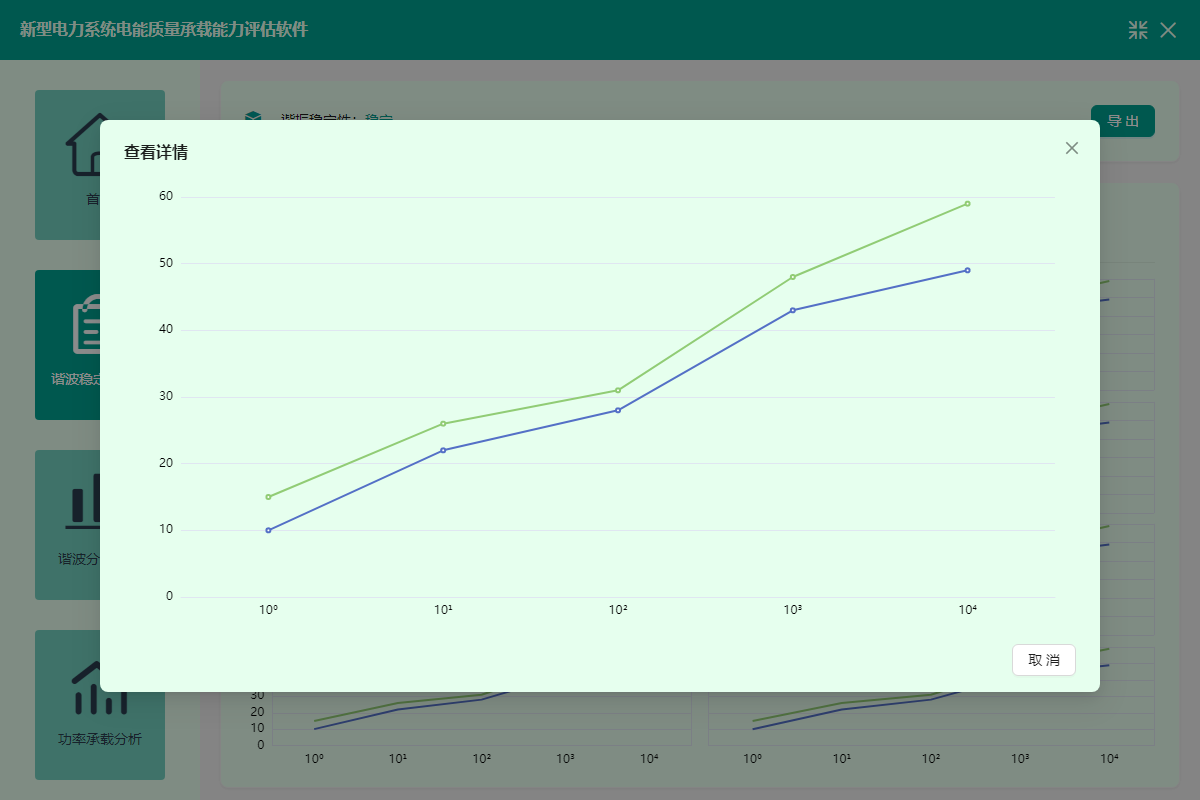
展示交流计算的dq阻抗、正负序阻抗、SISO正负序阻抗报告信息

* **输出**



* **处理**

点击图形内容可查看详情，放大展示图标详细信息



### 1.4.1.4 谐波分布分析报告

模块用于展示通过数据处理计算获取到的谐波分布分析报告数据。

* **输出**

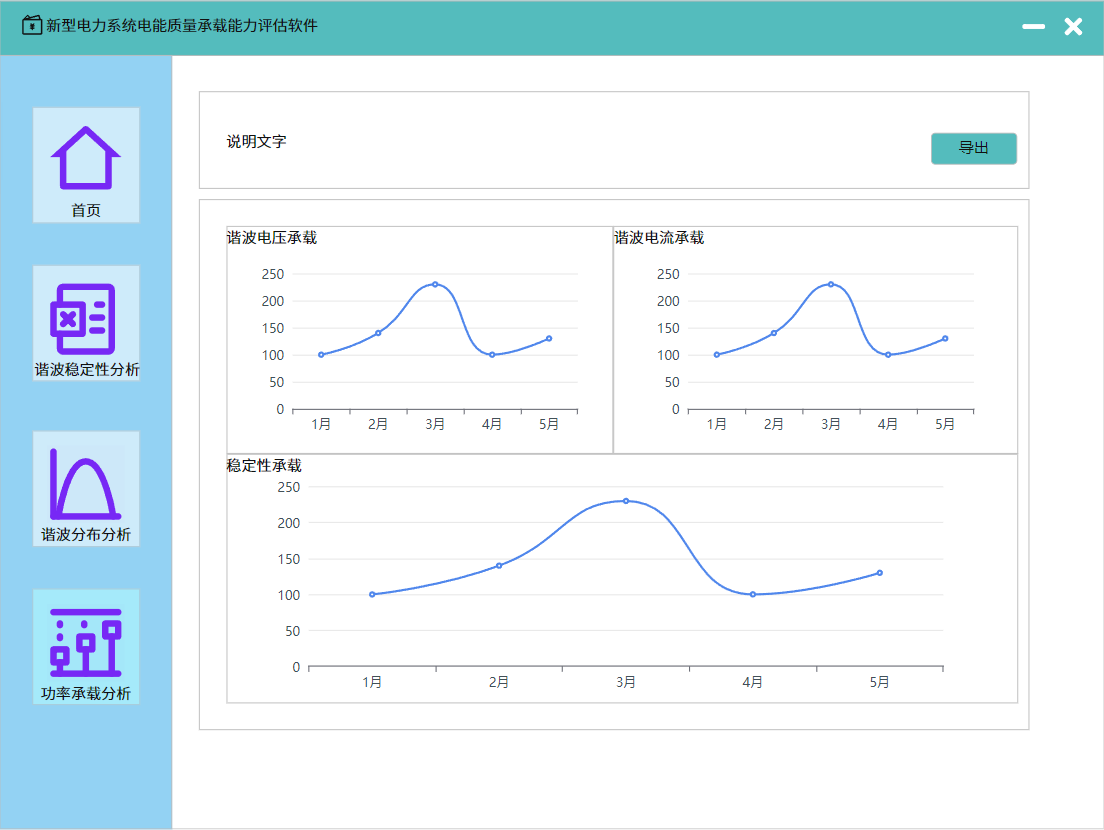


分为节点1、节点2、节点3分别展示谐波电压、谐波电流报告内容

### 1.4.1.5 承载功率分析报告

模块用于展示通过数据处理计算获取到的承载功率分析报告数据。

* **输出**



分为谐波电压承载、谐波电流承载、稳定性承载报告内容

## 技术架构

### 微服务

微服务是一项在云中部署应用和服务的新技术。微服务可以在“自己的程序”中运行，并通过“轻量级设备与HTTP型API进行沟通”。关键在于该服务可以在自己的程序中运行。通过这一点就可以将服务公开与微服务架构（在现有系统中分布一个API）区分开来。在服务公开中，许多服务都可以被内部独立进程所限制。如果其中任何一个服务需要增加某种功能，那么就必须缩小进程范围。在微服务架构中，只需要在特定的某种服务中增加所需功能，而不影响整体进程。

微服务的基本思想在于考虑围绕着业务领域组件来创建应用，这些就应用可独立地进行开发、管理和加速。在分散的组件中使用微服务云架构和平台使部署、管理和服务功能交付变得更加简单。

### Node.js

Node.js（下面简称Node）是一个可以快速构建网络服务及应用的平台。Node非常强大的功能在于其能够在服务器端上运行Javascript。手机浏览器环境限制了开发人员选择编程语言的自由，任何服务器与日益复杂的浏览器客户端应用程序间共享代码的愿望只能通过Javascript来实现。因此，Node发展迅猛并逐渐成为事实上的常用平台。

Node作为一个新兴的后台语言，有很多吸引人的地方，包括具备RESTful API和单线程特性。Node可以在不新增额外线程的情况下，仍然可以对任务进行并行处理。Node是单线程的，通过事件轮询来实现并行操作，充分利用这一点，可以尽可能的避免阻塞操作，取而代之，多使用非阻塞操作。另外，Node还具有非阻塞IO、V8虚拟机、事件驱动等特点，这也是Node的优势。

## 逻辑模型

#### 用户交互层

用户交互层关注用户与系统人机交互，业务界面展现。用户交互层并非SOA约束和规范的范畴，没有直接的标准和规范，但和用户易用性息息相关。用户交互层按照多岗位、多功能应用的模型，支撑平台根据岗位定制个性化功能交互。用户交互层更多是从技术上要求满足用户业务处理界面展现要求，包括对不同终端设备，操作系统，语言环境，网络环境的客户端支持。

#### 业务功能层

业务功能层关注业务活动分解，服务组装，流程编排，满足业务流程管理、设计、实现技术的各个方面要求。业务功能编排着重于业务功能逻辑内部实现，是一个可展现的业务功能点内对下层所提供的业务服务访问（调用）和组织，编排的主体是业务服务，依据是业务功能逻辑。业务流程配置着重于业务流程管理方面的实现，是业务功能之间按照业务规则进行编排，编排的主体是业务功能点，依据是业务管理流程。

#### 服务接入层

服务接入层负责服务的接入控制、服务路由和协议适配。保证系统对接入流量的控制，对服务负载均衡。在大并发情况下的稳定性。对系统内部服务调用接入层采用私有基于TCP/IP的高效协议，对外部应用及B/S应用则可通过协议适配转换成HTTP/HTTPS协议。对于在大规模系统服务需要考虑服务接入方式，提供多点接入，保证无单点故障点以及达到主动负载均衡的能力。

#### 服务实现层

服务实现层以服务的的形式对外提供业务功能的访问，必要时也可以多个服务编排组合成一个服务。服务对业务提供了各种粒度的支持，满足企业不同规模应用要求。

#### 系统资源层

系统资源层表示支撑组件层的可操作的系统资源，包括数据库、存储、各类操作系统资源如设备驱动，其他软件包、开发库，遗留的系统（需要在内部资源集成）等。电网管理平台选用大型关系型分布式数据库，具有较高的容错能力和恢复能力，提供较强的安全机制，以实现对个人电网管理平台数据的规范管理。

#### 信息集成

针对业务数据，为了保证数据交互的规范性、最大限度的降低对原有业务的改造，并且保证电网管理平台的稳定性和可靠性，电网管理平台主要通过RESTfull接口获取相关的业务数据；针对技术数据，采用数据中心进行抽取、清洗、加工、转换和存储来实现基础业务数据的集成；针对原有业务系统中已经实现的界面，同时为了实现页面的最大复用率，主要采取使用原有系统界面及UI元素适配的方式进行页面集成。

## 非功能设计

### 安全性

IT服务台优化项目参照安全级别为A级的要求进行项目安全管理，系统的安全需求根据信息安全管理体系文件《TP-ISR-066 信息系统安全控制表》中第1项控制点“安全需求与评审”的要求执行，具体措施如下：

* 保护敏感信息的加密存储和传输
* 使用复杂度高的加密算法
* 保护输入输出数据的安全性
* 保护数据库操作的安全性
* 对系统口令及登录安全做控制
* 对系统的权限进行分配与控制
* 配置统一的出错页面
* 保护文件操作的安全性
* 保护用户会话的安全性

### 可用性

* 系统支持 7×24 小时的正常运行及服务接口，整体可靠性应达到 99.99％以上。
* 针对不同的故障类型（硬件故障/网络故障/程序故障）具备快速解决的方案，相关的指标如下：

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 描述 | 指标 | 目标 |
| 非计划停机时间 | 系统故障导致的不可用时间比例 | 每年小于时间比例 | 1% |
| 故障次数 | 预期的使得服务失效的故障频率。 | 最大可承受故障数量/时间周期 | 12次/年 |
| 一般故障的恢复能力 | 在故障发生后需要多久服务才能恢复正常 | 恢复系统到正常运营状态所需的时间 | 1小时 |
| 严重故障的恢复能力 | 在故障发生后需要多久服务才能恢复正常 | 恢复系统到正常运营状态所需的时间 | 4小时 |

### 性能需求

* 响应时间：

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 描述 | 指标 | 目标 |
| 接口响应时间 | 系统调用接口必须满足的响应时间要求 | 最大值控制 | 响应时间: 不超过**5**秒  极端情况下响应实际不超过**20**秒 |

* 吞吐量：

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 描述 | 指标 | 目标 |
| 接口访问处理能力 | 系统在访问高峰期处理具备下述点击处理能力： | 最小值控制 | 接口访问次数/秒: 200 |

### 可伸缩性

平台基于微服务体系架构，平台业务解耦成一系列可以独立部署的微应用和微服务。这些微应用和微服务都打包成容器镜像，运行在南网云提供的容器化微服务环境中，能够充分发挥容器云平台的优势，实现应用的高可用的弹性伸缩，在提高业务稳定性的同时，提高了系统硬件的利用率。

无论是微应用还是微服务，都是在容器环境中以分组的方式提供集群服务，不存在单点问题。微服务在启动时完成向注册中心的自动注册，云平台维持着可提供服务的节点的实时信息。这种轻量级、自管理的体系架构使应用的动态伸缩成为可能，服务网关和服务消费者能够实时感知节点的变化，进而修改调用过程中的负载均衡策略，配合云平台提供的灰度升级技术，极大提升了平台的高可用。

针对平台微服务的每个部署单元，都可以定制弹性伸缩规则，可以基于CPU利用率、内存利用率、请求的QPS、平均响应时间等动态指标指定容器实例的伸缩规则。针对接入应用、设备管理、应用管理、内外中转等服务，就可以利用这种特性在业务高发期增加微服务运行实例，在业务低谷期适当缩减服务实例，从而达到服务供需平衡，不仅提升了业务能力，也在整体上降低了硬件的开销。

### 可扩展性

服务之间各司其责，层次松耦合，当新业务模块上线时，通过微服务向注册中心自动注册，无须停机部署，保障平台的快速扩展业务模块，增强平台的稳定性，提升平台的拓展性

## 应用系统设计

### 包命名规范

系统的包命名规范必须遵循中心的标准规范，要求：

* 包命名格式需为com.<公司缩写>.<项目名称>.<模块名称>.[代码类型]。
* 公司缩写为太平保险集团内各子公司英文缩写。如不对应任何公司，则命名为common。如：

com.cntaiping.project1.module1.WxBiz。

* 包命名中的项目名称，模块名称，代码类型，由各项目组自行指定。建议项目名称，模块名称是必须包含的命名内容，代码类型是可选的命名内容。

### 数据库编码规范

* 数据库需使用UTF-8字符集编码。
* PL/SQL以及脚本程序需遵守《PL/SQL编程规范》。

### 参数配置

* 数据源的配置在Spring的配置文件中，设置weglogic中设置的数据源的JNDI。
* 系统的需要持久化和需要临时变更的参数，按需要在properties中设置，或者系统表中持久化在项目启动时读取或者项目运行中再次获取刷新等。对配置信息需要逐台刷新反馈刷新信息等。

### 日志

应用日志包括文件日志，应用操作日志和数据批量日志：

* 文件日志
* 记录应用运行时的提示信息  
  包括出错代码，供代码调试和运行监控使用。通过log4j框架实现，日志门面库采用slf4j，可以通过修改log4j配置文件来调整输出日志的粒度（DEBUG/INFO/WARN/ERROR）和输出格式。
* 操作日志  
  对重要的业务操作进行记录以便于事后审计。定义的数据项包括：
  + 操作时间

包括开始时间和结束时间

* + 操作用户(来源IP)
  + 操作接口及输入参数
  + 操作结果

包括结果状态和异常情况。，如果异常，实时接口还会记录实时接口响应对象。

* 接口日志  
  对重要的外部接口调用进行日志记录，对错误的接口调用进行日志记录，便于查找、分析处理问题。定义的数据项包括：
  + 请求处理时间

包括请求时间和响应时间

* + 处理服务器IP
  + 请求报文、响应报文
  + 调用结果

### 第三方公共组件

|  |  |  |
| --- | --- | --- |
| **包名称** | **版本** | **组织** |
| **Log4j** | 1.2.16 | Apache |
| **Slf4j** | 1.6.1 | Qos.ch |

### 安全设计

对系统功能权限访问进行控制

敏感数据采用MD5+SALT（散列加密）进行保护处理或者SHA-2加密处理

调用外部微信接口，遵循腾讯接口规范进行https协议访问，AES加解密。

用户统一登录等才用接入统一认证平台系统进行账号权限处理等。

其他详细等总体的安全要求参照A级系统进行加强处理：

* 敏感信息加密存储和传输
* 系统采取相应的控制手段检测和保护用户数据、管理数据、鉴别信息以及系统重要业务数据在传输和存储过程中的完整性和保密性；
* 系统重要数据加密存储：对系统中的重要数据进行加密存放，确保除合法持有密钥者外，其余任何用户不能获得该数据，数据内容包括但不限于用户口令/密钥、系统密钥以及其它需要保密的敏感业务数据；
* 采用使用密钥的密码机制对重要存储数据完整性进行保护，检测或预防数据单元跳变、恶意破坏（修改、删除等）等数据完整性错误，如：计算MAC和数字签名；
* 对传输的**所有数据**采用**数字信封和端到端的数据加密方式**。针对互联网应用系统，应使用SSL进行传输加密。
* 加密算法管理

禁止使用纯MD5和SHA-1加密，建议使用如下算法：AES（对称加密），ECC和RSA（非对称加密），SHA-224和MD5+SALT（散列加密）。

* 输入输出数据的安全性

对输入数据进行验证，如数据长度、类型、范围等；对输入数据中特殊字符进行过滤；对输出数据中的特殊字符进行编码；

* 数据库操作的安全性

禁止使用动态组装的SQL语句，应使用预编译的SQL语句或者存储过程；

* 系统口令及登录安全控制

鉴别机制

* 主机系统、应用系统以及数据库系统等应提供专用的登录控制模块对登录用户进行身份鉴别，用户身份标识应唯一，且不具有被冒用的特点；
* 应启用登录失败处理功能，采取结束会话、帐户锁定、限制非法登录次数和自动退出等措施；
* 口令输入错误或登录失败3次账号强制锁定，联系管理员解锁，特殊情况（如：外网系统），用户账号被锁定后可以通过重置口令解锁账户；重置口令解锁时系统通过发送重置口令的链接供用户重置口令，系统如无法提供此方式重置口令时可考虑使用其他方式；
* 设置鉴别警示信息，提醒未授权访问可能导致的后果以及承担的责任；
* 采用**两种以上组合**的鉴别技术对管理用户进行身份鉴别，且身份鉴别信息至少有一种是难以伪造的；
* 用户认证通过后，如果在10分钟内无操作，用户需要进行确认性重认证。
* 如果账户3个月内没有登录系统，自动锁定账户,联系管理员解锁，特殊情况可采用用户自助解锁的方式。

口令安全

* 账号/口令信息的传输和存储采用密文方式；
* 口令应有一定的复杂度要求并按照规定定期更换；
* **长度不低于12位**，口令中同时包含大小写字母、数字和特殊符号等四项中的至少三项，特殊情况除外，如系统客观条件限制只能输入8位以下口令或者只能输入数字；
* 口定更改周期不超过三个月；
* 使用以前用过的相同密码的周期应至少**相隔六代**；
* 系统用户口令过期应能够自动提示；
* 用户输入口令字时不许回显；
* 系统具有“首次登陆提醒用户更改默认口令”功能。

资源控制

* 信息系统主机操作系统通过设定终端接入方式、网络地址范围等条件限制终端登录；
* 设置登陆终端的会话超时中断策略。
* 会话超时10分钟后自动退出，释放资源，如因特殊业务场景需要，须经相关责任人批准后可适当延长会话时间；4、系统提供服务优先级设定功能，并在安装后根据安全策略设定访问帐户或请求进程的优先级，根据优先级分配系统资源。
* 限制单个用户对系统资源的最大使用限度，明确一个访问帐户或一个请求进程占用的资源分配最大和最小限额，如：处理器、磁盘空间、内存、传输带宽等；
* 对系统的最大并发会话连接数进行限制；
* 对单个帐户的多重并发会话进行限制；
* 对系统的服务水平降低到预先规定的最小值时进行检测和报警。
* 权限的分配与控制
* 信息系统网络、主机和应用系统应具备访问控制配置与管理功能，依据安全策略控制用户对资源的访问，权限的分配遵循最小化原则；
* 系统配置文件中不能包含明文用户名和密码等敏感信息；
* 信息系统访问控制的覆盖范围应包括访问者、访问对象及它们之间的操作行为。
* 系统能根据角色分配权限，实现管理和应用帐户的分离，实现主机操作系统和数据库管理系统特权用户的权限分离；
* 信息系统禁用与业务或管理无关的默认账户；
* 应用系统严格控制用户对系统文件和数据库等重要客体的访问（可采用重要数据加密的方式，只有拥有密钥的用户才能解密访问）；
* 限制应用管理的IP地址范围；
* 信息系统任意帐号的访问权限不能覆盖权限全集,多角色帐号间权限互相制约，如:一个帐号不能同时具有审计员和管理员两种角色；
* 基于权限管理基础设施（PMI），实现权限和证书的产生、管理、存储、分发和撤销等功能。PMI能够与PKI和目录服务紧密地集成，并系统地建立起对认可用户的特定授权，对权限管理进行了系统的定义和描述，完整地提供了授权服务所需过程。
* 配置统一的出错页面

统一配置出错跳转页面，避免系统配置信息暴露在出错页面中；

* 文件操作的安全性

固定文件上传路径，对文件名以及文件类型做白名单验证或编码；

* 用户会话的安全性

使用Token机制保证会话的安全性。

* 第三方产品（框架）的使用

应使用第三方产品（框架）的安全稳定版本，避免使用存在重大安全漏洞的产品版本，已知重大安全漏洞产品清单请参考《重大信息安全漏洞产品清单》。

* 应用服务器访问数据库设计要求

针对互联网应用系统，应避免应用服务器直接访问内网数据库，建议在内网增加应用服务器作为服务端，供外网应用服务器远程调用。