**中国南方电网有限责任公司**

**资产管理项目**

**技术投标文件**

**（正本）**

**(采购编号：xxx)**

**报 价 人： xxxxxx有限公司**

**采购服务机构：中国南方电网有限责任公司招标服务中心**

**2017年5月**

目录

[1 前言 6](#_Toc417600239)

[1.1 项目背景 6](#_Toc417600240)

[1.2 参考资料 6](#_Toc417600241)

[2 需求分析 6](#_Toc417600242)

[2.1 系统应用需求 6](#_Toc417600243)

[2.1.1 建立评价管理 6](#_Toc417600244)

[2.1.2 建立供应商评价 6](#_Toc417600245)

[2.1.3 建立评价查询 6](#_Toc417600246)

[2.1.4 建立系统管理 7](#_Toc417600247)

[2.1.5 建立数据安全管理 7](#_Toc417600248)

[2.1.6 建立接口模块 7](#_Toc417600249)

[2.2 架构模式需求 7](#_Toc417600250)

[2.2.1 数据集成要求 7](#_Toc417600251)

[2.2.2 流程集成要求 7](#_Toc417600252)

[2.2.3 安全性要求 8](#_Toc417600253)

[2.3 系统管理技术需求 8](#_Toc417600254)

[2.3.1 权限管理要求 8](#_Toc417600255)

[2.3.2 操作日志管理要求 8](#_Toc417600256)

[2.3.3 软件版本管理要求 9](#_Toc417600257)

[2.3.4 备份管理要求 9](#_Toc417600258)

[2.3.5 系统接口要求 9](#_Toc417600259)

[2.4 其他需求 10](#_Toc417600260)

[2.4.1 实施要求 10](#_Toc417600261)

[2.4.2 验收要求 10](#_Toc417600262)

[2.4.3 性能要求 10](#_Toc417600263)

[3 建设原则 11](#_Toc417600264)

[4 建设目标与思路 12](#_Toc417600265)

[4.1 建设目标 12](#_Toc417600266)

[4.2 设计思路 12](#_Toc417600267)

[4.2.1 评价管理 12](#_Toc417600268)

[4.2.2 供应商评价 12](#_Toc417600269)

[4.2.3 评价查询 13](#_Toc417600270)

[4.2.4 系统管理 13](#_Toc417600271)

[5 系统总体设计 14](#_Toc417600272)

[5.1 系统总体结构 14](#_Toc417600273)

[5.2 可视化管理中心 15](#_Toc417600274)

[5.2.1 总体流程 16](#_Toc417600275)

[5.2.2 评价管理 16](#_Toc417600276)

[5.2.3 供应商评价 19](#_Toc417600277)

[5.2.4 评估查询 23](#_Toc417600278)

[5.2.5 系统管理 25](#_Toc417600279)

[5.2.6 系统权限控制 26](#_Toc417600280)

[5.2.7 接口模块 27](#_Toc417600281)

[5.3 网络部署设计 28](#_Toc417600282)

[5.4 应用体系架构设计 28](#_Toc417600283)

[5.4.1 均采用.NET技术框架 28](#_Toc417600284)

[5.4.2 多层应用体系架构设计 29](#_Toc417600285)

[5.4.3 SOA与OOAD相结合的分析与设计 33](#_Toc417600286)

[5.4.4 采用XML格式数据传输 35](#_Toc417600287)

[5.5 硬件环境要求 38](#_Toc417600288)

[5.6 软件环境要求 38](#_Toc417600289)

[5.7 接口技术方案 38](#_Toc417600290)

[5.7.1 与物资管理系统的接口方案 38](#_Toc417600291)

[5.7.2 采用WEB Service实现数据共享 39](#_Toc417600292)

[5.7.3 遵循XML数据交换规范 40](#_Toc417600293)

[5.7.4 消息队列保证消息的传递 40](#_Toc417600294)

[5.7.5 业务系统数据交换模块设计 41](#_Toc417600295)

[6 系统安全体系设计建议 42](#_Toc417600296)

[6.1 系统安全目标、策略与建设原则 42](#_Toc417600297)

[6.1.1 系统的安全目标 42](#_Toc417600298)

[6.1.2 系统的安全策略 43](#_Toc417600299)

[6.1.3 系统安全建设的原则 43](#_Toc417600300)

[6.2 系统安全体系概述 43](#_Toc417600301)

[6.2.1 基本安全防护系统 45](#_Toc417600302)

[6.3 建立完善的安全体系结构 45](#_Toc417600303)

[6.3.1 安全服务 45](#_Toc417600304)

[6.3.2 对等实体鉴别服务 45](#_Toc417600305)

[6.3.3 访问控制服务 46](#_Toc417600306)

[6.3.4 数据保密服务 46](#_Toc417600307)

[6.3.5 安全机制 47](#_Toc417600308)

[6.4 访问控制规则管理 49](#_Toc417600309)

[6.5 表格内容安全 49](#_Toc417600310)

[6.6 数据安全规则管理 50](#_Toc417600311)

[6.7 数据库系统的安全措施 50](#_Toc417600312)

[6.7.1 数据库系统安全与保密的特点 50](#_Toc417600313)

[6.7.2 数据库系统的安全措施 51](#_Toc417600314)

[6.8 安全管理 52](#_Toc417600315)

[7 项目管理与质量控制方案 53](#_Toc417600316)

[7.1 项目管理 53](#_Toc417600317)

[7.1.1 项目组织与人员承诺 53](#_Toc417600318)

[7.1.2 项目组织架构 53](#_Toc417600319)

[7.1.3 项目管理规范 56](#_Toc417600320)

[7.1.4 项目风险控制 58](#_Toc417600321)

[7.1.5 项目文档管理及承诺 59](#_Toc417600322)

[7.2 质量控制 59](#_Toc417600323)

[7.2.1 质量保证目的 59](#_Toc417600324)

[7.2.2 质量保证工作 60](#_Toc417600325)

[7.2.3 过程控制 61](#_Toc417600326)

[8 验收标准和实施方案 66](#_Toc417600327)

[8.1 验收标准 66](#_Toc417600328)

[8.1.1 验收承诺 66](#_Toc417600329)

[8.1.2 验收的阶段 67](#_Toc417600330)

[8.1.3 提交文档的清单 67](#_Toc417600331)

[8.2 实施方案 67](#_Toc417600332)

[8.2.1 实施承诺 68](#_Toc417600333)

[8.2.2 项目实施管理措施 68](#_Toc417600334)

[8.2.3 项目实施方案 68](#_Toc417600335)

[9 整体项目工期计划 70](#_Toc417600336)

# 前言

## 项目背景

针对南方电网一类物资的供应商履约评价管理的要求，系统提供对供应商的质量、服务的地市评分、省公司核对扣分，网公司最终汇总，然后根据评分系数及供应商的供货量进行最终的评分调整，建立统一的数据上报平台，为开展全网的针对一类物资供应商的履约评价服务；

## 参考资料

《**物资供应商履约评价项目-招标文件.doc》**

# 需求分析

## 系统应用需求

### PC管理端功能

以《XXXX-招标文件》为基础，依照中国南方电网责任有限公司的资产管理要求，构建PC管理端功能，提供组织管理、用户管理、系统管理、操作日志、物资管理等功能。

### PAD移动终端功能

以《XXXX-招标文件》为基础，依照中国南方电网责任有限公司的资产管理要求，构建PAD移动终端使用RFID功能，提供用户登录、登出、物资借入、物质归还等功能。

### 微信端功能

以《XXXX-招标文件》为基础，依照中国南方电网责任有限公司的资产管理要求，构建提供微信查询物资功能、用户绑定、微信通知等功能。

### 建立API服务

以《XXXX-招标文件》为基础，依照中国南方电网责任有限公司的资产管理要求，构建服务器数据与应用端（PC、PAD、微信端）数据交互功能模块，包括用户验证、用户权限控制。

## 架构模式需求

### 数据集成要求

新建业务系统应建立面向业务的信息模型，可以使用UML工具进行建模，应支持将信息模型转换为XML的描述。

新建业务系统与系统外需要交换的数据可以通过JSON格式进行数据交换。

### 安全性要求

新建业务系统应建立作为统一的身份管理系统，每次物资借入、归还的用户信息必须是唯一，并且对应的权限可以在管理端进行控制。

新建业务系统应在用户在物资借入、归还的流程中建立日志记录机制，提供管理员对操作人员的操作的查询功能。

## 系统管理技术需求

### 权限管理要求

1. 对组织结构、职务、权限应具备相应的管理功能，实现权限控制。
2. 按照组织结构的职务对用户进行授权。
3. 采用统一的管理方式，提供系统管理员对职务权限的分配。
4. 权限设置必须由被授权的系统管理员完成，管理员不能设置大于自身权限的权限。

### 操作日志管理要求

1. 系统对用户的每次操作都进行详细记录日志，并提供统计查询功能。
2. 系统可查询、统计、导出所有或单个操作日志内容，提供用户的各种操作统计报表。

### 软件版本管理要求

1. 本工程中必须具备其详细的软件版本信息，包括软件版本号、软件启用时间、测试时间等；
2. 应用系统应在登录界面上显示系统软件名称及软件版本号等信息；
3. 软件版本号可分为主版本号、次版本号、补丁号；
4. 版本号的修改应根据软件修改内容范畴而做相应的修改；
5. 应用系统能自动判断新的软件版本并支持自动或手工下载新软件；

### 备份管理要求

1. 数据备份设备要求有良好的安全性、可靠性；
2. 数据备份设备可与多种厂家的主机系统相连；
3. 数据备份设备应具有一定的平滑扩充能力，包括系统设备容量的扩充及I/O能力的扩充等；
4. 数据备份应包含必要的系统软件，支持同步和异步方式，提供方便快捷的数据同步和恢复手段，提供运行情况监控，并严格保证数据的一致性；

### 系统接口要求

系统的接入平台应满足下列基本要求：

1. **可伸缩性：**保证在充分利用系统资源的前提下，实现系统平滑的移植和扩展，同时在系统并发增加时提供系统资源的动态扩展，以保证系统的稳定性；
2. **可靠性：**应防止非系统级的数据丢失或出错，同时提供对系统级的数据丢失和出错实现恢复和容错的机制；
3. **可扩展性：**在进行扩容、新业务扩展和系统接口连接中，提供快速、方便和准确的实现方式；
4. **健壮性：**提供可靠的运行环境，保证系统在内部、外部的不可预知的出错情况下，能够提供正确的处理机制；
5. **安全性：**提供完善的信息安全机制，以实现对信息的全面保护，保证系统的正常运行；
6. **可管理性：**提供良好的系统管理机制，保证可在系统的运行过程中提供给管理员方便的管理方式，以处理各种情况。

## 其他需求

### 实施要求

中标方需根据本技术招标书的要求结合自身在开发电力行业应用的实践和项目经验，认真实施此次招标的目标应用系统。从项目的角度，中标方应根据本章的要求，对拟投入本项目设计、开发的组织结构做出安排，主要包括两个方面：

其一、中标方应根据本项目的特点，对拟投入本项目的人员情况进行说明，提供参与本项目的主要人员，同时需详细说明此项目组成员在设计、开发本应用系统所承担的职责和所具有的优势，从系统开发的人员方面确保项目的正常进行。

其二、根据系统开发所需要经历的各个阶段，对项目的安排做出详细的计划，并严格执行，确保供应商履约评价服务项目如期保质完成

中标方可据此要求在投标时就对项目的安排做出详细的计划，评标时将作为考察中标方在系统开发方面所具备的实力的重点内容。

### 验收要求

必须在合同签订后90个工作日内完成开发、实施并试运行，试运行3个月后组织验收，试运行验收后进入质保期，质保期为12个月。

### 性能要求

局域网内操作响应时间不超过10秒；简单的统计分析响应时间不超过20秒；复杂的统计分析根据具体情况而定；广域网以及城域网内操作响应时间不超过30秒；简单统计分析响应时间不超过30秒；复杂的统计分析根据具体情况而定；投标方要对系统的系统软硬件处理能力提出相应要求。

# 建设原则

1. **开放性：**支持多种硬件平台，采用通用软件开发平台开发，具备良好的可移植性。采用标准开放接口，支持与其它系统的数据交换和共享。
2. **标准化：**所有各项软件开发工具和系统开发平台应符合我国国家标准、信息产业部部颁标准、电力行业相关技术规范和要求。
3. **容错性：**提供有效的故障诊断及维护工具，具备数据错误记录和错误预警能力；具备较高的容错能力，在出错时具备自动恢复功能。
4. **安全性：**用户认证、授权和访问控制，支持数据库存储加密，数据交换的信息包加密，数据传输通道加密，可采用64位DES加密算法。发生安全事件时，能以事件触发的方式通知系统管理员处理。
5. **可靠性：**应能够连续7×24小时不间断工作，平均无无故障时间>8760小时，出现故障应能及时告警，软件系统应具备自动或手动恢复措施，自动恢复时间<15分钟，手工恢复时间<12小时，以便在发生错误时能够快速地恢复正常运行。软件系统要防止消耗过多的系统资源而使系统崩，系统支持双机热备运行，支持负载均衡并可以扩展。部分重要模块具有自检功能，能监视各功能模块的运行情况，随时发现系统自身的问题。
6. **兼容性：**满足向下兼容的要求，软件版本易于升级，任何一个模块的维护和更新以及新模块的追加都不应影响其他模块，且在升级的过程中不影响系统的性能与运行。
7. **易用性：**应具有良好的简体中文操作界面、详细的帮助信息，系统参数的维护与管理通过操作界面完成。
8. **可维护性：**当提交完整的产品时，必须提交易于安装的标准安装程序 (如主要软件包都放置于光盘)、相关接口规范和收集非标准的日志信息的开发规范。提供必要的操作维护手册及技术手册、口令管理手册、监控使用手册、配置管理文档、不同采集引擎安装手册、相关开发接口文件、应急预案。提供必要的培训。当进行版本升级时，提供版本差异的详细说明。

# 建设目标与思路

## 建设目标

1. 本期建设重点是对物资对应有序的管理，可对物资进行溯源。
2. 本期的建设内容主要有：
   1. PC端管理功能；
   2. PAD端使用功能；
   3. 微信通知功能；
   4. 接口服务建设
3. 通过本期建设的功能，能对物资进行一一跟踪处理。

## 设计思路

### PC管理功能

* 组织架构：按照公司的组织架构进行权限的管理设置，以－部们－职务－人员的方式，对职务进行权限设置，以达到用户权限的控制。
* 用户管理：单独对此系统用户进行管理。
* 物资管理：对物资的建立、修改、盘点、溯源等功能。

### PAD端功能

* 用户登录：用户可以使用用户名、读取RFID，结合密码的方式进行登录。
* 物资借入：借入用户登录后，可以使用物资借入功能，使用RFID读取物资并显示信息。
* 物资归返：已借入用户可以使用物资归还功能，使用REID读取归还物质，非借出物资不能归还。

### 微信端功能

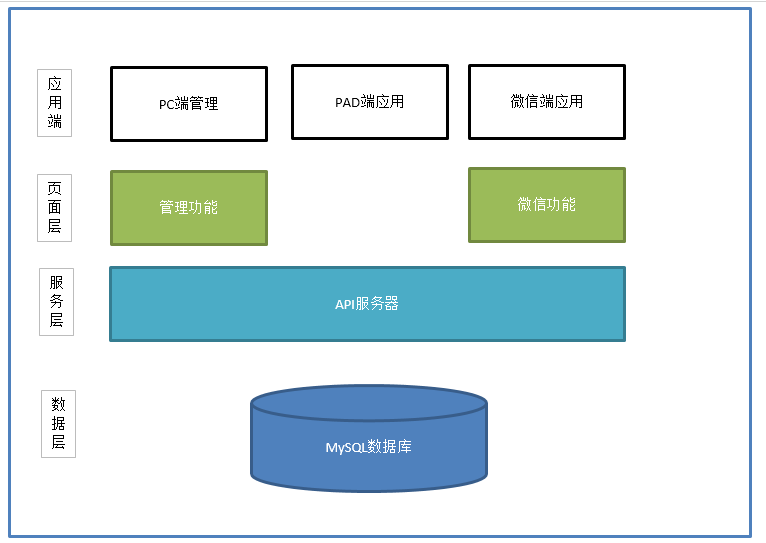
* 物资借入、借出通知：当物资借入时，通知绑定的管理员，当物资归还时，通过绑定的管理员；
* 物资查询：可以查询物资的历史记录情况；

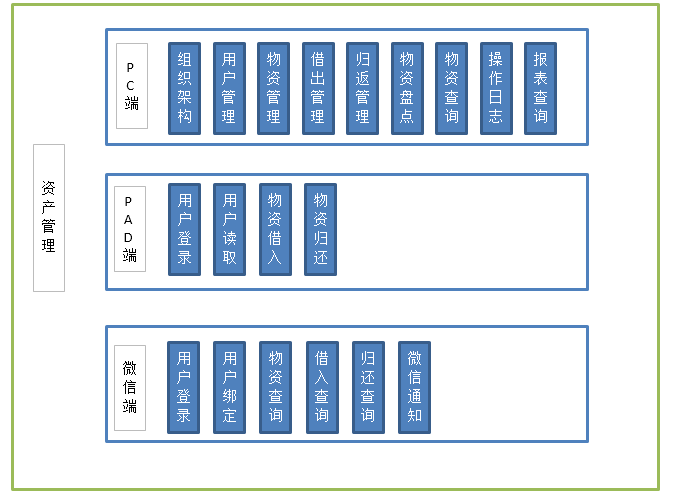
### 系统管理

* 组织、权限、用户管理：按照组织架构，对职务进行权限设置，以及管理用户人员。
* 物资管理功能：对物资资料进行维护以及查询物资使用情况。
* 系统日志记录策略：记录用户的日常操作记录。

# 系统总体设计

## 系统总体结构





**参与者说明**：

| *参与者* | *描述* |
| --- | --- |
| 物资管理员 | PC端功能，微信功能； |
| 物资使用员 | PAD端功能，微信功能； |

## 可视化管理中心

物资管理系统主要有PC端子系统、PAD端子系统、微信服务子系统组成。其中各个系统的子功能模块，如下表：

|  |  |  |
| --- | --- | --- |
| **系统名称** | **系统子模块** | **功能描述** |
| PC端 | 组织架构 | 设置系统公司架构、职务、职务权限、人员管理 |
| 用户管理 | 管理系统使用用户 |
| 物资管理 | 管理物资：增加、修改物资资料 |
| 借出管理 | 物资借出管理功能 |
| 归还管理 | 物资归还管理功能 |
| 物资盘点 | 物资盘点业务 |
| 物资查询 | 物资查询业务 |
| 操作日志 | 系统使用用户操作日志 |
| 报表查询 | 查询物资报表 |
| PAD端 | 用户读取 | 使用RFID读取用户身份信息 |
| 用户登录 | 使用用户名或者RFID+密码方式登录 |
| 物资借入 | 扫描RFID，登录人借入物资 |
| 物资归还 | 扫描RFID，登录人归还物资 |
| 微信端 | 用户登录 | 微信用户登录 |
| 用户绑定 | 用户绑定微信号 |
| 物资查询 | 物资查询业务 |
| 借入查询 | 登录用户借入物资情况 |
| 归还查询 | 登录用户归还物资情况 |
| 微信通知 | 借入、归还物资时，通知管理员 |

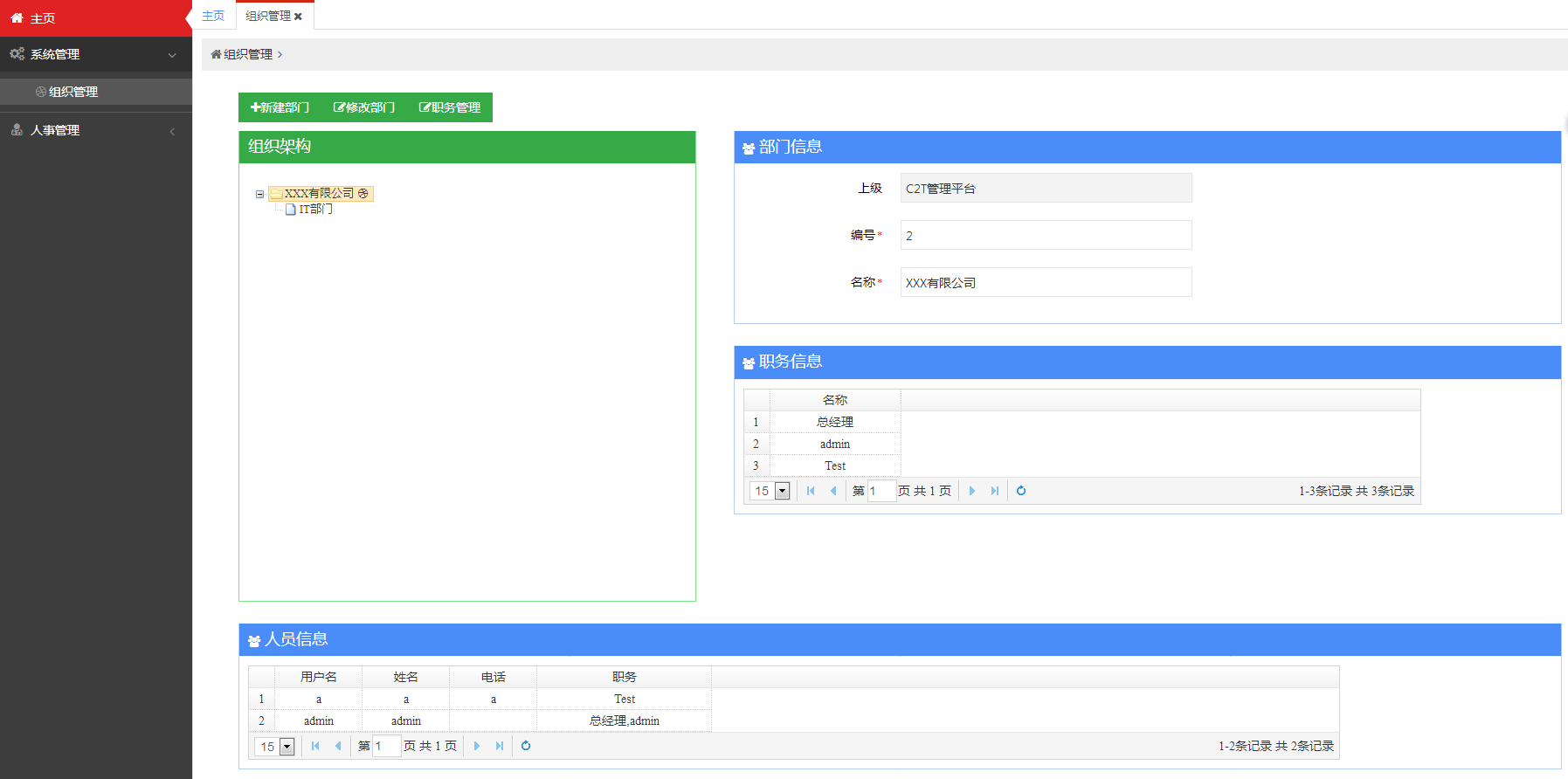
### 总体流程

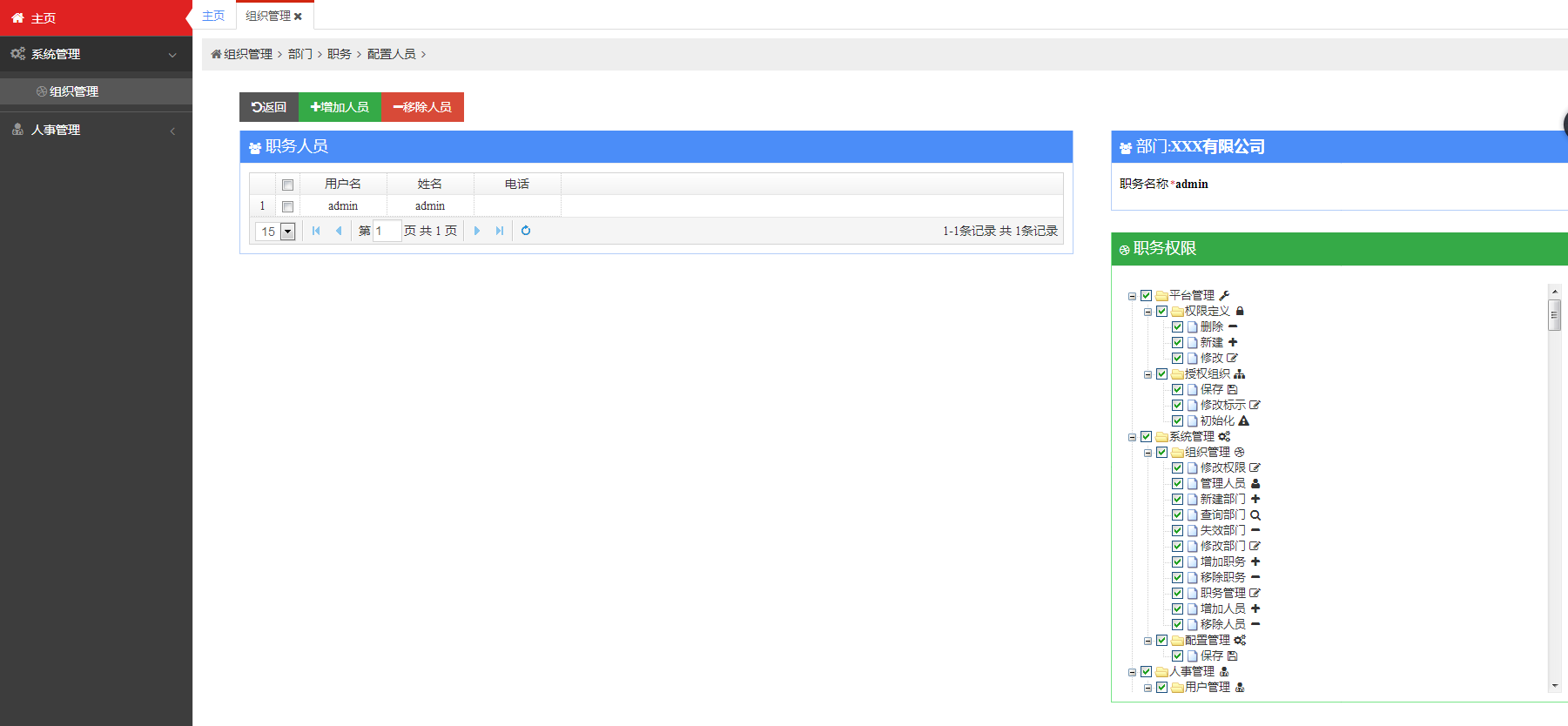
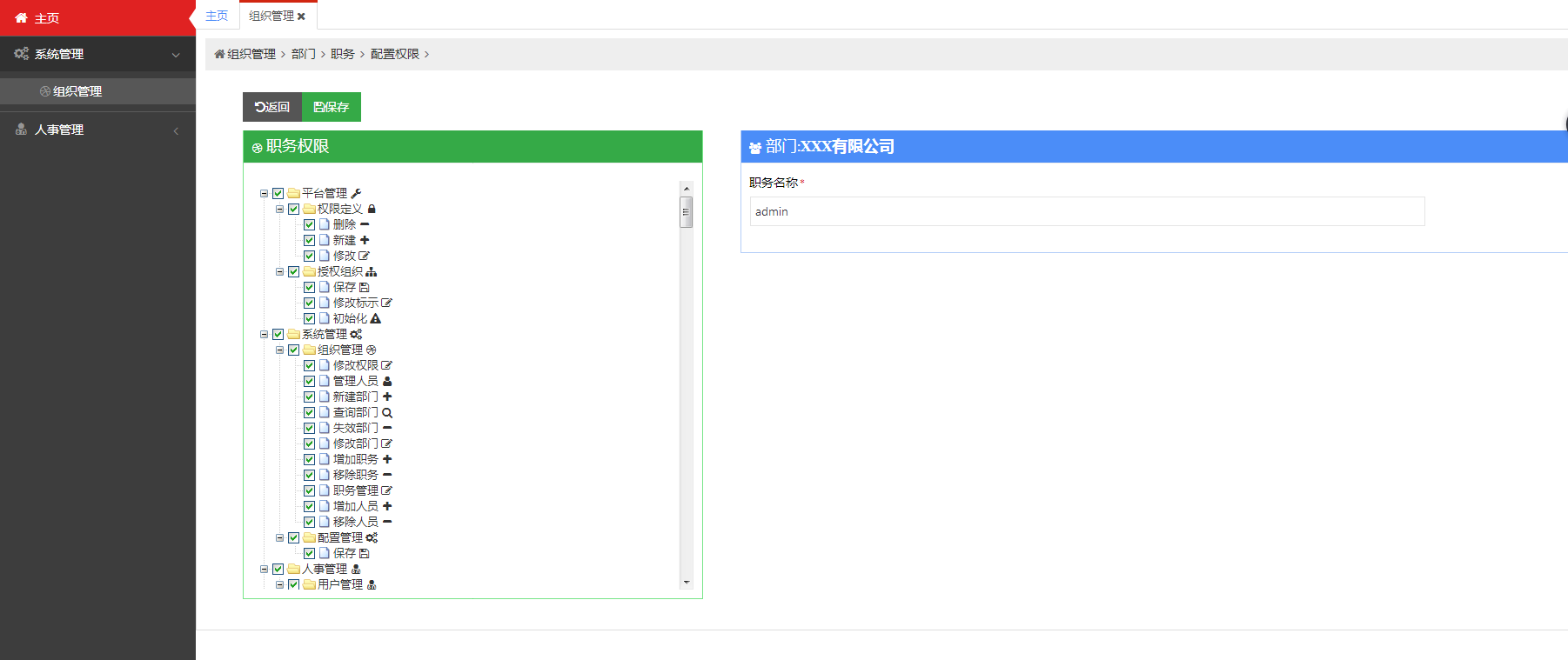
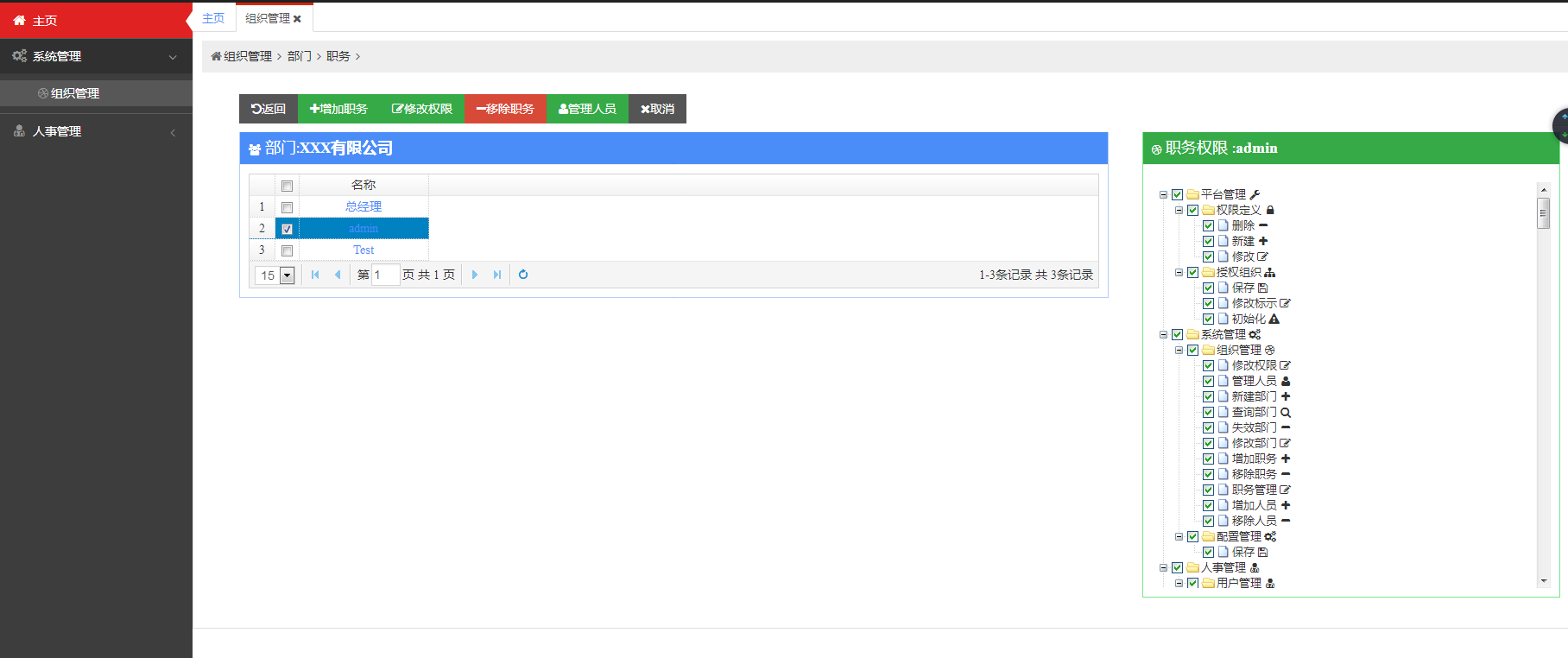
流程如下：

1. 物资管理员使用ＰＣ端功能，设置架构、权限以及管理使用用户；
2. 物资管理员使用ＰＣ端物资管理功能，设置物资信息；
3. 使用用户使用PAD登录系统，使用借入、归还功能；
4. 系统微信通知物资管理员接收、查询物资使用记录；

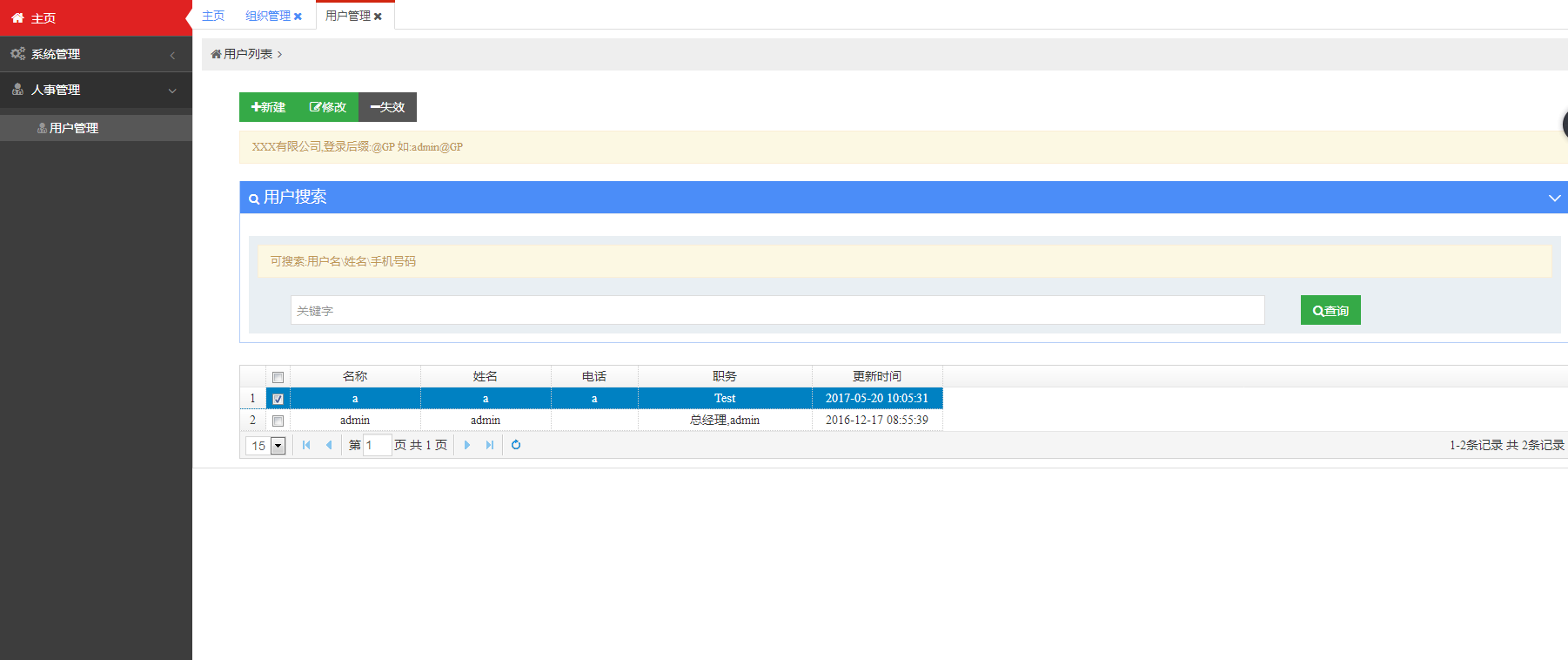
### PC端功能

#### 组织架构





#### 用户管理



#### 物资管理

#### 借出管理

#### 借入管理

#### 归还管理

#### 物资盘点

#### 物资查询

#### 操作日志

#### 报表查询

### PAD端功能

#### 用户读取

#### 用户登录

#### 物资借入

#### 物资归还

### 微信端功能

#### 用户登录

#### 用户绑定

#### 物资查询

#### 借入查询

#### 归还查询

#### 微信通知

## 网络部署设计



本次系统部署到idc的云主机上面。具体组网方式如下图：

## 应用体系架构设计

### 采用JAVA技术框架

JAVA框架着眼于未来技术发展的需要，在面向INTERNET和INTRANET的应用系统的支持方面提供了很好的基础平台，从各方面保证了系统的服务能力。而JAVA WEB的编译执行能力，可以很大幅度地提高系统的处理能力。JSON技术则对实现系统互联、提供数据共享能力方面是最佳的解决手段。

应用程序的主要原则是将应用程序逻辑地分为3个基本层： 表示层、业务逻辑层、数据服务层。通过按照这些原则对应用程序进行分层，使用基于组件的编程技术，并充分利用JAVA平台功能，开发人员可以生成具有高度可伸缩性和灵活性的应用程序。简单地分布式应用程序模型包含与中间层进行通讯的客户端，中间层本身由应用程序服务器和包含业务逻辑的应用程序组成。应用程序反过来又与提供和存储数据的数据库进行通讯。

表示层包括到应用程序的胖客户端接口。胖客户端通过直接使用 Microsoft Win32 API 或间接通过 Windows 窗体，为操作系统的功能提供完全的编程接口，并广泛地使用组件。本系统建议采用胖客户端的设计。

业务逻辑层被分为应用程序服务器与WEB服务，它们可用于支持客户端。可以使用JAVA框架编写 Web 应用程序以利用 JAVA WEB组件服务、JSON、消息队列 (MSMQ)、目录服务和安全性服务。应用程序服务反过来可以与数据访问层上的若干个数据服务进行交互。

数据服务层提供对数据库访问的支持。支持数据访问和存储的数据服务包括下列各项：

MyBatis：JAVA ORM框架，提供数据库连接服务。

SpringMVC：广泛应用的JAVA WEB框架。

JSON：用于指定数据结构的标记标准。

数据层需要处理能力很强的带有冗余存储硬盘的服务器。应用逻辑层需要处理能力很强的计算机，但不需要冗余存储硬盘。由于这些层都是互不相同，所以支持应用逻辑的计算机可以比支撑数据服务层的计算机便宜一些。对于比较复杂的情况，可以根据各个层次的需求调整软件。服务器可以根据后台进程的情况进行调整，对前台用户只有很少和没有交互。而客户机的情况则相反。数据服务层要求提供很好的硬盘和内存性能，而应用逻辑层则大量地使用内存，要求很好的CPU和网络I/O性能。

### 采用JSON格式数据传输

JSON(JavaScript Object Notation, JS 对象标记) 是一种轻量级的数据交换格式。它基于 ECMAScript 规范的一个子集，采用完全独立于编程语言的文本格式来存储和表示数据。简洁和清晰的层次结构使得 JSON 成为理想的数据交换语言。 易于人阅读和编写，同时也易于机器解析和生成，并有效地提升网络传输效率。

## 硬件环境要求

## 软件环境要求

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | 用途名称 | 主要配置说明 | 备注 |
| 1 | 服务器操作系统 | linux |  |
| 2 | 数据库服务器 | MySql |  |
| 3 | 中间件平台 | Tomcat6.0以上 |  |
| 4 | 客户机 | Windows XP |  |

# 系统安全体系设计建议

## 系统安全目标、策略与建设原则

### 系统的安全目标

根据系统网络结构和应用模式，针对可能存在的安全漏洞和安全需求，我们建议在不同的层次上提出安全级别要求，并提出相应的解决方案，制定相应的安全策略，编制安全规划，采用合理、先进的技术实施安全工程，加强安全管理，保证的信息系统的安全性。

### 系统的安全策略

正确处理保密、安全与开放之间的关系；安全技术与安全管理相结合；分析系统安全的风险，构造系统安全模型，从保护、检测、响应、恢复四个方面建立一套全方位的立体信息保障体系；遵循系统安全性与可用性相容原则，并具有适用性和可扩展性。

### 系统安全建设的原则

同步建设原则：安全系统建设与应用系统建设同步进行，按照系统的总体目标要求，总体设计安全系统。

适度复杂与经济合理原则：安全系统建设既要满足系统保护的需求，又要尽量减少复杂程度，要易于操作，低成本。

系统可扩展和可伸缩配置原则：安全系统要能够按不同规模伸缩配置，业务量小时配置系统基本框架和相应服务单元以具备良好的性能价格比，并且具有动态平滑扩展能力，业务量大时通过平滑增配相应的服务单元以适应业务的发展。

最小特权原则：系统不给用户超出执行任务所需权利以外的权利。

多人负责、任期有限、职责分离的管理原则：每一项与安全有关的活动，都必须有两人或多人在场；任何人都不能长期担任与安全有关的职务；未经领导批准，不参与职责以外的任何与安全有关的活动；合理划分人员与工作的分工职责。

## 系统安全体系概述

本项目的安全体系设计将在三维安全体系指导下，从物理安全、数据系统安全、网络系统安全、应用系统安全、安全管理五方面出发，综合运用各种安全技术，建立统一的安全支撑环境，保护全系统的安全。三维安全体系如下图所示。

aaa

安全支撑环境由基本安全防护系统和网络信任服务系统组成，同时结合数据中心的容灾备份与故障恢复可靠性措施。安全支撑环境如下图所示。

aaa

### 基本安全防护系统

基本安全防护系统包括物理安全、网络系统安全和数据安全。

（1）物理安全：包括环境安全、设备安全、媒体安全。系统运行环境，机房安全要符合国家规定的等级；从布局上分开各类设备，尤其是密码系统要与其它系统要有明确的隔离墙；按照国家有关规定安装与管理密码设备；密码系统实行分区控制、区域防护；机房设置安全防盗报警装置和监视系统；按照数据的重要程度，对数据进行分类备份，备份数据存放间具备防火、防高温、防水、防震能力；对核心网络，采用屏蔽布线、干扰器等措施，防止电磁辐射泄漏。

（2）网络系统安全：对网络单元和边界，采用防火墙、入侵检测、漏洞扫描、安全审计、病毒防治、Web信息防篡改、非法拨号监控、过滤控制、加密机等基础安全技术保障网络的安全。

业务专网与公共服务网逻辑隔离；业务专网各区域之间逻辑隔离，采用防火墙、入侵检测、漏洞扫描、安全审计等技术进行保护；对联接在互联网上的网站，采用Web信息防篡改、病毒防治、过滤控制等保护措施。

（3）数据系统安全

从数据库、数据传输、数据存储等方面考虑数据系统的安全。

选择具备安全控制功能的数据库系统，数据库系统应当包括系统权限、用户对象权限、角色权限三级权限管理结构，符合C2级安全标准，提供灵活的审计功能，具备异常情况下对数据的容错处理的能力和一致性保证措施。采用应用系统加密程序、VPN、链路加密机等技术保证敏感数据的传输安全。采用容错技术、多级备份机制、异地数据备份等措施保证数据存储安全。

## 建立完善的安全体系结构

### 安全服务

国际标准化组织（ISO）的计算机专业委员会根据开放系统互连参考模型（OSI）制定了一个网络安全体系结构，包括安全服务和安全机制，该模型主要解决对于网络信息系统中的安全和保密问题。

### 对等实体鉴别服务

这种服务是在两个开放系统同等层中的实体建立连接和数据传送期间，为提供连接实体身份的鉴别尔规定的一种服务。这种服务防止假冒或重放以前的连接，也即防止伪造连接初始化这种类型的攻击。这种鉴别服务可以是单向的也可以是双向的。

### 访问控制服务

这种服务可以防止未经授权的用户非法使用系统资源。这种服务不仅可以提供给单个用户，也可以提供给封闭的用户组中的所有用户。

### 数据保密服务

这种服务用加密的方法实现的。加密的目的有三种：

1. **密级文件改为公开文件**

无论是绝密文件还是机密文件，经加密都变成公开文件；这样在通信线路上公开发送，在非密的媒体中公开存放，不受密级管理的限制；

1. **实现多级控制需要**

密级划分也是等级划分，按不同密级加密是为了实现多级控制。密级划分只是多级控制的一部分。就一件事来说，这一部分人是有关人员，另一部分人是无关人员，但就另一件事来说，这有关人员和无关人员都可能发生变化。

1. **构建VPN的需要**

修筑加密通道，防止搭线窃听和冒名入侵。

数据保密服务包括以下内容：

1. **连接保密**

即对某个连接上的所有用户数据提供保密。

1. **无连接保密**

即对一个无连接的数据报的所有用户数据提供保密。

1. **选择字段保密**

即对一个协议数据单元中的用户数据的一些经选择的字段提供保密。

1. **信息流安全**

即对可能从观察信息流就能推导出的信息提供保密。

#### 数据完整性服务

数据完整性服务这种服务用来防止非法实体（用户）的主动攻击（如对正在交换的数据进行修改、插入，使数据延时以及丢失数据等），以保证数据接收方到的信息与发送方发送的信息完全一致。具体提供的数据完整性服务有以下五种：

1. **可恢复的连接完整性**

该服务对一个连接上的所有用户数据的完整性提供保障，而且对任何服务数据单元的修改、插入、删除或重放都可使之复原。

1. **无恢复的连接完整性**

该服务除了不具备恢复功能之外，其余同前。

1. **选择字段的连接完整性**

该服务提供在连接上传送的选择字段的完整性，并能确定所选字段是否已被修改、插入、删除或重放。

1. **无连接完整性**

该服务提供单个无连接的数据单元的完整性，能确定收到的数据单元是否已被修改。

1. **选择字段无连接完整性**

该服务提供单个无连接数据单元中各个选择字段的完整性，能确定选择字段是否被修改。

#### 数据源鉴别服务

这是某一层向上一层提供的服务，它用来确保数据是由合法实体发出的为上一层提供数据源的对等实体进行鉴别，以防假冒。

#### 禁止否认服务

这种服务用来防止发送数据方法送数据后否认自己发送过数据，或接受方接收数据后否认自己接收到过数据。该服务有以下的服务组成：

1. **不得否认发送**

这种服务向数据接收者提供数据源的证据，从而可防止发送者否认发送过这个数据。

1. **不得否认接收**

这种服务向数据发送者提供数据已交付给接收者的证据，因而接收者事后不能否认曾收到此数据。

上面这两种服务实际是一种数字签名服务。

### 安全机制

为了实现上述各种OSI安全服务，本方案将采用以下6种安全机制：

#### 加密机制

加密是提供数据保密的最常用方法。按密钥类型划分，加密算法可分为队称密钥加密算法和非对称密钥加密算法两种；按密码体制分，可分为序列密码和分组密码算法两种。用加密的其他技术相结合，可以提供数据的保密性和完整性。对于OSI的七层模型，除了对话层不提供加密保护外，加密机制将可能在其他各层上提供。与加密机制伴随而来的是密钥管理机制。

#### 数字签名机制

数字签名时解决网络通信中特有的安全问题的有效方法。特别是针对当通信双方发生争执时可能产生的如下安全问题：

1. **否认**

发送者事后不承认自己发送过某份文件。

1. **伪造**

接收者伪造一份文件，声称它发自发送者。

1. **冒充**

网上的某个用户冒充另一个用户接收或发送信息。

1. **篡改**

接收者对收到的信息进行部分篡改。

#### 访问控制机制

访问控制是按事先确定的规则决定主体对客体的访问是否合法。在本系统中，当一个主体试图非法使用一个未经授权使用的客体时，该机制将拒绝这一企图，并附带向监管及服务系统报告这一事件。监管及服务系统将产生报警信号或形成部分追踪审计信息。

#### 数据完整性机制

数据完整性包括两种形式：一种是数据单元的完整性，另一种是数据单元序列的完整性。数据单元完整性包括两个过程，一个过程发生在发送实体，另一个过程发生在接收实体。保证数据完整性的一般方法是：发送实体在一个数据单元上加一个标记，这个标记是数据本身的函数，如一个分组校验，或密码校验函数，它本身是经过加密的。接收实体是一个对应的标记，并将所产生的标记与接收的标记相比较，以确定在传输过程中数据是否被修改过。

在本系统中，要求要交换的数据会在发送方进行拆分、编号以形成单元序列，并附加时间标记，在接受方进行重新排序和拼接，对于传递过程中缺失的部分将进行重发，并对要交换的数据进行数字摘要验证，确保数据传递过程中不会出现数据的丢失，并防止假冒、丢失、重发、插入或修改数据。

#### 交换鉴别机制

交换鉴别是以交换信息的方式来确认实体身份的机制。在本系统中用于交换鉴别的技术有：

1. **口令**

由发方实体提供，收方实体检测。

1. **密码技术**

将交换的数据加密，只有合法用户才能解密，得出有意义的明文。在本方案中，这种技术还会与下列技术一起使用：

1. 时间标记和同步时钟
2. 双方或三方“握手”
3. 数字签名和公证机构
4. **利用实体的特征或所有权**

在本方案中采用的技术是数字证书。

#### 公证机制

在一个大型网络中，有许多节点或端节点，在使用这个网络时，并不是所有用户都是诚实的、可信的，同时也可能由于系统故障等原因使信息丢失、迟到等，这很可能引起责任问题。为了解决这个问题，就需要有一个各方都信任的实体——公证机构，如同一个国家设立的公证机构一样，提供公证服务，仲裁出现的问题。

## 访问控制规则管理

访问控制是系统安全管理中极其重要的一环。它是在身份识别的基础上，根据身份对提出的资源访问请求加以控制，防止非授权使用或者控制资源。它有助于达到信息的机密性、完整性、可控性和建立责任机制。作为提供信息安全保障的主要手段，及最为突出的安全机制, 被广泛地应用于多个方面。

访问控制是为了限制访问主体（或称为发起者，是一个主动的实体；如用户、进程、服务等），对访问客体（需要保护的资源）的访问权限，从而使计算机系统在合法范围内使用；访问控制机制决定用户及代表一定用户利益的程序能做什么，及做到什么程度。对于系统，它所提供的服务体现在：

在该系统中，用户对数据的访问必须是受控的，以便于管理和维护它的安全；

访问控制是由访问权限来实现的，它定义了用户是否可以以及如何访问系统的数据；

访问控制同时还是由一个安全系统来实现的，它是在计算机系统或操作系统之上附加和集成的。

审计跟踪：把系统中发生的所有安全情况存储在安全审计跟踪之中，以便分析原因，分清责任，及时采取相应的措施。审计跟踪的信息主要包括：事件类型、被管客体等级、事件时间、事件信息、事件回答以及时间统计等方面的信息。

系统对每一个用户组设定其模块级、操作级和数据级权限。在用户访问系统时，系统根据其所属的用户组来对其进行访问控制。

系统访问控制规则通过调整各用户组所具备的权限，各用户所属的用户组来管理。

## 表格内容安全

表格内容的安全正是体现访问控制规则管理和数据安全规则管理的具体应用。本系统是要经过领导的审批流程，所以下级对领导的审批意见不能删改、复制、剪贴等的操作，只有浏览权利。若对“领导批复”项进行上述操作，系统将自动记录该操作过程并锁定该项不能保存和打印该表格。当然我们还会通过自动判断操作人的身份，只有签署该意见的人才有权修改自己的审核意见，其它人只能依据自己拥有的权限浏览该审核意见，但不能做任何编辑操作。这样的话就可以完全防止对“领导批复”项的任何非法操作。

对于上报的数据必须保证数据的原始性，只有上报数据人可以修改，其他人只有浏览权限；而对于敏感的预警和案件处理信息，则只有具有一定的权限才可以处理。

## 数据安全规则管理

系统应保证系统数据安全的安全规则管理。对于系统的数据设定不同的安全级别，将此级别赋予相应的用户权限，拥有某一权限的用户根据其权限所对应的数据安全级别访问、操作数据库中的数据，从而进行维护数据安全的安全规则管理。系统数据的安全规则主要用于保证数据的保密性、完整性、不可否认性。

数据的保密性是系统中的信息不被泄露给非授权的用户、实体或过程，或供其利用的特性。即，防止信息泄露给非收钱个人或实体、信息只为授权用户使用的特性。保密性是在可靠性和可用心基础上，保障网络信息安全的重要手段。

数据的完整性是网络信息未经授权不能进行改变的特性，即网络信息在存储或传输过程中保持不被偶然或蓄意的删除、修改、伪造、乱序、重放、插入等破坏或丢失的特征。完整性是一种面向信息的安全性，它要求保持信息的原样，即信息的正确生成、正确存储和传输。完整性与保密性不同，保密性要求信息不被泄露给未授权的人，而完整性则要求信息不受到各种原因的破坏。影响网络信息完整性的因素有：设备故障、误码、人为攻击、计算机病毒等。

数据的不可抵赖性也称为不可否认性。在系统的使用过程中，确信参与者的真实同一性，即，所有参与者都不可能虚假的否认或抵赖曾经完成的操作和承诺。利用信息源证据可以防止发信息方不真实地否认已发送信息，利用递交收集证据可以防止受信息方否认已经接受的信息。与其它服务不同，不可抵赖性针对的是来自合法用户的威胁，而不是未知攻击者的威胁。它是为数据交换的双方提供不可否认的证据来解决因否认而产生的争议提供支持，在实际上是建立了数据交换双方的责任机制。因为参与者在系统运作时必须拥有权限，所以不可抵赖性是构建在认证服务之上。

## 数据库系统的安全措施

### 数据库系统安全与保密的特点

从安全与保密角度看，数据库系统的基本特点可以概括为：

1. 在数据库中要保护的客体比较多；
2. 数据库中数据的生存期限较长，对保护的精度要求更高；
3. 数据库的安全涉及到信息在不同程度上的安全；
4. 数据库系统中受保护的客体可能是复杂的逻辑结构，若干复杂的逻辑结构可能映射到同一物理数据客体上；
5. 数据库的安全与数据的语法有关。

数据库的安全与保密还应当考虑到对推理攻击的防范；推理攻击是指从非敏感的数据推理得出敏感数据的攻击方式。

从所面临的安全与保密威胁方面来看，数据库系统应该重点对付以下威胁：

1. **篡改（伪造）**

篡改就是修改数据，使其不真实。例如，删除定单、发货单或收据等。这是一种潜在的威胁，因为在其造成影响之前，很难发现数据已被篡改。对付篡改的一种实用措施是限制对特定数据的访问。例如，若数据库表存放在一个Micrsoft SQL服务器上，则必须限制赐ISQL/w程序的访问权，因为此程序能绕过限制直接接触数据。

1. **损坏**

数据的真正丢失是一个严重威胁。表格和整个数据库都可能被删除、移走或破坏，这样它们的内容就不可用了。数据被损坏的原因可能是恶意破坏、恶作剧或病毒等。

1. **窃取**

窃取数据的隐蔽性很强，甚至当数据丢失已经造成损害时，仍未被发现。通过对敏感数据的非法访问，可以将敏感数据拷贝到诸如软盘一样的可移动的介质上，或以打印报告的形式取走。

### 数据库系统的安全措施

数据库作为一种特殊的信息系统，它的安全保密措施与普通的网络信息系统的安全措施有许多共同之处，当然也有自身的一些特点。数据库的安全与保密措施的主要目的在于：

1. **保证数据库的完整性**

包括物理上的完整性(数据不受物理故障(如掉电)的影响，并有可能在灾难性毁坏后重组数据库)、逻辑上的完整性(保护数据库的逻辑结构)、数据库中元素的完整性(保证每个元素所含的数据准确无误)。

1. **保证数据库的保密性**

包括用户身份鉴别(保证每个用户是绝对可识别的，从而可对它进行审计跟踪，并可以保证对特定数据的访问保护)、访问控制(保证用户仅能访问授权数据，并保证同一组数据的不同用户可以被赋予不同的访问权限)、可审计性(有能力跟踪谁访问了数据库中的哪些元素)。

1. **保证数据库的可用性**

数据库系统对用户应该有友好的界面，可用简单方法访问数据库中所有授权访问数据。

为达到上述安全目的，数据库系统需要采取一系列的安全措施：

1. **数据备份**

为了防止数据库中的数据受到物理破坏，建议对数据库系统采取定期和在线备份系统中所有文件两种方式来保证来保护系统的完整性。

本方案建议将本系统数据库系统中的所有文件，使用相应的备份软件如Veritas NetBackup，实现网络数据存储。具体到方案中就是在平台中增加一台备份服务器，安装VERITAS NetBackup相关存储备份软件；同时在该备份服务器上连接一台磁带机，磁带7合，每天一合，一星期一个循环。在数据库服务器上安装相应软件，对操作系统和数据库数据进行备份，通过局域网将数据集中备份管理到磁带机上。

1. **访问日志**

为了在本系统出错时可以重组数据库，数据库管理系统将维护数据库系统的事务日志，以便用这种日志恢复系统故障时丢失的数据。

1. **事务管理**

如果在数据修改期间系统发生故障，数据库管理系统将会面临严重的问题。此时，一个记录甚至一个字段中，有的部分得到修改而其余部分维持原样。为了避免这种错误，本系统采用两阶段修改技术来保护数据的完整性。两阶段修改技术的第一阶段叫做准备阶段。这时，数据库管理系统完成修改所需的信息，进行修改前的准备工作。在此阶段，数据库管理系统收集数据，建立记录，打开文件并且封锁其他用户，然后计算最后结果。简言之，数据库管理系统完成修改所需的一切准备工作，但未对数据库作任何修改。第一阶段的最后一步叫做“提交”，它的任务是把“提交”标志写入数据库。提交标志是两阶段修改技术中两阶段的分界点，它意味着一旦数据库管理系统通过这个分界点后就不再返回，也就是说，一旦进入提交阶段数据库管理系统将开始进行永久性的修改。第二阶段叫做永久性修改阶段。在此阶段中，凡是属于提交前的任何动作都是不可重复的，但本阶段的修改活动本身则可重复多次。因此，若在第二阶段系统发生故障，则数据库中可能包含非完整的数据，但可以重复所有第二阶段的活动，使数据恢复完成。第二阶段完成以后，数据库管理系统将把“事务完成”标志写入系统的日志，并清除数据库中的“提交”标志。

1. **数据完整性校验**

为了保证数据库元素的完整性，本系统在数据输入时帮助用户发现错误和修改错误。在本方按种使用的方法有三种：首先，数据库管理系统利用字段检查，测试某一位置的值是否正确；其次，数据库管理系统利用访问控制的机制来维护数据的完整性，以防止非授权用户对主体数据的访问；第三种办法是数据库管理系统维持一个数据库的修改日志。修改日志记录数据库的每次修改，既有修改前的值也有修改后的值。借助于修改日志，数据库管理员可以在出错时“废除”任何修改而恢复数据的原值。

1. **身份鉴别**

本系统的数据库系统要求严格的用户身份鉴别。为了进一步加强数据库系统的安全性和保密性，必须对使用数据库的时间甚至地点加以限制。

1. **访问控制**

采取适当的访问控制机制。既可以是任意访问控制，又可以是强制访问控制。任意访问控制可以通过控制矩阵进行。强制访问控制通过与军事安全策略类似的方法来实现。具体地讲，在本系统的安全控制上引入级和范围（类别）的概念，每个主体制订一个范围许可级别，每个客体有相应的保密级别。范围许可级别和保密级别一般有四类：公开、秘密、机密和绝密。在服从强制控制的前提下，还可以结合任意控制访问机制，形成一种比较安全又比较灵活的多级安全模型。

1. **多层数据库**

采用多层数据库系统，即把操作系统的多级安全模型引入本系统的数据库系统设计之中。多层数据库对访问进行控制的一种简单方法是“分区”。数据库被划分为不同的子库（分区），每个子库都拥有各自的安全层次。这种方法破坏了数据库的基本优点，它增加了设计的冗余，而且在对某个字段进行修改时，可能要同时查询并修改其他分区中的相同字段，以维持设计的一致性。

多层数据库对访问控制的另一种方法是利用视图这个抽象概念。简言之，视图是数据库的一个子集，它仅包含用户有权访问的信息。这样单个用户的所有查询仅在自己的数据库子集上进行。子集视图保证用户不会访问允许范围之外的其他设计。除了元素之外，视图由数据库中相应的一系列关系构成。用户可以在已有的属性元素上进行相应的操作。

多层数据库的第一层完成访问控制，并进行数据库系统需要的用户身份鉴别，还应当完成数据传输给高层时的筛选工作。第二层完成基本的数据库索引及其计算功能。第三层把用户的视图转化为数据库的基本关系。

与多层数据库系统安全有关的还有并发控制、数据恢复、审计跟踪等技术。

## 安全管理

从机构、制度、教育三方面来加强安全管理。

建立东莞供电局应用开发项目的信息安全管理中心，负责管理信息安全工作。各分局和处室分别设立相应管理人员，以统一组织和协调食品安全网络服务平台开发项目的安全管理工作。

应用开发的安全保密管理制度主要有人员安全管理制度、设备安全管理制度、运行安全管理制度、安全操作管理制度、安全等级保护制度、有害数据防治管理制度、敏感数据保护制度、安全技术保障制度、安全计划管理制度等。

加强安全培训，提高管理人员、技术人员以及系统使用者的安全意识、法制观念和技术防范水平，保证系统安全运行。

# 项目管理与质量控制方案

为确保项目的成功实施，在工程建设过程中，必须在良好的计划、管理、控制和协调下，才能保证工程建设有序顺利地进行。因此，建立一套科学严密的管理体系，有效地调配人员、时间和资金等项目资源，对工程建设非常重要。我公司根据本工程的特点，按照严格的ISO9000质量保证体系，明确项目的管理目标，制定项目的管理方式、组织结构、实施计划、质量和安全保证体系，作为整个工程建设的实施指导。

## 项目管理

### 项目组织与人员承诺

为使工程按质、按量、按时及有序实施，我们将对本项目建立一个完善和稳定的管理组织机构。

在项目负责人员方面，包括一名专职负责的项目经理、一名具丰富研发经验的技术主管。在建设期内，接到采购人通知4小时内到达采购人现场处理问题或交流情况。

本项目的项目经理、技术主管具体负责项目的实施，在系统建设和免维期内，供应商承诺的项目经理和开发实施的主要人员未经用户同意不得调整，如中途更换项目经理、技术主管，必须征得用户同意。

我们驻东莞机构在本项目组人员不少于6人，将投入约15人。

### 项目组织架构

xxx公司在项目管理方面具有有效的方法和多年的经验，拥有完善的项目管理组织结构。xxx公司针对本项目将成立跨部门的项目团队，项目团队采用矩阵式的结构，一方面增加对客户需求的响应速度；另一方面得到各专业部门的指导和支持。

我们为有效进行资源控制、进度控制、质量控制、成本控制，确保项目工程顺利实施及系统维护的方便进行，我们建议由xxxx公司高层与采购方项目领导共同组成项目协调委员会，以把握和推动整个项目的执行，保证整个项目如期高质量地完成。

我们目前主要的技术方向就是J2EE开发，同时我们也有基于J2EE开发的自主知识版权的应用支撑平台，所以在J2EE开发方面既有系统平台人才、又有应用开发人才，在平台系统与业务系统配和方面有着丰富的经验和深刻理解。

为使工程按质、按量、按时及有序实施，我公司将建立一个完善和稳定的管理组织机构。我公司为本项目专门配有经验丰富的项目管理人员、技术专家，其他岗位的人员也是经过层层选拔而挑选出来的精英。下面介绍一下本项目我公司的项目人员架构以及相应的人员要求。

整个项目团队共15人，分为项目管理小组、质量管理人员、分析人员、设计开发人员、测试人员、系统实施人员、维护人员这七类人，部分人在本项目重的角色重叠。根据项目开发工作的需要和项目管理工作需要，结合我司筹建的项目团队的实际技能情况，项目团队中的主要角色需要执行的主要项目任务和所具备的技能，见下表：

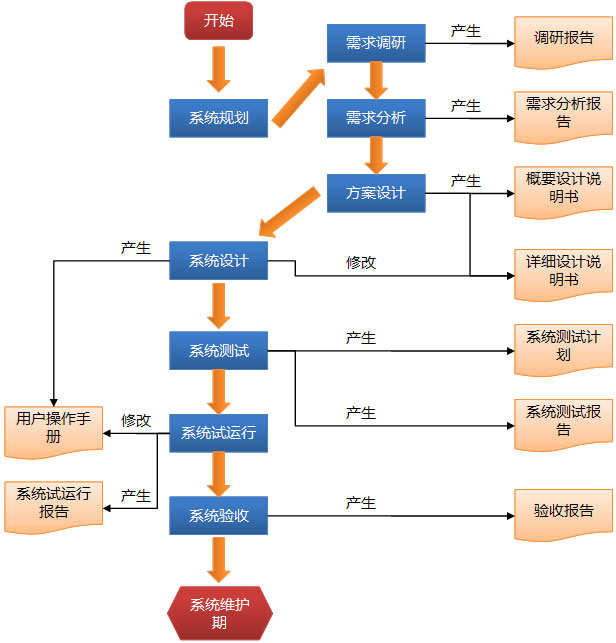


|  |  |  |
| --- | --- | --- |
| **项目角色** | **执行的主要项目任务** | **相关角色具备的技能** |
| 客户代表 | 确定项目的需求 参与重大项目活动的审批 参与项目验收 |  |
| 公司管理层 | 提供项目的资源保证 项目计划审批 项目进度监控 |  |
| 项目经理 | 全面负责项目管理 负责项目计划制定 协调安排项目团队工作 | 资深的项目管理经验 具备丰富的大型项目团队管理的经验 |
| 技术主管 | 确定技术方向和技术路线 协助客户代表和项目团队解决技术问题 协助项目经理制定项目计划 | 具备丰富的SOA架构设计开发经验 精通J2EE体系结构 精通OOA、OOD技术 精通UML技术 |
| 业务专家 | 负责对客户提出业务建议 对系统的业务合理性把关 协助客户代表解决业务问题 | 具有资深的电力行业系统建设经验 |
| 评审人员 | 参与业务建模评审 参与需求评审 参与设计评审 参与测试评审 | 具备丰富的项目管理经验 较多的软件开发经验 丰富的软件开发评审经验 |
| 系统分析员 | 明确需求 需求分析 | 具有多年电力行业系统的经验 熟悉应用开发及本系统相关信息化建设 精通需求分析技术 |
| 架构设计师 | 制定解决方案 体系结构决策 组件建模 操作建模 | 具备资深的分布式系统开发经验 精通SOA的解决方案 精通UML建模技术和建模工具 具备J2EE体系和中间件技术设计经验 具备丰富的大型数据库建设经验  熟悉应用开发及本系统相关信息化建设 Web 服务概念与平台、最佳实践 |
| 数据库设计员 | 业务实体分析和逻辑建模 数据库物理建模 数据库性能优化 数据库管理 | 精通UML建模技术和建模工具 具备丰富的大型数据库建设经验  熟悉应用开发及本系统相关信息化建设 精通数据库管理系统 精通数据建模技术 |
| 程序员 | 代码编码 服务请求者编码 代码文档化 设计执行单元测试 | 精通OOP技术 精通web service编程 熟悉UML建模工具 精通JSP、servlet、EJB、JMS、JTA XML、XML Schema Web 服务概念与平台、最佳实践 Junit测试工具 |
| 测试员 | 运行系统测试 分析测试结果，编写测试报告 缺陷跟踪 | 具备丰富的系统测试管理经验 |
| 系统安装人员 | 安装和配置统一的开发环境 系统的安装实施 协助系统的日常维护 | 丰富的系统管理维护经验 |
| 客户培训人员 | 用户培训材料的准备 实施用户培训 协助客户代表落实新的业务规范 | 丰富的系统实施经验 丰富的系统培训经验 |
| 客服人员 | 协助客户的定期走访 接收客户投诉 组织客户投诉的解决 |  |
| 系统维护人员 | 的售后服务 | 丰富的系统管理维护经验 |

### 项目管理规范

软件项目的实施需要严格的进行过程控制，目前在该领域的主要成果是软件工程学的发展。

根据我们多年的项目实施经验，并参考软件工程的相关规范，我们将软件项目的实施按照软件工程的方法作了规范的管理，详细过程如下图所示：



系统开发严格遵照国家软件工程规范或国际公认的SOA（面向服务的分析与设计）与OO（面向对象，包括OOA、OOD、OOP）的开发方法进行。

我们将在开发过程中提出合理的开发计划及详细的进度安排计划，在项目实施过程中进行追踪和控制，定时总结并提交开发进度月报。

所有软件工程阶段性文档由采购人组织专家咨询组评审，只有当本阶段的评审通过后才能进行下一阶段的工作。

提供良好的软件质量保证机制，包括系统软件开发的规范化保证，要有统一的命名规范，良好的编码风格，统一的代码布局格式，详尽的程序注解等，对软件开发的各个阶段都要进行质量评审，并提供评审报告。

对软件的测试应贯穿于系统开发的始终，提供详尽的测试计划、测试报告及结果分析报告。

我们首先拟出一个测试方案，具体到每一个测试步骤，与采购人讨论通过后，方可按计划进行测试。

安装调试及搭建测试环境在项目单位指定的地点进行。

我们负责全部应用软件的安装、调试及正式运行前的测试。

应用软件系统安装的主要目标不仅是使所有应用软件能够在相应平台上正常运行，而且必须具有对业务软件系统运行的监控测试手段，以证明系统优化运行。我们承诺使项目单位的系统达到以上目标。

### 项目风险控制

大型系统实施项目，风险巨大。事实上在全世界统计有近36％的大型项目以失败或近似失败而告终。

项目组织体系不仅应是单纯的项目管理组织机构，还应该是项目设施的风险防范机构。在项目实施过程中，应该充分考虑风险因素，及早规避，减少项目的损失。

#### 目标风险

目标风险是由于双方对阶段或整体目标的定义理解产生歧义而形成。

规避方法：由系统开发方提供给用户方详尽的咨询及分析建议，在实施过程中，根据各阶段实施的实际情况变化，调整和修改实施计划及阶段目标。

#### 规模风险

规模风险是由于双方最初对项目的结构规模、扩展能力、单位时间内推广规模估算有误而造成的。

规避方法：在项目规划前期由系统开发商提供给客户详尽的咨询及分析建议，并经过双方充分的研讨，使做出的项目规划合理适度且行之有效。

#### 质量风险

质量风险是由于在项目建设过程中未确立标准的质量考核体系以及对质量指标监控不严造成的。

规避方法：参照软件开发标准而制订相应的规范质量标准并严格考核执行。

#### 资源风险

资源风险是由于项目的人力资源及技术资源发生供需不平衡而形成的。

规避方法：在项目规划前期详尽考虑项目建设过程中所需的资源，做出适当的资源规划，合理调配资源。使各种资源达到最佳配置。

#### 管理风险

管理风险是由于项目管理层使用不适于本项目的管理方法而形成的。

规避方法：由双方对项目的管理结构进行分析，针对本项目提出适合的项目管理方案，在方案确立后，在项目建设过程中严格履行实施。

### 项目文档管理及承诺

为了使项目管理标准化、程序化、提高项目实施的可靠性，为项目的实施制定了一套制度化的项目标准表格和文件，绝大部分管理程序都可以通过这些表格和文件的提交、同意和认定来体现。项目过程中项目实施小组成员必须完整填写相应的表格和文件，保证整个项目过程可记录可追踪可控制。

本系统将根据招标文件以及双方签字确认后的需求说明书进行定制开发。为了保证项目开发的成功，并且便于运行和维护以及以后的扩展升级，在开发工作的每一阶段，都需要编制一定的文件。这些文件连同计算机程序及数据一起，构成为计算机软件。文件是计算机软件中不可缺少的组成部分，在软件开发的不同时期提供以下文档，保证系统在现有的基础上可供第三方可进行二次开发。

系统开发将严格遵照国家软件工程标准进行，根据开发进度及时提供有关开发文档，包括系统设计说明书、业务流程设计文档、软件需求说明书、数据规格说明书、数据库设计说明书、测试计划、用户手册、模块开发卷宗、测试分析报告、系统维护手册、操作手册、系统安装手册等；

最终提供的软件产品包括各阶段开发文档、运行稳定可靠的本系统安装程序、注释清晰明了的能够编译生成目前正在运行的应用程序的源代码等；

项目管理将提交软件开发和实施计划、进度报告、培训计划、培训记录、例会记录以及采购人认为必要的其他文档。

本项目所有的技术文件用中文书写。

## 质量控制

### 质量保证目的

为满足客户系统全年不停顿高可靠的运行，我们从项目的最初调研、设计、开发、测试、与实施的全过程的每个环节均严格按照质量标准进行，形成了一套完备严谨的质量保证体系。

我们会在项目中指派专门的软件质量保证工程师以独立审查方式，从第三方的角度监控软件开发任务的执行，就项目是否正遵循已制定的计划、标准和规程给开发人员和管理层提供反映产品和过程质量的信息和数据，提高项目透明度，同时辅助软件开发人员取得高质量的软件产品。从而达到下面四个目的：

1. 通过监控项目开发实施过程来保证产品质量；
2. 保证开发出来的软件和软件开发、实施过程符合相应标准与规程；
3. 保证软件产品、软件实施过程中存在的不符合问题得到处理，必要时将问题反映给高级管理者；
4. 确保项目组制定的计划、标准和规程适合项目组需要，同时满足评审和审核需要；

### 质量保证工作

为了使每个环节均严格按照质量标准进行，我们将提供良好的软件质量保证机制，包括系统软件开发的规范化保证，要有统一的命名规范，良好的编码风格，统一的代码布局格式，详尽的程序注解等，对软件开发的各个阶段都要进行质量评审，并提供评审报告。对软件的测试应贯穿于系统开发的始终，要提供详尽的测试计划、测试报告及结果分析报告。我们的软件质量保证工程师会进行5大类的工作：

SQA计划：软件质量保证工程师在项目早期根据项目计划制定与其对应的SQA计划，定义出各阶段的检查重点和在每个阶段SQA的输出。编写完SQA计划后会组织SQA计划的评审，并形成评审报告，把通过评审的SQA计划发送给软件项目经理、项目开发人员和所有相关人员。

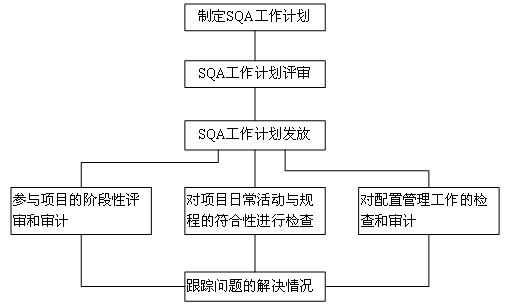
阶段性评审和审核：在SQA计划中通常已经根据项目计划定义了与项目阶段相应的阶段检查，包括本阶段的项目过程的审核和对其阶段输出的检查。通常是检查其阶段产品是否按计划按规程输出并且内容完整。SQA从保证评审过程有效性方面入手参与评审，如参与评审的人是否具备一定资格、是否规定的人员都参见了评审、评审中对被评审的对象的每个部分都进行了评审、并给出了明确的结论等等。

对项目日常活动的常规检查：SQA在两个阶段点之间设置若干小的跟踪点，来监督项目的进行情况，以便能及时反映出项目组中存在的问题，并对其进行跟踪，达到早问题、早解决。

对配置管理工作的检查和审核：SQA会对项目过程中的配置管理工作是否按照项目最初制定的配置管理计划进行监督，包括配置管理人员是否定期进行该方面的工作、是否所有人得到的都是开发过程产品的有效版本。

跟踪问题的解决情况：对于评审中发现的问题和项目日常工作中发现的问题，SQA会进行跟踪，直至解决。对于在项目组内可以解决的问题就在项目组内部解决，对于在项目组内部无法解决的问题，或是在项目组中跟催多次也没有得到解决的问题，会直接汇报给高层经理。

我公司建立了主要的SQA过程见下图：



首先我们需要建立SQA的工作计划，编写完SQA计划后会组织SQA计划的评审，并形成评审报告。评审通过后，质量管理人员会将SQA工作计划发放给项目的干系人，然后SQA工程师会按照计划进行评审。

### 过程控制

#### 概述

任何产品或服务的质量，都有一个产生、形成和实现的过程。从全过程的角度来看，质量产生、形成和实现的整个过程是由多个相互联系、相互影响的环节所组成的，每一个环节都或轻或重地影响着最终的质量状况。为了保证和提高质量就必须把影响质量的所有环节和因素都控制起来。

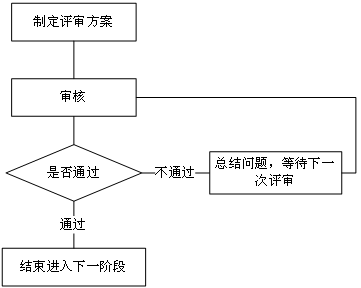
我们公司为了保证产品或服务的质量，根据ISO9001：2000的管理理念建立了一套过程的质量管理方法，做好过程的质量管理，把质量形成全过程的各个环节或有关因素控制起来，形成了一个综合性的质量管理体系。

#### 过程评审

**流程概述**

结合我们公司的实际工作，我们公司的过程控制主要体现在对项目过程中产生的工件和项目管理方面的评审工作和项目变更控制管理方面的工作。我们制定了项目管理过程评审的流程文档以控制项目的进度；并且制定了项目各个阶段评审标准和评审流程。

具体过程控制中的评审过程如下：



针对项目中每个里程碑都会根据这个评审过程进行评审工作。

项目经理根据具体要评审的过程制定与之相适应的评审方案，评审方案里包含了使用的评审标准、具体参与评审的人员、评审时间、评审方式等安排。SQA小组确认评审方案的有效性，并监控评审过程的有效进行。

评审工作主要以会议方式进行，评审人员根据评审标准对过程进行评审。记录员记录评审过程中的意见并将之整合发给项目经理，项目经理总结评审问题得出评审结果，并将评审报告发给文档编写人员和参与评审人员，若是评审通过则可以直接进入下一个阶段的工作，若是不通过则由项目经理安排相应的文档编写人员修改文档然后等待下次评审，直到评审通过。

**具体工作**

针对本项目具体有以下的评审工作：

业务建模评审

软件需求评审

架构设计评审

概要设计评审

详细设计评审

数据库设计评审

代码评审

测试评审

实施方案评审

**业务建模评审**

参与业务建模评审工作的具体人员角色：客户、项目经理、架构设计师、设计师、记录员。SQA小组会审核参与评审的人员的资格，以确保评审的有效性。

业务建模评审准则：

是否符合客户（目标组织）的结构及机制。

客户、最终用户和开发人员是否能够就目标组织达成共识。

是否能够导出支持目标组织所需的系统需求。

**软件需求评审**

参与软件需求评审工作的具体人员角色：客户、项目经理、业务流程分析员、架构设计师，记录员。SQA小组会审核参与评审的人员的资格，以确保评审的有效性。

软件需求评审的准则：

是否满足合同的要求；

是否符合业务模型；

是否满足一定的完整性，一致性，可追踪性；

是否与公司的其他系统有共同点，或有冲突；

**架构设计评审**

参与架构设计评审工作的具体人员角色：项目经理、业务流程分析员、系统分析人员、设计员、数据库设计员、记录员。SQA小组会审核参与评审的人员的资格，以确保评审的有效性。

架构设计评审的准则：

是否适用于实施环境

是否能够实现业务流程

架构是否合理、是否适合开发

**概要设计评审**

参与概要设计评审工作的具体人员角色：项目经理、业务流程分析员、系统分析人员、架构设计师、设计员、数据库设计员、记录员。SQA小组会审核参与评审的人员的资格，以确保评审的有效性。

概要设计评审的准则：

是否满足软件需求说明书的功能要求和非功能要求；

是否符合软件架构的要求

设计是否合理；

与公司的其他相关系统接口是否合理；

**详细设计评审**

参与详细设计评审工作的具体人员角色：项目经理、系统分析人员、架构设计师、程序员、记录员。SQA小组会审核参与评审的人员的资格，以确保评审的有效性。

详细设计评审的准则：

是否符合软件架构的要求

是否满足概要设计的要求

设计是否合理；

是否适合开发

**数据库设计评审**

参与数据库设计评审工作的具体人员角色：项目经理、业务流程分析员、系统分析人员、架构设计师、设计员、记录员。SQA小组会审核参与评审的人员的资格，以确保评审的有效性。

数据设计评审的准则：

是否符合软件架构的要求

设计是否合理、高效率；

是否包含所有业务数据；

是否利于程序编写。

**代码评审**

参与代码评审工作的具体人员角色：项目经理、设计员、数据库设计员、测试人员、记录员。SQA小组会审核参与评审的人员的资格，以确保评审的有效性。评审人员会针对程序员开发出来的代码按模块进行评审。

代码评审的准则：

是否符合概要设计、详细设计的要求；

是否符合相应的代码编写规范；

是否能够实现设计的要求；

代码实现方式是否合适；

**测试评审**

参与测试评审工作的具体人员角色：项目经理、系统分析人员、设计员、数据库设计员、程序员记录员。SQA小组会审核参与评审的人员的资格，以确保评审的有效性。

测试评审包括对单元测试、集成测试、系统测试的评审

单元测试评审的准则：

是否符合详细设计的规定

单元内部结构是否合理

是否能够实现指定的功能

集成测试评审的准则：

是否符合详细设计的规定

是否能够按照集成方案进行集成

各个构件是否能够按照设计中既定的意图、目的组合一起协作运行。

系统测试评审的准则：

是否实现软件需求中的所有的功能

整个系统能否按既定意图运行

**实施方案评审**

参与实施方案评审工作的具体人员角色：客户、项目经理、架构设计师、设计员、数据库设计员、系统实施人员、记录员。SQA小组会审核参与评审的人员的资格，以确保评审的有效性。

实施方案评审的准则：

是否符合系统架构的要求；

是否能够有效的进行新系统的构建；

是否能够很好的协调不同系统间的整合；

是否能够很好的完成原有系统的割接；

持续改进

**概述**

ISO管理体系的一个主要思想就是持续改进PDCA，即为Plan-Do-Check-Action（计划－执行－检查－措施）。质量管理的目标是顾客满意。顾客需要在不断地提高，因此，企业必须要持续改进才能持续获得顾客的支持。

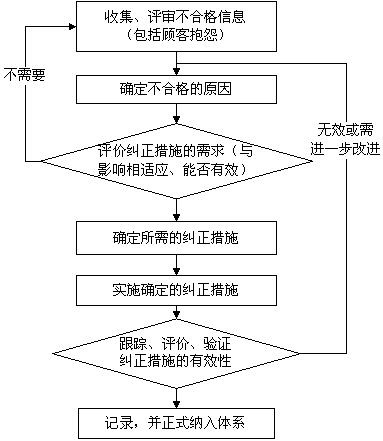
故为了搞好质量改进，我们公司高层领导对质量改进给予足够的重视，严格贯彻ISO质量管理体系的思想，进行ISO9001：2000标准的培训和对本公司形成的质量体系进行培训，将所有的规范、措施等等落实到个人，创造了良好的环境。使全体职工对质量改进形成和保持一种共同的观念和行为。在质量改进中全面贯彻了预防为主的思想，制定了各种预防和纠正措施。

公司全体员工本着从预防问题发生着手，而不是等出了问题、造成了质量损失再去改进的思想，积极地和准确把握进行质量改进的机会，为企业进行持续的质量改进奠定良好的基础，有效地保证了软件质量。

除了需要关注预防问题的发生外，还必须对已出现的问题进行纠正和管理，我们公司制定了一套缺陷跟踪管理的方法，对于不合格品的识别、评审和处理都有相关的ISO质量体系的程序文件做了相关的规定。

**纠正流程**

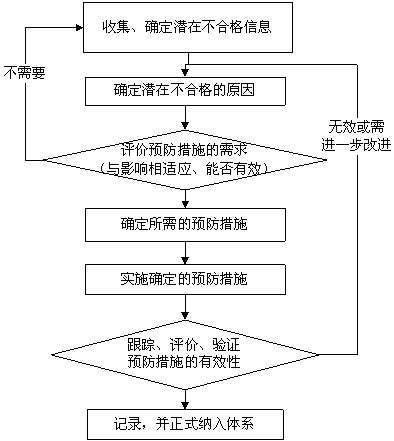
根据持续改进的思想，我们公司制定了以下的纠正流程：



在管理过程中发现的不合格信息，由不合格发现人生成不合格报告发给问题相关人员进行分析决定是否需要进行纠正，若是需要进行纠正，则制定纠正措施明确责任人和完成的进度，然后由责任人实施纠正措施，纠正完成后，由项目管理者评定纠正措施是否有效，若是有效则由质量管理人员记录并正式纳入体系。若是无效则重新确定不合格原因，重新根据流程纠正问题直到问题不存在。

**预防流程**

根据持续改进的思想，我们公司制定了以下的预防流程：



在管理过程中发现的不合格信息，由不合格发现人生成不合格报告发给问题相关人员进行分析决定是否需要建立预防措施，若是需要进行预防，则制定预防措施，然后由责任相关人员实施预防措施，由项目管理者评定预防措施是否有效，若是有效则由质量管理人员记录并正式纳入体系。若是无效则重新确定不合格原因，再次进入流程直到预防措施有效。

# 验收标准和实施方案

## 验收标准

### 验收承诺

我司将会严格按照用户的要求开展验收工作。我们负责在项目用户验收前将系统的全部各种相关的系统软件，各阶段开发文档，运行稳定可靠的本系统及其安装程序，注释清晰明了的、能够编译生成生产环境下正常运行的应用程序的源代码，以及有关产品和系统说明书、安装手册、技术文件、资料、及安装、测试、验收报告等文档汇集成册交付项目单位。只有文档齐全后才予以组织验收。

对整个项目的验收包括检查整个系统是否实现了采购人在本标书中所要求的功能，是否与中标人提出的解决方案中既定目标功能完全一致。

我们将依据项目总体设计目标和中标人的解决方案，随工程进展提出分阶段验收规范，作为工程分阶段验收的最后依据。

我们将根据系统总体设计方案提出验收方案和验收文档清单（包含需求调研、系统分析、软件设计、软件开发、系统测试、实施上线、运行维护等阶段），采购人将根据验收方案对系统每个部分进行逐一进行项目用户验收。

本项目的最终验收由东莞供电局组织专家组进行验收。

### 验收的阶段

验收的阶段划分将根据采购人依据项目总体设计目标和我司提供的系统总体设计方案，随工程进展而分阶段地制定的验收规范进行，作为工程分阶段验收的最后依据。我司将会根据验收阶段的最后依据来完成验收工作。

### 提交文档的清单

对整个项目的验收包括检查整个系统是否实现了东莞供电局在本标书中所要求的功能，是否与东莞供电局提出的解决方案中既定目标功能完全一致。

东莞供电局应依据项目总体设计目标和成交供应商的解决方案，随工程进展提出分阶段验收规范，作为工程分阶段验收的最后依据。

我们根据系统总体设计方案提出验收方案和验收文档清单（包含需求调研、系统分析、软件设计、软件开发、系统测试、实施上线、运行维护等阶段），东莞供电局应根据验收方案对系统每个部分进行逐一进行项目用户验收。

我司将按照标书的要求提交开发文档。提交的文档包括：

1. 软件需求说明书
2. 总体设计说明书
3. 数据库设计说明书（包含数据字典）
4. 试运行报告
5. 维护手册
6. 操作手册
7. 软件程序
8. 应用软件清单
9. 技术服务和技术培训等相关资料

当这些文档通过东莞供电局审查之后，我们将会按照采购方对验收的其他要求，准备相关的验收材料，并提交验收。由东莞供电局组织专家组进行验收。

## 实施方案

### 实施承诺

系统开发将严格遵照国家软件工程规范或国际公认的OO（面向对象，包括OOA、OOD、OOP）的方法进行。

我们在开发过程中提出合理的开发计划及详细的进度安排计划，在项目实施过程中进行追踪和控制，定时总结并提交开发进度月报。

我们将提供良好的软件质量保证机制，包括系统软件开发的规范化保证，要有统一的命名规范，良好的编码风格，统一的代码布局格式，详尽的程序注解等，对软件开发的各个阶段都要进行质量评审，并提供评审报告。

对软件的测试将贯穿于系统开发的始终，将提供详尽的测试计划、测试报告及结果分析报告。

我们承诺在系统建设和系统免维期中通过各种手段对系统进行不断的优化和调整，满足实际应用需要。

系统采用的系统软件、通用软件是具有在中国境内的合法使用权或版权的正版软件。本项目完成的系统设计、数据产品及所开发的应用系统，包括应用软件产品、各类文档等，版权属于东莞供电局，涉及到第三方提出侵权或知识产权的起诉及支付版税等费用由投标人承担所有责任及费用。

### 项目实施管理措施

为了保证项目能够按时、保质保量的完成，xxx公司在项目的需求分析、技术方案设计、技术方案实施、项目总体推进和售后服务方面对整体项目将进行全面的管理，措施包括：

（1）公司领导亲自牵头挂帅，从人力、财力、物力上进行最有力的实际保证，保证向客户提供符合质量要求的硬件设备和系统软件；

（2）抽调公司技术专家进行技术总体把关，保证整个系统设计方案的合理性、先进性、安全性；

（3）组织技术开发和工程实施经验的开发和实施队伍参与此项目；

（4）借鉴xxxx公司多个类似项目的建设经验，准确、深入调研需求，借助成熟的技术和设计思路，充分利用可重复利用的资源，保证整个系统顺利开发实施。

我公司针对本系统制定了一套完整的项目实施方案。整个项目的实施分为项目准备阶段、业务建模阶段、需求分析阶段、分析和设计阶段、编码实现阶段、测试阶段、部署阶段和项目收尾阶段。并在项目的开展过程中全程对其进行项目管理。以实现既定的项目目标、保证项目的成功、取得项目干系人最大程度的满意。

### 项目实施方案

**1、项目准备阶段**

项目准备阶段主要工作是根据系统建设的需要，组建项目开发团队和开发环境的准备工作。其中开发环境的准备是指项目经理组织相关人员根据系统建设的需要建立开发环境，建立标准开发过程。并制订统一开发规范，包括命名规范，业务建模规范，需求编写规范，设计规范，编码规则，测试指南等。

**2、业务建模阶段**

项目团队通过系统建设相关的业务处室组成的用户代表进行业务调研工作，了解系统建设项目的业务流程及其业务需求，并且得到用户的确认。

**3、需求分析阶段**

项目团队通过需求来描述系统功能需求，并使开发人员和用户就这一描述达成共识。经过需求分析后，项目团队编写需求说明书，并得到用户的确认。

**4、分析和设计阶段**

项目团队将需求转化成未来系统的设计，采用分层的方法，进行架构设计，并且在整个系统遵从统一的架构的原则下，经过分析和设计，得到实施模型。

**5、编码实现阶段**

项目团队通过实现过程中主要是以组件的形式实现类和对象，将开发出的组件进行单元测试和集成测试。

**6、测试阶段**

项目团队给出的测试计划和测试用例，与用户代表讨论通过后，方可按计划进行测试。系统每一项测试必须有详细的测试记录，测试过程的输出包括测试计划、测试记录和测试分析报告，阶段性的测试输出需要用户代表、开发商共同签字确认。

项目团队通过测试过程验证对象间的交互作用，验证软件中所有组件的正确集成，检验所有的需求已被正确的实现，识别并确认缺陷在软件部署之前被提出并处理。

测试工程师确定和描述要实施和执行的测试，制定测试计划。并完成测试用例的设计，并且核实系统是否符合原定的要求。

项目经理对于已经完成的测试用例组织一个有不同代表组成的专家小组，对测试用例进行仔细的检查，以验证测试用例能够覆盖项目所有的需求。

**7、部署阶段**

系统经过测试之后，项目团队提供完整的开发文档和用户支持文档，并协助用户将系统发布在用户相应的环境中。

系统实施人员制订部署计划并进行大量的准备工作， 以保证系统完成时， 能够在客户的使用环境下成功地部署系统。

文档编写人员生成部署时所需的材料，包括系统安装文档，用户手册，和培训材料等。

**安装系统：**系统安装人员将新建的系统部署到东莞供电局的网络上，并进行现场联调。

**系统整合：**系统安装人员将现有的部分业务系统进行数据整合，并进行现场联调。

**培训：**根据用户的需要， 项目经理会安排相关人员用幻灯片， 示例， 教程等方式编写培训教材， 并对用户进行必要的培训。

**试运行：**用户对系统所提供的功能进行实际的运行测试。

**验收：**系统实施人员确保按照“项目验收计划”进行测试时所需的所有软件和测试平台都已就绪。用户进行验收测试，并完成系统的移交工作。

**8、项目收尾阶段**

1）验收

依据项目合同及项目验收规范，由甲方组织相关的业务部门、专家以及开发方进行项目验收评审工作。项目验收通过，即象征此项目的开发和实施工作已经完成，将从此进入项目的售后服务阶段。我们将负责将系统的全部有关技术文件、资料及测试、验收报告等文档汇集成册交付项目单位。

2）总结

项目管理小组组织项目团队对项目进行总结。总结项目的开展情况以及在项目开展过程中获得的经验和教训。并得出总结报告，提交给公司的管理层。以供公司同事借鉴，并作为公司积累。

**9、项目文档管理**

1）文档管理的要求

我公司的系统开发是基于RUP的方法，严格遵照面向对象的方法进行组织的。所有文档的编写均需要按照相应模板进行编写，要符合相应的文档编写规范，所有软件工程阶段性文档由采购人组织评审，只有当本阶段的评审通过后才能进行下一阶段的工作。编写完成的文档要通过评审，然后提交相应的项目干系人，并且根据变更配置管理进行版本控制。

2）文档的范围

系统开发严格按照国家软件工程规范进行，根据开发进度及时提供有关文档，最终提供的软件产品包括各种相关的软件系统、各阶段开发文档、运行稳定可靠的本系统安装程序、注释清晰明了的能够编译生成目前正在运行的应用程序的源代码等。

3）项目文档移交

本项目所有需要向业主提交的文档由专门的文档管理人员在项目建设期间对文档进行检查和管理，并随时供采购人查阅，项目最终验收后全部移交采购人。

# 整体项目工期计划

由于本项目复杂程度高，制作难度大，质量要求高，我公司对此项目格外重视，并将调动公司全部资源来保证本项目的顺利实施，依据本项目执行的可行性与合理性，特制定了如下时间规划方案：

|  |  |  |  |
| --- | --- | --- | --- |
| **系统模块** | **子模块** | **开始时间** | **结束时间** |
| 需求分析 | 新增需求的整理 | 2017年6月 到2017年7月 | |
| 系统设计 |
| 系统数据优化 |
| PC端 | 组织架构 | 2017年7月 到2017年8月 | |
| 用户管理 |
| 物资管理 |
| 借出管理 |
| 归还管理 |
| 物资盘点 |
| 物资查询 |
| 操作日志 |
| 报表查询 |
| PAD端 | 用户读取 | 2017年8月 到2017年9月 | |
| 用户登录 |
| 物资借入 |
| 物资归还 |
| 微信端 | 用户登录 | 2017年8月 到2017年9月 | |
| 用户绑定 |
| 物资查询 |
| 借入查询 |
| 归还查询 |
| 微信通知 |

**<全文完>**