技术附件

通州区节水事务中心节水管理平台

技术方案

甲方：

乙方：

日期：2018年8月

前 言

本技术方案是在2017年建设成的通州区远传水表数据采集系统基础上升级改造方案，原系统功能目前已经完成一期水表数据采集功能，现阶段需要对已采集数据进行在线加工汇总、统计展现和开放权限需求，现阶段第二期升级方案需满足如下设计原则：

采用业界成熟的解决方案，采用BS模式，建立软件系统，建设统一的业务处理体系。

**先进性：**以促进工作安全发展为指导原则，确保系统成熟稳定的同时放眼未来迎合发展。

**兼容性：**系统平台为开放式、标准化平台，满足未来本单位各服务构建及各机关单位服务及应用的无缝对接。

**安全性：**系统应对数据库的存储和访问提供有效的安全措施，防止数据链及数据通讯链受到恶意攻击，访问调用有痕且追溯可查。

**可扩展性：**系统的构建及数据的交互满足共享模式，采用灵活、开放的模块化设计为系统扩展、升级及可预见的管理模式的改变留有余地。

**可靠性：**多维度确保系统的正常运转与数据安全可靠。

**经济性：**实现最优化的系统设备配置，降低系统造价及运营成本。

**易用和易维护性：**系统应采用简洁、友好的人机界面，在出现系统故障时，能够简便快捷的进行处理。

**共享性：**系统共享性的要求为了保障各业务体系间的数据流转的流畅且在安全性保障的前提条件下，构建协同校验、统一管理的建设精神。

# 技术指标

## 技术路线

* 应用平台：平台系统遵循JAVA EE或.NET标准；
* 运行模式：B/S模式的架构；
* 扩展接口：基于Web Service、JSON等标准规范，采用XML的数据传输格式；低耦合应用组件进行分布式部署、组合和使用，具备未来可扩展增减业务模块的架构；
* 安全架构：符合HTTPS的安全架构；
* 操作系统：支持UNIX、LINUX和Windows操作系统；
* 权限控制：基于角色的访问控制RBAC模型的权限控制，可动态支持功能操作权限和数据访问权限灵活配置；
* 登录模式：支持单点登录与统一安全认证、支持数字证书验证；
* 系统架构：分布式系统基础架构，采用基于Hadoop技术或其它类似技术的大数据处理框架；

## 系统架构

系统采用Browser/Server的B/S模式（浏览器/服务器模式），服务器端采用Windows Server版操作系统。网络中心配备若干台高性能服务器，实行应用和数据分离的原则，加强系统运行的稳定性和安全性。服务器采用Windows Server2003以上版本，后台采用SQL Server数据库，前后台开发工具采用.net等。

整体系统分为：基础设施层（系统所需的基础设备、系统、中间件等）、资源层（实现具体功能的各种数据与信息库）、应用支撑层（对所有应用系统提供各种数据访问功能的中心服务系统）、应用系统层（实现具体功能的各种应用系统）、服务层。

资源层提供集中的数据访问，包括数据连接池控制、数据库安全控制和数据库系统。集中的数据访问能够在大量用户同时并发访问时共享有关连接等信息，从而提高效率，集中的数据库安全控制，使任何来自互联网的数据库访问都必须经过强制的安全管理，不允许直接访问数据库的行为，杜绝安全隐患。

应用层通过提供统一的数据服务接口，为各个应用系统提供服务，应用系统的表现可以是网站、客户端系统、Web服务以及其他应用。并通过目录与负载均衡服务提供统一的负载均衡服务。任何一个应用服务器都可以同时启动多个服务，而通过目录与负载均衡服务来进行负载均衡，从而为大量用户并发访问时提供高性能服务。信息集成分析平台应用服务器提供核心服务，包括数据服务、管理服务、基本安全服务、其他业务服务等；数据同步服务器将数据有条不紊的同步到各个数据库；系统更新与版本升级服务器提供各个系统的版本升级管理，使任何一个系统都保持最新版本；Web日志分析服务提供用户访问分析，提高平台后期修改、维护、更新的针对性。

## 系统安全

（1）基于用户角色的权限控制实现应用层安全。

一是严格控制不经授权的用户访问系统。二是每个合法访问系统的用户都具备一定的权限，以限制其操作范围。在业务系统操作时，只有具备相应业务系统操作权限的人员，才可办理相应的业务。将结合统一用户与权限管理实现基于用户角色的权限控制实现应用层安全。

（2）权限管理方案

对岗位（角色） 的授权分为两个部分，一是业务操作的授权，菜单功能授权，二是数据的授权。通过管理员对分部门进行分别设置不同的角色，通过各种角色进行分配菜单和功能的权限，以及设置不同的数据权限。

（3）加密策略

加密主要包括数据的加密传输和数据的加密存储。

对于普通数据加密传输，可以通过SSL 加密在 Internet 上传输，保证数据不被窃取。

对于保密程度较高的信息可以加密存储，提供一个加密模块，采用 RSA 加密算法进行加密。通过加密模块，用户可以选择需要加密的数据表并存储下来。所有需要加密的数据表的数据在存储之前都需要通过加密模块检测，如果数据需要加密存储，则调用加密算法进行加密，加密后的密文存放倒数据库中；如果不需要加密，则直接存储明文。同样，在调阅数据的时候，如果是加密数据则通过加密算法进行解密还原成明文，展现在用户面前；否则直接提取数据展现在用户面前。

（4）信息保密

由于网络的互联性和开放性，信息在网络中的传输不可避免地存在被监听的可能，要实现信息传输的保密性只有对信息进行加密，以密文方式传输，即使被监听，监听者也无法明白密文所表示的信息。平台对采集或传输的数据按照标准的加密组件进行了数据的加密，当数据到达后由对应的解密组件进行解密，提供了信息的加解密机制。

信息也可能在传输过程中被截获篡改后再转发出去，造成信息的完整性受损，平台安全管理平台对接收后数据采用完整性校验算法进行完整性校验，被改动的信息即被认为是无效信息，并对无效信息进行丢弃不予保存，以此保证信息的完整性。

（5）数据备份

对于系统，应对重要数据服务器进行一次完全的系统的灾难备份，将系统及其上数据（成果数据或非成果数据）完全备份到磁带库中，将灾难备份介质按照介质安全措施安全保存。

对于成果数据，我们建议进行一次完全备份， 在完全备份的基础上进行差量备份。这主要是因为成果数据不经常被修改的缘故，备份起来比较方便。

对于非成果数据，我们建议进行一次完全备份，在完全备份的基础上进行增量备份，建议每进行一次修改后就进行增量备份，标记介质后保存好增量备份的磁带介质。

## 性能指标

(1)查询指标：简单查询：单类信息精确条件查询，要求响应时间小于3秒；关联查询：基于要素的不少于5类信息查询返回不大于5秒；组合查询：基于多条件组合查询，每1000万数据规模要求响应时间不大于1分。

(2)稳定性指标：系统平均无故障（影响业务正常办公的系统故障）时间≥300天。

(3)统计分析性能要求：常规统计报表生成时间≤1分钟；定制统计报表生成时间≤10分钟。

## 数据建设

平台数据量主要是检测数据，在不影响系统使用的情况下，通过扩展存储空间，适应未来业务数据容量的增长。

## 信息安全

* 文件加密：整个系统的文件支持三级加密策略：不加密；中度加密；深度加密加密方式由管理员直接配置，满足不同用户的需求；
* 密码加密：用户的密码在存储时进行不可逆的加密，保证了密码不会外泄。即使是管理员也无法获取用户的密码信息；
* 验证码：采用用户名+验证码登录模式登录系统；
* 加密锁：提供用户端加密锁，只有待有加密锁的用户才可以访问交互系统，适用于内外网分开控制；
* 新一代自主研发的云存储架构、数据冗余式备份、数据加密存储，确保数据存储安全；
* IPS入侵防御系统、内外网分离构架、SSL加密传输技术等，确保数据传输安全；
* 完善的安全管理制度，强大的多级权限管理功能，防止用户数据泄密，确保管理行为安全；
* 内外网分离架构，各模块采用独立内外网架构，以及冗余分布式设计，无单点故障，为系统对系统灾难的抵抗能力和恢复能力提供了保证；
* 支持HTTPS通道访问加密和防DOS攻击，记录访问请求日志，通过HTTPS保证传输信息加密安全性。同时可以防止蜘蛛爬虫的信息采样；
* 支持SSL传输加密POP/SMTP服务器收发邮件，SSL协议位于TCP/IP协议与各种应用层协议之间，为数据通讯提供安全支持，保证邮件传输过程中的信息不泄漏，包括用户的用户名、密码、信件等信息都会非常安全。SSL服务器证书由全球最大的安全证书机构verisign颁发。
* 完善的应用级别权限控制：基于个人、单位、部门、群组、角色、岗位、级别的多维度权限控制，系统可以针对以上属性进行灵活的权限设定，确保信息安全的可定义性和可执行性；
* 三员分离安全控制：为避免单一系统管理员的权限过于集中，引发风险，管理员将权利进行拆分，设立了三类管理员：系统管理员、安全管理员、审计管理员。系统管理员主要负责系统的日常运行维护；安全管理员主要负责账户管理、信息设置和分级授权；审计管理员主要对系统管理员、安全管理员和普通用户的操作行为进行审计跟踪分析和监督检查。通过这种分权管理，相互制约，相互监督的机制，可以满足国家对于涉密单位的信息系统专门制定了安全登记保护密码安全控制；
* 账号密码的更换周期控制：密码尝试失败的账户冻结控制；密码强弱度的校验等措施，有效保证了用户密码的安全使用；
* 定期对存储数据库进行自动备份。
* 操作日志监控功能，用户操作行为日志全程记录。
* 防SQL注入、页面篡改。

## 执行标准

**推荐**

* 《信息技术开放系统互连网络层安全协议》（GB/T 17963）
* 《软件工程术语》（GB/T 11457-1995）
* 《计算机软件可靠性和可维护性管理》（GB/T 14394-2008）
* 《计算机信息系统安全等级保护网络技术要求》（GB/T 387-2002）

**基础标准**

* 《信息技术软件工程术语》（GB/T 11457-2006）
* 《计算机软件开发规范》（GB 8566-88）
* 《信息处理各种图的文件编辑符号和约定》（GB/T 1526-1989）
* 《信息处理系统计算机系统配置图符号及约定》（GB/T 14085-1993）
* 《信息技术软件维护》（GB/T 20157-2006）
* 《信息安全技术-信息系统通用安全技术要求》（GB/T 20271-2006）
* 《信息技术软件生存周期过程开发标准》（GB/T 8566-2007）
* 《信息技术软件生存周期过程》（GB/T 8566-2001）
* 《软件支持环境》（GB/T 15853-1995）
* 《软件维护指南》（GB/T 14079-1993）
* 《算机过程控制软件开发规程》（SJ/T 10367-1993(2009)计）
* 《信息技术软件包质量要求和测试》（GB/T 17544-1998）
* 《计算机软件测试规范》（GB/T 15532-2008）

**文档标准**

* 《计算机软件文档编制规范》（GB/T 8567-2006）
* 《计算机软件产品开发文档编制指南》（GB/T 8567-1988）
* 《计算机软件需求规格说明规范》（GB/T 9385-2008）

**管理标准**

* 《计算机软件配置管理计划规范》（GB/T 12505-1990）
* 《软件工程产品质量》（GB/T 16260-2006）
* 《计算机软件质量保证计划规范》（GB/T 12504-1990）
* 《计算机软件可靠性和可维护性管理》（GB/T 14394-2008）
* 《信息技术软件生存周期过程风险管理》（GB/T 20918-2007）
* 《信息安全技术-信息系统通用安全技术要求》（GB/T 20271-2006）

**规范**

* 《计算机信息系统集成资质等级评定标准（最新）》
* 《计算机信息系统集成项目经理资质管理办法》

二、技术需求及方案

1. **系统概述**

节水管理平台由电脑端和微信小程序两部分组成，其中电脑端已在第一期完成部分功能，本期主要是电脑端平台改造、手机微信小程序开发，以及电脑端与手机端衔接的部分新增内容。

1. **需求说明**

通州区远传水表采集系统（一期）目前已完成与辖区内部分供/用水单位远传水表建立长期稳定的水表读书采集与数据展示等相关业务。主要功能可分为如下几个部分：

* 1. 基础信息：可录入单位信息、水表信息、水井信息、用水指标等
  2. 导航地图：地图标记用户位置
  3. 实时数据：远传水表定期进行表底数上报，系统自动计算净用水量，对水表进行状态分类，从未上报水表判定为未启用状态；48小时未上报判定为异常状态；净用水量为0判定为停用状态、水量以正数递增为正常状态；
  4. 读数查询：展示远传水表每次上报的表底数；
  5. 日用水量：按日展示远传水表的用水量；
  6. 月用水量：按月展示远传水表的用水量；
  7. 年用水量：按年展示远传水表的用水量

本期将在一期基础上增加统计报表模块、站内信模块、执法记录模块、用户查询模块、以及其他更改项更改，详细内容见下表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **平台** | **模块** | **页面** | | **详细说明** | **备注** |
| **PC端** | **实时数据** | **实时数据** | | 停用表为48小时累计和为0的表 净用水量为负数的表判断为异常 去掉添加、编辑、删除功能按钮 根据登录用户身份显示该用户所在单位的实时数据及新增查询条件及导出功能 |  |
| **导航地图** | **地图** | | 用水量统计方式更改为净用水量累加方式 |  |
| **基础信息** | **单位信息** | | 增加新单位编号、备注字段，添加、编辑删除界面相应修改，导入导出相应修改 位置信息改为可编辑，位置标记地图页面增加搜索功能（或去掉标记页面） |  |
| **水表信息** | | 添加编辑水表页面去掉单位编号，增加单位名称，可根据关键字选择 水表属性写成数据字典，相关内容改为选择 增加厂家字段，增加备注字段；添加编辑界面相应更改 |  |
| **水井信息** | | 添加编辑水井页面去掉单位编号，增加单位名称，可根据关键字选择 |  |
| **用水指标** | | 添加编辑用水指标页面去掉单位编号，增加单位名称，可根据关键字选择 |  |
| **统计查询** | **采集日志** | | 暂无 |  |
| **读数查询** | | 增加单位类型筛选项 添加、编辑页面、去掉单位编号、水源类型，增加单位名称，输入关键字后可选择单位； 表计地址根据单位名称筛选下拉选择。 根据登录用户身份显示该用户所在单位的各个水表读数查询及新增查询条件及导出功能 |  |
| **日用水量查询** | | 默认查询当日用水量 用水量采用净用水量累加方式统计 增加查询用量排序功能 添加所属乡镇筛选选项； 根据登录用户身份显示该用户所在单位的日用水量及导出功能 |  |
| **月用水量查询** | | 默认查询当月用水量 用水量采用净用水量累加方式统计 增加查询用量排序功能 添加所属乡镇筛选选项； 根据登录用户身份显示该用户所在单位的月用水量及导出功能 |  |
| **年用水量查询** | | 默认查询当年用水量 用水量采用净用水量累加方式统计 增加查询用量排序功能 添加所属乡镇筛选选项； 根据登录用户身份显示该用户所在单位的年用水量及导出功能 |  |
| **统计报表** | **状态统计** | | 单位数量统计  单位状态统计  一期二期分开统计，可按注册时间区分，也可在相应表中增加字段区分 |  |
| 水表数量统计  水表状态统计  一期二期分开统计，可按注册时间区分，也可在相应表中增加字段区分 |  |
| **用量统计** | | 日用水量统计，日用水量显示之前30天 |  |
| 日供水量统计，日供水量显示之前30天 |  |
| 月用水量统计，月用水量显示之前12个月 |  |
| 月供水量统计，月供水量显示之前12个月。 |  |
| **按日统计** | | 以日为横坐标，统计用水量 |  |
| **按月统计** | | 以月为横坐标，统计用水量 |  |
| **按年统计** | | 以年为横坐标，统计用水量 |  |
| **按单位统计** | | 以单位为横坐标，统计用水量 |  |
| **按行业统计** | | 以水表属性为横坐标，统计用水量 |  |
| **按水源类型统计** | | 以水源类型为横坐标，统计用水量 |  |
| **按乡镇统计** | | 以乡镇为横坐标，统计用水量 |  |
| **站内信** | **消息** | | 可经给指定用户发送站内信 管理员权限要求  可以查看站内信记录 用户收到站内信后有未读标记，阅读后取消 可快捷选择所有人，可按单位选择接收人 |  |
| **首页公告** | | 暂无 |  |
| **现场执法** | **执法记录** | | 可以查看、更改、删除现场执  可按单位、人员、时间查寻执法记录 |  |
| **系统管理** | **用户管理** | | 用户公司关联页-用户模块改造 新增维护微信账号登录授权信息模块页 |  |
| **其他更改项** |  | | 回车键功能为导出，需要更改统一到搜索 | 所有页面检查一遍 |
|  | | UDP协议解析方法更改 | 益都水表协议 |
|  | | TCP协议更改 | 京源水表协议 |
|  | | 异常处理，超过48小时算异常 |  |
| **微信小程序** | **登录** | | **微信登录** | 微信授权登录  微信绑定系统中已有账号 微信授权登录后，关联现有账户，获取现有账户权限 |  |
| **站内信** | | **消息** | 显示发送给自己的消息内容 |  |
| **公告** | 显示公告内容 |  |
| **水表查询** | | **实时数据** | 根据权限读取权限范围内的水表的实时数据和状态判断 登录后显示实时数据页面，点击表计地址调用读数查询页面，点击地址链接调用公司信息经纬度调用第三方导航。 |  |
| **读数查询** | 显示该表的历史读数，读数页面上方取30次数据画折线图，下方列表显示每次读数，最下方点击更多记录可显示更多，每次加载30条。 |  |
| **用量查询** | | **按日查询** | 可查询管辖单位日用水量 |  |
| **按月查询** | 可查询管辖单位月用水量 |  |
| **按年查询** | 可查询管辖单位年用水量 |  |
| **现场执法** | | **执法上报** | 标题、内容、执法人、时间、定位、照片 管理员权限 |  |
| **执法记录** | 管理员可查看所有人的记录 |  |
| **个人中心** | | **个人信息** | 显示用户信息、及用户相关功能 |  |
| **单位信息** | 显示管辖单位信息  点击地址可调用导航 |  |

**3 项目开发测试**

根据需求和设计方案，组织人员完成编码、测试工作。本阶段的主要活动是：

1. 根据需求文档和设计文档进行编码和自测。在设计方面完成功能设计、界面设计和系统管理设计；完成单元内测试和系统测试；
2. 编写项目使用手册；
3. 提交《项目使用手册》，双方对提交的文档认可；

三、运维服务

## 运维服务

项目第一期运维服务：2017年 月 日至2018年 月 日；

项目第二期运维服务：2018年 月 日至2018年 月 日。

### 系统硬件运维

系统部署在云端服务器，采用租用托管服务器方式。

目前由乙方申请的云端服务器，二期完成后，甲乙双方共同运维云端服务器。

### 操作系统管理

1) 空间管理：每周定期检查操作系统各分区使用情况，提供空间预测报告。

2) 性能优化管理：每月定期磁盘清理、整理磁盘碎片、系统参数优化形成系统变更记录表。

3) 日志管理：每周定期检查系统日志，及时预防处理潜在的问题形成日志检查报告。

4) 补丁管理：定期的补丁维护及时更新最新补丁，与最新补丁可更新时间不能超过2周，形成系统变更记录表。

5) 日常巡检：定期系统巡检，形成系统日常巡检记录单

### 数据库管理

1) 备份恢复管理：提供周期性的自动数据备份及恢复测试（频率以具体备份策略而定），形成备份记录及数据有效性报告。

2) 应急恢复服务：提供2小时内的系统紧急意外情况的应急恢复服务并形成事故报告单。

3) 性能优化管理：定期做系统性能监控，及时调整系统参数并形成数据库变更记录表。

4) 空间管理：定期检查数据文件大小，及时处理空间需求并形成空间预测报告。

5) 日常巡检：日常性的检查数据库日志，预防潜在的问题，形成巡检记录。

### 应用系统维护

1) 系统性能优化：定期做应用系统的性能监控，及时调整应用参数并形成应用配置变更表。

2) 系统用户权限管理：用户权限维护，并形成用户权限清单及权限变更记录（要有相应的权限申请流程）。

3) 系统日常巡检：日常性的检查应用系统日志，预防潜在的问题，形成巡检记录。

4) 系统变更管理：涉及系统变更的均需要在测试系统测试通过形成测试记录，才能在正式系统应用更改并形成正式系统变更记录表。