

# 延伸企业内部业务的移动信息平台功能应用设计及安全措施

杨君中<sup>1</sup>, 王 聪<sup>1</sup>, 谭 晶<sup>2</sup>

(1.泰州供电公司, 江苏 泰州 225300; 2.江苏电力信息技术有限公司, 江苏 南京 210024)

**摘 要:**文中针对电力企业安全生产和优质服务工作需求, 结合移动公众平台和运营商 APN 虚拟专网两种数据发布方式特点, 设计了移动信息平台功能应用方案, 并对有关安全防护措施做了探讨。

**关键词:**移动信息平台; 功能设计; 安全措施

## 0 引言

电力企业信息化已深入应用到安全生产及优质服务各个环节, 业务流程贯穿的部门、人员数量众多, 为保障流程贯通, 彼此协调配合、即时交流的要求也越来越高。随着移动通信技术的快速发展, 移动网络已通过手机终端全面融入人们的生活, 通过建立一个与企业内部信息系统紧密集成的移动信息平台, 与各专业部门日常业务工作相结合, 将桌面 PC 业务延伸至移动终端, 充分发挥 PC、手机、平板电脑等终端的各自优点, 定制挖掘企业数据, 推送内部信息, 则接收人员无论何处, 无论何时, 都能实现全方位沟通、互动, 保持全天候的信息畅通<sup>[1]</sup>。

## 1 移动信息平台功能应用设计方案

移动信息平台由企业内网及其信息系统、企业外网及数据服务器、DMZ 区信息发布服务器、信息安全防护设施、信息发布通道(本文指移动公众平台、运营商 APN 虚拟专网)、接收移动终端(客户端)等几个部分组成, 如图 1。

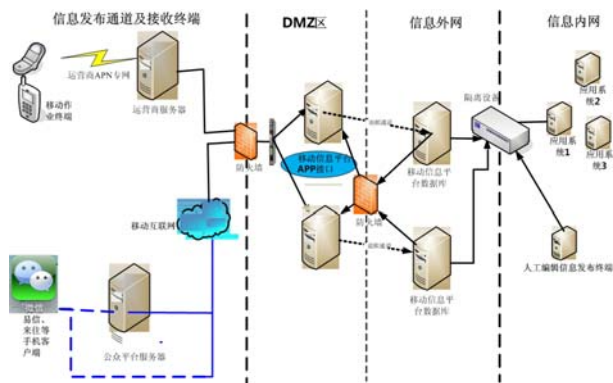


图 1 移动信息平台架构图

按照移动信息平台处理信息的业务性质、接收终端类型等特性, 企业内部业务信息数据完成采集加工后, 可选择“移动公众平台”、“运营商 APN 虚拟专网”两种数据发布通道之一到达接收终端。

由于移动公众平台直接连接移动互联网, 考虑到网络安全因素, 只能容许从主站单向发布信息到终端, 不允许接收终端信息回馈。目前应用较广泛的移动公众平台有腾讯的“微信”、中国电信和网易的“易信”、阿里巴巴的“来往”等, 使用普通智能手机安装相关客户端, 即可接收发布的信息。

运营商 APN 虚拟专网是企业与运营商之间交换数据的专用数据通道, 在边界安全防护措施齐全的前提下, 可进行信息数据的安全双向交互, 无须担心其他攻击源。运营商 APN 虚拟专网由中国移动、中国联通、中国电信等运营商提供, 需定制开发专门的移动终端应用。

## 2 移动信息平台功能应用的主要特点

### 2.1 扩大企业业务覆盖范围

充分利用企业内部网络及相关管理信息系统等现有软硬件条件, 紧密结合安全生产、优质服务等关键业务, 从内部海量数据源中提炼定制并推送数据; 利用移动信息网无处不在的特性, 实现企业业务在时间、空间上的全面延伸, 打破固有办公环境及条件的限制, 拓展业务处理方式, 实现随时、随地的业务信息传达贯通, 最大限度提高企业整体工作效率。

### 2.2 处理过程安全可靠

相关信息数据的挖掘分析、整理加工、内部传输等过程全部在企业内部网络完成, 生成的最终数据也存储于企业内部服务器的数据库。最终推送结果数据都经过多次提炼, 内容精简, 尽可能去除无

关内容，减少企业内部信息流出。

### 2.3 业务类型决定数据交互方式

移动公众平台覆盖面广，用户基数大，但使用限制较多，适宜单向发布一些短小精悍的一般性事务通知、消息通告，以备忘提醒为目的；运营商 APN 虚拟专网开发灵活性高，可自动推送消息，也可双向数据互动，实现现场生产辅助操作等业务拓展功能，即时处理内部生产业务，加快企业生产作业流程的流转，为线路、电缆、变电、配电等外勤生产岗位人员提供有力工具。

## 3 移动信息平台主要功能

经过对电力企业办公室、营销部、客户服务中心、输变电运行工区、配电抢修工区、党群工作部等众多专业部门的功能需求调研，移动信息平台应用功能主要包括“信息发布”、“信息采集”、“移动作业”、“信息反馈”等方面功能。结合信息安全防护要求，移动公众平台仅适宜手工发布信息的功能，数据交互功能适合在运营商 APN 虚拟专网上实现。

### 3.1 基于移动公众平台的信息发布功能

受限于移动互联网的安全隐患及运营商的使用约束，移动公众平台不宜直接读取内部数据，手工推送发布消息，是扬长避短的选择。

#### 3.1.1 常用信息发布

定义通知公告、计划任务、备忘预警等发布信息模板，发送信息一般通过人工编辑或人工导入，设定为普通发布优先等级。包括：

一周会议通知、值班提醒、停电计划、计划检修任务、廉政宣传、督查公告、指标跟踪、信息公告等。

#### 3.1.2 紧急消息推送

定义紧急消息模板，推送重要紧急消息，设定为紧急优先发布等级。包括：

临时紧急会议通知、生产设备或线路重（超）载等重大缺陷、恶劣天气预警、重大保电时间及要求、紧急抢修任务等。

每个信息模板单独定义权限，授权特定管理人员，防止越权滥发消息。

#### 3.1.3 微网站发布

建立移动信息平台微网站，提供历史通知公告、备忘信息查询等资讯，方便用户随时查看。

设立“消息签收”栏目，收集移动公众平台的通知接收情况反馈。

### 3.2 基于运营商 APN 虚拟专网的数据交互功能

运营商 APN 虚拟专网相当于借助第三方移动基站资源，将企业内部网络无限延伸覆盖，为野外信息化作业创造了条件；而虚拟专网较移动互联网的安全系数更高，也为自动采集并推送企业内部信息提供了可能。

#### 3.2.1 消息自动推送

通过定制企业内部信息系统的共享数据总线或相应的接口程序，可以定期采集内网信息系统的数据信息，自动发布给相关接收群体及人员。

##### 3.2.1.1 待办事宜提醒

从企业内部信息系统中，自动读取安全生产管理系统等应用系统的待办事宜，发送给指定群体、人员，形成待办消息。

##### 3.2.1.2 工单任务提醒

收集生产管理系统、95598 客服系统等应用系统的作业工单、抢修单信息，按标准模板转换后，即时推送给指定群体、人员，形成待办任务。

##### 3.2.1.3 其他信息定制

根据需要，还可定制营销系统、ERP 系统、车辆管理系统等信息系统的数据信息，推送给指定群体、人员。

#### 3.2.2 移动作业支持

通过定制移动作业终端，还能利用运营商 APN 虚拟专网，获取企业内部设备台账、任务信息、检修记录、隐患记录等信息，为现场作业提供参考；也可在现场工作完成后，上传设备参数、作业处理结果、新的隐患记录等内容至企业内部信息系统，保持现场与后台数据的实时更新同步。

### 3.3 反馈回执功能

为掌握重要紧急通知、重大故障抢修等消息的送达情况，主站需要接收回执，以确认接收对象已知悉消息；此外，生产现场的真实信息能反馈至主站，也有利于专家远程会诊、故障判断等工作。

#### 3.3.1 通知消息的反馈

由于移动公众平台只能发布单向数据，不能直接接收回馈信息，可通过在微网站中，设置“消息签收”功能，实现通知消息的反馈功能。

#### 3.3.2 地理定位信息反馈

反馈移动作业终端地理位置的定位信息至主站，便于安监部门远程督查安全生产工作负责人到岗到位等情况。

#### 3.3.3 现场故障辅助诊断

现场故障复杂、工作人员无法判断设备故障时,可反馈现场照片、视频等内容回主站,由资深专家远程协助诊断,提高故障诊断时效性与准确性。

## 4 移动信息平台的安全防护措施

相对而言,移动信息平台是一个独立的辅助功能系统,主要依托原有信息化资源而建立,其运行状态不会影响其他相关系统,性能要求、数据备份、数据传输、不间断运行等运维要求较低;另一方面,移动信息平台也是一个涉及多个系统、跨越多种网络(运营商无线网络、企业内部网络等)的应用系统,由于将企业内部的业务信息延伸至移动网络,其对外部入侵攻击、数据泄露、身份冒用、非授权访问等风险防护就显得尤为重要。其安全防护内容包括:

### 4.1 边界安全防护措施

移动互联网边界要部署防火墙、网络访问控制、入侵检测系统、安全监控审计系统、防病毒系统等信息安全措施,防止从移动互联网或运营商边界非法进入企业内部网络<sup>[2]</sup>;内外网之间要部署单向隔离装置,防止企业内外网之间互联互通;运营商APN虚拟专网边界应部署安全接入平台<sup>[3]</sup>,严密监控审计移动终端接入,确保移动终端数据交换安全可靠。

### 4.2 系统安全防护措施

网络及安全设备、服务器操作系统、数据库等关键设施应按国家信息安全等级保护要求,采取漏洞修复、权限控制、访问审计等安全加固防护手段,保障系统安全。

### 4.3 移动信息平台的安全管理防护措施

#### 4.3.1 发布信息管理员的身份鉴别认证

应建立与企业内部信息系统关联的统一认证架构,继承其身份认证体系,强制访问保护,防止冒用用户身份。

#### 4.3.2 接收客户端的身份鉴别认证

应建立信息接收人员的安全审核及身份验证流程,通过短信、电话、密码等验证方式,审核验明接收者身份,并根据功能定义,绑定用户与接收内容板块,防止消息误发至错误的接收人员。

### 4.4 内容安全防护措施

#### 4.4.1 数据加密传输

使用国内密码算法,采用 HTTPS 加密通信,

避免信息被截获泄漏的风险。

#### 4.4.2 设置信息发布审批流程

建立审核发布流程,设立审核员角色,对重要信息进行审批后再发布。

#### 4.4.3 敏感信息过滤

建立敏感字过滤数据库,开发内容审查过滤功能,对“秘密、方案”等敏感关键字进行筛选过滤,匹配敏感字的信息将无法推送出去。

#### 4.4.4 转发内容限制

无论是移动公众平台还是运营商 APN 虚拟专网的接收客户端,都限定为只能接收主站推送的信息,客户端之间不能直接交流,也不能转发信息,防止内容被误发至无关人员。

## 5 结论

本文提出了一种延伸企业内部业务的移动信息平台功能应用设计方案,并探讨了所涉及的主要安全风险及应对措施。在实施应用中,还应该结合企业的内部管理要求,明确使用者的信息安全目标责任,建立配套考核机制及信息编辑操作标准规范,确保移动信息平台安全、可靠、有效的发挥应有作用。

### 参考文献:

- [1] 王志高,叶飞跃.移动环境下的企业信息平台设计[J].计算机工程,2008(8).
- [2] 王黎璐,王鸿宇.移动互联网安全分析[J].信息网络安全,2013(10).
- [3] 国家电网公司.国家电网公司生产管理信息系统移动作业应用接入规范[Z].北京:国家电网公司,2011.

### 作者简介:

杨君中(1974—),男,广西桂平人,高级工程师,从事网络及信息安全工作,E-mail: tzyjz@js.sgcc.com.cn;

王 聪(1986—),女,江苏泰州人,工程师,从事信息系统运维管理工作;

谭 晶(1984—),男,江苏南通人,工程师,从事信息化项目管理工作。