|  |
| --- |
| f |



中国南方电网有限责任公司

终端安全管控平台研发项目

可行性研究报告

楚雄供电局

2017 年 5 月

批 准：

审 核：

校 核：

编 写：

目 录

1 概述 - 1 -

1.1 项目背景 - 1 -

1.2 项目依据 - 1 -

1.3 项目目标 - 1 -

1.4 项目范围 - 1 -

2 国内外研究水平综述【可选】 - 1 -

2.1 国外发展状况及产品介绍 - 2 -

2.2 国内发展状况及产品介绍 - 2 -

3 现状及需求分析 - 2 -

3.1 现状分析 - 2 -

3.2 需求分析 - 2 -

4 项目必要性分析 - 3 -

5 项目总体方案 - 3 -

5.1 建设思路 - 3 -

5.2 业务范围 - 3 -

5.3 应用范围 - 3 -

5.3.1 功能框架 - 3 -

5.3.2 功能划分 - 3 -

5.3.3 功能说明 - 3 -

5.4 技术路线 - 3 -

5.5 部署方式 - 4 -

5.6 系统集成 - 4 -

5.7 软硬件平台资源需求 - 4 -

5.8 安全方案 - 4 -

5.9 运维管理建议 - 4 -

6 项目实施方案 - 4 -

6.1 实施策略及计划 - 4 -

6.2 实施任务分解 - 4 -

7 项目投资估算 - 6 -

7.1 投资依据说明 - 6 -

7.2 总投资 - 8 -

7.3 资金计划建议 - 9 -

8 项目效益分析 - 9 -

8.1 管理效益分析 - 9 -

8.2 经济效益分析 - 9 -

8.3 社会效益分析 - 9 -

9 项目风险及保障措施 - 10 -

9.1 建设风险及对策 - 10 -

9.2 实施保障措施 - 10 -

10 项目可行性分析 - 10 -

11 项目研究结论及建议 - 10 -

# 概述

## 项目背景

近年来，信息安全形势日益严峻。一是来自境内外敌对势力的入侵、攻击、破坏越来越严重。二是针对基础信息网络和重要信息系统的违法犯罪持续上升。不法分子利用一些安全漏洞，使用病毒、木马、网络钓鱼等技术进行网络盗窃、诈骗、黑客攻击等违法犯罪活动，利用木马和“僵尸网络”实施分布式拒绝服务攻击的威胁加剧，防范难度越来越大。

随着云南电网公司不断提高风险防范意识，建立健全了网络与信息安全体系，网络端和服务器端的安全防护得以有效提升。然而，针对桌面终端的安全管理上还有很大的不足，目前楚雄供电局在桌面终端管理上，从资产管理方面楚雄供电局通过南方电网的资产管理系统和云南电网的ITSM系统进行管理，这两种资产管理方式目前还是传统的台账式管理模式，桌面终端的硬件配置信息复杂，更换频繁，台账式管理模式，很难实现资产的准确统计，难以实现桌面终端的责任人、使用人动态管理。通过华为的NAC完成终端的网络准入和设备管理，采用赛门铁克安全软件和金山安全软件实现病毒查杀、漏洞修复等基础安全防护，桌面终端设备的运维管理、应用运维管理则通过委托第三方进行现场运维，而设备运维也仅限于桌面终端的硬件可用性运维，应用运维也仅限于保证用户登录业务系统的可用性，对桌面终端安全管理、和合规性管理等方面尚存在诸多空白。2016年楚雄供电局针对部分桌面终端的软硬件配置及运行数据进行了采集、统计分析，发现终端运行存在大量安全问题，其中安装游戏类软件370多台，开放共享目录的终端有808台；有247款程序在侦听端口和提供网络服务。在桌面终端的配置上、安装软件的规范性、运行软件的规范性，系统合规性方面存在很多潜在隐患，信息安全风险较大，目前缺乏有效的技术管控手段。

另外，当前的桌面终端运维服务主要分为三个方面，一个是硬件检修，桌面终端属于精密电子产品，且大多开机时间较长，工作环境等因素不可避免的导致桌面终端出现这样或那样的硬件问题，出现问题后轻则影响桌面终端的使用效果，重则发生系统不能启动或数据丢失；第二是软件环境运维，目前桌面终端使用的应用软件越来越多，CSGII相应业务系统的正常运行都需要对本地环境进行相应的设置，大多业务系统应用故障都是由于系统环境设置不正确或各类插件异常导致，这些业务系统环境问题对一线员工来说难度较大，需要相应技术人员现场处理；第三是操作系统环境运维，网省公司针对桌面终端安全管理的相关要求，都需要通过现场服务，对操作系统及相关应用软件进行相应配置或打补丁来实现。

总体来讲，硬件维修方面，供电局购置的桌面终端大多为国内外大厂产品，产品质量有保障，售后服务支持较好，硬件故障所占比例已逐年减少。但是软件环境和操作系统相关的故障以及信息安全配置方面的故障，却呈快速增长状态，由于当前只能通过第三方服务工程师进行人工现场运维，效率低、成本高。随着南方电网CSGII的推广实施，一线员工的工作越来越依赖信息系统，桌面终端的工作状况直接影响到一线员工的工作质量与工作效率，为保证桌面终端良好的工作状态，楚雄供电局每年投入大量的人力物力，针对桌面终端提供维修服务，由于桌面终端分布在楚雄供电局辖区内的1市9县，地域跨度大，当终端出现故障后，运维响应较慢，严重影响业务工作开展。

针对上述现状，楚雄供电局迫切需要开发一套针对桌面终端的安全管控及自动化运维的技术支持平台，通过技术手段解决楚雄供电局桌面终端安全管控和软件环境运维方面存在的问题，在降低管理难度的同时，提升桌面终端的规范化、标准化管理水平。

## 项目依据

1. 《中国南方电网有限责任公司发展战略纲要》
2. 《南方电网公司“十三五”信息化规划》
3. 《南方电网公司面向服务的信息技术构架（SOA）框架规范》
4. 《南方电网公司管理信息系统安全等级保护标准》
5. 《南方电网公司信息化项目管理办法》
6. 《南方电网公司信息系统建设管理办法》
7. 《南方电网公司信息安全保障体系》
8. 《南方电网公司信息化工作管理规定》
9. 《南方电网公司信息化项目管理办法》

## 项目目标

通过对国内外目前主流的企业内部安全管理软件进行分析，针对楚雄供电局桌面终端的安全管理现状和楚雄供电局信息中心对桌面终端的管控及运维需求，定制开发一套桌面终端安全管控平台，通过终端安全管控平台的建设，建立桌面终端运行规范策略，对桌面终端的实时运行情况进行监测，实现安全隐患情况进行远程运维管理及督察整改，完成楚雄供电局本部及下属10个县公司桌面终端的安全管控及自动化运维管理，具体项目目标如下：

* 桌面终端的硬件配置信息采集，通过客户端软件完成桌面终端设备的相应参数采集，包括设备信息，核心硬件信息如CPU、内存、主板、存储设备等。
* 桌面终端的应用信息采集，通过客户端软件完成桌面终端上安装的应用信息采集，配合软件黑白名单及应用运行策略，可实现定制化的客户端应用管控。
* 桌面终端的运行时信息采集，通过客户端软件完成桌面终端的资源占用情况如CPU占用率、内存占用率、网络流量、磁盘剩余空间等运行时信息，完成实时运行应用和进程相关信息的采集
* 实现终端安全管控，终端安全管控主要包括应用安全管控、信息安全管控、网络安全管控、系统安全管控等四个方面。
* 制定桌面终端管控策略，通过对桌面管控要求进行分析制定桌面终端管控策略，桌面终端管控策略保存在服务器，终端登陆后根据自身所属分组下载和执行相应的管控策略，实现远程自动化运维。
* 实现我局的桌面终端应用软件库，包含必备软件、办公软件及相关的业务软件及相应业务系统的一键修复工具。
* 实现桌面终端的远程协助功能，通过管理终端实现和任意一台桌面终端的远程协助功能，终端管理员通过远程协助对桌面终端进行远程运维。
* 实现桌面终端之间的文件共享功能，桌面终端用户可通过桌面终端管控客户端设置本地共享目录或共享文件，并可设置相应的权限，实现局内桌面终端之间的文件共享。

## 项目范围

业务范围：本项目涉及的业务部门包含楚雄供电局信息中心、下属各县公司的信息部门及桌面终端IT资产管理部门，覆盖的业务范围包括桌面终端IT资产管理、桌面终端运维管理、网络安全及信息安全等。

应用范围：本系统使用对象为楚雄供电局信息中心及下属单位桌面终端运维管理人员，系统覆盖楚雄供电局局本部及下属10个县公司。

开发范围：本项目是新项目，包括开发项目和实施工作。

# 国内外研究水平综述

目前针对桌面安全类产品有很多，技术也很成熟，产品功能主要集中在病毒木马查杀，系统漏洞修复等安全领域，如南方电网公司已经在用的国外产品赛门铁克安全软件，县公司层面在用的国内安全软件金山安全软件等，但能够实现对桌面终端应用及管控的企业内部信息安全产品则相对较少，少数几款内网安全产品，也更多的侧重于网络准入、行为管理和病毒查杀、漏洞修复等方面，如华为的AnyOffice、360天擎、北信源内网安全管理系统等，对企业用户桌面终端的应用管理、应用策略管理、桌面终端的运维管理及安全管控基本都未有涉及，尤其是针对企业内部业务系统的运维或安全服务支撑目前国内外都没有通用的产品。

## 国内发展状况及产品介绍

随着互联网的发展，传统的信息安全形式也越来越严峻，各种网络安全事件层出不穷，上至国家下至企业都对信息安全提出了更高的要求，通过多年的建设，云南电网公司对业务系统、核心网络设备、数据中心机房等信息安全做了大量的工作，取得了良好的效果，但针对分布范围更广，用户数量更大，使用场景更复杂的桌面终端安全管控却存在许多不足。

华为的AnyOffice，云南电网的网络准入就是采用的AnyOffice通过和防火墙配合实现NAC，AnyOffice主要核心思想是从身份和设备可识别（Identity）、数据不泄密（Privacy）和设备可管理（Compliance）三个方面帮助企业全面应对挑战，为企业提供业界最广泛的安全性和最简单易用的管理方案。云南电网的AnyOffice从应用上更多关注的是网络准入和设备管理。

360天擎终端安全管系统是360面向政府、企业、金融、军队、医疗、教育、制造业等大型企事业单位推出的集防病毒与终端安全管控于一体的解决方案。360天擎终端安全管理系统，以大数据技术为支撑、以可靠服务为保障，它能够为用户精确检测已知病毒木马、未知恶意代码，有效防御APT攻击，并提供终端资产管理、漏洞补丁管理、安全运维管控、网络安全准入、移动存储管理、终端安全审计、XP盾甲防护诸多功能。360天擎更多关注的是桌面终端的安全。

北信源VRV EDP终端安全管理产品针对网络管理工作中遇到的实际管理需求，进行网络安全资源规划,如防止移动设备非法接入内部网络、IP资源分配管理、静态IP同MAC地址的绑定、提供设备资源登记及硬件设备（硬盘、CPU、内存等）变化报警、进行内部网络连接阻断等功能。同时，为有效解决网络中计算机非法接入和非法外联问题， VRV EDP系统提供实时监控的强大功能，即实时报警以及实时切断非法计算机同内网的连接。北信源终端安全管理产品主要侧重于网络安全管理。

# 现状及需求分析

## 现状分析

近年来，信息安全形势日益严峻。一是来自境内外敌对势力的入侵、攻击、破坏越来越严重。二是针对基础信息网络和重要信息系统的违法犯罪持续上升。不法分子利用一些安全漏洞，使用病毒、木马、网络钓鱼等技术进行网络盗窃、诈骗、黑客攻击等违法犯罪活动，利用木马和“僵尸网络”实施分布式拒绝服务攻击的威胁加剧，防范难度越来越大。

近年来，云南电网公司不断提高风险防范意识，建立健全了网络与信息安全管理制度，然而，针对桌面终端的安全管理上还有很大的不足，目前楚雄供电局在桌面终端管理上，从资产管理方面楚雄供电局通过南方电网的资产管理系统和云南电网的ITSM系统进行管理，这两种资产管理方式目前还是传统的台账式管理模式，桌面终端的硬件配置信息复杂，更换频繁，台账式管理模式，很难实现资产的准确统计，难以实现桌面终端的责任人、使用人动态管理。通过华为的AnyOffice完成终端的网络准入和设备管理，采用赛门铁克安全软件和金山安全软件实现病毒查杀、漏洞修复等基础安全防护，桌面终端设备的运维管理、应用运维管理则通过委托第三方进行现场运维，而设备运维也仅限于桌面终端的硬件运维，应用运维也仅限于保证用户在用业务系统的可用性，对应用的安全管理、桌面终端的合规性管理等方面缺乏全面有效的技术手段，存在较大的安全隐患。桌面终端的运维工作都需要运维人员现场运维，运维效率低，成本高。

现有基础：

* 网络情况：目前楚雄供电局及下属县公司都在云南电网公司内网之内，实现了全网内网覆盖，随着2013年综合数据网IP网络改造、2013年局域网升级与优化等项目的实施，供电局的网络向万兆的升级，骨干层网络已实现万兆平台的升级，各县公司网络的接入带宽也升级到千兆。
* 设备情况：目前楚雄供电局信息中心机房已经简称虚拟化平台，可根据项目具体需要配置相应的计算资源和存储空间。
* 现有信息系统建设及应用情况：目前楚雄供电局准入系统采用华为的AnyOffice，安全软件局本部采用赛门铁克，县公司采用金山安全软件，部分用户还存在自主安装其它安全类软件的情况。
* 存在的问题分析：目前楚雄供电局在桌面终端的管控上，存在资产配置情况不清晰，资产责任人和使用人不明确，应用管理缺失，信息安全隐患大，桌面安全类软件功能重叠或相互独立，难以实现桌面终端的统一安全管理，桌面终端运维难度大、效率低，缺乏自动化运维或故障诊断的能力等问题。

## 需求分析

### 业务需求：

楚雄供电局终端安全管控与自动化运维平台，是楚雄供电局信息中心针对楚雄供电局桌面终端的管理现状，为解决楚雄供电局在用桌面终端资产管理、应用管理、运维管理及桌面终端安全管理上存在的问题而提出的定制化解决方案，通过该凭他平台的建设提升楚雄供电局桌面终端的管理能力，降低安全风险，消除安全隐患，提升桌面终端应用水平。

总的来讲，楚雄供电局终端安全管控平台的业务需求主要包含以下几个方面：

* **实现在用桌面终端的详细资产信息梳理**，通过在桌面终端部署数据采集程序对桌面终端的详细硬件配置信息进行采集，解决现有台账式资产管理不准确的问题
* **实现桌面终端的使用过程管理**，通过对桌面终端的准入USBKEY的识别和跟踪，解决桌面终端责任人、使用人无法准确定位的问题，实现设备与人的精确匹配。初步建立桌面终端与组织机构、人员岗位和访问权限的准确关联关系。
* **实现桌面终端的应用管理，**通过桌面终端安全管控平台客户端对桌面终端的已安装应用进行数据采集，配合应用的黑白名单，解决桌面终端应用安装随意，应用使用无管控的的问题，实现应用的安全管控。
* **实现桌面终端的运行时监控，**通过桌面终端安全管控平台客户端实时采集桌面终端的运行是状态，对桌面终端的性能、应用的运行等数据进行采集与分析，准确分析桌面终端的性能瓶颈，解决桌面终端更新无依据的问题。
* **实现桌面终端的合规性实时监测、修复、跟踪，**根据网省公司的桌面终端合规性要求，通过桌面终端安全管控平台对桌面终端的相应合规项进行实时检测，根据合规项检查策略进行报警、提示用户修复或自动进行修复，解决桌面终端合规性审查难、整改难、跟踪难的问题、提升楚雄供电局的信息安全管控、网络安全管控、系统安全管控的能力，全面提升楚雄供电局桌面终端的终端安全水平。
* **实现终端分级分类配置管理，**完成在线桌面终端的分级、分类、分组管理；完成桌面终端各类自动化运维策略的配置管理，如信息安全类配置、终端使用规范类配置。
* **实现桌面终端的故障自动诊断或远程诊断，**通过桌面终端安全管控平台自动对桌面终端的软硬件配置进行自诊断，在影响用户终端使用之前上报相应问题，或自动对相应问题进行修复，解决终端运维效率低、成本高的问题，从被动运维实现到主动运维，从事后运维实现到事前运维，通过本地生成诊断报告可对离网故障提供远程运维辅助支撑。
* **实现桌面终端的远程主动运维，**桌面终端的安全运维及管控，可通过制定桌面终端的安全策略模板，桌面终端通过下载安全策略模板并部署或由终端运维人员通过远程协助实现桌面终端的远程运维，解决桌面终端目前的现场运维、手工运维的问题。
* **实现桌面终端的消息推送、文件推送，**桌面终端安全管控平台需要提供消息推送、文件推送功能，系统管理员根据需要对所有终端进行消息推送，对安全整改脚本，系统管控或修复工具及其它需要部署或推送到桌面终端的文件，通过文件推送功能，推送到指定桌面终端，并根据策略由桌面管控终端的客户端程序进行相应操作。
* **实现网络运行检测，**对桌面终端进行流量监测，对桌面终端的网络行为进行实时监控，通过桌面终端实现楚雄供电局的网络拓扑、应用可用性检测等网络相关功能，对楚雄供电局的网络运维提供基础数据支撑。
* **辅助工具支撑类，**业务系统一键修复工具如“6+1”各业务系统一键修复工具，楚雄供电局内部信息系统相应修复工具，文件共享工具等辅助类功能。

### 功能需求：

**实现桌面终端的资产管理**。通过客户端软件采集桌面终端详细配置信息，包括桌面终端的厂家、型号、核心硬件设备信息如CPU、内存、主板、硬盘、网络设备等基本信息采集和统计汇总，实现桌面终端与责任人、使用人的对应，生成桌面终端唯一标识（指纹信息），通过唯一标识可实现桌面终端的全生命周期管理。

**实现桌面终端的运行管理**。通过客户端软件可实时获取桌面终端的运行情况，包括实时CPU使用率、内存占用率、硬盘空间、网络流量等基本运行时状态数据，还可以实时获取桌面终端的当前开启的应用、进程等应用类信息。

**实现桌面终端的应用安全管控**。包括必备软件检测与安装，如准入系统相关软件、杀毒软件等进行自动检测、修复或安装；应用策略管理，通过对各岗位必备应用软件进行梳理，实现应用可在指定对象、指定时间进行运行或禁止；CSGII运行时环境一键安装/修复，针对CSGII各业务系统运行是依赖环境和参数设置，提供一键安装与修复工具；应用黑白红名单维，可根据岗位或部门设置应用的黑白红名单，通过该名单实现应用软件合规性判断。

**实现桌面终端的信息安全管控。**包括桌面终端的侦听端口检测、外联程序监控、网络共享检查、弱口令、默认用户检测等涉及网公司规定的合规性检测，根据策略可选择报警、自动修复等操作。

**实现桌面终端的网络安全管控**。包括桌面终端网络流量监测，实现楚雄供电局内的网络拓扑、业务系统或应用可用性检测等功能。

**实现桌面终端的系统安全管控**。通过客户端软件实现本机故障自动诊断功能，包括硬件设备和应用软件诊断，实现桌面终端硬件环境和业务系统软件环境的自诊断和自动修复，维护桌面终端的系统安全。

**实现桌面终端安全策略的批量配置**。通过对桌面终端的使用人岗位职责或工作场景，批量设置与维护桌面终端的安全策略，通过桌面终端群组管理批量设置桌面终端的安全策略，实现桌面终端的安全策略的集中维护，自动设置。

**实现桌面终端的远程协助功能**。网省公司规定桌面终端的远程桌面功能必须关闭，为了实现桌面终端间的远程协助功能可通过桌面终端安全管控平台客户端来实现桌面终端之间的远程协助功能。

**实现桌面终端的消息推送及文件推送**。桌面终端安全管控平台提供消息和文件推送的相关接口，通过管理终端可实现对指定或所有终端的消息及文件推送功能。

### 性能需求：

系统的性能指标要求，包括并行用户数要求、精度要求、实时性要求、兼容性要求等。

并行用户数要求：楚雄供电局全局在用桌面终端在3000台左右，按5分钟回送一个心跳数据（运行时状态回送），系统需要满足平均10个用户并发要求，考虑到上班高峰期集中开机对系统的冲击，系统并发数按100个用户并发请求进行设计。

精度要求、实时性要求：楚雄供电局在用桌面终端在3000台左右，考虑到系统对网络的冲击及运维管理精度要求，按照每5分钟回送一次实时运行数据（心跳），用户查看桌面终端的实时运行状态，在线用户数据精度最大不超过心跳时间，有实时需求的可通过管理终端实时抓去指定桌面终端的运行态数据。

兼容性要求：楚雄供电局目前在用操作系统均为Windows 7及以上操作系统，桌面终端安全管控平台客户端软件要求兼容Windows 7及以上各版本32位或64位操作系统。

### 业务集成需求：

楚雄供电局桌面终端安全管控平台是一个全新建设的系统，主要面向楚雄供电局信息部门针对桌面终端安全管控，从数据来源上楚雄供电局桌面终端安全管控平台需要准入系统账户信息，可通过一次导入来实现。当桌面终端安全管控平台客户端部署率超过80%以后，可以考虑将桌面终端安全管控平台客户端同NAC系统进行集成，确保所有在用桌面终端必须安装桌面终端安全管控平台客户端软件。

### 安全需求：

楚雄供电局桌面终端安全管控平台是一个全新的信息系统，主要用于对辖区内桌面终端的资产管理和安全管控，不涉及业务系统，也不设计核心业务数据，但依然需要完善的权限管理保证核心管控功能的可靠性，避免错误设置和误用导致桌面终端的不可用。

### 信息量估算：

楚雄供电局全局在用桌面终端数量按3000台计算，按每台桌面终端每日上传2MB数据计算，每年每台桌面终端产生数据730MB，3000台桌面终端每年产生数据2.2TB左右。系统运行初期可按照保存3个月历史数据估算，需要500GB左右的存储空间。

# 项目必要性分析

## 桌面终端规范管理的需要

楚雄供电局目前对桌面终端的管理缺少相应的规范，在桌面终端的资产管理上通过南网的资产管理系统和云网的ITSM系统进行管理，但这两套系统都是台帐类管理模式，需要通过人工录入，难以跟踪桌面终端的配置变化，资产台帐的准确性差；在桌面终端的责任人和使用人关联上也缺乏相应的技术手段，传统的台帐式管理难以及时跟踪桌面终端的责任人及使用人的变化，久而久之供电局内部的桌面终端资产台帐和实物帐物不符现象严重；在对桌面终端的应用管理上缺乏相应的规范，桌面终端的应用安装及运行无管控，存在较大的安全隐患；通过桌面终端安全管控平台的建设，通过技术手段精准获取桌面终端配置信息和应用软件信息，通过对采集的相关数据进行分析，制定相应的桌面终端管理规范，最终实现桌面终端的规范化管理。

## 桌面终端安全管控的需要

南方电网公司对信息安全合规性管控越来越严格，楚雄供电局针对桌面终端的合规性管控目前缺少相应的技术手段，从合规性检查及不合规项目的整改上大多需要手工进行，要及时进行桌面终端的信息安全合规性检查和修复，并跟踪整改结果，如果没有信息系统的支撑是难以实现的，通过桌面终端安全管控平台的建设可实时对桌面终端的合规性进行检测，根据安全管控的设置可实现不合规项的报警或自动修复。

## 降低桌面终端运维管理及管控成本的需要

楚雄供电局的桌面终端分布在全州70余个乡镇，在用桌面终端的数量在3000台左右，目前的桌面终端运维采用现场运维的模式，桌面终端的运维及管控效率低，成本高，通过桌面终端安全管控平台的建设，可实时监控和获取桌面终端的运行情况，通过应用运行策略和安全管控策略可实现桌面终端的远程监控和相关项目的自动运维，可大幅降低桌面终端的运维及管控成本，提升运维及管控效率。

# 项目总体方案

## 建设思路

楚雄供电局桌面终端安全管控平台充分考虑南方电网和云南电网对桌面终端资产管理和信息安全合规性管控的相关要求，并结合楚雄供电局桌面终端运维管理的相关要求，建设一套符合楚雄供电局桌面终端运维管理和信息安全管控的信息系统，实现楚雄供电局桌面终端全面安全管控。

为了保证平台的可靠运行，需要具备很强的高可用性、高性能、可扩展性和易维护性，还要充分考虑未来与其他系统进行数据的同步、交换，所以需要具备集成性和先进性，同时需要保证系统的安全性。

桌面终端安全管控平台建设以价值为导向，以战略为驱动，以能力为基础。在设计中，既考虑桌面终端管理的最新理论与最佳实践，又充分考虑南方电网信息安全建设与管理能力和现状。桌面终端安全管控平台设计需遵循如下的原则：

1. 遵循信息化规划

桌面终端安全管控平台要全面贯彻落实科学发展观，以公司战略为导向，以创新为载体，引入先进的经营理念，在桌面终端的运维及安全管控上按照“统一管理、统一规划、统一标准、统一建设（四统一）”原则和定制化开发的研发建设思路，建设符合南网IT资产的管理要求、满足南方电网的信息安全合规性、适应楚雄供电局桌面终端运维管理需求的桌面终端安全管控平台。

1. 战略承接性

开展桌面终端安全管控平台建设，是为了为全面落实南方电网和云南电网对桌面终端的管控要求，提升桌面终端的信息安全防护能力，降低桌面终端的安全风险。桌面终端安全管控平台建设必须紧密承接公司战略思路，推动战略落地。

1. 重点突出性

在借鉴国内外内网安全管控系统和终端运维系统建设最佳实践的基础上，充分理解和吸收南方电网、云南电网及楚雄供电局在桌面终端管理上的最新理念与精髓，抓住楚雄供电局当前桌面终端资产准确性和信息安全管控的主要矛盾，予以重点解决。

1. 功能实用性

桌面终端安全管控平台的功能设计，将紧密贴合楚雄供电局针对桌面终端的安全管控及运维需求，防止出现华而不实，追求简单实用，体现公司管理精益化“精、简、益、善”的精髓。

## 业务范围

桌面终端安全管控平台涉及的业务域如图 5‑1所示。



图 5‑1业务域

在总体架构业务分类视图中，桌面终端安全管控平台支撑的业务分类如下图所示（用红色框标示项目支撑的业务分类）：

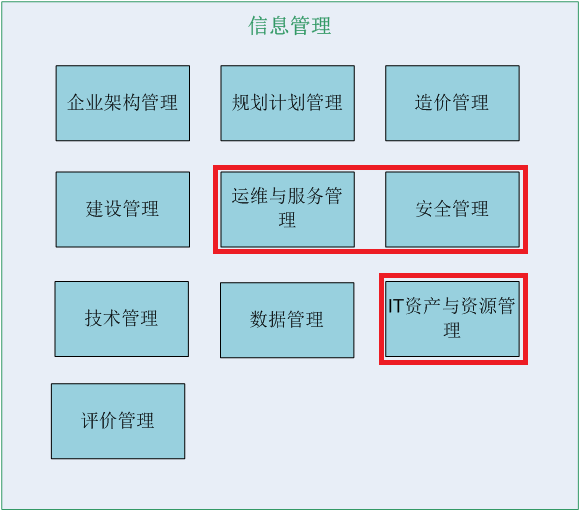


图 5‑2 业务分类

在总体架构业务分类表中，所支撑业务分类如下表所示：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **业务领域编号** | **业务域名称** | **一级业务分类编号** | **一级业务分类名称** | **二级业务分类编号** | **二级业务分类名称** |
| AD0008 | 信息管理 | BC0086 | 运维与服务管理 | BC0086.0001 | 运维管理 |
| AD0008 | 信息管理 | BC0086 | 运维与服务管理 | BC0086.0002 | 服务管理 |
| AD0008 | 信息管理 | BC0087 | 安全管理 | BC0087.0001 | 安全防护管理 |
| AD0008 | 信息管理 | BC0087 | 安全管理 | BC0087.0002 | 安全等级保护管理 |
| AD0008 | 信息管理 | BC0087 | 安全管理 | BC0087.0003 | 安全督查管理 |
| AD0008 | 信息管理 | BC0087 | 安全管理 | BC0087.0004 | 安全事件管理 |
| AD0008 | 信息管理 | BC0090 | IT资产与资源管理 | BC0090.0001 | IT资产管理 |

## 应用范围

### 功能框架

【描述项目建设所包括系统主要功能框架、系统建设和推广应用所涉及的范围，关于系统的功能框架部分，需要细分每一项功能，以及每项功能的具体描述。每项功能描述完后，增加该项功能所涉及到的内部数据、外部数据情况】

楚雄供电局桌面终端安全管控平台功能框架如下图：



图 5‑3 功能框架图

桌面终端安全管控平台从功能框架上看主要由四个层次构成，具体如下：

* 客户端，客户端分为两类，一类为部署在桌面终端的客户端程序，客户端程序由托盘程序和守护进程构成，其中守护进程负责监视托盘程序是否在运行，运行状态是否正常及客户端的版本检测服务；托盘程序负责完成桌面终端的各项数据采集和针对桌面终端的远程或自动操作。另一类为管理终端，管理员通过管理终端实现对桌面终端安全管控平台的综合配置及管理。
* 接入层，接入层有两种，一种为http接入，通过Web服务器实现，另一种为基于TCP/IP或UDP协议的接入，主要为实现管理终端直连桌面终端进行消息推送或远程管理。
* 服务层，桌面终端的客户端程序及管理终端的所有操作都由部署在应用服务器 的具体服务来执行，由服务层对根据相应请求对数据进行加工处理后存入数据库或提交管理中端进行数据展现。
* 存储层，桌面终端安全管控平台需要存储两类数据，一类为关系型数据，如桌面终端的资产类数据、应用类数据和运行时数据等动态数据，关系型数据存储在关系型数据库；另一类为非结构化数据，如需要推送的文件、策略配置文件，客户端详细配置信息文件等，这一类数据存储在文件服务器中，如FTP服务器。

### 功能划分

楚雄供电局桌面终端管控平台功能架构图如下：

图 5‑4 功能架构图

桌面终端管控平台可分为六个一类功能模块，分别为系统管理、资产管理、运行管理、终端安全、运维管理及查询统计模块。

### 功能说明

楚雄供电局桌面终端安全管控平台共有六的大的业务模块，具体有可分为20个二类功能，46个三级功能，具体功能说明可参加下表：

|  |  |  |  |
| --- | --- | --- | --- |
| **桌面终端安全管控平台功能清单** | | | |
| **一级功能** | **二级功能** | **三级功能** | **功能说明** |
| 系统管理 | 组织机构管理 | 分子公司维护 | 维护楚雄供电局及下属现公司的组织机构 |
| 部门/班组维护 | 部门或班组维护 |
| 岗位维护 | 岗位维护，通过岗位可确定岗位职责，通过岗位进行应用策略管理或必备软件检测 |
| 人员管理 | 人员维护 | 维护系统操作员及桌面终端使用人员信息，将人员信息与UKEY信息进行关联。 |
| 权限管理 | 权限维护 | 对系统操作员进行权限维护 |
| 准入数据导入 | 准入数据导入 | 为简化人员维护工作量，可通过从准入系统或4A系统中导出人员及组织机构数据，导入系统后在进行维护。 |
| 资产管理 | 资产基本信息 | 桌面终端信息 | 查询所有已部署安全管控平台客户端的桌面终端资产类信息，包括设备厂家、型号，核心配件参数等基础数据。 |
| 移动设备信息 | 查询曾经在已部署安全管控平台客户端的桌面终端上曾经使用的移动设备信息 |
| 资产历史 | 资产历史信息管理 | 当桌面终端设备属性或责任人发生变化时，进行记录，通过次功能可查询到桌面终端全生命周期信息 |
| 运行管理 | 设备运行管理 | 在线设备管理 | 查看当前在线终端的相关信息 |
| 设备运行时状态 | 获取桌面终端的运行时状态，包括CPU、内存、网络、磁盘空间等 |
| 应用运行管理 | 应用信息查询 | 获取桌面终端已安装应用信息、正在运行的应用信息。 |
| 进程信息查询 | 获取桌面终端正在运行的进程信息 |
| 终端安全管理 | 应用安全管理 | 黑白名单维护 | 信息中心根据对岗位或终端使用人的工作性质梳理应用的黑白名单，黑名单为禁止安装类软件，白名单为允许安装类软件 |
| 必备软件维护 | 根据管控要求桌面终端必须要安装的软件维护，可细分到岗位或终端，或终端组 |
| 必备软件检测 | 根据必备软件维护通过客户端软件进行检测并上报结果 |
| 应用策略管理 | 根据岗位、人员或终端设置软件应用策略，允许指定的人或指定的设备在指定的时间运行或禁止某些应用的使用 |
| 软件合规性检测 | 根据黑白名单对桌面终端安装的应用进行合规性检测并上报检测结果 |
| 信息安全管理 | 安全策略库维护 | 根据岗位、人员或终端设置桌面终端的安全策略，如复杂口令等具有普遍性的安全策略，客户端根据终端使用人自动下发并更新相关策略，实现自动运维 |
| 网络应用白名单管理 | 根据对必备应用和业务相关应用的梳理，可以明确存在网络应用的进程名称及相关端口和协议类型，并建立存在网络应用的进程黑白名单 |
| 网络应用合规性检测 | 根据网络应用黑白名单对桌面终端存在网络应用的进程进行检测，并上报检测结果 |
| 网络共享检测 | 根据信息安全合规性要求对桌面终端的共享目录进行检测并上报结果 |
| 默认用户检测 | 根据信息安全合规性要求对桌面终端的操作系统默认用户进行检测并上报结果 |
| 网络安全管理 | 终端网络流量监控 | 监控桌面终端的上下行数据流量 |
| 网络拓扑发现 | 根据管理终端下发目标IP，桌面终端客户端软件发起对目标IP的路由追踪，根据追踪结果实时绘制网络拓扑图 |
| 应用/功能可用性检测 | 根据管理终端下发的请求信息，桌面终端客户端发起相应请求，并记录请求路由，响应时间的信息，实现业务系统全局可用性追踪，提高系统维护效率和故障提前预警。 |
| 系统安全 | 终端硬件检测 | 对桌面终端进行硬件设备检测，包括驱动程序安装等信息，桌面终端用户可手工检测，系统管理员也可以通过管理终端远程发起检测 |
| 业务系统环境检测 | 根据业务系统制定和完善相应业务系统的运行环境检测，为业务系统终端运维提供数据支撑 |
| 运维管理 | 文件推送 | 推送计划制定 | 完成文件推送计划的制定、包括推送时间、对象等信息制定 |
| 推送计划审批 | 文件推送管理人员对相应的推送计划进行审批，审批通过后系统按推送计划进行文件推送。 |
| 推送结果查询 | 对推送结果进行查看，可提供成功与失败清单及相关原因。 |
| 消息推送 | 推送计划制定 | 完成消息推送计划的制定、包括推送时间、对象等信息制定 |
| 推送计划审批 | 消息推送管理人员对相应的推送计划进行审批，审批通过后系统按推送计划进行文件推送。 |
| 推送结果查询 | 对推送结果进行查看，可提供成功与失败清单及相关原因。 |
| 终端策略维护 | 终端分组管理 | 对所有在线终端可根据组织机构或岗位及相关工作性质对桌面终端进行分组管理 |
| 终端及配置策略维护 | 根据不同的管控需求，制定不同的终端配置及相应策略维护。 |
| 终端分组策略维护 | 对终端分组和终端及配置策略进行关联，实现终端配置及配置策略和终端分组的关联。 |
| 远程协助 | 远程协助管理 | 实现对远程协助的配置管理，包括身份二次验证，远程协助的权限管理功能 |
| 远程协助客户端开发 | 桌面终端安全管理管控平台客户端实现远程管理模块相应功能。 |
| 软件仓库 | 必备软件库管理 | 对网省公司要求必须安装的软件进行管理。 |
| 办公软件库管理 | 对常用办公软件进行管理。 |
| 常用软件库管理 | 对常用软件进行管理 |
| 软件配置管理 | 对所有入库软件进行配置管理，包括软件说明，测试人、上传人等信息进行维护。 |
| 共享管理 | 文件共享配置管理 | 设置本地共享的目录和文件并设置相应的权限，共享权限包括访问对象及操作权限 |
| 辅助工具管理 | 业务系统一键修复工具 | CSGII业务系统一键安装及修复工具 |
| 统计分析 | 统计分析 | 统计分析 | 根据系统采集的相关数据，形成相应的统计分析报表，辅助管理人员进行终端安全管理或运维。 |

## 技术路线

楚雄供电局桌面终端安全管控平台，全面部署后客户端数量在3000台左右，设计并发数为100，客户端与服务端采用短连接方式进行数据交互，由客户端主动发起请求，或管理终端直连客户端进行实时数据采集和管控。针对上述场景，桌面终端管控平台的整体技术路线主体采用SOA技术路线，针对本项目的应用场景进行适当变化，具体架构如下图：



采用SOA的技术路线，所有客户端的数据回送和请求都被封装成独立的服务，可大幅提高系统的并发能力和可扩展性。SOA技术路线是南方电网CSGII采用的技术架构，技术架构成熟可靠，便于扩展。

桌面终端安全管控平台在针对具体桌面终端进行远程管理和运维时，SOA的技术架构不能在桌面终端和管理中端建立直接的数据连接，通过SOA服务进行周转会降低效率，整体架构会变的更加复杂，针对需要直连的部分业务功能，在技术路线选择上采用传统的C/S架构，管理终端直接和桌面年终端的客户端程序通过Socket建立连接，大大提高系统的效率和整体的安全性稳定性，对由于跨网段或安全管控管理中端不能和客户端直连的，可通过在服务端部署一个Socket转发器进行中转链接。

## 部署方式

桌面终端安全管控平台采用供电局集中部署，服务器部署在楚雄供电局信息中心机房，保证辖区内所有桌面终端都可以访问，客户端软件通过AnyOffice推送到所有在用桌面终端静默安装，通过在桌面终端安装桌面安全终端并注册自启动服务，客户端软件在推送前需要经过第三方安全测试，如只有通过360开放软件平台的测试，在推送安装过程中才能够不被拦截，保证推送的成功率。

## 系统集成

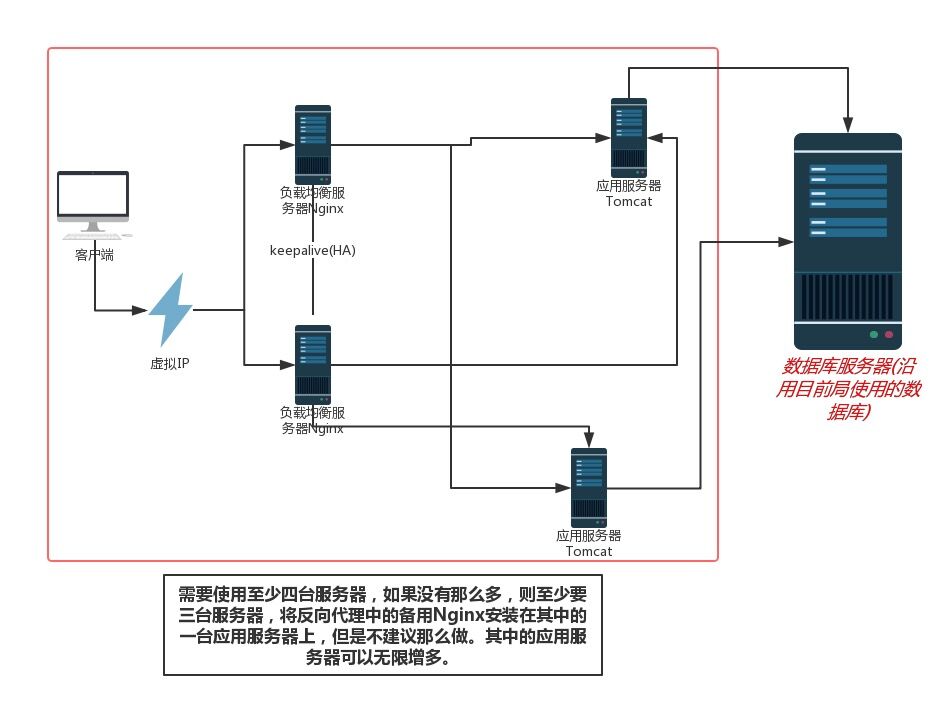
楚雄供电局桌面终端安全管控平台是一个独立系统，主要完成全局所有在用桌面终端的安全管控，因桌面终端需要定位到使用人，为准确读取UKEY信息做好数据对应，可通过准入系统导出楚雄供电局的职工UKEY账号信息，减少桌面安全管控系统组织机构维护和人员岗位维护的工作量。

在系统推广后期，当桌面安全管控终端部署量超过80%以后，可以考虑将桌面安全管控终端与NAC系统集成，将桌面安全管控终端的安装运行和准入系统绑定，提高桌面安全终端的部署率和运行率。

## 软硬件平台资源需求

【明确系统所需的软、硬件平台资源、物理架构图，硬件资源主要包括计算资源、存储资源、网络资源，软件资源主要包括数据库、中间件。计算、存储资源应根据《中国南方电网有限责任公司软硬件平台架构和资源分配指导意见》进行估算，

楚雄供电局桌面终端安全管控平台物理架构图如下：



所有设备可采用数据中心的虚拟计算资源，采用两台虚拟机作为接入服务器其中一台开启软负载均衡，两台虚拟机作为应用服务器，所有服务部署在两台应用服务器上，数据库采用数据中心的Oracle或MySQL数据库，使用数据中心存储。软硬件资源需求如下：

接入服务器（软负载均衡服务器）：2台，CPU\*1\*2Core，内存≥8GB，硬盘≥146GB，操作系统CentOS7。

应用服务器：2台，CPU\*1\*2Core，内存≥8GB，硬盘≥500GB，操作系统CentOS7。

数据库服务器：1台，CPU\*1\*4Core，内存≥32GB，硬盘≥2TB，操作系统CentOS7。

为节约计算资源，文件服务器可部署在一台接入服务器上并适当加大硬盘空间即可。

## 安全方案

楚雄供电局桌面终端安全管控平台是一个针对全局在用桌面终端定制化开发的一个终端安全管控的信息化运维管理平台，平台不涉及业务系统相关的敏感数据，所采集的桌面终端软硬件信息可作为楚雄供电局对桌面终端资产配置管理、终端安全管控和远程终端运维依据，系统数据损坏或丢失后，安全管控终端可即时采集相关数据，不会对桌面终端使用造成任何影响，对信息部门终端运维人员会造成一定影响，影响终端安全管和运维管理工作的高效开展。对此楚雄供电局桌面终端安管控平台其安全保护等级可设定为一级。在系统开发和部署实施过程中严格按照信息系统登机保护一级要求进行。

## 运维管理建议

桌面终端安全管控平台是楚雄供电局自建的系统，主要目标为提高楚雄供电局桌面终端的安全水平，提升桌面终端可用性，降低安全风险，通过桌面终端安全管控平台可大幅减少楚雄供电局桌面终端的运维量，提升工作效率。

桌面终端的运维可以分为硬件运维和软件运维，通过桌面终端安全管控平台可获取到桌面终端的软硬件信息，由于终端的软硬件环境一直在发生变化，桌面终端安全管控平台也要跟随软硬件的变化不断的进行调整。桌面终端安全管控平台的运维主要就是要不断的根据桌面终端的软硬件环境变化适时进行调整，以保证桌面终端安全管控平台的持续有效。桌面终端安全管控平台的运维主要有以下两个方面：

* 软硬件平台运维：保持桌面终端安全管控平台服务端良好的工作状态，和持续不断的跟踪解决客户端软件在不同操作系统和硬件环境下的运行状态。
* 安全管控参数修订及安全管控策略运维：根据不断发展的桌面终端安全形势，适时调整相应的管控策略，持续有效的保证桌面安全管控平台的有效性。

针对上述运维工作内容，建议未来采用混合运维模式，软硬件平台运维和合并到楚雄供电局信息中心机房运维工作中，安全管控参数修订及安全管控策略运维相对专业，建议由厂家持续跟踪软硬件环境的变化，定期进行调整修订，运维规模为平台软件一套，数据中心服务器4台，数据库服务器1台，桌面终端3000台左右。根据上述运维规模，运维成本建议按技术服务模式进行测算，按厂家提供3人的技术服务小组，按每月现场运维一次，每次5个工作日，则每年180人.日，每年运维成本为21.6万元。

# 项目实施方案

## 实施策略及计划

项目实施策略将紧密围绕桌面终端安全管控要求，统一规划，分步、分阶段设计一个先进实用的符合楚雄供电局桌面终端安全管控现状的平台，具体原则包括：

1. **质量第一，重点突出**

项目质量是衡量项目成败的决定性要素。在项目实施过程中我们遵循质量第一、重点突出的原则。质量管理可分成如下三步：首先根据项目的总体目标、项目范围以及项目进度计划，双方确定有效的项目质量标准。其次，在项目执行过程中采取有效措施监测项目的实际运行，为了达到有效监测的目的，通常采取的监测和沟通渠道包括项目进度报告、项目例会、里程碑会议、各种会议纪要等。再次，把项目实施过程中的实际表现与项目质量衡量标准进行比较，分析出差异。最后，根据具体情况采取合理的纠正措施。经过比较与分析，如果发现偏差，就要采取适当的措施进行纠正，让项目实施回到正轨。

1. **设计先进性和适用性**

在设计过程中，将充分借鉴国内外实施经验，利用成熟的产品和技术；同时充分考虑楚雄供电局的实际情况。并立足今后发展需要，使之成为适合楚雄供电局桌面终端安全管控需求，既能够保证先进性和成熟性，也可又保证系统的适用性。

1. **有效沟通，多点落实**

采用有效沟通、多点落实的沟通原则：首先识别项目的各个干系人，关注各个干系人的期望与需求；其次在项目实施过程中采用项目总结、项目例会、项目周报、临时会议等方式充分和项目相关人员进行沟通；最后沟通的结果会形成书面记录以便有效执行。全过程、多层次的沟通确保了双方目标一致、信息同步，从而有利于项目中各种问题的解决。

1. **全程参与，知识转移**

项目实施采用关键用户全程参与的方式来达到知识转移的目的。在项目实施过程中按照转移方式不同将知识内容分为显性知识和隐性知识，其中，显性知识包括系统客户化方法、系统操作方法、系统数据库结构及二次开发规范；隐性知识则是指难以用文字记录和传播的知识，是与人结合在一起的经验性的知识，难于通过常规方法收集、也难于通过常规的信息工具传播，主要包括技术要素（主要指技术诀窍、技能和能力）、认知要素（主要指选择和分析问题、判断力、前瞻性）、经验要素（指经验、阅历和文化要素）和价值要素（包括文化和行为准则规范等）。显性知识转移通过培训、项目实施文档进行转移，隐形知识需要关键用户参与需求分析、方案编写、客户化设置等系统实施的全过程。

1. **系统标准化和扩展性**

在标准化方面，数据上遵循各种国家标准及南方电网企业标准；应用系统上应该符合企业本身制定的一些安全标准和管理标准；建设过程中也应该遵循企业的项目管理和各种开发管理的标准。

在扩展性方面，新增数据情况下模型可扩展性；在数据量、用户访问量和处理复杂性增加的情况下平台可扩展性；基于SOA的技术路线能够支撑对新的功能模块的建设。

按照管理应用开发类项目实施方法论，结合楚雄供电局实际情况，本项目实施阶段包括项目准备、需求分析、方案设计、功能设计、应用开发、系统初验、系统试运行、系统终验等阶段，实施计划框架如下：

| **年度** | **阶段** | **开始时间** | **完成时间** | **主要内容及交付项** |
| --- | --- | --- | --- | --- |
| 2017 | 项目准备 | 2017年6月 | 2017年6月 | 《工作方案》 |
| 需求分析 | 2017年6月 | 2017年6月 | 调研楚雄供电局桌面终端安全管控相关需求，形成《应用需求规格说明书》。 |
| 功能设计 | 2017年7月 | 2014年7月 | 设计系统应用功能，形成《桌面终端安全管控平台功能详细设计说明书》。 |
| 系统开发 | 2017年8月 | 2017年10月 | 保证系统开发、测试阶段的进度，形成《现场部署方案》、《培训方案》，开发系统功能。 |
| 系统初验 | 2017年11月 | 2017年11月 | 系统初验，形成《功能验收评审意见》 |
| 系统试运行 | 2017年11月 | 2017年11月 | 系统试运行。 |
| 应用优化 | 2017年12月 | 2017年12月 | 根据试运行中反馈意见开展优化。 |
| 项目结题 | 2017年12月 | 2017年12月 | 完成终验，形成《竣工验收评审意见》。 |

## 实施任务分解

|  |  |  |
| --- | --- | --- |
| **序号** | **工作内容** | **人天数** |
| 1 | **项目准备阶段** | **3** |
| 1.1 | 组建项目组织结构 | 1 |
| 1.2 | 编制系统实施推广工作方案 | 1 |
| 1.3 | 召开实施推广启动会议（约定问题处理机制、实施流程，项目协同支撑等） | 1 |
| 2 | **实施环境准备** | **1** |
| 2.1 | 准备服务器环境（包括机器、中间件软件等），软硬件集成 | 1 |
| 2.2 | 搭建现场办公环境（场地、电话、网络等） | 0 |
| 3 | **数据清理阶段** | **6** |
| 3.1 | **环境数据准备及系统配置** |  |
| 3.1.1 | 开展环境数据准备 | 2 |
| 3.1.2 | 进行环境数据配置实现 | 2 |
| 3.1.3 | 进行系统模拟测试 | 2 |
| 4 | **业务配置阶段** | **20** |
| 4.1 | **基础数据(权限，用户，角色)收集及系统配置** |  |
| 4.1.1 | 开展基础数据收集 | 2 |
| 4.1.2 | 进行基础数据收集结果的校验、检查与整改、确认 | 2 |
| 4.1.3 | 进行基础数据的配置实现 | 2 |
| 4.1.4 | 进行系统模拟测试 | 2 |
| 4.2 | **业务数据清理及数据导入（业务数据初始化、原有系统数据的清理和导入）** |  |
| 4.2.1 | 开展业务数据收集 | 2 |
| 4.2.2 | 开展业务数据清理 | 2 |
| 4.2.3 | 进行业务数据清理结果的检查、校验、整改 | 2 |
| 4.2.4 | 进行业务数据清理结果的导入、验证 | 2 |
| 4.2.5 | 进行业务数据清理结果确认 | 2 |
| 4.2.6 | 开展系统总体环境测试 | 2 |
| 5 | **投入运行准备阶段** | **9** |
| 5.1 | **系统培训及应用演练** |  |
| 5.1.1 | 制定培训方案与计划 | 1 |
| 5.1.2 | 进行培训课件的准备 | 1 |
| 5.1.3 | 进行培训环境的准备 | 0 |
| 5.1.4 | 开展系统全面培训及应用演练 | 2 |
| 5.2 | **上线准备** |  |
| 5.2.1 | 确定系统上线方案及切换计划 | 0 |
| 5.2.2 | 进行系统正式环境搭建 | 0 |
| 5.2.3 | 开展第三方功能测试、性能及安全测试 | 2 |
| 5.2.4 | 进行系统上线演练 | 1 |
| 5.3 | **系统上线切换** |  |
| 5.3.1 | 进行系统正式环境切换 | 0 |
| 5.3.2 | 进行系统功能验收 | 1 |
| 5.3.3 | 召开系统上线启动会议 | 1 |
| 6 | **实施推进及运行支持（安排人员数量）** | **22** |
| 6.1 | 解答与处理一线用户问题（操作咨询、权限配置等现场可以直接处理的问题）要包含现场和后台人员。 | 5 |
| 6.2 | 管理及跟踪反馈二线用户问题（系统缺陷、功能改进、功能需求等现场不能直接处理的功能性问题） | 5 |
| 6.3 | 进行应用服务器及数据服务器的日常运行监控 | 5 |
| 6.4 | 进行服务器平台调优与日常维护 | 5 |
| 6.5 | 进行系统竣工验收 | 1 |
| 6.6 | 开展轮巡工作 | 0 |
| 6.7 | 召开系统运行总结及支持性会议 | 1 |
| **总工作量合计** | | **61** |
| **人工单价（万元/天）** | | **0.12** |
| **实施总费用** | | **7.32** |

# 项目投资估算

## 投资依据说明

1、整体单价取费原则：根据《中国南方电网有限责任公司信息化项目预算编制与计算方法》确定。

2、根据《中国南方电网有限责任公司信息化项目预算编制与计算方法》，开发费采用**功能点估算法**进行测算，计算公式如下：

开发费=开发人员单价（元/人天）\*（（（内部数据功能点分值\*内部数据个数+外部数据功能点分值\*外部数据个数）\*规模变更因子\*功能点耗时率/8 )\*调整因子）

公式中各参数取值说明如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **参数名称** | **参数取值** | **说明** |
| 1 | 内部数据功能点分值 | 35 | 内部数据所对应的功能点分值，取行业统计数 |
| 2 | 外部数据功能点分值 | 15 | 外部数据所对应的功能点分值，取行业统计数 |
| 3 | 规模变更因子 | 2 | 参考业界数据 |
| 4 | 功能点耗时率 | 13.4 | 每个功能点所消耗的人时数,取行业中值 |
| 5 | 调整因子 | 1 | 新建系统=1，改造系统<1。本系统为新建系统，取1 |

内外部数据列表:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **功能大项** | **功能子项** | **功能描述** | **内部数据** | **外部数据** |
| 1 | 系统管理 | 组织机构管理 | 完成组织机构的增删改查 | 系统组织机构表 |  |
| 用户管理 | 对系统用户进行新增、修改删除等管理 | 系统用户表 |  |
| 权限管理 | 针对岗位、用户、菜单，分类的业务处理及查询设置权限进行新增删除修改等管理 | 系统权限表 |  |
| 准入数据导入 | 从准入系统导出用户和组织机构数据，导入到系统 | 系统组织机构表、系统用户表 |  |
| 2 | 资产管理 | 资产基本信息 | 对桌面终端的厂家配置等信息进行采集，生成设备指纹信息 | 终端资产表 | 终端配置信息表 |
| 资产历史 | 桌面终端发生使用人变更或设备配置参数变化的添加历史记录，可查询统计相关信息 | 终端资产历史表 | 终端资产信息表 |
| 3 | 运行管理 | 设备运行管理 | 完成在线终端及其运行状态的数据采集及查看 | 终端资产表、终端运行状态表 | 终端实时运行数据表 |
| 应用运行管理 | 采集桌面终端已安装的应用信息和正在运行的应用及进程信息 | 终端资产表、终端运行应用表、终端运行进程表 | 终端运行应用表、终端运行进程表 |
| 4 | 终端安全管理 | 应用安全 | 针对桌面终端上安装的应用软件进行梳理规范，制定黑白名单、运行策略等应用软件安全管理 | 终端安装应用表、应用软件黑白名单表、应用策略配置表 |  |
| 信息安全 | 针对桌面终端的网络应用设置黑白名单，监控存在网络侦听或外联的应用，监控本地网络流量，对网络共享，默认账户等进行合规性检查 | 网络应用黑白名单、网络共享表、默认账号表、网络侦听表 |  |
| 系统安全 | 对桌面终端的硬件设备进行检测，对业务系统支持环境进行检测，提供系统自检功能，实现辅助运维 | 终端硬件设备检测表、业务系统支持环境检测表 |  |
| 5 | 运维管理 | 文件推送 | 完成文件推送计划制定、审批和推送结果查看，包含相应的增删查改 | 文件推送计划表、文件推送数据表 |  |
| 消息推送 | 完成消息推送计划制定、审批和推送结果查看，包含相应的增删查改 | 消息推送计划表、消息推送数据表 |  |
| 终端策略维护 | 管理员维护终端策略，上传服务器，桌面终端下载后更新本地策略，支持按岗位，终端分组等模式进行配置管理 | 终端策略配置表、终端分组表 |  |
| 远程协助 | 提供远程协助功能，管理员可远程对桌面终端进行协作运维。 | 远程协助日志表 |  |
| 软件仓库 | 实现对局内应用软件进行配置管理 | 软件配置数据表 |  |
| 辅助工具管理 | 业务系统一键安装及修复工具管理 | 分系统一键修复工具配置表 |  |
| 共享管理 | 实现桌面终端之间的文件共享功能 | 文件共享数据传输协议 |  |
| 6 | 统计分析 | 统计分析 | 根据系统采集的相关数据，形成相应的统计分析报表，辅助管理人员进行终端安全管理或运维。 |  |  |

## 总投资

项目费用汇总表 单位：元

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 建设单位 | 项目名称 | 投资估算(按费用性质) | | | 投资估算(按费用类别) | | | | |
| 资本性 | 费用性 | 合计 | 建设费 | 维护费 | 设备购置费 | 其他费用 | 合计 |
|  | 云南电网公司楚雄供电局 | 楚雄供电局桌面终端安全管控平台 | 1716500 | 73200 | 1789700 | 1689700 |  | 100000 |  | 1789700 |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  | 合计 | 1716500 | 73200 | 1789700 | 1689700 |  | 100000 |  | 1789700 |

具体各单位项目投资估算情况详见附件《[楚雄供电局桌面终端安全管控平台可行性研究估算书](楚雄供电局桌面终端安全管控平台建设%20-%20可研估算书V1.0.xls)》。

## 资金计划建议

【如果项目存在跨年度情况，需描述各年度投资额估算】。

本项目各年度投资建议如下：

单位：万元

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 建设单位 | 项目名称 | 总投资 | 2017年 | | |
| 资本性 | 费用性 | 合计 |
| 1 | 云南电网公司楚雄供电局 | 桌面终端安全管控平台建设项目 | 178.97 | 171.65 | 7.32 | 178.97 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

初步规划项目总体资金进度计划如下表所示：

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 合同项 | 采购方案登记 | 采购完成 | 签订合同 | | 项目初验 | | 项目终验 | |
| 完成  时间 | 累计完成资金（万元） | 完成  时间 | 累计完成资金（万元） | 完成  时间 | 累计完成资金（万元） |
| 1 | 系统开发及实施 | 2017.6 | 2017.6 | 2017.7 | 54 | 2017.11 | 125 | 2017.12 | 179 |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

（注：项目终验的累计完成资金进度应为100%）

项目资金计划需要根据年度下达投资及项目实际进度及时调整。

# 项目效益分析

## 管理效益分析

桌面终端管理一直依托人力进行现场运维，无法实现快速高效的全局桌面终端的数据采集和运维，按照传统方式，全面采集一次桌面终端相关数据，按每天完成一个乡镇，全州共有70多个乡镇，最低需要3个月完成一次全州数据采集，采集后进行数据整理分析，最低也需要1个月完成，传统采集方式至少要4个月才能完成一次全州在用桌面终端的数据采集和分析工作，且采集周期过长，时间跨度大，几个月后的数据其有效性存疑，影响对桌面终端管理的策略制定。而采用桌面终端安全管控平台，可实现实时采集在线桌面终端的静态、动态参数，实时对采集到的数据进行分析和展现，让管理人员从繁琐的数据收集和整理事务中解脱出来，专注于终端的运行分析和监控工作，能够及时的发现桌面终端存在的问题，大大提高了工作质量和效率。

传统的桌面终端运维都是被动运维，当桌面终端出现软硬件故障，或桌面终端性能影响到正常工作开展时，由终端使用者通过电话等方式报修，运维人员到现场进行问题处理的工作方式。而通过本次技术服务，通过定制化的桌面终端信息采集工具，可实时获取终端状态，系统运维管理人员可第一时间识别异常终端，并制定相应的处置方案，将问题处理在发生之前，大幅提高了终端运维的效率，增强了运维人员的工作有效性，降低了终端运维成本。

通过对桌面终端*静态信息和动态信息的*实时收集与分析，可实时监控桌面终端可能存在的风险，如可疑的网络侦听程序，不应该存在的网络共享目录等可能存在信息安全隐患，指导运维人员精准的解决相关安全隐患，提升桌面终端的安全防护能力，防患于未然，解决了传统的通过IP端口扫描的方式来识别安全隐患，提高了工作效率，提升了桌面终端的安全防护能力。

## 经济效益分析

楚雄供电局目前的桌面终端运维通过委托第三方进行运维，运维也仅限于桌面终端发生软硬件故障后通知运维人员来现场运维，工作效率低，严重影响使用人正常开展工作，且运维人员也仅能处理硬件故障和基本的软件环境问题，对涉及到的信息安全相关内容，基本无法做到，按照传统的运维方式，达到南方电网下达的信息安全合规性要求，需要投入大量的人力物力，楚雄供电局覆盖全州70多个乡镇，按每个乡镇5人天计算，全部进行一次现场处理需要350多人日，包含差旅等费用，按人日2100元计算，需要73.5万元。桌面终端安全实时都在发生变化，要保证桌面终端安全需要定期对桌面终端进行安全合规性检查和修复，针对不断出现的各种信息安全风险需要持续跟进，按照一个季度进行一次现场处理，一年的桌面终端安全管控费用将在300万元左右，而通过建设桌面终端安全管控平台，桌面终端的安全管控不需要到达现场，通过平台可快速对全局在线桌面终端安全合规性进行检查，对发现的风险问题能够自动修复的可通过客户端软件自动修复，不能够自动修复的可以通过远程协助进行修复，大大提高工作效率，降低投入。通过桌面终端安全管控平台也可大大降低桌面运维工作量，通过桌面终端安全管控平台的建设尽在桌面终端安全和运维上首年可节约100多万元，投产后每年可节约费用200多万元。

## 社会效益分析

通过桌面终端安全管控平台的建设，可极大提高楚雄供电局桌面终端安全性和可用性，降低信息安全风险，避免因为桌面终端发生信息安全事故而影响到电网的稳定运行，提升桌面终端使用人员的工作效率，间接对稳定供电，提高服务质量，提升客户满意度提供了基本保障。

# 项目风险及保障措施

## 建设风险及对策

根据国内外内网安全系统实施的经验，系统实施和运行过程中会受到公司内部和外部诸多因素的影响，下列是项目实施中可能出现的主要风险，并针对性提出应对措施：

1. **技术风险**

桌面终端安全管控平台是一个和操作系统密切相关的系统，需要获取大量的操作系统级别数据，需要对各类操作系统有深刻的理解。

安全管控设计的知识面广，从硬件到软件到网络套信息安全，都需要全面的深入的了解，在某些领域需要达到专家级别的水平，涉及底层的部分技术可以参考的资料较少，需要进行一定的技术攻关。

通过和同行业进行交流，选择有丰富经验的开发商可降低技术风险。

1. **项目推广的风险**

桌面终端安全管控平台需要在全局所有在用桌面终端进行部署，在推广部署过程中需要解决各类安全软件的拦截与误报，需要同各安全厂家进行联系测评，提高推广成功率。

桌面终端安全管控平台在一定程度上会获取到终端用户的部分数据，如当前正在运行的应用等信息，需要和终端用户做好培训，防止终端用户出现逆反心里，保证系统推广实施得以顺利开展，安装部署成功后保持持续的开机启动状态。

## 实施保障措施

项目管理贯穿整个项目的始终，持续控制项目风险，解决项目问题，提高项目质量、控制范围和成本；处理项目管理工作中的各项日常工作，监测项目进展；汇报项目情况，从各方面保障项目的成功。具体地，主要有以下保障措施：

1. **建立有效的沟通机制**

通过对关键沟通对象分析，制定行之有效的沟通策略；组织召开项目指导委员会层面定期会议；汇报和解决项目过程中产生的各种问题。

1. **建立业务及技术方案审核机制**

通过建立业务及技术交付品审核机制，对各类项目交付品进行交叉审核或专家评审，确保各项业务及技术设计的准确性。

1. **增强组织协同性**

加强公司内部沟通，促进相关人员了解项目产生的影响，确保相关人员对业务流程变化等方面的适应性，做好转变管理工作；获取公司层面领导和归口部门的大力支持，完善相关配套制度等修订等方面的工作。

1. **制定详实的开发规范**

针对项目各开发阶段、各种类型成果制定详实的开发规范，一方面确保了项目的开发能够有计划、有规范、有效率地进行，另一方面能够使项目开发过程的各项成果得到有效的继承。

1. **制定并执行合理的培训及知识转移计划**

有计划地、系统性地举办用户培训，提高广大员工对系统变化的熟悉程度，尽可能地消除恐惧和排斥心理；为广大的系统最终用户提供实用的辅助性资料和工具，帮助员工自我练习，自我解决较为简单应用使用问题。

# 项目可行性分析

根据本可行性研究的前述内容，对出本项目的可行性分析如下：

1. **桌面终端运行技术支持服务发现了存在的问题和不足**

楚雄供电局在2016年针对桌面终端运行开展了一次技术支持服务，通过本子服务发现了楚雄供电局桌面终端管理上存在的众多不足，依靠传统的技术和手段难以达到整改和持续跟踪的要求，且南方电网公司对桌面终端的信息安全要求越来越严格，依靠现有的手段难以达到要求，桌面终端的安全隐患难以消除。

1. **南方电网的信息安全合规性要求指明了方向**

南方电网公司出台了信息安全合规性检查，其中涉及桌面终端的项目较多，大多数要求都可以通过信息系统来进行自动检查和整改，通过桌面终端安全管控平台的建设可大大减少在桌面终端安全管控上的人力投入。

# 项目研究结论及建议

综上所述，本项目**具有较强的可行性和迫切性**，根据南方电网公司招标采购管理规定，建议楚雄供电局桌面终端安全管控平台建设项目纳入公司一级采购目录，根据南方电网公司招标采购管理规定，建议楚雄供电局桌面终端安全管控平台建设纳入公司二级采购目录。

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 采购项 | 一级采购/二级采购 | 说明 |
| 1 | 楚雄供电局桌面终端安全管控平台建设 | 二级采购 | 本表仅为采购建议，具体以实际的采购计划为准。 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |  |