NSFOCUS

# 绿盟科技
# 能源行业成功案例集锦

## NSFOCUS SUCCESS STORIES
## WITH THE ENERGY SECTOR

NSFOCUS

**THE EXPERT**
**BEHIND GIANTS**
**巨人背后的专家**

多年以来，绿盟科技立足能源行业，致力工控系统信息安全研究，为电网、发电、石油石化、煤炭、天然气等能源行业用户提供了一系列具有核心竞争力的咨询评估服务和工控安全解决方案，保障客户业务的安全可靠运行。在这些巨人背后，他们是备受信赖的行业信息安全专家！

www.nsfocus.com

关注绿盟科技官方微博　关注绿盟科技官方微信　移动客户端绿盟安全管家

# 目录 CONTENTS

# 01 引言
# INTRODUCTION



## 引言
## INTRODUCTION


绿盟科技自2000年成立以来，致力于安全攻防研究多年。在信息安全行业领域取得了卓越的成绩，并且获得了业内极高的评价，成为了国内信息安全领域的领军企业。多年以来，绿盟科技结合在信息安全领域的最佳安全实践，深耕包括电力、石油、石化、煤炭在内的能源行业，为能源行业用户提供了具有核心竞争力的安全产品、安全服务及解决方案，并且积累了大量优秀的成功案例。

# 02 电力
# ELECTRIC POWER



# 电力
ELECTRIC POWER

## 2.1 电网社会邮箱敏感邮件阻断项目

### 2.1.1 项目场景

随着办公自动化的发展，电子文挡资料的日益丰富，许多内部员工也经常会选择利用电子邮件将机密资料发送，容易被不发分子利用，以达到他们的非法目的。企业对电子邮件系统的使用，缺乏安全审计管理的措施，严重威胁到了企业的生存。2011年底CSDN"泄密门"事件，导致600万用户注册邮箱和密码被泄露，涉及帐号、密码2.78亿条。大约76%的网络安全威胁来自于企业内部，其危害程度更是远远超过黑客攻击及病毒造成的损失，而这些威胁绝大部分与内部各种网络行为如邮件收发有关。电网外网邮箱通过邮件网关进行敏感信息的检测和阻断，但针对社会邮箱缺乏相关的敏感信息检测、阻断及审计措施。

### 2.1.2 解决方案

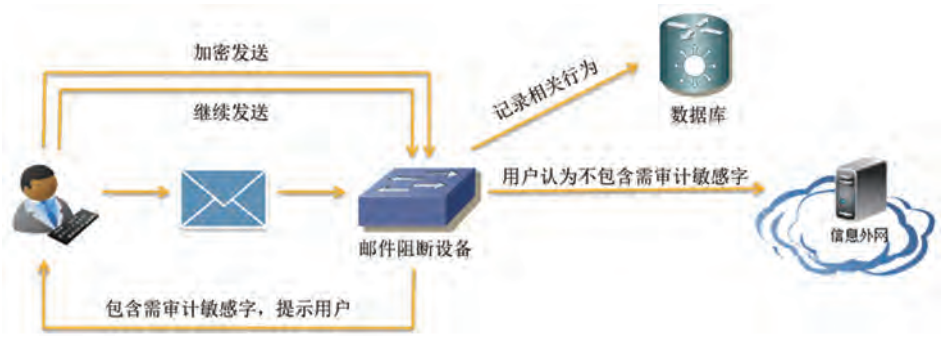
通过在互联网出口部署的社会邮箱敏感邮件审计设备，实现邮件内容审计、敏感邮件提醒和阻断。支持基于时间、用户、内容关键字、应用协议等多种条件组合，对邮件收发(Web Mail、SMTP、POP3、IMAP)进行全面信息外发管理，实时告警、阻断、还原。

实现功能如下：

友好提醒功能：用户收到提示邮件；如果用户认为邮件没有问题，进行确认后，可不做修改进行发送而不做阻断。

支持加密发送功能：当用户收到提示邮件后，用户可选择加密发送，在输入加密密码后，该邮件以压缩加密的方式进行重新投递。

相关行为的记录与统计：对阻断邮件进行信息统计和备份，并对用户的继续投递和加密发送行为进行统计。




## 2.1.3 客户价值

项目从2012年开始，经过三期建设过程，实施范围覆盖了电网总部、省公司、直属单位及部分地市公司，实施设备数量达到300多台。实现了针对国家电网信息外网用户使用社会邮箱收发邮件的敏感信息关键字进行监控、审计、阻断及告警功能，并与日常考核结合，从管理和技术角度





两个角度实现阻断敏感信息外泄、实时监控敏感信息、敏感字告警、阻断告警。

# 2.2 国网某网省信息安全实验室建设项目

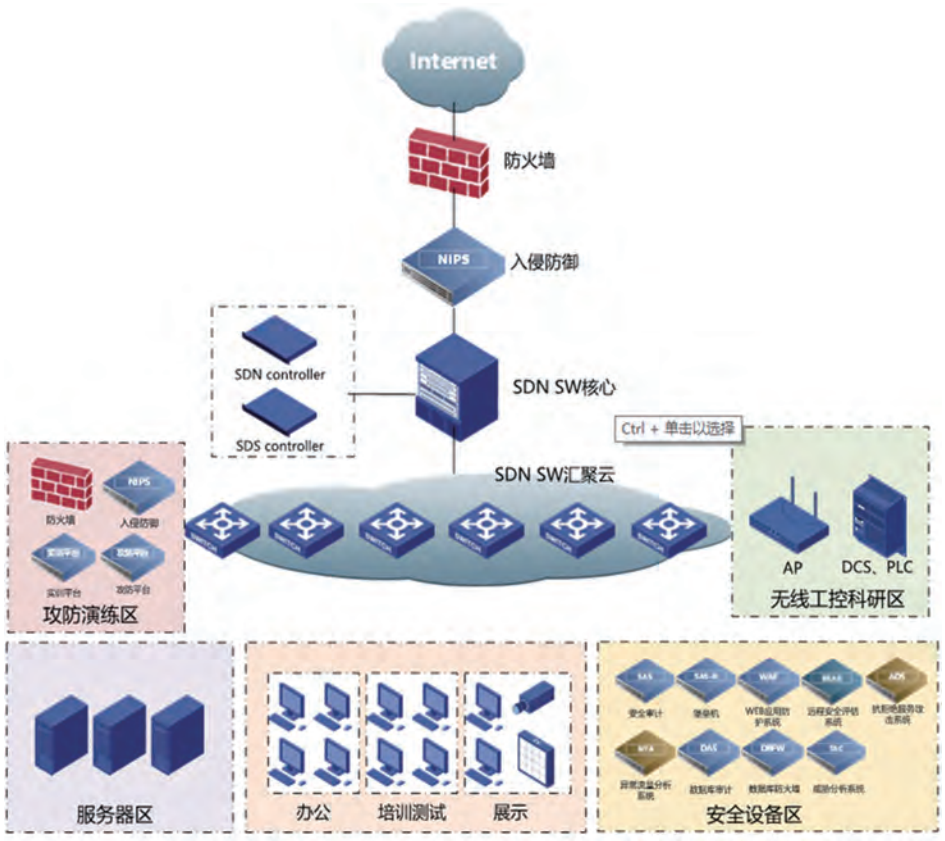
## 2.2.1 项目背景

随着国网公司”SG186工程、智能电网以及三集五大体系的深入推进，内部运转和对外服务依托大量业务信息系统，系统安全稳定运行和数据资产内容安全作为信息化深入推进的重要保障。国网公司高度关注信息网络、信息系统的运行安全，采取多种安全手段和措施保障信息系统的安全稳定运行，有效的降低了信息安全事故的发生率。但随着云计算、大数据、物联网、移动业务等新技术新应用在国网公司的陆续使用，势必在数据安全、Dockers安全、无线安全等领域带来挑战。

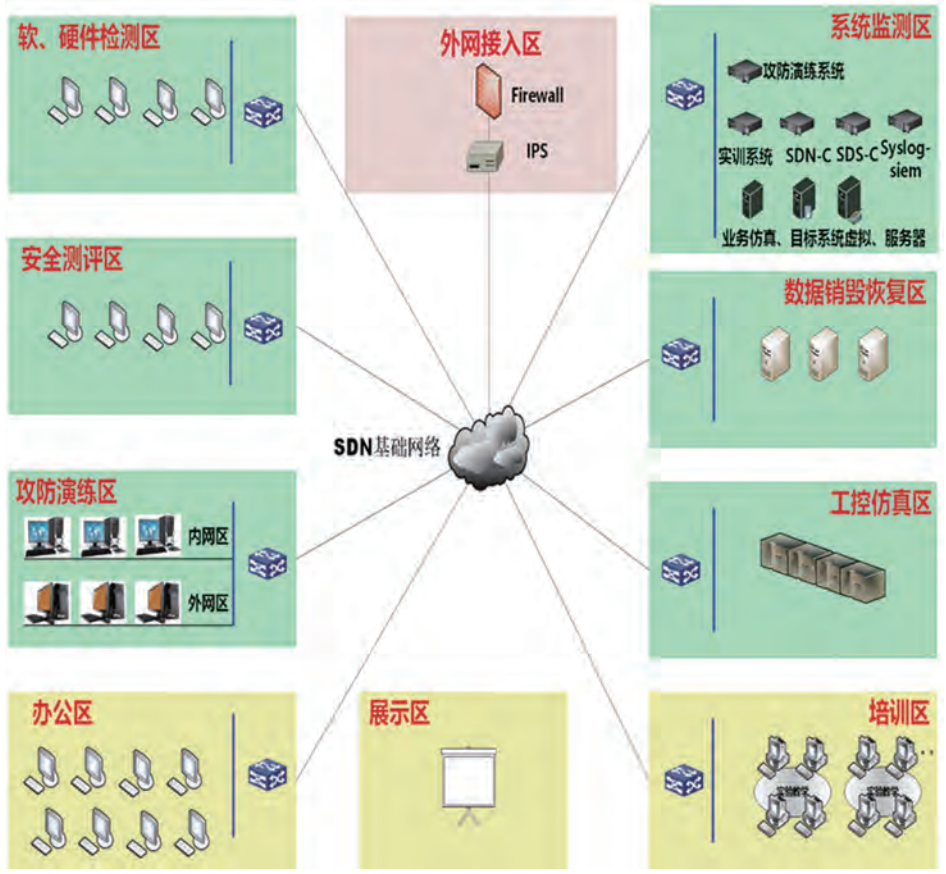
在国网公司范围内，目前除中国电科院建立了具有相关测评资质的信息安全实验室之外，黑龙江、浙江、四川、江苏公司的安全实验室已申请成为中国电科院安全实验室分中心，安徽、甘肃、湖南电力公司安全实验室正在申请过程中。虽各网省公司申报分中心实验室时侧重点有所不同，但大部分网省公司工作重点均集中在攻防演练以及培训方面。

## 2.2.2 解决方案

实验室通过SDN基础网络承载，按逻辑功能将区域划分为系统监测区、数据销毁恢复区、工控仿真区、软硬件检测区、安全评测区、攻防演练区、展示区、培训区及办公区。


Internet
防火墙
NIPS
入侵防御
SDN controller
SDS controller
SDN SW核心
Ctrl + 单击以选择
SDN SW汇聚云
AP
DCS、PLC
无线工控科研区
攻防演练区
服务器区
办公
培训测试
展示
安全设备区

物理架构


软、硬件检测区
外网接入区
Firewall
IPS
系统监测区
攻防演练系统
实训系统
SDN-C
SDS-C
Syslog-siem
业务仿真、目标系统虚拟、服务器
安全测评区
数据销毁恢复区
SDN基础网络
攻防演练区
内网区
外网区
工控仿真区
办公区
展示区
培训区

逻辑架构

#### 2.2.2.1 实验室基础功能

★ 信息安全技能培训：基础安全运维技能、攻防技能及信息安全岗位化技能实训；

★ 红蓝对抗演练：通过动态的攻击和防守操作提高人员安全技术实操能力；

★ 业务环境模拟：对各种业务系统运行环境进行仿真模拟，构建实验检测环境；

★ 业务系统消缺：挖掘系统安全漏洞，具备安全评估能力；

★ 应急演练：还原系统真实缺陷，提升对业务系统安全事件的应急处置能力。

#### 2.2.2.2 新技术安全研究

★ 云安全研究：开展云环境中基础设施、平台和应用的安全研究，构建软件定义的安全体系，抵御云环境下的恶意攻击；

★ 无线网络安全研究：开展无线用户认证与访问控制研究，实现无线接入侧的入侵检测及防护；

★ 数据安全研究：研究云环境下用户终端数据加密与通道传输技术，构建电力企业数据防泄漏体系模型。

★ 新能源安全接入技术研究：研究不同新能源发电设施的接入安全问题，制定针对性的安全防护措施。



02 绿盟科技能源行业成功案例集锦
SUCCESS STORIES WITH THE ENERGY SECTOR
电力 绿盟科技能源行业成功案例集锦

#### 2.2.2.3 信息安全公共服务技术支撑

★ 具备信息安全实验、测试能力，满足信息安全公共服务技术支撑所需的环境及设备要求；

★ 具备软件测评和信息安全评估服务能力、具备满足基本的系统测评和加固技术能力、具备信息安全应急响应服务能力。

### 2.2.3 客户价值

通过信息安全实验室建设，提高信息安全人员队伍的整体技术水平与安全技术服务能力。具体价值点体现如下：

★ 为省公司信息网络及信息系统安全稳定运行提供技术支持；

★ 对已上线和待上线的信息系统进行安全测评；

★ 为政府相关部门提供信息安全技术支撑；

★ 依托省公司技术优势，开展信息安全专项研究；

★ 提升信息安全人员专业技术水平，建立常态化信息安全督查及测评体系；

## 2.3 某大型发电集团信息安全攻防体系建设项目

### 2.3.1 项目背景

信息安全发展形势从过去广泛、漫无目的的攻击威胁，在数年内迅速的转化为针对受害者组织将造成严重后果的高级可持续威胁(Advanced Persistent Threat)。此类APT威胁往往可以绕过防火墙、IPS、AV以及网闸等传统的安全机制，悄无声息的从大型企业或政府机构获取高级机密资料。在2012年Verizon信息外泄调查报告中可以看到，2011年发生的重大信息数据外泄的受访组织中，有59%是在相关执法机构告知后才知道信息外泄的情况。

随着此类高级可持续威胁(APT)的不断延伸和扩散，各类新的攻击手段和入侵方法也越来越多样，这对企业内部的安全防护要求也越来越高，传统的安全防护设备已无法满足新的安全需求，企业亟需完善自身整体安全攻防体系及处理、能力，才能更好的应对新的安全风险和攻击手段。

### 2.3.2 解决方案

整体信息安全攻防体系建设项目分为调研阶段、方案编制阶段、体系建设阶段、体系完善阶段四个阶段：

前期调研阶段：通过人工访谈、现场勘查、文档调阅、问卷调查等方式了解当前中国广东核电集团的安全现状细节(人员、设备、网络架构、业务现状等)和安全隐患(DDoS攻击、蠕虫、病毒、泄密等)，并提供面向攻防体系整体层面所需的风险评估报告，为攻防体系设计提供准备。



02 绿盟科技能源行业成功案例集锦
SUCCESS STORIES WITH THE ENERGY SECTOR
电力 绿盟科技能源行业成功案例集锦

方案编制阶段：该阶段主要分为方案沟通、方案设计、方案确定三个子阶段。

1.方案沟通

首先就前期风险评估的结果中存在疑问点进行深入分析和内外部的沟通，确定相关问题点、风险点在可控的范围内；

2.方案设计

整理、分析风险评估及方案沟通阶段发现的内容，并设计攻防体系建设的方案初稿，初步确立攻防体系建设方向。

3.方案确定

最后进行内、外部的沟通、对比分析，对攻防体系建设方案初稿内容进行细化、完善，确定最终可落地的执行方案，如体系建设的实施计划及路线图，各阶段工作重心，职责分工，汇报机制等。

体系建设阶段：该阶段分为制度建设阶段和团队建设阶段

1.制度建设阶段

主要帮助制定攻防体系框架内容，包含内部培训体系、基础安全运维体系(相关制度、应急预案、变更预案等)，攻防研究建设思路(研究重点、研究方向、内部研究形式)，软件开发安全体系建设思路，攻防演练体系(对抗形式、对抗对象，对抗内容等)，信息安全事件应急响应体系(各类安全事件处理流程、制度、问责机制)以及风险合规体系(包含工作职责，工作内容、考核方式等)；

2.团队建设阶段

主要为攻防体系方案落地阶段，主要协助用户制定团队安全成员招聘计划、招聘要求、招聘方式及招聘规模等，最终能够成立自身的安全队伍，涵盖安全建设的各个领域，能够覆盖到制度建设中各个层面的职责。

体系完善阶段：该阶段分为体系试运行阶段、体系修订阶段、体系确定阶段、体系监控阶段。

1.体系试运行阶段

首先，协助针对体系运行初期存在的各类问题进行分析和辅助，协助内部团队按照预期方向顺利运行。

2.体系修订阶段

针对发现的各类问题进行记录，并中途协助对部分制度、流程进行完善，使体系更加符合内部实际运维情况。

3.体系确定阶段

确立最终攻防体系方案，对前期试运行、试修订阶段存在的问题点进行最终校对和修正，结合用户人员现状、业务需求进行最终体系方案确定，并协助制定后期体系优化计划。

4.体系监控阶段

在后续工作中，保持对体系运行效果的监控，观察体系运行效果，针对体系进行持续优化。



02 绿盟科技能源行业成功案例集锦
SUCCESS STORIES WITH THE ENERGY SECTOR
电力 绿盟科技能源行业成功案例集锦

### 2.3.3 客户价值

绿盟科技结合自身在能源行业的安全建设经验积累和用户安全现状，协助用户建立了信息安全攻防体系，同时组建了信息安全攻防团队，使用户具备应对内、外部网络环境的已知或未知的威胁的能力，为集团的信息化安全建设提供长远支持。

## 2.4 某发电企业信息安全等级保护建设项目

### 2.4.1 项目背景

随着我国国民经济和社会发展信息化进程的全面加快，我国信息化的程度越来越高，关系国计民生的重要领域信息系统已经成为国家的关键基础设施。这些基础信息网络和重要信息系统安全，已经严重关系国家安全和社会稳定，关系到企业单位的集体利益，关系广大人民群众切身利益。

从国家层面，实行等级保护可以有效解决我国信息安全面临的威胁和存在的主要问题，充分体现“适度安全、保护重点”的目的，将有限的财力、物力、人力投入到重要信息系统安全保护中，按标准建设安全保护措施，建立安全保护制度，落实安全责任，有效保护基础信息网络和关系国家安全、经济命脉、社会稳定的重要信息系统的安全，有效提高我国信息安全保障工作的整体水平。另外，开展信息安全等级保护工作是保护信息化发展、维护国家信息安全的根本保障，也是信息安全保障工作中国家意志的体现

从企业层面，实行等级保护，可以让我们明确企业的安全需求，可以根据企业信息系统的实际安全需求，因地制宜地对系统进行安全定级，并根据所确定的信息系统级别，按照国家相应的标准进行规范的保护，在有限的财力、物力、人力投入条件下，能够将资源放入到最重要的地方，达到“经济安全”的目的，按照等级保护标准，还可以建立完善的安全保护制度，有效地保护企业信息系统的安全。

## 2.4.2 解决方案

依据国家相关信息安全等级保护政策及技术标准，结合客户实际业务需要，依据信息安全等级保护设计方案，进行的信息安全等级保护整改工作，包括设备采购、系统集成和实施工作，从而进一步做好信息系统等级保护工作。

整体分为三个阶段进行：信息安全咨询设计阶段、信息安全整改实施阶段和信息安全等级测评及运行维护阶段。

★ 第一阶段：完成信息系统定级、备案等工作，进行信息系统总体安全规划和设计。

★ 第二阶段：在信息系统总体安全规划和设计基础上，提出系统整改实施方案；对当前信息系统的不符合项进行整改。

★ 第三阶段：通过信息安全等级测评机构对已完成等级保护建设的信息系统进行等级测评，确保信息系统的安全保护措施符合相应等级的安全要求，推进下属单位整改和测评工作。



02 绿盟科技能源行业成功案例集锦
SUCCESS STORIES WITH THE ENERGY SECTOR
电力 绿盟科技能源行业成功案例集锦

整体服务流程框架如下图所示


## 2.4.3 客户价值

通过信息系统安全等级保护项目的实施，以等级保护为核心思想，建立科学的信息安全保障体系；通过等级保护项目建设，全面识别业务系统在信息安全技术层面和管理层面的不足和差距，充分借鉴国内信息安全实践和成熟的理论模型，设计合理的安全管理措施和技术措施，通过

建设实践，建立起符合内部需要和外部监管的信息安全保障体系。本项目依据国家相关信息安全等级保护政策及技术标准，结合实际业务需要，依据信息安全等级保护设计方案，进行的信息安全等级保护整改工作，包括设备采购、系统集成和实施工作，从而进一步做好信息系统等级保护工作。

## 2.5 国网某网省信息内网安全监控项目

### 2.5.1 项目背景

国网公司”SG186”工程安全防护要求各安全域分为网络边界、网络环境、主机系统及应用环境四个层次实施安全防护措施。目前网络环境作为整个信息化系统建设的基础承接平台还缺少有效的监控手段，大量的报警时间过多，难以有效分析处理，建立本部到基层单位的两极分布式监控服务管理，形成统一的管理组成管理部署构架，集中收集和处理实现全面的信息收集。通过建立网络安全监控响应体系结合日常巡检。可有效提高信息内网网络安全运行水平。

### 2.5.2 解决方案

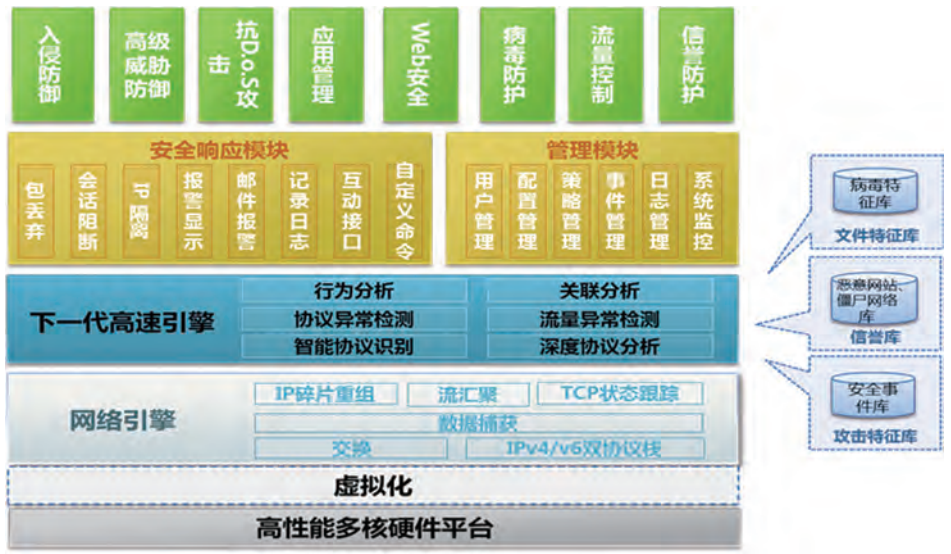
建立国网某网省公司全网监控服务中心，在多个服务器网段，基层汇聚交换机，各信息区域汇聚接入交换机，以及地市级供电公司，直属单位信息内网建设总共20多个监控点。

绿盟科技提供分级内网检测解决管理方案，分两级网络上部署NSFOCUS NIDS的安全中心，



02 绿盟科技能源行业成功案例集锦
SUCCESS STORIES WITH THE ENERGY SECTOR
电力 绿盟科技能源行业成功案例集锦

在网省公司安全中心统一管理，保持整个系统的安全策略的完整统一性。




★ 入侵检测

实时、主动拦截黑客攻击、蠕虫、网络病毒、后门木马、D.o.S等恶意流量，保护企业信息系统和网络架构免受侵害，防止操作系统和应用程序损坏或宕机。

★ 高级威胁防护

高级威胁防护能够基于敏感数据的外泄、文件识别、服务器非法外联等异常行为检测，实现内网的高级威胁防护功能。

★ 僵尸网络发现

基于实时的信誉机制，结合企业级和全球信誉库，可有效检测恶意URI、僵尸网络，保护用户在访问被植入木马等恶意代码的网站地址时不受侵害，第一时间有效拦截Web威胁，并且能及时发现网络中可能出现的僵尸网络主机和C&C连接。

★ 应用管理

全面监测IM即时通讯、P2P下载、网络游戏、在线视频，以及在线炒股等网络行为，协助企业辨识非授权网络流量，更好地执行企业的安全策略。

## 2.5.3 客户价值

在全网省公司范围内形成两级全网信息安全监控体系，通过集中运行监控平台，优化现有



02 绿盟科技能源行业成功案例集锦
SUCCESS STORIES WITH THE ENERGY SECTOR
电力 绿盟科技能源行业成功案例集锦

It运维支撑系统，实时掌握网络与系统的运行情况，及时发现入侵、病毒、流量异常、网络等安全问题及安全隐患，迅速定位，并尽快解决，为日常安全管理、业务稳定运行提供有力的保障。

# 2.6 某电力公司ERP系统安全咨询项目

## 2.6.1 项目背景

某电力公司开展业务系统建设工作，业务系统将采用ORACLE的基本ERP模板，并根据自身业务需求进行定制，虽然通过该业务项目可以大大提升工作效率，企业管理的标准化水平，但是如果实施的系统中存在安全漏洞，与国家相关法律法规和行业内监管标准存在偏差，则反而会对电力企业正常运作、企业形象造成负面影响。

为对公司ERP系统建立完整的信息安全防护体系，规避系统建设投运后的各类信息安全风险，根据国家相关部门对于重要信息系统建设在信息安全方面的“规定动作”，满足“信息系统安全等级保护测评准则”、上市企业风控管理等相关政策要求，也为落实集团公司对于年度重要信息系统安全建设“三同时”工作部署(同时设计、同时实施、同时投运)，因此在公司ERP项目建设的同时，同步启动“公司ERP系统信息安全咨询和测评服务”项目。

## 2.6.2 解决方案

在ERP系统信息安全咨询和测评服务”项目中，绿盟科技根据前期的现场调研提供了一整套的安全咨询服务内容，包括：

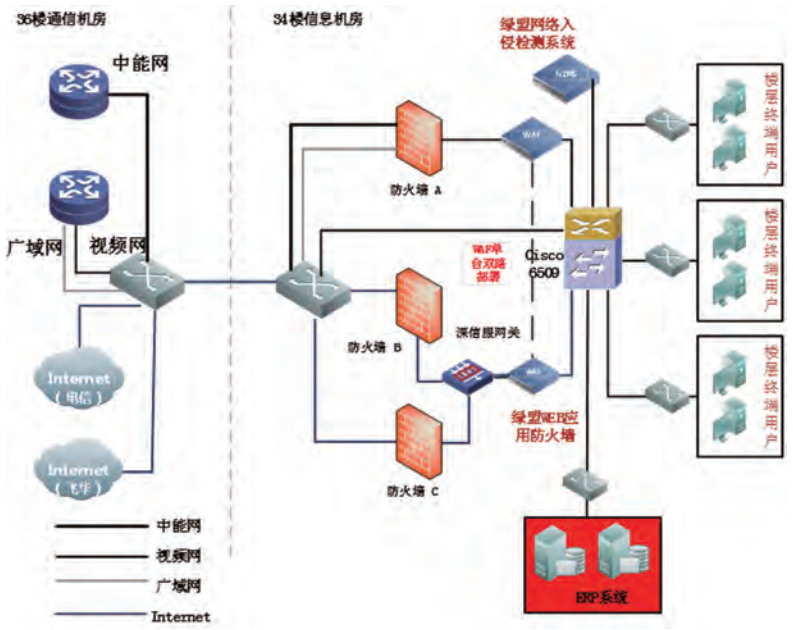
1.ERP系统等级保护建设工作，包括符合性测评、差距分析、建设整改等工作

2.ERP系统风险评估工作，包括安全基线、渗透测试、代码审计等工作

3.ERP系统应急预案编制工作

4.人员安全培训工作

并且在后期的ERP系统安全整改中，部署绿盟网络入侵防护系统和WEB应用防火墙两套设备，抵御ERP服务器群组面临的各类安全威胁，满足合规要求。








### 2.6.3 客户价值

绿盟科技通过专业、可靠、持续的安全服务，使用户用低廉的费用就可以拥有科学、规范和专业的安全服务，从而无忧地专注于自身业务的发展，降低安全风险、提高网络系统安全水平，达到了《电力行业信息系统安全等级保护基本要求》，并且顺利通过测评，以最少的投资实现既定的安全控制目标。

## 2.7 某省供电局ISO27001信息安全体系建设项目

### 2.7.1 项目背景

为对XX供电局局的关键信息资产进行全面系统的保护、使信息风险的发生概率和结果降低到可接受水平，全面、专业地规范信息安全管理工作，提高XX供电局信息安全管理水平，适应南方电网公司信息安全管理工作一体化的要求，ISO27001信息安全管理体系建设项目作为XX省电网公司2012年第二批信息化试点项目下达。在本项目能够取得良好效果后，将在全省范围进行推广。

### 2.7.2 解决方案

采用绿盟安全体系框架与ISMS体系框架两者有效结合。以业务风险为中心，以流程为导向，围绕信息系统生命周期，逐步建立由安全组织、管理和技术构成的具有自我完善能力的安全保障

体系。建立一个有效的、完善的信息安全管理体系，国际公认的、最有效的方式是采用ISO27001建议的PDCA过程方法，并参照ISO27002的最佳实践，分部门、分系统的逐步建立并实施信息安全管理体系。

绿盟科技在国际信息安全管理标准ISO27001的11类要求基础上，将PDCA(Plan、Do、Check和Act)持续改进的信息安全管理模型作为贯穿整个项目过程的主要指导思想。


PDCA 模型

为了建设信息安全管理体系(ISMS)， 首先应确定来自客户、合规方面的需求和期望，明确认证范围，然后：



02 绿盟科技能源行业成功案例集锦
SUCCESS STORIES WITH THE ENERGY SECTOR
电力 绿盟科技能源行业成功案例集锦

★ 在计划(Plan)阶段通过风险评估来了解安全需求，然后根据需求设计解决方案；

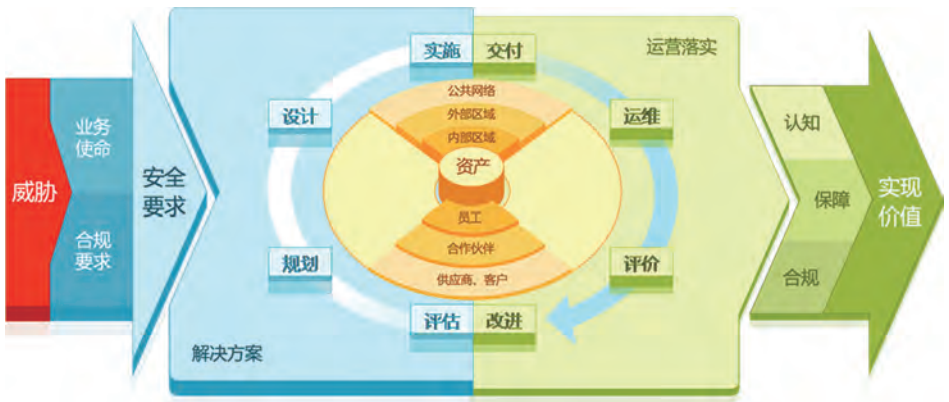
★ 在实施(Do)阶段将解决方案付诸实现；

★ 在检查(Check)阶段监视和审查解决方案是否有效，是否有新变化；

★ 在改进(Act)阶段予以解决发现的问题，以改进ISMS。

通过这样的过程周期，绿盟科技协助用户提供培训和技术转移，帮助用户掌握自行运作和管理ISMS的能力，以保证组织将确切的信息安全需求和期望转化为可管理的信息安全体系。

多年来，绿盟科技一直致力于协助用户建立有特色的信息安全体系，在安全建设的过程中了解到了众多客户的共性疑惑，并针对性的提出了绿盟科技的典型信息安全建设过程。




绿盟科技安全建设过程

威胁是永远存在的，它会对企业/组织的业务施加影响，加之企业/组织所处环境的合规要求，安全需求驱动了安全建设的过程。

商业机密、重要资产对企业/组织的重要性不言而喻，对它们的保护已经成为企业/组织业务活动中重要的过程。安全保证的过程是复杂的，因此需要整体性的安全思路。

风险管理是企业/组织安全活动的基本过程，以资产为核心，考虑到内部员工、合作伙伴、供应商、客户，内部区域、外部区域和公共网络。人和空间的不同，已经让安全变得复杂。

绿盟科技认为，安全建设的过程应涵盖如下阶段：评估、规划、设计、实施、交付、运维、评价、改进，它基于 PDCA 的思想。

通过绿盟科技安全建设过程，我们协助用户提高安全认知、获得安全保证、满足合规要求。用户会了解到当前的现状、与目标的距离、与要求的差距、科学的思维方式、良好的工作方法；也会得到信心、放心、省心的安全保证；用户不再为日益严厉的合规要求所困惑。

整体的安全思路，让安全变得清晰和简单。

### 2.7.3 客户价值

在遵循国家的信息安全政策法规及相关管理标准规范下，为XX供电局梳理出一套标准化，层次化，一体化的管控体系框架，以适应于南方电网公司信息安全管理工作一体化的要求，提升



02 绿盟科技能源行业成功案例集锦
SUCCESS STORIES WITH THE ENERGY SECTOR
电力 绿盟科技能源行业成功案例集锦

Xx供电局信息安全管理体系的可用性、可行性和可落地性。

★ 完善及优化XX供电局的信息安全管理标准框架。

★ 完善和深化标准：推广和落实南方电网公司、XX省电网公司信息安全管理标准，结合管控流程促进标准规范落地。

★ 强化XX供电局信息安全管理自我改进能力：

★ 使XX供电局的信息安全管理达到ISO27001的认证要求。

## 2.8 某发电厂电力二次系统安全防护整改项目

### 2.8.1 项目背景

发电厂是生产为主要业务方向，对于信息安全的关注度不足。从技术上安全防护措施不足，基本是以边界安全防护为主，而边界防护基本以防火墙为主要防护措施。而管理也存在很的薄弱环境，如生产系统中无相关的安全人员和与信息安全相对应的制度等。本方案提供的方案内容主要从技术和管理两个方面为电厂的信息安全防护提供相关的思路。其中技术方面包括：

★ 网络安全域设计

★ 网络边界安全防护

★ 网站安全防护

★ 数据防泄露

★ 运维安全

★ 电力监控系统安全防护

其中管理方案包含：

★ 电厂安全风险评估

★ 运维安全设计

★ 应急响应建设

★ 安全培训

某发电厂依据国家经贸委[2002]第30号令《电网和电厂计算机监控系统及调度数据网络安全防护的规定》、发改委[2014]14号令《电力监控系统安全防护规定》、国家能源局《电力行业等级保护指导规范》和国家能源局36号文《发电厂监控系统安全防护评估规范》的要求，参照信息安全等级保护三级评判标准，于2012年针对本厂计算机监控系统开展等级保护测评和风险评估工作。主要评估计算机监控系统相关资产面临的威胁以及威胁利用脆弱性导致安全事件的可能性，并结合安全事件所涉及的资产价值来判断安全事件一旦发生对单位造成的影响。目的是规范和统



02 绿盟科技能源行业成功案例集锦
SUCCESS STORIES WITH THE ENERGY SECTOR
电力 绿盟科技能源行业成功案例集锦

一我国电网和电厂计算机监控系统及调度数据网络安全防护的规划、实施和监管，以防范对电网和电厂计算机监控系统及调度数据网络的攻击侵害及由此引起的电力系统事故，保障我国电力系统的安全、稳定、经济运行，保护国家重要基础设施的安全。

本项目主要涉及某发电厂的计算机监控系统的安全建设。在项目方案中从技术和管理两个来分析发电厂面临的安全威胁，涉及技术和管理两个维度来解决发电厂所面临的安全问题。内容中涉及了安全策略、技术、管理和运维四大子体系。

本项目的目标是：

★ 针对测评过程中发现的问题，设计一套适用于某发电厂计算机监控系统信息安全需求的方案，保障业务的稳健运行，保障信息系统业务使命的顺利达成，满足业务的安全需求和合规性要求。

★ 控制网络安全风险，降低系统风险。并且可以更好的利用系统安全措施，发挥安全设备的利用率。

★ 通过技术与管理的结合来提升企业在安全防护上的能力，规避由于信息安全风险给企业所带来的影响。

★ 建立起一套适用于电厂的有纵深的防护体系，最大限度的保障电厂各个系统的安全，做到威胁可感知、威胁可防护。

## 2.8.2 解决方案

结合电力二次系统安全防护的要求，从生产控制大区区域来考虑信息安全的建设，考虑信息

安全建设中同时兼顾技术和管理两个方面安全建设的需求。防护思路是依据对现有电厂信息安全建设方面分析出的薄弱项同时结合P2DR模型中的思路，对于生产控制大区，主要以满足新的发改委14令要求及业界最佳实践为依据，形成一套针对电力生产系统的安全安全防护思路。

**生产控制大区**

**基于14号令要求、SP800-82**

**安全防护基本要求**
网络：网络审计、网络入侵检测
主机：主机审计、主机加固、登录认证
应用：业务审计、登录认证
数据：数据备份及数据安全
**安全管理：**
组织、制度、人员职能
**风险评估：**
技术、管理

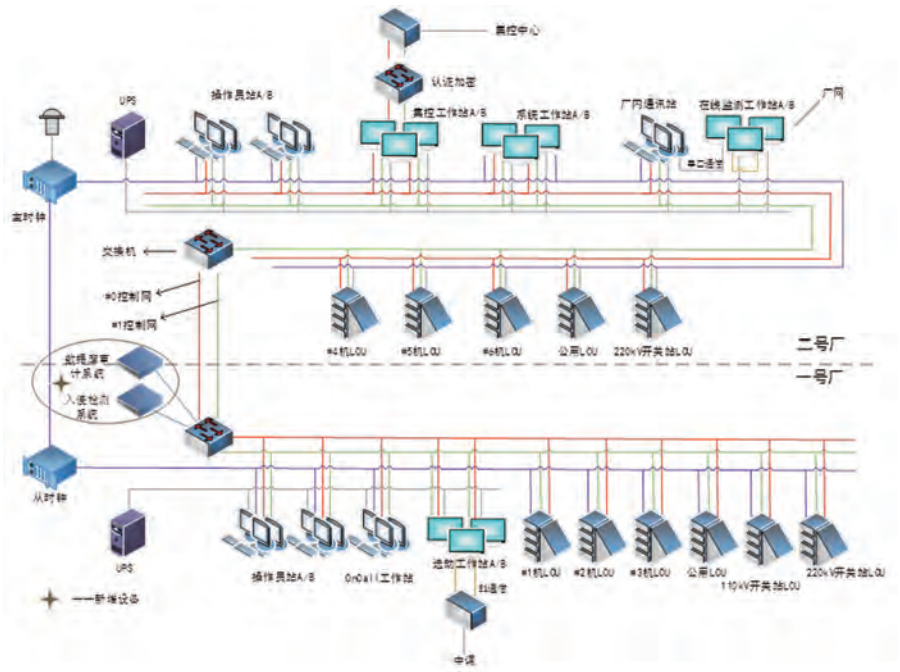
**纵深防护要求**
入侵安全检测
异常行为审计
信息安全应急响应



02 绿盟科技能源行业成功案例集锦
SUCCESS STORIES WITH THE ENERGY SECTOR
电力 绿盟科技能源行业成功案例集锦

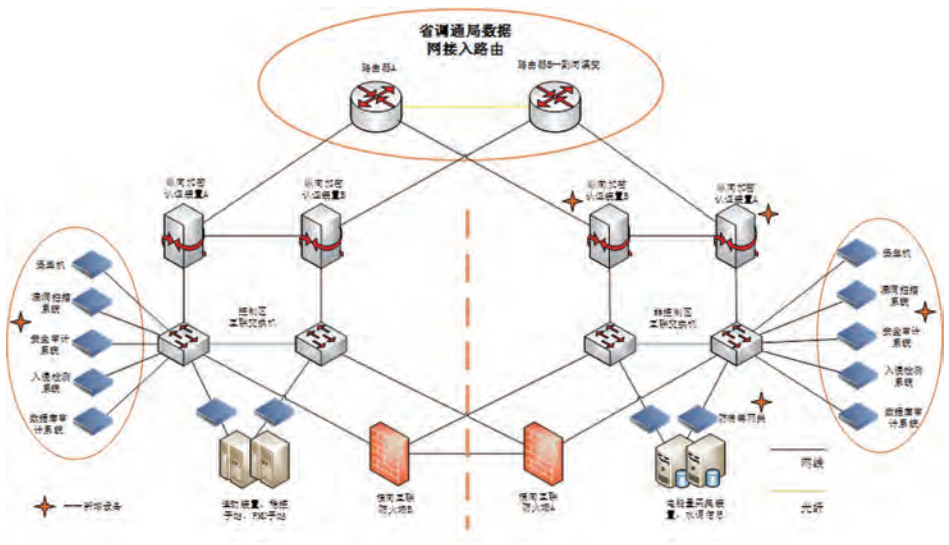
### 2.8.2.1 安全技术方案

根据《电力行业信息系统安全等级保护基本要求》对生产控制系统的安全保护要求，以及第三章对于计算机监控系统面临的一系列安全风险分析， 通过为满足物理安全、网络安全、主机安全、应用安全、数据安全五个方面基本技术要求进行综合防护建设，通过立体、纵深的安全保障防御体系，提升工控系统整体的安全保护能力，建议将网络进行如下调整：




某发电厂计算机监控系统网络拓扑图（增强版）

其中，入侵检测系统针对计算机监控系统中的可疑流量进行检测，数据库审计系统针对系统中的历史站操作进行审计。




某发电厂至省调通局、集控中心二次安防网络拓扑图（增强版）





### 2.8.2.2 安全服务方案

★ 电厂安全风险评估

通过安全评估发现电厂某个系统的安全隐患及其可能危害，全面了解信息系统的安全现状，为组织解决安全问题、降低安全事件发生的风险提供依据。

★ 应急计划及事件响应

应急计划是在信息系统发生紧急安全事件（包括入侵事件、软硬件故障、网络病毒、自然灾害等）之后，为尽快恢复其正常运行，降低安全事件的负面影响而制订的预案。有关应急计划内容应包括计划制订、计划培训和计划演练。

事件响应是在安全事件发生后根据应急计划对事件进行监控、处置和报告，采取措施将损失降到最低程度并从中吸取教训的活动。事件响应工作应包括事件监控和事件处置。

★ 安全培训

将安全教育和培训统一纳入到电厂人力资源管理的教育培训流程中去，安全教育和培训是通过宣传和教育的手段，确保相关工作人员和信息系统管理维护人员充分认识信息安全的重要性，具备符合要求的安全意识、知识和技能，提高其进行信息安全防护的主动性、自觉性和能力。

该项工作在管理体系中明确，选择有相关服务资质和经验的安全厂商或咨询厂商提供培训，每年1-2次。

### 2.8.3 客户价值

#### 2.8.3.1 管理效益

管理效益主要体现在以下几个方面：

★ 固化管理模式，使安全思想能贯彻到日常业务活动中；

★ 保障业务安全运行，提升业务处理效率；

★ 实时准确掌握企业信息安全动态和数据，为企业管理者提供有效的决策支持；

★ 实现对非法人员的可知、可拦、可查，强化企业的内部控制。

#### 2.8.3.1 水平提升

水平的提升主要体现在几个方面：

★ 通过安全规划的实施，可以使信息系统达到电力企业关于电力信息安全等级保护的基本要求，并提升合规性水平；

★ 通过信息安全队伍的建设可以提高信息安全意识水平；

★ 信息安全防范技术水平将得到普遍的提高；

★ 提升安全综合防护的能力，做到可防、可控、可恢复。





## 2.9 某大型发电集团工业控制系统信息安全保障咨询项目

### 2.9.1 项目背景

近十年来，随着信息技术的迅猛发展，信息化在企业中的应用取得了飞速发展，互联网技术的出现，使得工业控制网络中大量采用通用TCP/IP 技术，工业控制网络和企业管理网的联系越来越紧密。另一方面，传统工业控制系统采用专用的硬件、软件和通信协议，设计上基本没有考虑互联互通所必须考虑的通信安全问题。企业管理网与工业控制网的互联也减弱了控制系统与外界的隔离，工业控制系统的安全隐患问题日益严峻。

2011 年工信部发布《关于加强工业控制系统信息安全管理的通知》，通知明确指出：“SCADA、DCS、PCS、PLC 等工业控制系统广泛运用于工业、能源、交通、水利以及市政等领域，用于控制生产设备的运行。随着计算机和网络技术的发展，特别是信息化与工业化深度融合以及物联网的快速发展，工业控制系统产品越来越多地采用通用协议、通用硬件和通用软件，以各种方式与互联网等公共网络连接，病毒、木马等威胁正在向工业控制系统扩散，工业控制系统信息安全问题日益突出。2012 年国务院颁发《关于大力推进信息化发展和切实保障信息安全的若干意见》，强调工控系统信息安全事关工业生产运行、国家经济安全和人民生命财产的安全，必须切实加强工控系统信息安全管理。

按照电力二次系统安全防护要求和国能36号文要求，强化了对于电力系统边界的安全防护要求。但是，随着能源互联网、互联网+在能源生产系统中的应用，传统封闭的电力工业控制系统会

逐步向开放的架构发展，同时阶段来说从外部运维管理、内部运维管理、人员管理操作、相关控制设备以功能实现为主，设备潜在的安全隐患和预留相关的调试和通信方式等问题，给工控系统的安全性带来很大的不确定。

## 2.9.2 解决方案


防护方案总体架构





以成熟度、复杂度高的火电为研究对象，参照电力二次系统安全防护的技术成果，遵循国际工控信息安全标准，结合我国工业过程测量、控制和自动化网络与系统信息安全标准，从技术和管理两个层面设计、规划工业控制系统安全防护体系。在满足合规性要求基础上，为了进一步提升工控系统抵御外部威胁的能力，需要从工控系统全生命周期的安全的角度来考虑系统的安全建设，结合业务过程中对安全性的要求及验收规范的要求，通过对系统投运前的安全检测来尽可能的减少系统中潜在的安全隐患。工控系统的特殊性，决定了通信过程的确定性，采用异常检测的手段有效的发现系统中存在的流量过载情况及未知的通信流量，进而发现系统中潜在的异常行为，同时结合在主机终端侧的进程级白名单的机制、通信过程的白名单及业务规程结合，来发现隐藏正常通信和应用过程中的异常通信。

## 2.9.3 客户价值

通过本项目涉及的一系列重要措施的落地实施方案，包括重要专项管理措施实施方案、技术防护体系实施方案、重要专项防护措施实施方案，这些实施方案要能够体现出清晰的实施内容、目标、方式、路线以及项目预算等内容；重点管理专项方案能够指导具体的工作程序与管理活动，技术专项方案能够指导后续防护系统建设的采购、部署与运行。

★ 满足合规性要求，如14号令（国能36号文）的落地要求；

★ 提升了组织架构在安全能力方面的适应性，做到生产环境人员的岗位匹配；

★ 由合规性安全能力逐步向全生命周期的安全管控能力提升；

## 2.10 国网某网省公司智能变电站安全建设项目

### 2.10.1 项目背景

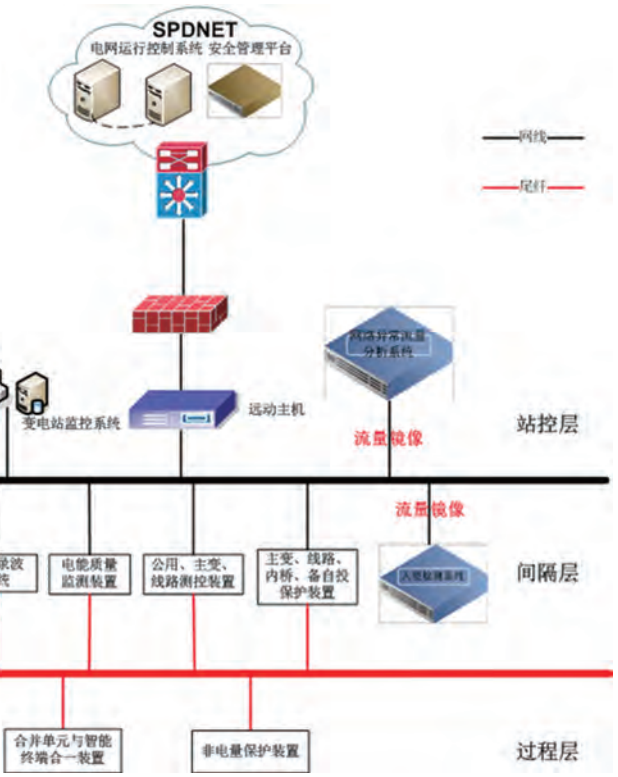
伴随着全球经济的不断增长，大电网向着远距离、超高压甚至特高压方向发展，网络规模日益庞大，结构日益复杂，大电网的复杂性网络特征日益显露，大电力系统脆弱性分部更加广泛，不得不承受着发生多重故障或连锁性故障所引起的大面积停电事故的更大潜在风险。变电站作为智能电网发-输-变-配-用-调各个环节中呈上启下的关键环节，是智能电网的核心支撑资源，直接关乎着不同区域电量的供给问题，在大电力的统一框架之内，变电站安全防护体系的研究凸显非常迫切的要求。

### 2.10.2 解决方案

智能变电站二次系统的防护目标是抵御黑客、病毒、恶意代码等通过各种形式对变电站二次系统发起的恶意破坏和攻击，以及其它非法操作，防止变电站二次系统瘫痪和失控，并由此导致的变电站一次系统事故。安全防护体系将由安全管理、平台加固、通信防护、集中监控这四个部分组成。

### 2.10.3 客户价值

通过智能变电站的安全防护体系建设，除了要满足电力二次系统安全防护总体原则“安全分区、网络专用、横向隔离、纵向认证”的基本要求外，还实现了以“安全管理、平台加固、通信防护、集中监控”为核心的立体全面的安全防护体系。




智能变电站安全防护逻辑拓扑图

# 03 石油、石化
# PETROLEUM AND PETROCHEMISTRY



# 石油、石化
PETROLEUM AND PETROCHEMISTRY

## 3.1 某大型油化央企大规模分布式威胁识别集中管控项目

### 3.1.1 项目背景

随着我国石油石化业务系统的推广，大量的应用系统建设于总部和各分支企业，不断增加的应用在提高工作效率、带来经济效益的同时，日益庞杂的信息系统也为运维管理人员带来了更大的挑战。其中利用已知或未知的系统漏洞，对信息系统造成入侵和损害，窃取敏感信息，危害业务系统的正常运行等行为，已经成为各种安全事件发生的主要根源之一。

如何高效统一的对单位总部、各区域网络中心和各分支企业的资产如网络设备、主机系统、中间件及Web应用程序进行漏洞扫描和配置检查，及时全面的发现信息系统中存在的各种脆弱性问题，集中实现信息安全漏洞告警和相关风险，并给出相关漏洞威胁的解决办法，成为亟待解决的问题。

### 3.1.2 解决方案

本方案通过分布式部署，统一管理的方式，将绿盟远程安全评估系统(RSAS)部署集团公司、各区域中心和各下属企业，并在集团总部部署绿盟ESPC作为管理中心，统一管理各地远程安全评估设备。通过此方案，绿盟科技针为用户提供如下功能：

★ 对网络设备、操作系统、数据库、中间件等进行漏洞扫描和安全基线检查；

★ 实现统一管理中心与信息安全管控中心集成；

★ 实现统一管理中心与统一身份管理系统和CA系统结合；

★ 实现统一管理中心审批管理工作流程。

### 3.1.3 客户价值

通过本项目的实施部署，项目单位建立了全集团自动的威胁识别系统，形成了漏洞管理、安全基线管理的全方位网络威胁管理体系，能够对全集团的网络设备、主机系统、中间件及Web应用程序进行漏洞扫描和配置检查，全面发现信息系统中存在的各种网络脆弱性问题。

★ 项目单位能够利用此系统对全集团做网络安全检查，并了解集团网络脆弱性情况。

★ 用户通过本系统，统一了全集团的网络安全检查的标准。

通过本系统，用户能够掌握集团内各单位进行网络脆弱性自查的频率情况。



03 绿盟科技能源行业成功案例集锦
SUCCESS STORIES WITH THE ENERGY SECTOR
石油、石化 绿盟科技能源行业成功案例集锦

04 煤炭
COAL



# 煤炭
COAL

## 4.1 某大型煤炭集团广播电视网络信息安全保护研究与应用项目案例

### 4.1.1 项目背景

如今，广播电视网正朝着数字化、网络化、信息技术高度集成化方向迅猛发展。各种数字广播电视业务比如：信息资源采集、编辑、播出等依靠网络技术和信息技术的发展也获得了突飞猛进的效果，但是这些技术对网络技术日益依赖，表现出了安全上的脆弱性。

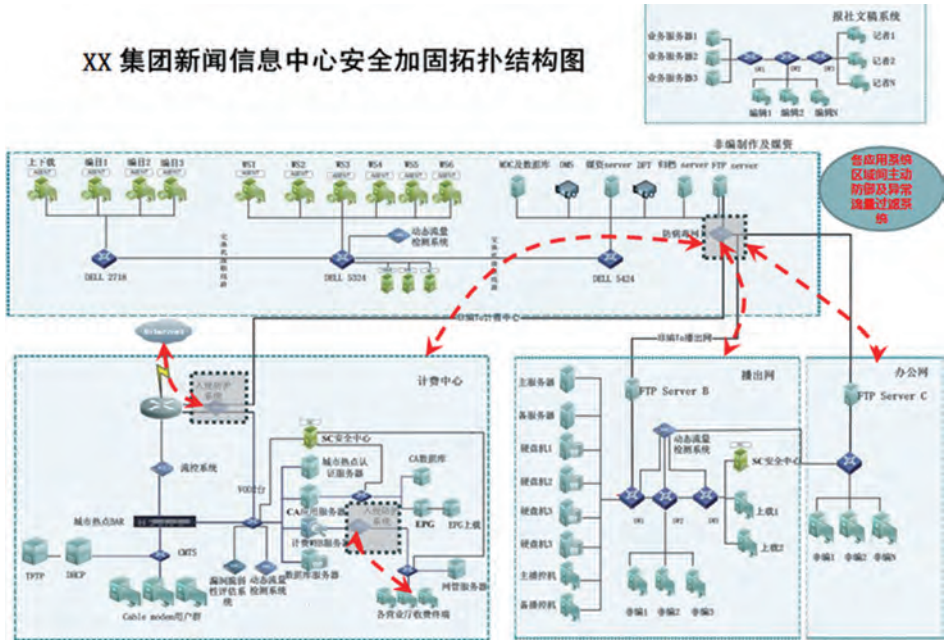
广播电视网作为支撑集团经济、精神、文化传播的核心重要平台，如何保障广播电视网高效、稳定、安全运行就成为一个重要的研究课题。

国家十二五发展规划对广播电视网信息安全保护提出了明确要求，并且制定了相关信息安全防护规范，如：《广播电视相关信息系统安全等级保护基本要求》《广播电视安全播出管理规定》(总局62号令)等。广播电视信息系统安全防护的核心是保证与播出相关的信息系统具备与其安全保护等级相适应的安全保护能力。

### 4.1.2 解决方案

1.外部、各区域边界入侵防护及病毒过滤系统建设

通过对网络架构和新闻信息中心数据业务流向的分析，在计费中心、非编网、播出网、办公网四个区域 网络之间都存在数据交互和边界安全的问题。

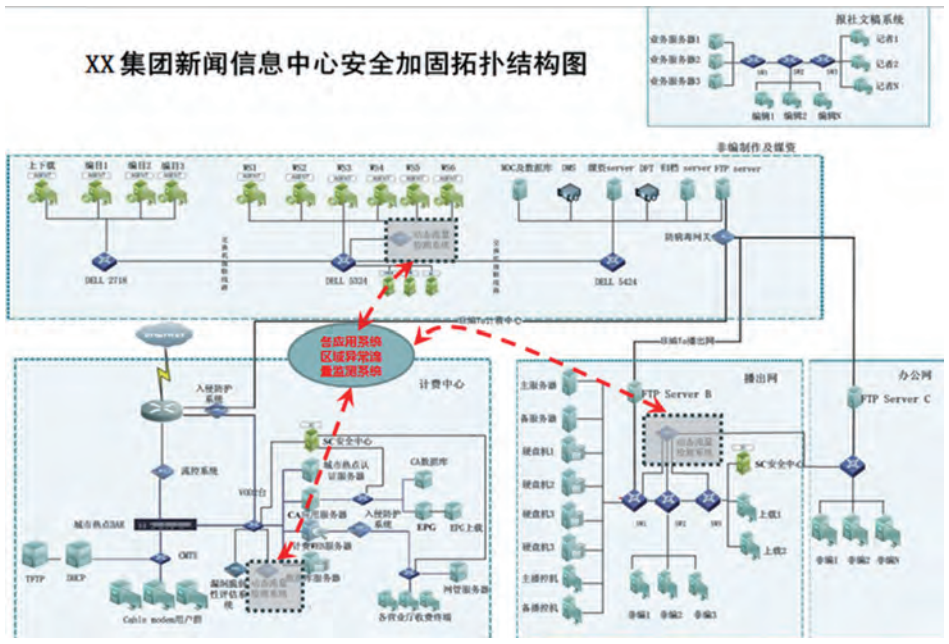



2.内部异常流量动态监测及安全风险度量建设

在计费中心、播出网、办公网、非编制作及媒资四个区域网络内部署动态流量检测系统，实时检测四个网络区域内的的网络行为和异常流量。对网络区内的流量变化情况进行实时掌握并当攻击发生时进行快速定位追踪。

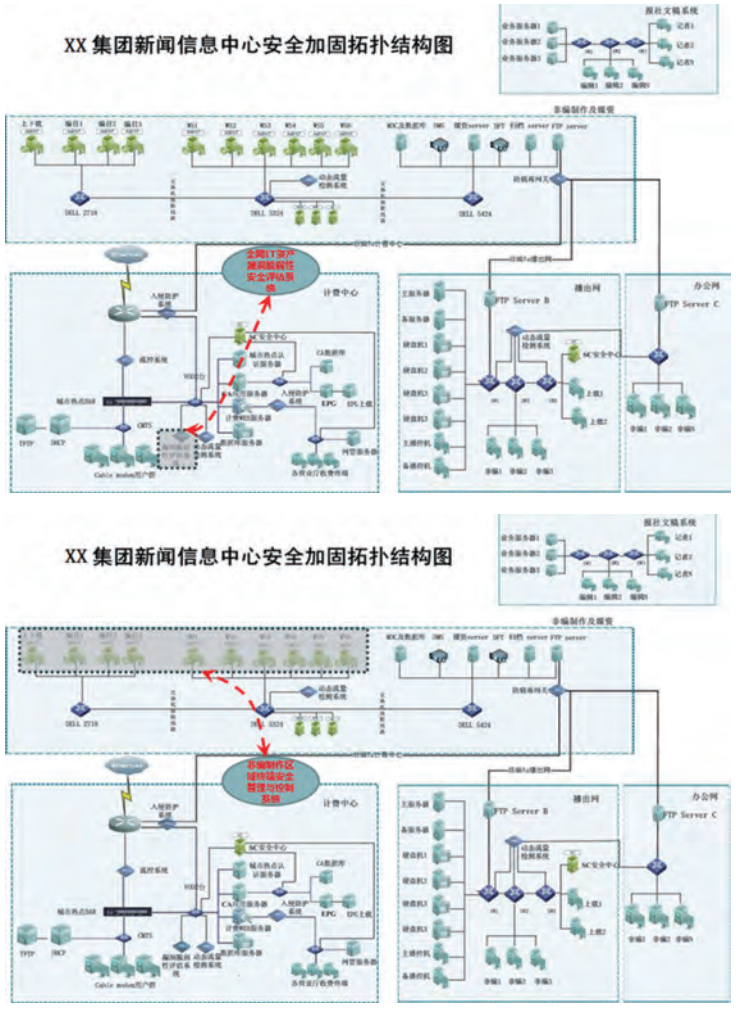


04 绿盟科技能源行业成功案例集锦
SUCCESS STORIES WITH THE ENERGY SECTOR
煤炭 绿盟科技能源行业成功案例集锦




3.内网安全威胁管理及边界流量控制建设

对信息系统的恶意代码、补丁升级等进行集中统一管理；对网络设备、服务器、应用系统、安全设备等的安全事件信息进行关联分析及风险预警；对信息系统网络设备、终端、服务器以及应用系统威胁统一分析。在非编制作及媒资网络区域内的终端上部署终端安全管理系统，并在本网络内部署一台EPS管控中心对本区域内的所有终端实施有效地管控。




04 绿盟科技能源行业成功案例集锦
SUCCESS STORIES WITH THE ENERGY SECTOR
煤炭 绿盟科技能源行业成功案例集锦

## 4.1.3 客户价值

在信息安全防护方面，随着计算机网络的普及，带来了越来越多的安全课题，本课题从新闻信息中心内部网络的防护为出发点，研究信息系统的安全保障体系，取得成果之后，逐步向全集团公司推广，保障XX集团的信息安全和网络运行稳定。