1.1 案例十一：某火力发电厂工控安全解决方案——护航火力发电厂工业控制系统安全

1.1.1 方案概述

本方案针对DCS系统、SIS系统的安全问题进行完善，按照国家和电力行业相关网络安全防护的政策与网络安全防护体系要求，针对火力发电生产控制技术发展，利用当前先进的网络安全防护理念、技术与产品，建设纵深立体的网络安全防护体系，辅助企业建立网络安全监测、通报预警与联动处置机制，为综合安全防护能力提供技术支撑，为火力发电企业生产控制系统安全运行提供必要的网络安全保障。

1.方案背景

电力系统的安全发展和安全稳定运行关系到国计民生，而在电力系统当中，要保证电力系统的安全、稳定运行，网络安全防护工作显得十分重要。近年来，针对电力系统的网络安全攻击事件屡屡发生，“伊朗核电站震网病毒事件”、“ 乌克兰电网大面积停电事件”等，更给电力系统的网络安全防护工作敲响警钟。

2017年6月，《中华人民共和国网络安全法》的实施，提出实行等级保护制度，明确网络运营单位应当按照网络安全等级保护制度的要求，履行安全保护义务，采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。《中华人民共和国网络安全法》及GB/T 22239-2019 《网络安全等级保护基本要求》等一系列法律及行业规定要求的颁布实施，更进一步凸显电力系统运营单位开展网络安全防护工作的重要性、逼迫性和必要性。

2.方案简介

本方案主要是针对某火力发电厂的DCS系统、SIS系统等工控系统安全防护建设。

某火电厂建设2台66万千瓦燃煤机组。其机组配套DCS系统控制系统为和利时DCS分散控制系统，两台单元机组、公用系统均独立组网，整体构成某火电厂发电监控系统。DCS通过UDP接口程序将生产数据经过单向隔离装置发送到SIS系统。SIS系统为大唐先一建设集成，采集1#DCS、2#DCS、公用等数据，通过SIS核心网络写入实时数据库，实时数据库经单向隔离同步到管理信息大区的镜像数据库，用于生产经营应用。

3.方案目标

依据电力行业已发布的国家与行业标准规范，设计、建设DCS系统、SIS系统加固信息安全防护体系：

深度检查：面向应用层对特有的工业通讯协议进行内容深度检查，告别病毒库升级缺陷；

安全审计：完善的安全审计平台，对网络运行日志、操作系统运行日志、安全设施运行日志等进行集中收集、自动分析，及时发现各种违规行为以及病毒和黑客的攻击行为；

威胁检查：部署于网络边界的威胁检测系统能够快速准确发现入侵监控系统的病毒和恶意代码，并实施清除并报警。

实时报警：所有部署的工控信息安全产品都能由管理平台统一进行实时监控，任何非法的（没有被组态允许的）访问，都会在管理平台产生实时报警信息，从而故障问题会在原始发生区域被迅速的发现和解决。

实现以下建设目标：

（1）提高DCS系统、SIS系统信息安全防护能力

基于某火电厂 DCS 系统、SIS 系统网络安全现状，在工业控制系统的主机层和网络层进行安全加固、入侵检测、安全审计和边界防护以有效抵御来自工控网络内部、外部的病毒、入侵、渗透以及违规操作行为对 DCS 系统、SIS 系统造成破坏，防范信息安全事故的发生。

（2）满足合规性要求

方案建设满足能源局 36 号文中综合防护的要求，提供网络内部入侵检测、主机与网络设备加固、安全审计和恶意代码防护的要求，使某火电厂 DCS 系统、SIS 系统安全防护措施达到国家监管部门对发电企业的要求。

（3）方案成果的应用

此方案的进一步加强了某火电厂 DCS 系统、SIS 系统信息安全的重视程度和实施力度，将切实保证免受病毒、恶意代码等威胁，保持安全稳定运行的状态。

1.1.2 方案实施概况

方案结合火力发电厂工业控制系统的实际安全需求和等级保护 2.0、电力 36 号文“安全分区、网络专用、横向隔离、纵向认证、综合防护”，实现事前预警、事中防范和事后取证等安全能力。

1. 方案总体架构和主要内容

（1）顶层设计架构

本方案参考《信息安全技术网络安全等级保护》、电力 36 号文等相关技术要求，以纵深防御的防护理念为核心，结合火力发电行业工业控制系统网络的业务特点，构建以工业控制网络、设备、数据、控制、应用为目标防护对象的立体安全防护思路。

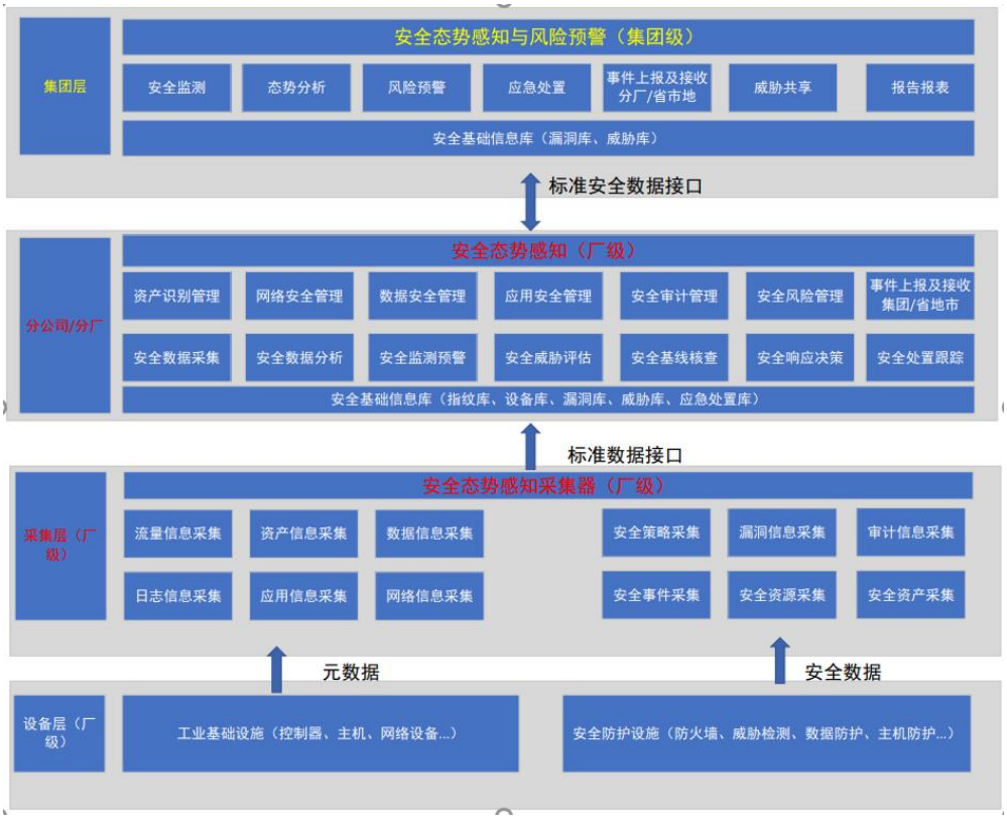

图 11-1　设计思路

安全技术防护和安全管理防护是工业控制系统纵深防御的核心内容，是保障工业控制系统安全运营之两翼，缺少其中一个，都无法确保系统的安全。在安全技术方向，方案遵从 P2DR 模型，主要从威胁防护、监测感知、处置恢复三个维度展开技术防护工作。

在安全管理方向，主要从火力发电厂行业工业控制系统的全生命周期安全风险管理、企业安全建设目标、系统安全建设策略三个方面展开安全管理工作。

2. 网络、平台或安全互联架构

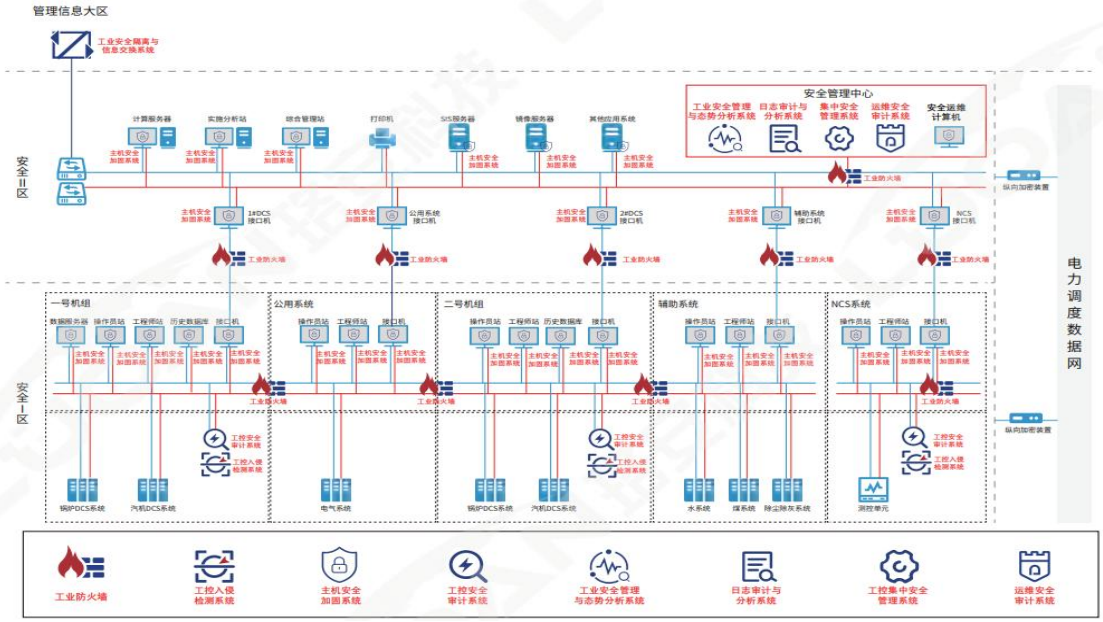

图 11-2　整体防护架构图

方案总体技术架构参考等级保护要求，结合防护指南和 36 号文等相关要求，基于某火电厂生产系统的工业网络安全防护需求，依靠安全现状和需求，建设某火电厂 DCS 系统、SIS 系统工控网络防护体系框架，设计电力企业网络安全综合防护平台基础机构，建设安全态主动防御平台，提升某火电厂统一管理与主动防御能力，构建多层次一体化工业网络安全防御能力，为安全生产提供保障。

拓扑说明：

（1）边界隔离

为保障火电厂生产控制大区安全防护标准已以满足行业防护需求和建设原则，秉承安全分区网络专用原则，生产控制大区内部应 DCS 机组之间应进行有效的边界隔离和防护手段，生产区域内各业务系统边界部署工业防火墙实现业务系统逻辑隔离。

（2）入侵检测

采用旁路方式在厂级监控信息系统（SIS）核心交换机和场站生产系统交换机部署工业入侵检测系统，实现包括入侵检测、协议解析、病毒检测、DNS 监测、DDOS 攻击检测等安全监测能力。

（3）安全审计

在厂级监控信息系统（SIS）及现场设备层各生产域交换机采用旁路方式，部署工控网络安全审计系统，检测生产控制系统中的操作行为和异常网络行为，便于进行事件取证和定责。

（4）主机加固

针对火电厂所有操作系统，采用工业主机安全防护系统进行安全加固和防护，提供主机系统加固、白名单可信防护、恶意代码拦截、系统数据访问控制、外设管控等多种安全能力。

（5）集中管控

根据等保标准“安全管理中心”相关要求，部署集中安全集中管理平台，采集生产网络中各工控安全设备及系统的数据，实现全局化安全管控，加强电力监控系统安全管理水平，和监管能力。

（6）运维管控

为保证电力监控系统生产网络的安全运维，部署运维安全审计系统，通过账号集中管理、细粒度访问权限、操作审计，让运维人员的操作处于可管、可控的状态下，规范运维操作。

（7）日志分析

通过部署日志审计与分析系统对一区、二区的各网络设备、安全设备、操作站、Windows、Linux、的运行状态信息、告警信息进行集中采集、分类、过滤、范式与合并，对网络全局的日志安全事件进行自动联系分析，跟系统默认的或自定义的规则来识别网络威胁和负责的攻击模式，从而确定事件的真实性、进行事件分级并进行有效的响应 。通过对日志内容的深度分析，对采集到的日志数据进行动态分析，将网络非法访问、数据违规操作、系统进程异常、设备故障等高危安全事件，从海量日志数据中提取出来，并通过内置告警规则采用

桌面屏幕、邮件、短信、SYSLOG、SNMP 等方式通知管理员及时处理。

（8）态势感知与威胁预警

通过态势感知与预警平台能够实现针对发电厂生产系统全局风险的感知，比如工控资产分类与统计、资产存在的漏洞等级与数量统计，同时依据国内外最新通报的安全事件和威胁信息，通过内置威胁感知引擎和外部威胁情报的支持，利用现场安全设备的告警日志、网络流量异常状态、主机安全状态分析，针对潜在的风险进行高级动态分析和定位，提供网络安全应急处置策略和建议，同时，为使用方提供威胁预警能力，基于少量的异常行为和特征信息预测当前将要出现的网络攻击和威胁，为决策指挥人员提供技术依据和支撑，便于有针对制定安全防范措施和预案。

3. 具体应用场景和安全应用模式

本套方案可以广泛应用于电力、智能制造、石油石化、天然气、水利、铁路、轨道交通、城市市政以及其他与国计民生紧密相关领域的工业控制系统，提供可定制化和可扩展的安全解决方案。

系统整体可采用分布式架构，支持单级或多级应用部署（厂区级、分公司级、集团级）满足不同层级的用户应用场景。支持全方位工控安全数据采集，主要包括来自于工控主机、工控网络设备、工控网络安全设备、工控数据库软件的威胁事件、操作日志，以及关键位置的工控流量数据采集。

并通过对安全大数据的深度挖掘，借助 AI 智能技术，充分利用资产管理、流量分析、威胁感知、关联分析、风险评估、可视化等技术和功能，实现整体安全防护能力和运营能力的提升。

4. 安全及可靠性

本方案通过以下技术加强系统自身安全可靠：

基于 SSL 的远程管理：通过网络可以直接对工控安全审计系统进行管理和配置。所有通讯采用了 SSL 加密技术，所有数据和所有配置管理信息在网络上全部以密文传输，可以防止恶意攻击者使用网络监听工具窃取信息。

部分关键控制接口，可通过国密 SM3 算法保护数据。

基于角色的分权分级管理，更便于系统权限划分，减少对系统的滥用。

通过可信设备授权，只能通过已经授权的 IP（或者 IP 段）登录。

用户口令尝试次数限制和锁定时间限制，有效防止暴力破解登录密码。

可支持信息安全管理体系的三权分立管理。

5. 其他亮点

集成了工控环境下白名单、黑名单、IP/MAC 地址绑定、异常流量等常用的安全策略，辅以自定义的安全策略，能调用工业防火墙、工控安全审计、主机加固等安全产品实现对工控网络 APT 攻击、异常行为和非法数据包等多种威胁进行多方式保护，对发现的威胁进行告警和阻断，保护工业控制网络安全，有效的提高网络的安全性。

以工控资产及业务为核心，以安全事件管理为关键流程，采用安全域划分的思想，建立一套实时的风险模型，实现对各类资产和业务的信息采集、关联分析、日志审计、事件监控、流量分析、网络攻击防范、态势感知、安全预警和快速响应，做到“集中监控、统一管理、全面分析、快速响应”。

1.1.3 下一步实施计划

1. 计划 1

研制分布式全流量、全空间、全时间的网络安全动态预警装置，

能提高网络安全监控的力度，提升针对火力发电行业工控网络安全的自动化运维程度；

建立基于多维度的通信流量抓取的网络安全分析评估模型，实现对网络状态的全方位掌握。

2. 计划 2

构建火力发电行业网络安全事件快速定位机制，网络安全问题的快速、准确定位。

建立火力发电行业网络安全预测和预警训练模型，实现全网络、全时段的网络安全的动态预警。

1.1.4 方案创新点和实施效果

1. 方案先进性及创新点

原有的网络安全监测主要依靠网络流量进行采集和展示，且流量源有限，协议解析能力有限，对危险的识别也有限，并且各自成体系，无法形成统一的网络安全管理系统，造成网络安全监测“死角”的存在，无法做到事前预测、事中防御、事后追溯的效果。通过扩展安全数据源、增强协议解析能力，同时增加 AI 安全大数据分析和挖掘，训练出更适合当地系统的安全分析、预测、决策模型，并以快速定位、易理解、易管理的展示形式，形成一套完整的火力发电厂企业安全防护和态势感知系统。

2. 实施效果

优化了网络安全管理模式，减轻网络安全运维人员的网络安全现状检查及分析的工作；同时，按照近年各行业事故数量和经济损失统计估算，本成果推广应用预期可对事故发生进行合理规避，减少经济损失。

既做好了安全风险把控，又节省了人力物力，节约了工作成本，

减少经济损失，提升了经济效益。

增强对全局工控系统信息安全的掌控能力，提升网络安全防护管理和运营水平，实现了国家、行业和企业对网络安全的要求。

1.1.5 单位基本信息

北京珞安科技有限责任公司（简称：珞安科技）专注于工业网络空间安全，是国家创新型高科技企业和国家级专精特新“小巨人”企业。

珞安科技成立于 2016 年，秉承“守护工业网络空间安全，为国家关键信息基础设施安全保驾护航”的企业使命，聚集国内工业网络空间安全领域顶尖人才，组建工业网络空间安全研究实验室及工控安全专家团队。在北京、武汉、西安、天津建立四大研发中心，以零信任理念和体系化思想为指导，自主研发了“实战化、易部署、易维护”工控网络安全产品体系，全面覆盖工控安全、业务安全和工业互联网安全，构建了资产可见、威胁可感、安全可视、攻击可溯、主动防御的工业网络空间安全防护体系。目前，拥有公安部第一研究所、中国网络安全审查技术与认证中心和中国电子工业标准化技术协会颁发的安全建设、安全服务和运行维护能力认证证书，具备质量管理体系、信息安全管理体系、信息技术服务管理体系国际化标准认证等 100+ 资质体系认证、100+ 软件著作权、80+ 发明专利。

珞安科技依托强大的技术原厂商实力，积极开展安全服务和安全运营，业务遍布发电、电网、石油石化、轨道交通、智能制造、煤炭、钢铁、化工、市政、水利、烟草、军工、教育等 20 多个工业行业，覆盖 600 多家监管机构和大型工业企业，服务近 2000 家中小企业，创造多个业内大规模安全产品部署成功案例，获得政府主管部门和行业、产业界的高度认可，并揽获多项省部级科技进步奖。

珞安科技总部位于北京，在武汉、西安、上海、杭州、广州、成都、南京、重庆、宁夏、天津等核心城市设有 20+ 家分子公司及办事处，坚持以保障国家关键信息基础设施运行安全为己任，全力打造国内科技创新高地、人才聚集高地，为中国工业的信息化和智能化安全保驾护航。