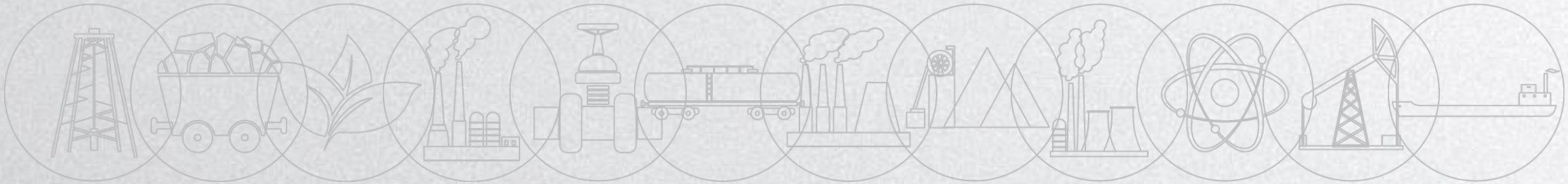
发电厂工控网络安全防护解决方案

北京威努特技术有限公司

公司简介

威努特
WINICSSEC

- 北京威努特技术有限公司是国内专注于工控安全领域的高新技术型企业。以研发工控安全产品为基础，打造多行业解决方案，提供培训、咨询、评估、建设、运维全流程安全服务。
- 首次提出工业网络“白环境”理念，迄今已服务电力、石油、石化、市政、烟草、化工、军工、轨道交通等行业近百家客户，落地项目遥遥领先，市场占有率全国第一。



什么是工业控制系统信息安全

工业控制系统信息安全与通用信息技术（IT）安全有一定的区别，有一定的共性，有时也有一定的交集，取决于工业控制系统的架构。

在IEC62443中对工业信息安全的定义：1. 保护系统所采取的措施；2. 由建立和维护保护系统的措施所得到的系统状态；3. 能够免于对系统资源的非授权访问和非授权或意外的变更、破坏或者损失；4. 基于计算机系统的能力，能够保证非授权人员和系统及无法修改软件及其数据又无法访问系统功能，保证授权人员和系统不被阻止；5. 防止对工业控制系统的非法或有害入侵，或者干扰其正确和计划的操作。

目 录

01

第一部分

发电厂工控安全安全背景

安全趋势　　安全事件　　国家政策、标准

近年来发电厂工控信息安全事件

国内事件Ⅰ

2016年上海某100万机组的电厂，遭受kido病毒攻击，攻击造成SIS接口机数采网络中断

国外事件Ⅰ

2016年贡德雷明根核电站遭受网络攻击，安全专家在这起事件中检测到Conficker和Ramnit恶意软件

国内事件Ⅱ

2015年某电力公司生产的故障录波装置被发现“时间逻辑炸弹”，全国共146套装置存在问题

国外事件Ⅱ

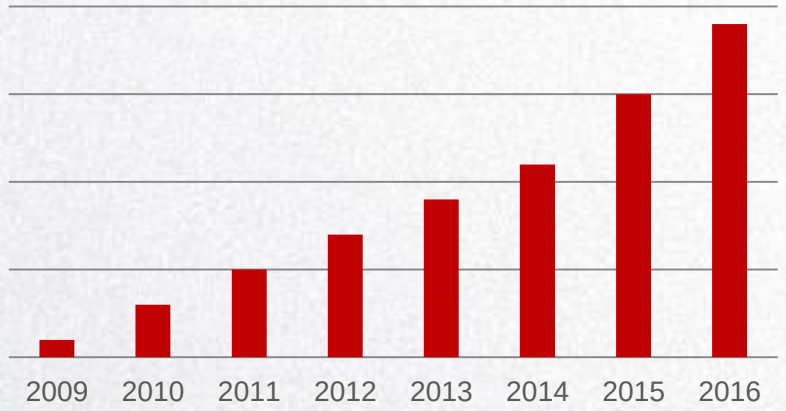
2015年韩国水力与核电公司核电遭受网络攻击，并致使核电工艺图纸，历年发电量，员工信息等数据外泄

国内事件Ⅲ

2003年12月30日，龙泉、政平、鹅城换流站计算机系统发现病毒,经调查确认是技术人员在系统调试中用笔记本电脑上网所致

国外事件Ⅲ

2014年，美国俄亥俄州核电站受到SQL Slammer蠕虫病毒攻击，网络数据传输量剧增，导致系统变慢，控制计算机连续数小时无法工作



- 中国是全球网络攻击**最大**受害国
- 自2009年以来网络攻击增长**15倍**
- 其中30%是针对国家基础设施
- 攻击的重点则集中在电力行业

政策法规

- 2016年7月首次全国范围的关键信息基础设施网络安全检查工作启动，能源行业是检查重点对象之一

中共中央网络安全和信息化领导小组办公室
Office of the Central Leading Group for Cyberspace Affairs

- 2016年11月3日工业和信息化部印发《工业控制系统信息安全防护指南》

中华人民共和国工业和信息化部
Ministry of Industry and Technology of the People's Republic of China

- 2016年11月7日第十二届全国人民代表大会常务委员会第二十四次会议通过《网络安全法》,并于2017年6月开始落地

全国人民代表大会
The National People's Congress of the People's Republic of China

网络安全法 2017年6月落地执行

第三章（第一节）

第二十一条 **国家实行网络安全等级保护制度。**网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务。

第三章（第二节）

第三十一条 国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域…**关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。**

第三章（第二节）

第三十八条 关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和**可能存在的风险每年至少进行一次检测评估。**

第五章

第五十七条 因网络安全事件，发生**突发事件**或者**生产安全事故**的，应当依照《中华人民共和国突发事件应对法》、《中华人民共和国安全生产法》等**有关法律、行政法规的规定处置。**

第六章

第五十九条 **关键信息基础设施的运营者**不履行本法……第三十八条规定的网络安全保护义务的，由有关主管部门责令改正，**给予警告**;拒不改正或者导致危害网络安全等后果的，**处十万元以上一百万元以下罚款**;对直接负责的主管人员处一万元以上十万元以下罚款。

电力监控系统安全防护总体方案（国能安全36号文）

逻辑隔离

控制区与非控制区之间应采用逻辑隔离措施，实现两个区域的逻辑隔离、报文过滤、访问控制等功能，其访问控制规则应当正确有效。**生产控制大区应当选用安全可靠硬件防火墙，**其功能、性能、电磁兼容性必须经过国家相关部门的检测认证。

安全审计

生产控制大区的监控系统应当具备**安全审计系统**，能够及时发现各种违规行为及病毒和黑客的攻击行为。

恶意代码的防范

应当及时更新经测试验证过的特征码，查看查杀记录。禁止生产控制大区与管理信息大区共用一套防恶意代码管理服务器。**（使用”白明单“安全机制替代传统杀毒软件，更满足工控系统安全防护特点）。**

入侵检查

生产控制大区可以统一部署一套网络入侵检测系统，应当合理设置检测规则，及时捕获网络异常行为、分析潜在威胁、进行安全审计。

访问控制

能量管理系统、厂站端生产控制系统、电能量计量系统及电力市场运营系统等业务系统，应当逐步采用电力调度数字证书，对用户登录本地操作系统、访问系统资源等**操作进行身份认证，根据身份与权限进行访问控制，并且对操作行为进行安全审计。**

工控系统等级保护标准正在出台

公安执行检查

边界防护

摘录 7.1.2
a) 应对**控制网络和非控制网络的边界**，以及**控制系统内安全域和安全域之间的边界**，进行监视和控制区域边界通信;
c) 应在控制网络和非控制网络的边界，以及控制系统内安全域和安全域之间的边界上，**阻止任何通过的非必要通信；**

网络和通信安全

摘录 7.1.4.1
e)应采取技术措施对网络行为进行分析，**实现对网络攻击特别是未知的新型网络攻击的检测和分析**；
f)当检测到攻击行为时，**记录攻击源IP、攻击类型、攻击目的、攻击时间**，在发生严重入侵事件时应提供报警；
b) 应在**关键网络节点处对恶意代码进行检测**和清除

设备和计算安全

摘录 7.1.4.2
d)应在所有**入口和出口提供恶意代码防护机制**；
e)应能**管理恶意代码防护机制** ；
b) 审计内容应包括重要用户行为、系统资源的异常使用、重要系统命令的使用等系统重要的安全相关事件；

应用和数据安全

摘录 7.1.4.3
a) 应提供覆盖到**每个用户的安全审计功能**，对应用系统重要安全事件进行审计
b) 应保证无法单独中断审计进程，无法删除、修改或覆盖审计记录；
c) **审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等**；

工业控制系统信息安全防护指南 工信部指导建设

安全软件选择与管理	配置和补丁管理	边界安全防护	物理和环境安全防护	安全监测和应急预案演练
在工业主机上采用经过离线环境中充分验证测试的防病毒软件或**应用程序白名单软件，只允许经过工业企业自身授权和安全评估的软件运行。**	**做好工业控制网络、工业主机和工业控制设备的安全配置**，建立工业控制系统配置清单，定期进行配置审计。	1）通过**工业控制网络边界防护设备对工业控制网络与企业网或互联网之间的边界进行安全防护**，禁止没有防护的工业控制网络与互联网连接。 2）**通过工业防火墙、网闸等防护设备对工业控制网络安全区域之间进行逻辑隔离安全防护。**	拆除或封闭工业主机上不必要的USB、光驱、无线等接口。**若确需使用，通过主机外设安全管理技术手段实施严格访问控制。**	1）在工业控制网络部署**网络安全监测设备，及时发现、报告并处理网络攻击或异常行为。** 2）在重要工业控制设备前端部署**具备工业协议深度包检测功能的防护设备，限制违法操作。**

02

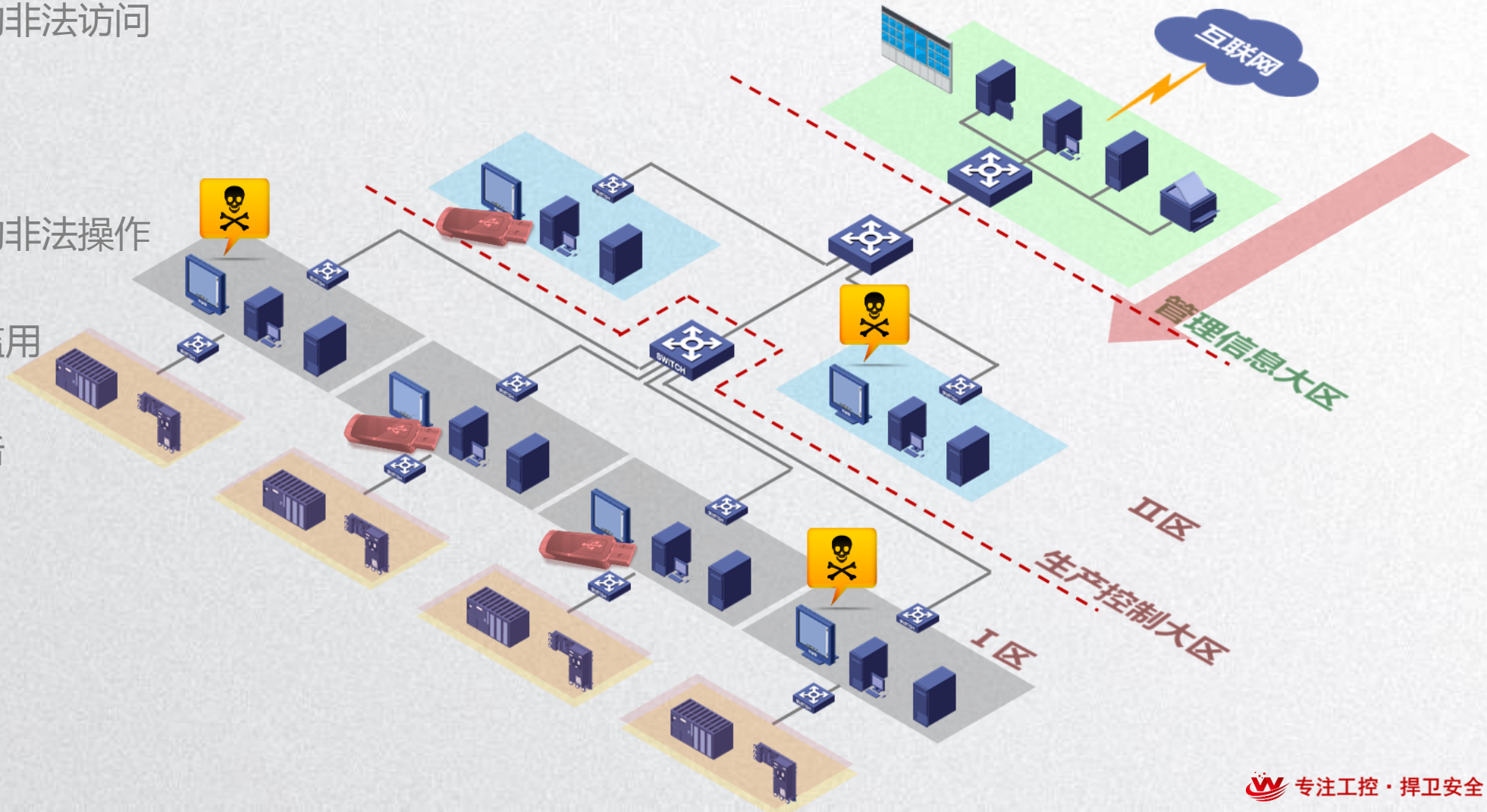
第二部分

发电厂工控安全问题分析

安全威胁分析　　安全问题分析　　常见安全措施

发电厂常见安全威胁

- 从互联网而来的非法访问
- 远程维护通道
- 用户有意无意的非法操作
- 移动存储介质滥用
- 针对漏洞的攻击
- ……



发电厂常见工控安全问题

- **我们的网络运行时间不短了，也没发生什么事情，不需要……，但从现场检查来看**
  - 生产控制区的传统防火墙策略基本为空
  - 现场存在远程维护端口或远程后门（如：TeamViewer软件）
  - 操作员站或工程师站能上互联网
  - 只有28%的主机安装了杀毒软件
  - 90%的杀毒软件未及时升级病毒库
  - 不少的上位机安装了与工作无关的软件（如：游戏、视频等）
  - U盘使用的控制，采用易碎贴封堵的算是情况好的
  - 部分发电厂已经发现如乌克兰电网事件的病毒样本，但用户全然不知
  - 不少电厂采用了已经明确报出漏洞的PLC等设备
  - ……

发电厂工控安全问题（一）

安全问题（一）

- **现场设备**：存在多种接入方式、基础和核心设备严重依赖国外产品和技术。
- **控制系统**：组成部件多、协议复杂，工业协议缺乏加密认证、运行环境存在大量漏洞和隐患并缺乏防护、缺少针对工业控制设备的信息安全检测手段、标准和方法。
- **监控信息系统**：体系架构缺乏基本的安全保障、控制人员缺乏网络安全意识。
- **网络边界**：边界隔离采用传统物理隔离，缺乏相应的访问控制策略，系统直接暴露在互联网上的风险较大。

发电厂工控安全问题（二）

安全问题（二）

- **嵌入式操作系统**：存在系统内核的漏洞、误操作或内部的破坏、数据窃取、数据篡改、假冒攻击、重播攻击、“拒绝服务”攻击和病毒攻击等问题 。
- **HMI站操作系统**：操作系统不易更新、漏洞难打补丁。存在0day漏洞、系统提权漏洞、缓冲区溢出漏洞、UPNP漏洞、RDP漏洞等。
- **实时数据库服务**：黑客通过B/S应用、基于Web窃取工控系统数据库中数据，数据泄露发生在内部，运维人员直接接触敏感数据。
- **杀毒软件**：病毒库需要不定期经常更新，不适合于工业控制环境，且它对新病毒处理滞后。
- **控制器** ：存在硬件和软件代码设计错误，如逻辑错误漏洞、副本安装、未使用的块及隐藏跳转等软件设计错误漏洞。

发电厂工控安全问题（三）

安全问题（三）

- **SCADA系统监控软件，仿真软件，OPC软件，网络管理软件以及在数据服务器、操作员站，工程师站上安装的应用软件：**软件种类多、漏洞多，存在SQL注入漏洞、跨站脚本漏洞、本地提权漏洞、缓冲区溢出漏洞和逻辑错误漏洞等软件安全问题。
- **安全管理策略和管理流程：**存在管理和技术障碍，安全策略和管理流程欠缺、有待完善。
- **通信协议：**协议存在拒绝服务漏洞、栈缓冲区溢出漏洞、缺乏有效认证，无授权等漏洞。
- **网络审计：**系统对网络安全性、可靠性有较大依赖，对实时性要求较高，实时控制网络缺少审计。
- **传输控制：**工控系统的数据和指令传输为明文传输、传统加解密算法复杂、执行时间长。

发电厂工控安全重点需求

- 符合国能安全[2015]36号 发电厂监控系统安全防护方案要求
- 安全措施的引入不能影响工业生产的业务持续性
- 重点解决生产控制大区内部不同区域之间的隔离问题
- 重点解决上位机及服务器主机加固和防病毒问题
- 要有技术手段支撑用户了解工控网络整体安全状态，如日志、告警等
- 针对已经投产并存在漏洞的PLC等设备要采取有效的防护手段

发电厂常见安全措施

常见安全措施

- 生产控制大区和管理信息大区采用单向网闸隔离
- 与第三方接入（如：环保、安全等部门）采用单向隔离装置
- 部分主机安装了杀毒软件，但未及时更新病毒库
- 部分电厂针对生产控制大区采用了传统防火墙进行逻辑隔离，但效果平平
- 安全措施不完善，没有基于等保“一个中心、三重防护”进行建设
- 采用的安全产品不适应工业控制网络
- 安全建设核心思想依然沿用传统IT网络“黑名单”的方式

03

第三部分

发电厂工控安全建设方案

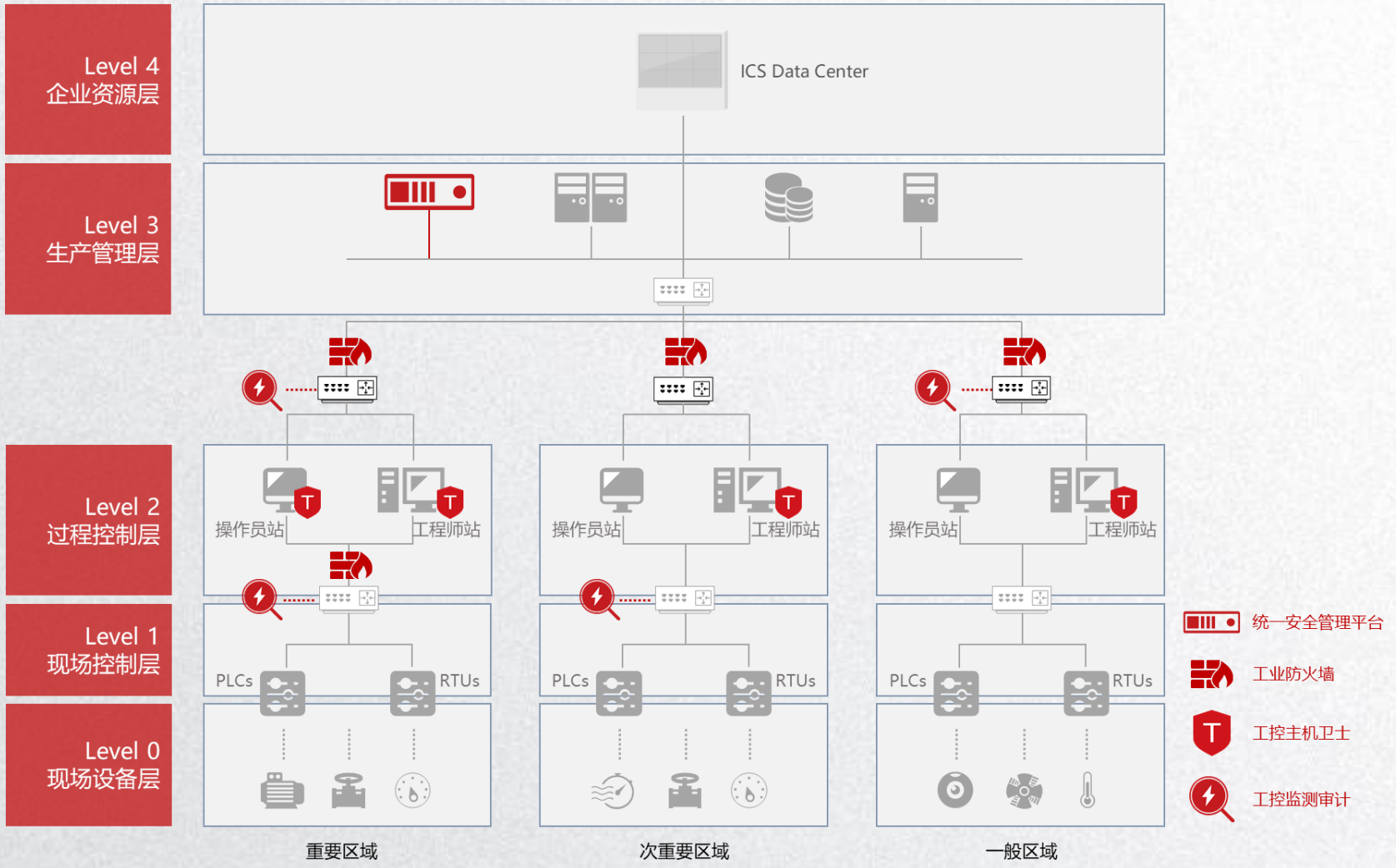
方案理念　核心思想和原则　安全解决方案设计　行业案例说明

威努特工控解决方案模型

国内首家提出工业网络安全“**白环境**”解决方案体系的工控安全厂商，迄今已为上百家关键行业客户建立自主可控、安全可靠的工控安全整体防护体系

核心技术理念：

- 纵深防御
- 白名单机制
- 工业协议深度解析
- 实时监控审计
- 统一平台管理



工业控制系统“白环境”解决方案理念

方案核心安全理念

创新性提出了建立工控系统的**可信任网络白环境**和**工控软件白名单**的理念为客户构筑工控系统“安全白环境”整体防护体系，保护国家基础设施安全。

- 只有可信任的**设备**，才能接入控制网络
- 只有可信任的**消息**，才能在网络上传输
- 只有可信任的**软件**，才允许被执行

技术亮点及创新点

- 从“黑”到“白”
- 从“被动防御”到“主动防护”

解决方案设计依据

电厂工业控制系统安全解决方案设计依据

- **《电力监控系统安全防护总体方案》国能安全[2015]36号文**
- 《电力监控系统安全防护规定》（国家发展和改革委员会令2014年第14号）
- 《工业控制系统信息安全防护指南》
- 《信息安全技术 网络安全等级保护基本要求 第5部分：工业控制系统安全扩展要求》
- 《信息安全技术 网络安全等级保护测评要求 第5部分 工控安全扩展要求》
- 《信息安全技术 网络安全等级保护安全设计技术要求 第5部分：工业控制安全要求》

本方案主要设计依据如上政策标准

国能安全36号文介绍

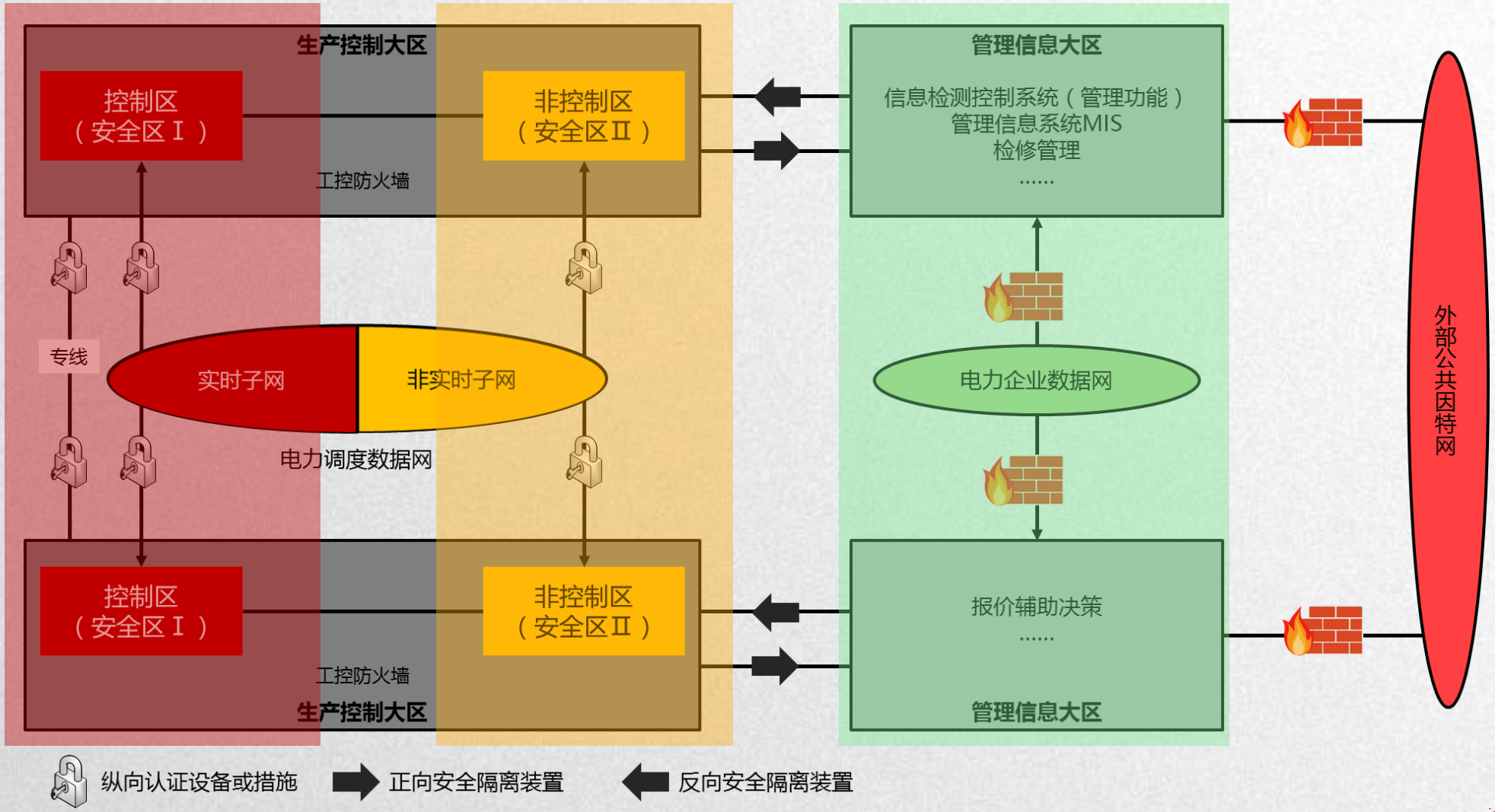
为了加强电力监控系统安全防护工作，根据《电力监控系统安全防护规定》（国家发展和改革委员会2014年第14号），国家能源局制定了《电力监控系统安全防护总体方案》等安全防护方案和评估规范，即国能安全[2015]36号。

国能安全[2015]36号

- **附件1电力监控系统安全防护总体方案**
- 附件2省级以上调度中心监控系统安全防护方案
- 附件3地级调度中心监控系统安全防护方案
- **附件4发电厂监控系统安全防护方案**
- 附件5变电站监控系统安全防护方案
- 附件6配电监控系统安全防护方案
- 附件7电力监控系统安全防护评价规范

附件：
《电力监控系统安全防护总体方案》
《省级以上调度中心监控系统安全防护方案》
《地级调度中心监控系统安全防护方案》
《发电厂监控系统安全防护方案》
《变电站监控系统安全防护方案》
《配电监控系统安全防护方案》
《电力监控系统安全防护评价规范》

安全分区、网络专用、横向隔离、纵向认证



边界安全防护

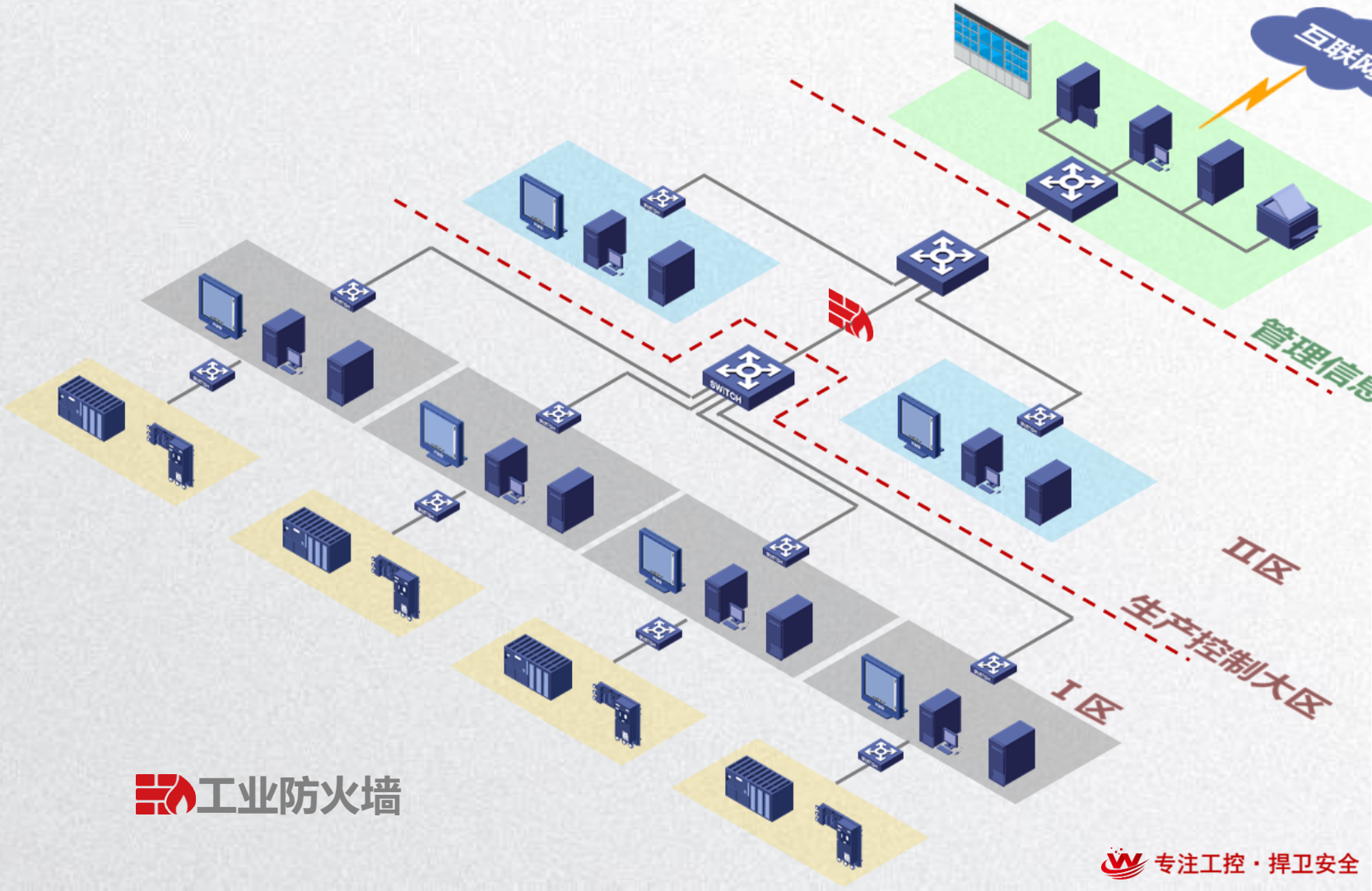
分类		基本要求
国能安全[2015]36号发电厂监控系统安全防护方案 **-4边界安全防护**	4.1横向边界防护	4.1.1 生产控制大区与管理信息大区边界安全防护；
		4.1.2 控制区（安全区I）与非控制区（安全区II）边界安全防护；
		41.3 系统间安全防护 火电厂内同属于控制区的各机组监控系统之间、机组监控系统与控制系统之间、统一机组的不同监控系统之间，同属于非控制区的各系统之间，各不同位置的场站网络之间，采用一定强度的逻辑访问控制措施；
	4.2纵向边界防护	a) 电厂控制大区系统与调度系统通过电力调度数据网进行远程通信时，采用认证、加密访问控制、加密等技术措施实现数据的远方安全传输以及纵向边界的安全防护； b) 参与系统AGC、AVC调节的电厂应当在电力调度数据网的边界配置纵向加密认证装置进行安全防护； c) 对于不具备建立调度数据网的小型火电厂可以通过远程拨号、无线等方式接入相应调度机构的安全接入区
	4.3第三方边界安全防护	a) 火电厂控制大区中的业务系统与环保、安全等政府部门进行数据通信时，其边界应采用与生产控制大区与管理信息大区之间的防护方式进行隔离； b) 信息管理大区与外部网络之间采用防火墙、VPN等保证边界数据传输的安全; c) 禁止外部系统直接与生产控制大区的业务系统或设置采用远程拨号等方式直接访问，而不经过安全隔离

边界隔离（Ⅰ区和Ⅱ区之间）

从Ⅱ区而来的非法访问，可能引起Ⅰ区实时网络的异常

部署对工业协议深度解析的隔离阻断装置实现网络分层分区，边界访问控制，避免无授权设备对区域的访问

部署对工业协议深度解析的隔离阻断装置实现基于通信“白环境”边界攻击防御和过滤



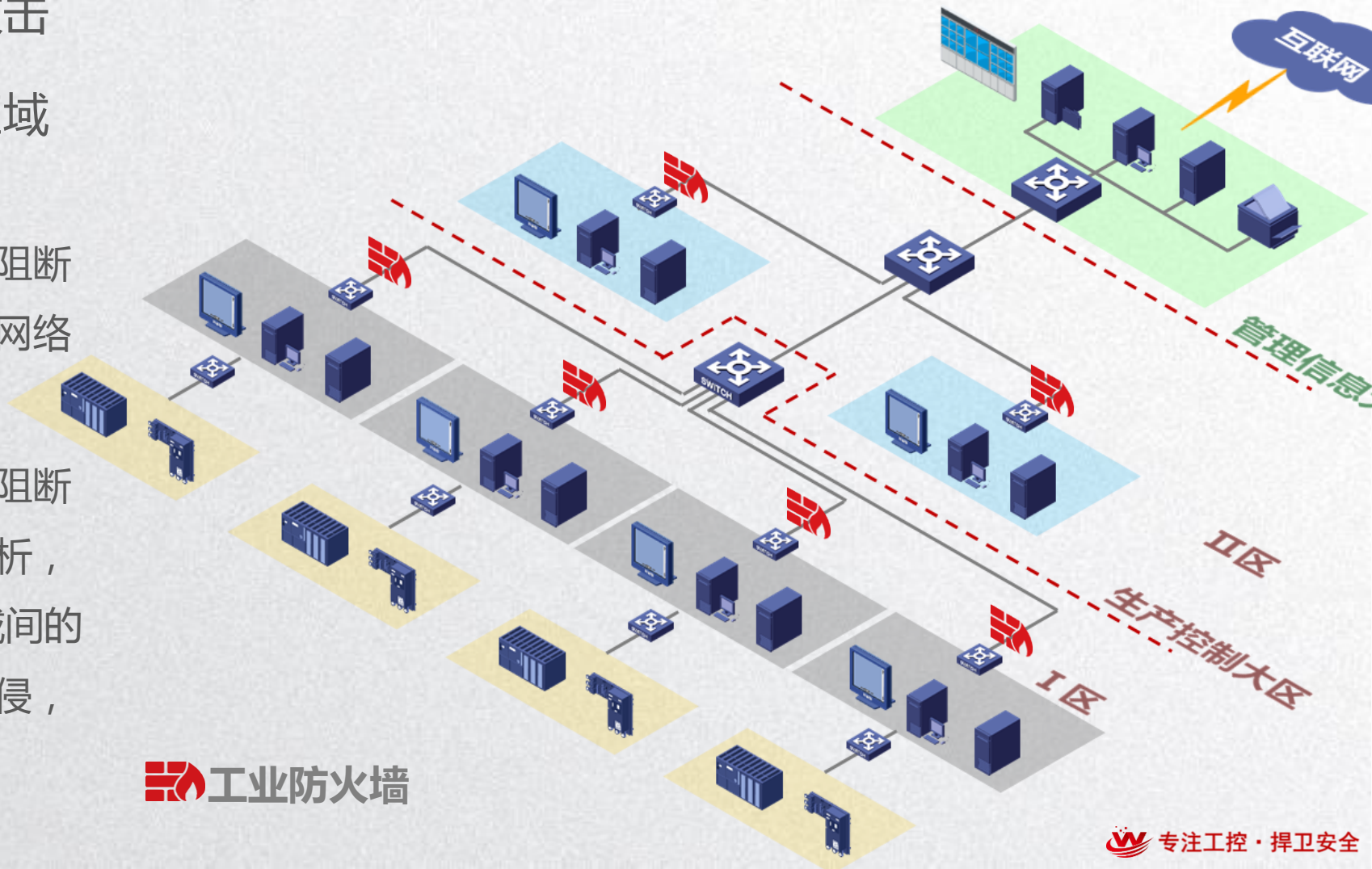
区域隔离（ 生产控制大区内部）

针对某个区域指定的非法攻击

区域内部问题影响至其他区域

部署对工业协议深度解析的隔离阻断装置实现基于区域和功能的区域网络划分及隔离

部署对工业协议深度解析的隔离阻断装置实现对工业专有协议深度解析，建立通讯“白环境“，阻止区域间的越权访问，病毒、蠕虫扩散和入侵，将危险源控制在有限范围内



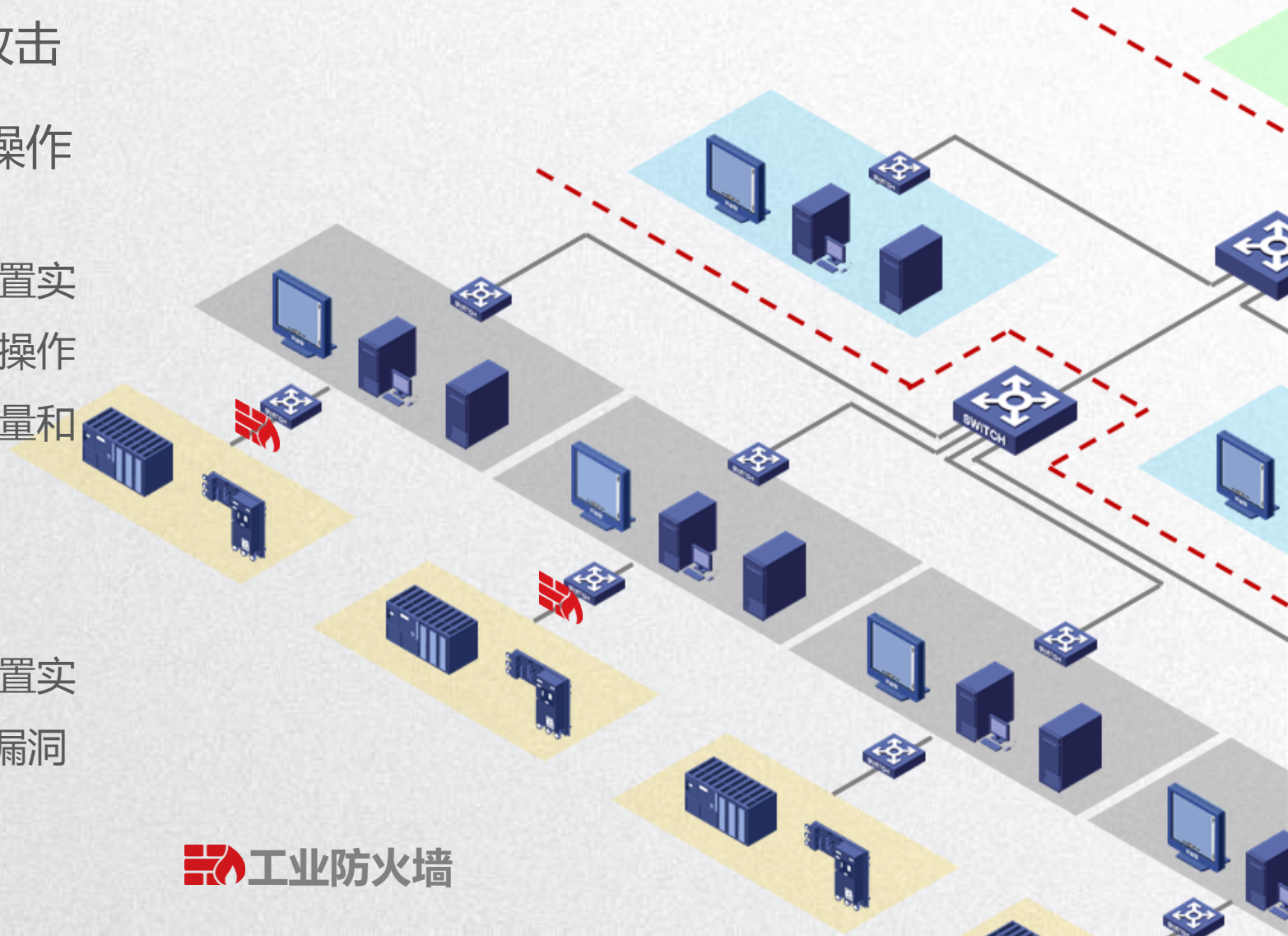
重要系统隔离

从上位机而来，针对重要PLC的攻击

操作员或工程师有意无意的非法操作

部署对工业协议深度解析的隔离阻断装置实现对工业专有协议深度解析，学习正常操作流量，建立通讯“白环境”，对异常流量和非法行为进行告警及阻断，并记录日志

部署对工业协议深度解析的隔离阻断装置实现针对PLC、DCS等工控设备已知安全漏洞利用等行为的阻断

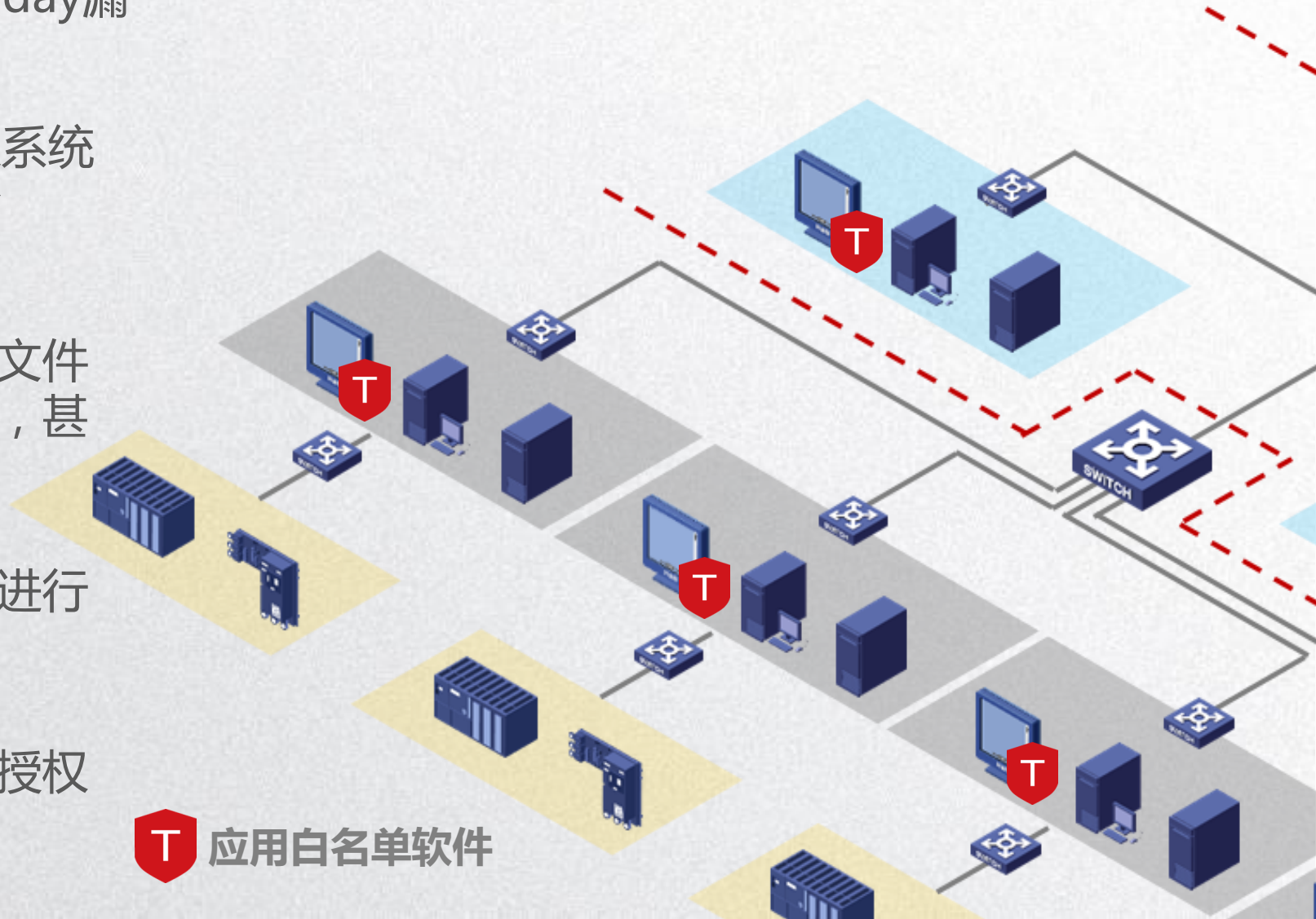


主机与设备安全防护

分类		基本要求
国能安全[2015]36号发电厂监控系统安全防护方案 **-5.2主机与网络设备加固**	主机加固	发电厂厂级信息监控系统等关键应用系统的主服务器，以及网络边界处的通信网关机、web服务器等应当使用安全加固的操作系统。加固方式包括：安全配置、安全补丁、采用专用软件强化操作系统访问控制能力以及配置安全的应用程序，其中配置的更改和补丁的安装应当经过测试。
	网络设备加固	a）非控制区的网络设备与安全设备应当进行身份鉴别、访问权限控制、会话控制等安全配置加固。可以应用电力调度数字证书，在网络设备和安全设备实现支持HTTPS的纵向安全web服务，能够对浏 b）览器客户端访问进行身份认证及加密传输。 生产控制大区中除安全接入区外，应当禁止具有无线通信功能的设备；管理信息大区业务系统使用无线网络传输业务信息时，应当具备接入认证、加密等安全机制。
	外设管控	应当对外部存储器、打印机等外设的使用进行严格管理。

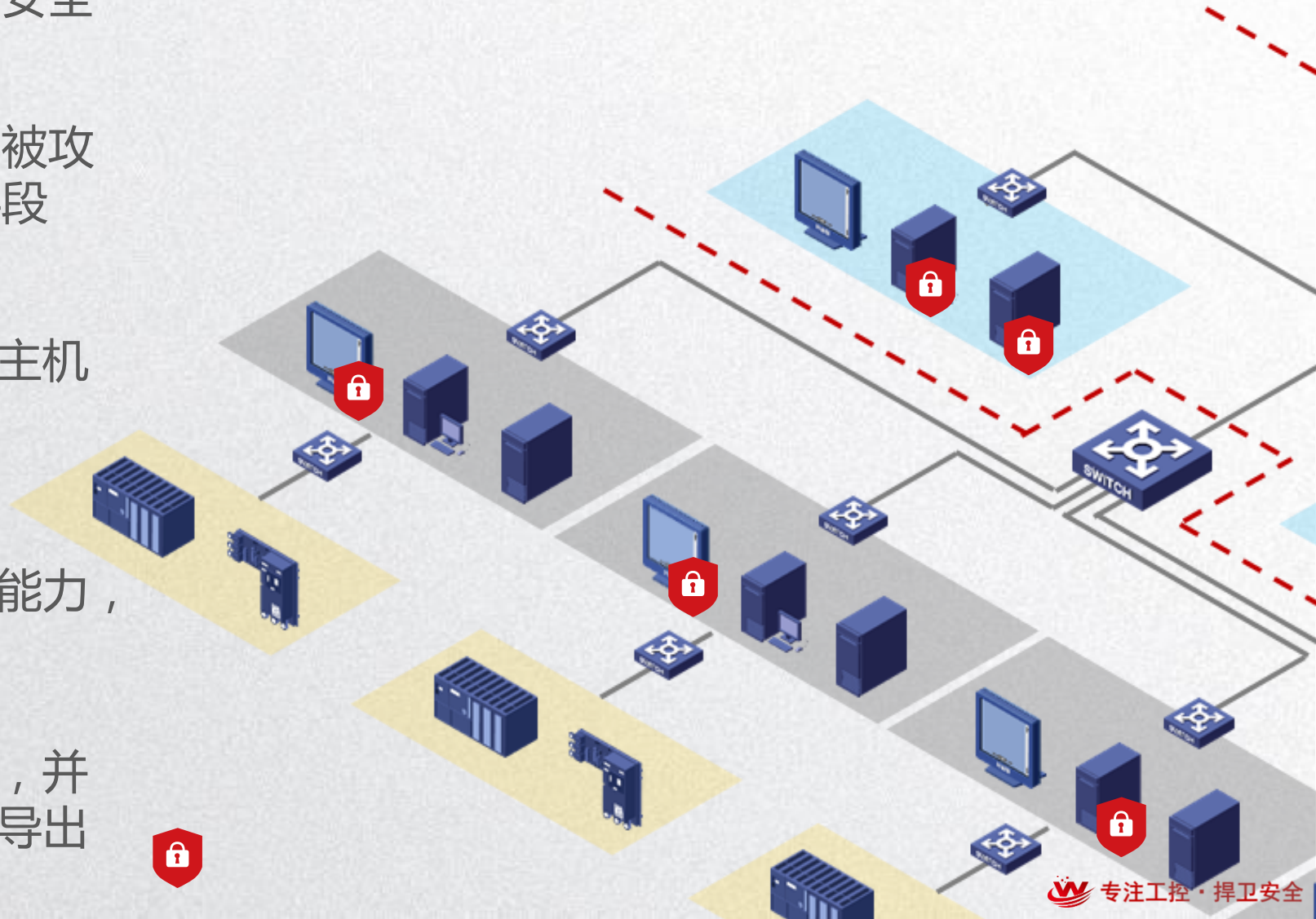
主机安全防护（防病毒）

- 病毒、木马感染上位机，甚至0-day漏洞的利用导致系统不可用
- 上位机系统安全策略缺失，引起系统或用户行为失当，导致安全风险
- 部署应用白名单软件建立可执行文件“白名单”，阻止恶意软件执行，甚至是0-day漏洞的利用
- 通过应用白名单软件对操作系统进行加固，如注册表、配置文件等
- 通过应用白名单软件实现阻止未授权软件的安装



主机加固

- 个人计算机使用水平参差不齐，安全意识存在差异
- 计算机自身安全脆弱，容易成为被攻击的对象，且缺少统一配置的手段
- 通过主机加固类的产品统一工业主机操作系统安全配置
- 提高工业主机操作系统访问控制能力，如提高至强制访问控制
- 对操作事件如登陆、功能停用等，并提供日志的查询、删除、备份和导出



综合安全防护

分类		基本要求
国能安全[2015]36号发电厂监控系统安全防护方案 **-5综合安全防护**	5.1 入侵检测	生产控制大区可以统一部署一套网络入侵检测系统，应当合理设置检测规则，检测发现隐藏于流经网络边界正常信息流中的入侵行为，分析潜在威胁并进行安全审计；
	5.3应用安全控制	发电厂厂级信息监控系统等业务系统应当逐步采用用户数字证书技术，对用户登录失败处理功能，根据身份与权限进行访问控制，并且对操作系统行为进行安全审计。对于发电厂内部远程访问业务系统的情况，应当进行会话控制，并采用会话认证、加密与抗抵赖等安全机制。
	5.4 安全审计	生产控制大区的监控系统应当具备安全审计功能，能够对操作系统、数据库、业务应用的重要操作进行记录、分析，及时发现各种违规行为以及病毒和黑客的攻击行为。对于远程用户登录到本地系统中的操作行为，应该进行严格的安全审计。
	5.5 专用安全产品的管理	安全防护工作中涉及使用横向单向安全隔离装置、纵向加密认证装置、防火墙、入侵检测系统等专用安全产品的，应当按照国家有关要求做好保密工作，禁止关键技术和设备的扩散。
	5.7 恶意代码防范	应当及时更新特征码，查看查杀记录。恶意代码更新文件的安装应当经过测试。禁止生产控制大区与管理信息大区公用一套防恶意代码管理服务器；
	5.8 设备选型与漏洞整改	发电厂电力监控系统在设备选型及配置时，应当禁止选用经国家相关管理部门检测认定并经国家能源局通报存在漏洞的风险的系统及设备；对于应经投入运行的系统及设备，应当按照国家能源局及其派出机构的要求及时进行整改，同时应当加强相关系统与设备的运行管理和安全防护。

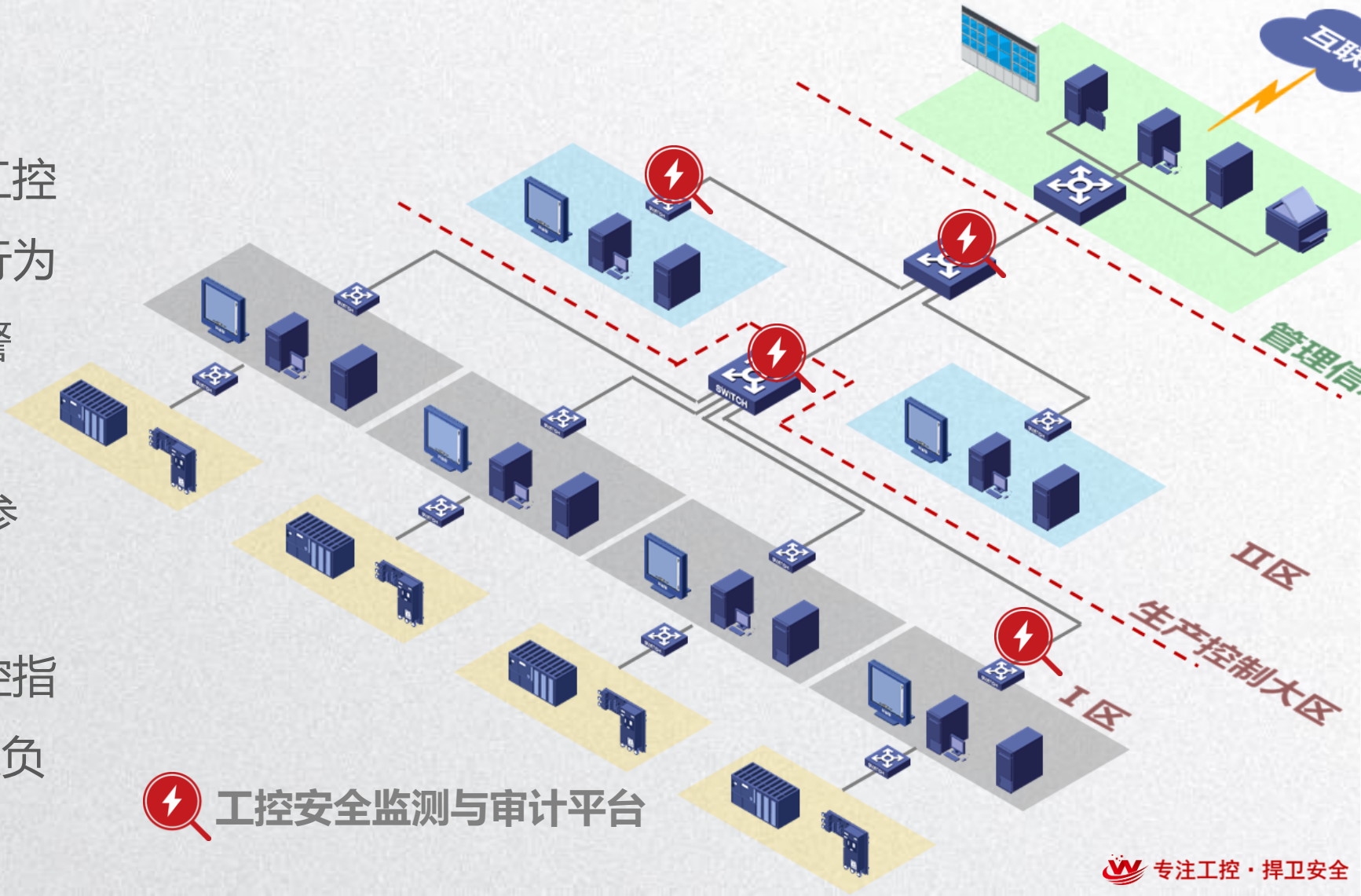
工控网络监测与审计

隐蔽不可知的恶意流量

部署监测与审计系统记录工控协议通信，建立正常通信行为模型，对异常操作进行告警

识别并检测工控协议攻击、TCP/IP攻击、网络风暴、参数阈值检测

对工程师站组态并更、操控指令变更、PLC程序下装以及负载变更等关键事件告警



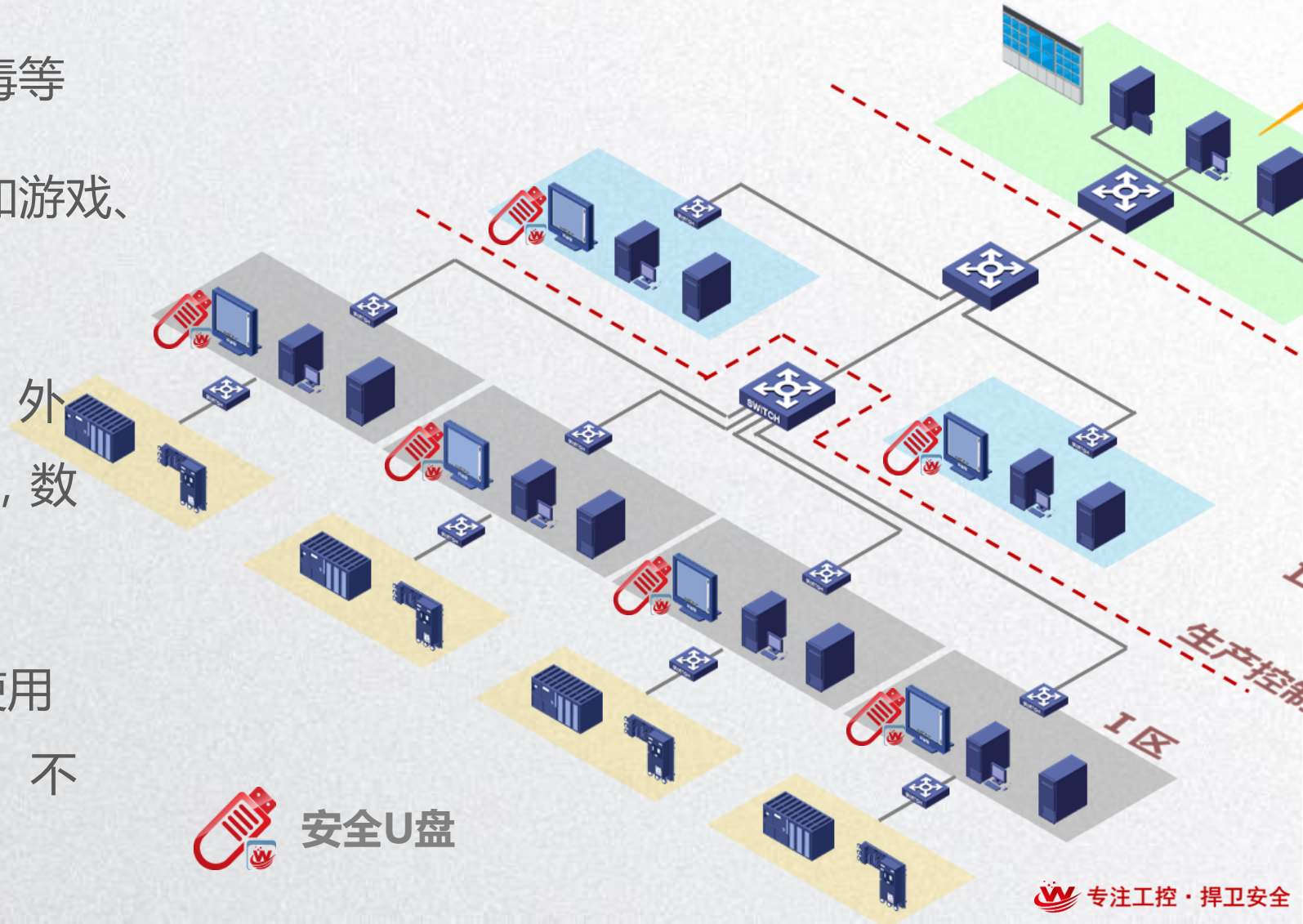
文件安全传递

普通U盘随意插拔，带来未知病毒等

通过U盘带入与工作无关数据，如游戏、视频、程序等，导致系统不可用

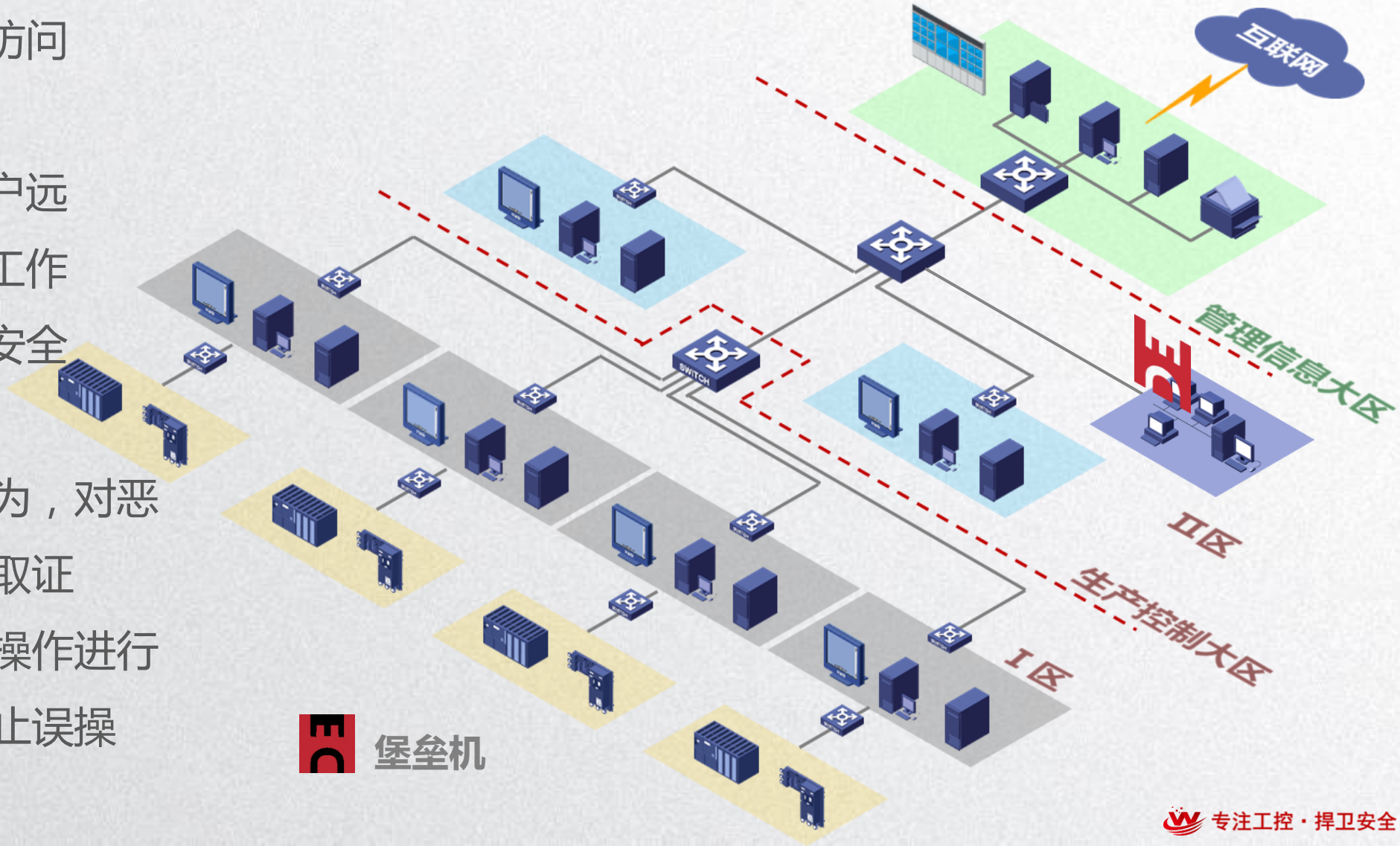
采用安全U盘，仅能在内部使用，外部无法使用，自带硬件安全芯片，数据安全存储

针对普通U盘，控制普通U盘的使用权限，包括禁止使用、只读使用、不控制



应用数据安全之网络设备防护&审计&身份鉴别

- 阻止非授权用户访问网络、安全设备
- 阻止非授权的用户远程维护服务器、工作站、网络设备、安全设备等
- 全程记录维护行为，对恶意维护行为进行取证
- 对远程维护行为操作进行监测、审计，阻止误操作、恶意操作



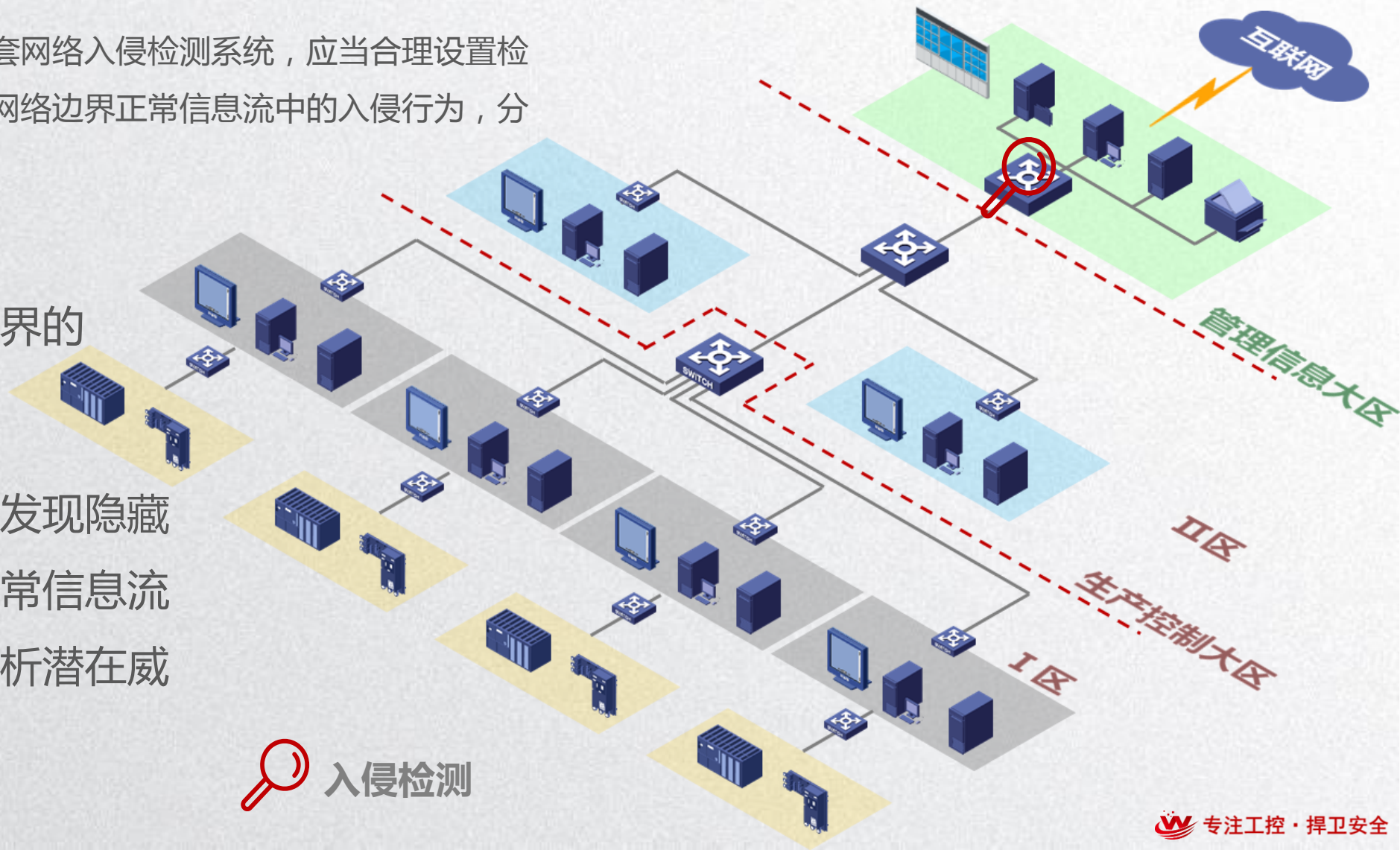
入侵检测

国能安全[2015]36号：

生产控制大区**可以**统一部署一套网络入侵检测系统，应当合理设置检测规则，检测发现隐藏于流经网络边界正常信息流中的入侵行为，分析潜在威胁并进行安全审计

隐藏于流经网络边界的入侵行为

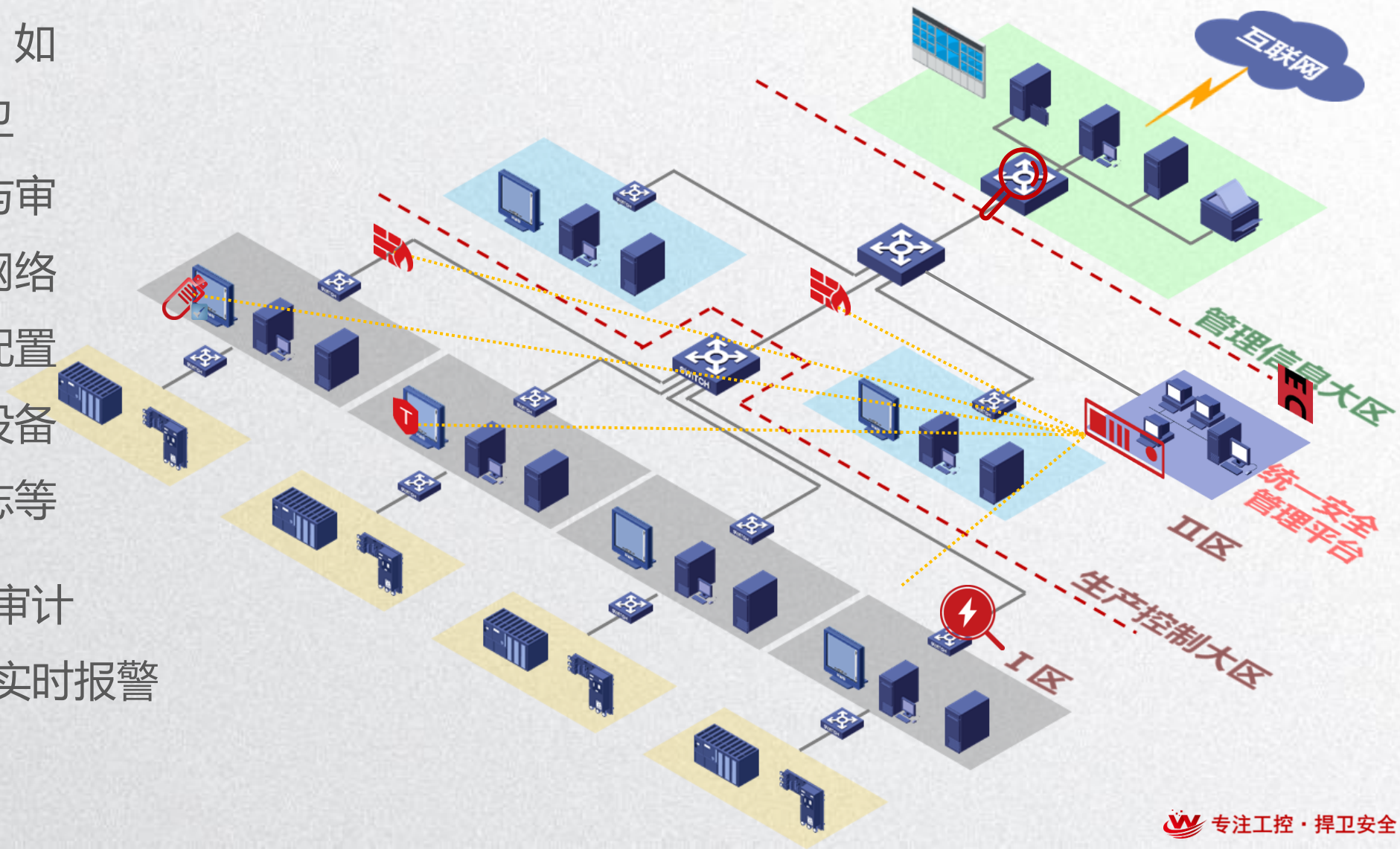
部署入侵检测检测发现隐藏于流经网络边界正常信息流中的入侵行为，分析潜在威胁并进行安全审计

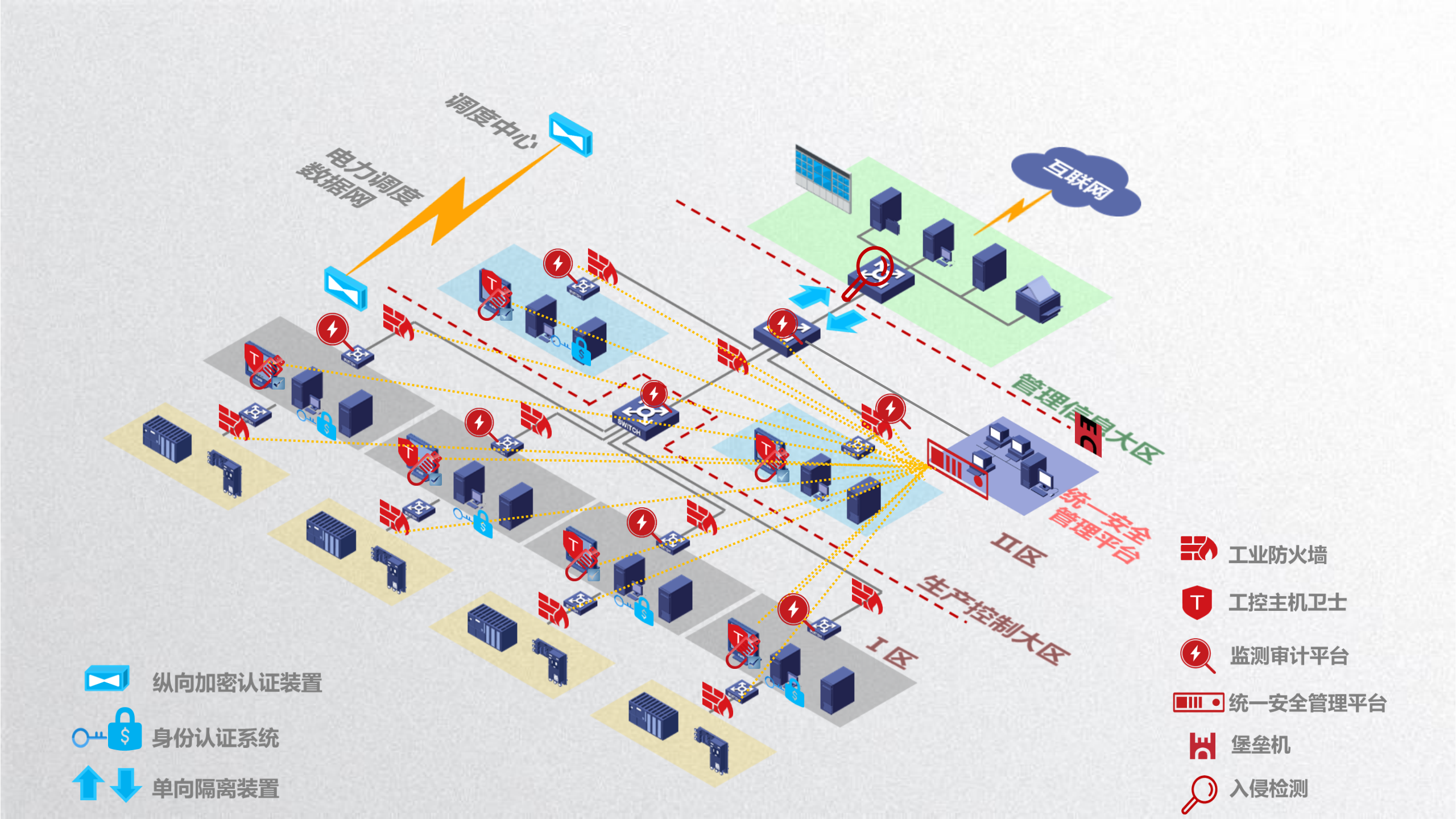


统一安全管理

集中管理安全设备：如工业防火墙、可信卫士、工控安全检测与审计系统，实现工控网络的拓扑管理、安全配置及安全策略管理、设备状态监控、告警日志等

- 集中的安全日志审计
- 工作站终端异常实时报警
- 分级分权限管理




调度中心
电力调度数据网
互联网
管理信息大区
统一安全管理平台
Ⅱ区
生产控制大区
Ⅰ区
纵向加密认证装置
身份认证系统
单向隔离装置
工业防火墙
工控主机卫士
监测审计平台
统一安全管理平台
堡垒机
入侵检测

上海某火电厂

客户需求

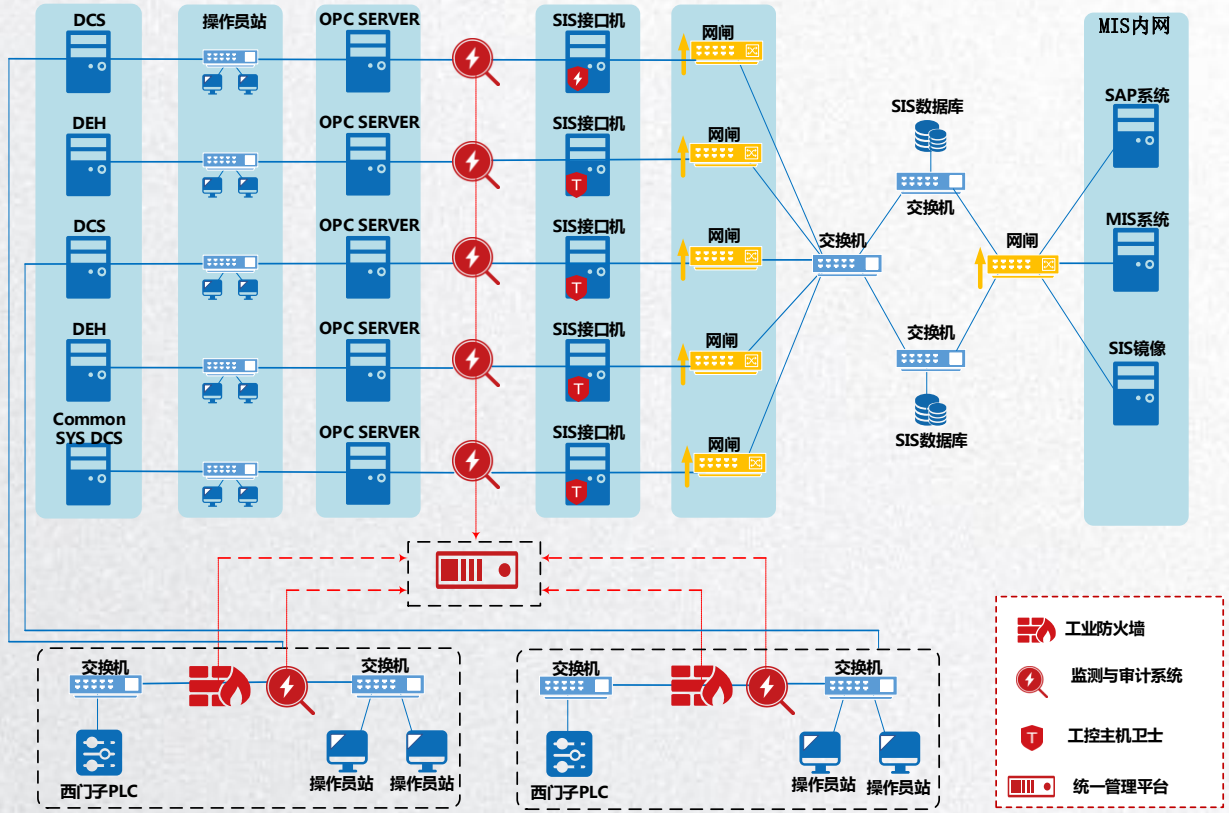
- 对生产控制系统中的DCS系统和PLC设备采取严格访问控制；
- 各生产区之间、生产区内各区域之间需要采取安全隔离和入侵防范措施；
- 工程师站、操作员站没有有效的防病毒手段，阻止恶意代码传播。

解决方案

- 在各区域出口和入口交换机上部署监测审计平台，实时发现针对PLC、DCS等重要工业控制系统的攻击和破坏行为，为工业控制网络安全事件溯源提供依据；
- 在各场站PLC/DCS等工控设备的网络出口位置部署工业防火墙，对外来访问进行严格控制；
- 在工控主机及应用服务器上部署工控主机卫士，阻止各种已知和未知恶意代码的运行，增强主机防范恶意代码的能力；
- 部署统一安全管理平台对工业控制系统安全防护产品进行统一维护、统一管理、统一展示，增强网络安全性的同时减轻运维管理压力。

客户价值

- 对现有网络架构进行整改，避免网络出现单点故障，提升了网络可用性；
- 实现了生产网络的纵深防御，保障了监控业务网络的连续性；
- 帮助客户定位自身安全问题，有力支撑了电厂工控系统安全



某水力发电总厂

客户需求

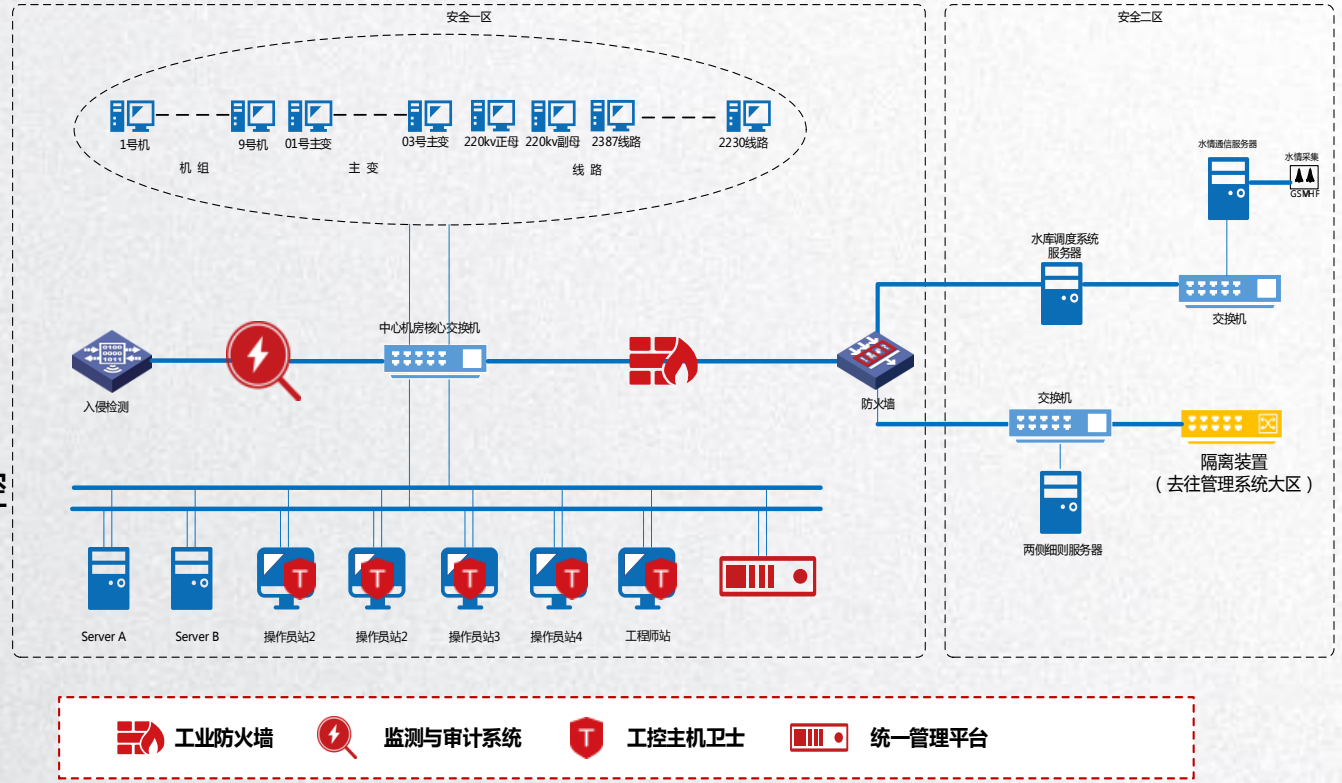
- 需对工控网络中病毒、恶意代码、蠕虫、木马等攻击行为进行防御；
- 对工程师站、操作员站及服务器进行安全加固和病毒防范；
- 安全I区与安全II区需要采取安全监测与审计措施；
- 安全I区与安全II区间需采取横向逻辑隔离的安全措施。

解决方案

- 在操作员站、工程师站等重要工控主机上部署工控主机卫士，通过“白名单” 防护机制,有效防止操作员站、工程师站被非法入侵；
- 在网络边界部署工业防火墙，阻止任何来自边界区域外的非授权访问，抑制病毒、木马在工控网络中的传播和扩散；
- 部署监测审计平台，实时发现针对SCADA、DCS等重要工业控制系统的攻击和破坏行为以及病毒、木马等恶意程序的扩散和传播行为；
- 部署统一安全管理平台对安全设备进行统一安全管理。

客户价值

- 满足电力行业等保三级安全防护标准要求；
- 实现水电站总体安全现状分析，帮助客户了解自身安全状况；
- 全面提高生产控制网络的整体安全性，为安全生产保驾护航；
- 可通过技术手段弥补人工管理方式上的缺陷，提高企业工控网络安全管理效率。



04

第四部分
安全解决方案合规性分析

合规性（36号文 附件4）

安全要求	安全子项	安全要求	是否符合	涉及产品
安全区域划分	控制区 （安全区Ⅰ）	与控制相关的DCS、AGC、AVC、SIS等系统放置在控制区（安全区Ⅰ）	--	Null
	非控制区 （安全区Ⅱ）	非控制系统，与发电相关的调度、电能采集、录波等	--	Null
	管理信息大区	SIS的管理功能、报价辅助决策、ERP等	--	Null
边界安全防护	横向边界防护	生产控制大区与管理信息大区边界安全防护	符合。通过部署电力专用正、反向隔离实现Ⅱ区、Ⅲ区的安全隔离，确保只有合规合法的业务数据可以交互	正向隔离装置 反向隔离装置
		控制区与非控制区边界安全防护	符合。通过逻辑隔离措施实现Ⅰ、Ⅱ区的横向边界防护，根据业务的需要选用合适的安全产品和措施。	工业防火墙 网闸 VLAN
		系统间安全防护	符合。通过逻辑隔离措施实现不同系统间的边界防护，根据业务的需要选用合适的安全产品和措施。	工业防火墙 VLAN
	纵向边界防护	发电厂与调度端的边界防护	符合。发电厂生产控制大区与调度数据网的连接处使用国家制定部门检测认证的电力加密装置进行防护，实现双向身份认真数据加密和访问控制。	纵向加密装置
	第三方边界安全防护	生产控制大区与环保、安全等政府部门进行数据传输……	符合。应采取生产大区与管理信息大区同样的防护措施。	正向隔离装置

合规性（36号文 附件4）

安全要求	安全子项	安全要求	是否符合	涉及产品
综合安全防护	入侵监测	生产控制大区可以部署一套网络入侵检测系统……	符合。检测发现隐藏于流经网络边界正常信息流中的入侵行为，分析潜在威胁并进行安全审计；	入侵检测
	主机加固	……应当使用安全加固的操作系统。加固方式包括：安全配置、安全补丁、采用专业的软件强化操作系统访问控制功能。	符合。安全配置、安全补丁、采用专业的软件强化操作系统访问控制功能。	配置核查软件
	应用安全控制	……应当逐步采用数据证书技术，对用户登录应用系统、访问系统资源等操作进行身份认证，提供登录失败处理功能……	符合。发电厂厂级信息监控系统等业务系统应当逐步采用用户数字证书技术，对用户登录失败处理功能，根据身份与权限进行访问控制，并且对操作系统行为进行安全审计。	身份认证系统
	安全审计	生产控制大区的监控系统应当具备安全审计功能，能够对数据库、操作系统、业务应用的重要操作进行记录。对于远程用户登录到本地系统中的操作行为，应该进行严格的安全审计。	符合。生产控制大区的监控系统应当具备安全审计功能，能够对数据库、操作系统、业务应用的重要操作进行记录。	堡垒机
			符合。对于远程用户登录到本地系统中的操作行为，应该进行严格的安全审计。	工控安全监测与审计
	专用安全产品的管理	……涉及的安全产品应当按照国家有关要求做好保密工作，禁止关键技术和设备的扩散	安全防护工作中涉及使用横向单向安全隔离装置、纵向加密认证装置、防火墙等专用安全产品的管理。	Null
	备份容灾	管理信息大区做备份，生产控制大区做冗余	定期对关键业务数据备份，数据异地保存。	Null
	恶意代码防范	要有恶意代码防范机制	符合。在工作站阻止恶意代码层序执行，漏洞利用。	工控主机卫士
	设备选型及漏洞整改	禁止选用国家已认定有漏洞的产品，如已投产及时整改	符合。发电厂电力监控系统在设备选型及配置时，应当禁止选用通报存在漏洞的风险的系统及设备。	漏洞扫描 工控漏洞挖掘

05

第五部分

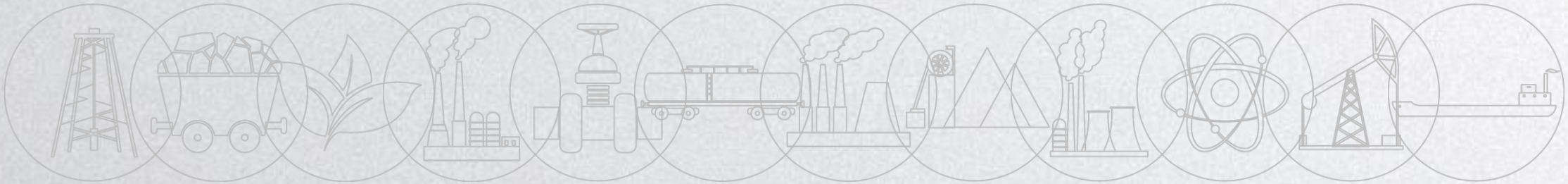
威努特公司与产品服务介绍

公司简介　安全事记　一点成绩　产品与案例

公司简介

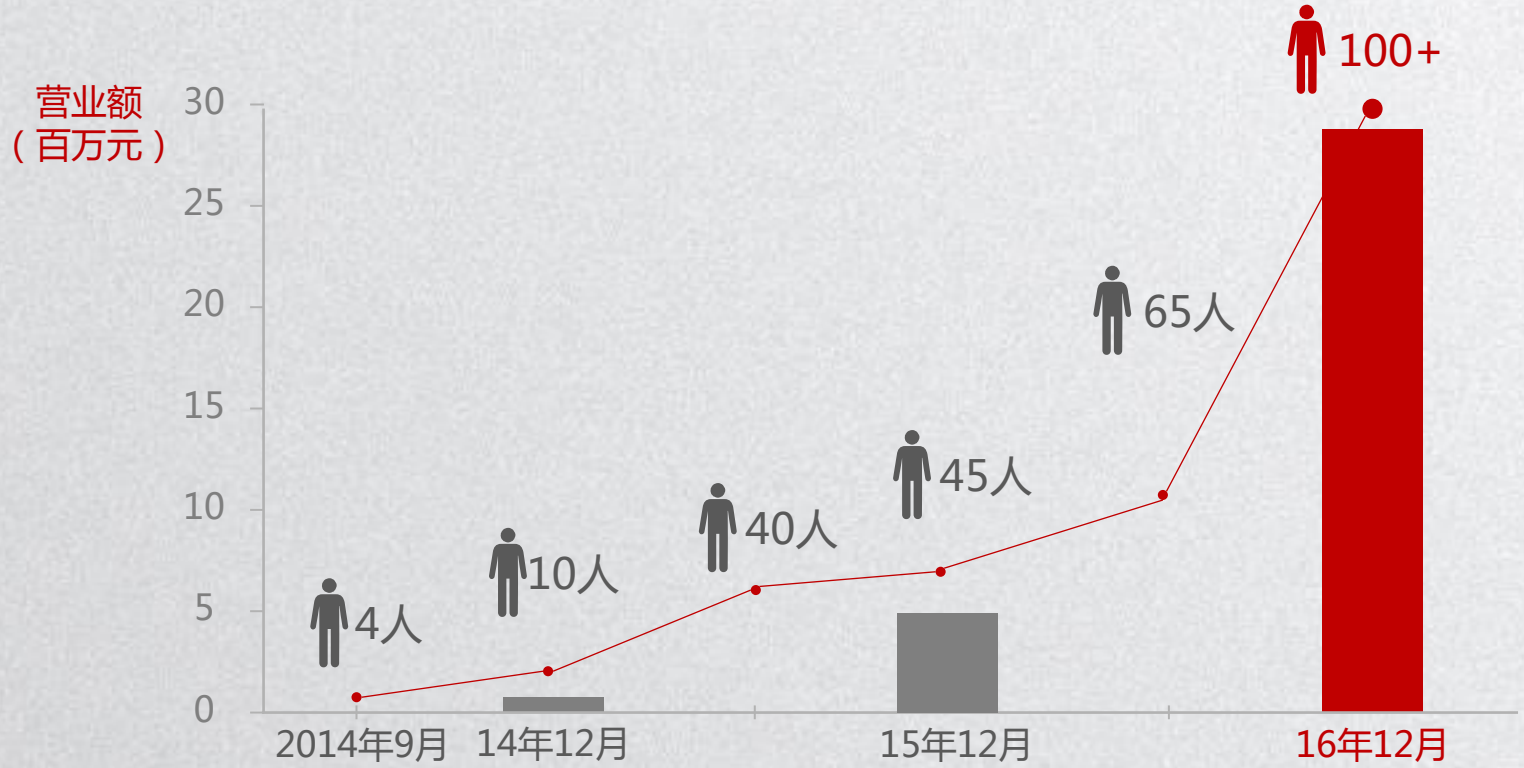
威努特
WINICSSEC

- 北京威努特技术有限公司是国内专注于工控安全领域的高新技术型企业。以研发工控安全产品为基础，打造多行业安全解决方案，提供培训、咨询、评估、建设、运维全流程安全服务。
- 国内首家提出工业网络“白环境”理念，迄今已服务电力、石油、石化、市政、烟草、化工、军工、轨道交通等行业近百家客户，落地项目遥遥领先，市场占有率全国第一。



人员组成

- 公司规模100余人，60%以上是信息安全和自动化领域的技术人才，平均从业年龄超过10年，组建了近50人的研发团队，获得近20项国家发明专利，工控安全项目落地数量全国遥遥领先。



1/2为研发人员

超过60%信息安全和自动化专家

分支机构

- 总部设于北京；沈阳、河南、山东、上海、广州、内蒙设有分支机构，在全国主要城市有紧密合作伙伴。威努特产品和服务已经是工控安全市场上最令人信服的品牌

总部　分支机构

威努特工控安全大事记

2015年

- 推出国内首款千兆工业防火墙
- 推出国内首款适用于工业现场的主机卫士
- 推出国内首款工控漏洞挖掘设备
- 推出工控安全监测与审计平台

2014年

- 北京威努特技术有限公司正式注册成立
- 工信部授权设立全国信息技术人才培养工程培训基地

2016年

- 发布工业网络空间安全态势感知系统
- 公安部授予工控安全技术支持单位
- 受聘保障G20杭州峰会网络安全
- 成为国家信息安全漏洞库支撑单位
- 成为国家高新技术企业
- 多行业落地项目50+ ，产品通过考验

保障关键信息基础设施的运行安全

2017年

- 成功举办威努特工控安全沙龙
- 成为信息安全等级保护安全建设服务机构
- 亮相北京国际网络安全周，得到领导高度评价

资质荣誉

ISO9001/14001/27001

国家网络与信息安全
信息通报机制技术支持单位

国家信息安全漏洞库支撑单位

2016杭州
G20峰会网络安保单位

国家工控安全实验室理事单位

国家高新技术企业

信息安全等级保护安全
建设服务机构能力评估

牵头&配合制定
多项国家及地方标准

“一带一路”
高峰论坛安保单位

全国工业和信息化人
才培养工程培训基地

技术积累

- 软件著作权30余款
- 发明专利近20项
- 工控漏洞业内含金量最高

积极参与工控安全标准制定工作

国家标准

- 信息安全技术 信息系统安全等级保护基本要求 第5部分 工业控制安全扩展要求
- 信息安全技术 信息系统安全等级保护测评要求 第5部分 工业控制安全扩展测评要求
- **信息安全技术 工业主机应用程序白名单软件安全技术要求和测试评价方法**
- 信息安全技术 电力监控系统安全等级保护实施指南
- 信息安全技术 工业控制系统专用防火墙技术要求
- 信息安全技术 工业控制系统网络审计产品安全技术要求
- 信息安全技术 工业控制网络安全隔离与信息交换系统安全技术要求
- 信息安全技术 工业控制网络监测安全技术要求及测试评价方法
- 信息安全技术 工业控制系统漏洞检测技术要求及测试评价方法

地方标准

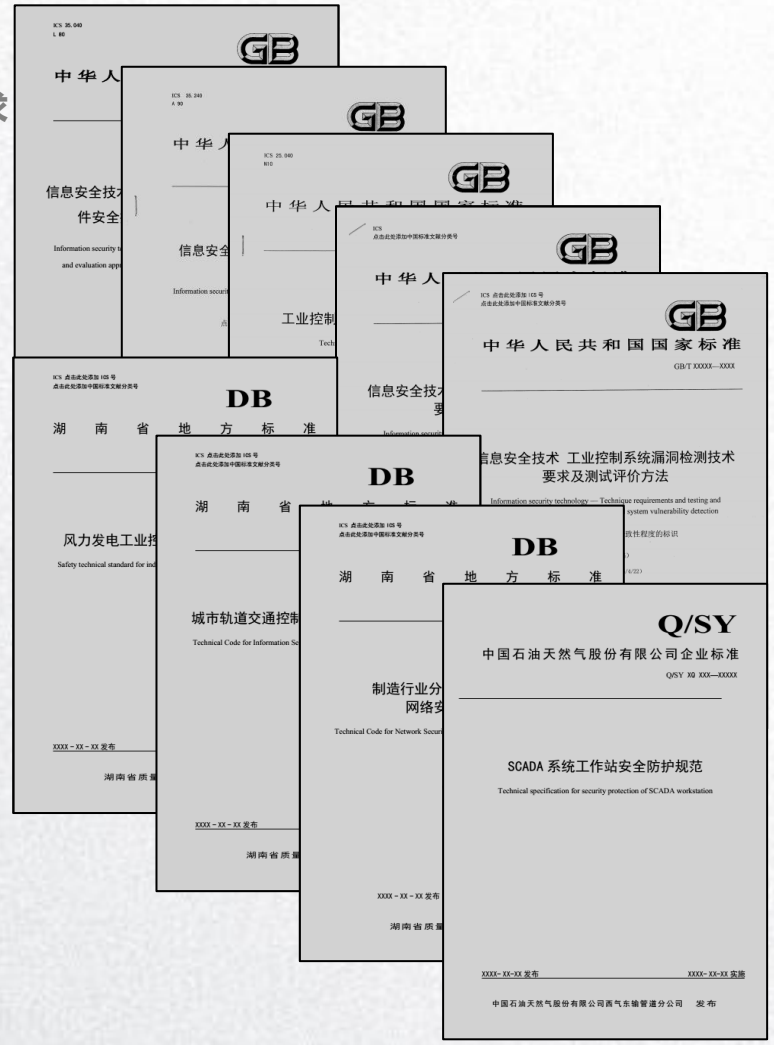
- **湖南省地方标准 《城市轨道交通控制系统信息安全技术规范信息安全技术》**
- **湖南省地方标准 《风力发电工业控制系统安全技术标准》**
- **湖南省地方标准 《制造行业分布式控制系统DNC网络安全技术规范》**

企业标准

- **中国石油天然气股份有限公司企业标准 SCADA系统工作站安全防护规范**

监管要求

- 工信部 《工业控制系统信息安全防护指南》
- **工信部 《工业控制系统信息安全防护指南》解读**
- **工信部 《工业控制系统信息安全防护指南》培训教材**



承担多项国家及行业工控安全课题

国家课题

- 2016年工业转型升级（中国制造2025）
- 工信部DCS仿真安全测试平台项目
- 工信部工业互联网安全漏洞监测系统建设项目
- 国家科技部漏洞挖掘课题项目
- 发改委丹江口水利枢纽网络安全专项项目建议书

行业研究

- 国网电科院 智能电网工控安全攻防技术研究及验证等信息化
- 国网电科院 智能电网工控安全攻防技术研究及验证仿真环境建设攻防工具
- 南网电科院 用电防护侧工控安全研究
- 广东电科院 嵌入式设备漏洞测试挖掘方法及成套检测综合平台开发

产品全家福

平台类

工控统一安全管理平台

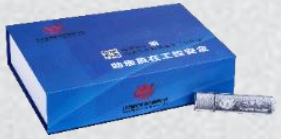
工控综合检测系统

防御类

单向隔离网关

工业防火墙

运维管理系统（堡垒机）



工业主机安全
安全U盘

检测类

工业网络监测审计

评估类

工控漏洞挖掘平台

工控漏洞扫描平台

等保工具箱

产品全家福

科研类

行业仿真攻防平台

漏洞挖掘平台

工业网络态势感知

工业防火墙

产品定位

- 保护控制网与管理信息网的边界
- 阻止来自管理信息网的威胁
- 防止安全域内的攻击扩散

产品特点

- 国内第一款千兆工业防火墙
- 十数种工业协议深度解析
- 低延迟 < 60us

1. 状态检测防火墙
2. 白名单智能学习
3. 工控协议(如OPC)的只读控制
4. 工控协议(如OPC)深度白名单
5. 仅放开OPC动态端口
6. MODBUS TCP值域控制
7. 违规报警及报告(支持短信)
8. 统一平台管理

监测审计平台

- **产品定位**
  - 监控并记录工控系统运行过程中的一切操作行为
  - 为事故追溯、责任划分提供证据
- **产品特点**
  - 对工控网络**“零影响”**
  - 忠实记录网络一切动态
  - “白名单”思想，无需升级

1 **网络异常检测**
忠实记录工控协议通信记录，自学习建立正常通信行为基线模型，对偏离基线异常操作行为进行告警上报；

2 **网络攻击检测**
识别并检测工控协议攻击、TCP/IP攻击、网络风暴、参数阈值检测

3 **关键事件检测**
例对工程师站组态并更、操控指令变更、PLC程序下装以及负载变更等关键事件告警

4 **工业网络可视化**
提供多维度网络流量视图，统计视图

工控主机卫士

1. 应用白名单
2. 实时报警
3. 智能学习
4. 自身保护
5. 安全U盘
6. 观察模式
7. 日志审计

国内首家利用“白名单”技术保护工控系统主机安全的防护软件。保证只有经过认证的“白名单”软件才可以运行，其他病毒、木马、违规软件都被阻止。

统一安全管理平台

- 对工控网络安全设备统一管理；
- 集中收集工控网络安全设备日志，统一关联分析
- 可视化展示网络中安全动态；
- 平台管理员支持三权分立，分权分级；
- 可对接其他厂商安全产品，实现工控“SOC”。

堡垒机（运维管理系统）

- 账户集中管控，清晰了解运维现状；
- 运维权限细粒度划分，自然人与系统账户一一对应；
- 运维操作过程全程审计，实时监控查询；
- 运维操作过程回放；
- 降低运维误操作和恶意操作带来的风险；
- 缩短故障处理时间，提高业务连续性；
- 安全审计、安全评估。

工控漏洞扫描系统

- 支持对西门子、施耐德、GE、亚控等主流工控厂商的SCADA/HMI软件的漏洞扫描；
- 支持对西门子、施耐德、GE等主流工控厂商的DCS系统、PLC控制器的漏洞扫描；
- 支持Modbus、Profibus等主流现场总线的漏洞扫描；
- 支持Autodesk、Dassault等主流数字化设计制造软件平台的漏洞扫描；
- 支持工业控制系统漏洞生命周期管理、评估漏洞安全风险、漏洞验证、提供漏洞修复建议等。

工控漏洞挖掘平台

- 针对工业控制系统中各类设备进行通讯健壮性专业评测；
- 建立我国工控安全防护标准的理论支撑和测试工具；
- 完全自主知识产权，杜绝国外产品后门隐患；
- 提供了发现工业控制系统和设备零日漏洞的工具；
- 提供了设备漏洞根源分析和定位解决的工具；
- 能够有效丰富我国自有工业控制系统漏洞库；
- 增强产品出厂时的健壮性和安全性；
- 提高评测认证通过能力，提升生产效率；
- 减少漏洞修补费用，降低产品召回风险。

工控安全攻防演练平台

工控安全服务

工控安全检查

- 工控漏洞检测
- 工控安全审计
- 工控系统配置检查

工控安全评估

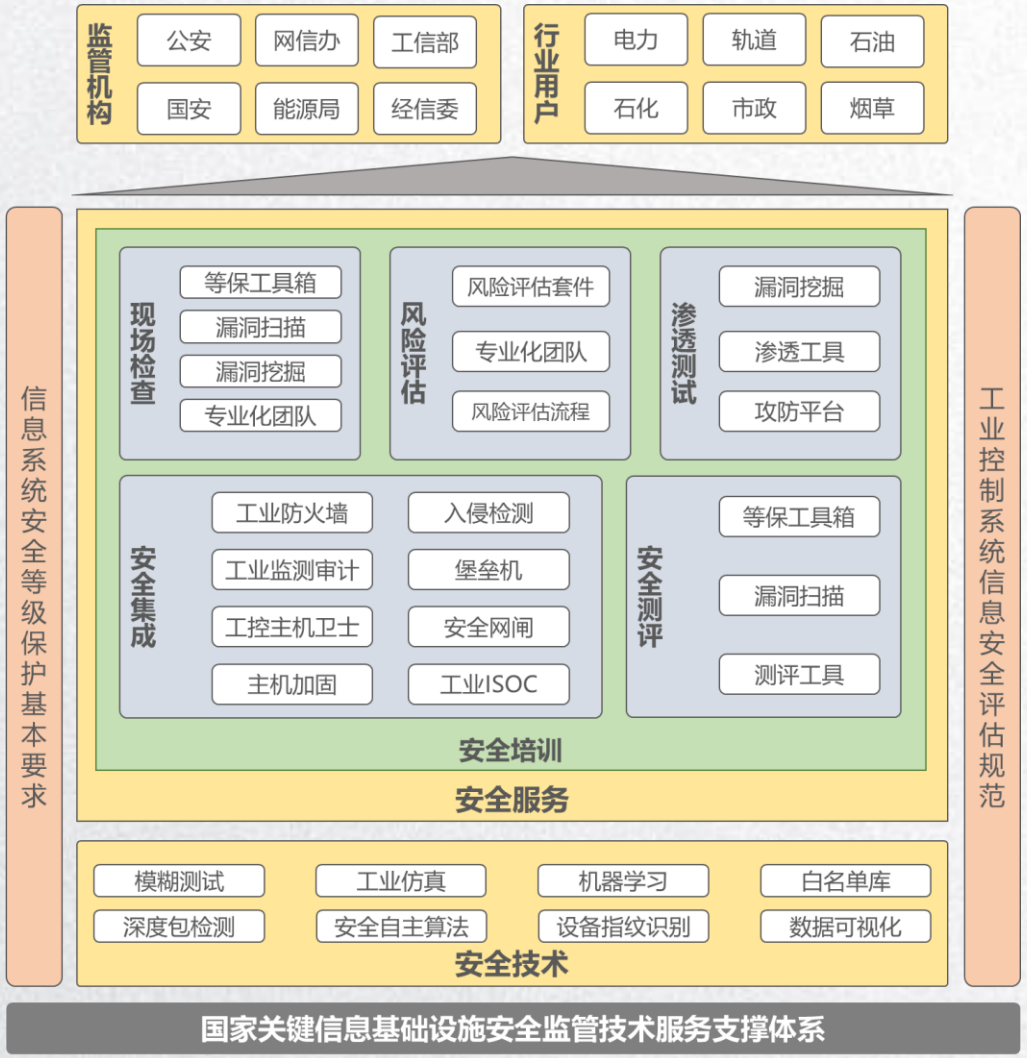
- 识别工控安全风险
- 工控渗透服务
- 制定标准/制度/流程

工控安全建设

- 建立工控安全业务模型
- 建立安全监控预警平台
- 建立工控安全防护平台

工控安全培训

- 工控安全意识宣贯
- 国家政策标准解读
- 工控安全防护方法



典型案例

发电行业	其他能源行业	市政/化工/智造	科研院所	高校/其他	工控系统厂商
上海外高桥第三电厂	西气东输西二线	重庆燃气	国家测评中心	浙江大学	和利时
山东邹县电厂	新疆风城油田	浙江台州燃气	中科院信工所	上海第二工业大学	浙大中控
沈阳金山电厂	长庆油田	山西燃气	工信部第一研究所	上海电力学院	霍尼韦尔
宜兴水电厂	兖州煤矿	榆林煤化工	国家工控安全实验室	华北电力大学	艾默生
新安江水电厂	神华煤炭	旭阳焦化	工信部信通院	济南某军校	康吉森
桐柏水电厂	平顶山煤矿集团	北汽股份	中国电科院	宝钛集团	新华中控
新疆众和电厂	广利核华龙一号验证系统	湖南中烟	南网电科院	中核太原某实验室	……
……	……	……	……	……	

威努特 WINICSSEC

专注工控·捍卫安全