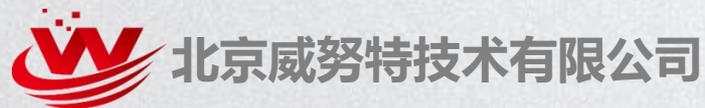


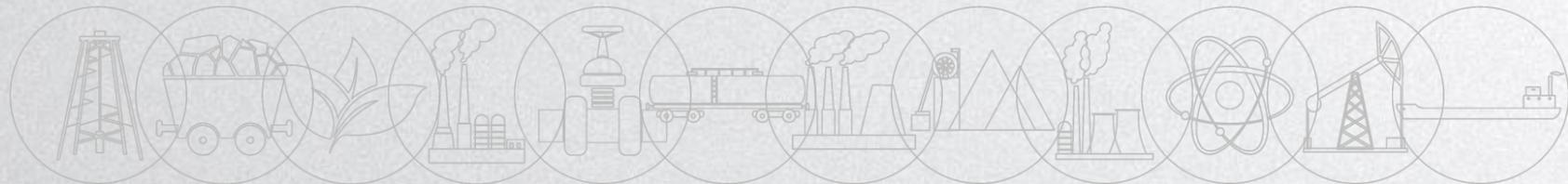
智慧油田工控网络安全防护解决方案



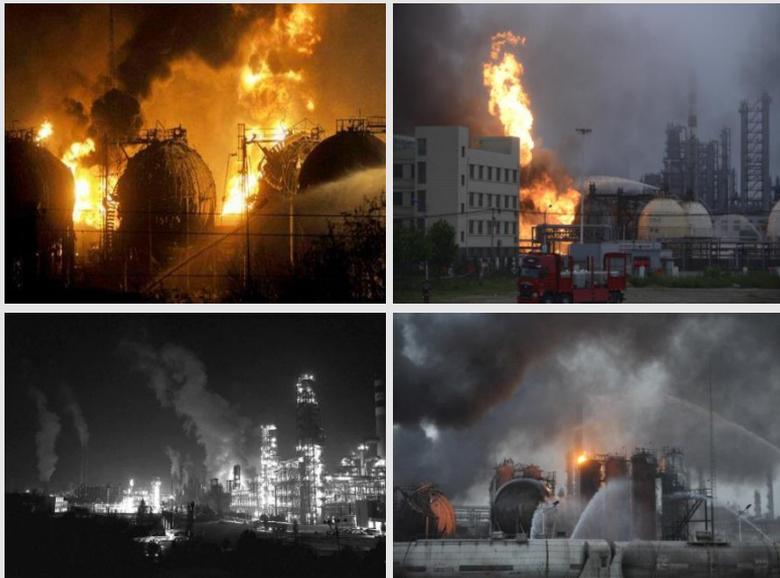
公司简介



- 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

油田工业控制系统安全背景

02

油田工业控制系统安全风险分析

03

油田工业控制系统安全解决方案

04

公司&产品服务介绍

05

方案合规性分析

01

第一部分

智慧油田工业控制系统安全背景

安全趋势 安全事件 国家政策、标准

近年来工控安全事件

安全事件 I

2016年，新疆某油田自动化监控网络感染conficker蠕虫病毒，导致主机和服务器无法正常提供服务。

安全事件 IV

2012年，美国加州Chevron石油、计算机系统曾受到震网病毒的袭击，一旦病毒侵害了真空阀，就会造成离岸钻探设备失火、人员伤亡和生产停顿等重大事故。

安全事件 II

2011年，我国某石化企业某装置控制系统分别感染Conficker病毒，造成控制系统服务器与控制器通讯不同程度地中断。

安全事件 V

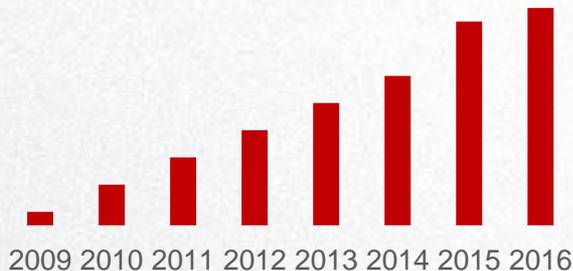
2017年5月12日，“WannaCry”勒索病毒爆发，全球100多个国家和地区超过10万台电脑遭到了攻击、感染。其中某油田就是其中的受害者之一。

安全事件 III

2015年乌克兰电网遭遇黑客攻击一事震惊世界，直接造成约70万个家庭在圣诞前夜陷入一片黑暗。

安全事件 VI

2014年，Havex病毒席卷欧美，劫持电力工控设备，阻断电力供应，在中国也发现少量样本传播。



- 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
- 智慧石油业安全风险逐渐增大

30%

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10月17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》，2017年6月1日正式实施



全国人民代表大会

The National People's Congress of the People's Republic of China

政策法规

- 《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



国家质量监督检验检疫总局

General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China



中国国家标准化管理委员会

STANDARDIZATION ADMINISTRATION OF THE PEOPLE'S REPUBLIC OF CHINA

- 《关于加强工业控制系统信息安全管理的通知》
工信部协[2010]451号



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

网络安全法

2017年6月1日落地执行

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。

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

指导建设

一、安全软件选择与管理

(一) 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**。

二、配置和补丁管理

(一) **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。

三、边界安全防护

(二) 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。

(三) 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**。

四、物理和环境安全防护

(二) 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。

七、安全监测和应急预案演练

(一) 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**。

(二) 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

智慧油田工业控制系统安全风险分析

安全建设现状分析 安全风险分析

油田工业控制系统现状

ICS系统组成现状

- 油、气、水井口和一些无人值守阀室、站，其特点是温度要求范围大，环境比较恶劣，常使用RTU系统；
- 在增压站、转油站、联合站等场合实时性要求高，逻辑联锁控制较多，常使用PLC系统；
- 在集气站、气处理站及轻烃回收等场合控制点数多，回路控制多，常使用DCS系统；
- 管理层局、厂级监控和指挥调度中心往往要求多系统集成，常建设一个SCADA中心，用于辖区内各工业控制系统实时数据的接入。

系统通讯现状

- 井口较多的使用无线仪表，如无线载荷位移传感器、无线压力、温度传感器等；
- 控制器与上位机之间以及上位机与上位机之间目前大多数采用基于以太网的工业协议；
- 在地理条件比较好的地方一般采用光纤通讯；
- 在山区可视情况比较好的地方采用无线网桥；
- 在偏远地区不适合大规模组网时利用移动网络GPRS/CDMA/3G/4G等方式。

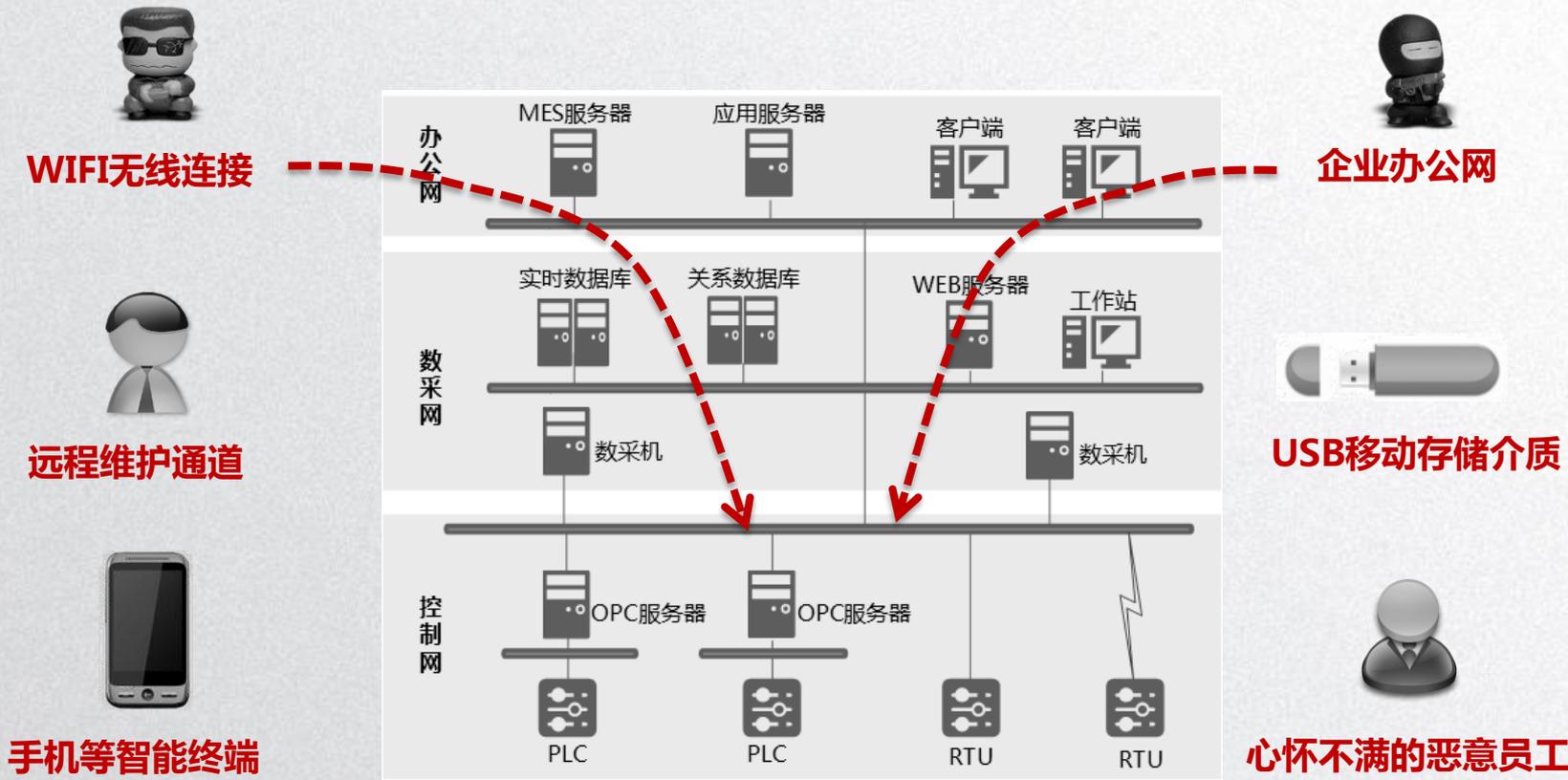
油田工控网络安全现状



通过大量的现场调研得出以下安全现状：

- 大部分企业在自动化网络与办公网络之间使用传统防火墙进行隔离，或者利用一些三层交换机的安全策略进行网络隔离和保护；但由于业务需求和工作的便捷性，防火墙策略基本是全开的或没有严格的访问控制，让整个控制网络暴露在办公网中。
- 在监控计算机上安装了必要的杀毒软件防止一些恶意软件和病毒木马的入侵，但因为局域网限制病毒库得不到及时更新，并且存在误杀、漏杀的情况，对病毒木马的防护也相当脆弱。

油田工控网络的入侵途径



油田工控网络安全风险分析

操作系统安全漏洞

- 主机系统、注册表完整性遭受破坏，导致主机不可用；
- 工程师站、操作员站或服务器操作权限受控。

应用软件安全漏洞

- 应用软件可用性遭受破坏；
- 应用软件权限受控，参数被篡改等。

网络安全设备局限性

- 单一的安全设备解决不了所有问题；
- 安全功能的缺陷，导致安全隐患依然存在。

无线网络安全漏洞

- 黑客通过无线网络进入生产网；
- 无线网络遭受破坏，导致数据无法通信；
- 通过无线网络攻击远端的控制设备、传感器等。

不安全的通信协议

- 协议缺乏认证机制，很容易被破解或遭受泛洪攻击；
- 协议无加密，很容易被篡改或假冒；
- 协议可编程，可用来自RTU、PLC注入恶意代码。

03

第三部分

智慧油田工业控制系统安全解决方案

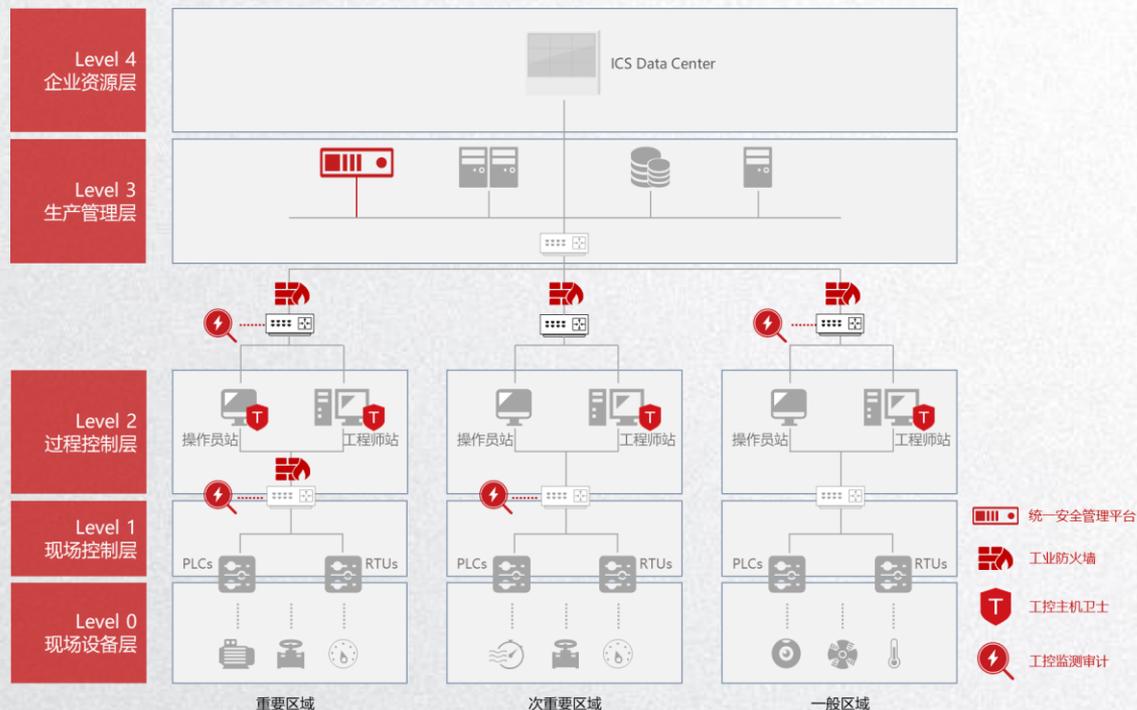
方案理念 设计依据 等级保护要求 安全解决方案设计 行业案例说明

威努特工控安全解决方案模型

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
-
- 从“黑”到“白”
 - 从“被动防御”到“主动防护”

技术亮点及创新点

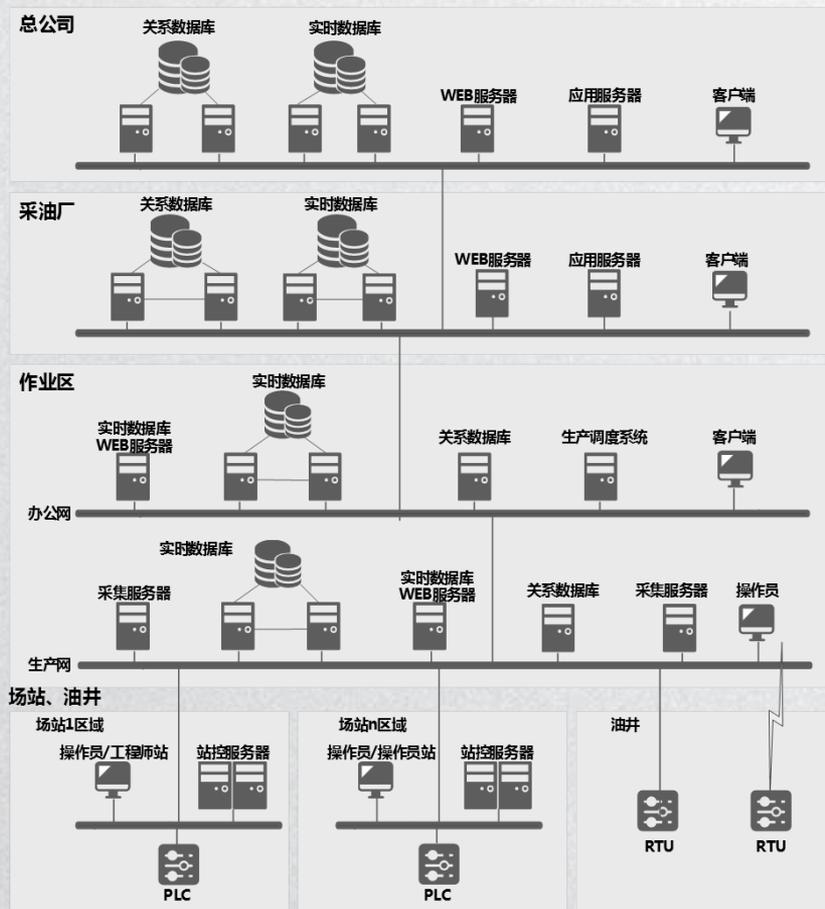
设计依据

油田 工业 控制系统 安全 解决方案 设计 依据

- 《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》
- 《工业控制系统信息安全防护指南》
- 《GB / T26333-2010 工业控制网络安全风险评估规范》

本方案重点解决以上政策标准中的核心问题

“智慧油田”网络解读



按照管理级别划分为四级

- **第一级：管理级（总公司）。**以采油厂数据（实时、关系）平台为数据源对象，将总公司需要的数据同步上来，建立总公司管理子模块。
- **第二级：采油厂级。**实时数据库接收管理区（作业区中）送来的数据，实现实时监控、工况分析、安全管理、报表管理、设备管理子系统模块。
- **第三级：作业区级。**包含管理区办公网和管理区生产网。
- **第四级：油井、场站级。**油井采用RTU采集数据，并上传数据，场站含控制系统，以有线网络为基础。

等级保护介绍

等级	级别名称	对象	侵害客体	侵害程度	监管强度
第一级	自主保护级	一般系统	合法权益	损害	自主保护
第二级	系统审计保护级		合法权益	严重损害	指导
			社会秩序和公共利益	损害	
第三级	安全标记保护级	重要系统	社会秩序和公共利益	严重损害	监督检查
第四级	结构化保护级	重要系统	社会秩序和公共利益	特别严重损害	每半年强制监督检查
			国家安全	严重损害	
第五级	访问验证保护级	极端重要系统	国安安全	特别严重损害	专门监督检查

工控等级保护介绍

工控等级保护基本要求

技术要求

物理和环境安全

边界防护

集中管控

网络和通信安全

设备和计算安全

应用和数据安全

管理要求

安全策略和管理制度

安全管理机构和人员

安全建设管理

安全运维管理

生产管理层、过程监控层、现场控制层、现场设备层所共同要求

方案设计之边界防护&网络与通信安全

标准规范	基本要求	
《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	7.1.2 边界防护	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 ； b) 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，默认拒绝所有非必要的网络数据流，允许例外网络数据流；
	7.1.4 生产管理层安全要求 7.1.4.1 网络和通信安全 7.1.4.1.3 访问控制	i) 应在网络边界或安全域之间根据访问控制策略设置访问控制规则 ，默认情况下，受控接口拒绝所有非允许的通信； ii) 应删除多余或无效的访问控制规则，优化访问控制列表，并 保证访问控制规则数量最小化 。
	7.1.5 过程监控层安全要求 7.1.5.1 网络和通信安全 7.1.5.1.4 访问控制	
	7.1.6 现场控制层安全要求 7.1.6.1 网络和通信安全 7.1.6.1.4 访问控制	

方案设计之网络与通信安全

标准规范	基本要求	
《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	7.1.5 过程监控层安全要求 7.1.5.1 网络和通信安全	7.1.5.1.6 安全审计 a) 应能生成安全相关审计记录，包括：访问控制、请求错误、操作系统事件、备份和恢复事件、配置改变、潜在的侦察活动和审计日志事件。单个审计记录应包括时间戳、来源（源设备、软件进程或人员用户帐户）、分类、类型、事件ID和事件结果； b) 应能集中管理审计事件并从系统多个组件收集审计记录，系统范围(逻辑或物理)的时间相关审计踪迹...例如，安全信息和事件管理； c) 当分配审计记录存储值达到最大审计记录存储容量的配置比例时，系统应能发出警告...
		7.1.5.1.5 入侵防范 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；

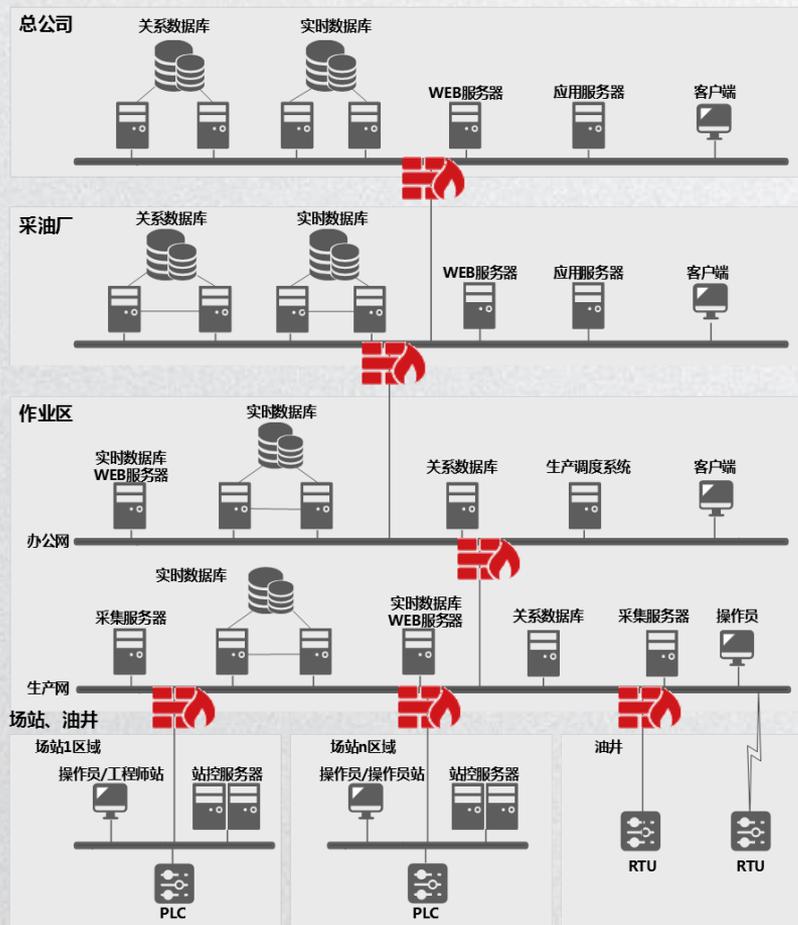
方案设计之网络与通信安全

标准规范	基本要求	
《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	7.1.5 过程监控层安全要求 7.1.5.1 网络和通信安全	7.1.5.1.5 入侵防范 a) 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；
	7.1.6 现场控制层安全要求 7.1.6.1 网络和通信安全	7.1.6.1.5入侵防范 b) 应在关键网络节点处检测从外部发起的网络攻击行为； c) 应在关键网络节点处检测从内部发起的网络攻击行为； d) 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； e) 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。

方案设计之网络与通信安全

标准规范	基本要求	
<p>《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</p>	<p>7.1.6 现场控制层安全要求 7.1.6.1 网络和通信安全</p>	<p>7.1.6.1.3 无线使用控制</p> <p>a) 应对所有参与无线通信的用户（设备）提供唯一性标识和鉴别；</p> <p>b) 根据普遍接受的安全工业实践，对无线连接的授权、监视以及执行使用限制；</p> <p>c) 识别在控制系统物理环境中发射的未经授权的无线设备，报告未经授权试图接入或干扰控制系统行为。</p>

访问控制&恶意代码防范



解决方案

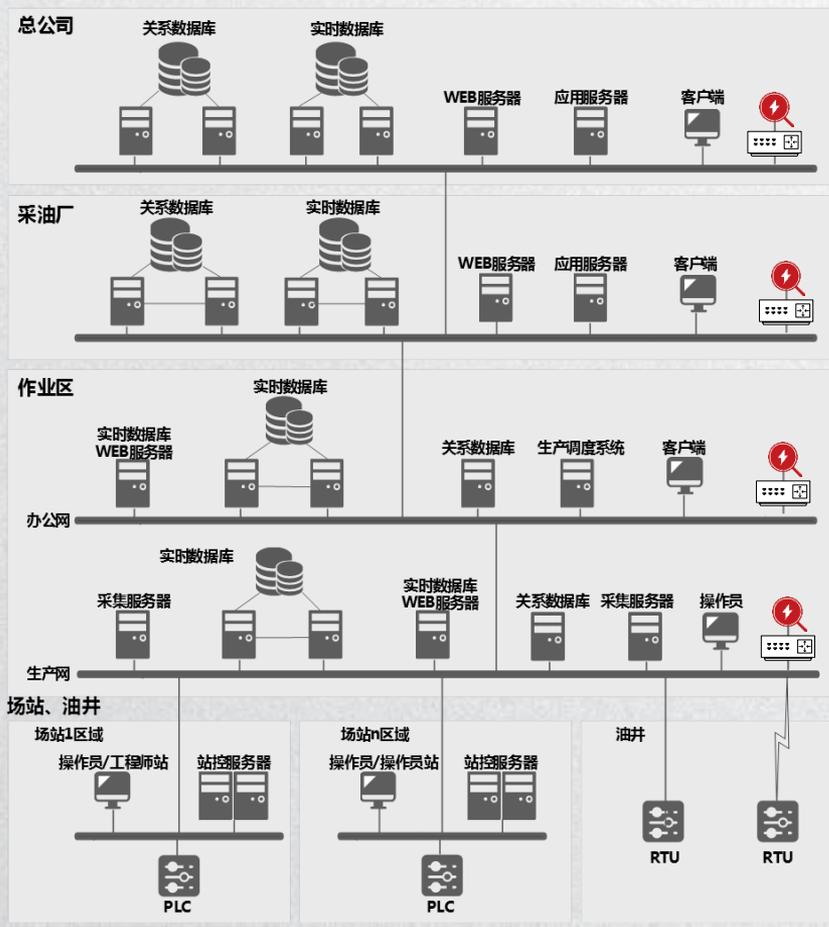
■ 解决方案

在总公司与采油厂之间、采油厂与作业区之间、在办公网与生产网之间，及各场站、油井工控网络的出口位置串联部署边界隔离设备。

■ 解决的问题

- 1) 阻止来自外部系统攻击行为；
- 2) 阻止不同系统之间的越权访问行为；
- 3) 阻止病毒、蠕虫恶意软件扩散和入侵攻击，保护控制系统安全运行；
- 4) 阻止非授权设备的接入。

网络监测审计



解决方案

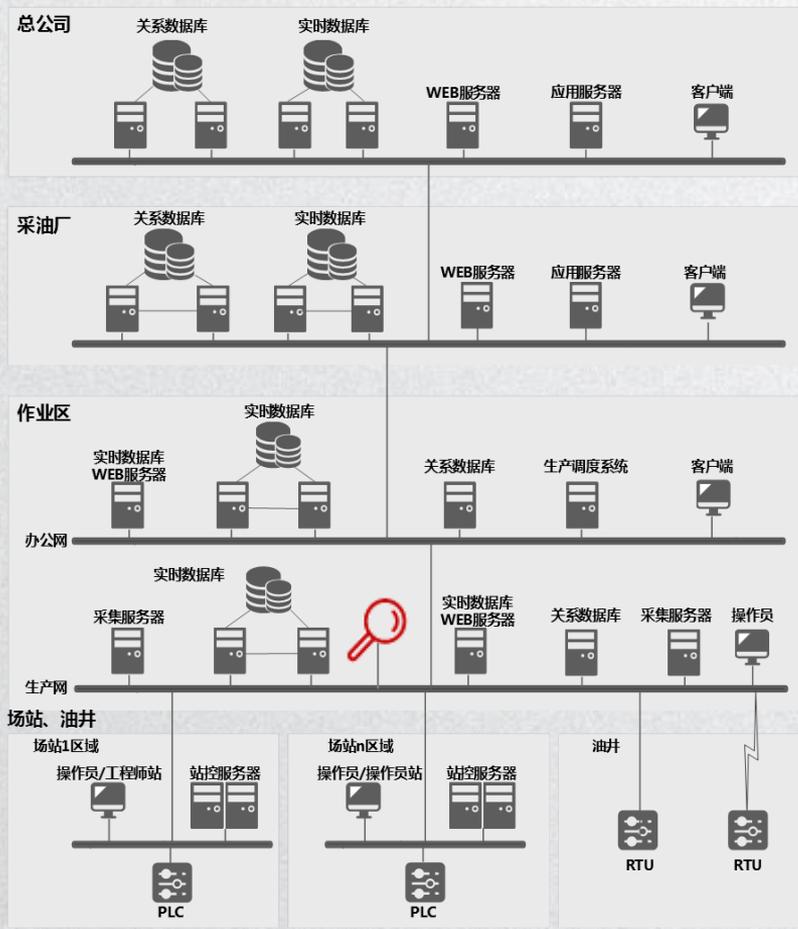
■ 解决方案

在总公司、采油厂、作业区办公网和生产网中旁路部署网络监测与审计类产品。

■ 解决的问题

- 1) 实时监测工控网络中的恶意攻击、误操作、违规行为、非法设备接入以及蠕虫、病毒等恶意软件的传播，帮助客户及时采取应对措施，避免发生安全事故；
- 2) 详实记录一切网络通信流量，包括网络连接、网络协议、网络会话、工控协议指令等，为安全事故调查取证提供技术支撑。

网络入侵检测



解决方案

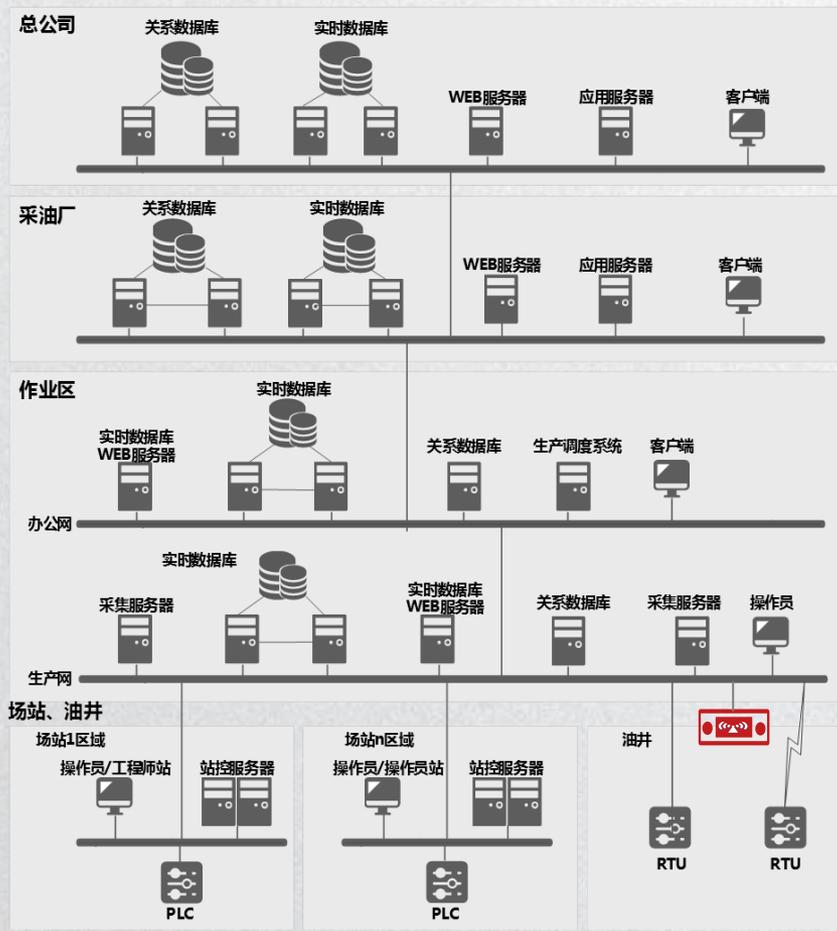
■ 解决方案

在生产网络出入口的核心交换机上旁路部署入侵检测类产品。

■ 解决的问题

- 1) 实时检测来自办公网以上和场站、油井区域的恶意行为，以及蠕虫、病毒等恶意软件的入侵，帮助客户及时采取应对措施，避免发生安全事故；
- 2) 通过网络入侵检测分析，并形成图形化的日志报表，帮助安全管理员实时展现工控网络中潜在的安全威胁和安全级别。

网络无线使用控制



解决方案

■ 解决方案

在场站、油井无线局域网内部部署无线防护类产品。

■ 解决的问题

- 1) 为场站、油井提供安全无线生产网络的同时，扫除潜在的车间生产信号干扰风险；
- 2) 防止非法设备进入工控生产网络；
- 3) 阻止非法用户对无线为网络的入侵。

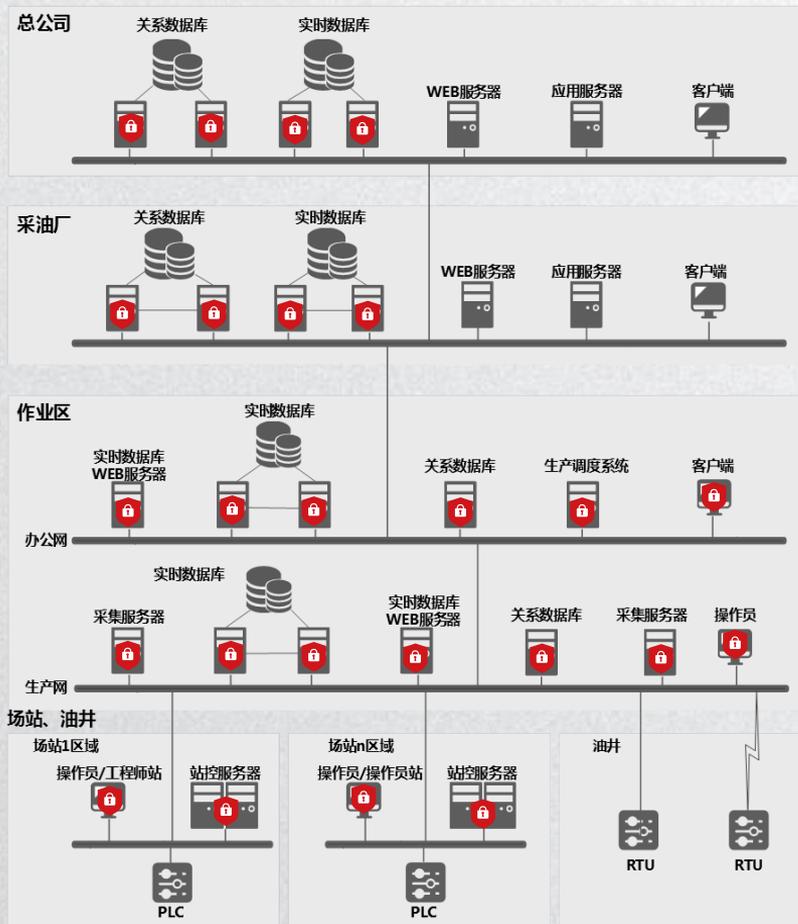
方案设计之设备和计算安全

标准规范	基本要求	
<p>《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</p>	<p>7.1.5 过程监控层安全要求 7.1.5.2 设备和计算安全</p>	<p>7.1.5.2.2 访问控制 c) 对于所有接口，应根据职责分离和最小权限对特定用户（人员、软件进程或设备）实施控制系统的控制使用授权； d) 应授权用户或角色对所有人员用户的访问权限进行规定和修改； e) 在日常维护时，应支持安全功能操作的验证和报告异常事件；</p>
		<p>7.1.5.2.6 资源控制 d) 应对工程师站、操作员站、服务器等系统运行资源进行监视，包括CPU、硬盘、内存、网络等资源的使用情况；设置预警限值并在触发时预警。</p>
	<p>7.1.6 现场控制层安全要求 7.1.6.2 设备和计算安全</p>	<p>7.1.6.2.1 身份鉴别 a) 应对设备的远程管理、组态文件下装等重要操作进行身份鉴别……； b) 禁止使用默认账户和口令，口令应有复杂度要求……，口令应设定有效期限，并定期更换； c) 应具有鉴别失败处理功能……，限制非法登录次数并报警，当登录连接超时自动退出等相关措施；</p>
		<p>7.1.6.2.2 安全审计 a) 应提供生成安全相关审计记录的能力……，单个审计记录应包括时间戳、来源（源设备、软件进程或人员用户帐户）、分类、类型、事件ID和事件结果；</p> <p>7.1.6.2.3 入侵防范 c) 应关闭不需要的系统服务、默认共享和高危端口； d) 停机维护期间，应能发现可能存在的漏洞，并在经过充分测试评估后，及时修补漏洞。</p>

方案设计之设备和计算安全

标准规范	基本要求	
《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	7.1.5 过程监控层安全要求	7.1.5.2.4 入侵防范 d) 所有主机设备操作系统采用最小化系统安装原则，除了必要的安全组件或软件外， 只安装与自身业务相关的操作系统组件及应用软件 ，如工程师站、组态软件.....与此相关的操作系统组件。
	7.1.5.2 设备和计算安全	7.1.5.2.5 恶意代码防范 a) 应对可能造成损害的移动代码技术执行使用限制 ，包括：防止移动代码的执行.....，限制移动代码传入/传出控制系统.....； c) 应采取保护机制 ，防止、检测、报告和 减轻恶意代码或未经授权软件的影响 ，应更新防护机制。

主机身份鉴别&访问控制&审计&资源控制



解决方案

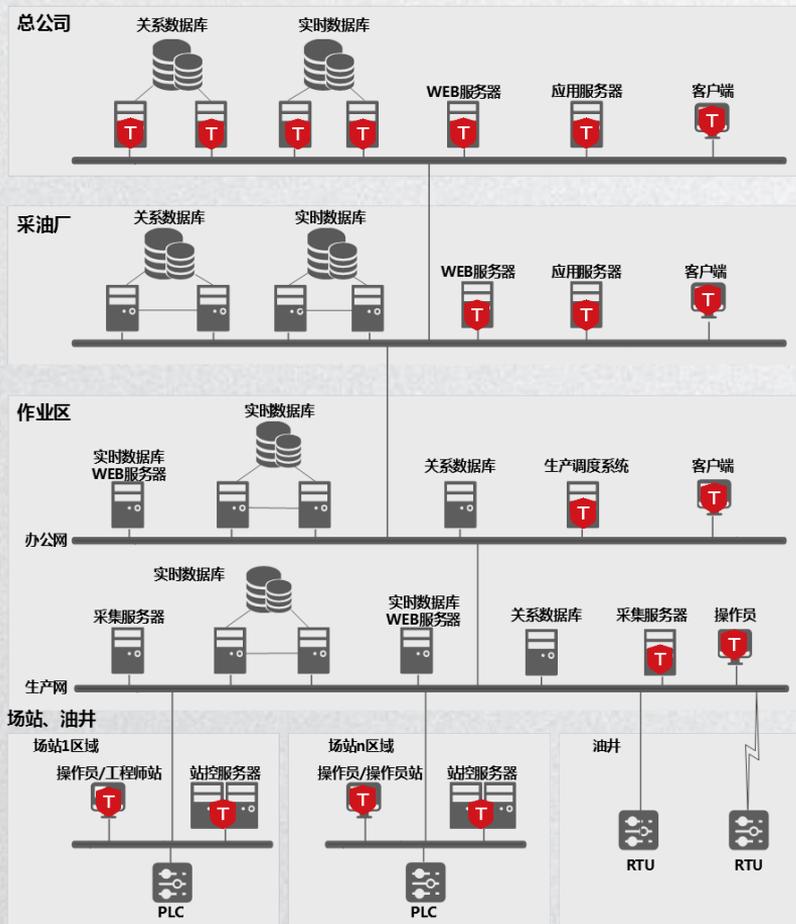
■ 解决方案

在工控网络的关键主机和服务器中安装主机加固类产品。

■ 解决的问题

- 1) 采用双重身份认证鉴别技术，强化口令鉴别（USBKEY）加用户名密码鉴别，保障终端和服务不被非法用户控制。
- 2) 实行强制访问控制，将主体的访问操作权限控制到指定的客体（IP、账户、文件、进程、服务）实现权限最小原则。
- 3) 对所有主机、服务器被操作的日志、事件日志等信息进行记录，为事后审计追踪溯源提供依据。
- 4) 实现对服务器CPU、硬盘、内存、网络等资源的使用情况进行监视，触发预警限值时发出预警提示。

主机入侵防范&恶意代码防范



解决方案

■ 解决方案

在工控网络的关键主机和服务端中安装主机白名单类产品。

■ 解决的问题

- 1) 阻止非授权软件或进程的安装和运行，防止恶意代码攻击“0-day”漏洞的利用。
- 2) 避免升级病毒库及漏洞库，变被动为主动；
- 3) 防止操作员使用移动介质带入病毒在业务网中扩散；
- 4) 杜绝信息非法窃取、数据和系统遭受非法破坏的行为发生。

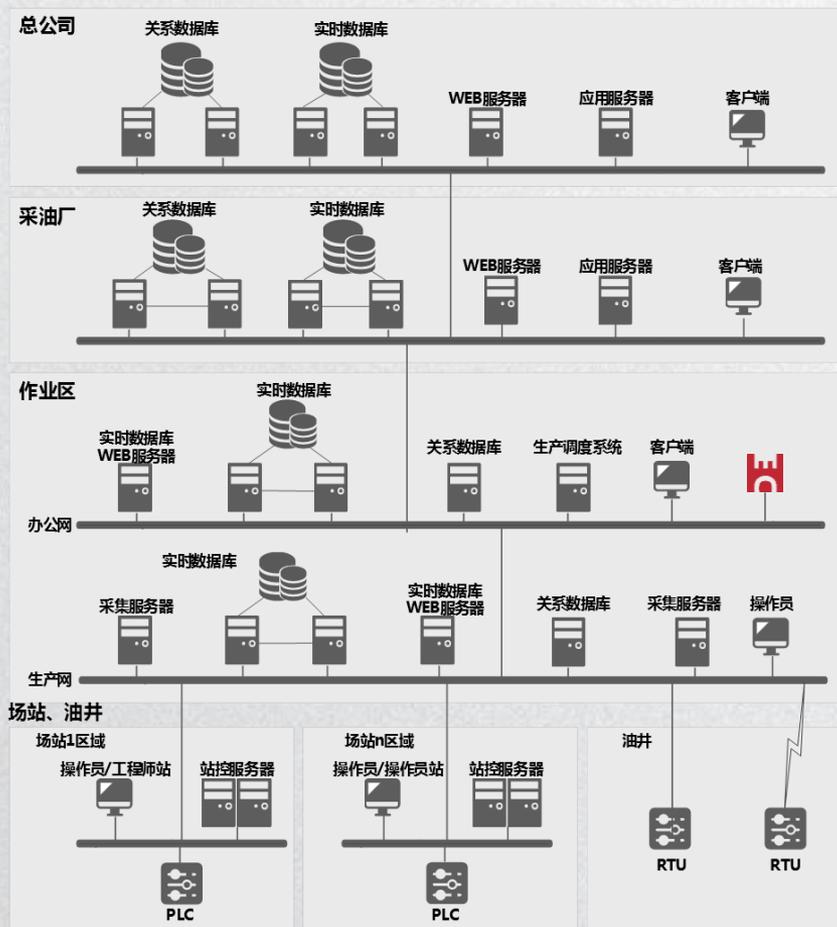
方案设计之应用和数据安全

标准规范	基本要求	
<p>《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</p>	<p>7.1.5 过程 监控层安全 要求 7.1.5.3 应用和数据 安全</p>	<p>7.1.5.3.2 身份鉴别</p> <p>a) 应唯一地标识和鉴别所有人员用户.....。当有人员用户访问时.....实施职责分离和最小权限；</p> <p>c) 应防止任何已有的用户账户重复使用同一批口令，并加强用户口令的最大和最小有效期的使用.....；</p> <p>d) 应在可配置时间周期内.....，当访问次数超出限制后，应进行报警；对于代表关键服务或者服务器运行的系统账户，应不允许交互式登录；</p>
		<p>7.1.5.3.3 访问控制</p> <p>a) 应支持授权用户来管理所有帐户，包括添加、激活、修改、禁用和删除帐户；</p> <p>b) 应支持统一账户管理；</p> <p>c) 应通过手动或在一个可配置非活动周期后，系统自动启动会话锁定防止进一步访问，.....直到拥有会话的人员用户或其它授权的人员用户使用适当的身份标识和鉴别规程重新建立访问；</p> <p>d) 对于所有接口，应根据职责分离和最小权限对所有用户实施控制使用授权；</p> <p>e) 应为授权用户或角色提供这样的能力，对所有人员的访问权限进行规定和修改；</p>
		<p>7.1.5.3.4 安全审计</p> <p>a) 应生成安全相关审计记录，类别有：访问控制、请求错误、配置改变和审计日志事件。单个审计记录应包括时间戳、来源（源设备、软件进程或人员用户帐户）、分类、类型、事件ID和事件结果；</p> <p>d) 应具备以可配置频率的，与系统时钟同步的能力；</p> <p>f) 授权人员和/或工具应使用只读方式访问审计日志；</p>

方案设计之应用和数据安全

标准规范	基本要求	
《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	7.1.6 现场控制层安全要求 7.1.6.3 应用和数据安全	7.1.6.3.1 无线使用控制 a) 应对所有参与无线通信的用户（人员和软件进程）提供唯一性标识和鉴别。

网络设备防护&审计&身份鉴别



解决方案

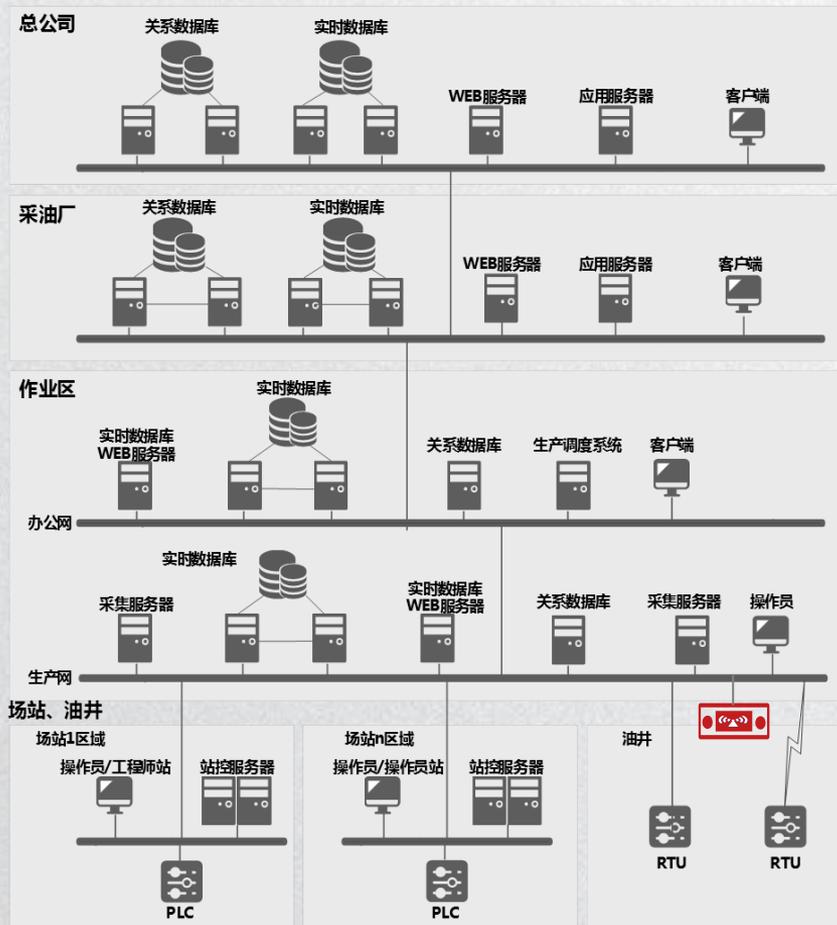
■ 解决方案

在工控网络核心管理网的前端部署运维审计类产品。

■ 解决的问题

- 1) 阻止非授权用户访问网络、安全设备；
- 2) 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；
- 3) 对远程维护行为操作进行监测、审计，阻止误操作、恶意操作；
- 4) 全程记录维护行为，对恶意操作行为进行取证。

无线使用控制



解决方案

■ 解决方案

在工控网络的无线局域网内部署无线防护类产品。

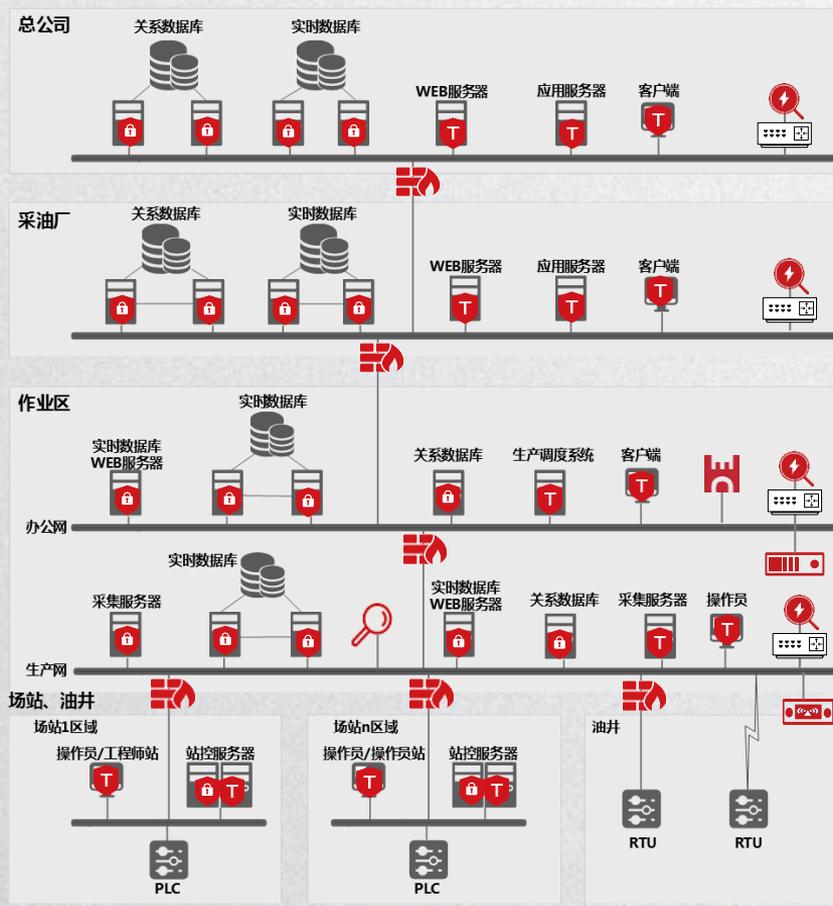
■ 解决的问题

- 1) 对每个无线用户进行唯一性标识，防止非法用户的访问；
- 2) 防止非法用户对传输数据的篡改和窃听；

方案设计之统一管理

标准规范	基本要求
<p>《信息安全技术 网络安全等级保护基本要求》</p> <p>附录D 基于可信计算技术的工业控制系统安全等级防护</p>	<p>D.2 可信保障的三重防御多级互联技术框架</p> <p>d) 可信/安全管理中心：对工控系统的安全策略以及计算环境、应用区域边界和通信网络上的安全机制实现统一管理的平台。在安全管理中心内部又分为系统资源管理、安全控制和审计三部分。</p>

工控网络统一安全管理



解决方案

■ 解决方案

在工控网络可达位置部署统一安全管理系统。

■ 解决的问题

- 1) 统一管理安全设备，如策略制定、下发等；
- 2) 对安全日志进行关联分析，并通过图形、报表方式对当前安全状态进行可视化展示；
- 3) 便于上级级维护人员进行维护管理，实现安全事件报警管理。

行业典型案例—新疆某油田

客户需求：

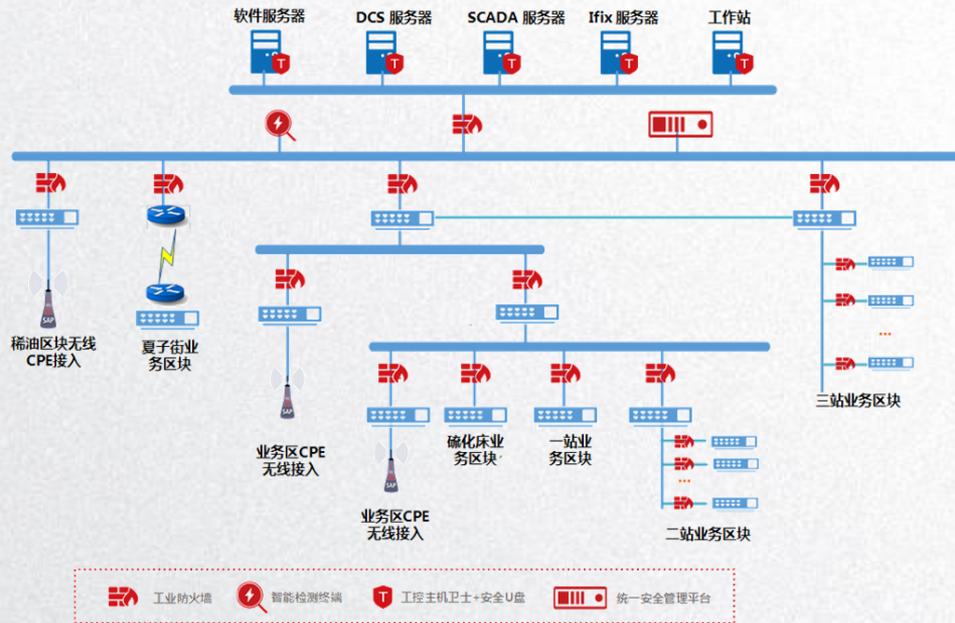
- 实时网络访问管控；防范工控主机病毒感染及扩散；
- 对各类入侵行为进行实时监测、告警和记录；
- 防止越权操作和误操作，避免造成生产事故。

解决方案：

- 部署工业防火墙对采油厂工控网络分区分域，配置不同的访问控制策略。
- 在采油厂各工程师站、操作员站上部署工控主机卫士；
- 部署监测审计平台，对操作人员的行为进行审计和记录；
- 部署统一安全管理平台，对网络中的安全设备进行统一配置和管理。

客户价值：

- 满足油田发展规划要求及工控安全防护要求。
- 全面改进作业区业务人员 产安全保驾护航。的安全水平和安全意识，提高安全生产管理水平、工作效率和管理效率。
- 全面提高油田生产网络的整体安全性，确保设备、系统、网络的可靠性、稳定性和安全性。



行业典型案例—中国石油某油田公司

客户需求：

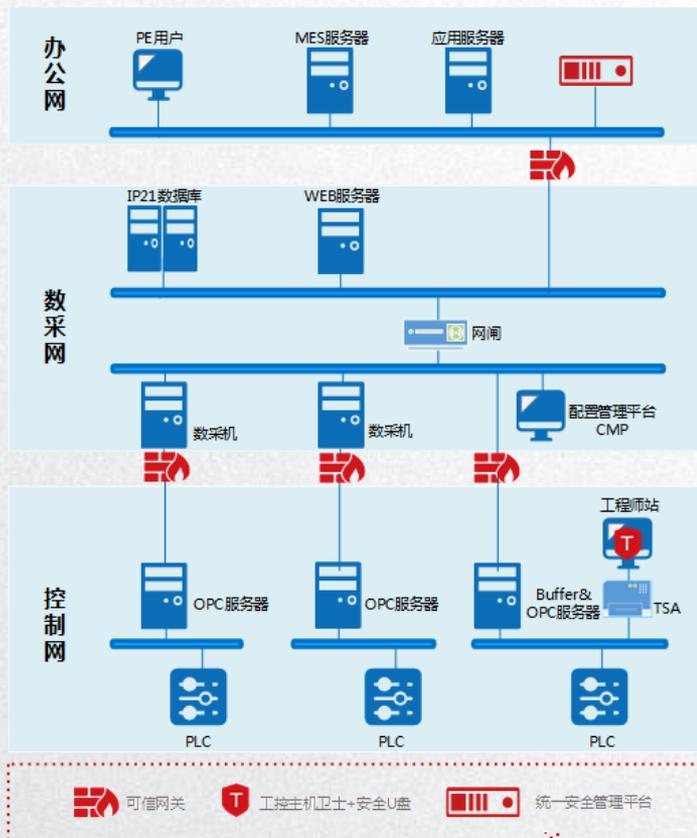
- 对办公网、数采网、控制网进行安全隔离，降低网络的安全风险和事件影响范围；
- 对于老旧的主机和操作系统，需要相应的技术措施保障应用系统服务器、上位机等终端不被病毒入侵。

解决方案：

- 在数采网和控制网边界部署工业防火墙，对各功能区之间的访问进行严格控制，防止非法访问；
- 在工程师站和操作员部署工控主机卫士，实现主机防护。

客户价值：

- 满足国家及行业政策法规有关安全防护的要求。
- 提高了数采通讯安全性，保障石油生产系统安全稳定运行。
- 全面提高油田生产网络的整体安全性，确保设备、系统、网络的可靠性、稳定性和安全性，为石油生产安全保驾护航。





04

第四部分
方案合规性分析

信息安全技术 网络安全等级保护基本要求
工业控制系统信息安全防护指南

工控等保

边界防护&访问控制

标准规范	基本要求		方案符合度	涉及产品
《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	7.1.2 边界防护	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 ； b) 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，默认拒绝所有非必要的网络数据流，允许例外网络数据流；	符合 。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部署 边界防护设备 ，采用“白名单”机制，拒绝非必要访问流量，只允许正常生产相关的流量出入。	工业防火墙 工业网闸
	7.1.4 生产管理层安全要求 7.1.4.1 网络和通信安全 7.1.4.1.3 访问控制	i) 应在网络边界或安全域之间根据访问控制策略 设置访问控制规则 ，默认情况下，受控接口拒绝所有非允许的通信； ii) 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化。		
	7.1.5 过程监控层安全要求 7.1.5.1 网络和通信安全 7.1.5.1.4 访问控制			
	7.1.6 现场控制层安全要求 7.1.6.1 网络和通信安全 7.1.6.1.4 访问控制			

工控等保

安全审计&入侵防范

标准规范	基本要求		方案符合度	涉及产品
<p>《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</p>	<p>7.1.5 过程监控层安全要求 7.1.5.1 网络和通信安全</p>	<p>7.1.5.1.6 安全审计 a) 应能生成安全相关审计记录，包括：访问控制、请求错误、操作系统事件、备份和恢复事件、配置改变、潜在的侦察活动和审计日志事件。单个审计记录应包括时间戳、来源（源设备、软件进程或人员用户帐户）、分类、类型、事件ID和事件结果； b) 应能集中管理审计事件并从系统多个组件收集审计记录，系统范围(逻辑或物理)的时间相关审计踪迹...例如，安全信息和事件管理； c) 当分配审计记录存储值达到最大审计记录存储容量的配置比例时，系统应能发出警告...</p>	<p>符合。在过程监控层核心交换机上部署监测审计系统，记录各类安全事件和信息，特别是不符合工业现场正常生产行为的事件或行为进行检测，为事件追踪溯源提供依据。</p>	<p>监测审计系统</p>
<p>7.1.5.1.5 入侵防范 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；</p>				

工控等保 入侵防范

标准规范	基本要求		方案符合度	涉及产品
<p>《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</p>	<p>7.1.5 过程监控层安全要求 7.1.5.1 网络和通信安全</p>	<p>7.1.5.1.5 入侵防范 a) 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；</p>	<p>符合。在过程监控层关键节点旁路部署入侵检测系统及安全隔离设备（如防火墙等）检测并限制网络攻击行为。</p>	<p>入侵检测系统 工业防火墙</p>
	<p>7.1.6 现场控制层安全要求 7.1.6.1 网络和通信安全</p>	<p>7.1.6.1.5 入侵防范 b) 应在关键网络节点处检测从外部发起的网络攻击行为； c) 应在关键网络节点处检测从内部发起的网络攻击行为； d) 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； e) 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。</p>		

工控等保 无线安全防护

标准规范	基本要求		方案符合度	涉及产品
《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	7.1.6 现场控制层安全要求 7.1.6.1 网络和通信安全	7.1.6.1.3 无线使用控制 a) 应对所有参与无线通信的用户（设备）提供唯一性标识和鉴别； b) 根据普遍接受的安全工业实践，对无线连接的授权、监视以及执行使用限制； c) 识别在控制系统物理环境中发射的未经授权的无线设备，报告未经授权试图接入或干扰控制系统行为。	符合。 在AP所在LAN交换机上旁路部署无线入侵安全防护系统，扫除潜在的生产信号干扰风险，使生产运行更加可靠，构建高安全的网络生产环境。	无线安全防护系统
	7.1.6 现场控制层安全要求 7.1.6.3 应用和数据安全	7.1.6.3.1 无线使用控制 应对所有参与无线通信的用户（人员和软件进程）提供唯一性标识和鉴别。		

工控等保 主机安全防护

标准规范	基本要求	方案符合度	涉及产品
《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	7.1.5 过程监控层安全要求 7.1.5.2 设备和计算安全	符合。 在关键主机和服务站上部署 白名单 类产品，阻止一切不在白名单库中的软件、程序的安装和执行。	主机白名单产品
	7.1.5.2.4 入侵防范 d) 所有主机设备操作系统采用最小化系统安装原则，除了必要的安全组件或软件外， 只安装与自身业务相关的操作系统组件及应用程序 ，如工程师站、组态软件.....与此相关的操作系统组件。 7.1.5.2.5 恶意代码防范 a) 应对可能造成损害的移动代码技术执行使用限制 ，包括：防止移动代码的执行.....，限制移动代码传入/传出控制系统.....； c) 应采取保护机制 ，防止、检测、报告和 减轻恶意代码或未经授权软件的影响 ，应更新防护机制。		

工控等保 主机加固

标准规范	基本要求		方案符合度	涉及产品
<p>《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</p>	<p>7.1.5 过程监控层安全要求 7.1.5.2 设备和计算安全</p>	<p>7.1.5.2.2 访问控制 c) 对于所有接口，应根据职责分离和最小权限对特定用户（人员、软件进程或设备）实施控制系统的控制使用授权； d) 应授权用户或角色对所有人员用户的访问权限进行规定和修改； e) 在日常维护时，应支持安全功能操作的验证和报告异常事件；</p>	<p>符合。在工控网络中的关键主机和服务器上部署主机加固类产品，对主机基线、主机资源的访问权限、用户的身份鉴别等进行严格的管控。</p>	<p>主机加固系统</p>
		<p>7.1.5.2.6 资源控制 d) 应对工程师站、操作员站、服务器等系统运行资源进行监视，包括CPU、硬盘、内存、网络等资源的使用情况；设置预警限值并在触发时预警。</p>		
	<p>7.1.6 现场控制层安全要求 7.1.6.2 设备和计算安全</p>	<p>7.1.6.2.1 身份鉴别 a) 应对设备的远程管理、组态文件下装等重要操作进行身份鉴别； b) 禁止使用默认账户和口令，口令应有复杂度要求.....，口令应设定有效期限，并定期更换； c) 应具有鉴别失败处理功能.....，限制非法登录次数并报警，当登录连接超时自动退出等相关措施；</p>		
		<p>7.1.6.2.2 安全审计 a) 应提供生成安全相关审计记录的能力.....，单个审计记录应包括时间戳、来源（源设备、软件进程或人员用户帐户）、分类、类型、事件ID和事件结果；</p>		

工控等保

主机加固&漏洞挖掘&漏洞扫描

标准规范	基本要求	方案符合度	涉及产品
《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	7.1.6 现场控制层安全要求 7.1.6.2 设备和计算安全	符合。 在工控网络中的关键主机和服务服务器上部署 主机加固类产品 ，对主机基线、主机资源的访问权限、用户的身份鉴别等进行严格的管控。	主机加固系统
		7.1.6.2.3 入侵防范 d) 停机维护期间，应能发现可能存在的漏洞 ，并在经过充分测试评估后，及时修补漏洞。	符合。 在停机维护期间，采用 工控漏扫、漏挖类产品 对工控系统进行已知和未知漏洞发现，并提出修改建议

工控等保 运维审计

标准规范	基本要求		方案符合度	涉及产品
<p>《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</p>	<p>7.1.5 过程监控层安全要求 7.1.5.3 应用和数据安全</p>	<p>7.1.5.3.2 身份鉴别</p> <p>a) 应唯一地标识和鉴别所有人员用户……。当有人员用户访问时……实施职责分离和最小权限；</p> <p>c) 应防止任何已有的用户账户重复使用同一批口令，并加强用户口令的最大和最小有效期的使用……；</p> <p>d) 应在可配置时间周期内……，当访问次数超出限制后，应进行报警；对于代表关键服务或者服务器运行的系统账户，应不允许交互式登录；</p>	<p>符合。在工控网络的核心管理区出口部署运维审计类产品，对运维人员的操作权限、操作内容等进行严格的管控。</p>	<p>运维审计系统</p>
		<p>7.1.5.3.3 访问控制</p> <p>a) 应支持授权用户来管理所有帐户，包括添加、激活、修改、禁用和删除帐户；</p> <p>b) 应支持统一账户管理；</p> <p>c) 应通过手动或在一个可配置非活动周期后，系统自动启动会话锁定防止进一步访问，……直到拥有会话的人员用户或其它授权的人员用户使用适当的身份标识和鉴别规程重新建立访问；</p> <p>d) 对于所有接口，应根据职责分离和最小权限对所有用户实施控制使用授权；</p> <p>e) 应为授权用户或角色提供这样的能力，对所有人员的访问权限进行规定和修改；</p>		
		<p>7.1.5.3.4 安全审计</p> <p>a) 应生成安全相关审计记录，类别有：访问控制、请求错误、配置改变和审计日志事件。单个审计记录应包括时间戳、来源（源设备、软件进程或人员用户帐户）、分类、类型、事件ID和事件结果；</p> <p>d) 应具备以可配置频率的，与系统时钟同步的能力；</p> <p>f) 授权人员和/或工具应使用只读方式访问审计日志；</p>		

工控等保 集中管理

标准规范	基本要求	方案符合度	涉及产品
《信息安全技术 网络安全等级保护基本要求》附录D 基于可信计算技术的工业控制系统安全等级防护	D.2 可信保障的三重防御多级互联技术框架 d) 可信/安全管理中心：对工控系统的安全策略以及计算环境、应用区域边界和通信网络上的安全机制实现统一管理的平台。在安全管理中心内部又分为系统资源管理、安全控制和审计三部分。	符合。部署 统一安全管理中心 ，实现安全设备、系统的统一管理、日志收集等。	安全管理中心产品

工业控制系统信息安全防护指南

标准规范		基本要求	方案符合度	涉及产品
工业控制系统信息安全防护指南	一、安全软件选择与管理	<p>(一) 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。</p> <p>(二) 建立防病毒和恶意软件入侵管理机制，对工业控制系统及临时接入的设备采取病毒查杀等安全预防措施。</p>	符合。采用 应用程序白名单软件产品 ，阻止非授权软件或进程的安装和运行，防止恶意代码攻击。	应用程序白名单软件产品
	三、边界安全防护	<p>(一) 分离工业控制系统的开发、测试和生产环境。</p> <p>(二) 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。</p> <p>(三) 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。</p>	符合。采用 工业防火墙、网闸 等安全隔离措施实现控制网络与企业网或互联网之间的安全隔离。	工业防火墙、网闸
	四、物理和环境安全防护	<p>(二) 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。</p>	符合。采用 主机外设安全防护系统 实现主机外设的安全管理，防止外设滥用导致病毒感染、传播及扩散。	主机外设安全防护系统

工业控制系统信息安全防护指南

标准规范		基本要求	方案符合度	涉及产品
工业控制系统 信息安全防护 指南	五、身份认证	(一) 在工业主机登录、应用服务资源访问、工业云平台访问等过程中使用 身份认证管理 。对于 关键设备、系统和平台的访问采用多因素认证 。	符合。采用 运维安全审计系统 实现运维过程的全面监控和审计,以及账户权限分配、账号、密码复杂度设置等。	运维安全 审计系统
		(二) 合理分类设置账户权限,以最小特权原则分配账户权限 。		
		(三) 强化工业控制设备、SCADA软件、工业通信设备等的登录账户及密码, 避免使用默认口令或弱口令,定期更新口令 。		
	六、远程访问 安全	(一) 原则上严格 禁止工业控制系统面向互联网开通HTTP、FTP、Telnet等高风险通用网络服务 。	符合。采用 工业防火墙 实现访问主客体的权限设置,只开放必须开放的服务。	运维安全 审计系统、 日志审计 系统
		(二) 确需远程访问的,采用 数据单向访问控制等策略进行安全加固 ,对访问时限进行控制,并采用加标锁定策略。		
		(四) 保留工业控制系统的相关访问日志,并对操作过程进行安全审计 。		

05

第五部分

公司&产品与服务介绍

公司介绍 安全产品 安全服务

05

第五部分

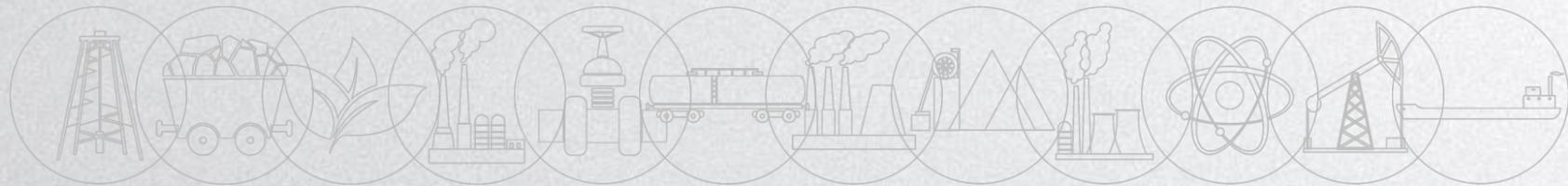
公司与产品服务介绍

公司简介 安全事记 一点成绩 产品与案例

公司简介

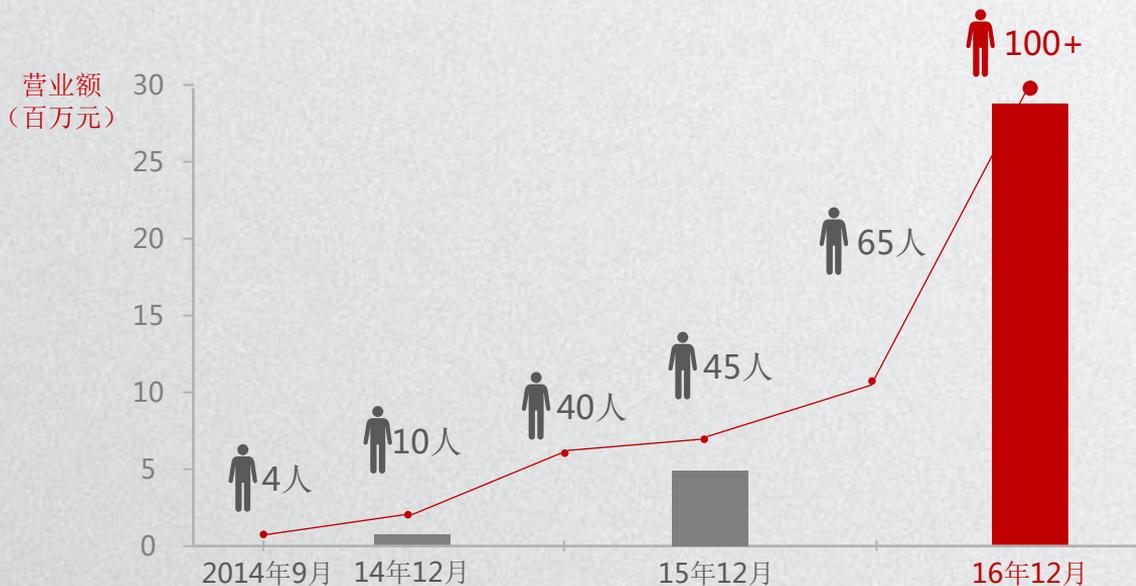


- 北京威努特技术有限公司是国内专注于工控安全领域的高新技术型企业。以研发工控安全产品为基础，打造多行业安全解决方案，提供培训、咨询、评估、建设、运维全流程安全服务。
- 国内首家提出工业网络“白环境”理念，迄今已服务电力、石油、石化、市政、烟草、化工、军工、轨道交通等行业近百家客户，落地项目遥遥领先，市场占有率全国第一。



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



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

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

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



资质荣誉



ISO9001/14001/27001



国家高新技术企业



国家网络与信息安全
信息通报机制技术支持单位



信息安全等级保护安全
建设服务机构能力评估



国家信息安全漏洞库支撑单位



牵头&配合制定
多项国家及地方标准



2016杭州
G20峰会网络安保单位



“一带一路”
高峰论坛安保单位



国家工控安全实验室理事单位



全国工业和信息化人
才培养工程培训基地

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

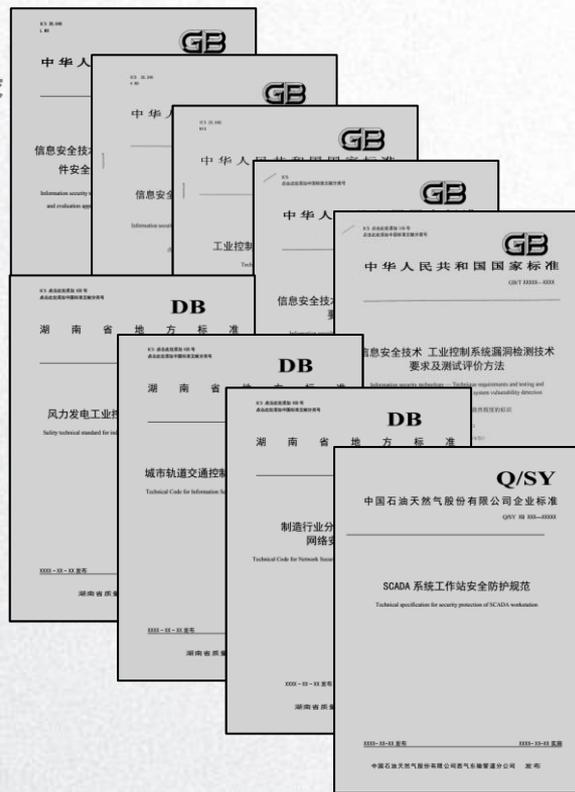
湖南省地方标准 《城市轨道交通控制系统信息安全技术规范信息安全技术》
湖南省地方标准 《风力发电工业控制系统安全技术标准》
湖南省地方标准 《制造行业分布式控制系统DNC网络安全技术规范》

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



工业主机安全
安全U盘

防御类



工业防火墙



单向隔离网关



运维管理系统 (堡垒机)

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

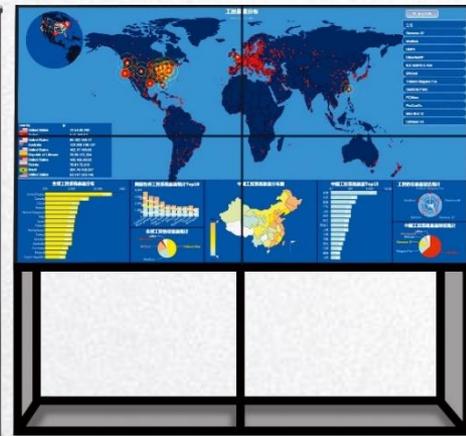
科研类



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

例对工程师站组态变更、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



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。

- 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

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

上海外高桥第三电厂
山东邹县电厂
沈阳金山电厂
宜兴水电厂
新安江水电厂
桐柏水电厂
新疆众和电厂
.....



其他能源行业

西气东输西二线
新疆风城油田
长庆油田
兖州煤矿
神华煤炭
平顶山煤矿集团
广利核华龙一号验证系统
.....



市政/化工/智造

重庆燃气
浙江台州燃气
山西燃气
榆林煤化工
旭阳焦化
北汽股份
湖南中烟
.....



科研院所

国家测评中心
中科院信工所
工信部第一研究所
国家工控安全实验室
工信部信通院
中国电科院
南网电科院
.....



高校/其他

浙江大学
上海第二工业大学
上海电力学院
华北电力大学
济南某军校
宝钛集团
中核太原某实验室
.....



工控系统厂商

和利时
浙大中控
霍尼韦尔
艾默生
康吉森
新华中控
.....





威努特
WINICSSEC

| 专注工控 · 捍卫安全

