DNC网络安全防护解决方案

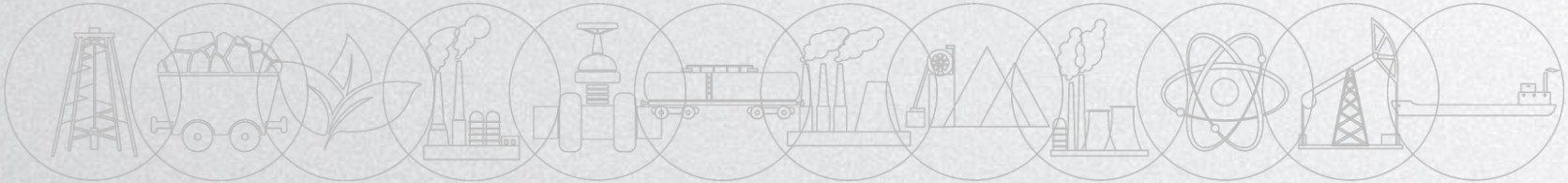
北京威努特技术有限公司

目录

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。

01

第一部分
DNC网络工控安全背景

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

2005年，Zotob蠕虫事件导致全美13个汽车制造厂被迫关闭，造成巨大经济损失超过$1,400,000

安全事件II

安全专家从2016款奥迪Q3发现遥控钥匙密码可被置于附近的设备捕捉到，存在这一缺陷总数接近1亿辆

安全事件III

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，包含了大量的工业现场主机

安全事件IV

2014年，Havex病毒病毒席卷欧美，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

安全事件V

2010年，伊朗核燃料工厂遭遇“震网病毒”袭击，导致控制系统失效，1000台离心机损坏

安全事件VI

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
- 据ICS-Cert报告，2015年关键制造业成为本年度受攻击最多的行业，占比达33%

中国制造2025

- 2014年10月，李克强总理访德期间，中德双方共同发表了以“共塑创新”为主题的《中德合作行动纲要》，宣布两国将开展“工业4.0”合作。
- 2015年5月8日，国务院正式发布《中国制造2025》规划，要求**推进信息化与工业深度融合，把智能制造作为两化深度融合的主攻方向…加强智能制造工业控制系统网络安全保障能力建设，健全综合保障体系。**

政策法规

- 2016年7月首次全国范围关键信息基础设施网络安全检查工作正式启动

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》，并于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

- 《关于深化制造业与互联网融合发展的指导意见》（国发〔2016〕28号）

中华人民共和国中央人民政府
www.gov.cn

- 《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

中国国家标准化管理委员会
STANDARDIZATION ADMINISTRATION OF THE PEOPLE'S REPUBLIC OF CHINA

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

- 《武器装备科研生产单位一级保密资格标准》
《武器装备科研生产单位一级保密资格评分标准》

国家保密局
Secrecy Administration Bureau

国家国防科技工业局
State Administration of Science, Technology and Industry for National Defence, PRC

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。

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**。

DNC工控网络安全要求 政策要求

涉密政策要求

- 《武器装备科研生产单位一级保密资格标准》明确要求“因特殊工作需要，涉密网络与非涉密网络、工业控制系统连接实时进行特定信息交换的，应当制定专门的安全保密方案报国家保密行政管理部门审查。”
- 《武器装备科研生产单位一级保密资格评分标准》第125条规定：测试、调试、仿真、工控、数控等专用信息设备或者信息系统，接入涉密信息系统未制定专门的安全保密方案并报国家保密行政管理部门审查的，扣10分的。第159条规定：测试、调试、仿真、工控、数控等专用信息设备或者信息系统，未明确涉密等级和保护要求的，或者未采取相应安全控制措施的，扣2分。

国家及行业政策要求

- 国务院《关于印发工业转型升级规划（2011—2015年）的通知》国发〔2011〕47号,要求...推进信息化与工业化深度融合...
- 2015年5月8日，国务院正式发布《中国制造2025》规划，要求推进信息化与工业深度融合，把智能制造作为两化深度融合的主攻方向...加强智能制造工业控制系统网络安全保障能力建设，健全综合保障体系。
- 工业和信息化部 国家标准化管理委员会关于印发《国家智能制造标准体系建设指南（2015年版）》的通知指出：信息安全...包括软件安全、设备信息安全、网络信息安全、数据安全、信息安全防护等五个部分。
- 2016年5月13号，国务院发布《关于深化制造业与互联网融合发展的指导意见》（国发〔2016〕28号）。《意见》明确指出“以建设制造业与互联网融合'双创’平台为抓手，发展智能制造.....与互联网融合新模式，.....提高工业信息系统安全水平.....”

02

第二部分
DNC网络信息安全风险分析

安全风险分析　　安全建设现状分析　　安全建设必要性

DNC工控网络的安全现状

- 高精尖数控设备绝大多数依赖进口，无法进行自主维护，依赖国外厂商；
- DNC工控控制网络防护建设不够完善，仅通过传统防火墙、防病毒软件等进行防护；

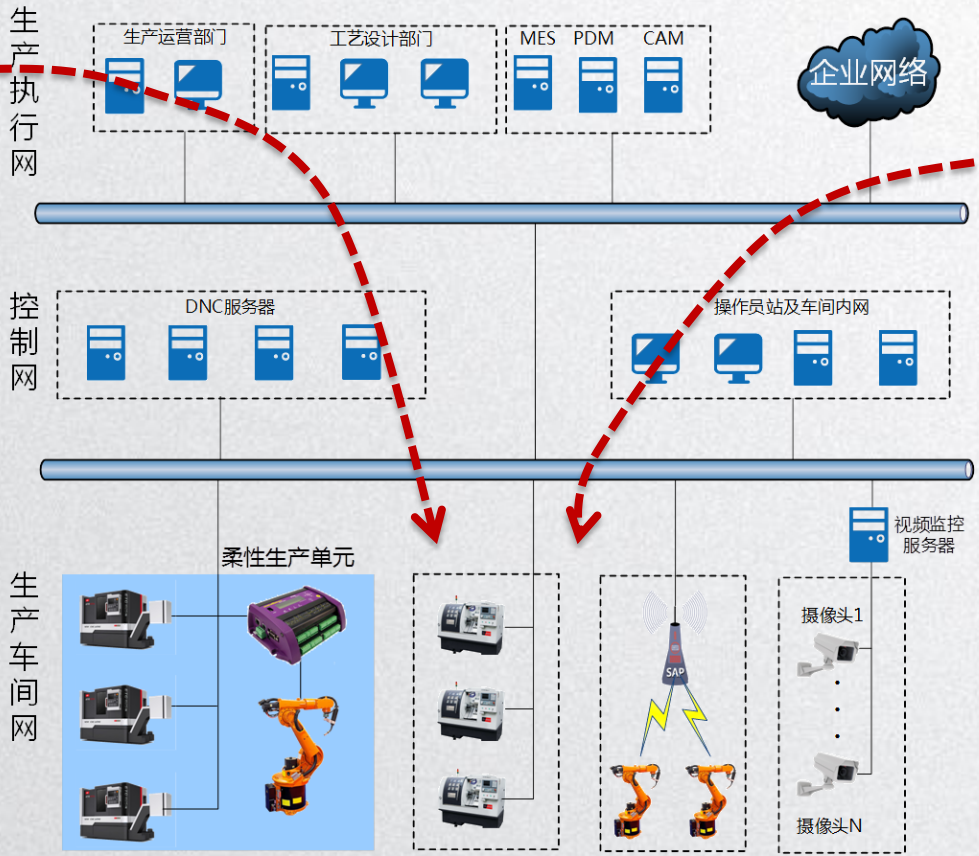
- 缺乏对信息安全问题的高度重视，对企业核心技术知识和国家机密的信息安全风险并未有足够的认识；
- 国务院、工信部、国家保密局、国防科工局、总装备部对数控系统与管理网络的链接进行了严格规定。

智能制造工控网络入侵途径分析

WIFI无线连接

远程维护通道

手机等智能终端



企业办公网

USB移动存储介质

心怀不满的恶意员工

智能制造工控网络的安全风险分析

- DNC服务器、客户端等大部分是Windows系统，使用传统的数据库，系统老旧且不更新补丁，存在很大安全隐患；
- 数控机床所使用通讯协议存在安全上的设计缺陷，漏洞较多；
- 数控专用工控操作系统无适配的杀毒软件；
- 使用外来数据传输介质进行NC程序传输，无技术监控手段，管理难度大，危及设备安全；
- 数控设备或系统在业务指令发生异常时无法及时发现；
- 维修用数字设备在无安全监督或未经安全监测的情况下接入数控设备，带来潜在安全隐患；
- 来自管理网的病毒和攻击行为影响DNC系统；
- DNC系统大量使用无线网络进行生产活动，无线非法接入、篡改、伪造等行为可能会造成生产中断、效率降低、良品率下降等。

03

第三部分
智能制造工控安全防护解决方案

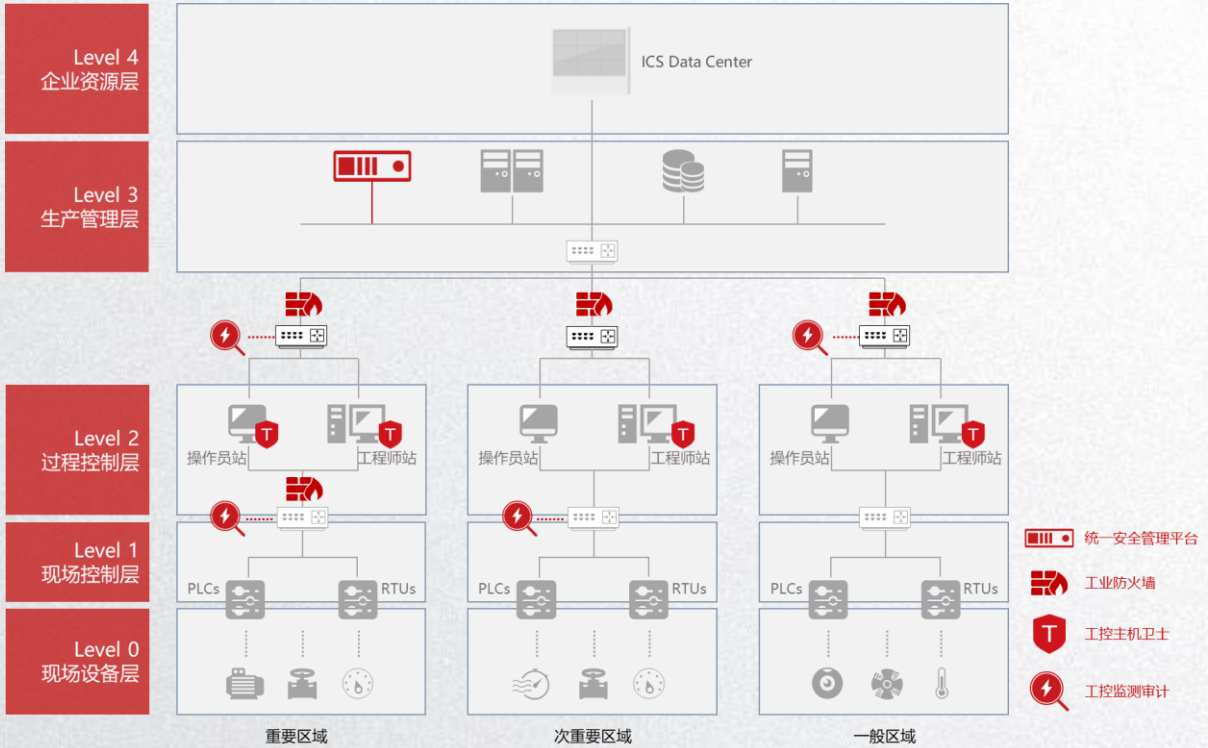
方案理念　设计依据　等级保护要求　安全解决方案设计　行业案例说明

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

技术亮点及创新点

- 从“黑”到“白”
- 从“被动防御”到“主动防护”

设计依据

DNC网络工控安全解决方案设计依据

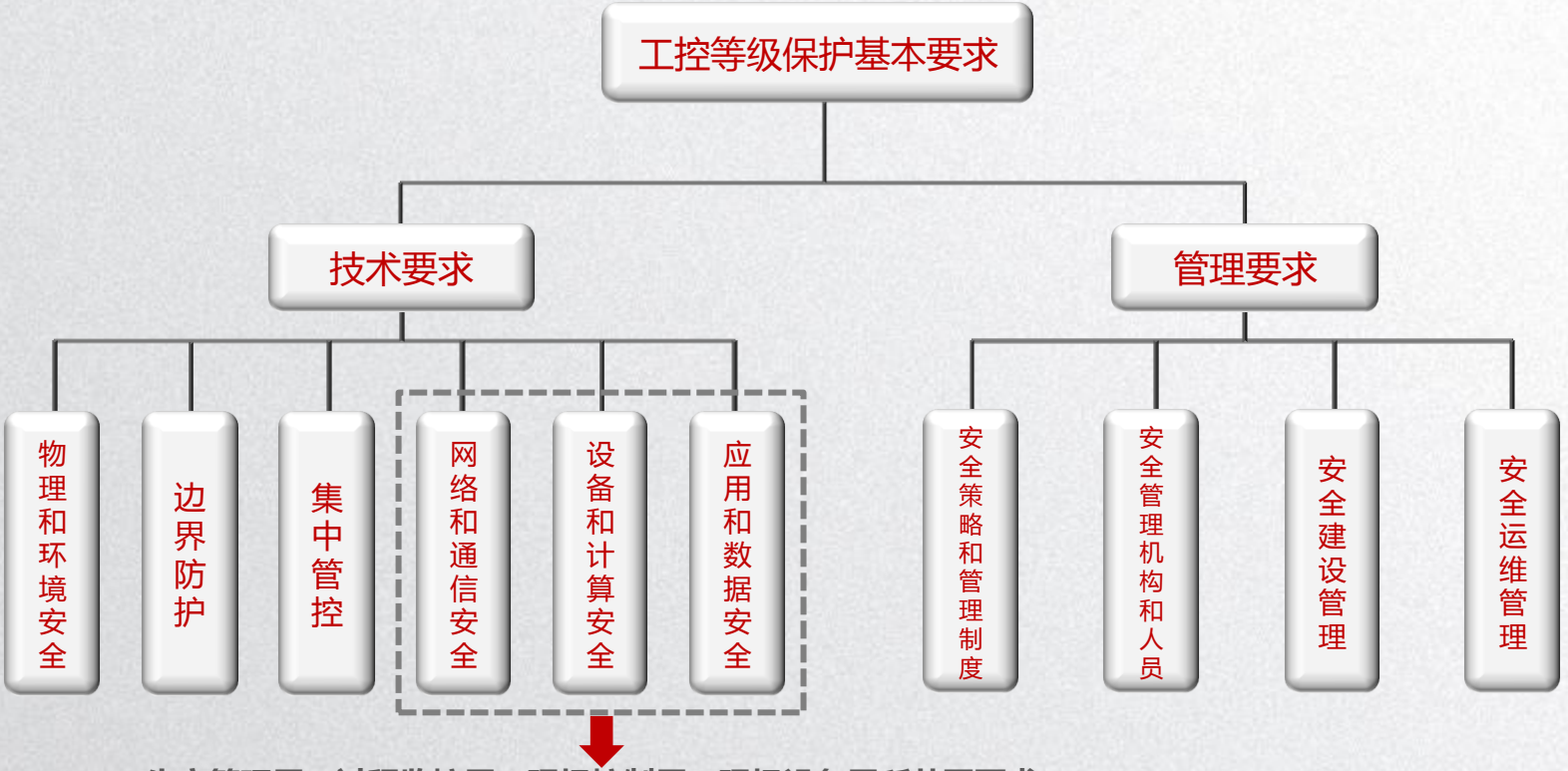
- 《工业控制系统信息安全防护指南》
- 《GB / T26333-2010 工业控制网络安全风险评估规范》
- 《信息安全技术 网络安全等级保护基本要求 第5部分：工业控制系统安全扩展要求》
- 信息安全技术 网络安全等级保护测评要求 第5部分 工控安全扩展要求
- 信息安全技术 网络安全等级保护安全设计技术要求 第5部分：工业控制安全要求

本方案重点解决以上政策标准中的核心问题

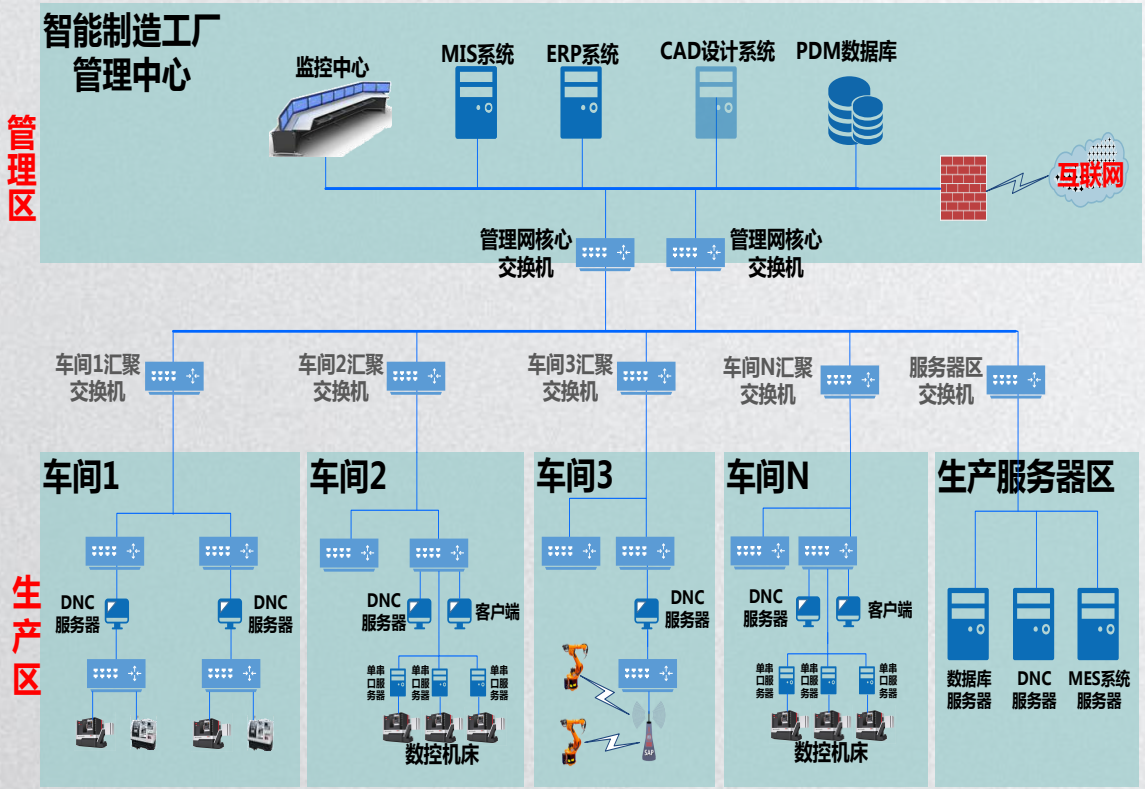
等级保护介绍

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
管理要求
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
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

DNC系统网络架构



DNC系统网络架构介绍

系统层级自下而上共五层，分别为设备层、控制层、车间层、企业层和协同层。具体包括：

- 设备层级包括传感器、仪器仪表、条码、射频识别、机器、机械和装置等，是企业进行生产活动的物质技术基础；
- 控制层级包括可编程逻辑控制器（PLC）、数据采集与监视控制系统（SCADA）、分布式控制系统（DCS）和现场总线控制系统（FCS）等；
- 车间层级实现面向工厂/车间的生产管理，包括制造执行系统（MES）等；
- 企业层级实现面向企业的经营管理，包括企业资源计划系统（ERP）、产品生命周期管理（PLM）、供应链管理系统（SCM）和客户关系管理系统（CRM）等；
- 协同层级由产业链上不同企业通过互联网络共享信息实现协同研发、智能生产、精准物流和智能服务等。

方案设计之边界防护&网络和通信安全

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**	

方案设计之网络和通信安全

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；

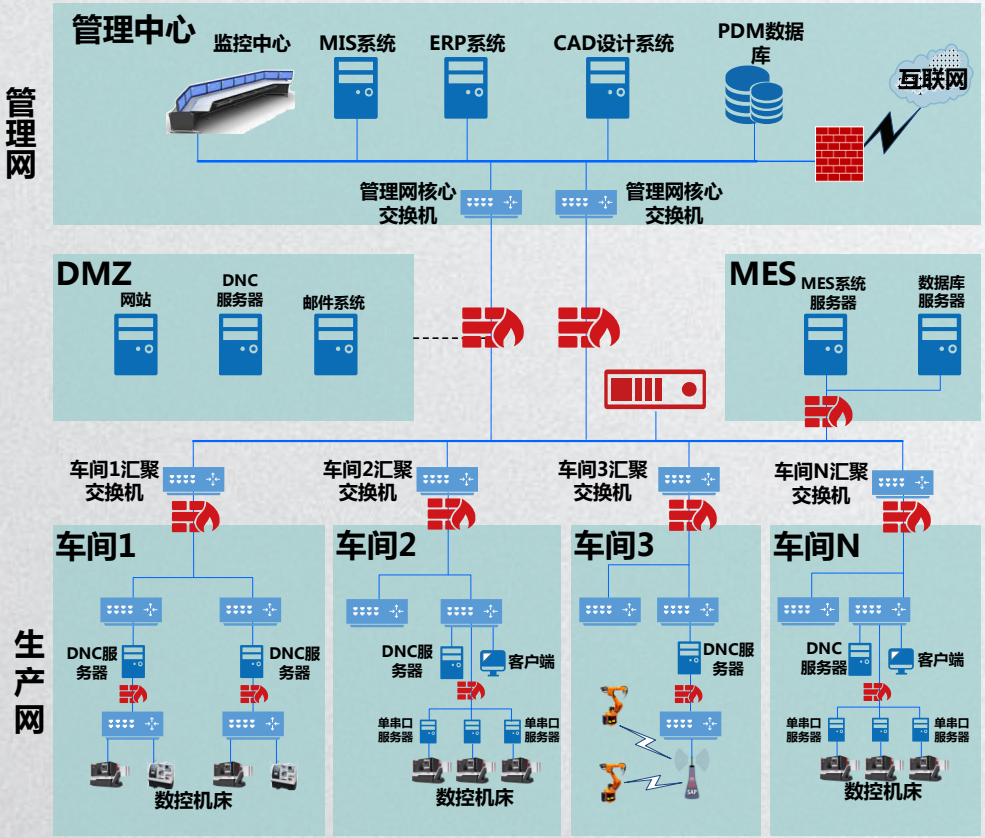
方案设计之网络和通信安全

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。

方案设计之网络和通信安全

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	7.1.6　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。

结构调整&边界防护&访问控制



解决方案

■ 构建DMZ区

中国制造2025要求发挥互联网聚集优化各类要素资源的优势，构建开放式生产组织体系，大力发展**个性化定制、服务型制造**等新模式，需通过互联网访问DNC系统实现个性化生产定制，在数控网与管理网之间部署防火墙，构建DMZ区实现数控网与办公网的安全逻辑隔离。

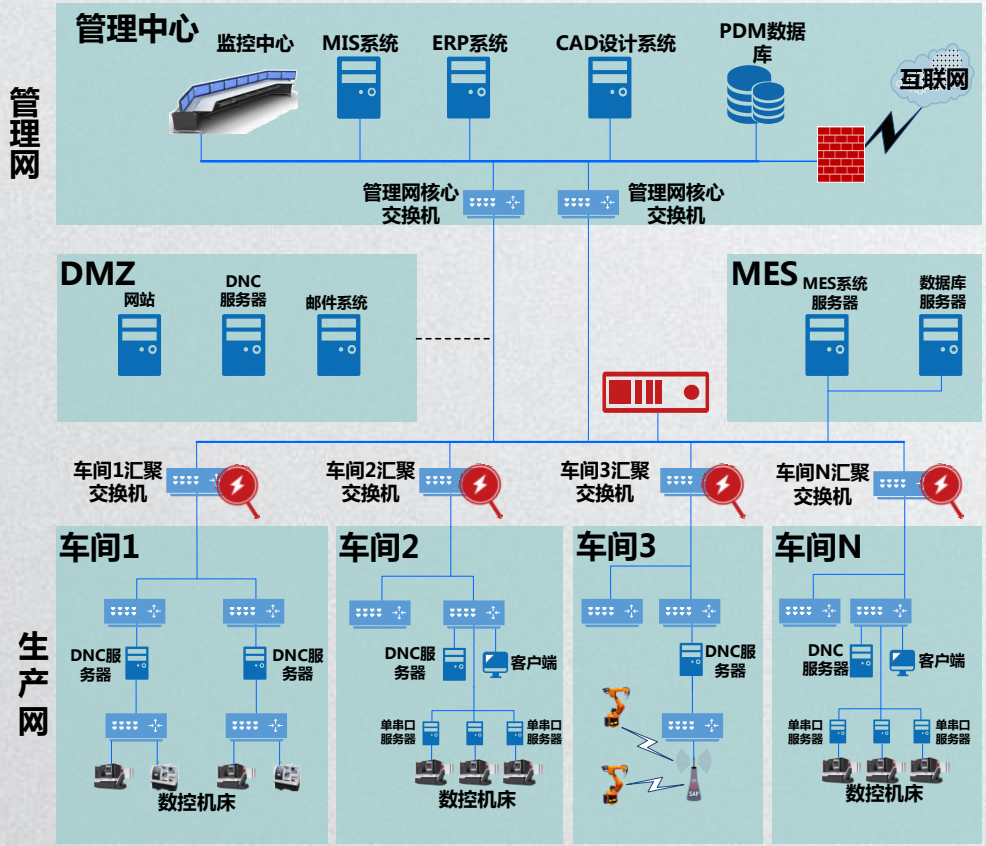
■ **访问控制**

1）部署在生产网与管理网之间，防范外部攻击；

2）部署在各车间出口位置，阻止不同车间及工艺流程之间的越权访问行为；

3）部署在各数控机床、机械臂前端，对关键控制指令或参数进行保护，防止误操作或恶意行为。

监测审计



解决方案

■ **解决方案**

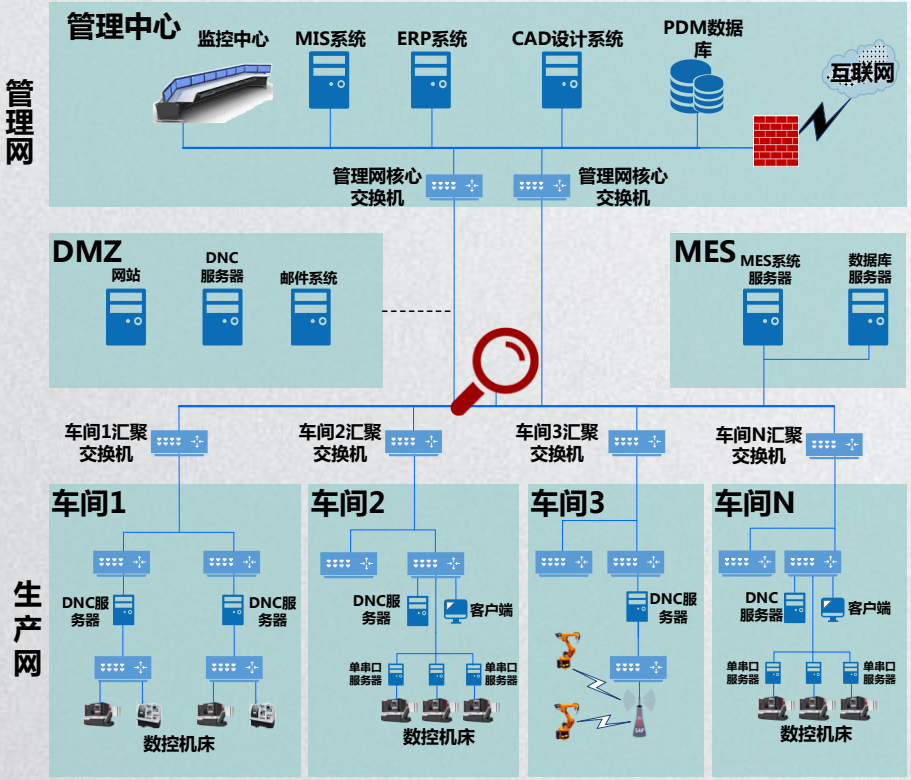
在车间汇聚交换机上旁路部署监测审计系统；

■ **解决的问题**

1）实时检测DNC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。

入侵检测



解决方案

■ 解决方案

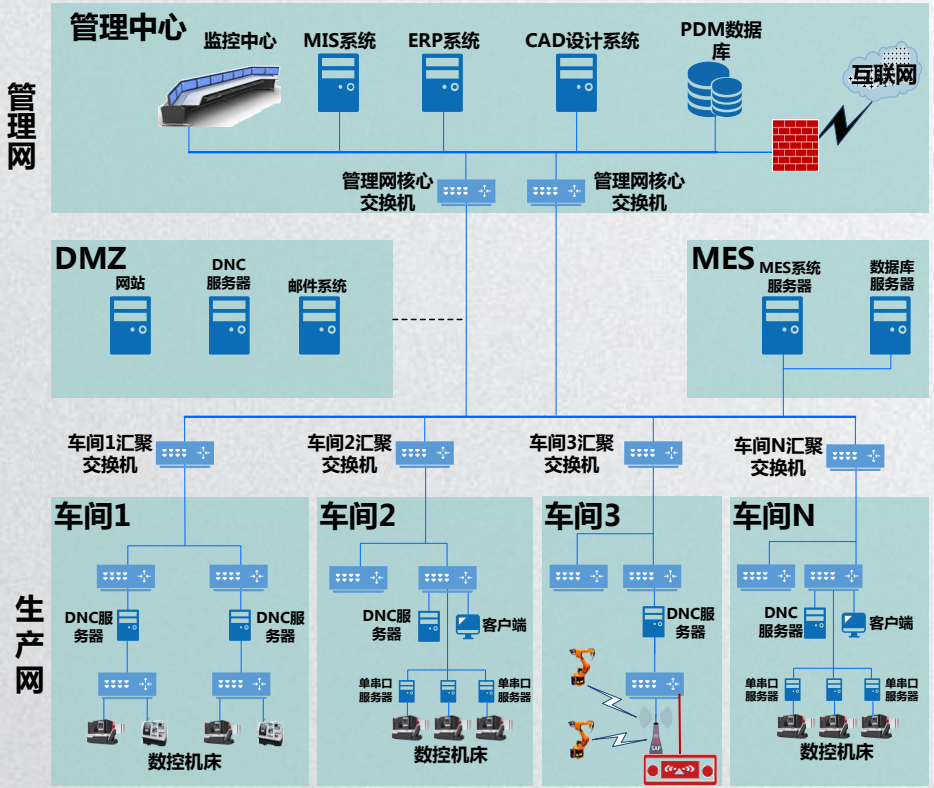
在核心交换机上旁路入侵检测系统，实时检测可能存在的恶意攻击行为；

■ 解决的问题

1）实时检测来自管理网、互联网和各个车间的恶意行为，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）通过网络入侵检测系统，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。

无线使用控制



解决方案

■ **解决方案**

1）在无线局域网内部署无线安全防护系统；

■ **解决的问题**

为DNC网络提供安全的无线生产网络同时，扫除潜在的车间生产信号干扰风险，使生产运行更加可靠，为构建高安全的DNC网络生产环境打下了坚实基础。

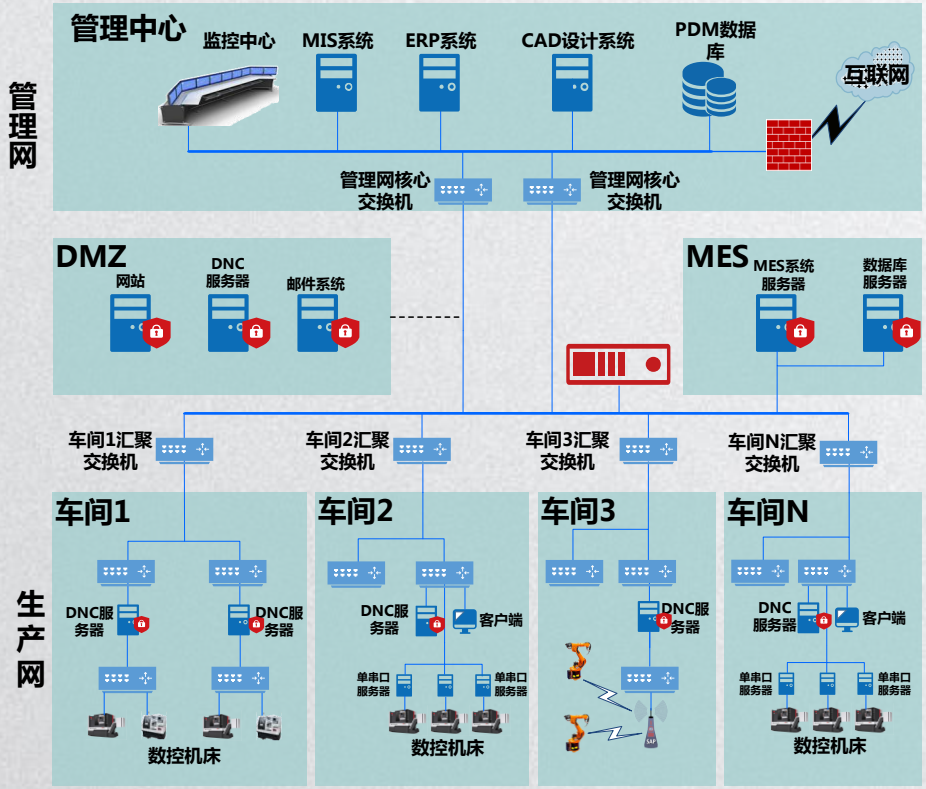
方案设计之设备和计算安全

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 设备和计算安全	**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；
		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。
	7.1.6 现场控制层安全要求 7.1.6.2 设备和计算安全	**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；
		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；
		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。

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 设备和计算安全	**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。
		7.1.5.2.5 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。

主机加固



解决方案

■ 解决方案

在各车间的DNC客户端、服务器及MES服务器、数据库服务器和单串口服务器部署主机加固类软件；

■ 解决的问题

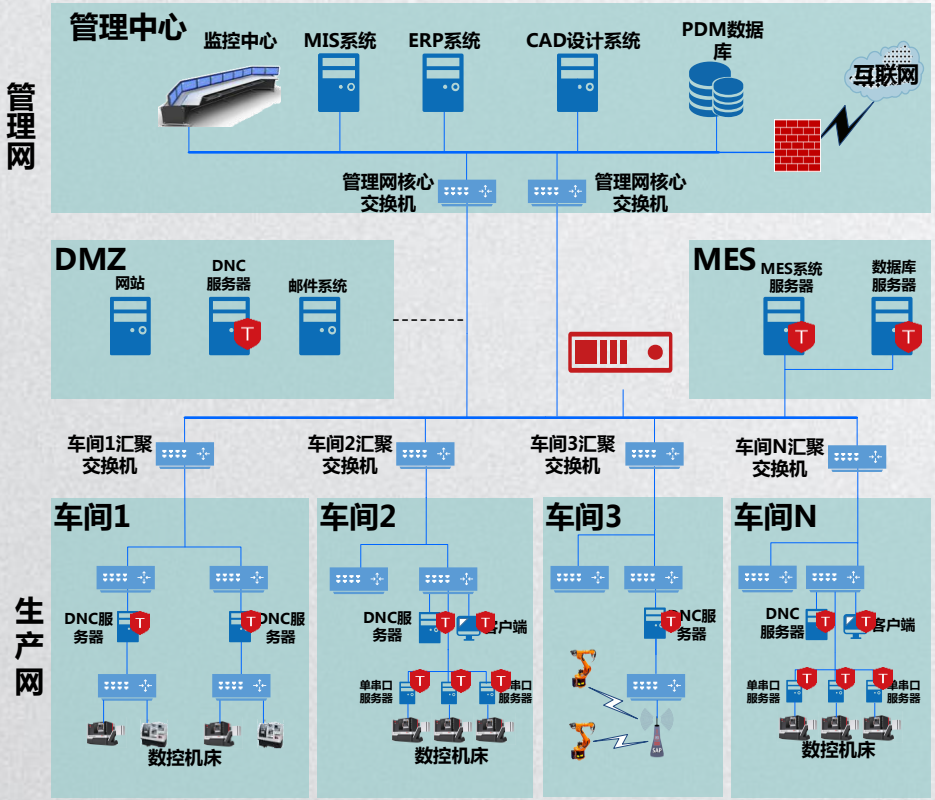
1）阻止非授权软件或进程的安装和运行，防止恶意代码攻击；

2）避免升级病毒库及漏洞库，变被动为主动；

3）防止使用移动介质拷贝NC程序过程中带入病毒在数控网中扩散；

4）杜绝信息被非法窃取。

主机安全防护



解决方案

■ 解决方案

在各车间的DNC客户端、服务器及MES服务器、数据库服务器和单串口服务器上部署工控主机安全防护类软件；

■ 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；

2）避免升级病毒库及漏洞库，变被动为主动；

3）防止使用移动介质拷贝NC程序过程中带入病毒在数控网中扩散；

4）杜绝信息被非法窃取。

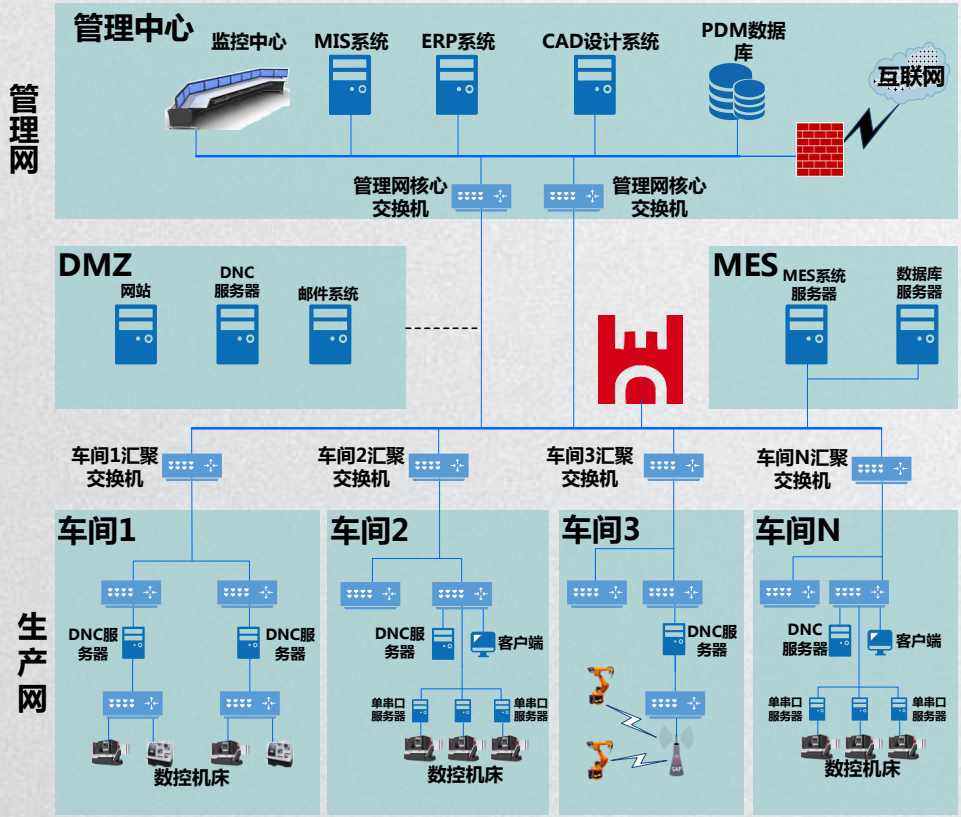
方案设计之应用和数据安全

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	7.1.5 过程监控层安全要求 7.1.5.3 应用和数据安全	7.1.5.3.2 身份鉴别 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； 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……； 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；
		7.1.5.3.3 访问控制 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； b) 应支持统一账户管理； 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； 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； 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；
		7.1.5.3.4 安全审计 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； d) 应具备以可配置频率的，与系统时钟同步的能力； f) 授权人员和/或工具应使用只读方式访问审计日志；

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。

运维安全审计



解决方案

■ **解决方案**

在生产网交换机上旁路部署运维安全管理系统；

■ **解决的问题**

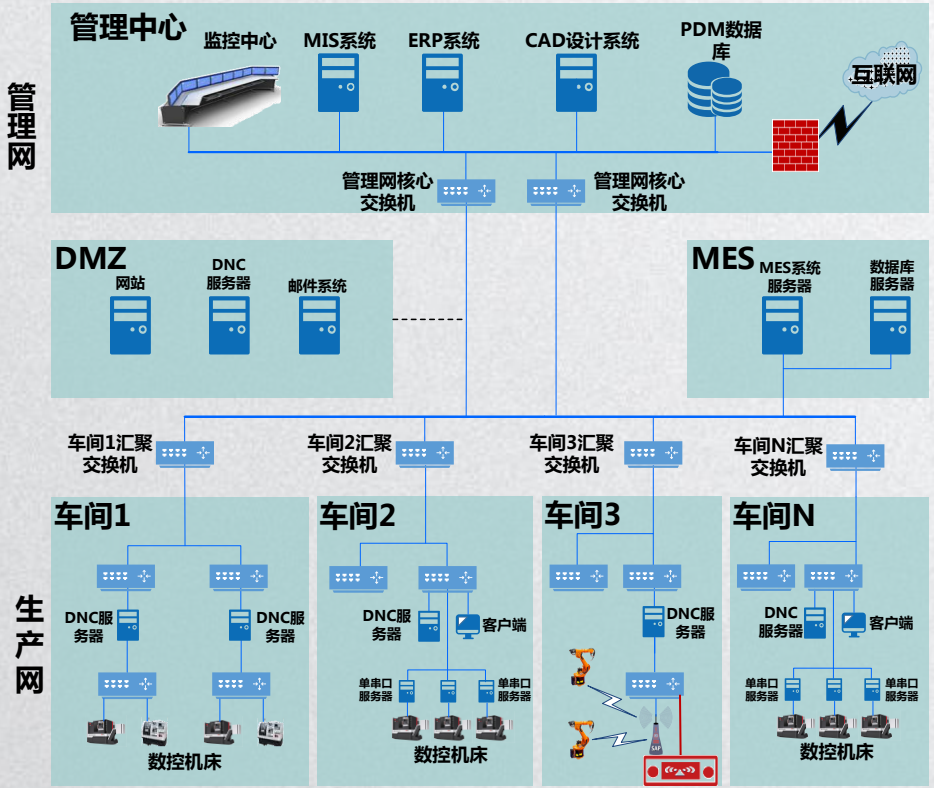
1）阻止非授权用户访问网络、安全设备；

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**

1）在无线局域网内部署无线安全防护系统；

■ **解决的问题**

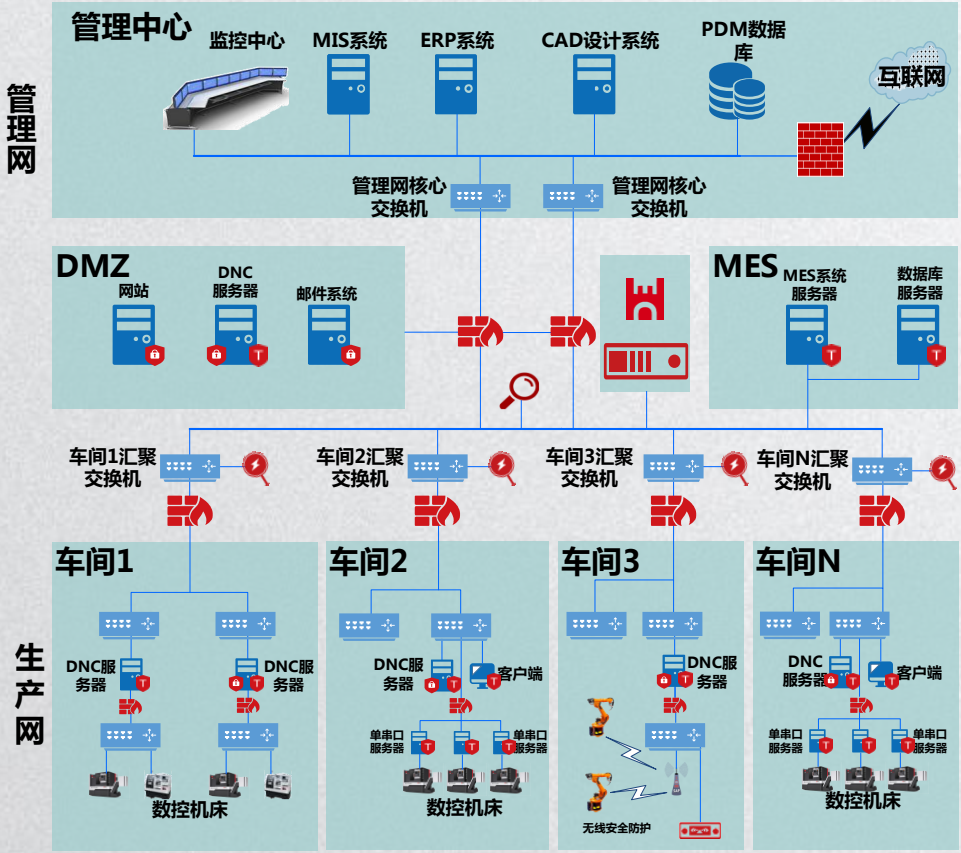
1）对车间内每个无线用户进行唯一性标识，防止非法用户的访问；

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
《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。

统一管理



解决方案

■ 解决方案

1）在生产网交换机上旁路部署集中安全管理系统；

■ 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。

典型案例—某汽车集团有限公司

客户需求

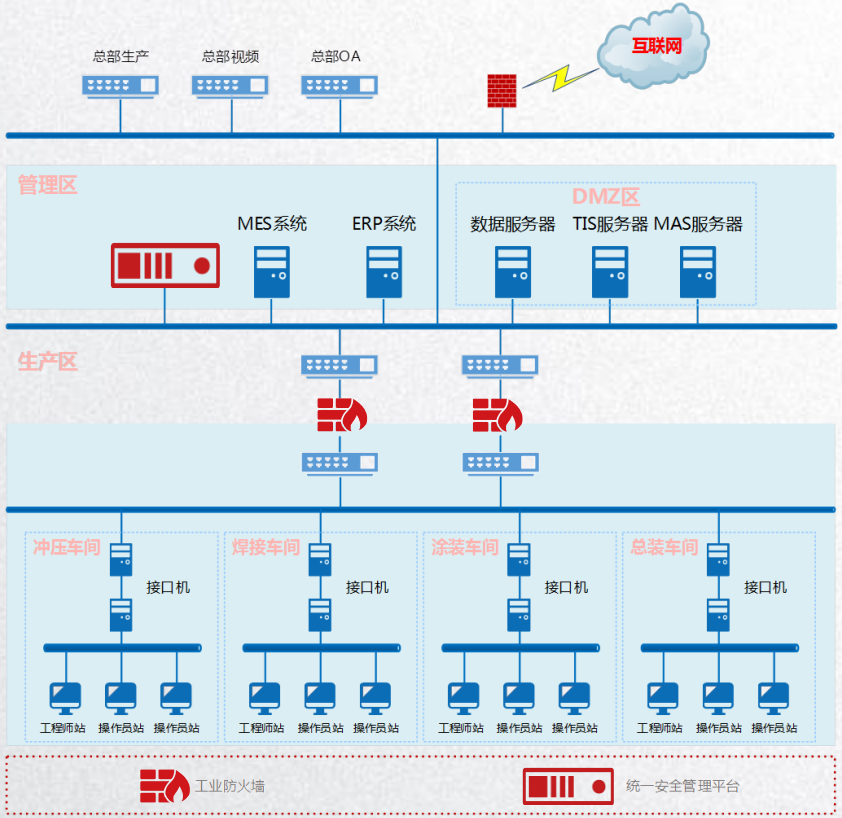
- 管理网络与生产网络之间、生产网络生产区与控制区之间、各生产区域之间缺乏必要的隔离控制措施，迫切需要对其进行安全防护；
- 保护工程师站、操作员站等主机免遭病毒、蠕虫、木马等恶意软件入侵；
- 采用技术手段实现对工业网络中的恶意攻击行为、误操作行为等的实时检测和记录。

解决方案

- 在管理网核心交换机和生产网核心交换机之间部署工业防火墙，A网B网冷备，与原有传统防火墙组成全面的边界安全隔离措施，完善网络边界的安全防护；
- 在虚拟服务器与生产服务器之间部署工业防火墙，对生产服务器设置对外只读控制策略，防止生产服务器数据被恶意篡改。

客户价值

- 满足国家政策法规要求及自身安全需求；
- 增强了企业自身信息安全防护能力，降低生产安全风险；
- 提升了企业的精益化管理水平。



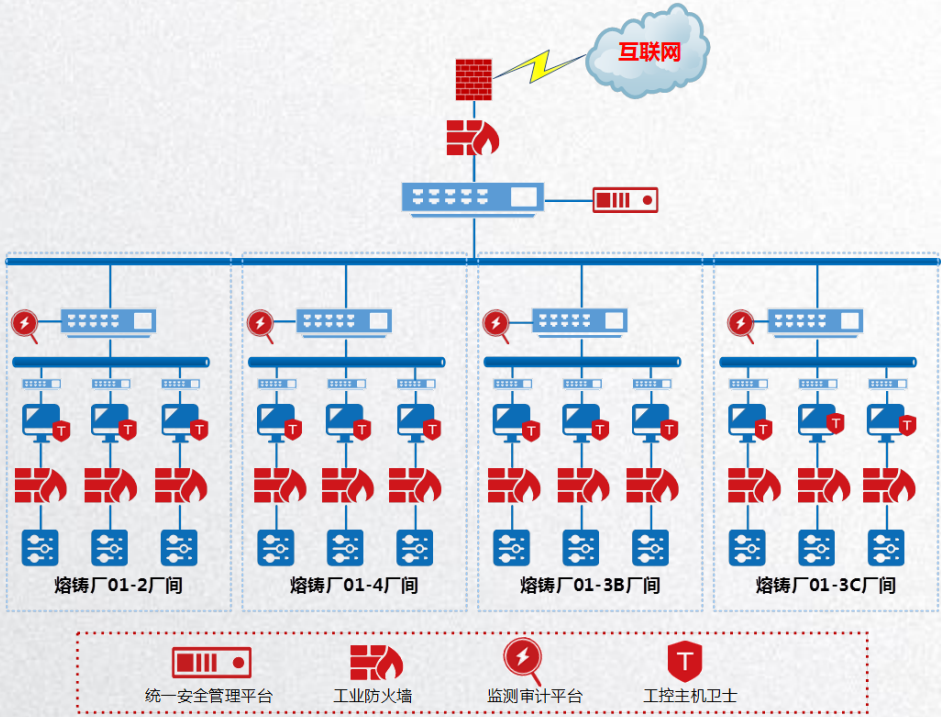
典型案例—某集团有限公司

客户需求

- 进行有效的区域划分及安全访问控制；
- 解决系统及设备漏洞难以及时处理、工业控制协议先天安全性不足等的安全隐患问题；
- 解决缺乏安全审计手段的问题；
- 通过技术手段防范因安全政策、管理制度执行力度不够以及人员安全意识缺乏导致的安全隐患。

解决方案

- 在生产网边界和内部区域部署工业防火墙，阻止任何来自安全区域外的非授权访问；
- 在操作站、服务器上部署基于白名单机制的主机安全加固软件，有效防止病毒感染及U盘滥用导致的安全问题；
- 在生产车间的各区域网络旁路部署监测审计平台，实时发现针对PLC、DCS等重要工业控制设备或系统的攻击破坏行为，为工业控制网络安全事件调查提供依据。



客户价值

- 提高了企业安全防护能力，降低了核心数据被窃取的风险；
- 全面提升了业务人员的安全意识，提高了安全管理水平和效率；
- 协助企业完善工控安全防护体系，巩固了行业标杆地位，形成了良好的示范效应。

04

第四部分

方案合规性分析

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
《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...	**符合**。在过程监控层核心交换机上部署监测审计类系统，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。	监测审计系统
		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；		

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
《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；	**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。	入侵检测系统 工业防火墙
	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。		

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	**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。	**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
		7.1.5.2.5 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
《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	**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；	**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。	主机加固系统
		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。		
	7.1.6 现场控制层安全要求 7.1.6.2 设备和计算安全	**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；		
		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；		

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	**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；	**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。	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	工控漏扫扫描产品 工控漏洞挖掘产品

方案合规性分析 运维审计

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 7.1.5.3 应用和数据安全	7.1.5.3.2 身份鉴别 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； 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……； 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；	**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。	运维堡垒机
		7.1.5.3.3 访问控制 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； b) 应支持统一账户管理； 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； 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； 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；		
		7.1.5.3.4 安全审计 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； d) 应具备以可配置频率的，与系统时钟同步的能力； f) 授权人员和/或工具应使用只读方式访问审计日志；		

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	（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。	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
		（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。		
	三、 边界安全防护	（一）分离工业控制系统的开发、测试和生产环境。	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
		（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。	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。	符合。采用运维安全审计系统、日志审计系统等实现访问日志的全面记录，便于事后追踪回溯。	

05

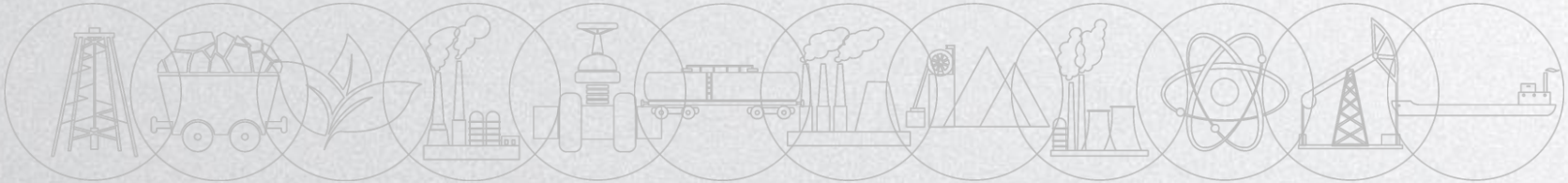
第五部分
公司与产品服务介绍

公司简介　安全事记　一点成绩　产品与案例

公司简介

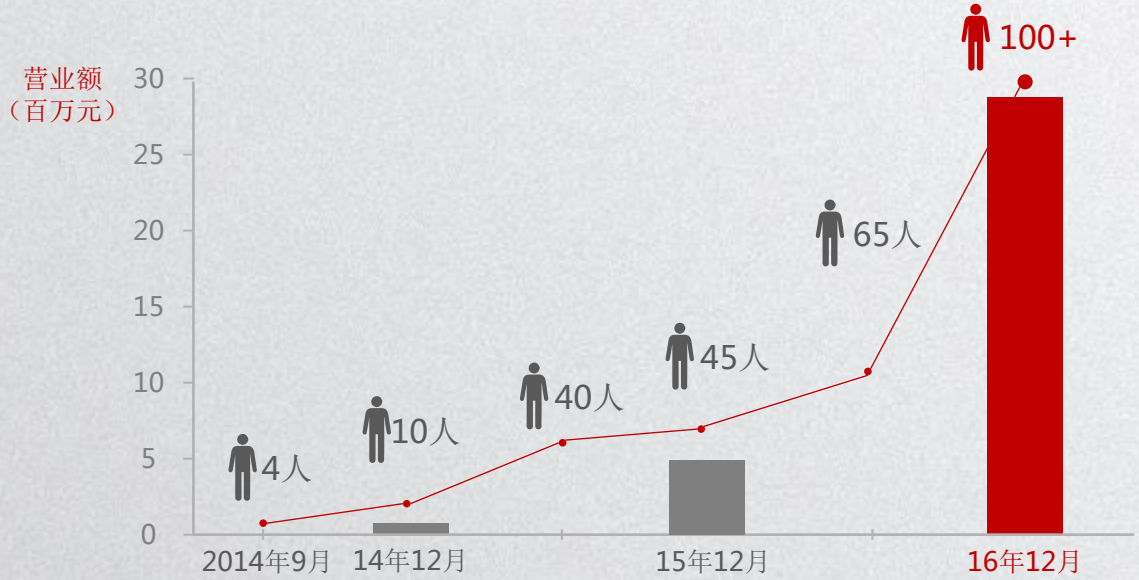
威努特
WINICSSEC

- 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

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

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

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

保障
关键信息基础
设施的运行安全

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

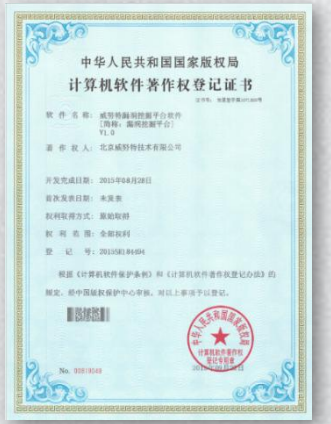
信息安全等级保护安全
建设服务机构能力评估

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20款
- 发明专利11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

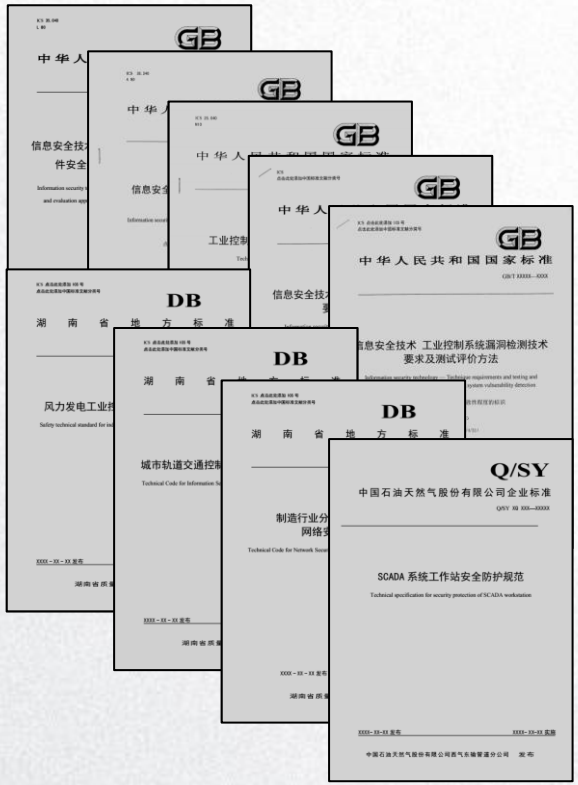
- **湖南省地方标准 《城市轨道交通控制系统信息安全技术规范信息安全技术》**
- **湖南省地方标准 《风力发电工业控制系统安全技术标准》**
- **湖南省地方标准 《制造行业分布式控制系统DNC网络安全技术规范》**

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

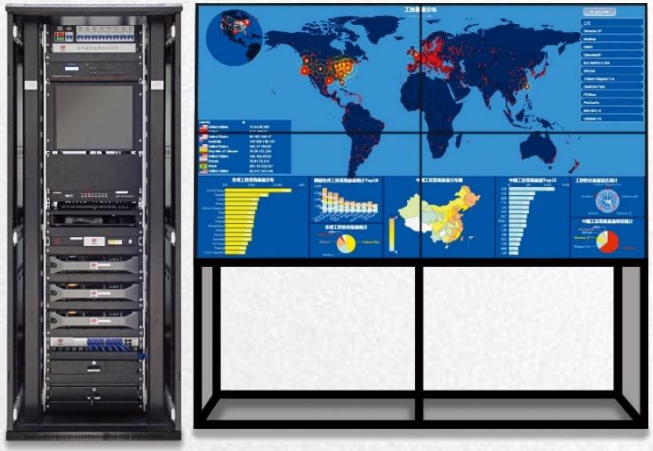
专注工控 · 捍卫安全

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

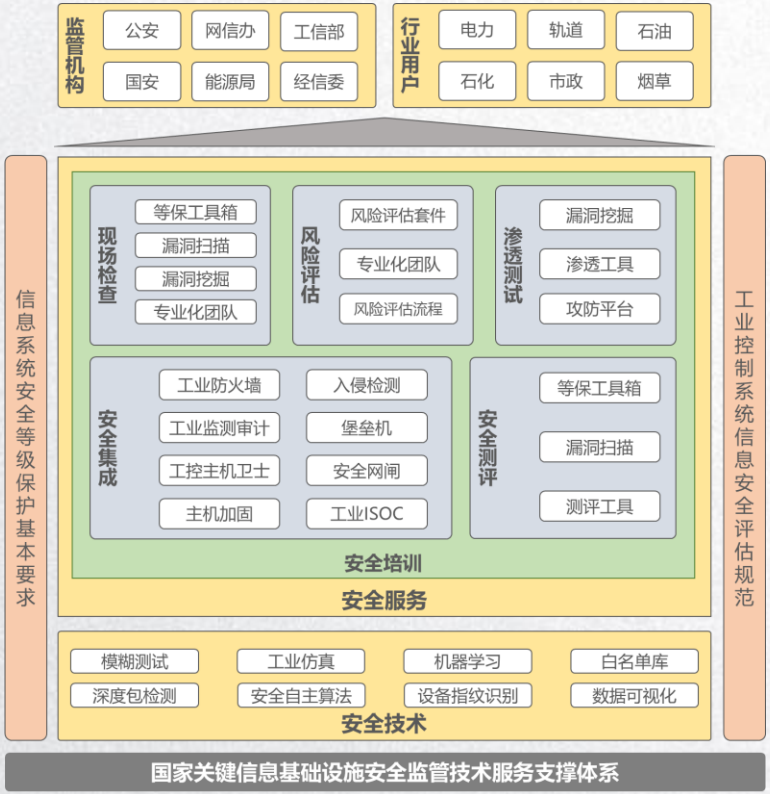
- 识别工控安全风险
- 工控渗透服务
- 制定标准/制度/流程

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

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
……

专注工控·捍卫安全