



---

# 新疆油田工控安全实践与启示

---



## 一、概述

## 二、工控安全建设

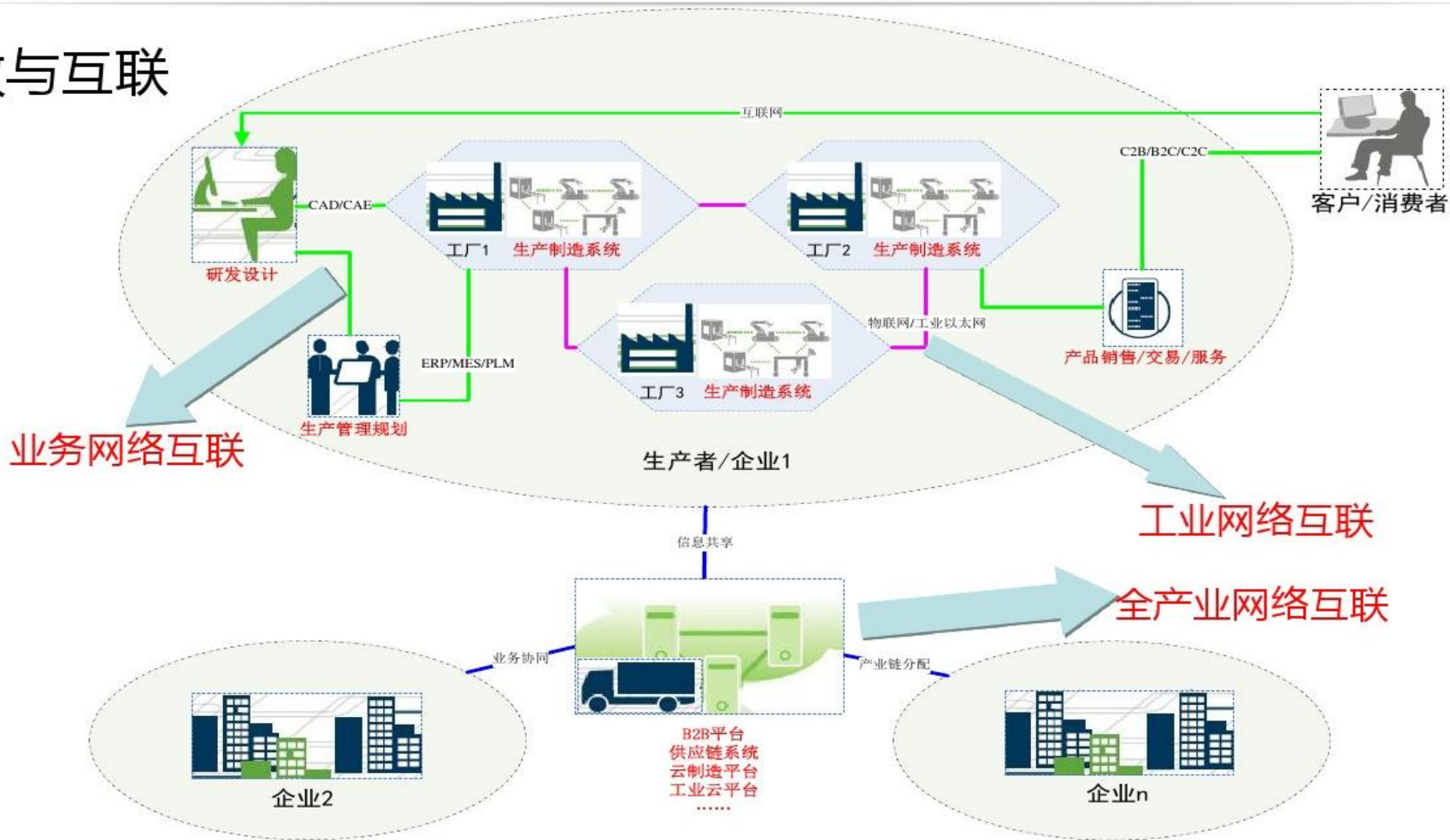
## 三、启示



# 工业互联网发展

## 工业互联网的发展与应用

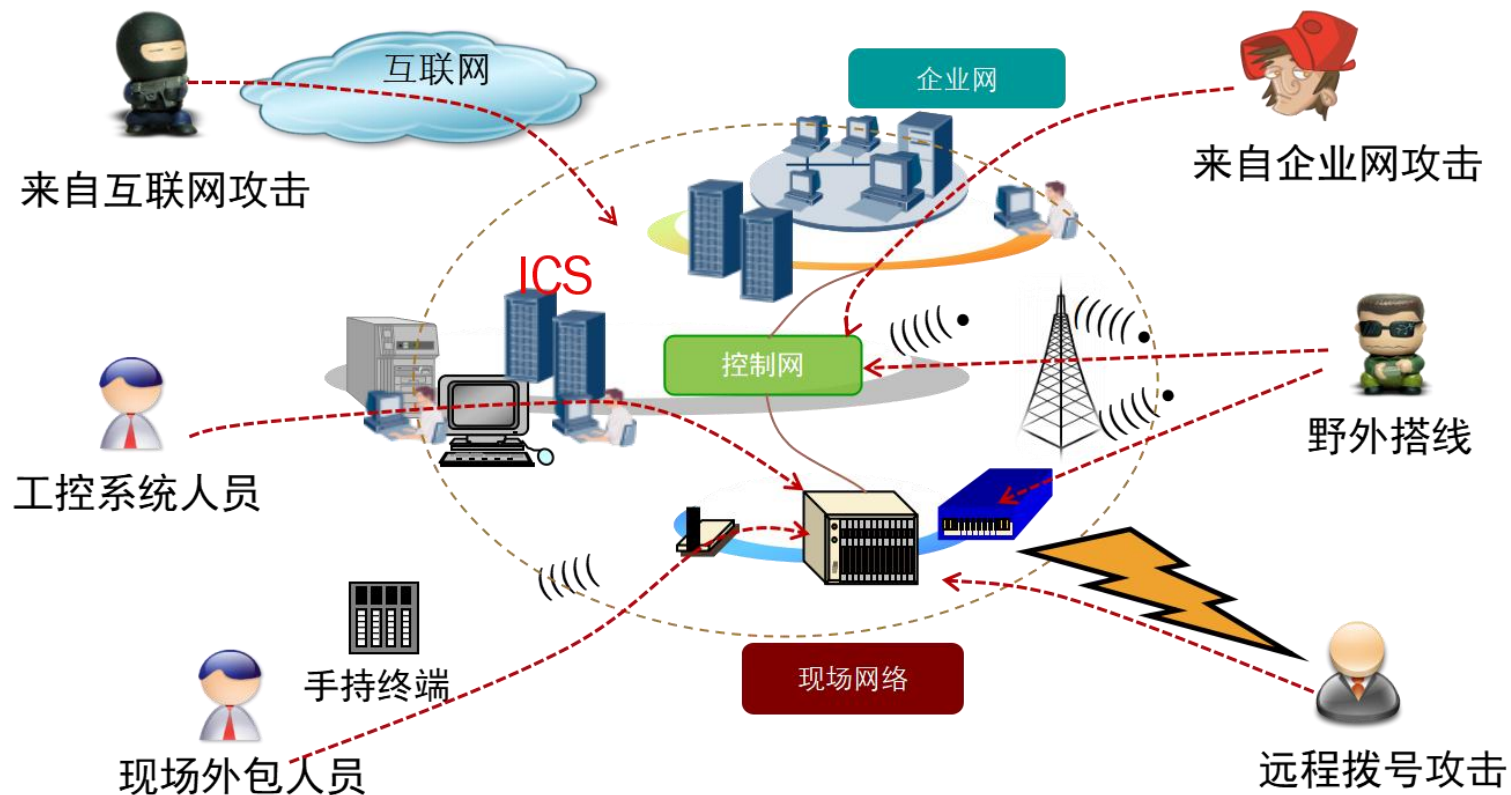
### ● 开放与互联





# 工业互联网安全挑战

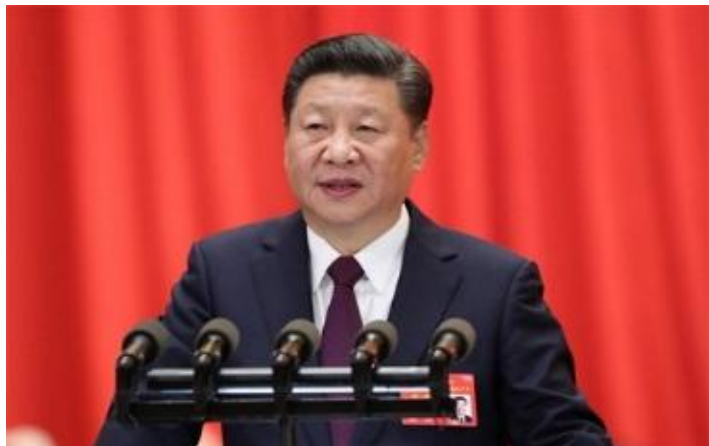
工业控制系统主要考虑高可靠性、实时性、精确性，普遍运行在较为独立封闭的生产环境。在互联、开放、智能发展的今天，移动应用、云计算、大数据等新技术应用，使工业控制系统从封闭走向了开放，就会受到来自各方面的威胁。



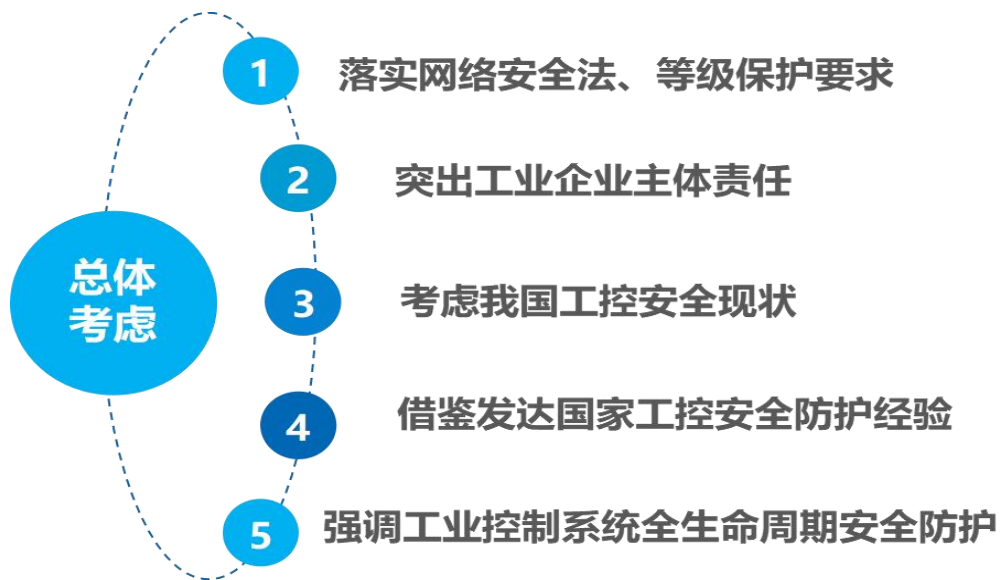


# 总体国家安全观要求

近年来国内外基于商业和政治目的，对工业控制领域发起的网络攻击事件层出不穷。随着我国工业数字化、网络化、智能化加快发展，工控系统面临安全漏洞不断增多、安全威胁加速渗透、攻击手段复杂多样等新挑战。为防止石油生产工业控制系统网络受到大规模攻击行为，以及受到攻击时能够及时响应，快速处置，将风险和损失降至最低，为生产安全保驾护航，需要建立企业网络安全保障机制。



总书记强调“**坚持总体国家安全观**”，提出“**加快建设制造强国、网络强国**”。





## 一、概述

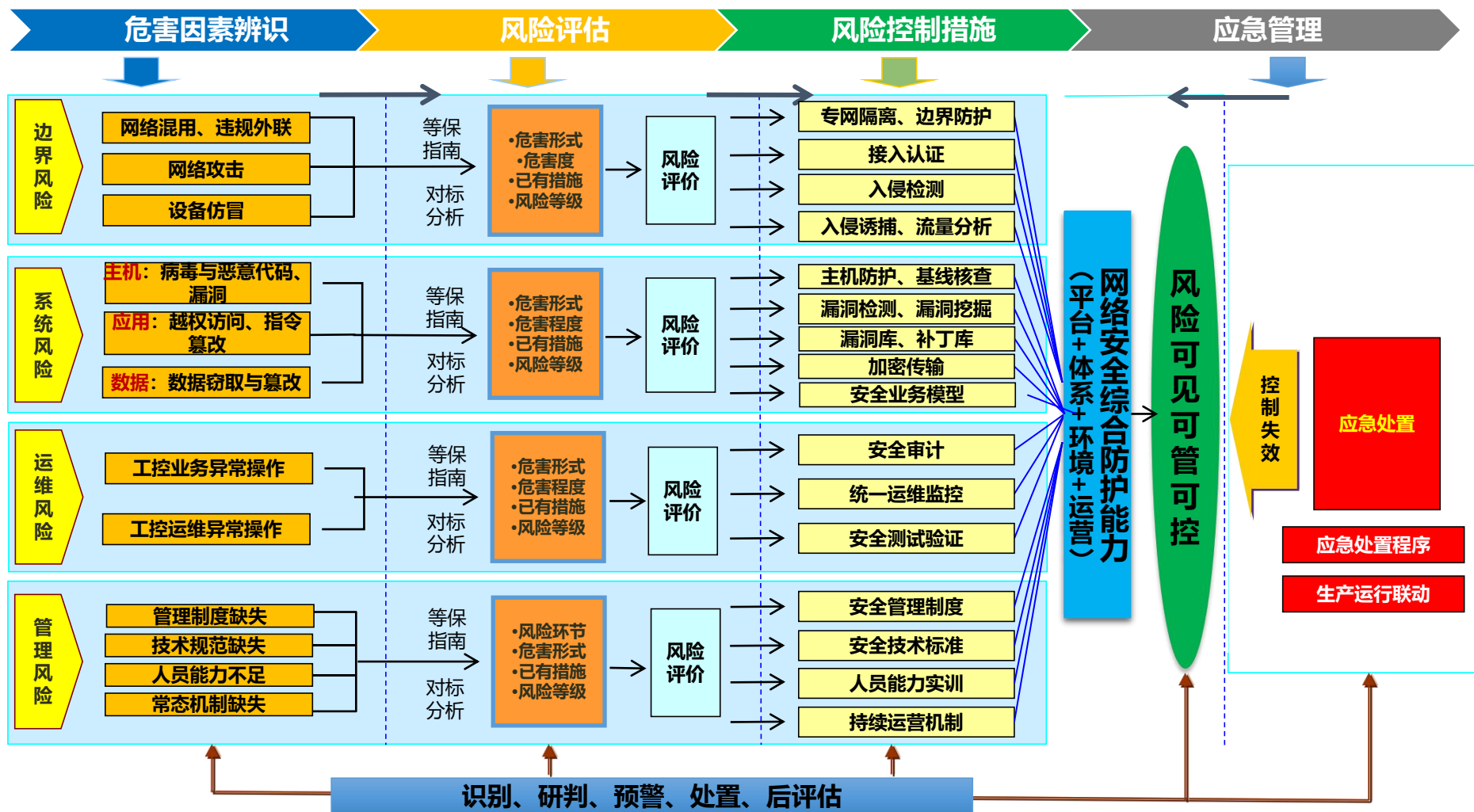
## 二、工控安全建设

## 三、启示



# 建设思路

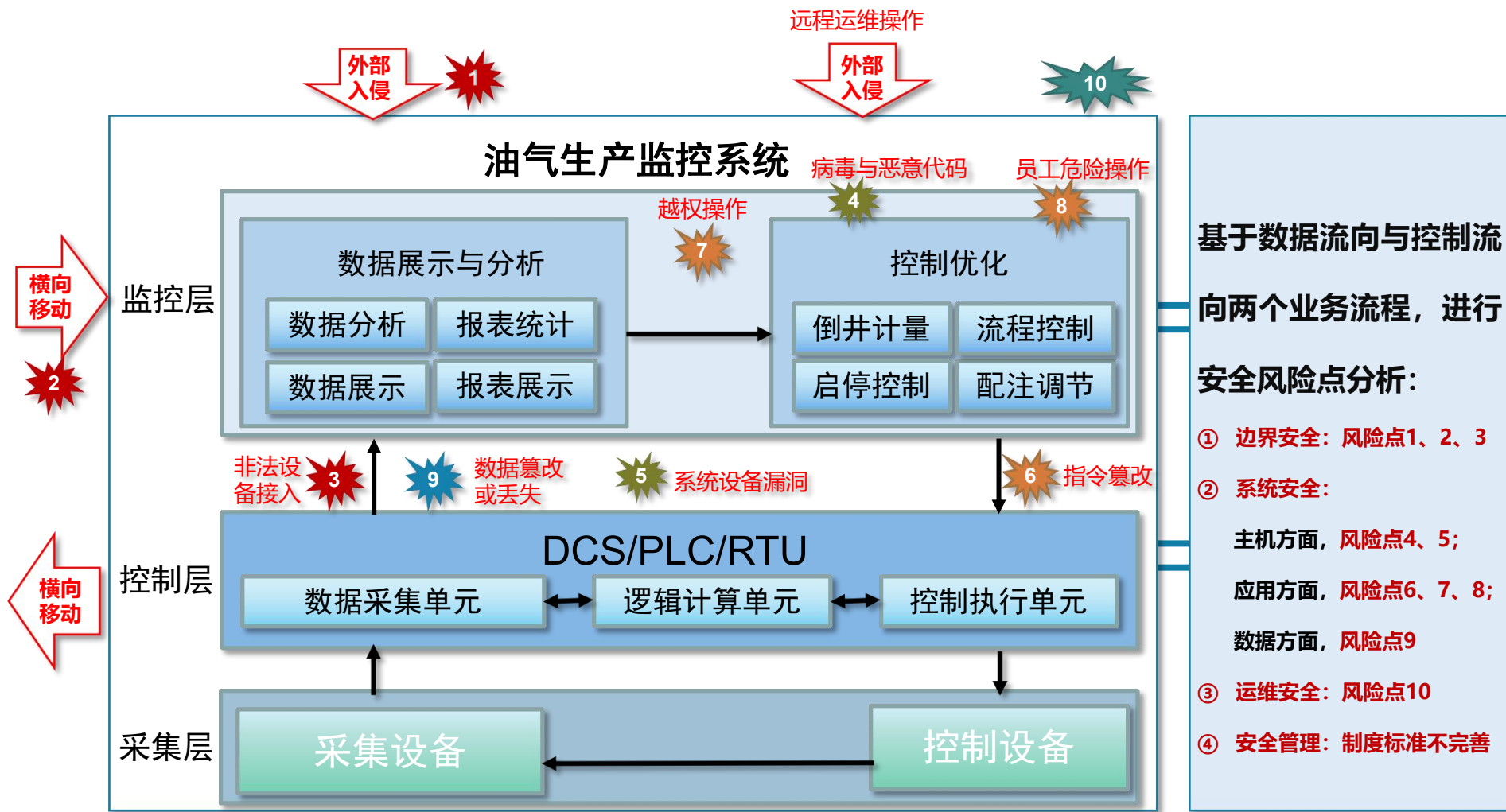
借鉴HSE工作思路，结合网络安全风险分析手段和管控工具，建立工控安全工作目标。





# 风险分析

## 业务流程及风险点分析







# 规划方案

**感**

**全面感知  
准确预警**

**感知生产异常**

感知设备接入  
感知资产信息  
感知漏洞信息  
感知安全风险  
感知安全威胁  
感知网络攻击

**控**

**纵深防御  
精准控制**

**保护工控核心**

纵深防御体系  
协同联动机制  
攻击自动阻断  
精准溯源定位  
阻止横向蔓延

**仿**

**业务仿真  
漏洞挖掘**

**业务场景仿真**

业务流程仿真  
关键操作仿真  
系统漏洞挖掘  
设备漏洞挖掘

**验**

**安全测试  
技术验证**

**防护能力验证**

安全策略验证  
设备安全检测  
安全方案验证  
处置流程验证  
技术能力培养  
新技术应用研究

**优**

**安全优化  
能力提升**

**提升安全能力**

优化防护方案  
优化安全策略  
优化网络结构  
优化应急流程  
提升防护能力  
提升处置能力



# 系统建设

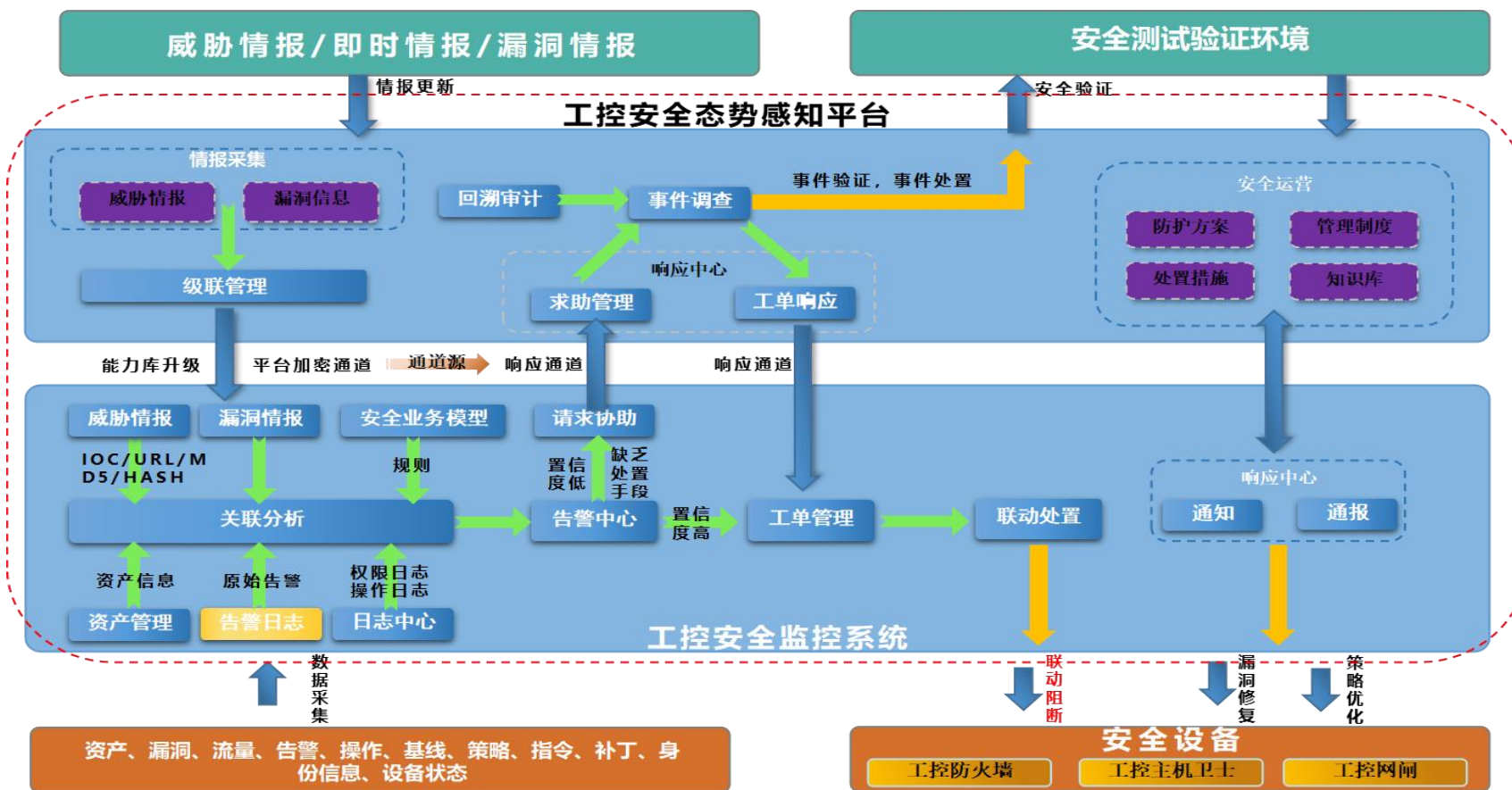
建成了基于“一平台、一体系、一环境”的工业控制系统网络安全技术防护屏障，形成了包括安全策略、管理办法、标准规范等在内的安全管理制度体系，创建了以风险评估、基线核查、攻防演练等为主要措施的安全运维机制，三者有机协同，确保生产工业控制系统安全平稳运行。





# 态势感知平台

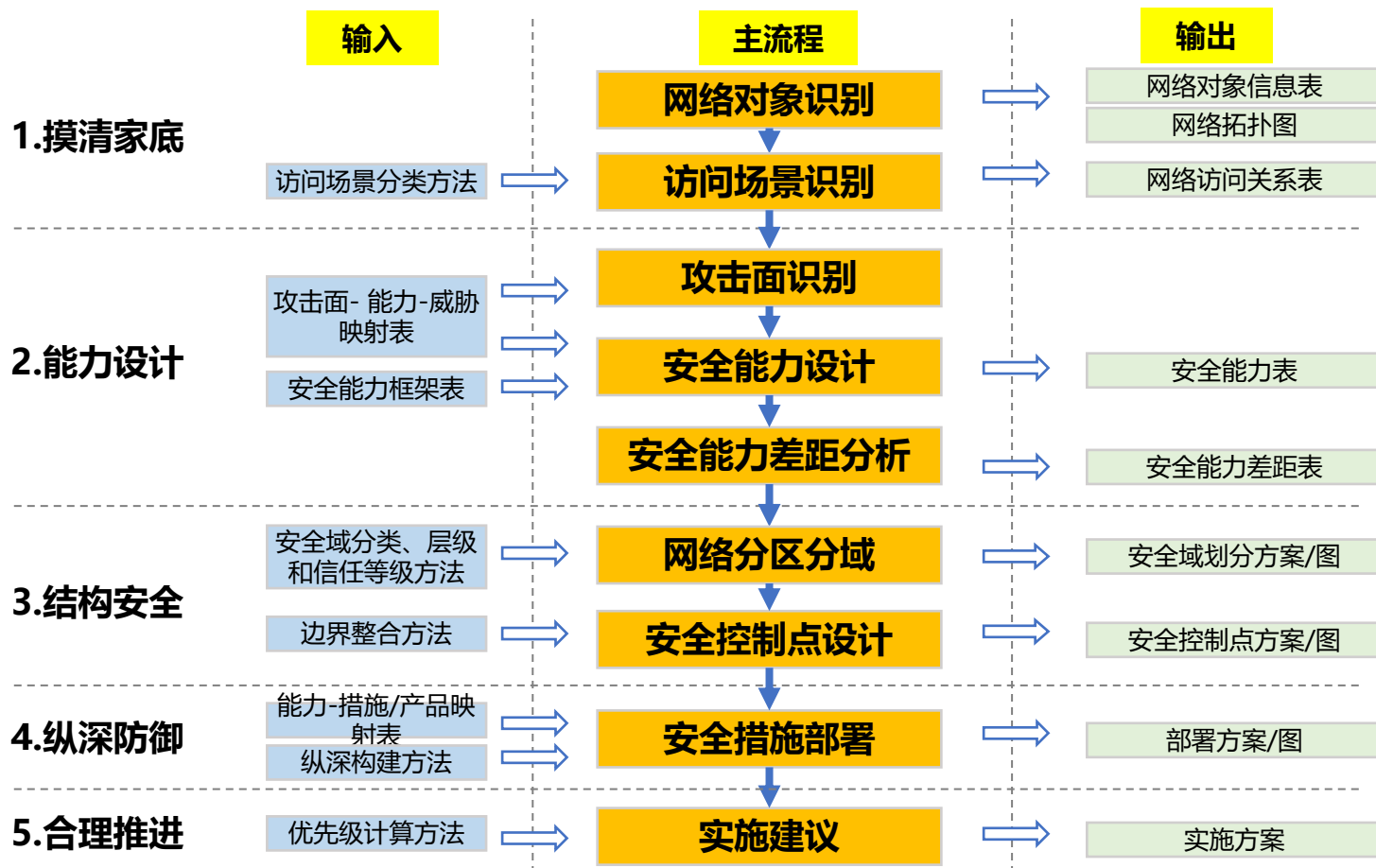
态势感知平台作为安全信息汇总枢纽与安全决策中心，与安全监控系统、工控系统安全测试验证环境协同联动，人员、工具、安全管理和运维一体化协同运行。





# 纵深防御体系

## ✓ 纵深防御建设路线图

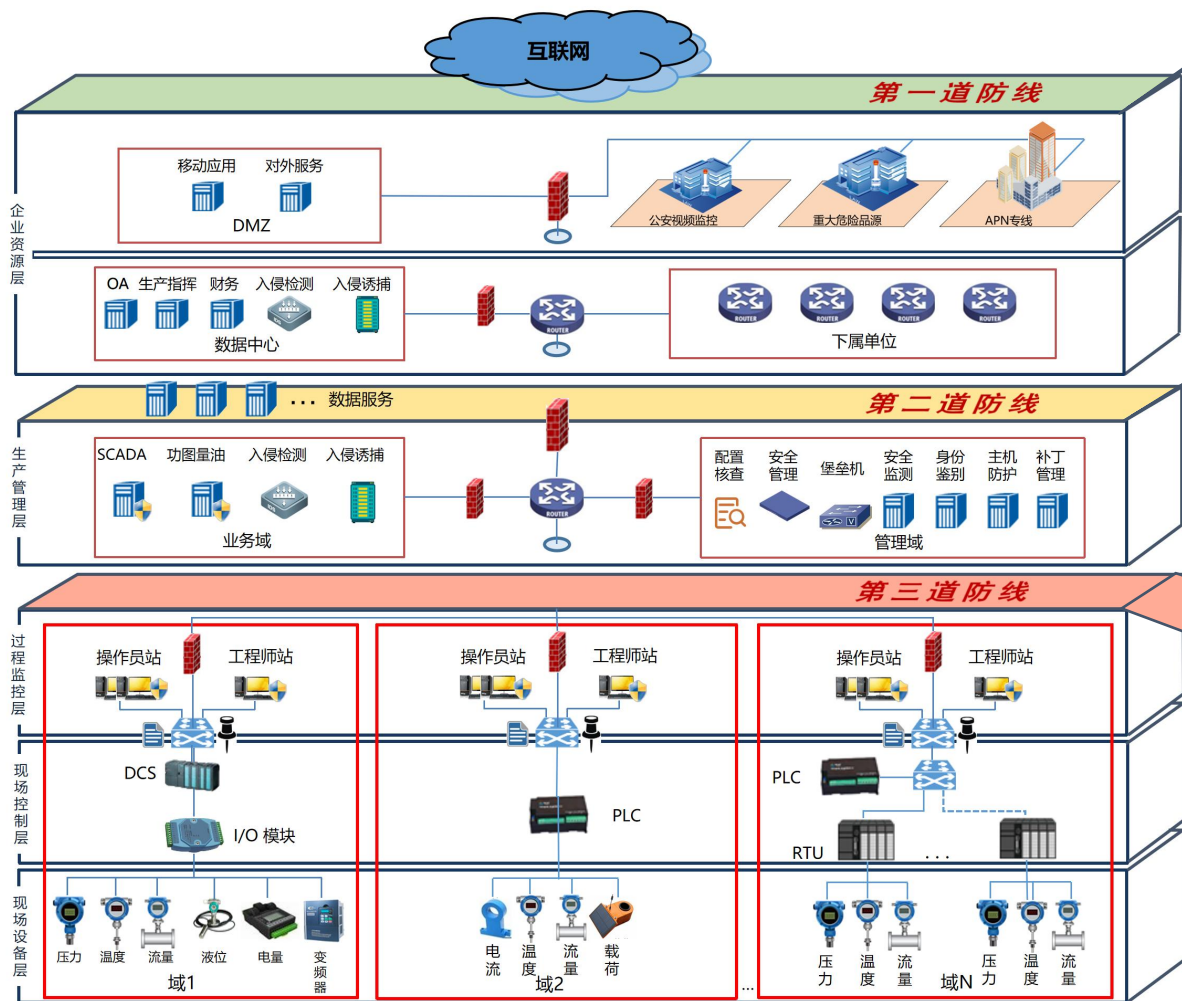






# 纵深防御体系

## 纵深防御体系：网络“三道”防线



**防护重点:** 防外网攻击, 防外网入侵

**防护技术:** 边界隔离、威胁分析、流量检测、流量清洗、态势感知、统一运维管理、溯源分析

**防护效果:** 监测阻断扫描探测、Web攻击等, 有效抵御传统常规网络攻击行为

**防护重点:** 防内网攻击, 防内网恶意行为

**防护技术:** 边界防护、入侵检测、安全监测、入侵诱捕、漏洞挖掘、溯源分析、统一运维管理

**防护效果:** 监测阻断跳板攻击、边界突破等, 有效防范工控协议级攻击行为

**防护重点:** 防病毒蔓延, 防系统被控制、防数据窃取与指令篡改

**防护技术:** 域间隔离、主机安全防护、工控审计、安全业务模型、接入认证、传输加密、配置核查、白名单机制

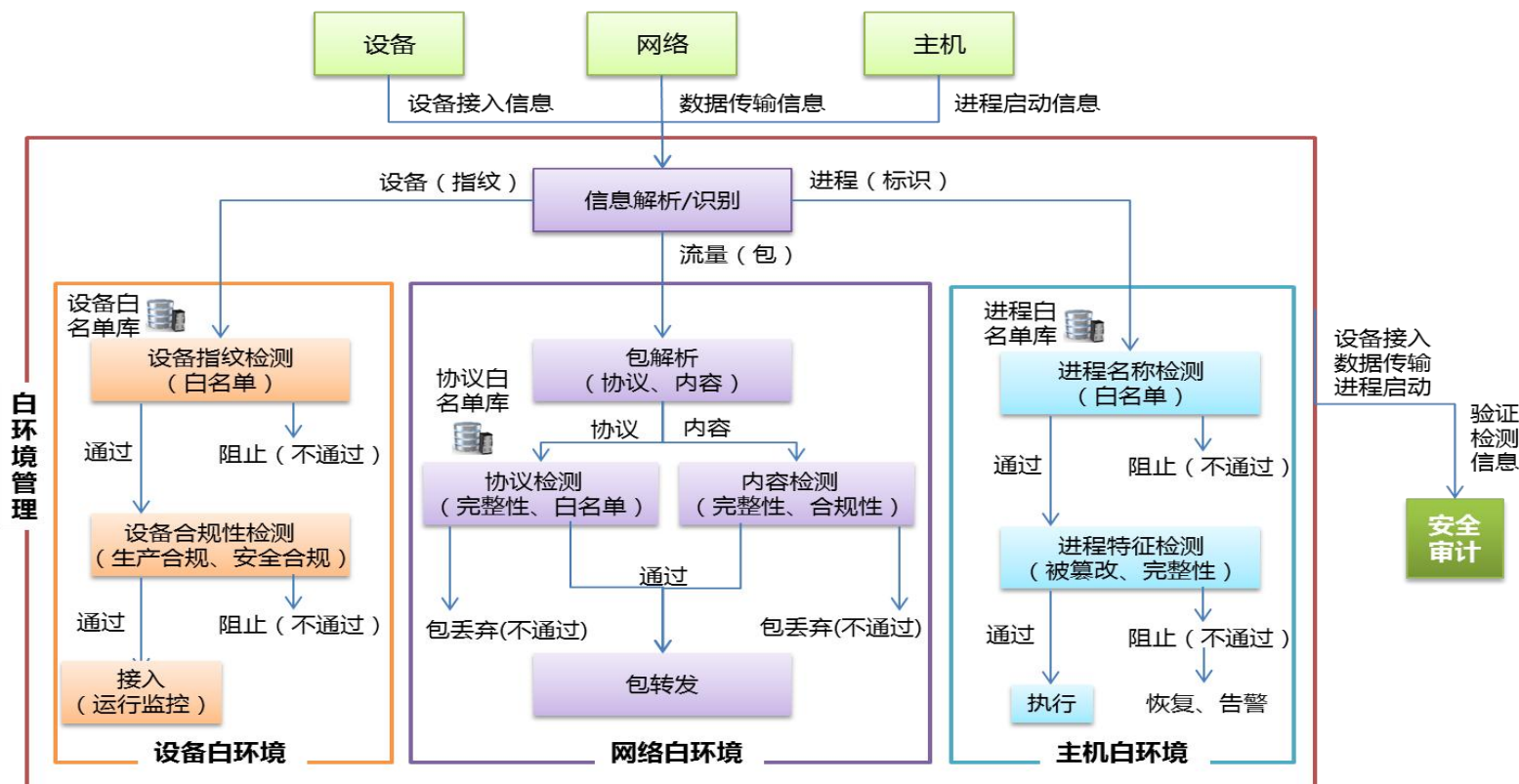
**防护效果:** 监测阻断跨域攻击、主机被控等, 有效防范工控指令级、系统进程级、控制设备级攻击行为



# 加强工控网络内部防护-白环境

## ➤ 建成白环境应用场景

白环境场景由设备白环境、网络白环境和主机白环境组成，当设备接入时，对设备信息识别、解析后，对比设备指纹白名单检测库，进行设备合规性检测，允许合法设备接入；上位机加载进程时，通过进程白名单库进行特征对比，只允许合法软件运行；当传输数据信息时，对协议和IP进行检测，比对网络访问白名单库。阻断非法设备接入、非法软件运行及异常数据传输。





# 加强系统本质安全-认证与加密机制

## ➤ 实现国密标识认证技术在油气生产场景的试点应用

为提升油气生产现场控制设备本质安全能力，攻关接入认证与加密传输技术，完成玛湖油田**120口井52台**RTU设备安全改造，形成了国产密码技术嵌入工控设备的成功示范案例。

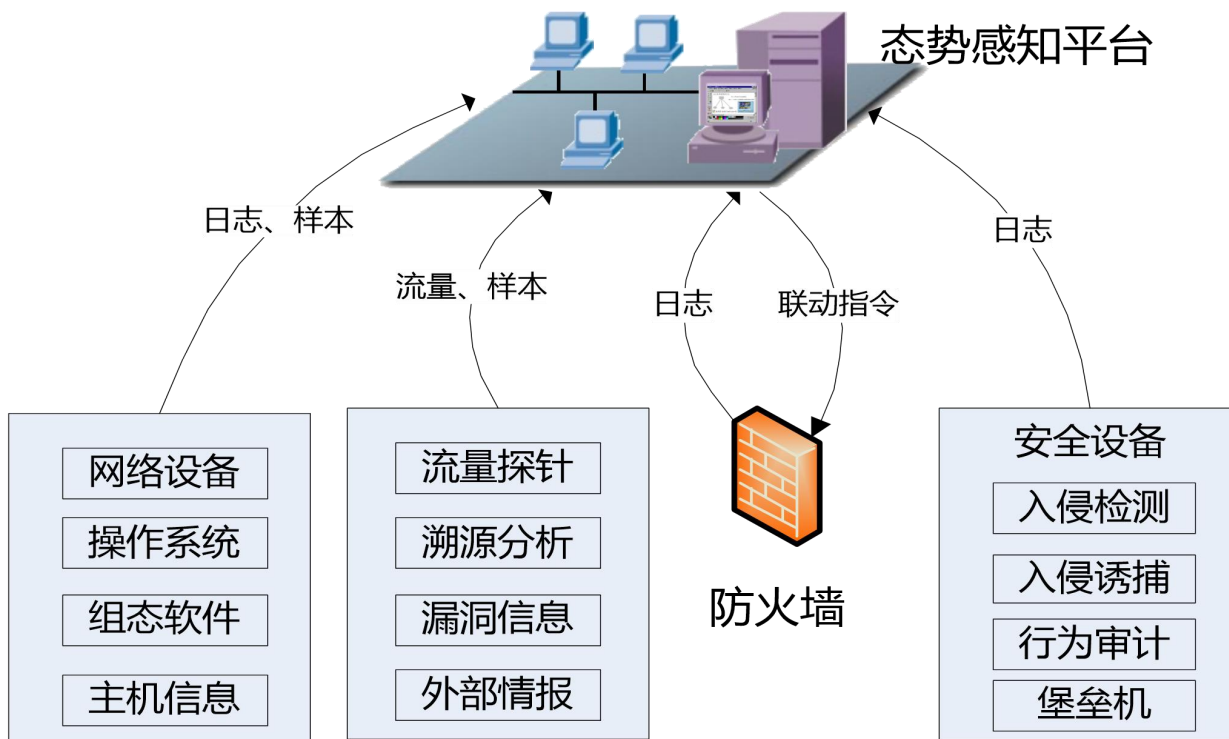
- 适配油气生产场景现场设备量大分散、计算性能低等特点，将具备轻量级、易管理、低成本等特点的国密SM9算法嵌入RTU设备，实现签名验签速率**28次/秒以上**。
- 基于TLS优化的轻量级密码传输协议，延迟控制**100毫秒**以内，满足油气生产<150毫秒的实时性响应需求。
- 实现现场控制设备接入认证，有效**防范设备假冒风险**。
- 实现生产数据与控制指令实时加密传输，达到**防窃密、防篡改**效果。



# 提升应急处置能力-协同联动机制

## ➤ 建成协同联动的应急处置机制

规范运维管理监控处置流程，建立人、系统、设备的协同联动处置机制。系统运维监控中，态势感知平台根据防火墙、入侵检测、入侵诱捕、流量探针、主机卫士等设备采集的日志、流量等安全要素，结合外部情报等综合分析判断正在进行的攻击行为或病毒扩散趋势，确定关键节点防火墙设备，事态严重时，一键下发安全阻断策略，防止事态扩展。







# 安全验证环境

建成了油气开采、油气储运、炼化生产、加油站、石油机械加工等石油石化行业关键工艺仿真环境，搭建了竞赛、靶场、实训等平台，具备场景验证、安全检测、策略验证、漏洞挖掘、攻防实训等功能，解决了在真实生产环境下无法开展方案验证、技术试验、策略与补丁验证、安全检测等难题。





# 运维管理

通过工业控制系统综合防护能力建设，形成“感、控、仿、验、优”一体的运维模式，将制度流程、技术工具和运维人员有机结合，全面提升工控安全风险监控、事件应急处置等能力，保障物联网、生产装置安全稳定运行。





**一、概述**

**二、工控安全建设**

**三、启示**



## (1) 强化顶层设计，健全工控系统安全保障体系

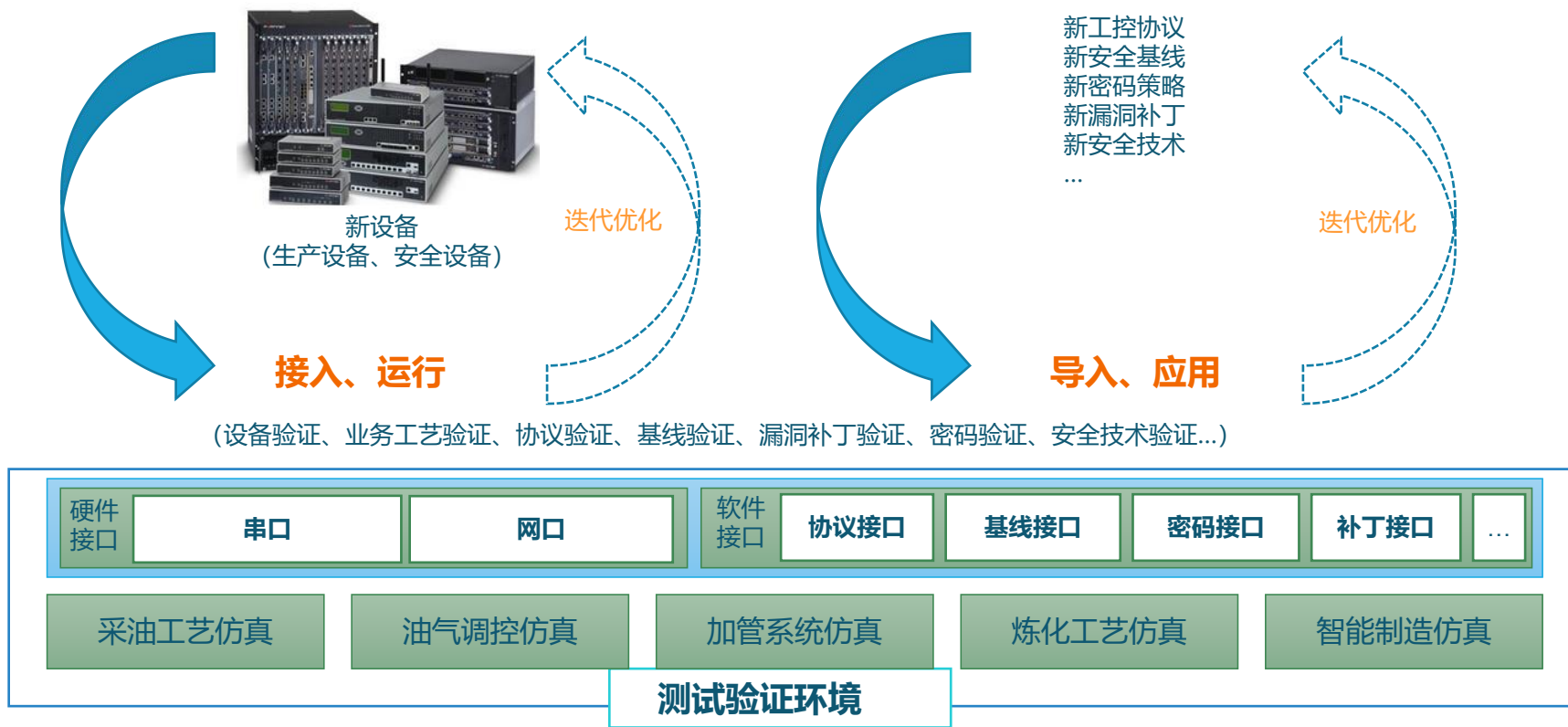
以保障生产业务系统安全稳定运行为核心，贯彻总体设计、分步实施、逐步完善的思路。通过纵深防御体系、评估与应急管理、制度标准完善等措施，实现整体防护、精准防护。





## (2) 夯实验证环境，构建工控系统安全测试生态

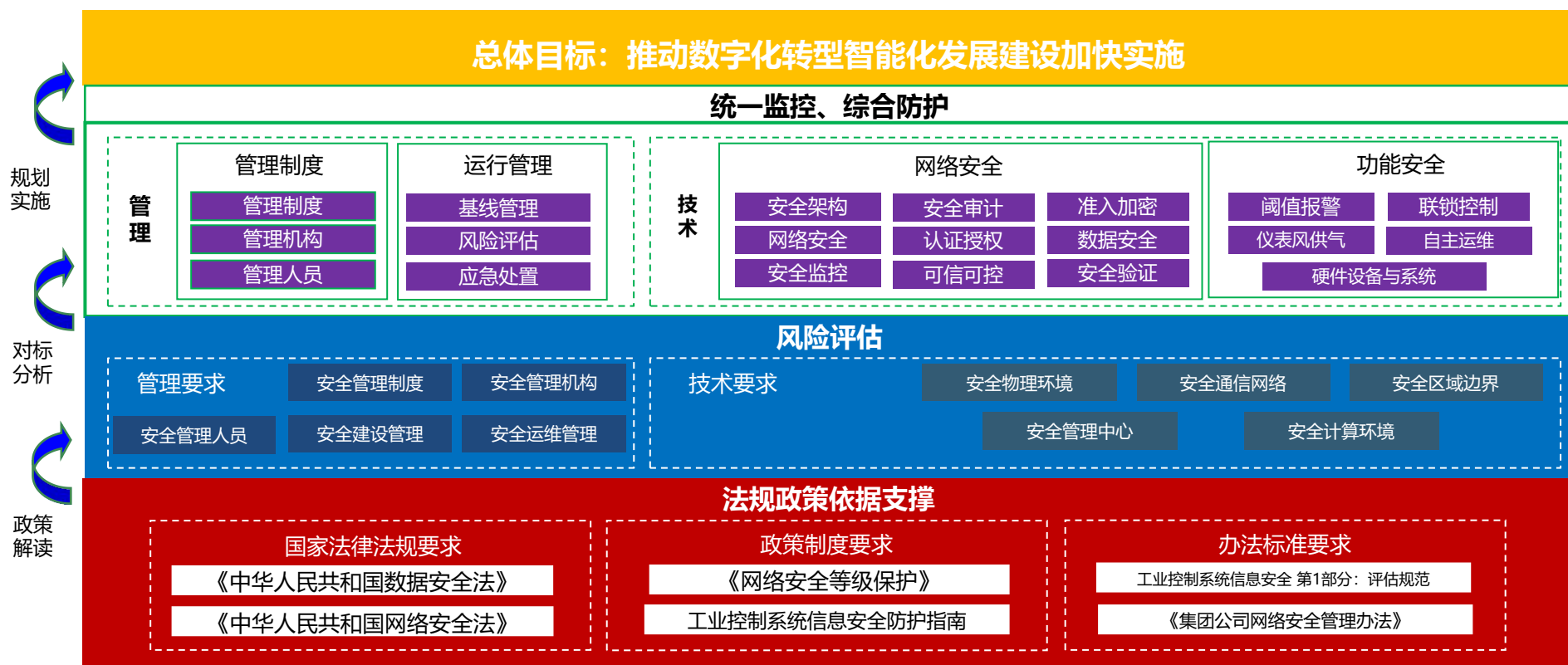
加强供应链管理，以测试验证环境为手段，建立工控系统、设备安全检测机制，**规避和最大程度减轻网络安全风险**，**提高工控系统抗风险能力**，从而推动整体设备测试生态建设，为石油石化行业生产安全保驾护航。





### (3) 转变防护理念，探索行业场景安全解决方案

油气生产、油气储运、炼化生产、成品油销售、装备制造等生产场景工控系统有其各自的特殊性，照搬传统网络安全防护理念解决工业场景问题的办法不可行。需要生产业务人员、信息人员密切协作，共同梳理需求，以适应业务发展带来的变化为着力点，探索适用工业场景的解决方案，促进信息化和工业化的深度融合。





谢谢！