UWNTEK 优稳

# 工控安全产品

杭州优稳自动化系统有限公司
HANGZHOU UWNTEK AUTOMATION SYSTEM CO., LTD.

UWNTEK
打造优秀的控制系统产品

# UW工业防火墙

UW工业防火墙系列支持多种工业协议的识别和过滤，如Modbus、DNP3、OPC等，能够深入解析和监控工业通信，检测异常行为和潜在威胁。此外，还具备实时监控、日志管理和事件追溯等功能，帮助企业及时发现和应对安全事件，保障生产过程的连续性和安全性。其坚固耐用的设计适用于各种严苛的工业环境，提供高可靠性和长寿命的网络安全防护。

## 产品型号

- **UW7752** 工业防火墙 — 控制域间基本级
- **UW7752e** 工业防火墙 — 控制域间增强级
- **UW7852** 工业防火墙 — 现场控制层基本级
- **UW7852e** 工业防火墙 — 现场控制层增强级

## 客户价值

- **提高安全性**：预防恶意攻击事件，避免重大损失
- **降低生产成本**：预防员工误操作，降低生产成本
- **提升网络可见性**：全面了解网络运行状态
- **降低运营成本**：一键省心部署，全面覆盖安全域
- **满足合规要求**：资质齐全，助力等保合规测评

## 目标客户

石油、化工、电力、水处理

## 产品优势

- **种类广**：支持工控协议深度解析，种类 20+
- **高度可塑性**：支持完全自定义的模板，支持 100+ 主流工控协议
- **高可靠性**：1Gbps线速下，数据包 0丢包 0乱序
- **低延迟**：1Gbps线速下，64字节短包延迟小于30us

## 主要功能

工业流量深度解析和过滤

异常事件实时监控

入侵及时防御

统一云平台管理

UWNTEK
打造优秀的控制系统产品

# UW工业主机安全卫士

工业主机安全卫士是一款专为工业环境设计的主机安全防护软件。它提供实时监控、威胁检测、漏洞修复和策略管理等功能，全面保护工业主机免受各种安全威胁。通过智能分析和自动响应，快速处理潜在风险，确保工业系统的稳定运行。该软件还支持日志收集和合规管理，帮助企业满足安全法规要求。工业主机安全卫士简化了安全管理流程，提升了整体防护能力，是保障工业系统安全的可靠选择。

## 客户价值

**提高系统安全性**
通过白名单机制和USB管控，有效防范恶意软件和未经授权的设备使用，提升整体安全水平

**防止数据泄露**
严格的USB设备管控措施，保障敏感数据不被非法拷贝和传输。

**符合合规要求**
全面的安全防护功能，帮助企业满足各类安全法规和标准，降低合规风险。

**保障网络安全**
网络连接控制功能阻止非法网络访问，确保网络环境的安全性。

**简化管理流程**
统一云平台管理，集中监控和配置各项安全策略，降低管理复杂度，提高效率。

## 产品型号

- **UW7831** 工业主机安全卫士 — Windows
- **UW7831e** 工业主机安全卫士 — Linux

## 产品优势

**高安全性**
通过白名单和USB管控提供多层次防护

**灵活管理**
支持网络连接控制适应不同安全需求

**强兼容性**
适用于多种工业主机易于集成部署

**高效运维**
统一云平台管理简化运维操作

## 目标客户

电力 · 石油 · 化工 · 水处理

## 主要功能


可信应用白名单


USB设备管控


网络连接控制


统一云平台管理

UWNTEK
打造优秀的控制系统产品

# UW工控网络安全审计系统

工控网络安全审计系统可实时监控和分析工控网络流量，识别异常行为和潜在威胁。支持多种工业协议的深度识别和解析，确保通信安全性和数据完整性。集成入侵检测功能，实时告警恶意攻击。具备强大的日志管理和事件追溯功能，快速追溯安全事件源头。直观的可视化仪表盘和自定义报表功能，帮助安全人员全面管理网络安全态势，确保系统安全、稳定运行。

## 产品型号

- UW7811 工控网络安全审计系统 基本级
- UW7811e 工控网络安全审计系统 增强级

## 客户价值

**风险识别**
提前发现并解决网络漏洞和威胁

**提升合规**
确保工控网络符合安全法规和标准

**降低成本**
自动化审计流程减少人工成本，提高效率

**优化性能**
分析和监控网络流量减少故障和停机时间

**决策支持**
提供详细审计报告优化安全策略

## 目标客户

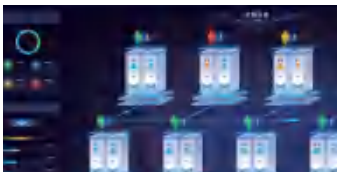
石油 化工 电力 水处理

## 产品优势

- 支持工控协议种类 100+
- 超级大屏 多维度监控
- 机器自学习生成采集策略 优化日志生成质量
- 深度数据挖掘 多维日志关联分析
- 原始报文全保存 轻松实现事件追溯

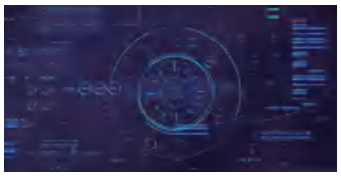
## 主要功能

主流工控协议深度解析



超级大屏实时监控异常

全报文审计助力事件溯源



统一云平台管理

UWNTEK
打造优秀的控制系统产品

# UW工业安全产品综合管理平台

工业安全产品综合管理平台是一款用于局域网内同系列安全产品的综合管理工具。平台提供状态监控、策略下发、日志收集和关联分析等功能。通过实时监控安全产品的运行状态，集中配置和更新安全策略，收集并分析安全事件日志，平台简化了多设备管理流程，提升了整体安全防护水平，是企业信息安全管理的有力助手。

## 产品型号

- UW7802 工业安全产品综合管理平台 **基本级**
- UW7802e 工业安全产品综合管理平台 **增强级**

## 客户价值

**提高管理效率**
集中管理简化操作
节省时间和人力

**增强安全防护**
实时监控和智能分析
快速识别威胁

**支持决策**
提供详尽数据和分析报告
优化安全策略

**降低运营成本**
自动化流程
减少人力资源投入

**确保合规性**
全面日志收集
满足合规要求

## 目标客户

石油　化工　电力　水处理

## 产品优势

支持UW全系列
安全产品集中管理

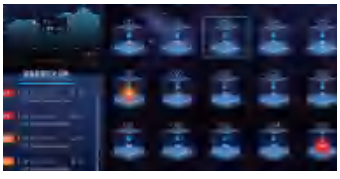
安全策略统一下发
确保一致性

智能关联分析
发现潜在威胁和漏洞

多维度日志收集
便于审计和追溯

多个综合监控面板
全面监控异常事件

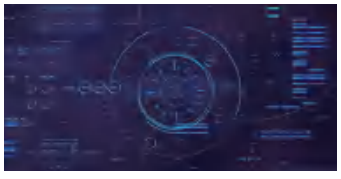
## 主要功能



实时状态监控

统一情报中心

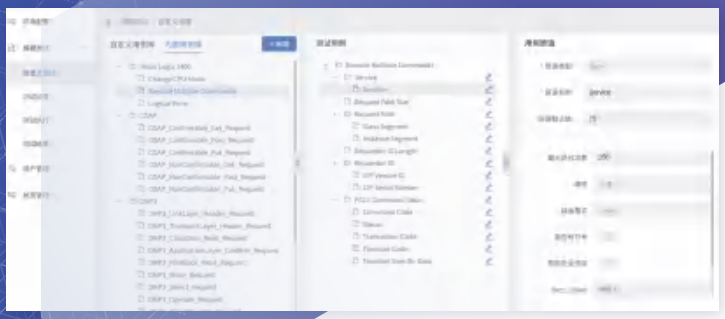
统一设备管理



日志关联分析

UWNTEK
打造优秀的控制系统产品

# UW工控网络漏洞挖掘系统



工控网络漏洞挖掘系统是一款采用智能模糊测试技术，对工控设备、工控系统等工业资产进行未知漏洞挖掘、安全性及协议健壮性测试的检测评估设备。

## 产品型号

▶ **UW7823** 工控网络漏洞挖掘系统

## 客户价值

**提高安全性**
帮助用户测试所用工控设备的安全性

**提供参考方案**
漏洞挖掘为用户提供工控网络安全防护方案

**降低运营风险**
提前发现和修复漏洞，确保业务稳定性

**提高竞争力**
打造安全的工控设备

**支持安全合规**
深入漏洞挖掘，确保系统符合安全合规性要求

## 目标客户

- 工业生产企业
- 科研院所
- 工控设备生产商

## 产品优势

### 未知漏洞挖掘能力

内置**主流厂商**的**私有工业协议**测试样例；
可对工控设备进行全面深入的**检测**、**挖掘**和**评估**。

### 自定义协议测试

支持用户**自定义**各类工业资产**私有协议**；
支持**10+种**模糊测试原语，提供不同的协议数据构造方法；
支持**5种**类型监视器。

### 测试过程可视化

提供**测试过程中**被测**设备状态**的外部**实时监视**；
支持端口监视，如ARP监视、ICMP监视、TCP端口监视等。

## 主要功能

内置主流工控厂商
私有协议测试样例

支持用户私有协议
测试样例自定义

工控网络设备模糊测试
执行与监视

发现并定位被测设备
的未知缺陷

UWNTEK
打造优秀的控制系统产品

# 石化

在石油化工行业中，石油炼化工控网络的工业控制系统已广泛应用，主要工业控制系统包括：集散控制系统（DCS）、安全仪表系统（SIS）、可编程逻辑控制器（PLC）、可燃气体和有毒气体检测系统(GDS)、安防视频监控系统、工业机房门禁控制系统、火灾报警系统（FAS）等，并已成为石油化工行业重大的基础设施。在“两化”融合的行业发展需求下，信息化与工业化深度融合，系统的互联互通性逐步加强，工控网络与办公网、互联网也存在千丝万缕的联系。

## 遵循标准

《中国石化工业仪表控制系统安全防护实施规定》

《工业控制系统信息安全防护指南》

GB/T 22239-2019
《信息安全技术 网络安全等级保护基本要求》

## 解决方案

### 核心理念

工控网络“白名单”

### 安全区域边界

各区域的边界之间部署UW7752工业防火墙，实现分层级的安全防护，抵御已知的安全威胁，通过对工控协议的深度解析，来保障通信数据的合法性，实现对工业控制网络的深度防护。

### 安全通信网络

部署UW7811工控网络安全审计系统，通过特定的安全策略，快速识别出控制系统网络非法操作、异常事件、外部攻击；对系统环境进行安全配置审计，生成审计报告，帮助进行安全合规性审计和事件调查取证。

### 体系架构

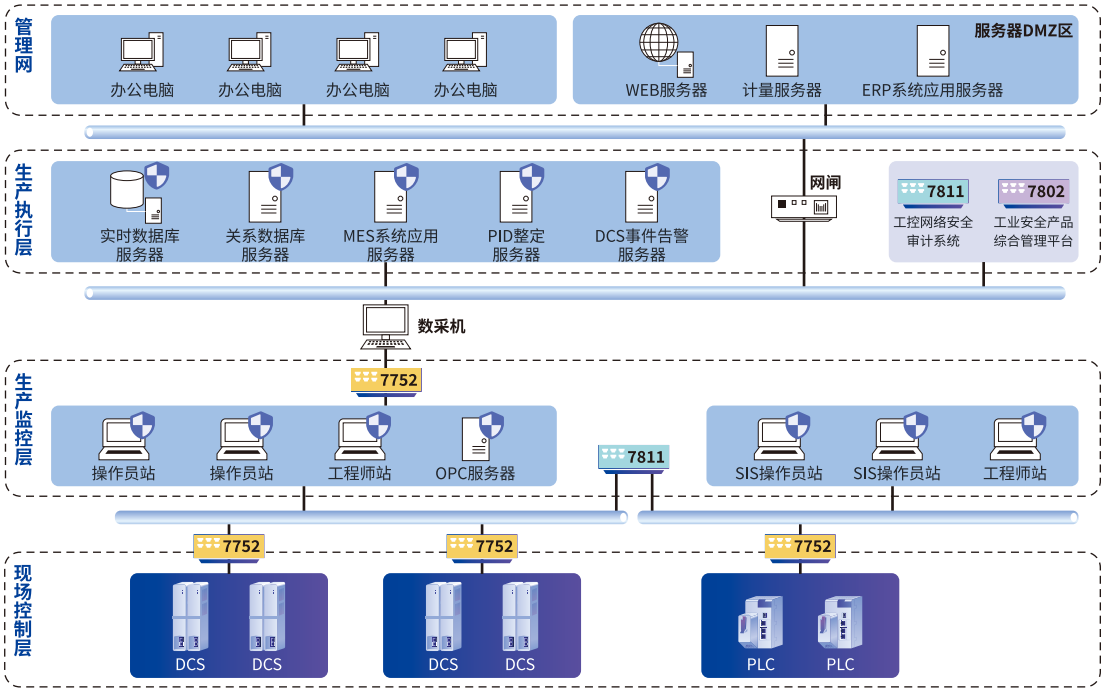
基于
“一个中心，三重防护”

### 安全计算环境

在系统的各工作站、操作员站、服务器安装UW7752工业主机安全卫士，开启白名单功能，禁止不可信任的程序运行；开启外设管控功能，禁止不安全的移动存储介质接入。

### 安全管理中心

部署工业统一行为安全管理平台，实现对部署在整个工控系统的安全设备统一化的安全监管和运维，支持对工控安全设备的集中管理、策略下装、状态监视，打破安全孤岛，使他们成为一个有机体系统来抵御网络中的各种威胁。




**UW7831**
**工业主机安全卫士**

**UW7752**
**工业防火墙**

**UW7811**
**工控网络安全审计系统**

**UW7802**
**工业安全产品综合管理平台**

UWNTEK
打造优秀的控制系统产品

# 火电

我国以煤炭为燃料的火力发电量长期占据全国总发电量七成左右比例，电力系统的安全发展和安全稳定运行关系到国计民生。在工业控制网络安全大背景下,控制系统的安全是整个电力行业不可忽略的重点。

## 遵循标准

GB/T 22239-2019
《信息安全技术 网络安全等级保护基本要求》

《中华人民共和国网络安全法》

《工业控制系统信息安全防护指南》

## 解决方案

### 核心理念

工控网络“白名单”

### 体系架构

基于
“一个中心，三重防护”

### 基本原则

“安全分区、网络专用、横向隔离、纵向认证”

### 安全区域边界

网络边界处部署UW7752工业防火墙，采用适用于工控网络的“白名单”机制，深度解析工控系统网络协议，对非法及异常访问行为进行拦截阻断，保障网络边界的安全。

### 安全通信网络

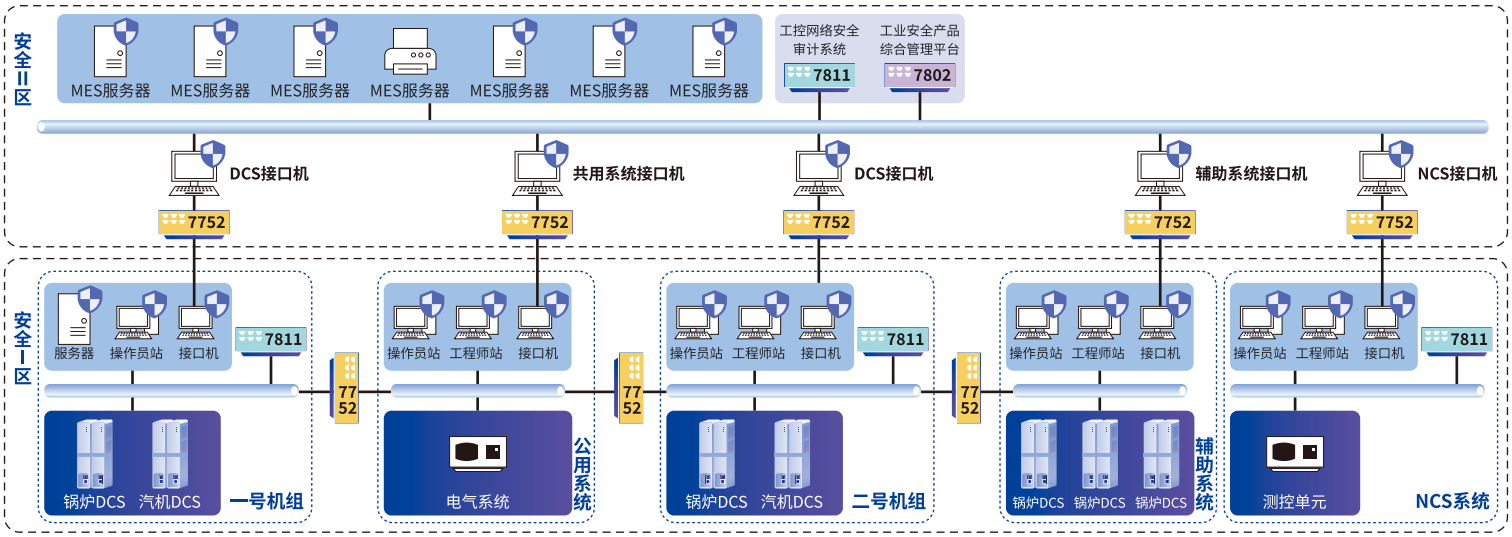
在各主机、辅控系统网络核心交换机中旁路部署UW7811工控网络安全审计系统，实现对网络流量、异常事件、操作行为和数据内容等安全审计，对异常行为进行实时警报，实现网络行为监测和审计。

### 安全计算环境

通过在系统的服务器和工作站部署UW7752工业主机安全卫士，采取黑白名单技术措施，实现对病毒的免疫，保障服务器和工作站的系统安全。

### 安全管理中心

部署UW7802工业安全产品综合管理平台，实现对网络安全设备的统一安全管控，实现安全设备的状态监控、审计管理和策略管理等集中管控功能，构筑安全管理中心平台，提升整体网络安全防护和运维管控水平。




### UW7831 工业主机安全卫士

对操作系统、服务器提供主机白名单可信防护、恶意代码拦截、外设管控等安全能力，实现安全防护。

### UW7811 工控网络安全审计系统

主要部署安全二区内的各个系统分区下。

### UW7752 工业防火墙

安全分区，部署在网络区域边界处与各系统边界处，隔离安全一区与安全二区；对安全二区内部的各个系统、机组进行安全隔离、防护。

### UW7802 工业安全产品综合管理平台

所在分区或系统区域的工业主机安全卫士、工业防火墙、工控网络安全审计系统进行统一管理、状态监控。

UWNTEK
打造优秀的控制系统产品

# 水处理

水务行业产业链主要涉及从自然水体中取水、水的加工处理、供应和污水处理等环节。随着“两化”融合的步伐正在不断加快，传统物理隔离的水务行业工控系统逐步向互联、智能方向发展。如何保护好水务工业控制系统安全，已经成为政府机构、企事业单位所关注的重点。

## 遵循标准

GB/T 22239-2019
**《信息安全技术 网络安全等级保护基本要求》**

工信部信软(2016)338号
**《工业控制系统信息安全防护指南》**

## 解决方案

### 策略

“纵深防御、分区防护”

### 安全区域边界

依据“分层、分域、分级、分时”的防护要求，按照重要安全域与其他安全域分离、专网与公众网络逻辑隔离的安全策略，建立统一的交互边界。

### 安全通信网络

部署UW7811工控网络安全审计系统实时分析、审计网络全流量，收集和解析系统日志，用于事件分析、取证和合规性审计。

### 体系框架

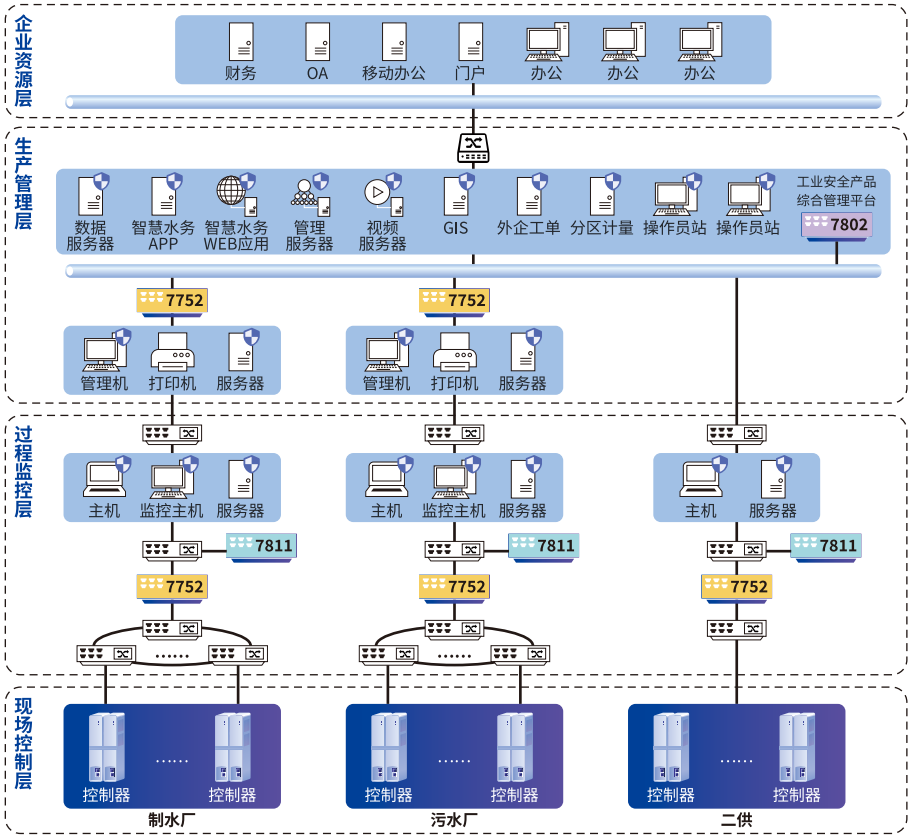
基于
“一个中心、三重防护”

### 安全计算环境

轻量级“白环境”。在操作员站、工程师站和服务器等部署UW7752工业主机安全卫士，实现对工控主机恶意代码防护、外设端口的管理和操作系统的安全防护，全面提升工控主机安全防护能力。

### 安全管理中心

部署UW7802工业安全产品综合管理平台管理平台，对安全计算环境，安全通信网络，安全区域边界进行统一管理，构建“一个中心，三重防护”体系，满足行业政策法规及技术要求。




### UW7831 工业主机安全卫士

对生产管理、过程监控层的操作系统、服务器提供主机白名单可信防护、恶意代码拦截、外设管控等安全能力，实现安全防护。

### 7752 UW7752 工业防火墙

安全分区，部署在网络区域边界处与各系统边界交换机处。

### 7811 UW7811 工控网络安全审计系统

主要部署在关键交换机处，实时分析、审计网络流量并记录审计日志。

### 7802 UW7802 工业安全产品综合管理平台

部署在关键交换机处，对此网络部署的工业主机安全卫士、工业防火墙、工控网络安全审计系统进行统一管理、状态监控。

UWNTEK
打造优秀的控制系统产品

# 烟草行业

随着IT系统在生产、经营和监管等各个环节的渗透，信息化与行业发展战略、生产经营和决策管理在更大范围、更深层次、更高水平上融为一体。故提高信息化建设水平已经成为整个烟草行业在改革和发展过程中提高管理水平的重要途径。为提升工控网络的安全性，采用有效的安全加固技术和建立完备的网络安全防护体系显得尤为重要。

## 遵循标准

**《工业控制系统信息安全防护指南》**
（工信软函〔2016〕338号）

**《GB/T 22239-2008 信息系统安全等级保护基本要求》**

**《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号文）

## 解决方案

### 核心理念

工控网络“白名单”

### 安全区域边界

“纵向分层、横向分区”。工业控制边界部署UW7752工业防火墙进行管理网和生产网、监控网的逻辑隔离，在网络边界上加强防护，在各个区域及各生产线之间进行有效的安全隔离，对两网间数据交换进行安全防护，确保生产网不会引入管理网所面临的风险。

### 网络监控审计

各安全区域的关键节点上对网络流量、通信等行为进行审计，部署UW7811工控网络安全审计系统收集和解析系统日志，用于事件分析、取证和合规性审计。

### 体系架构

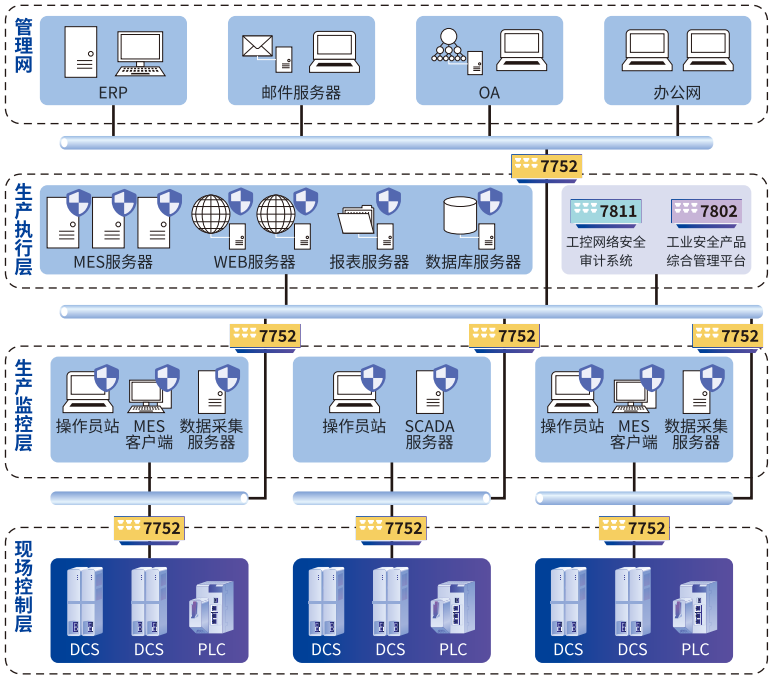
“纵深防御安全防护体系”

### 主机安全防护

建立轻量级“白环境”。在工程师站、操作员站以及关键服务器上部署UW7752工业主机安全卫士，实现对病毒、木马及其它恶意程序攻击行为的阻断，对外设端口的管控，提升主机安全防护能力。

### 统一管理

“统一管控，集中分析”。部署UW7802工业安全产品综合管理平台对安全设备进行集中管理、策略下装、状态监视，同时基于安全设备产生的日志数据、告警数据进行安全事件关联分析。




### UW7831 工业主机安全卫士

针对生产执行层、生产监控层所有操作系统、服务器，提供主机白名单可信防护、恶意代码拦截、外设管控等安全能力，实现安全防护。

### 7752 UW7752 工业防火墙

生产网与管理网之间、生产网内部层级之间使用进行隔离，避免管理网风险引入生产网，生产控制内部之间应进行有效的边界隔离和防护手段。

### 7811 UW7811 工控网络安全审计系统

主要部署生产监控层、生产执行层，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。

### 7802 UW7802 工业安全产品综合管理平台

主要部署在生产执行层、生产监控层，对所部署的工业主机安全卫士、工业防火墙、工控网络安全审计系统进行统一管理、状态监控。

UWNTEK
打造优秀的控制系统产品

# 石化工程大型工业装置的数字孪生系统

**模型库支撑系统**
初馏过程、常压加热过程、常压精馏过程、常压提馏过程、减压精馏过程、减压提馏过程等重要子系统

**数据规模**
10000点以上

**模型库涵盖范围**
初馏过程、常压加热过程、常压精馏过程、常压提馏过程、减压精馏过程、减压提馏过程

**石化工程模型库**
简捷精馏塔、多侧线严格精馏塔、石油物料流等 28 个单元设备模型

**可扩展迁移场景**
石油炼化业务场景、精细化工业务场景等

**控制系统涵盖范围**
初馏塔控制系统、常压塔顶串级控制系统、常压塔底串级控制系统、常压炉串级控制系统、减压炉串级控制系统、减压塔控制系统等重要控制系统

**数字孪生精度**
关键参数：稳态偏差<±1%，动态偏差<±2.5%
非关键参数：稳态偏差<±2%，动态偏差<±3%

**验证示范场景**
1000万吨级炼油的常减压装置

**支持工控软件**
石化行业国内外主流品牌

**应用场景**
1000万吨级炼油的常减压装置

## 工艺特点

**多领域**
机械、流体、化工热力学等

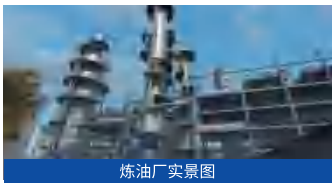
**多系统**
初馏、常压精馏、常压提馏、减压精馏、减压提馏等

**多工况**
运行环境多变

**多目标**
多目标全生命周期优化

## 1000 万吨级炼油常减压装置系统和工艺流程

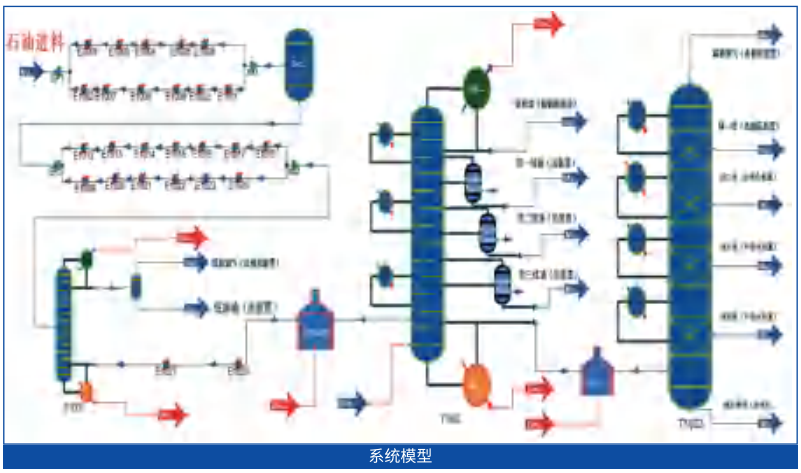
### 炼油厂、设备图与系统模型


炼油厂实景图


精馏塔

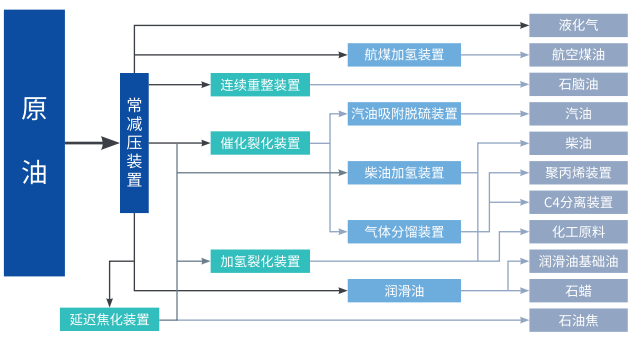

列管式换热器

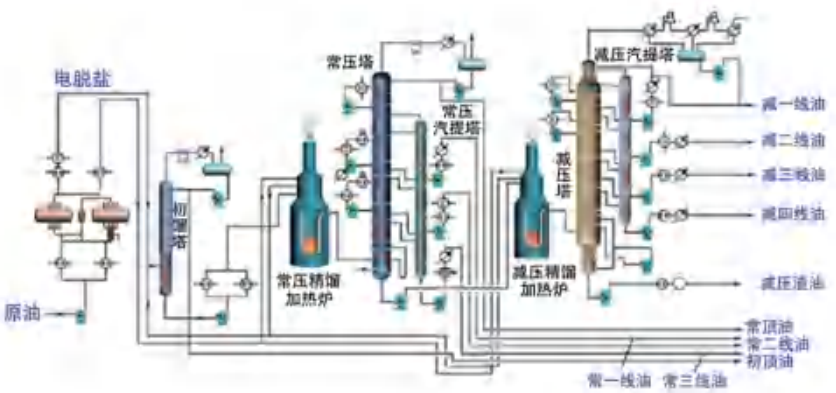

管式加热炉



系统模型

### 工艺流程



UWNTEK
打造优秀的控制系统产品

# 电力工程大型工业装置的数字孪生系统

**电力工程模型库**
汽轮机级组、炉膛、脱硫塔、磨煤机等39个单元设备模型

**模型库支撑系统**
燃烧系统、汽水系统、电气系统、风烟系统等重要子系统

**数字孪生精度**
关键参数：稳态偏差<±1%，动态偏差<±2%
非关键参数：稳态偏差<±2%，动态偏差<±3%

**支持工控软件**
电力行业国内外主流品牌

**可扩展迁移场景**
火电业务场景、热电业务场景等

**数据规模**
10000点以上

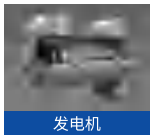
**验证示范场景**
1000MW超超临界火电机组

**控制系统涵盖范围**
FSSS、DEH、CCS 等重要控制系统

## 超超临界 1000MW 火电厂系统和工艺流程

### 电厂、设备图与系统模型

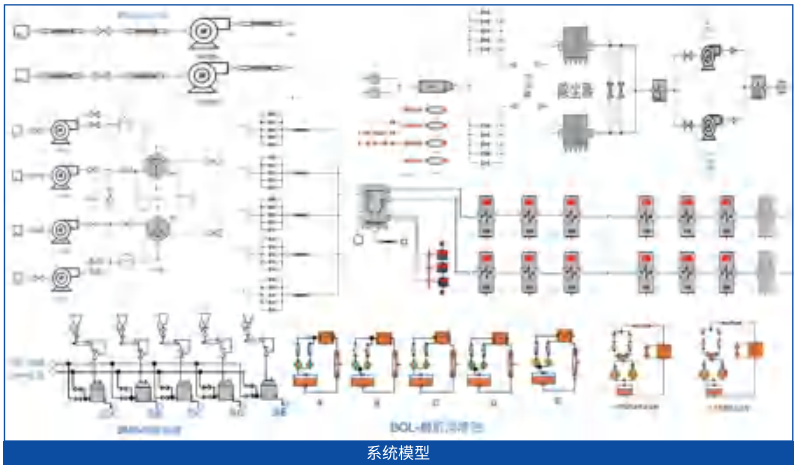

火力发电厂全貌


发电机


汽轮机


空气预热器


轴流风机


系统模型

## 工艺特点

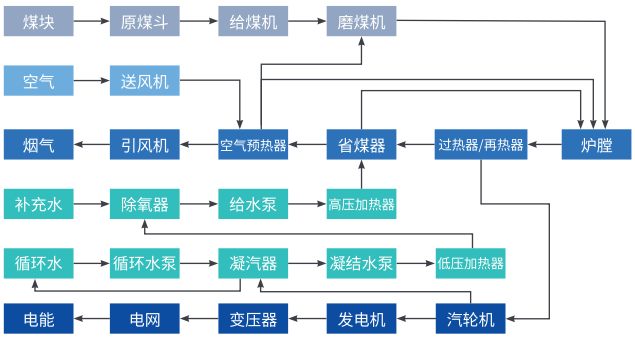
**多领域**
电力、机械、热力学、流体等

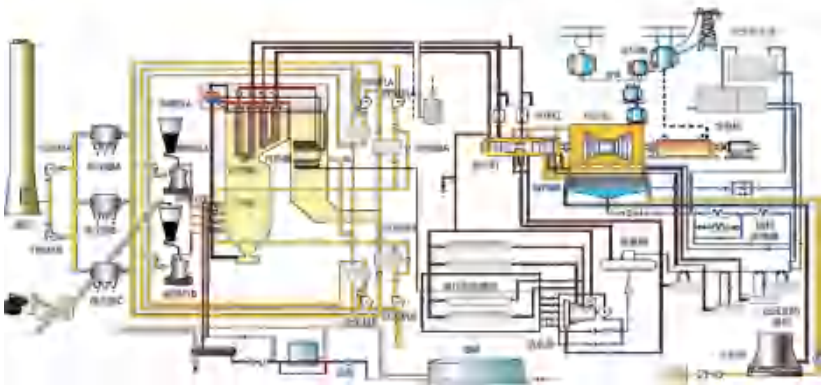
**多系统**
风烟系统、汽水系统、电气系统等

**多工况**
运行环境多变

**多样化**
调峰决策多样化

## 工艺流程



UWNTEK
打造优秀的控制系统产品

# 公用工程大型工业装置的数字孪生系统

**模型库支撑系统**
一级处理系统、二级处理系统、三级处理系统、污泥处置系统等重要子系统

**数据规模**
3000点以上

**公用工程模型库**
缺氧池、好氧池、二沉池、污泥厌氧消化池等14个单元设备模型

**可扩展迁移场景**
污水处理场景

**控制系统涵盖范围**
基于污水处理运行特征的预测控制系统、污水处理过程的多目标预测控制系统、污水处理过程的多速率预测控制系统、多层结构的污水处理过程监控系统、厂级监控系统等重要控制系统

**数字孪生精度**
关键参数：稳态偏差<±1%，动态偏差<±2.5%
非关键参数：稳态偏差<±2%，动态偏差<±3%

**验证示范场景**
污水处理装置

**支持工控软件**
公用工程行业国内外主流品牌

## 工艺特点

**多领域**
机械、流体、生化等

**多系统**
一级处理、二级处理、三级处理、污泥处理等

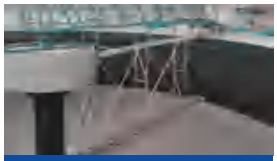
**多工况**
运行环境多变

**多工艺**
可扩展支持
多种污水处理工艺

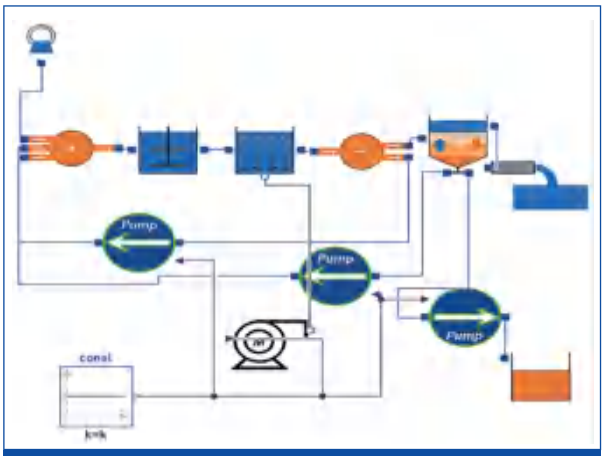
## 污水处理厂系统和工艺流程

### 污水处理厂、设备图和系统模型


污水处理厂全貌

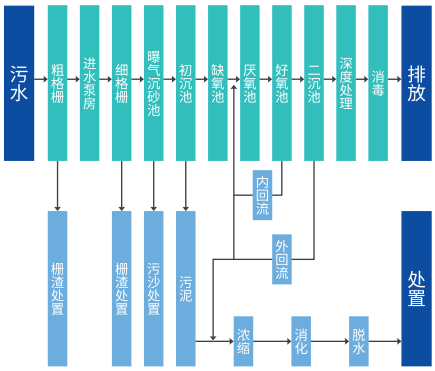

二沉池

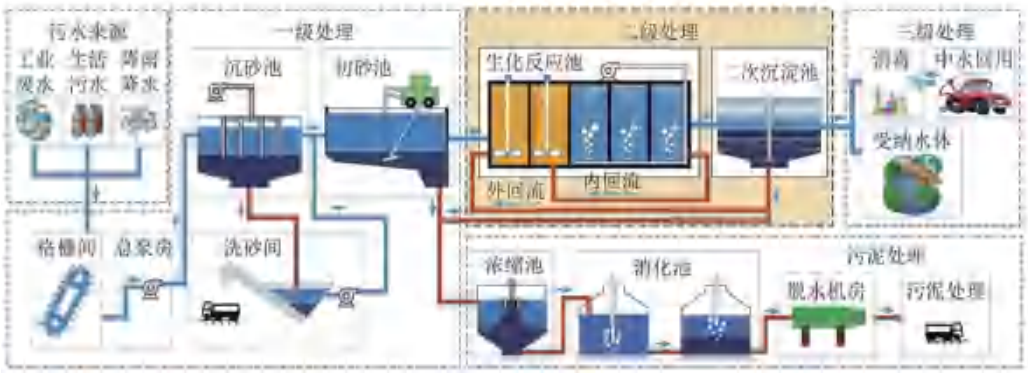

曝气池



系统模型

### 工艺流程



UWNTEK
打造优秀的控制系统产品

# 管理控制与监测评估系统

## 安全监测评估平台

### 基本介绍

安全监测评估平台由资产识别与漏洞扫描、通用协议模糊测试系统、工控协议模糊测试系统以及综合安全评估系统构成，提供多种安全检测评估工具，实现工控系统网络及设备的漏洞扫描、通用协议及工控协议的漏洞挖掘、工控系统网络的综合评估；支持工控环境的渗透测试和脆弱性发现。

### 核心指标

支持主流工控厂商的工控设备发现与识别，可识别工业资产大于 1000 种；支持漏洞检测数量大于 1000 个；支持对多种通用协议的安全检测；支持对 35 种工业控制协议的模糊测试功能。

### 特色亮点

支持 PPI 协议、MPI 协议、ProfiBus 协议等串口协议的模糊测试；支持 ProfiNet 协议、S7comm_Plus、UMAS 协议等网络协议的模糊测试；支持电力、石化主流 DCS 系统协议的分析测试，覆盖率 90% 以上；支持导入未知协议数据包样本，开展未知协议逆向分析，生成测试用例，实现未知协议的全过程闭环测试。

### 应用场景

目标场景的资产识别与漏洞扫描；工控设备协议的模糊测试及漏洞挖掘；目标场景的综合安全评估。

## 红蓝演练平台

### 基本介绍

信息安全红蓝演练系统提供了演练靶场平台，通过虚拟化平台构建上层拓扑网络，并物理接入控制系统，与数字孪生模型连接，一同构建仿真环境，可开展知识训练、技能训练、比武竞赛、实战演训、渗透测试、安全评估、技术验证等活动，实现学、练、赛、训、评全流程的统一管理，全面提高人员及机构的网络安全意识、防护水平和实战能力。

### 核心指标

支持 300 人以上的红蓝演练；支持调度组件资源进行场景虚拟化搭建以及创建剧情任务进行协同工作；支持对场景配置的保存、配置文件的生成和版本控制；支持从多个维度对攻击效果和防御效果进行评估。

### 特色亮点

工控安全事件场景复现，涵盖 ATT&CK 矩阵数十种攻击方式，采用虚拟化与物理环境结合的方式构建场景，真实反映攻击效果。

### 应用场景

人员安全培训；重大工控安全事件复现；举办工控安全比赛；安全演练与红蓝对抗。

## 新一代工业控制系统信息安全大型实验装置**其他测试环境**

| 名称 | 型号 | 规格 |
|---|---|---|
| **控制系统功能 / 性能测试实验室** | | |
| 静电放电抗扰度测试系统 | EMC-Partner | 符合 IEC 61000-4-2 |
| 瞬态抗扰度测试系统 | EMC-Partner | 符合 IEC 61000-4-4、IEC 61000-4-5、IEC 61000-4-8/-9、IEC 61000-4-11、IEC 61000-4-16。 |
| 射频传导抗扰度测试系统 | Schloder | 符合 IEC 61000-4-6 |
| **数字孪生系统仿真测试实验室** | | |
| 电力电子高精度 FPGA 实时仿真器 | Typhoon HIL 606 | 支持实现 4 台电机或者 8 套通用变流器的高精度实时仿真，最小仿真步长 200ns；实现含风电、光伏、发电机、储能以及多样化负载系统的实时模拟。 |
| **控制系统安全测试实验室** | | |
| 资产识别与漏洞扫描系统 | ELEXTEC | 支持识别 20 款主流工控专用设备；支持常规漏洞扫描；可检测常见应用和服务漏洞；支持主流工业控制设备漏洞扫描；支持 16 种协议弱口令猜测。 |
| 通用协议模糊测试系统 | ELEXTEC | 支持对多种通用协议的安全检测，包括但不限于 FTP、TFTP、HTTP、Telnet、SSH、SNMP、RPC、ICMP、DNS、POP3、SMTP、DHCP 等。 |
| 私有工控协议模糊测试系统 | ELEXTEC | 支持对工业控制系统公开 / 私有协议的模糊测试；支持工控协议种类 >35 种，工控协议测试用例 >200 个；支持对各类私有协议的自定义测试；支持未知协议的全过程闭环测试。 |
| 综合安全评估系统 | ELEXTEC | 支持对工业控制系统搭建过程中的基础配置项进行合法化检查；支持基于漏洞库的安全性评估；支持对工业控制系统边界防护的安全性检查；支持对工业控制系统中的工程师站、数据库、服务器等的访问控制权限进行安全性评估；支持对工业控制系统中所有设备的通用网络服务检查。 |


打造优秀的控制系统产品

UWNTEK

浙 江 大 学
NGICS大平台

公司总部：杭州市余杭经济开发区临港路 6 号
技术中心：浙大优稳控制装备与控制系统研究院
技术支持：400-007-0089
电　　话：0571-88371966
传　　真：0571-88371967
www.uwntek.com
uwntek@uwntek.com

2024 年 11 月版