# 工业控制系统网络安全

黄 辉

360企业安全 安全第一® 企业安全领军者

# CONTENTS目录


PART / 01 工业控制系统简介/组成

PART / 02 工业控制系统网络安全现状

PART / 03 工业控制系统安全理念与防护技术

PART / 04 最新360工控安全

# 大型机械设备

大型机械设备

# 现场设备

- **输入设备 – 测量设备**
  - 仪器仪表
  - 传感器：温感、压感、液位等
- **输出设备 – 执行设备**
  - 开关
  - 阀门

Inputs

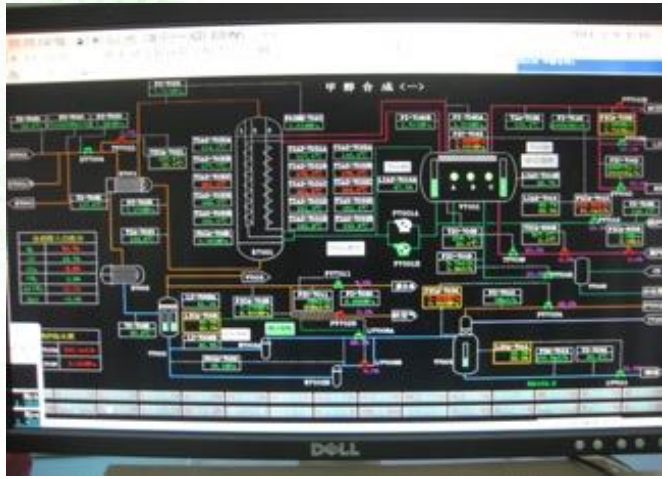
Outputs

# 核心工控系统

西门子840D CNC

西门子S7-300 PLC

LT-CNC GJ301



一个DCS

一个SCADA

# 工业控制系统介绍

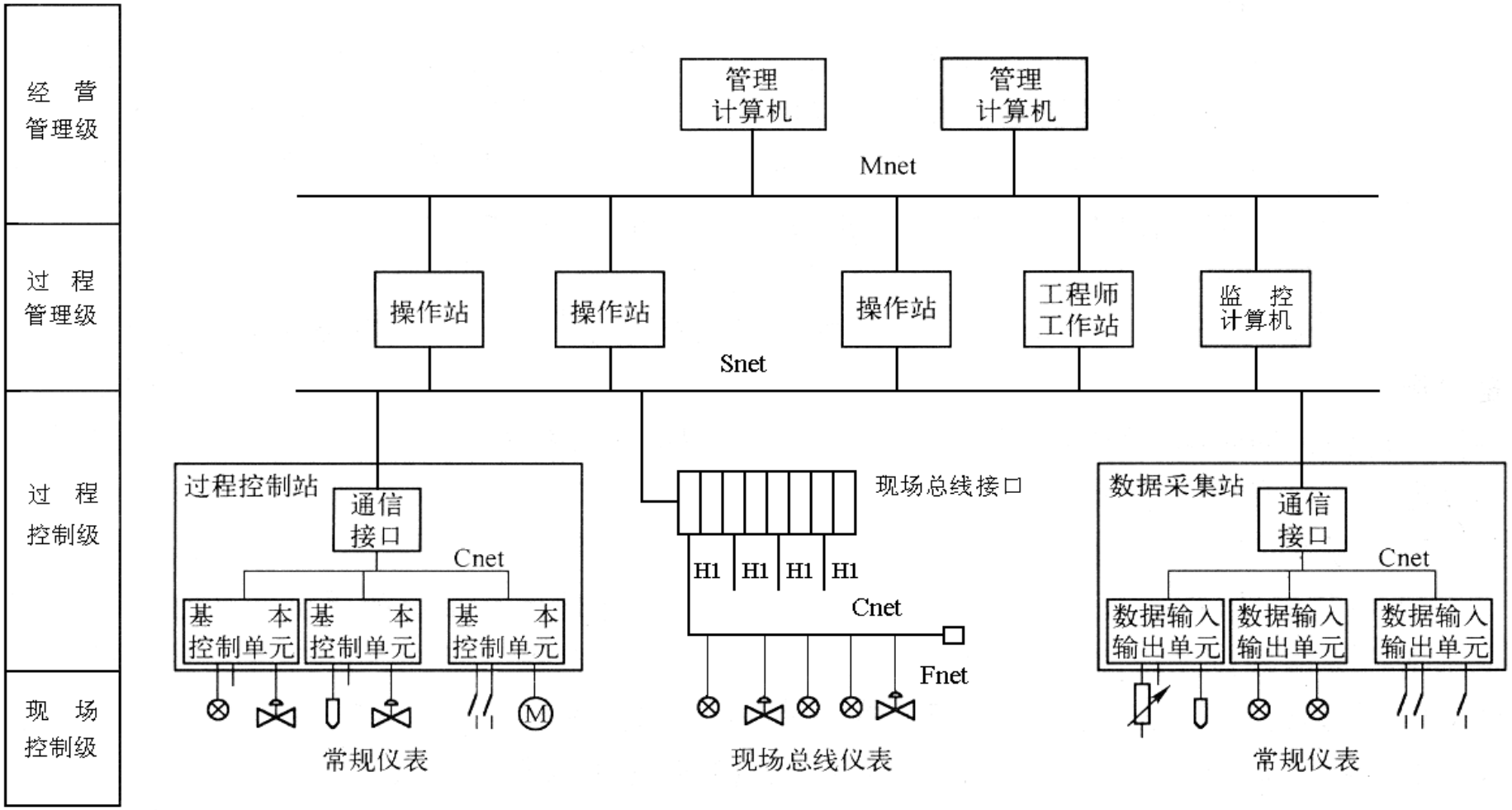
- 工业控制系统ICS（Industrial Control Systems），是由各种自动化控制组件以及对实时数据进行采集、监测的过程控制组件，共同构成的确保工业基础设施自动化运行、过程控制与监控的业务流程管控系统。

# 工业控制系统ICS

工业控制系统（Industrial Control System，ICS）是一个总称，包括以下几种类型：

- DCS（集散控制系统）
- PLC（可编程逻辑控制器）
- FCS（现场总线控制系统）
- SCADA（监控控制与数据采集）
- ISCS（综合监控系统）
- 任何其他自动化控制系统

# 典型DCS系统架构


经营管理级
过程管理级
过程控制级
现场控制级
管理计算机
管理计算机
Mnet
操作站
操作站
操作站
工程师工作站
监控计算机
Snet
过程控制站
通信接口
Cnet
基本控制单元
基本控制单元
基本控制单元
M
常规仪表
现场总线接口
H1
H1
H1
H1
Cnet
Fnet
现场总线仪表
数据采集站
通信接口
Cnet
数据输入输出单元
数据输入输出单元
数据输入输出单元
常规仪表

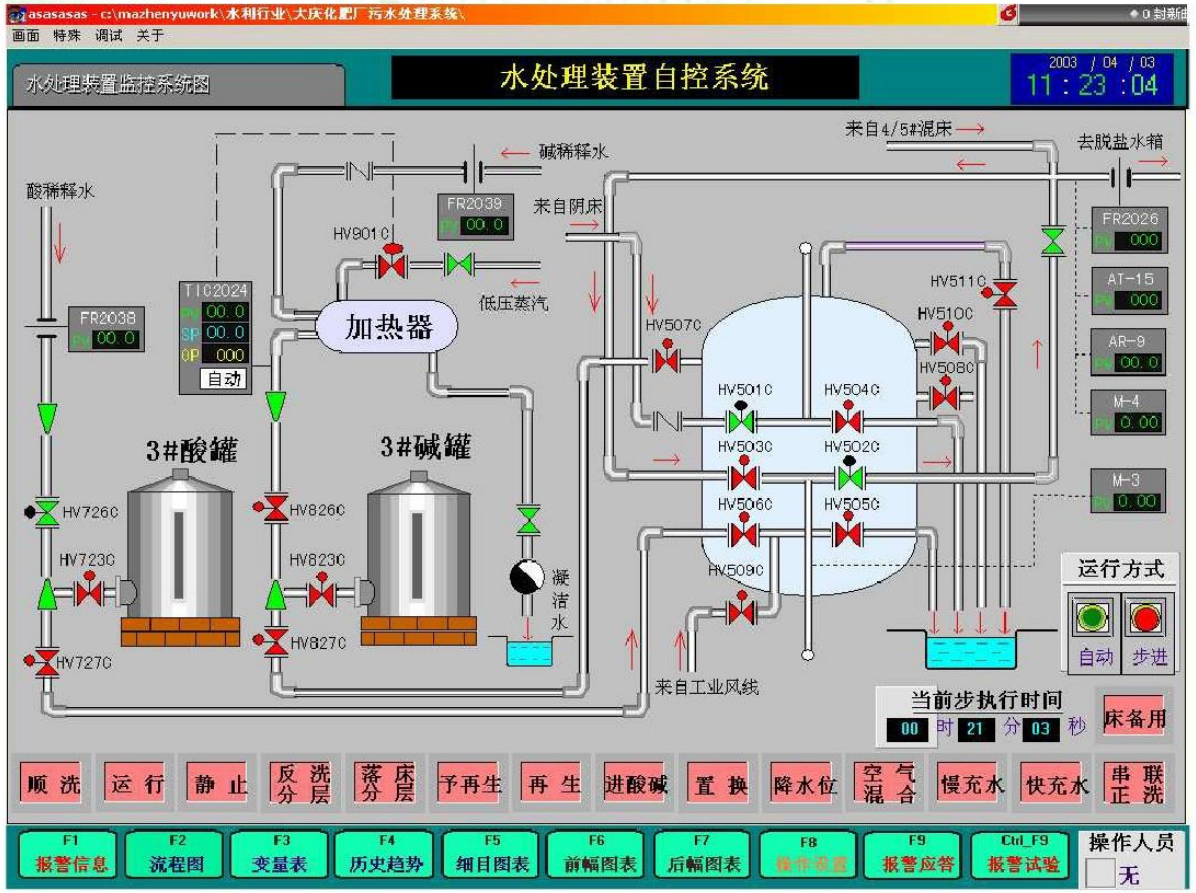
# DCS系统软件编程

360企业安全 安全第一®

**数据采集和I/O数据接口定义**

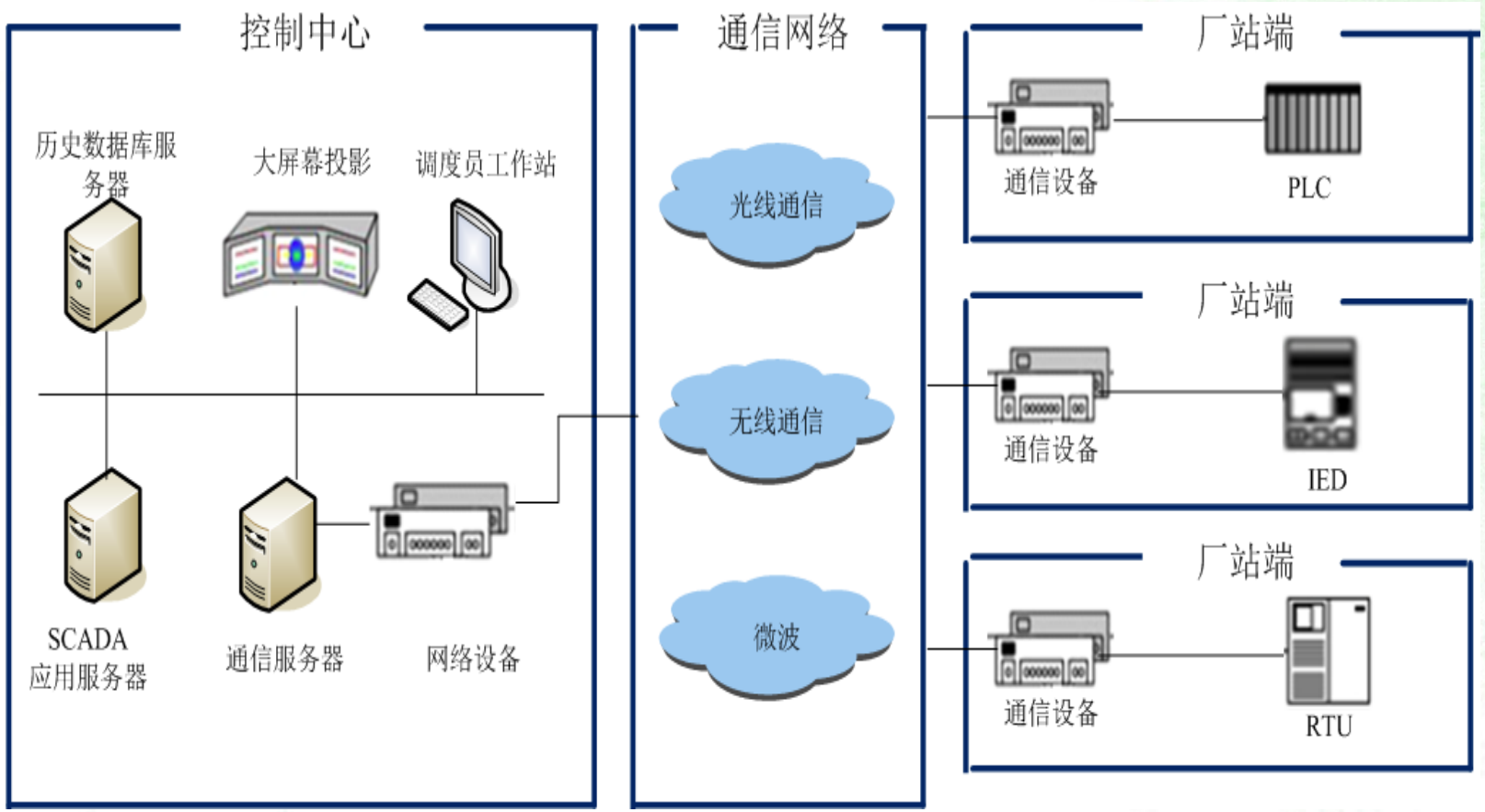
**人机监控界面和监控参数定义**

**过程控制逻辑定义和编程**

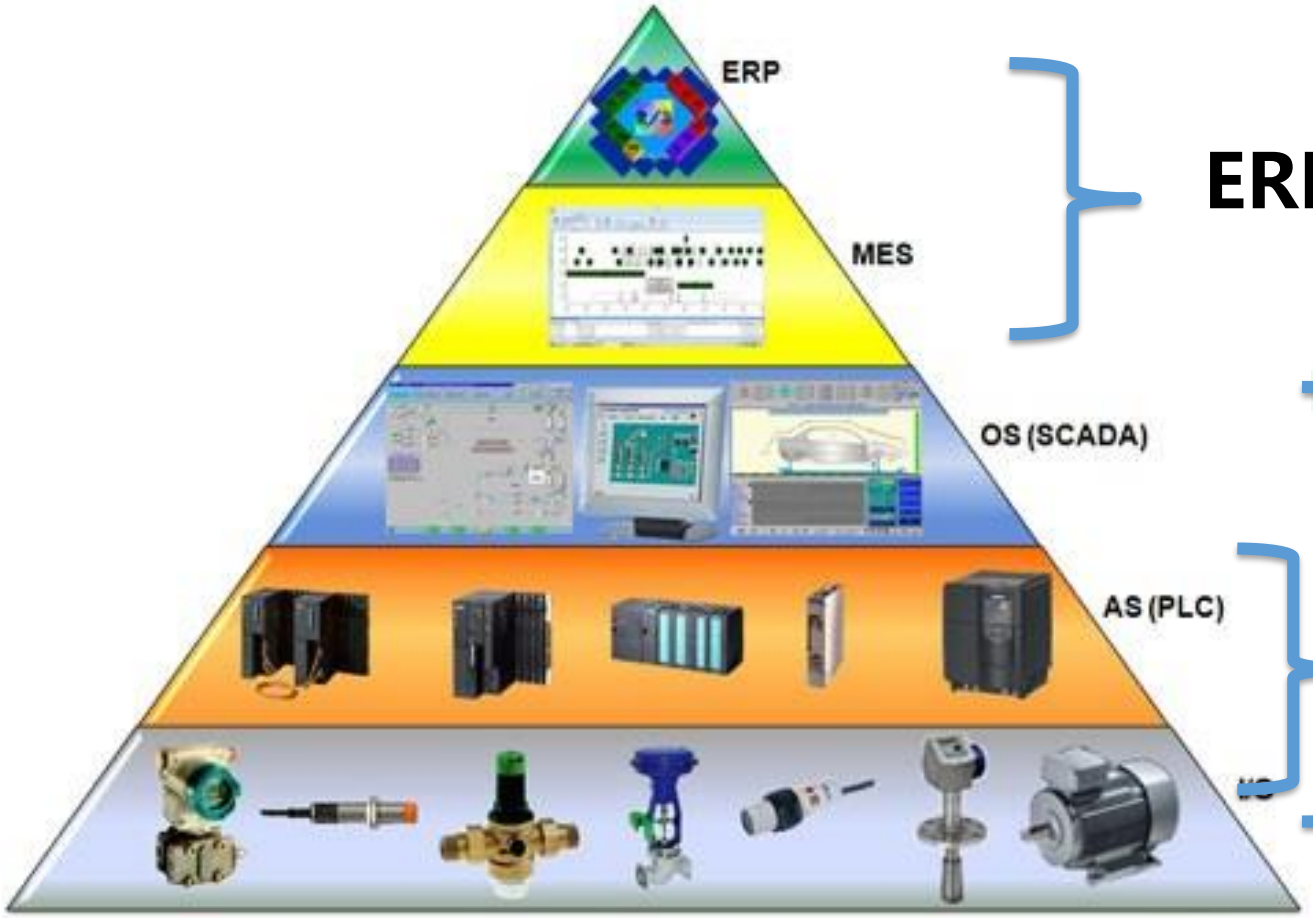


# SCADA系统软件

SCADA系统是一类功能强大的计算机远程监督控制与数据采集系统，它综合利用了计算机技术、控制技术、通信与网络技术，完成了对测控点分散的各种过程或设备的实时数据采集，本地或远程的自动控制，以及生产过程的全面实时监控，并为安全生产、调度、管理、优化和故障诊断提供必要和完整的数据及技术手段。



# 典型工业控制网络结构




ERP（管理系统）

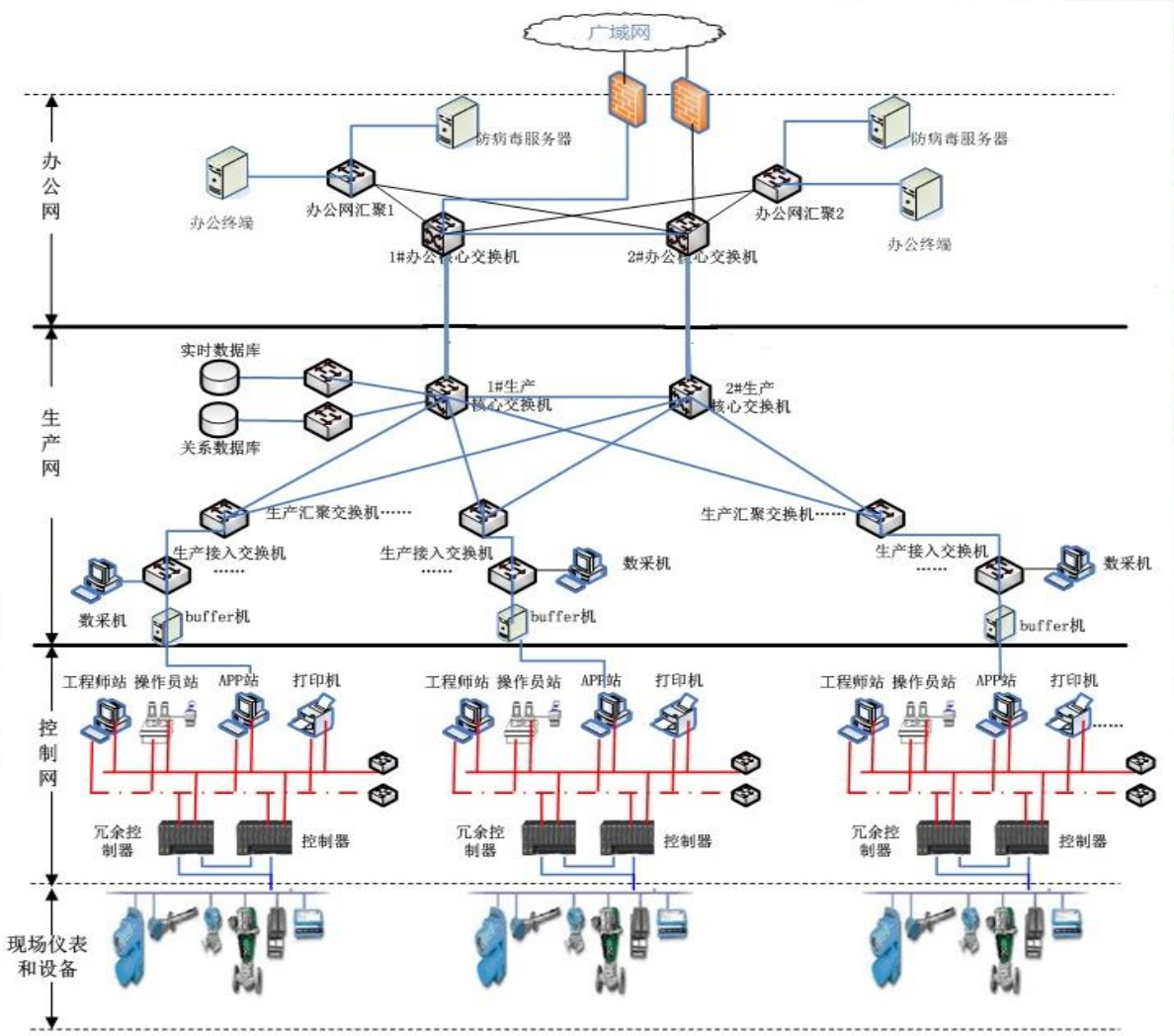
DCS控制系统

FCS控制系统

管控一体化系统

# 典型工控系统架构

- 办公网
  - 包括ERP等应用系统，从实时数据库读取数据
- 生产网
  - MES 系 统 区 域，通 过 OPCServer 从 控 制 网 中 采集数据，保存到实时数据库中
- 控制网
  - 现场控制



# 工控系统组件和IT系统对应关系

| | 传统IT部分 | 工控部分 |
|---|---|---|
| 硬件平台 | 终端、服务器、通信设施 | IPC、工业交换机、工业环网、PLC、RS485、RS232、CANBus现场总线 |
| 系统平台 | 通用系统（基本上都是基于windows XP、win7 、 win8 、 windows2003 、 windows2008） | 通用系统（基本上是基于windows XP、win7、windows2000、windows2003） |
| 通讯协议 | TCP/IP、HTTP等通用协议 | 工业协议如： OPC、Profinet/TCP、Modbus、S7、DNP3、IEC103/104、61850、CC-LINK、 |
| 数据库 | 关系数据库Oracle、SQL Server | 实时数据库，Rockwell-RSSQL<br>GE FANUC-iHistorian、PHD |
| 开发环境和语言 | 常见开发语言和工具、C、java、PHP等 | 组态软件RSlogix、RSlinx、WINCC、STEP7、iFIX等、LAD、FBD、SL、ST、SFC五种编程语言 |
| 应用软件 | IT应用系统 | 工业控制系统 |

# 工控系统和IT系统的差异

| 类别 | IT系统 | 工控系统 |
| --- | --- | --- |
| 性能需求 | ●非实时通信<br>●响应一致性<br>●高吞吐量<br>●允许存在延迟和抖动 | ●实时通信<br>●响应的时间关键性<br>●中等吞吐量<br>●不允许存在延迟和抖动 |
| 可用性需求 | ●允许重启系统<br>●以系统的功能需求为主，可用性居其次 | ●不允许重启系统<br>●高可用性需求，部署前需要详尽的测试<br>●需要冗余系统<br>●中断等操作需要提前计划 |
| 风险管理需求 | ●数据的保密性和完整性是第一位的<br>●容错性是次要的—短暂停机不是主要风险<br>●主要风险是商业运作的影响延迟 | ●人的安全保护放在第一位，其次是控制过程的保护<br>●容错是必不可少的，任何停机都是不能接受的<br>●主要风险是经常性的不合规定、环境影响、人身伤亡、设备及生产损失 |

# 工控系统和IT系统的差异

| 类别 | IT系统 | 工控系统 |
| --- | --- | --- |
| 结构安全焦点 | ●重点是保护IT资产、信息存储和传播<br>●中央服务器需要更多保护 | ●首要目标是保护系统边际设备，如过程控制现场设备<br>●中央服务器同样需要保护 |
| 非预期后果 | ●安全解决方案都是围绕典型的IT系统设计的 | ●安全工具必须在与现场类似的ICS系统上进行严格地线下测试，确保其上线后不应影响正常的ICS运作 |
| 资源约束 | ●系统需要有足够的资源来支持第三方的安全解决方案应用加入 | ●系统是以特定工业过程为目标设计的，没有足够的内存及其他计算机资源来支持增加的安全功能 |
| 时间关键性作用 | ●应急事件处理不是关键<br>●按等级划分的严格访问控制 | ●对人和其他应急事件的响应非常关键<br>●ICS的访问需要严格控制，但不应阻碍和干扰人机交互 |
| 系统操作 | ●依托典型的操作系统设计<br>●升级可以通过自动进行 | ●一般使用无内置安全功能的专有操作系统<br>●由于控制算法或添加、移除硬件所做的软件变更一般有软件供应商进行专门处理 |

# 工控系统和IT系统的差异

| 类别 | IT系统 | 工控系统 |
| --- | --- | --- |
| 通信 | ●标准通信协议<br>●主要是包含无线网络接入的有线网络<br>●典型的IT网络实施方法 | ●很多专有和标准通信协议<br>●多种通信媒介，包括专用线和无线(无线电和卫星)<br>●网络复杂，需要具有专门知识的控制工程师 |
| 软件变更管理 | ●软件变更在当前完备的安全策略和过程中容易实现，变更过程通常是自动的 | ●需变更的软件需要完整的测试并进行增量部署，以确保控制系统的完整性<br>●故障处理必须制定详尽的计划<br>●ICS可能使用厂商已经不再进行技术支持的操作系统 |
| 管理支持 | ●允许多种支持方式 | ●服务支持往往仅通过单一供应商 |
| 生命周期 | ●一般为3~5年 | ●一般为15~20年 |
| 组件访问 | ●组件通常部署在本地并易于接入访问 | ●组件被隔离部署在远处，需要多方面的物理支持才能够访问 |

# CONTENTS目录


PART / 01 工业控制系统简介/组成

PART / 02 工业控制系统网络安全现状

PART / 03 工业控制系统安全理念与防护技术

PART / 04 最新360工控安全

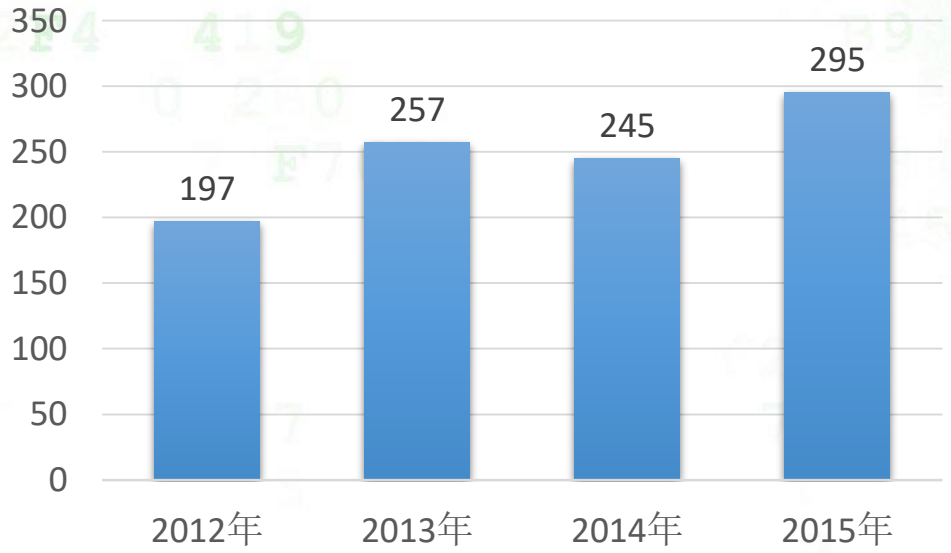
# 全球工控信息安全态势

**工业控制网络安全事件在近几年呈现稳步增长的趋势，2015年被ICS-CERT收录的攻击事件达到295件**

工控漏洞及相应的工控产品统计

| | 2012年 | 2013年 | 2014年 |
|---|---|---|---|
| 工控漏洞报告 | 147 | 181 | 167 |
| 涉及的工控产品 | 343 | 285 | 362 |

工业控制网络安全事件在近几年呈现增长趋势



# 全球工控信息安全态势

## 工业控制网络安全事件呈逐年增加趋势

## 工控网络安全成为各国网络空间主战场和反恐新战场：

- 美国、欧盟等增加预算抵抗日益升级的网络威胁
- 恐怖主义威胁渗透到工业控制系统，关键基础设施成为主要攻击目标
- 国防网络化和反恐网络化将把工控网络安全领域的对抗提升为国家核心竞争力

**2001年** 黑客侵入监管加州电力传输系统的独立运营商

**2003年** 美国俄亥俄州核电厂控制网络内的计算机蠕虫所感染

**2006年** 美加电网大停电事故　国内某电网停电事故

**2008年** 黑客劫持南美洲的电网控制系统，敲诈政府

**2010年** 伊朗核电站举世闻名的“震网”事件

**2014年** 西班牙智能电表被爆存在高危漏洞

“HaveX” 导致多家能源企业单位被感染，信息泄露

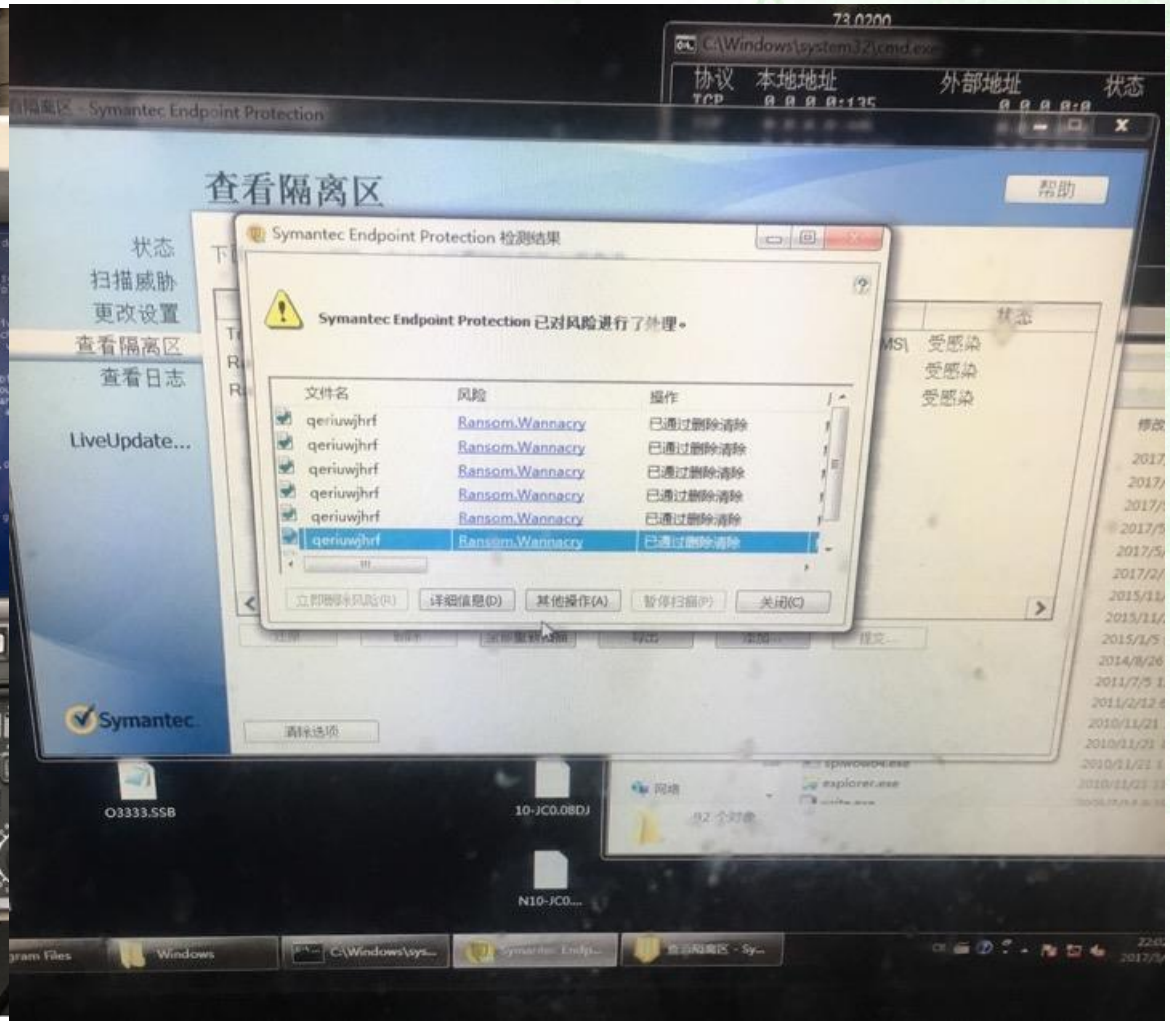
**2015年** 乌克兰电网BlackEngery病毒

**2016年** 德国核电站负责燃料装卸系统遭恶意程序攻击

乌克兰最大机场遭网络攻击

**2017年** 永恒之蓝肆虐全球，工控系统也遭受攻击

# 永恒之蓝




5月下旬在某央企，智能制造车间，数控系统受永恒之蓝影响蓝屏，影响生产！

# 我国工控网络安全现状

- 2000年10月13日，四川二滩水电厂控制系统收到异常信号停机，7秒甩出力89万，川渝电网几乎瓦解。
- 2003年12月30日，龙泉、政平、鹅城换流站控制系统发现病毒，外国技术人员在系统调试中用笔记本电脑上网所致。
- 2010年青岛某炼化厂因感染蠕虫病毒，导致控制设备中断工作，致使企业停产。后西门子厂商对系统进行了大规模升级，并更改了原先的网络结构。
- 2011年11月，深圳蛇口线多趟列车**暂停运行**，造成大量乘客被迫多次换乘，并滞留在沿线车站。深圳地铁运营方称因不明信号干扰，列车启动自动防护功能，自动防护会导致列车无法高速行驶
- 2015年国内某军工企业采购的国外某品牌数控机床设备运入某秘密基地生产时无法开机，后发现该机床中植入了GPS芯片，可根据定位远程锁定机床。
- 2015年6月 中石化“内鬼”事件，系统内部技术人员，通过提供给中石化华东公司的SCADA系统（油管监控系统）对应开发了一套病毒程序，病毒爆发导致系统无法运行

# 各国工控信息安全发展情况

| 国别 | 国家政策 | 监管部门 | 法律法规 | 标准规范 |
| --- | --- | --- | --- | --- |
| 美国 | 1.2003年《网络空间安全国家战略计划》；<br>2.2006年“国家基础设施保护计划”；<br>3.2010年“控制系统安全计划（CSSP）”； | 美国国防部、国土安全部、能源部、国家标准局、审计署和财政部、ICS-CERT等。 | 1.2013年“国家赛博安全和关键基础设施保护法案”；<br>2.2015年第二版网络战略报告； | 1.2014 年 ISA/IEC62443 工业自动化和控制系统（IACS）系列标准；<br>2.NIST SP800-82工业控制网络安全指南； |
| 欧盟 | 1.2005年的《保护信息时代社会安全战略》<br>2.2013 年“欧洲关键基础设施保护项目（EPCIP）”；<br>3.2013年《关键基础设施保护计划》； | 欧洲委员会、欧洲高级议会、欧洲对外行动处、欧洲防务局、欧洲网络犯罪中心和欧洲标准机构、欧洲网络应急响应组CERT-EU等。 | 1.2013年《欧盟网络安全战略》<br>2.2014年《Certification of Cyber Security skills of ICS/SCADA professionals》； | |
| 日本 | 1.2013年《网络安全战略》（2015年5月25日更新）； | 2015年日本成立内阁网络安全中心 | | |
| 新加坡 | 1.新加坡2014年《国家网络安全总体规划》 | 2015年新加坡成立网络安全局 | | |
| 印度 | 1.印度2013年《国家网络安全政策》； | | | |

# 工控行业合规

**《国家网络安全法》**
关键基础设施安全，自2017年6月1日起施行

**《习总书记在4.19讲话》2016年**
网络安全和信息化工作座谈会上讲话

**网络安全等级保护2.0**
物联网、大数据、云计算、移动互联、工业控制系统

**电力14号令和36号文**
《电力监控系统安全防护规定》《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》

**产品类标准**
工业控制系统安全检测类、保护类、审计类、管理类产品在编，国标

**工信部451号文 2011年**
《关于加强工业控制系统信息安全管理的通知》

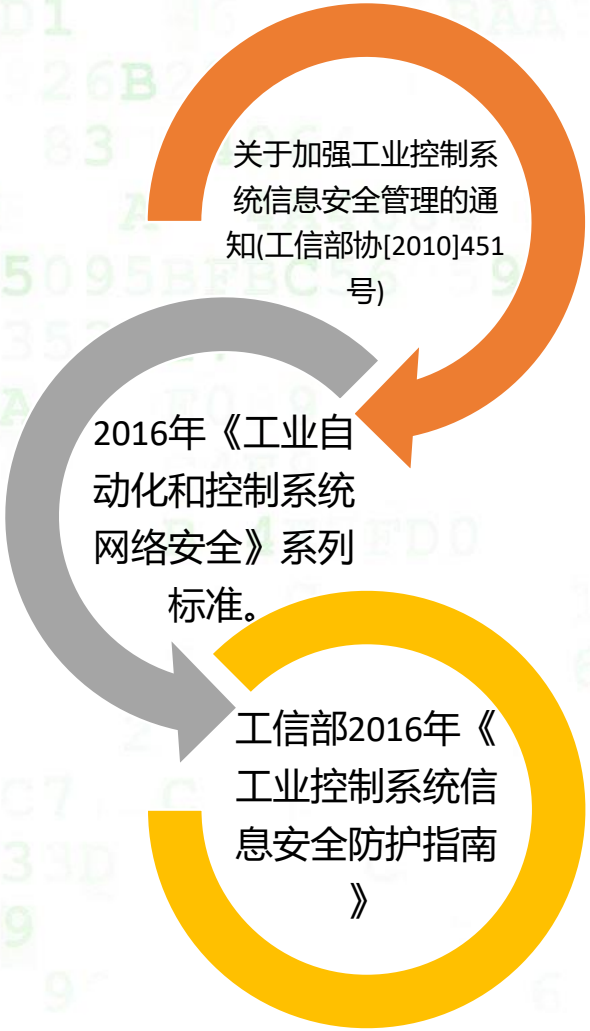
**工信部338号文 2016年**
《工业控制系统信息安全防护指南》

**工信部188号文 2017年**
《工业控制系统信息安全防护能力评估工作管理办法》

**国家网信办 2017年**
《关键信息基础设施安全保护条例（征求意见稿）》

**国家网信办等四部委 2017年**
《网络关键设备和网络安全专用产品目录（第一批）》

# 工业控制系统信息安全防护指南




**《工业控制系统信息安全防护指南》**
技术实现2016年10月

**安全软件：**工业主机上采用白名单方式的防病毒及恶意软件

**边界防护：**在工控网络同企业网，企业网同互联网间边界防护

**安全检测：**在工控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

**主机物理安全：**拆除或封闭工业主机上不必要的USB、光驱接口

**访问安全：**审计工业控制系统主机访问日志

# CONTENTS目录


PART / 01 工业控制系统简介/组成

PART / 02 工业控制系统网络安全现状

PART / 03 工业控制系统安全理念与防护技术

PART / 04 最新360工控安全

# 工业互联网内涵

**定义**

工业互联网是满足工业智能化发展需求，**低时延、高可靠、广覆盖**的关键**网络**基础设施，是新一代信息通信技术与**现代**工业深度融合所形成的**新兴业态与应用模式**

新一代信息通信技术　　现代工业

深度融合

工业互联网

**新兴业态**

工业云服务　　工业大数据服务

新型工业APP

**新应用模式**

智能化生产　　网络化协同

服务化延伸　　个性化定制

# 体系架构：网络是基础、数据是核心、安全是前提

360 企业安全 安全第一®

**数据**

**数据智能在工业中的全周期应用**，包括“采集交换-集成处理-建模分析-决策与控制”，形成优化闭环，驱动工业智能化。

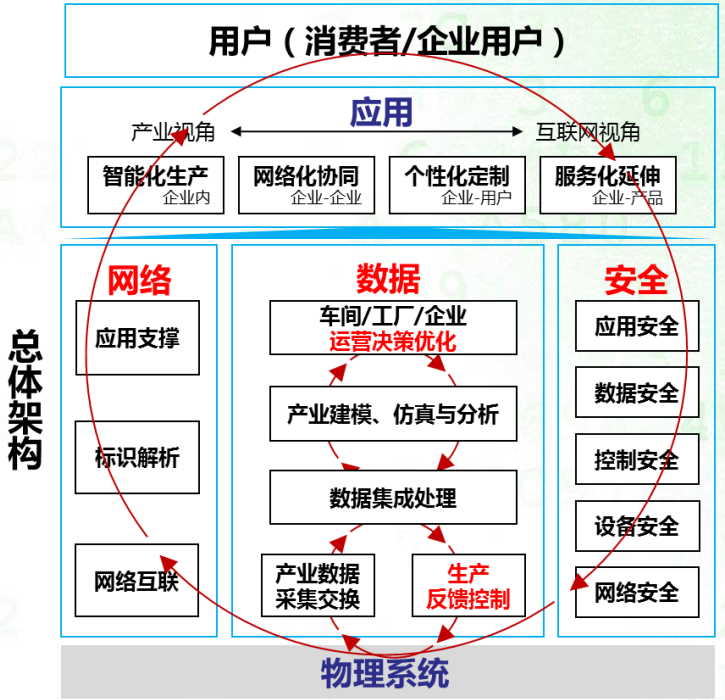
**网络**

**实现数据智能的网络基础**，包括网络互联、标识解析、应用支撑三大体系。

**安全**

工业/产业互联网各个领域和环节的**安全保障**，包括设备安全、控制安全、网络安全、应用安全等。

**工业互联网体系架构**

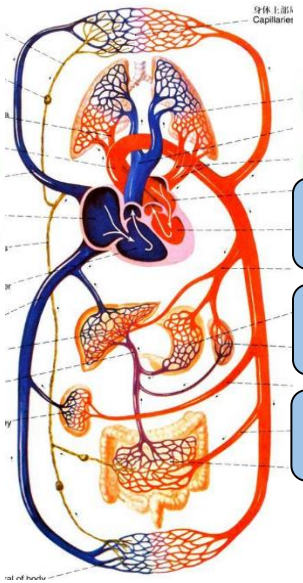



来源：《工业互联网体系架构白皮书》

# 工业互联网的三大关键要素

360企业安全 安全第一®

## 血液循环系统

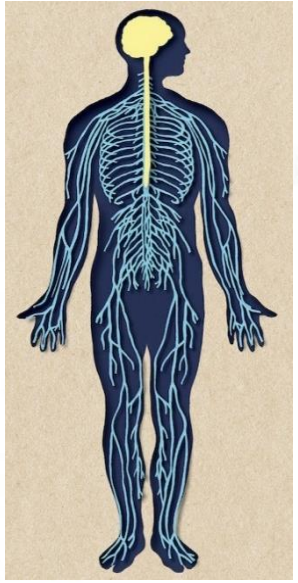


支撑作用

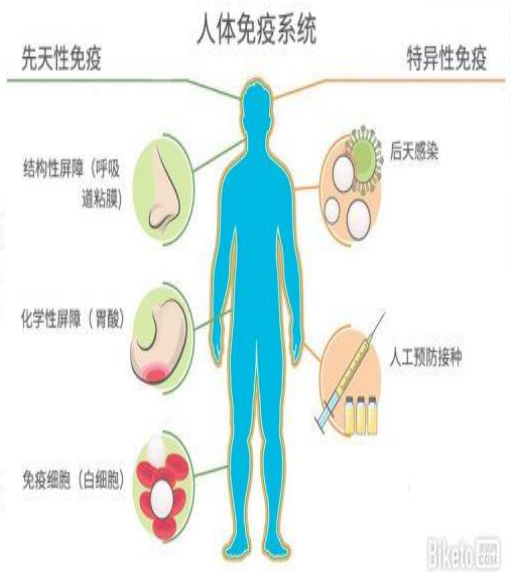
驱动作用

引领作用

## 神经控制系统



## 免疫防护系统




**网络**

全系统、全流程、全产业链、全生命周期的网络连接

**数据+平台**

工业互联网平台及基于平台的大数据分析服务成为智能优化决策的核心

**安全**

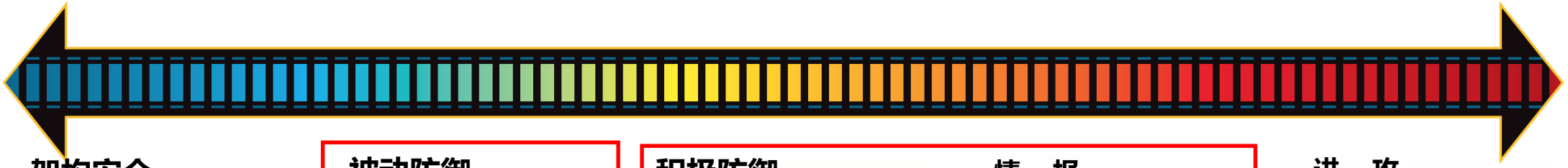
同步构建设备、网络、控制、应用和数据的安全保障，

**工业网络安全是生产安全的核心保障**

# 工业信息安全发展思路

360 企业安全 安全第一®

## 滑动窗口模型



### 架构安全

安全评估
等保评估
渗透测试

**ARCHITECTURE**

The planning, establishing, and upkeep of systems with security in mind

### 被动防御

自动化、层次化安全体系建设：

- 网络安全防护
- 主机安全防护
- IoT安全防护
- 统一安全防护

**PASSIVE DEFENSE**

Systems added to the Architecture to provide reliable defense or insight against threats without consistent human interaction

### 积极防御

安全大数据平台
态势感知
云端威胁情报自动化应用体系
事件分析
安全协同

**ACTIVE DEFENSE**

The process of analysts monitoring for, responding to, and learning from adversaries internal to the network

### 情　报

威胁数据源采集
威胁情报生产
威胁情报验证
威胁情报分发体系

**INTELLIGENCE**

Collecting data, exploiting it into information, and producing Intelligence

### 进　攻

法律手段
反制

**OFFENSE**

Legal countermeasures and self-defense actions against an adversary

# 工业信息安全发展思路

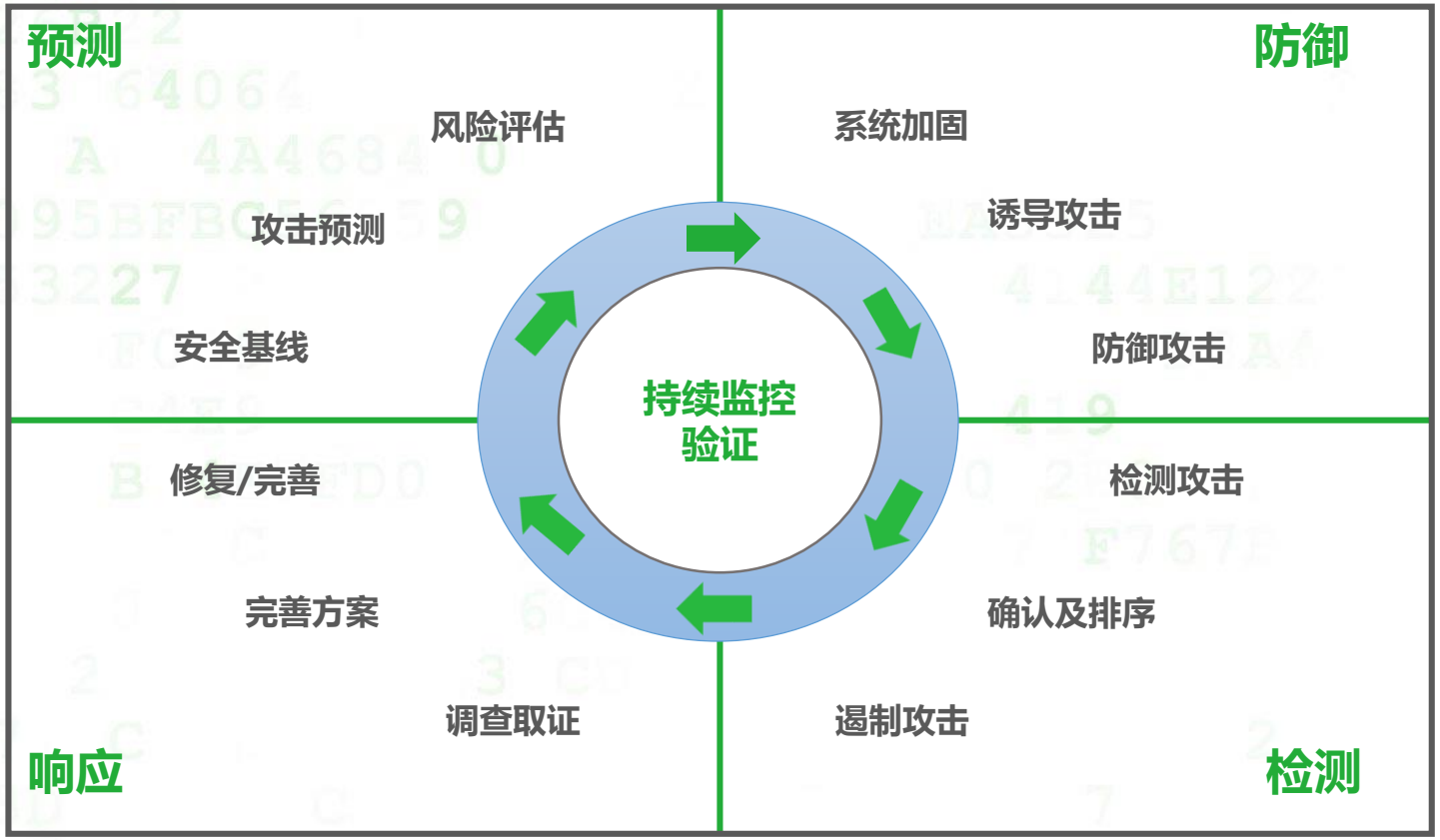
360 企业安全 安全第一®

**3**

借助新技术手段预先发现

**2**

迅速理解问题原因和影响，并作处理




**4**

快速干预防御策略，防止损害扩大

**1**

发现那些真正需要处理的问题

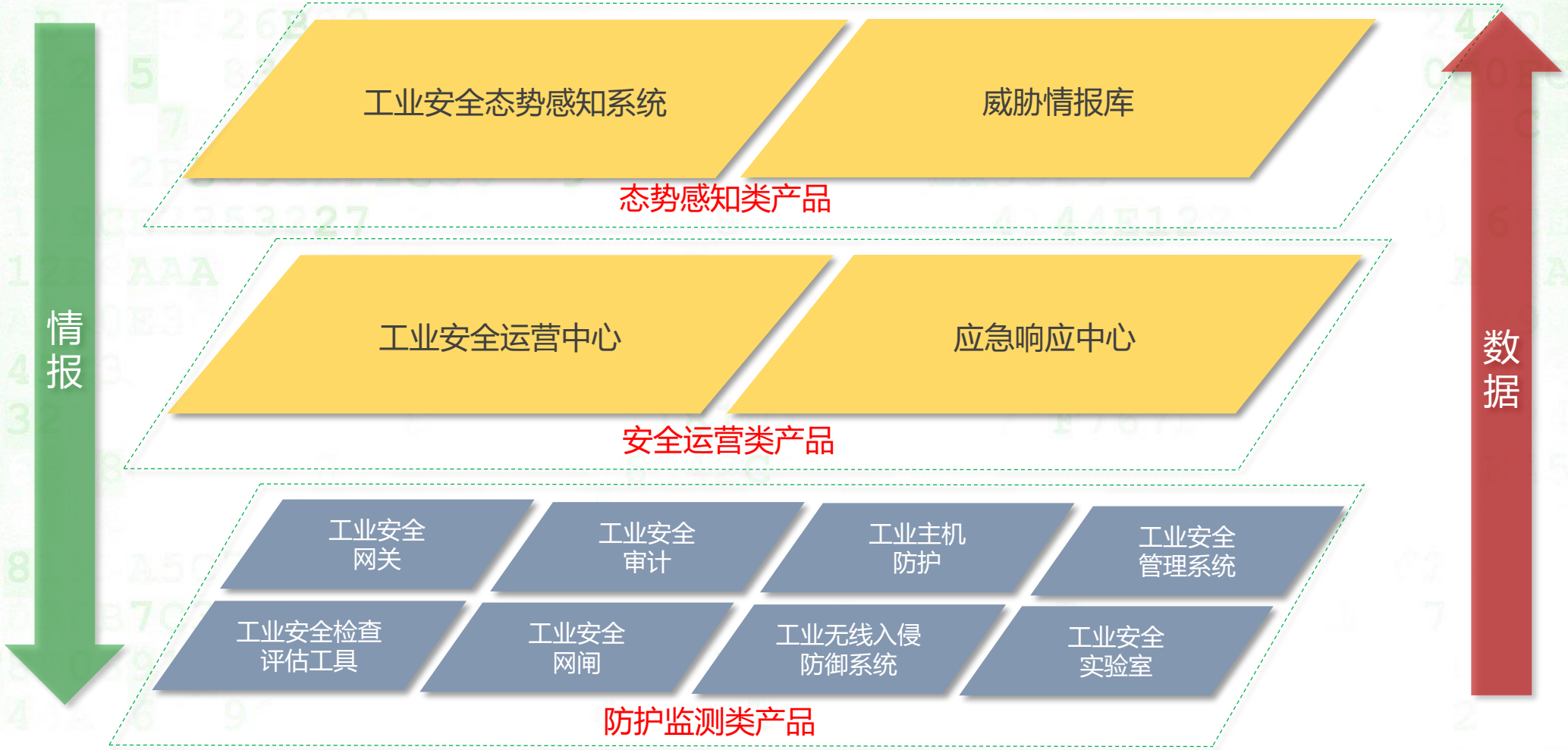
**核心** 全方位,不间断的对网络、系统进行监控

# 工控安全防护能力建设

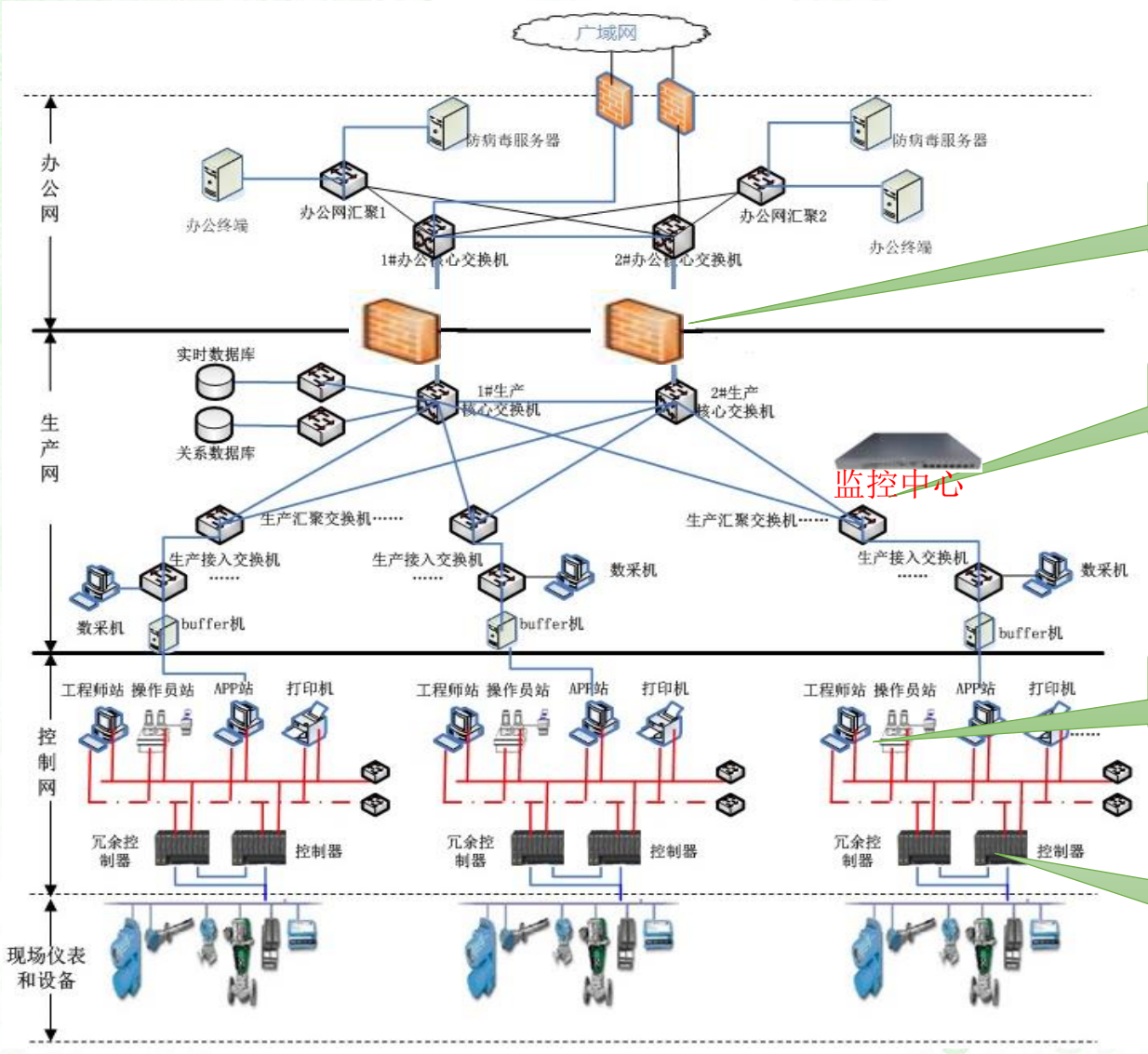
360 企业安全 安全第一®

| 技术防护能力 | | | 人员与机制 |
|---|---|---|---|
| （1）物理环境安全 | 物理安全和制度体系建设 | | 安全制度 |
| （2）安全策略与流程 | | | |
| （3）安全层域划分 | 区域隔离和控制 | 异常流量和行为分析 | 人员组织、制度体系、安全建设 |
| （4）部署安全防护方案 | 漏洞安全管理 | 风险分析和威胁评估 | |
| （5）系统安全加固 | 工控安全监控审计 | 工控安全入侵防护 | |
| （6）应用安全管理 | 应用数据安全加固 | 终端安全白名单环境 | |
| （7）终端安全加固 | | | |
| （8）持续性风险管理 | 威胁态势感知、统一运维管理数据分析 | | 应急响应、风险处置、应急演练 |

# 工业信息安全落地防护


情报
数据
工业安全态势感知系统
威胁情报库
态势感知类产品
工业安全运营中心
应急响应中心
安全运营类产品
工业安全
网关
工业安全
审计
工业主机
防护
工业安全
管理系统
工业安全检查
评估工具
工业安全
网闸
工业无线入侵
防御系统
工业安全
实验室
防护监测类产品

# 工控安全领域关键技术与防护




## 关键技术

- 边界隔离
- 威胁监测
- 终端防护
- 漏洞挖掘

纵深防御

## 主要防护功能

- 阻止网络非授权访问
- 阻止网络层网络攻击
- 发现APT等网络攻击
- 发现病毒传播
- 发现生产安全异常
- 支持取证分析
- 防止终端病毒

# 工业控制安全网关-产品介绍

360企业安全 安全第一®

## 产品定位

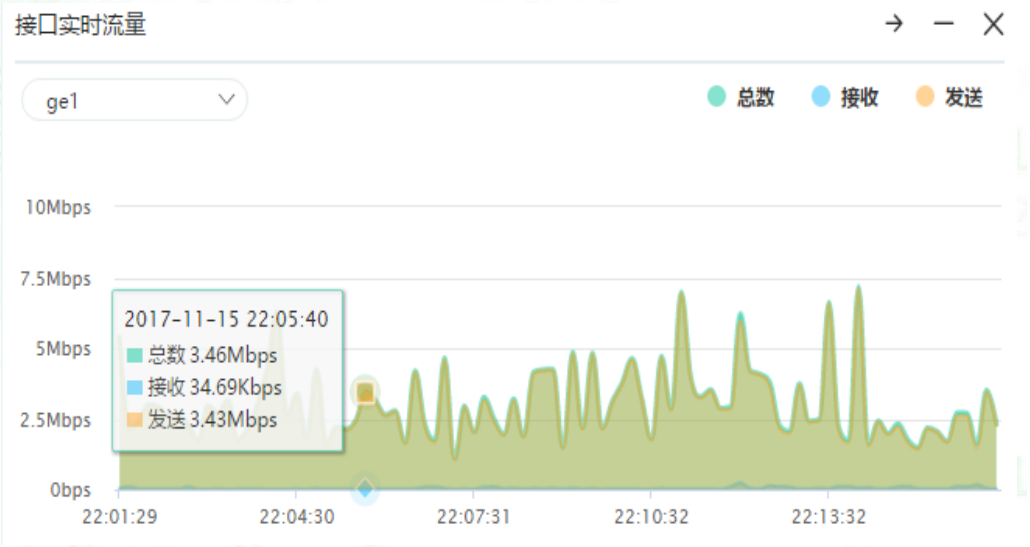
- 工控系统专用、高可靠性防火墙
- 阻止来自防止安全域内的攻击扩散
- 管理信息网的威胁

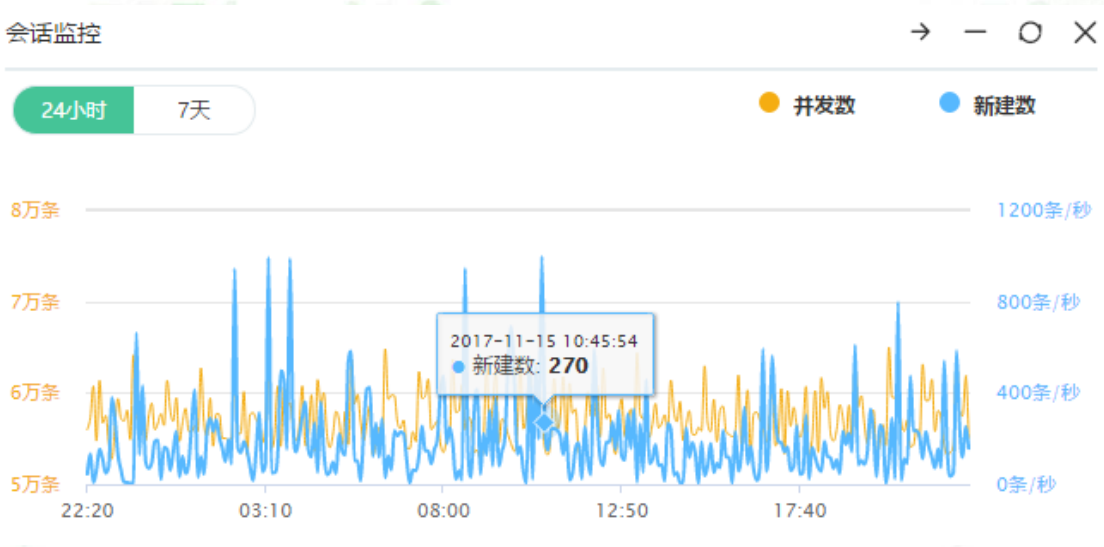
## 产品特点

- 基于既有防火墙平台开发，可靠性增强，质量稳定
- OT、IT流量深度识别与解析
- 白名单智能学习

1. 三段式工作模式
2. IT、工业协议深度数据包解析
3. 白名单智能学习
4. 多维度一体化安全策略
5. 防病毒、入侵防御等威胁防护
6. 丰富的路由功能
7. 文件防泄漏
8. 流量可视化展现

# 工业控制安全网关-全面风险信息展示及分析

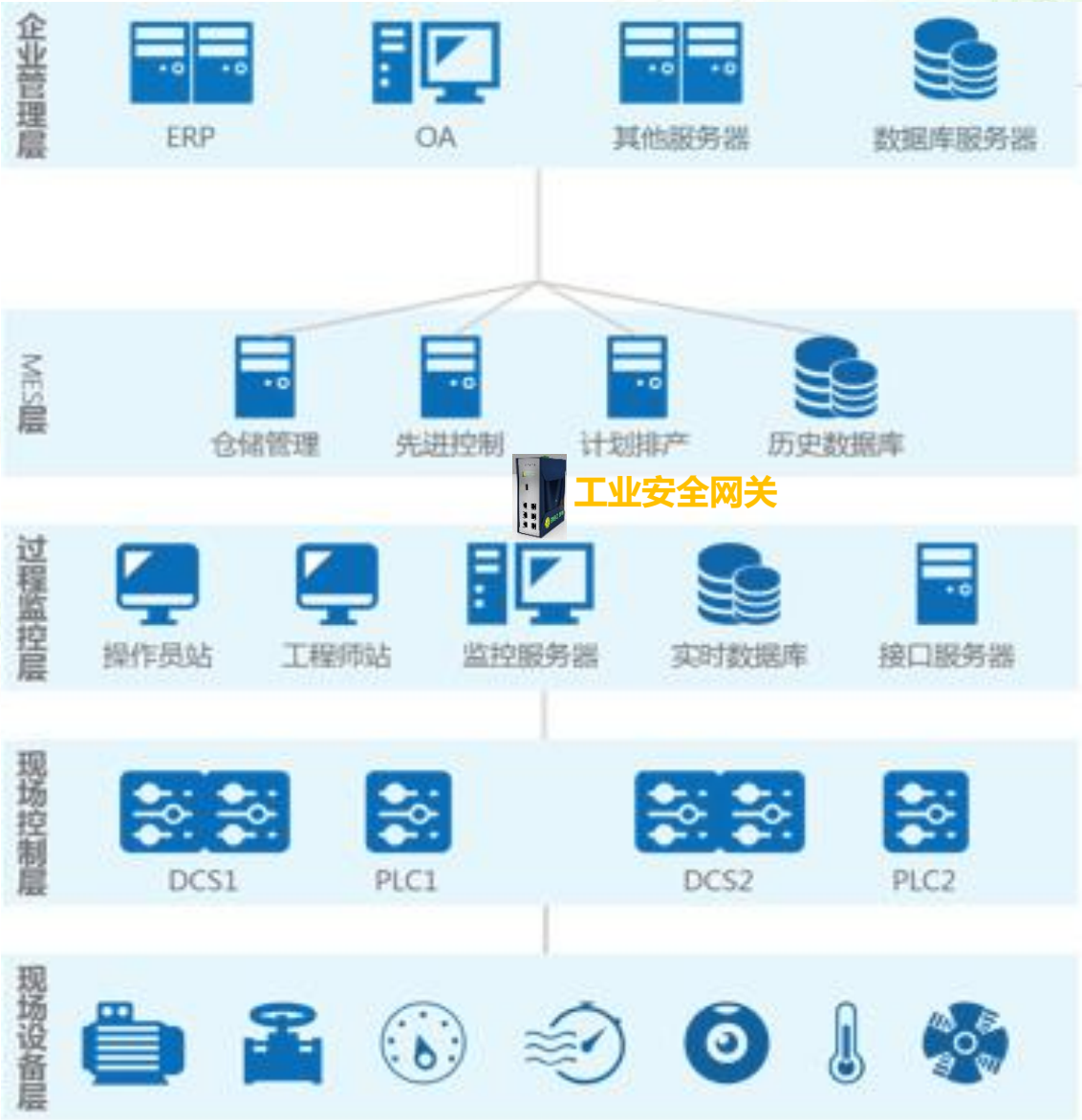


# 工业控制安全网关-产品应用

**MES、监控与现场控制间：**

- 白名单（OPC）防护
- 威胁检测
- 安全策略过滤
- 攻击防护
- 流量及日志审计



# 工业安全审计平台

- **产品定位**
  - 监控并记录工业控制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**
  - 对工业网络“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**

忠实记录通讯协议通信记录，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**

识别并检测通讯协议攻击、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、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

# 工业安全检查评估工具-产品介绍

工业安全检查评估工具是一款应用于工业互联网（IT/OT）安全检查，风险评估，等保测评的一款软硬一体便携式设备。主要功能有工控项目管理、工控合规性检查、工控资产发现、工控漏洞扫描、工控协议深度解析、工控流量分析、安全事件统计、威胁情报分析、行为日志审计、协议流量分析、报告自动生成等功能。

- **产品名称：**工业安全检查评估工具（工业互联网威胁感知系统）
  （360网神新一代威胁感知系统）

- **产品定位：工业 安全 检查 评估 工具**

➢ 工业：应用于工业环境；
➢ 安全：专注于安全领域；
➢ 检查&评估：用于检查和评估，符合行业标准和等保规范；
➢ 工具：是一款使用工具产品，方便携带；

# 工业安全检查评估工具-产品功能

360 企业安全 安全第一®

01

**工控合规性检查**

工控安全检查指引（网安）、工控安全防护能力评估方法（工信）、电力监控系统安全防护总体方案（电力36号文）等合规性检查，自动生成，整改建议，报告导出。

02

**工控资产发现**

工控设备资产发现（西门子PLC、施耐德PLC、罗克韦尔(AB)PLC、通用电气(GE)PLC、三菱PLC），上位机操作系统识别，工控组态软件，数据库资产等。

03

**工控协议解析**

具备主流工控协议的识别/解析能力：Modbus/Tcp、Siemens S7、OPC_DA等。

04

**工控漏洞扫描**

工控漏洞扫描的主要功能是基于被动流量接收扫描，与已发现的工控资产进行特征匹配，发现漏洞。

05

**工控流量分析**

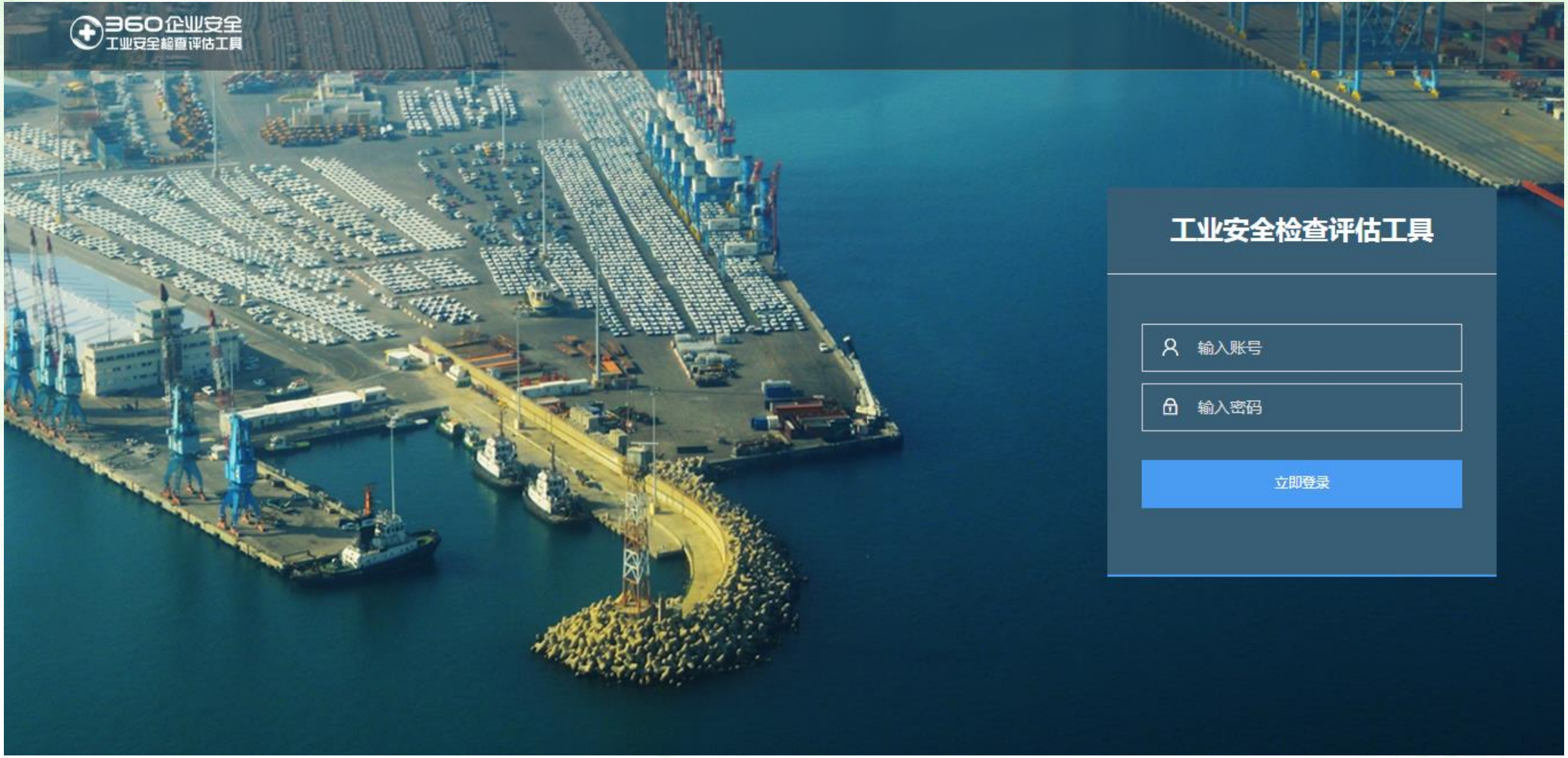
基于工业控制系统的工控协议流量解析，进行流量大小、异常分析，直观展示，根据流量的大小、异常发现问题。

06

**威胁情报检测**

基于威胁情报进行实时流量检测，发现网络中具有威胁进行实时告警，最后生成攻击事件。

# 工业安全检查评估工具-产品功能



# 工业安全检查评估工具-产品功能

360企业安全 安全第一®

360企业安全 工业安全检查评估工具

首页 | 项目管理 | 合规检查 | 资产发现 | 漏洞扫描 | 安全事件 | 威胁情报 | 行为日志 | 分析中心 | 报表中心

57Mbps

360

信息传输、软件和信息技术服...

检测进行中 收起

出口IP

开始时间 2018-04-10 20:27

持续时间 0天13小时34分

累计流量 48.96MB

360

工业安全事件数 0

威胁情报命中数 0

受害主机数 0

行为日志数 0

攻击事件 更多 >

| 序号 | 发现时间 | 威胁级别 | 攻击IP | 受害IP | 检查引擎 | 威胁标签 | 通信协议 | 状态 |
|---|---|---|---|---|---|---|---|---|

暂无数据

受害主机 Top5 更多 >

| 序号 | IP | 主机MAC/网关MAC | 被攻击数 |
|---|---|---|---|

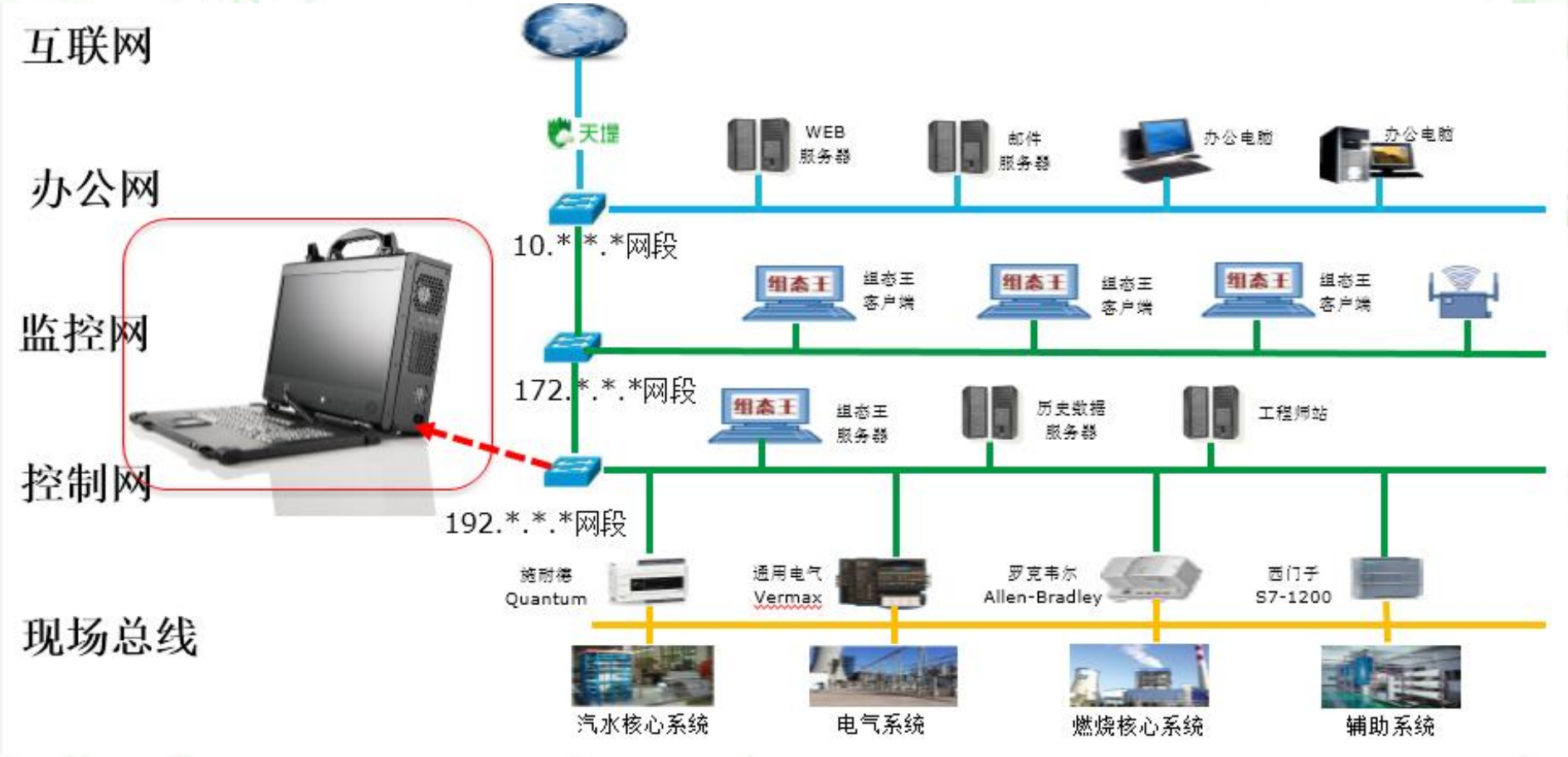
暂无数据

威胁情报命中 Top5 更多 >

| 序号 | 威胁名称 | 威胁类型 | 感染主机数 |
|---|---|---|---|

暂无数据

# 工业安全检查评估工具-产品应用-旁路部署



# 工控安全态势感知

360企业安全 安全第一®

# 工控安全仿真实验室

（1）采用硬件在环仿真测试模式

从“控制系统视角”无法区分控制对象是真实环境，还是虚拟环境；即“控制系统视角”看到的与真实场景高度相似

（2）高仿真

平台以轨道交通为背景，采用沙盘、半实物仿真和软件模拟的方式构建真实、全面的工业场景

（3）覆盖工业系统主要的业务流程。

平台采用目前成熟的和广泛应用的工业控制系统网络结构，包括现场系统层、控制系统层、监控系统层、业务系统层。

（5）模块化

平台的工业场景部分和控制系统部分均采用模块化设计，易于拆卸安装和搬运。

（6）攻击事件模拟/防御验证。

通过office漏洞，发动鱼叉攻击，控制内网主机等几类常见的攻击，通过现场演示更直观了解整个攻击过程

# CONTENTS目录

PART / 01 工业控制系统简介/组成

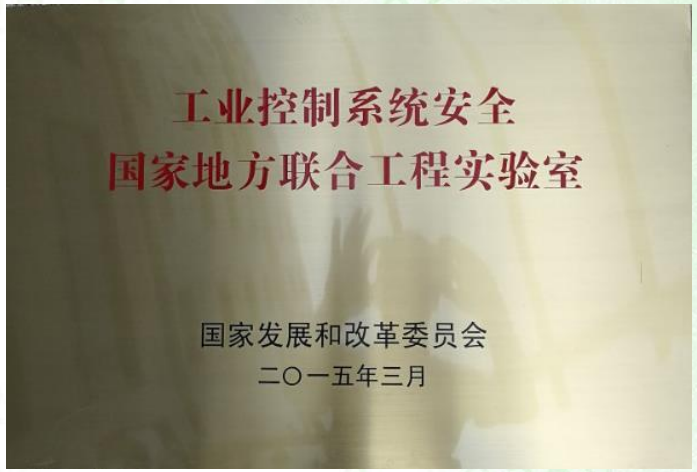
PART / 02 工业控制系统网络安全现状

PART / 03 工业控制系统安全理念与防护技术

PART / 04 360工控安全

# 360的优势

- 工业控制系统安全国家地方联合实验室（国家级）
- 中国工业互联网产业联盟-副理事长、安全组组长
- 边缘计算产业联盟-安全组组长
- 国家工业信息安全产业发展联盟 风险通报与应急服务组 副组长
- 中关村网络安全与信息化产业联盟智能制造信息安全专委会任副主任理事
- 工业控制系统信息安全产业联盟-副秘书长单位
- 网信军民融合发展联盟 智能计算与态势感知专委会 副主任
- 2017年中国自动化领域年度优质工业安全服务商
- 2018工业信息安全优秀实践案例(峰会)
- 独家安全技术支持工信部“工业信息安全技能大赛”




工业控制系统安全国家地方联合工程实验室

# 工控行业成果展示

360企业安全 安全第一®

## 协助修复严重漏洞 施耐德电气官方致谢360企业

360企业安全 6月15日

近日，全球知名工业企业施耐德电气发布
U.motion builder由360安全监测与响应中
漏洞（CVE-2018-7784、CVE-2018-7785

- CVE-2018-7784：程序对提交的数据过滤不严，
行。通过这个漏洞，攻击者可以在存在漏洞的机
息或者引发程序报错。
- CVE-2018-7785：远程命令注入漏洞，攻击者可
漏洞的主机执行任意远程命令。

两个漏洞的影响评分（CVSS v3.0）为最高级别的10
有版本都受影响，均可导致远程代码执行。

## 360捕获持续8年针对我国的网络间谍组织

360企业安全 4天前

近日，360追日团队（Helios Team）、360安全监测与响应中心与
报中心发布《蓝宝菇（APT-C-12）核危机行动揭露》报告，首次披
的持续8年攻击中国大陆地区的网络间谍组织——蓝宝菇。

据报告透露，从2011年开始至今，高级攻击组织蓝宝菇（APT-C-12）
军工、科研、金融等重点单位和部门进行了持续的网络间谍活动。核工
关行业信息是该组织的重点窃取目标。

## 360工业互联网安全监测与预警平台获 2018领先科技成果奖

360企业安全 5月27日

2018中国国际大数据产业博览会于5月26至29日在贵阳召开。作为全球科技
的风向标，2018数博会领先科技成果奖也正式公布。360工业互联网安全监
预警平台成功入选。

## 360企业安全集团荣获中国工业信息安全大会优秀实践案例奖

360企业安全 5月26日

由工信部指导，国家工业信息安全发展研究中心、工业信息安全产业发展联盟主办的首届中国工业信息安全大会于5月24号-25号在北京举行。大会以“筑工信安全，建网络强国”为主题，旨在加快推进工业信息安全建设，深化工业信息安全产业交流合作，促进我国工业信息安全全面发展。

5月25日上午，在中国工业信息安全大会工业信息安全发展趋势分论坛上360企业安全集团工业安全产品线副总监王弢受邀在大会上做了题为“数据驱动工业安全”的主题演讲，分析了新时代的网络安全形势、工业信息安全发展思想、大数据驱动的工业安全防护体系以及在工业信息安全领域的优秀案例实战。

# 工控行业布局

## 首届中国工业信息安全大会开幕 数据驱动安全引

360企业安全 5月24日

5月24日，由工信部指导，国家工业信息安全发展研究
联盟主办的首届中国工业信息安全大会在北京举行，大
国”为主题，旨在加快推进工业信息安全建设，深化工业
我国工业信息安全全面发展。360企业安全集团受邀参
信息安全方法论、产品和解决方案。

## 30位行业大咖分享：工业互联网安全全球趋势和应对指南

360企业安全 5月17日

日前，工业互联网产业联盟工作组第七次全会在重庆成功召开，会议期间，360联合AII安全组副组长单位共同发起了工业互联网安全沙龙，来自360企业安全集团、富士康、六方云科技、爱加密等著名工业企业的安全专家参与了沙龙。

安全沙龙由AII安全组执行主席、360工业安全负责人陶耀东博士和树根互联首席信息安全官彭卓共同主持，现场嘉宾就工业互联网安全发展趋势、工业互联网风险评估、“工业上云”的安全问题以及工业移动APP的安全风险等话题积极发言，亮点频出。我们将本次沙龙上的精彩观点进行了整理，分享给大家：

360企业安全集团陶耀东博士根据在RSAC2018的所见所闻，分享了**IT-OT安全发展的四大趋势。**

## ！360企业安全荣获

业安全 4月13日

018中国自动化产业年会暨
业安全集团在此次盛典上当

17年，360工业信息安全相
得了良好的应用效果，得到
提供优质的风险评估、安全
供了完备的安全态势分析服务

0企业安全集团首次将安全
安全大会发布”工业安全运营
面的优势，对工控系统通信
常和针对工控系统的威胁，通
告警和响应的自动化发布、跟踪

## 海南省工业和信息化厅领导来360公司调研考

360企业安全 5月15日

2018年4月13日在庆祝海南建省办经济特区30周年
主席、中央军委主席习近平宣布，党中央决定支持
支持海南逐步探索、稳步推进中国特色自由贸易港
贸易港政策和制度体系，其中要积极发展新一代信
联网、物联网、大数据、卫星导航、人工智能同实
海南又迎来了改革开放的重大历史机遇。

## 海南省公安厅与360集团、360企业安全集团签署战略合作协议

360企业安全 3天前

7月5日，海南省公安厅与360集团、360企业安全集团在北京签署战略合作协议，就全面提升海南省网络社会安全综合防控体系建设、网络安全监测预警防护响应等方面的能力以及共建网络犯罪预防与打击（海南）研究中心和海南省网络安全防范研究中心等开展深入合作，海南省公安厅党委委员、副厅长商万森、360集团技术总裁、首席安全官谭晓生、360企业安全集团高级副总裁曲晓东等出席签约仪式。

# THX