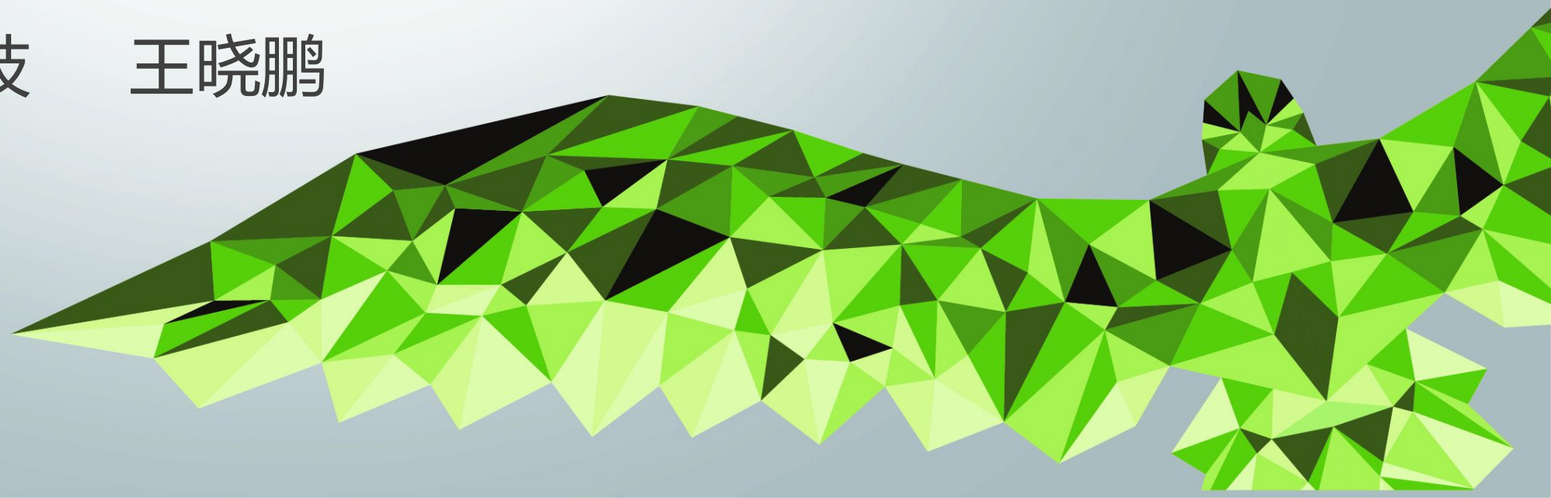
2016
LET'S START RIGHT NOW

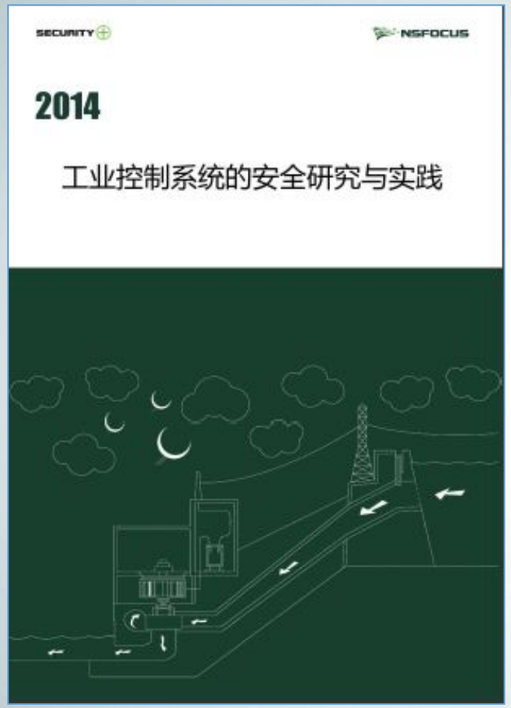
NSFOCUS

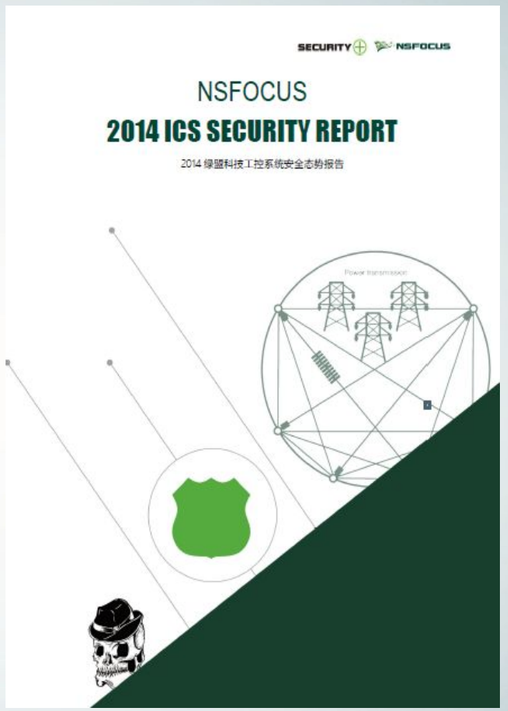
浅析工控系统安全态势的变化与应对措施

绿盟科技　　王晓鹏




NSFOCUS
2013
工业控制系统及其安全性研究报告

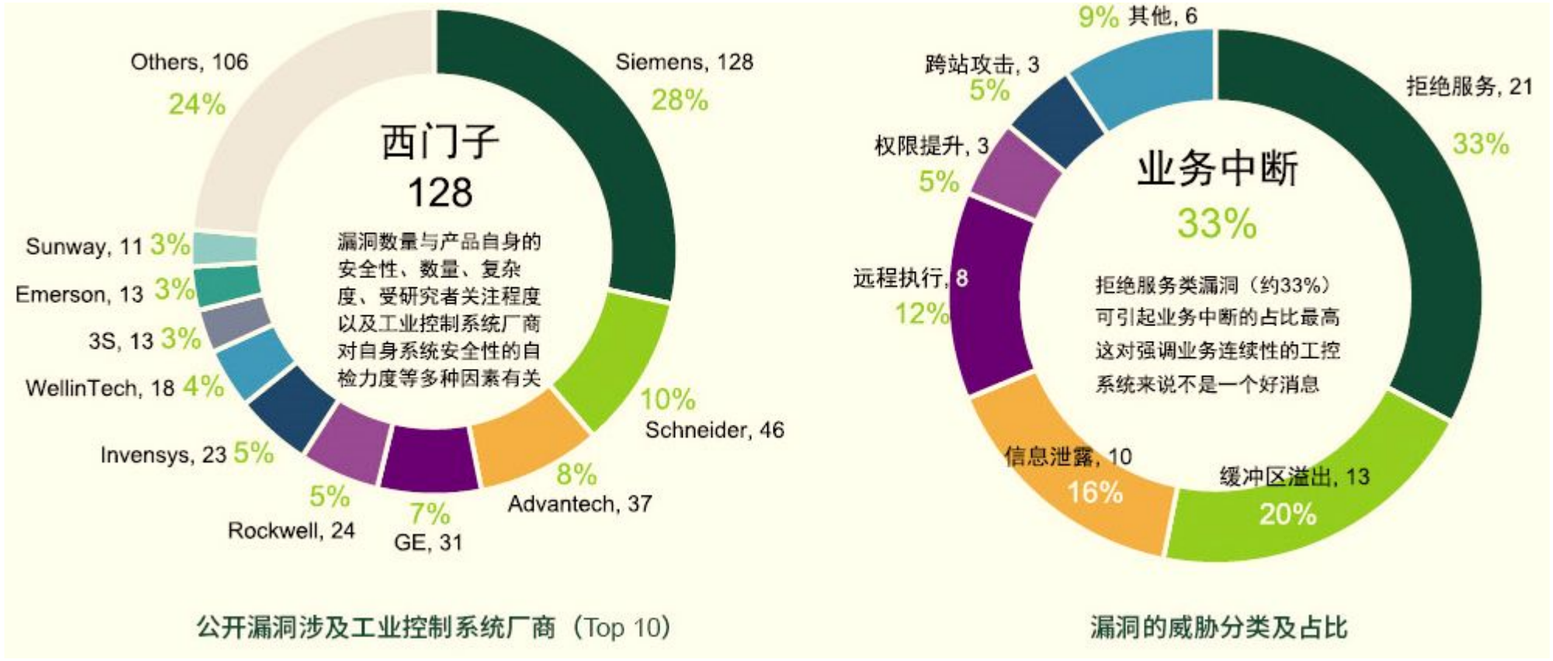

SECURITY
NSFOCUS
2014
工业控制系统的安全研究与实践


SECURITY
NSFOCUS
NSFOCUS
2014 ICS SECURITY REPORT
2014 绿盟科技工控系统安全态势报告


NSFOCUS
2015 NSFOCUS ICS Security Framework Whitepaper
2015 绿盟科技工控安保框架
白皮书
© 2016 绿盟科技

持续研究与产出

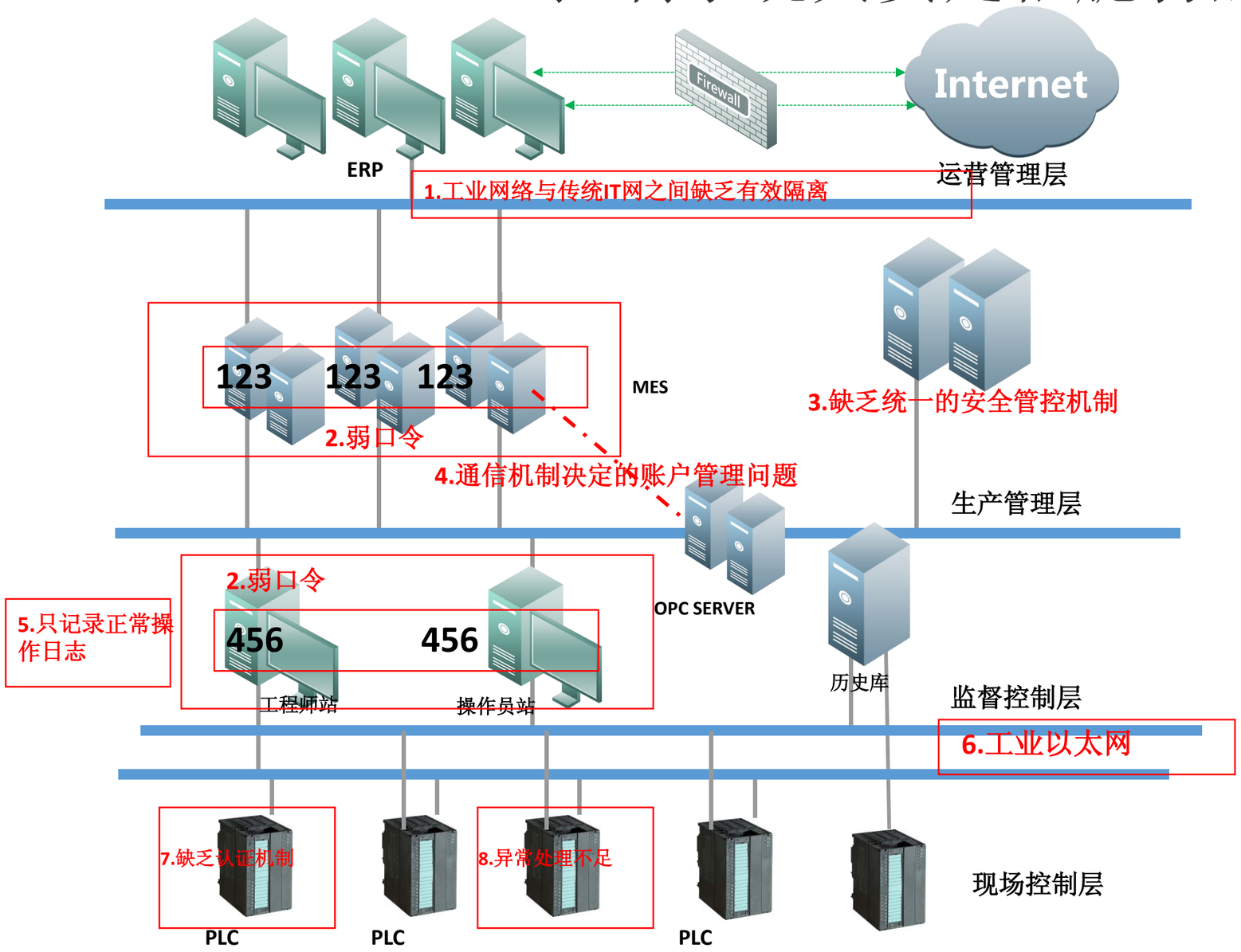
传统安全防护照顾不到的角落 – 工业控制环境



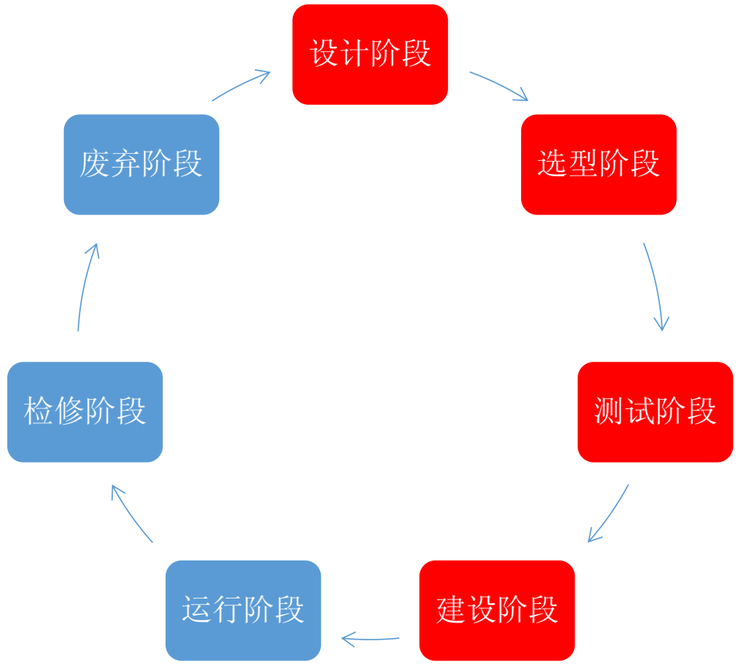
工控系统一旦 被入侵或感染，往往后果严重。

- 2007 加拿大某水利SCADA被入侵，取水调度的控制计算机被破坏
- 2008 波兰某城市地铁系统被入侵，致四节车厢脱轨
- 2009
- 2010 伊朗政府宣布布什尔核电站员工电脑感染Stuxnet病毒，严重威胁核反应堆安全运营
- 2011
  - 美国伊利诺伊州供水系统遭入侵
  - Duqu病毒可从工制系统制造商收集情报数据
  - 中国某石化企业控制系统感染Conficker，致控制系统服务器与控制器通讯不同程度中断
- 2012
  - 美国电厂工控系统遭USB病毒攻击
  - 多个中东国家感染可搜集敏感数据的Flame病毒
- 2013 中国某大型冶金厂车间控制系统发现病毒，因员工在某工作站私自安装娱乐软件带入在控制网扩散
- 2014
- 2015 乌克兰伊万诺弗兰科夫斯克地区圣诞前夜遭受攻击造成大面积停电

工业控制系统其实是很脆弱的

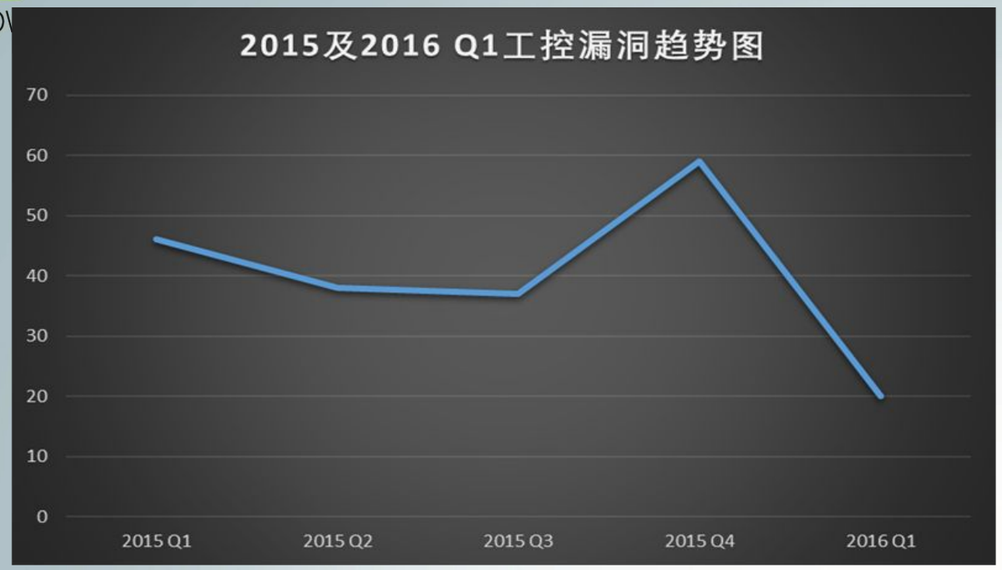


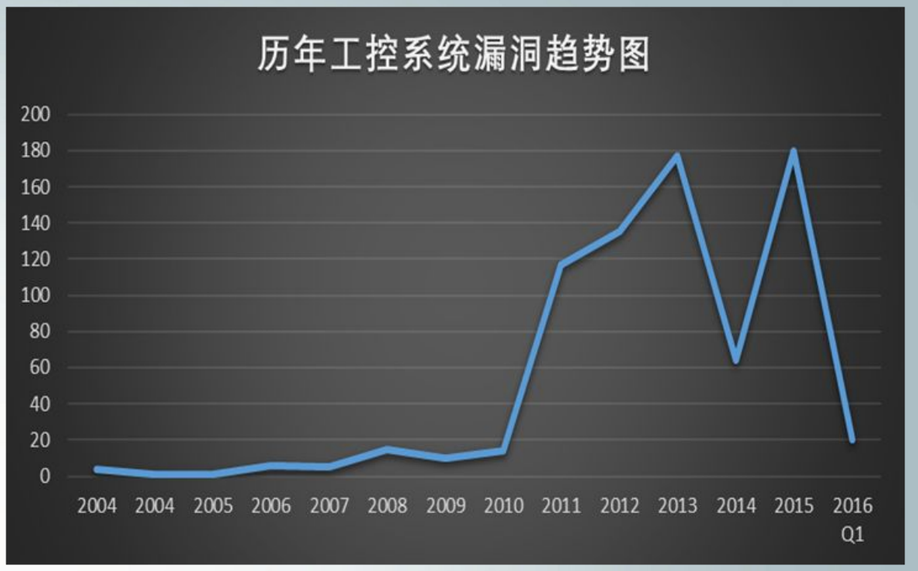
工控系统的全生命周期

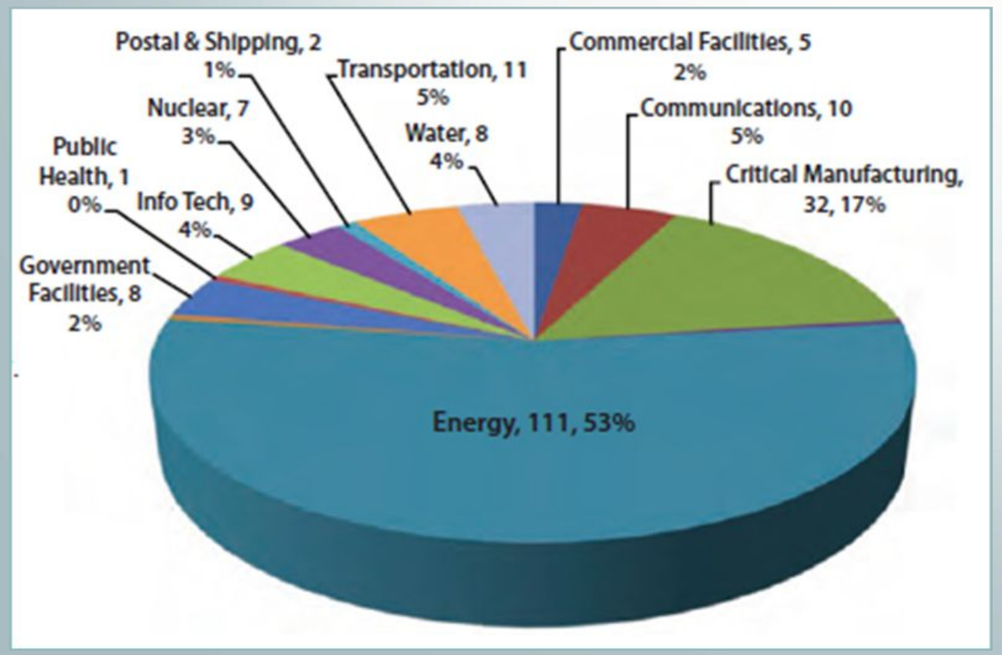


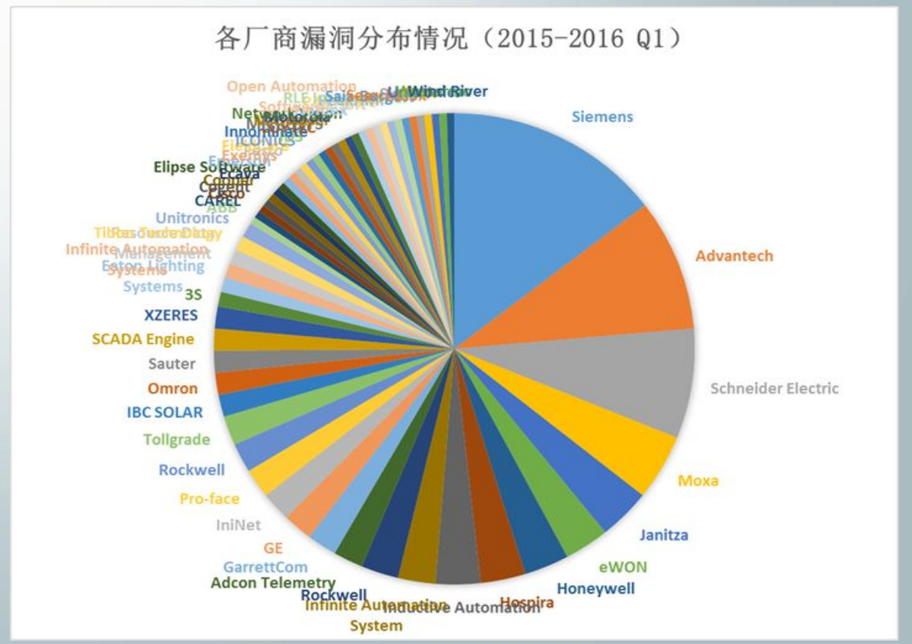
缺乏有效的安全保障，导致系统“**有毒带菌**”运行。

工控漏洞的分布情况：

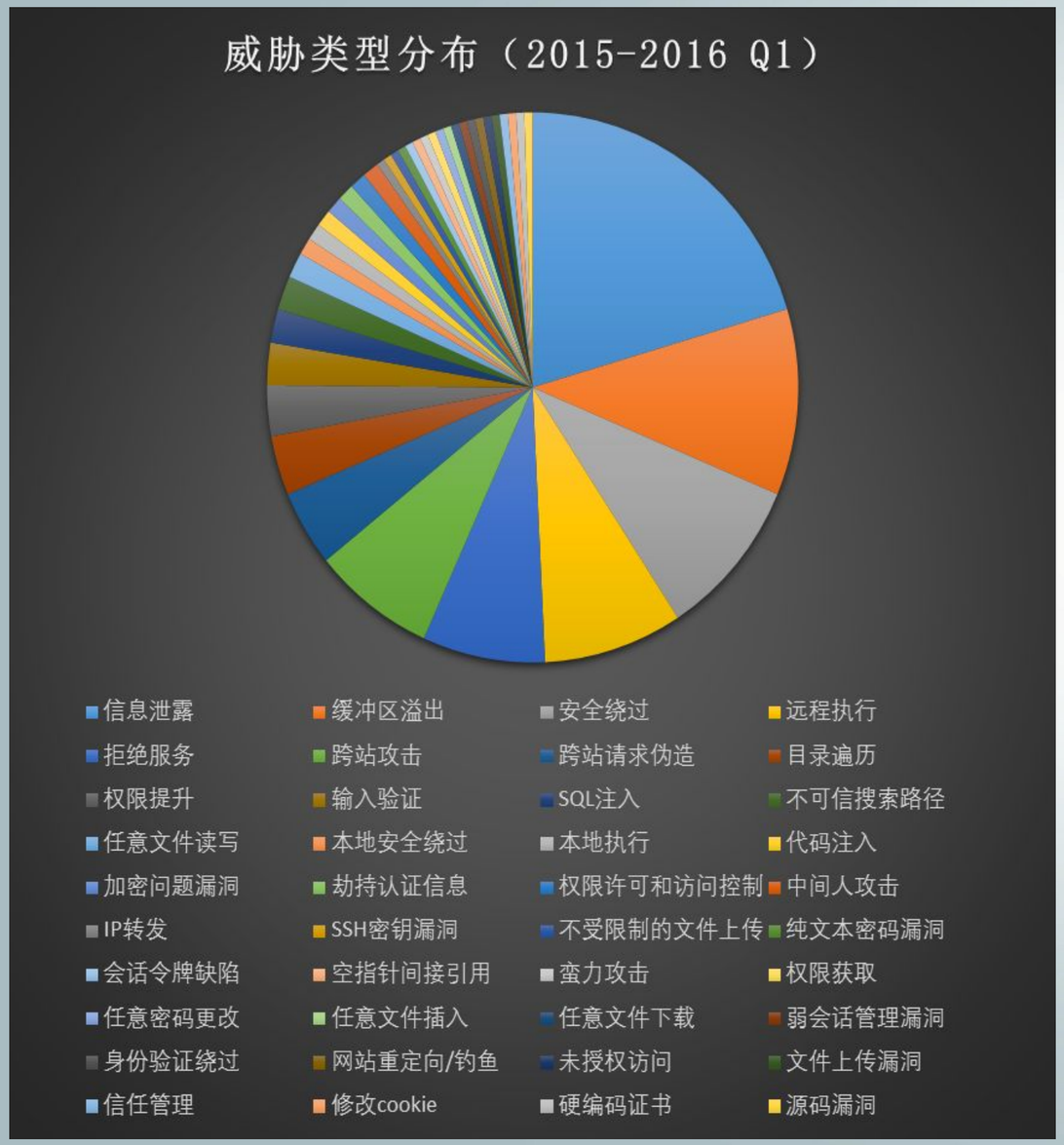

2015及2016 Q1工控漏洞趋势图
70
60
50
40
30
20
10
0
2015 Q1
2015 Q2
2015 Q3
2015 Q4
2016 Q1


历年工控系统漏洞趋势图
200
180
160
140
120
100
80
60
40
20
0
2004
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016 Q1


Postal & Shipping, 2
1%
Transportation, 11
5%
Commercial Facilities, 5
2%
Nuclear, 7
3%
Communications, 10
5%
Public
Health, 1
0%
Water, 8
4%
Critical Manufacturing,
32, 17%
Info Tech, 9
4%
Government
Facilities, 8
2%
Energy, 111, 53%


各厂商漏洞分布情况（2015-2016 Q1）
Siemens
Advantech
Schneider Electric
Moxa
Janitza
eWON
Honeywell
Hospira
Rockwell
Adcon Telemetry
GarrettCom
GE
IniNet
Pro-face
Rockwell
Tollgrade
IBC SOLAR
Omron
Sauter
SCADA Engine
XZERES
3S
Unitronics
CAREL
Elipse Software
Wind River

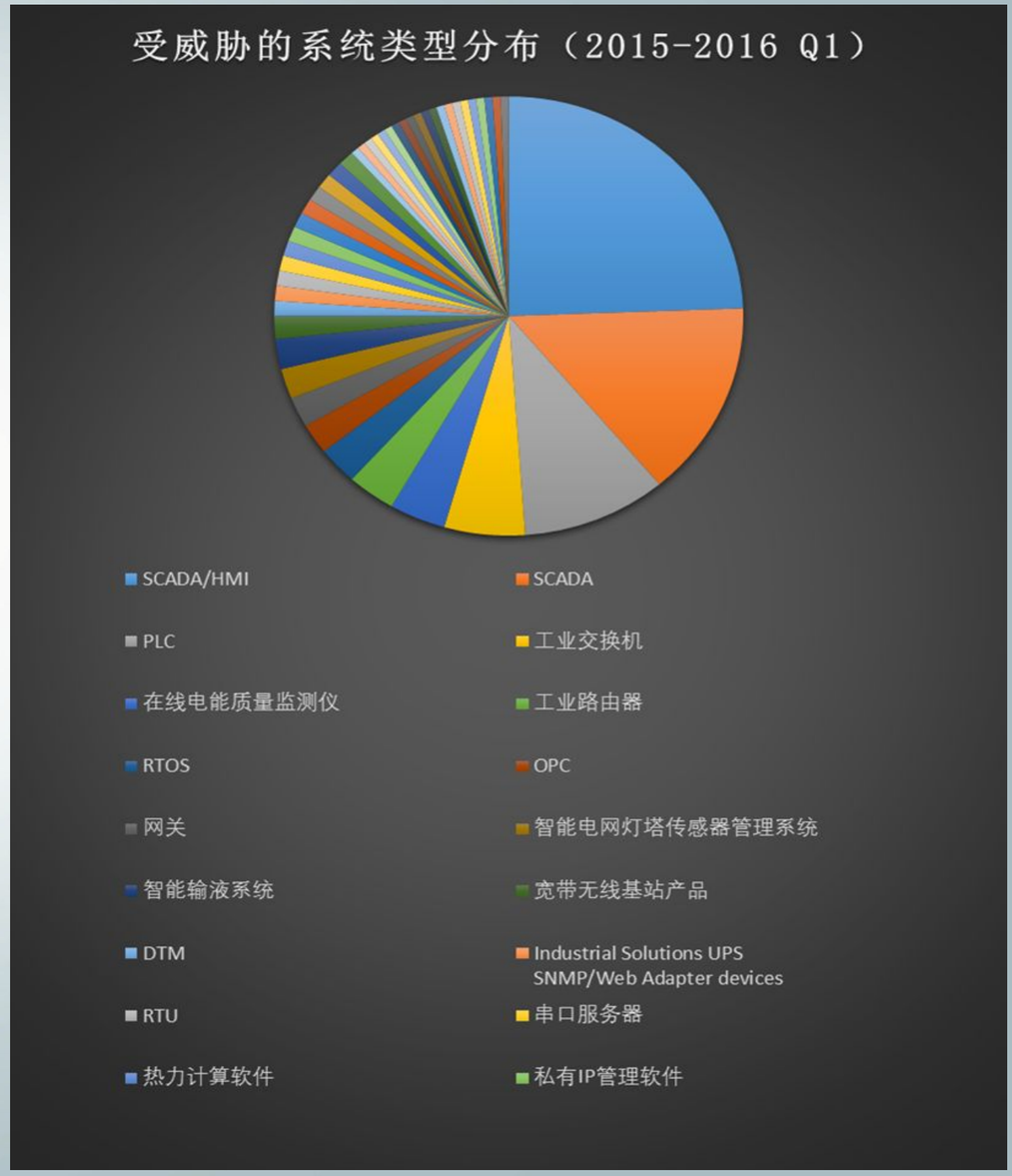
威胁类型分布及受威胁系统类型分布

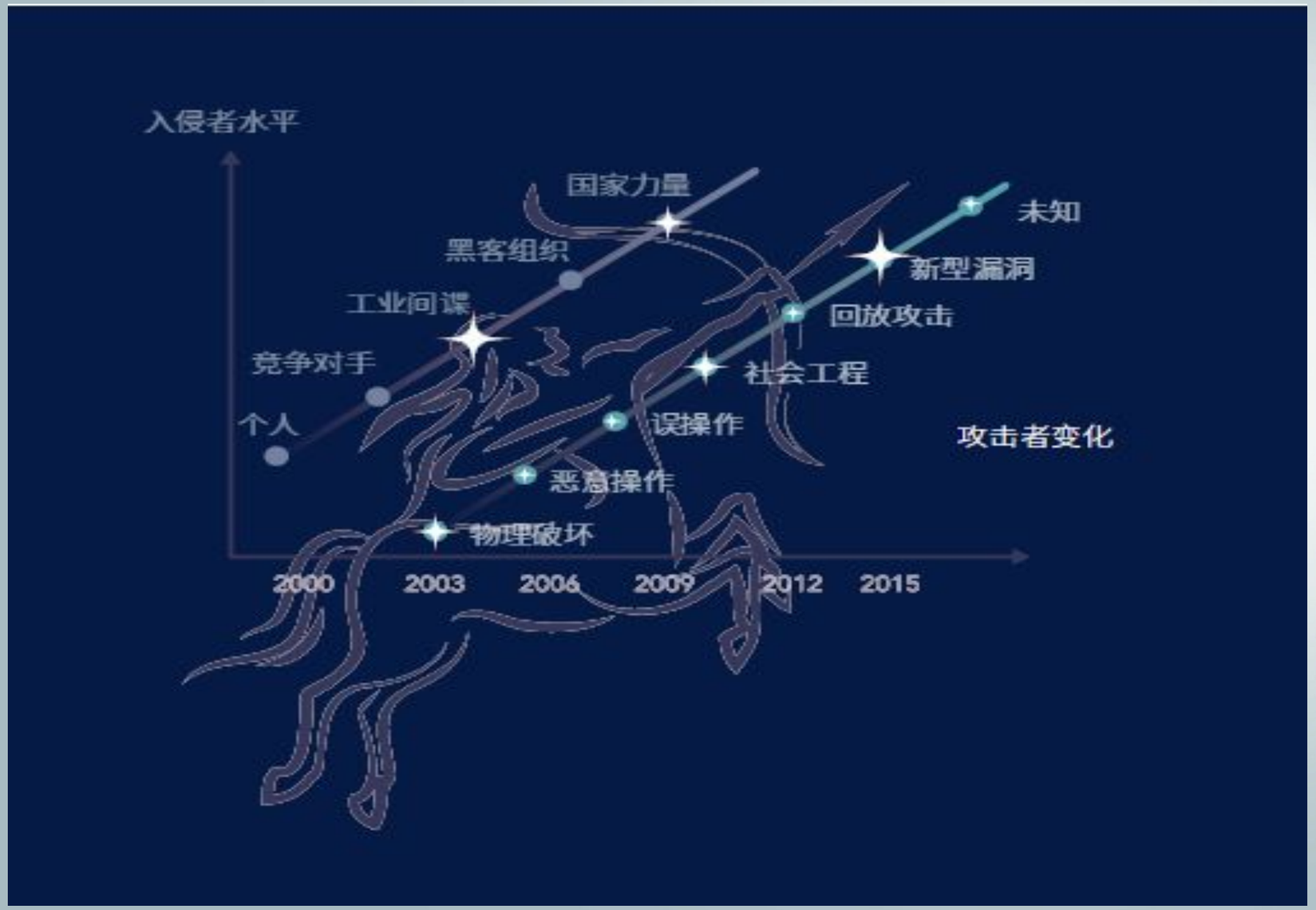


主要威胁类型：信息泄露 拒绝服务 提权

主要受威胁系统类型分布:

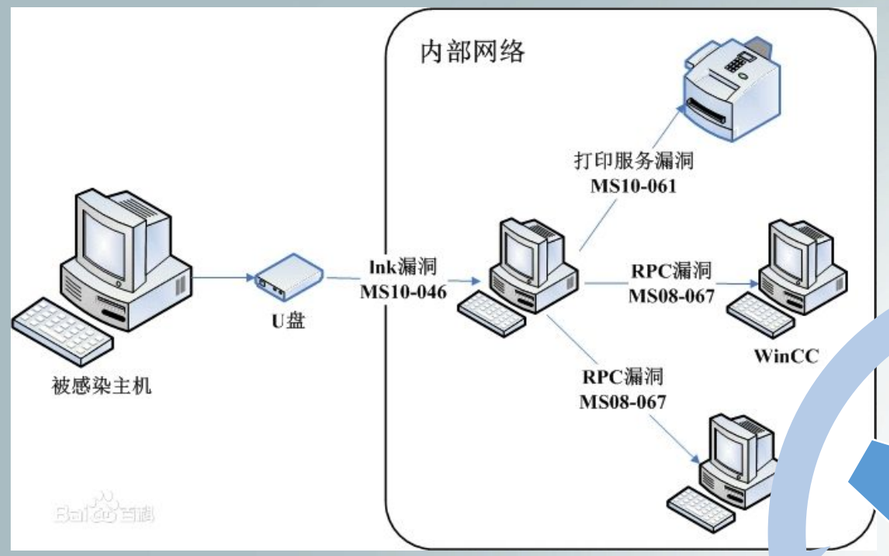
- HMI
- SCADA
- PLC

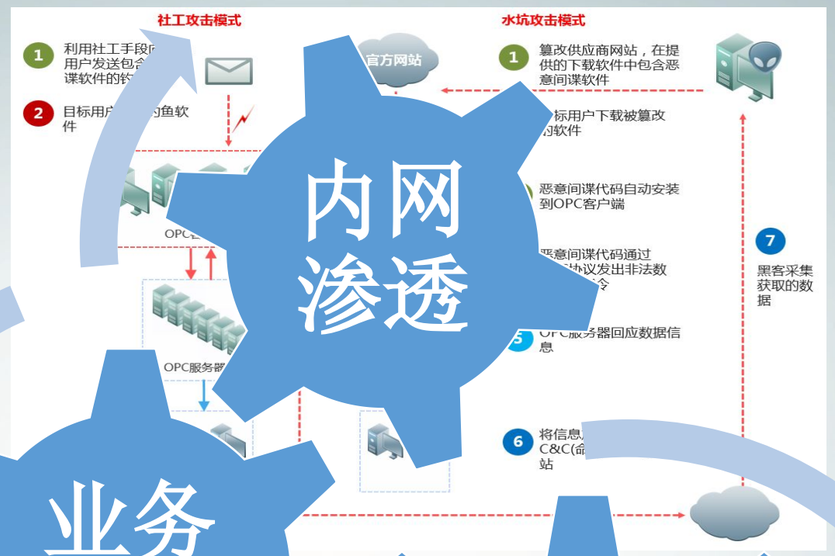




- 攻击目标聚焦：攻击目标明确，通常针对关键基础设施和重要机构。
- 攻击者水平：攻击代码愈加专业化，个人很难开展，黑客组织（竞争对手、工业间谍、尤其是有某些国家幕后支持的黑客组织）已成为当前工控系统所面临的主要攻击发起者。
- 攻击时间演变：攻击事件持续时间很长，甚至长达数年；
- 攻击态度演变：攻击者逐步变为极具耐心，不断尝试，一步一步获取目标系统的权限，然后长期蛰伏、收集信息，如此反复。
- 攻击手段演变：由破坏通信过程，引起上位机与下位机通信中断，到通过控制上位机恶意下装引起控制器运行逻辑问题，到通过综合应用IT 和OT 结合的攻击手段引起上位机和下午整体逻辑异常，到通过攻击供应链提前预制恶意软件达到对控制系统进行攻击的目的。
- 攻击范围扩大：攻击者关注的范围，由市政、电力等基础设施扩大到油化、冶金、制造业、智能部件、物联网等范围。

攻击方法的特点

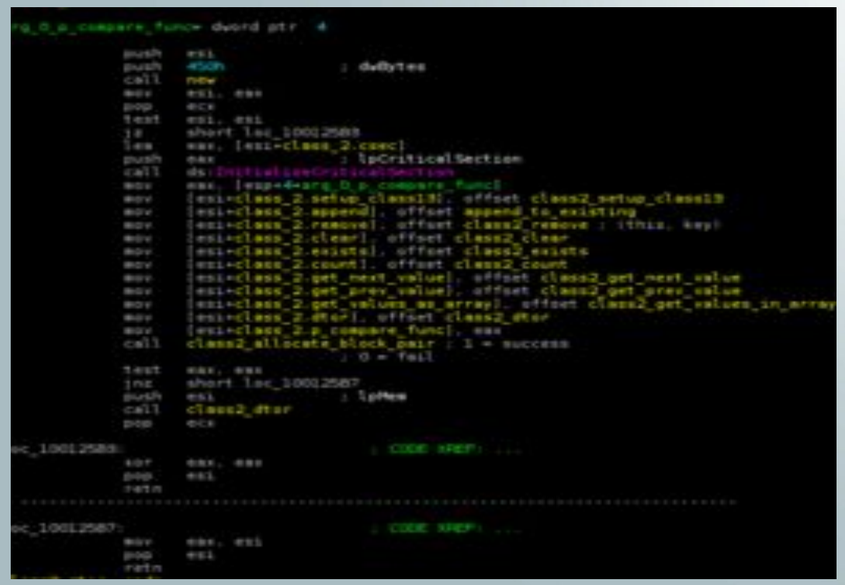


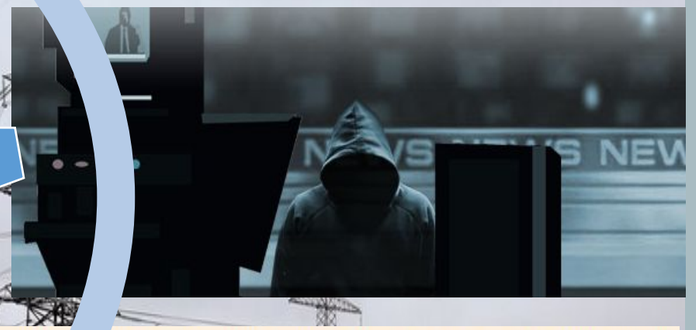


内网渗透

业务融合

攻击聚焦





乌克[illegible]部的电力公司Prykarpattyaoblenergo表示，12月23日的"大规模[illegible]致数个区域断电几个小时，该公司将此次故障归因于"干扰"。停电区域包括该地区首府伊万诺-弗兰科夫斯克(Ivano-Frankivsk)，这座城市有140万居民。

•创建一套测试平台，旨在测试电网等关键性基础设施的防御能力水平。这项工作将由美国国土安全部、

•商务部以及能源部负责推进。定一套方案以证明物联网设备之安全性

2013 年 2 月

美国总统发布了总统行政命令 13636 号，制定了“NIPP 2013 美国国家基础设施保护预案”，旨在建立国家基础设施的安全，维护网络环境，管理网络安全风险。

2013 年

欧盟发布了 COM (2013) 48—— 关于 NIS （Network and Information Security 网络与信息安全）指令的提案，该提案在 2009/140/EC 指令的基础上为网络运营商建立了安全要求。欧盟 2009/140/EC 指令是“公共网络运营商和服务商对安全风险和安全措施的管理”，以保障网络和服务的安全性。

2015 年

IEC 将建立网络安全评估，也就是检测与认证计划。这是针对产品生产商、供应商 / 系统集成商、运营商 / 资产拥有者的一套基于 IEC 62443 标准的网络安全评估体系； 是对产品、流程和人员的网络安全认证。对工控系统网络安全的检测与认证，能为资产拥有人提供保障，证明他们的产品符合 IEC 国际标准，符合基本的安全要求；同时也意味着产品的认证报告将被全球 60 多个国家认可。

2014 年 3 月

卡塔尔国发布了国家 ICS 安全标准。

国际标准 IEC62443 系列：这是国际电工标准委员会 IEC 制定的一套关于“工业通信网络和控制系统供应链的网络安全风险”的标准。

互联互通、标准化的工业协议逐步会得到应用。从美国工业互联网到德国工业4.0到中国制造2025，信息安全能力是保障业务稳定运行的基本能力。

工控安全需要实现跨领域、跨行业的多方位合作

包括国家、行业监管部门、工业控制系统的企业（用户）、工业控制系统提供商、信息安全提供商等

工控系统用户

1、制订人员、系统管理制度及规范，明确职责、提高安全意识

2、建立基于工控系统全生命周期的安全风险检测、管控及应急响应体系

3、系统上线前安全检查及检修阶段的安全风险再评估及整改……

国家/行业监管部门

1、政策、法规、标准、规范

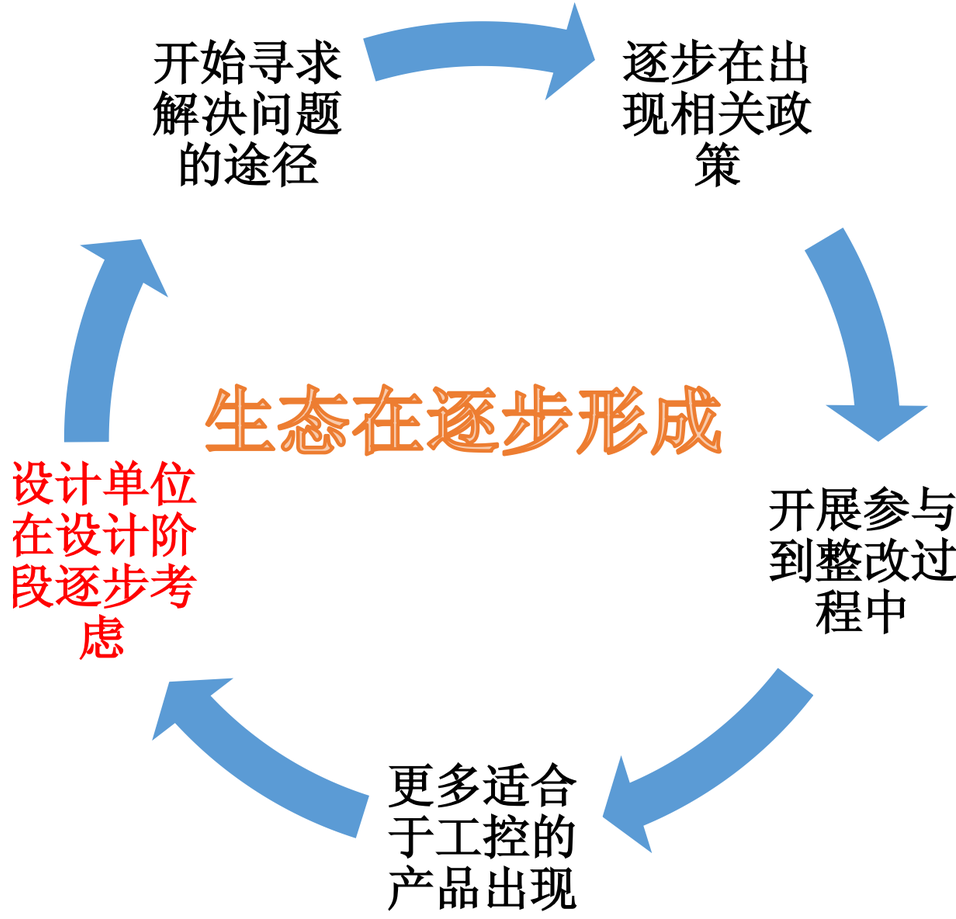
2、行业安全监管及安全检查

3、基于行业的工控漏洞发布机制、建设并维护漏洞信息共享平台……

安全服务强调的是安全保障能力

需要工控系统厂商与信息安全厂商间的协同合作来提供

信息安全厂商	工控系统厂商
• 工业控制系统安全相关的技术研究、产品开发及安全解决方案提供 • 提供工控系统脆弱性检测、分析及风险评估服务，更新行业漏洞库 • 协助国家行业监管部门进行安全检查或协助用户进行安全整改	• 工控系统脆弱性的发现、分析及解决方案（安全补丁等，需经过指定第三方验证）提供；支持行业漏洞库的漏洞信息更新 • 在工控企业用户进行系统安全整改提供技术支持



国家发改委组织工控系统产品安全测试工作

点击数：316　发布时间：2014-09-04 11:24

分享到：QQ空间 新浪微博 腾讯微博 微信 更多 0

随着工业领域生产系统网络化，系统化，高度自动化的发展，信息安全问题在工业中一下子凸显起来了，SCADA、DCS、PLC等工业控制系统面临的信息安全问题已日益严重，保证工业信息安全刻不容缓

对此，国家发展改革委日前发布通知对部分国家信息安全专项工业控制领域项目产品进行测试。通过测试的项目产品，将依照现有的管理规定，获得公安部颁发的《计算机信息系统安全专用产品销售许可证》、中国信息安全测评中心颁发的《工业控制系统安全技术测评证书》、国家信息技术安全研究中心颁发的《工业控制系统产品安全性检测评估证书》、国家密码管理局颁发的《商用密码产品型号证书》（如适用）、中国信息安全认证中心颁发的《国家信息安全产品认证证书》（如适用）。

此次参加测试的项目有“面向现场设备环境的边界安全专用网关产品”（16项），包括“核电仪控系统信息安全网关产品产业化”、“工业控制系统边界安全网关及其管控系统研发及产业化”等；“面向集散控制系统（DCS）的异常监测产品”（7项），包括“面向集散控制（DCS）的异常监测产品产业化”等；“安全采集远程终端单元（RTU）产品”（13项），包括“通用工业通讯安全网关产品研发产业化”、“智能型安全远程测控终端产业化”等；“工业应用软件漏洞扫描产品”（4项），包括“工业控制系统通用漏洞扫描产品产业化”等。

电子信息产业网 www.cena.com.cn | 中国电子报 电子版

当前位置：首页 〉 产业要闻 〉 产业分析

工业控制系统信息安全技术国家工程实验室成立

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

各省、自治区、直辖市人民政府，国务院有关部门，有关国有大型企业：

工业控制系统信息安全事关工业生产运行、国家经济安全和人民生命财产安全，为切实加强工业控制系统信息安全管理，经国务院同意，现就有关事项通知如下：

一、充分认识加强工业控制系统信息安全管理的重要性和紧迫性

数据采集与监控（SCADA）、分布式控制系统（DCS）、过程控制系统（PCS）、可编程逻辑控制器（PLC）等工业控制系统广泛运用于工业、能源、交通、水利以及市政等领域，用于控制生产设备的运行。一旦工业控制系统信息

中华人民共和国国家发展和改革委员会令

第 14 号

《电力监控系统安全防护规定》已经国家发展和改革委员会主任办公会审议通过，现予公布，自2014年9月1日起施行。

国家发展改革委主任　徐绍史

2014年8月1日

— 1 —

国家能源局关于印发《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》的通知

国能安全〔2015〕36号

2015年2月4日

国家能源局深入开展电力工控系统安全防护专项监管

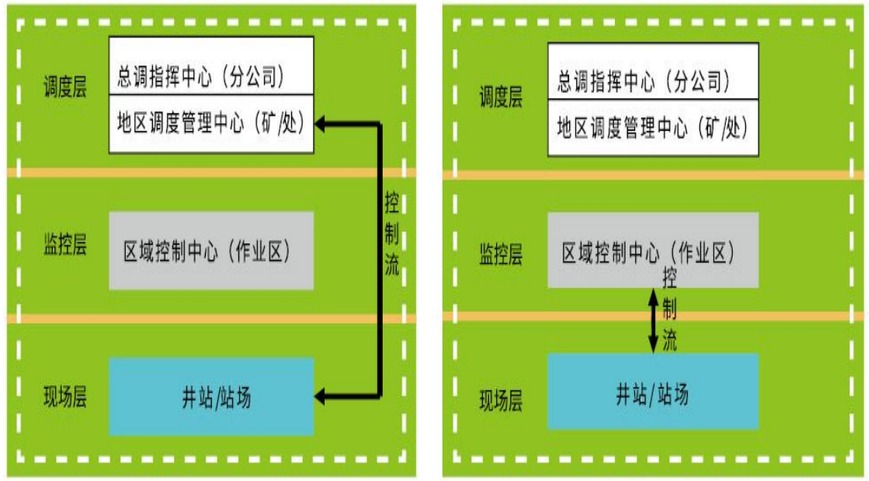
发布时间：2016-05-11　来源：国家能源局　大 中 小

按照《电力工控系统安全防护专项监管工作方案》，2015年6月至12月，国家能源局在全国范围内组织开展了电力工控系统安全防护专项监管工作，重点对电力行业电力工控系统网络安全管理、管理规定制度落实、总体技术防护策略落实、PLC设备隐患排查及漏洞整改、宣传教育培训等工作开展情况进行监督检查。

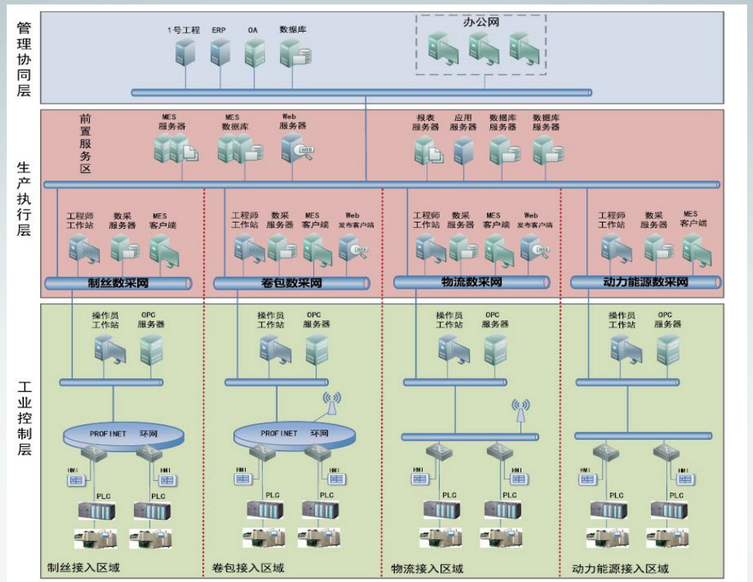
此次专项监管发现，在电力行业各单位的高度重视下，近年来我国电力工控系统安全防护水平不断提高，但依然存在一定的问题和不足。主要包括，在管理方面，一是未及时修订电力监控系统安全防护等管理制度；二是安全防护评估工作开展不到位；三是安全防护人员配置及培训存在不足；四是安全防护技术监督工作存在不足。在技术方面，一是网络边界防护措施不完善、安全威胁较大；二是纵深防御管控不足、终端防护薄弱；三是PLC设备隐患排查不到位、安全风险仍然存在；四是物理安全防护措施不到位、安全隐患频现。

针对当前电力工控系统安全存在的问题，国家能源局提出了加强电力工控系统安全防护工作的具体意见：一是加强安全防护管理体系建设，逐层逐级抓好安全主体责任的落实。二是强化安全防护措施制定和问题的持续整改，切实提高安全防护能力。三是扎实推进安全防护评估及等级保护工作，积极构建网络安全管理常态机制。四是切实抓好安全防护应急管理，有效提升信息安全事件应急处置能力。五是加强信息安全教育和专业技术培训，强化从业人员的安全管理。六是规范产品选型，提高电力工控系统安全可控能力。

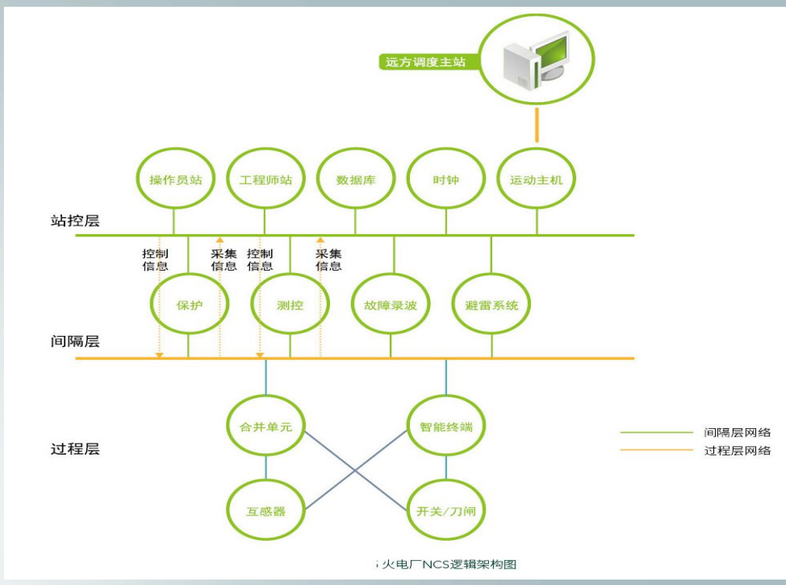
我们调研的一些行业情况



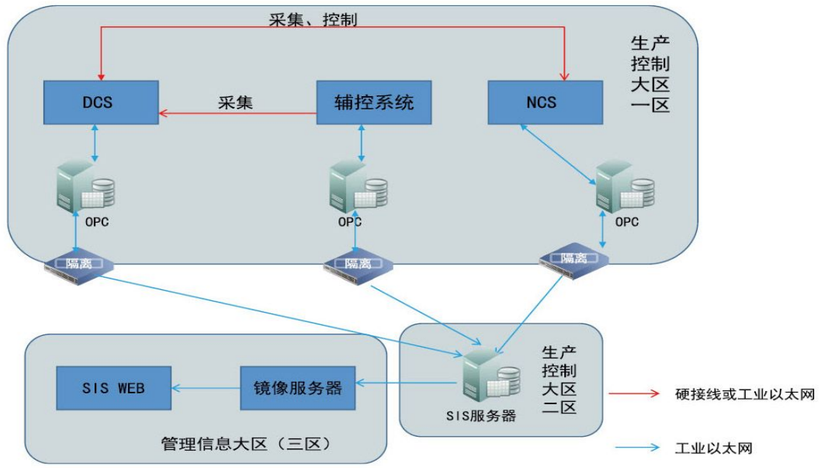
SCADA系统控制流



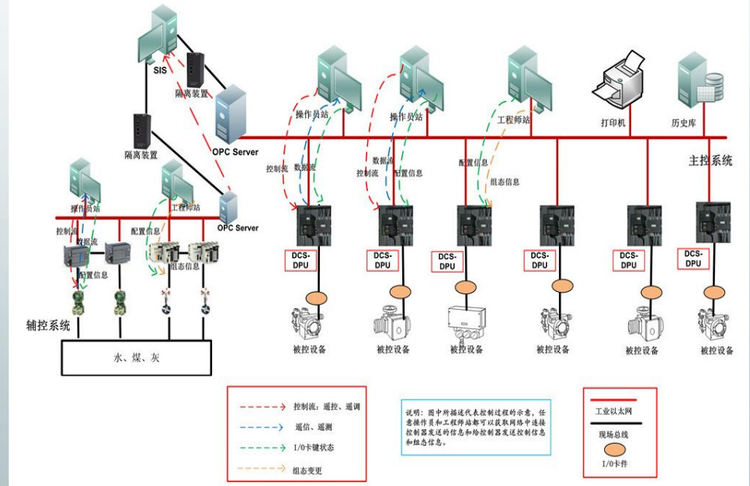
卷烟生产企业安全域架构设计示例



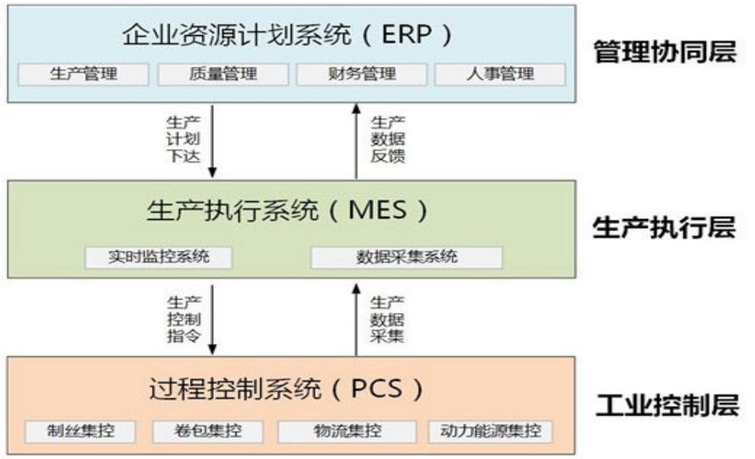
：火电厂NCS逻辑架构图



火电厂NCS逻辑架构图



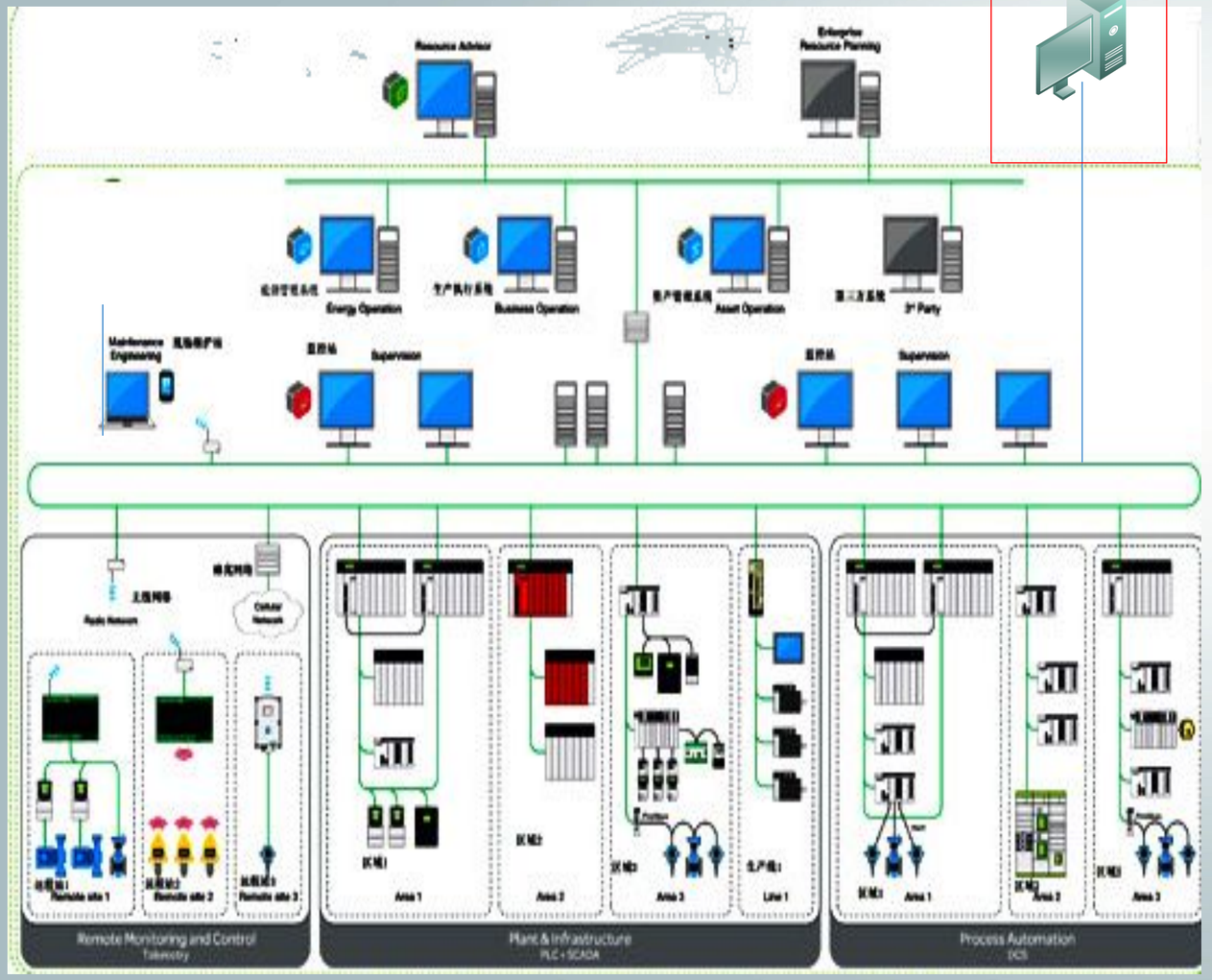
火电厂主控与辅控系统逻辑架构图



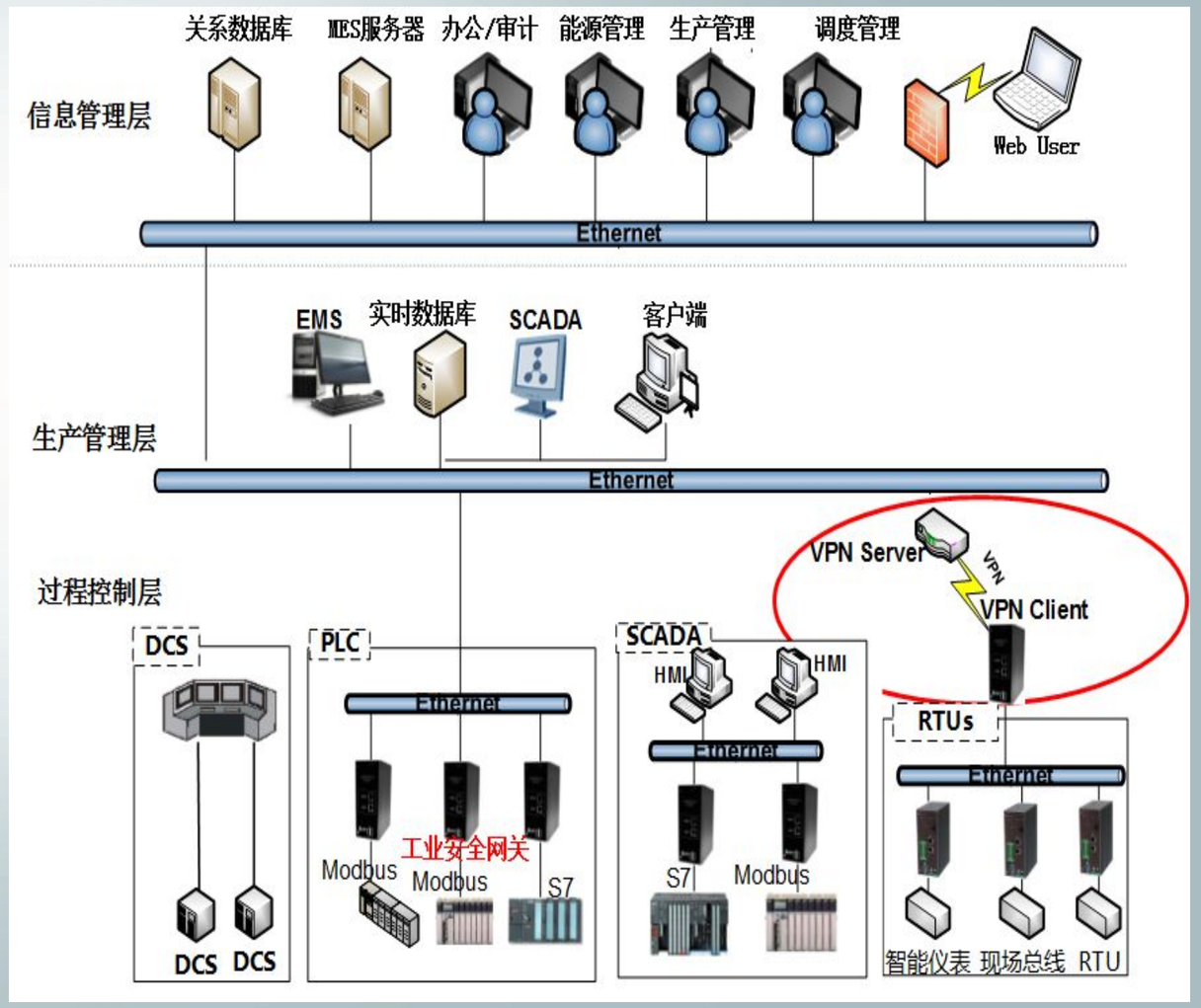
卷烟工业生产应用系统层次结构

生产外联依然存在（实例）

业务需要私自搭建的连接通道



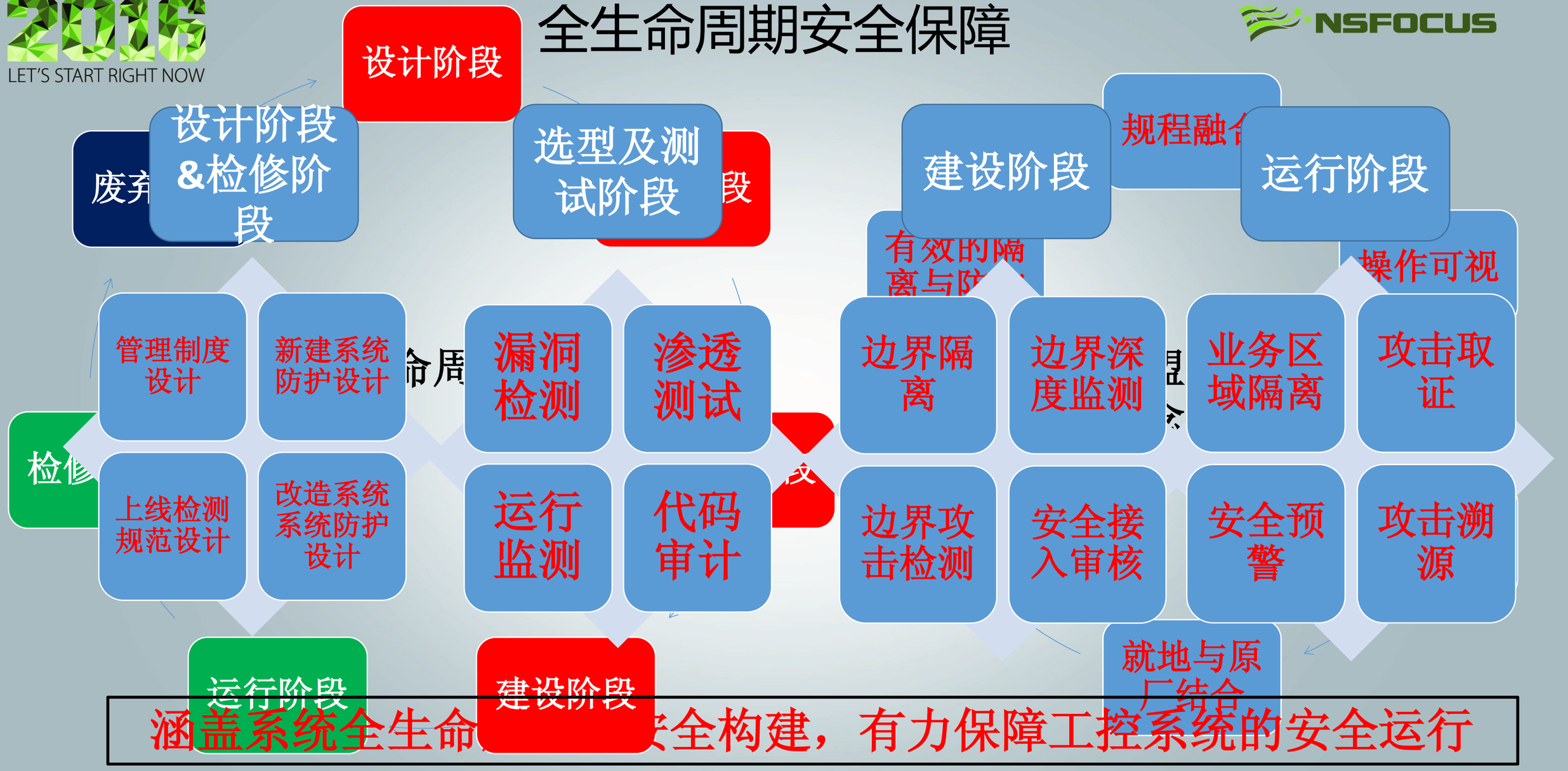
第三方远程运维通道



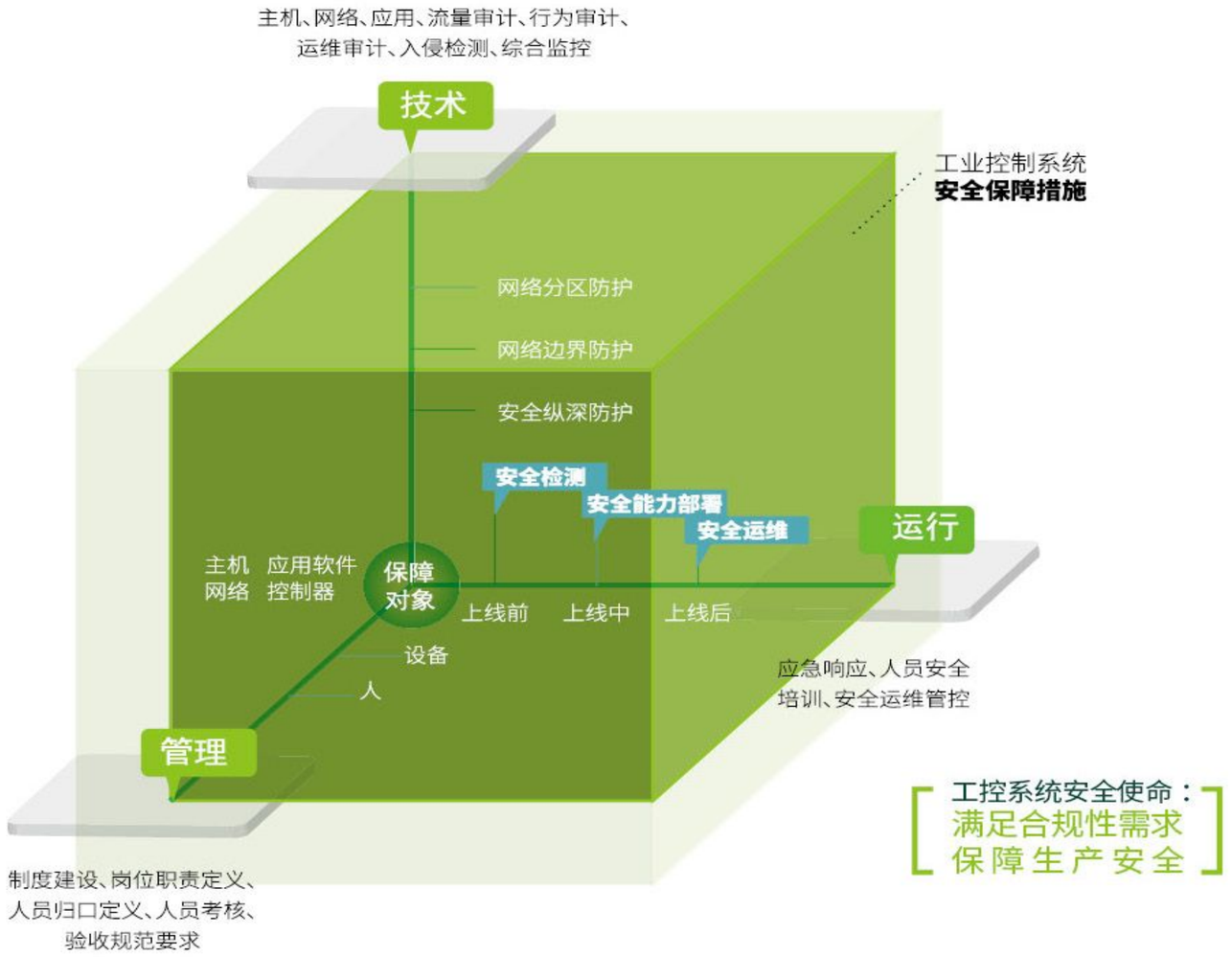
安全防护仍然缺乏技术手段

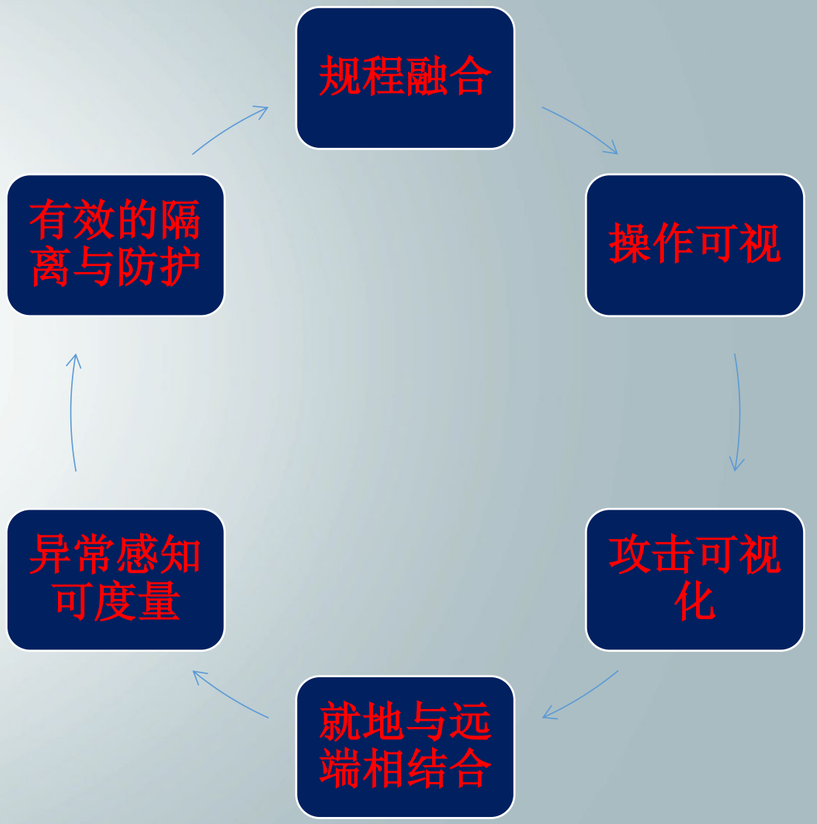
涵盖系统全生命周期的安全构建，安全要求（上线要求）---边界防护（生产隔离）-----纵深防护（生产安全监测）

全生命周期安全保障

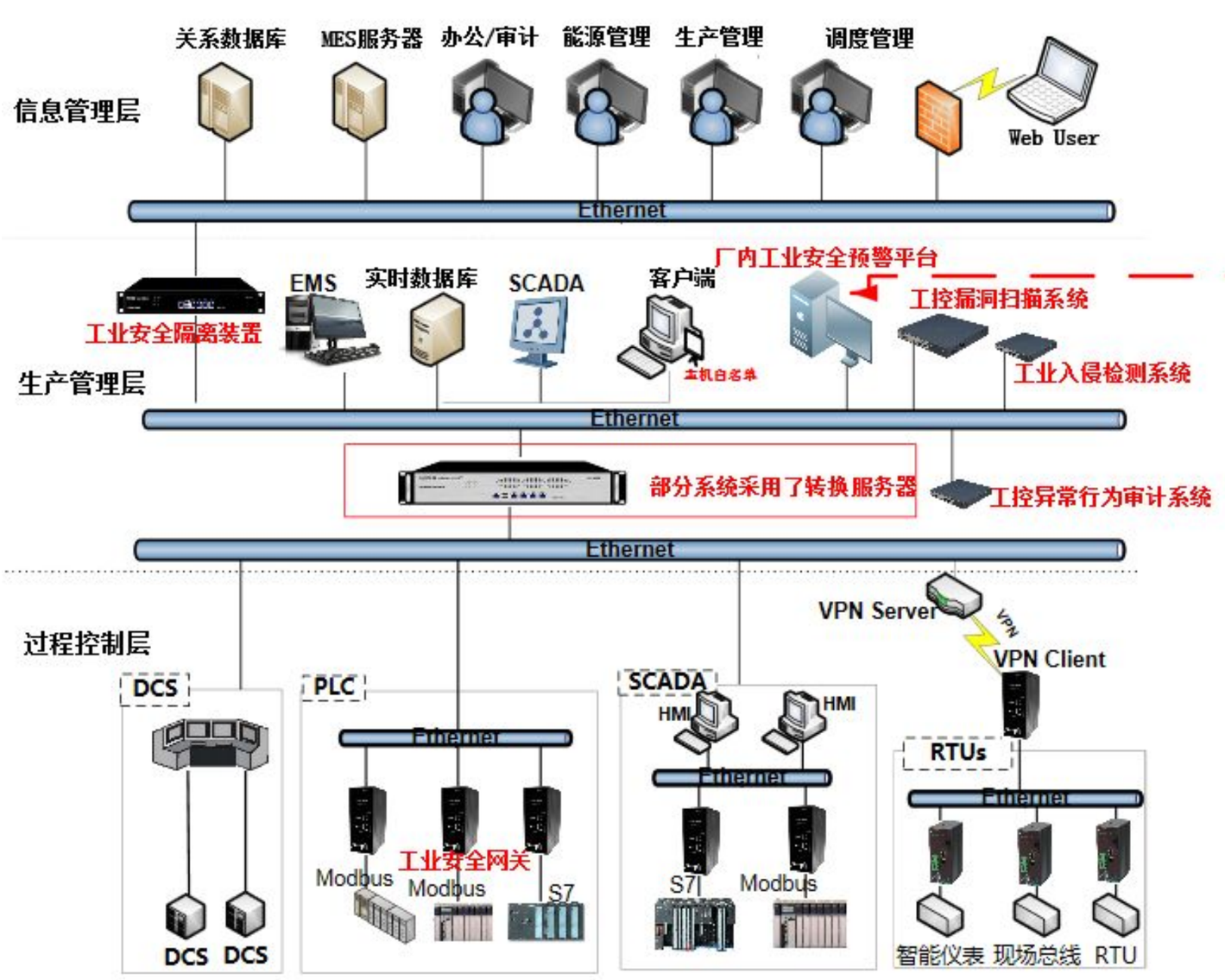

设计阶段
设计阶段&检修阶段
选型及测试阶段
建设阶段
运行阶段
管理制度设计
新建系统防护设计
上线检测规范设计
改造系统系统防护设计
漏洞检测
渗透测试
运行监测
代码审计
边界隔离
边界深度监测
边界攻击检测
安全接入审核
业务区域隔离
攻击取证
安全预警
攻击溯源
操作可视
就地与原厂结合
涵盖系统全生命

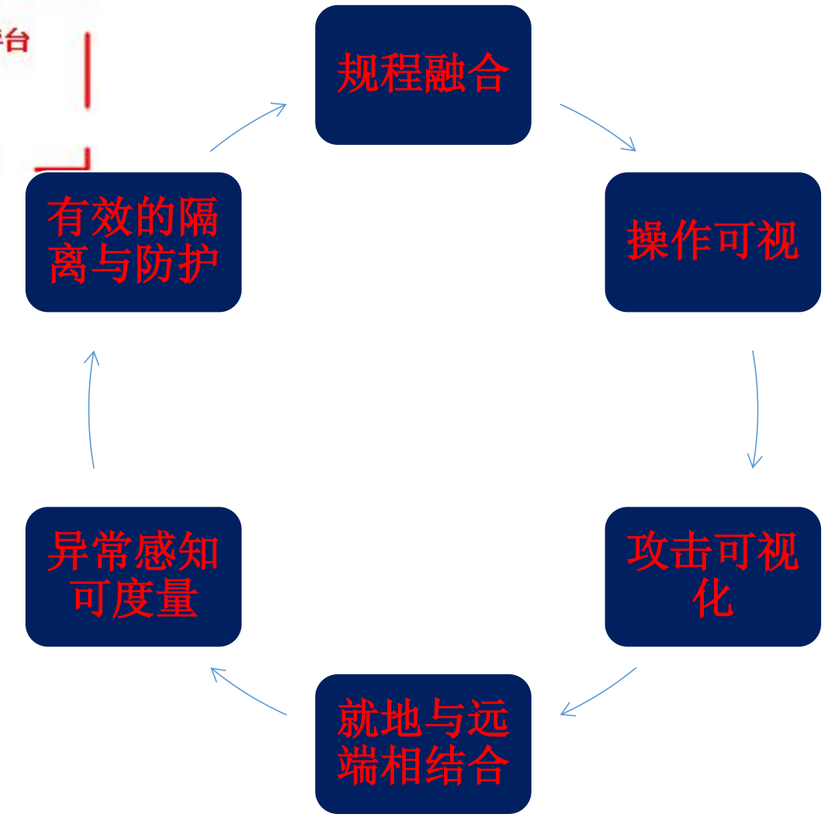
总体安全保障框架


主机、网络、应用、流量审计、行为审计、
运维审计、入侵检测、综合监控
技术
工业控制系统
安全保障措施
网络分区防护
网络边界防护
安全纵深防护
安全检测
安全能力部署
安全运维
运行
主机 应用软件
网络 控制器
保障对象
上线前
上线中
上线后
设备
人
管理
应急响应、人员安全
培训、安全运维管控
制度建设、岗位职责定义、
人员归口定义、人员考核、
验收规范要求
工控系统安全使命：
满足合规性需求
保障生产安全

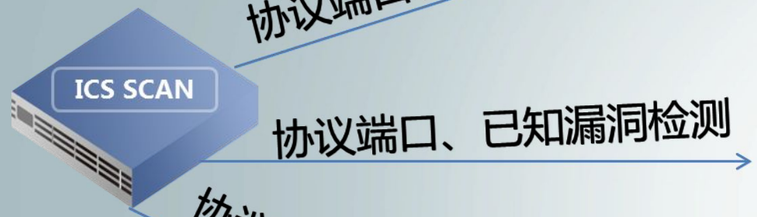

规程融合
操作可视
攻击可视化
就地与远端相结合
异常感知可度量
有效的隔离与防护

工控安全解决方案


关系数据库
MES服务器
办公/审计
能源管理
生产管理
调度管理
信息管理层
Web User
Ethernet
广域网
分级部署的
工业安全预警平台
厂内工业安全预警平台
EMS
实时数据库
SCADA
客户端
工控漏洞扫描系统
工业安全隔离装置
主机白名单
工业入侵检测系统
生产管理层
Ethernet
部分系统采用了转换服务器
工控异常行为审计系统
Ethernet
VPN Server
VPN
VPN Client
过程控制层
DCS
PLC
SCADA
HMI
HMI
Ethernet
Ethernet
RTUs
Ethernet
工业安全网关
Modbus
Modbus
S7
S7
Modbus
DCS
DCS
智能仪表
现场总线
RTU


规程融合
操作可视
攻击可视化
就地与远端相结合
异常感知可度量
有效的隔离与防护

漏洞的管理



协议端口、已知漏洞检测

协议端口、已知漏洞检测

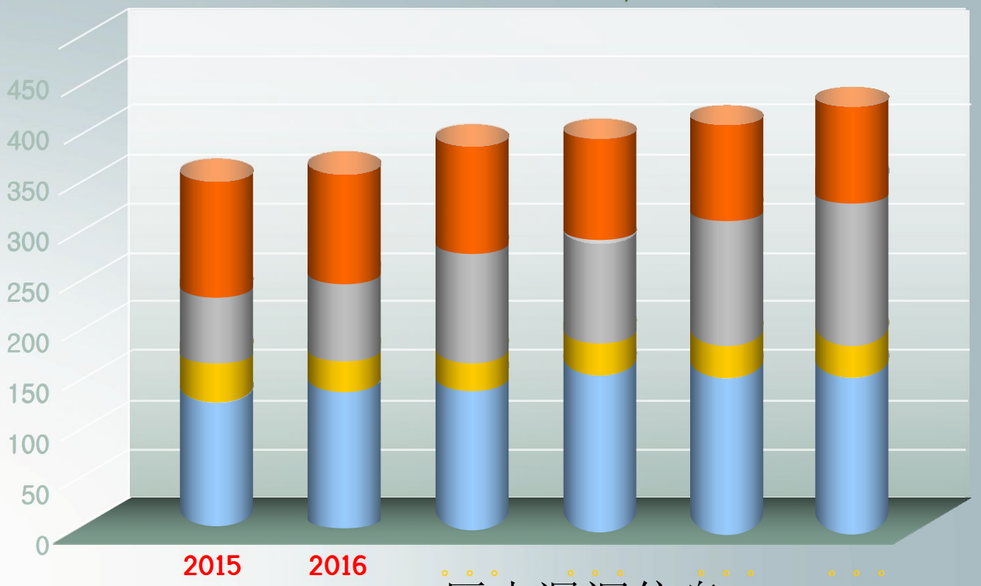
协议端口、已知漏洞检测

modbus	60870-5-1-4
512	2404

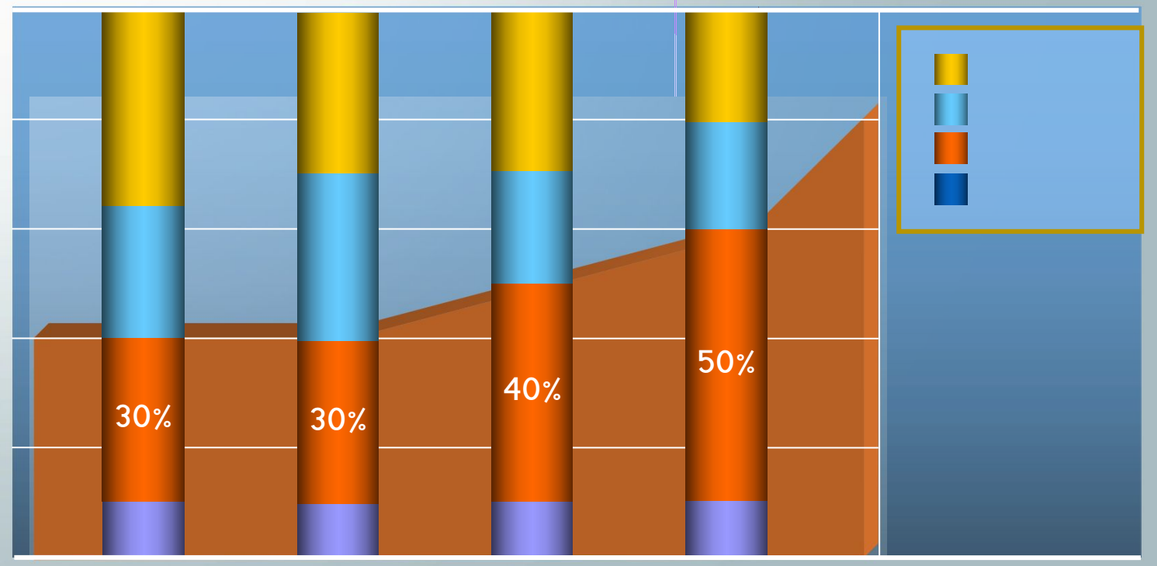
4.1漏洞分布

漏洞类别：高风险[11] 中危险[8] 低风险[7]

序号	漏洞名称	影响主机个数	影响主机百分比	出现次数
1	Ecava IntegraXor ActiveX save函数缓冲区溢出漏洞(CVE-2010-4597)	1/1	100%	1
2	WellinTech KingSCADA栈缓冲区溢出漏洞(CVE-2014-0787)	1/1	100%	1
3	Ecava IntegraXor < 4.00.4283 ActiveX 远程缓冲区溢出(CVE-2012-4700)	1/1	100%	1
4	Ecava IntegraXor igcom.dll Traversal 任意文件改写漏洞(CVE-2012-0246)	1/1	100%	1
5	Ecava Integraxor SCADA Server任意文件读写漏洞(CVE-2014-2375)	1/1	100%	1
6	Ecava IntegraXor 基于栈的缓冲区溢出漏洞(CVE-2014-0753)	1/1	100%	1
7	多款Schneider Electric产品存在安全漏洞(CVE-2013-2824)	1/1	100%	1
8	Ecava IntegraXor < 3.60.4050 Unspecified sql注入漏洞(CVE-2011-1562)	1/1	100%	1
9	WellinTech KingSCADA/KingAlarm&Event/KingGraphic 远程代码执行漏洞(CVE-2013-2827)	1/1	100%	1
10	Ecava Integraxor SCADA Server SQL注入漏洞(CVE-2014-2376)	1/1	100%	1
11	WellinTech KingSCADA 3.1 < 2012-04-16 user.db Base-64 Encoding 本地认证信息泄露(CVE-2012-1977	1/1	100%	1

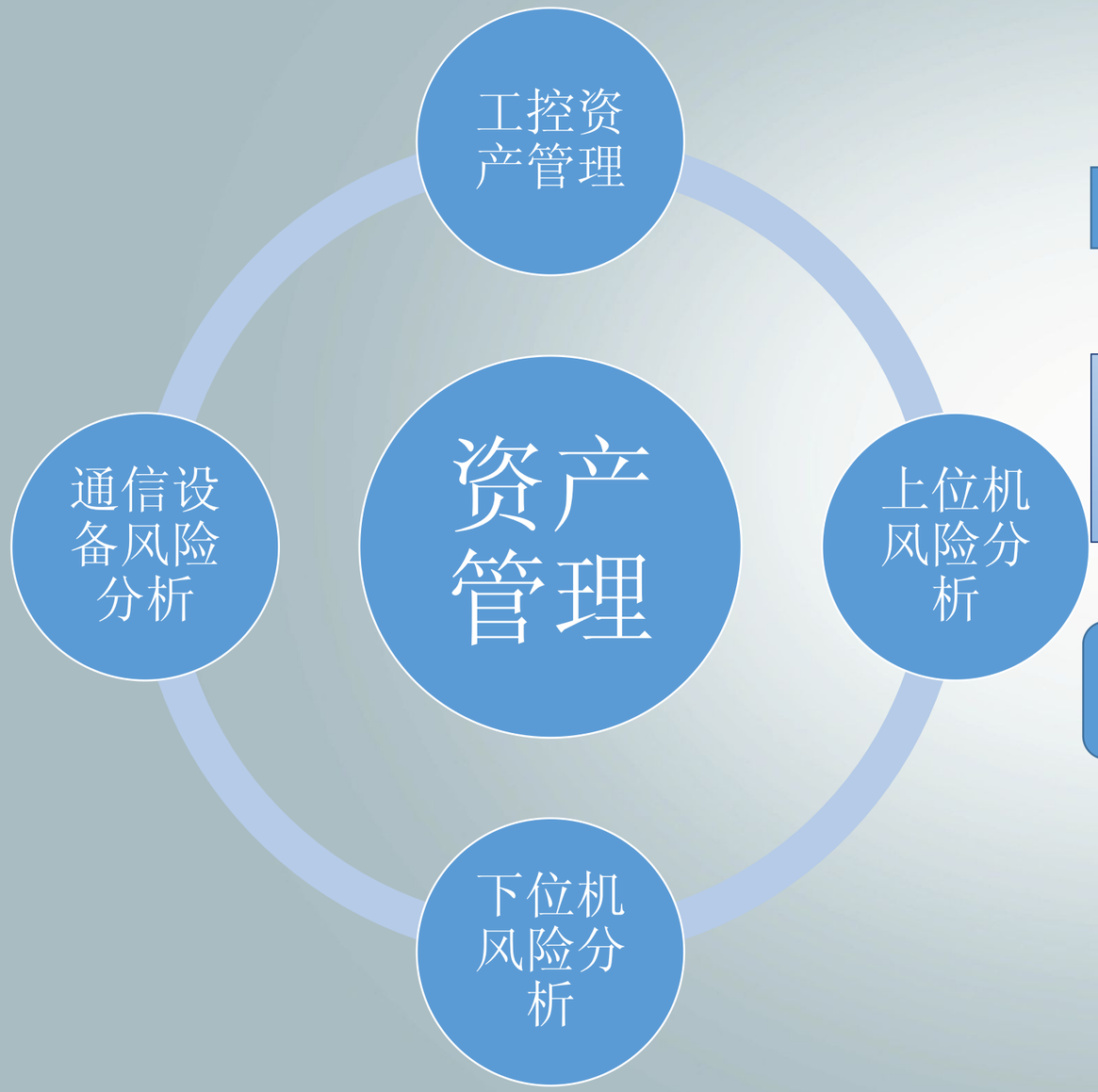


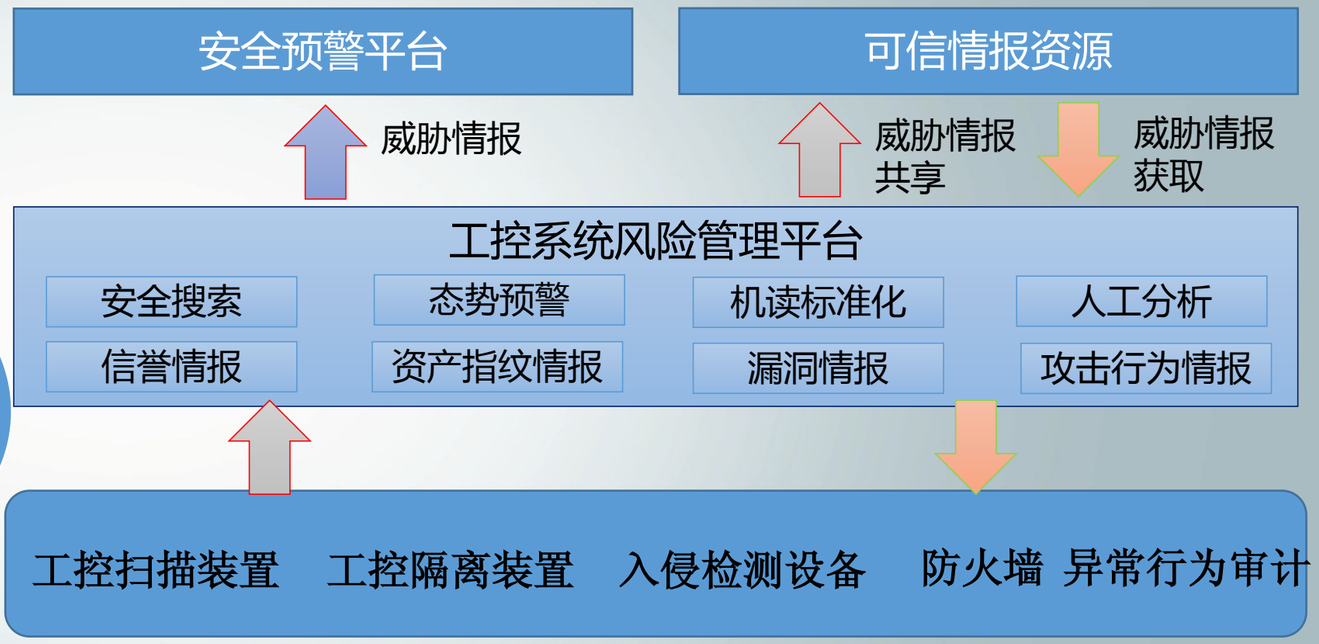
历史漏洞信息



当期漏洞信息

威胁管理---业务过程管理


工控资产管理
通信设备风险分析
资产管理
上位机风险分析
下位机风险分析


安全预警平台
可信情报资源
威胁情报
威胁情报共享
威胁情报获取
工控系统风险管理平台
安全搜索
态势预警
机读标准化
人工分析
信誉情报
资产指纹情报
漏洞情报
攻击行为情报
工控扫描装置
工控隔离装置
入侵检测设备
防火墙
异常行为审计

工控告警信息

- EventName=SOE变位报警
- EventName=SOE变位报警恢复
- EventName=开关量闭合报警
- EventName=开关量闭合报警恢复
- EventName=模拟量越上上限报警
- EventName=模拟量越上上限恢复
- EventName=模拟量越上限报警
- EventName=模拟量越上限恢复
- EventName=模拟量越下限报警
- EventName=模拟量越下限恢复
- EventName=模拟量越下下限报警
- EventName=模拟量越下下限恢复
- EventName=模拟量限值报警
- EventName=模拟量越高三限恢复
- EventName=模拟量越低三限报警
- EventName=模拟量越低三限恢复

序号	告警名称	通俗解释	产生原因	故障预判
1	广播风暴	网络中出现大量的重复报文，挤占了网络资源。	装置检测到某个端口在1秒内收到重复的报文超过阈值	检查交换机是否发生故障
2	流量异常	网络中的流量很大，会影响通信质量。	装置检测到某个端口收到的报文的流量超过阈值	检查交换机是否发生故障或者智能设备通信故障
3	流量突变	网络中的流量突然变大或变小	装置检测到某个端口的流量突然变大或变小	检查交换机是否发生故障或者智能设备通信故障
4	报文格式错误	网络中的报文格式不符合61850协议标准。	对GOOSE或SV进行ASN.1解码时出现错误，GOOSE或SV参数配置错误	网络分析仪厂家给出错误原因和对应的报文，由装置厂家对该原因进行分析。

大量业务相关的数据，是传统信息安全中不涉及的，工控安全需要考虑工控安全的特点，以及与信息安全之间的融合。

2016
LET'S START RIGHT NOW

NSFOCUS

预警 Warning | 监视 Monitor | 检测 Detection | 防护 Protect | 响应和处理 Response

安全评估服务 | 网络安全防护 | 异常行为检测 | 主机安全防护 | 通信环境感知 | 应急响应服务 | 安全度量服务 | 合规报告服务

安全预警平台

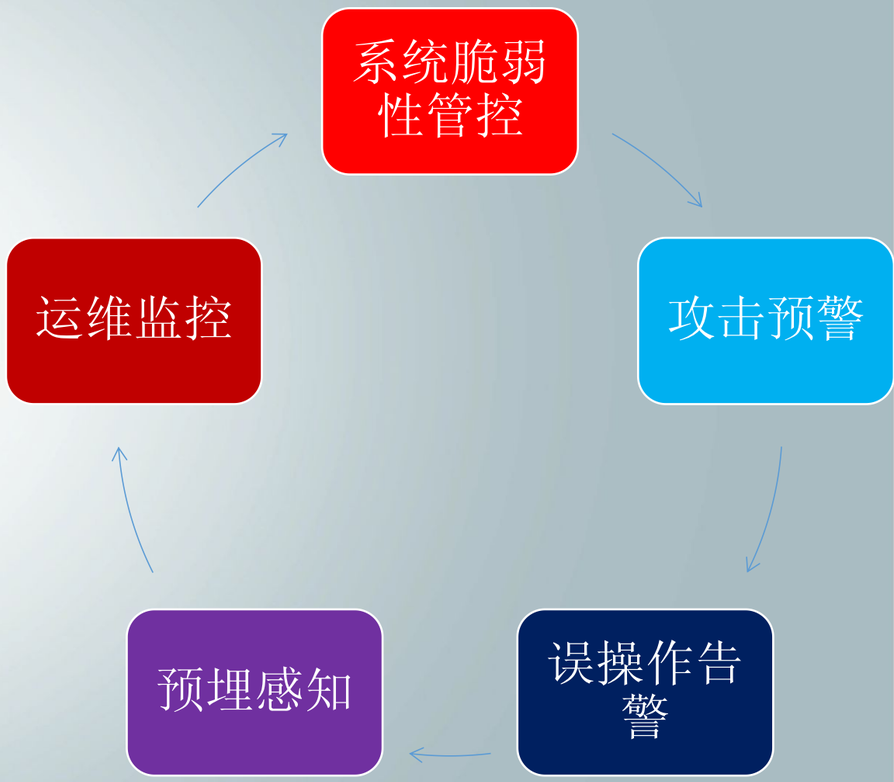
工控安全预警平台 IT&OT

流量子系统平台 | 协议子系统平台 | 行为子系统平台

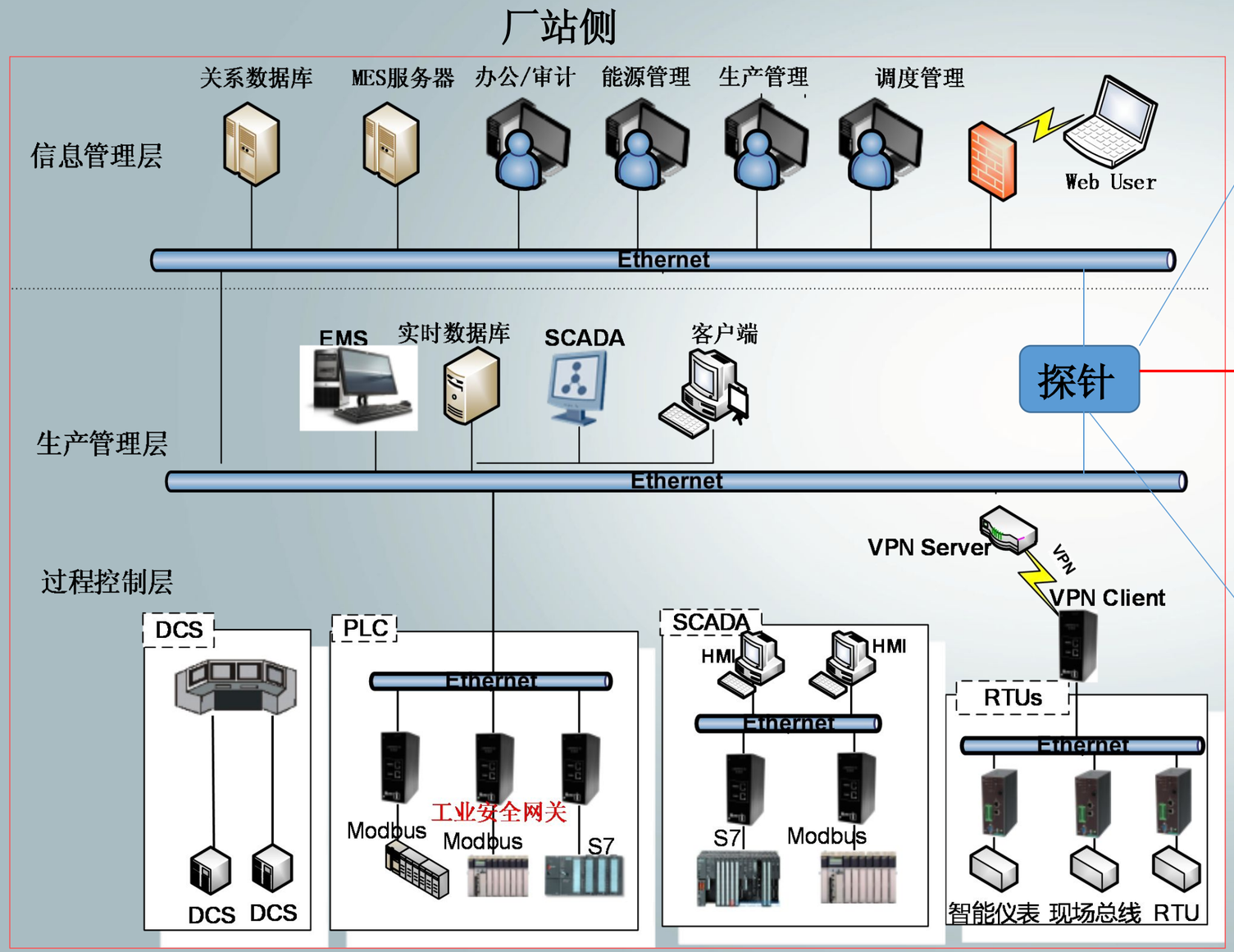
流量日志 | 流量基线 | 协议分布 | 异常协议 | 操作审计 | 规程基线

流量探针 | 流量统计分析 | 流量DPI | 协议分析器 | 组态监测 | 操作行为监控

组态软件 | 监视软件 | 网络设备 | 安全设备 | 控制器



工控安全预警平台



采集数值范围的log信息

通信基线

操作基线

流量基线

协议基线

协议规约解析

规程定制

全流量获取，取证分析

2016
LET'S START RIGHT NOW

NSFOCUS

入网测试

态势感知

工控安全

边界防护

深度防御

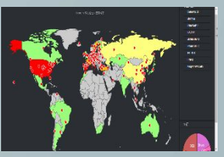
工控扫描及漏洞挖掘

国内第一款工控漏扫检测产品亚太地区唯一进入Garter视野的工业专用漏洞检测产品

工业安全网关及工业隔离装置

工业入侵检测机及工业异常行为审计

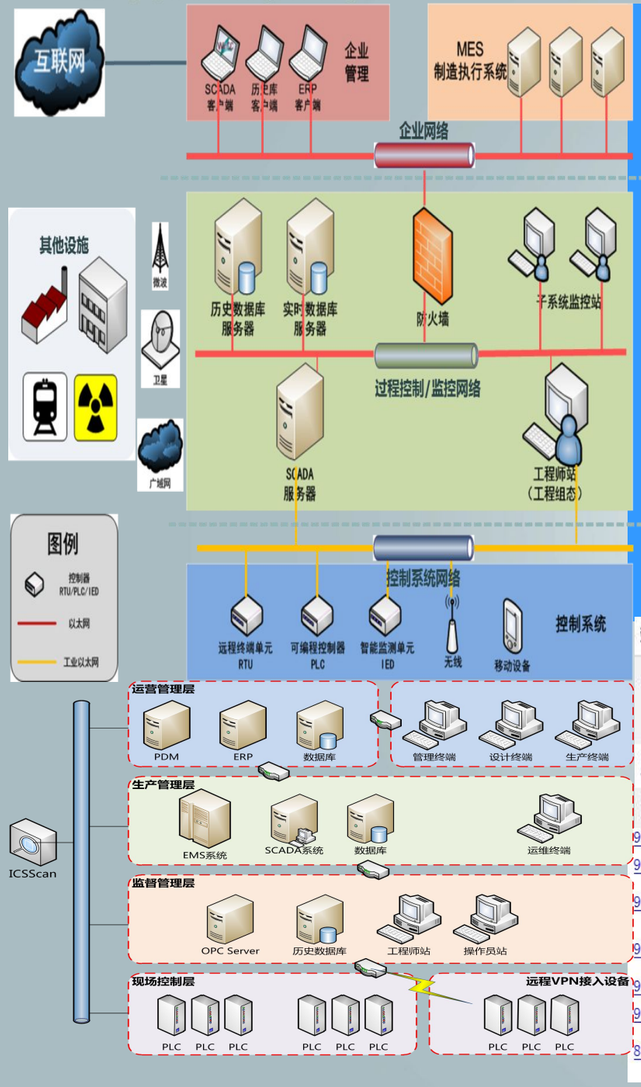
工业网络故障录波装置



工业安全监测与预警平台

2016
LET'S START RIGHT NOW

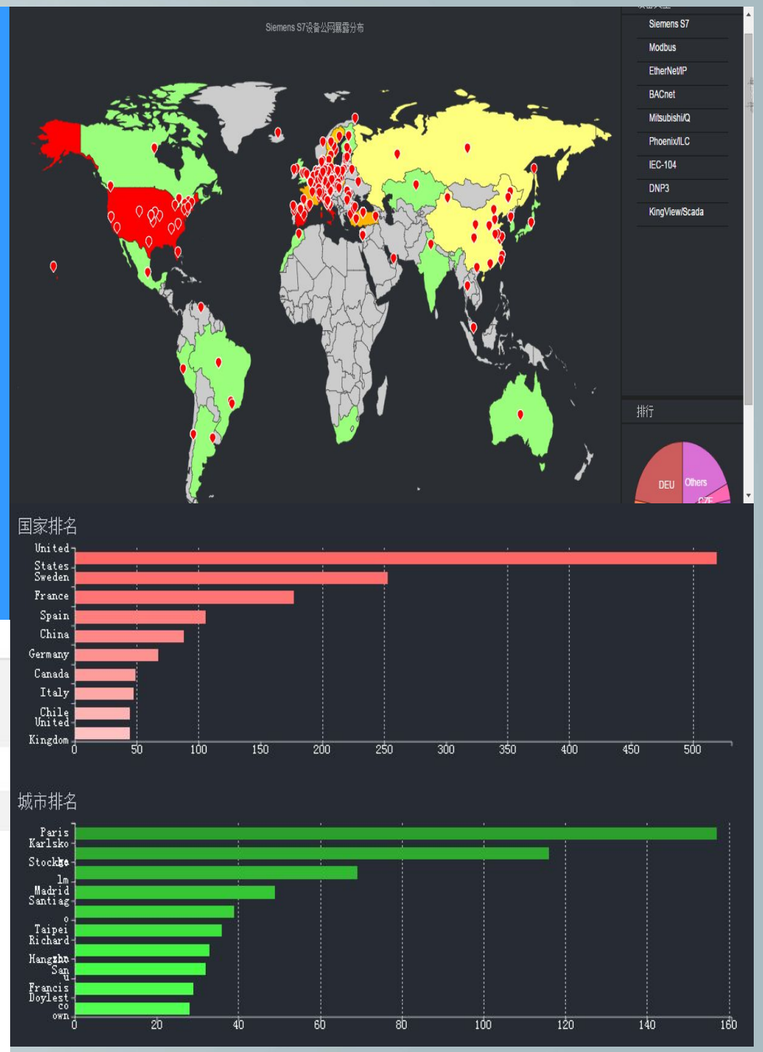
NSFOCUS



1）工业漏洞库覆盖广
◆ 支持400+的工业漏洞
◆ 支持上位机、控制器和工业通信设施
2）支持嵌入式操作系统漏洞检测
◆ 支持VXWORDK
◆ 嵌入式LINUX
◆ QNX系统
3）现场级的无损扫描技术
◆ 应用于电力、石化石化、燃气等能源行业的现场扫描
◆ 应用于烟草、军工等制造业等行业的现场扫描
◆ 应用于轨道交通、市政处理等行业的现场扫描
4）可识别国外主流厂家的工业协议
IEC 60870-5-104、IEC 601850 、DNP3、MODBUS、OPC、PROFIENT 、S7、ETHENET/IP

端口	协议	服务	漏洞
--	--	--	ICMP timestamp请求响应漏洞 允许Traceroute探测
21	TCP	ftp	FTP服务器版本信息可被获取
17185	UDP	soundsvirtual	检测到VxWorks启用了不安全的WDB服务

97727	2013-09-25	Schneider Electric SCADA Expert ClearSCADA Crafted Web Request Handling Remote DoS
96752	2013-08-29	MatrikonOPC SCADA DNP3 OPC Server Crafted DNP3 Packet Handling DoS
95864	2013-06-18	General Electric (GE) Proficy HMI/SCADA - CIMPLICITY CimWebServer.exe Broadcase/Init Crafted Request szOptions Field Handling Stack Buffer Overflow
95865	2013-06-18	General Electric (GE) Proficy HMI/SCADA - CIMPLICITY CimWebServer.exe Password Decoding Crafted Request szPassword Field Handling Stack Buffer Overflow
93851	2013-04-08	WellinTech KingSCADA XML External Entity (XXE) Injection Arbitrary File Access
91136	2013-03-11	Clorius Controls ICS SCADA /html/info.html Internal IP Address Remote Disclosure
89489	2013-01-22	General Electric (GE) Intelligent Platforms Proficy HMI/SCADA - CIMPLICITY CimWebServer Crafted Packet Parsing Remote Command Execution



NSFOCUS

THANKS