SIEMENS

西门子(中国)有限公司 | 胡建钧 | 2013

从检测到防护，构建安全的工业控制系统

主要内容

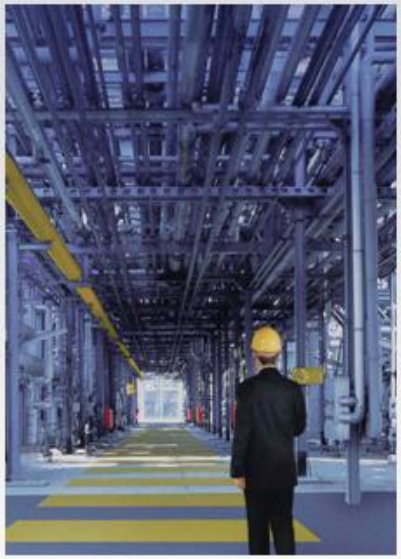
信息安全的新战场 - 工业基础设施

工业基础设施构成了我国国民经济、现代社会以及国家安全的重要基础，而工业基础设施的核心是其工业控制系统（ICS）

与传统的IT信息安全不同，工业基础设施中关键ICS系统的安全事件会导致：

- 系统性能下降，影响系统可用性
- 关键控制数据被篡改或丧失
- 失去控制
- **环境灾难**
- **人员伤亡**
- 公司声誉受损
- **危及公众生活及国家安全**
- **破坏基础设施**
- 严重的经济损失等

工业基础设施面临安全威胁



工业信息安全就是要为工业自动化系统提供安全防护

目前，工业基础设施面临的安全威胁包括：

- 窃取数据、配方等
- 破坏制造工厂
- 由于病毒、恶意软件等导致的工厂停产
- 操纵数据或应用软件
- 对系统功能的未经授权的访问

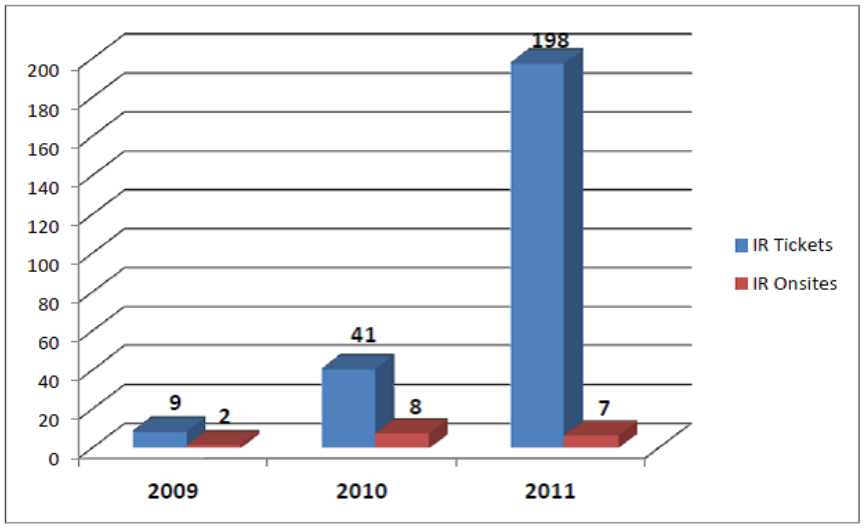
近年来，各种安全事件已经充分说明当前工业自动化控制系统存在着安全脆弱性

美国的工业安全事件分布- 源自ICS-CERT

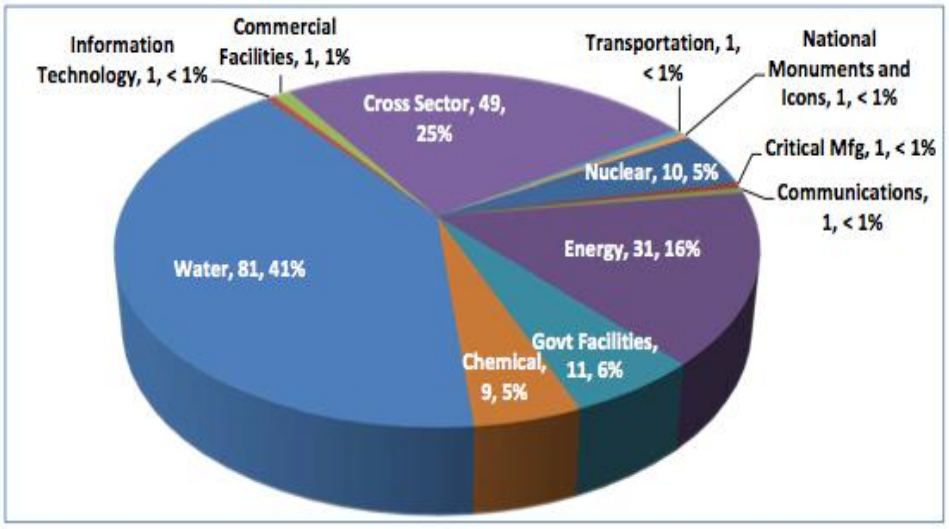
The ICS-CERT Incident Summary Annual Report tells the story

Cyber threats to Industrial Control Systems (ICS) are on the rise

There is a critical need to protect our critical infrastructure from cyber attacks



ICS-CERT incident response trends data



Incident reports by sector (2011)

搜索互联网可见的工业控制系统

Shodan and ERIPP

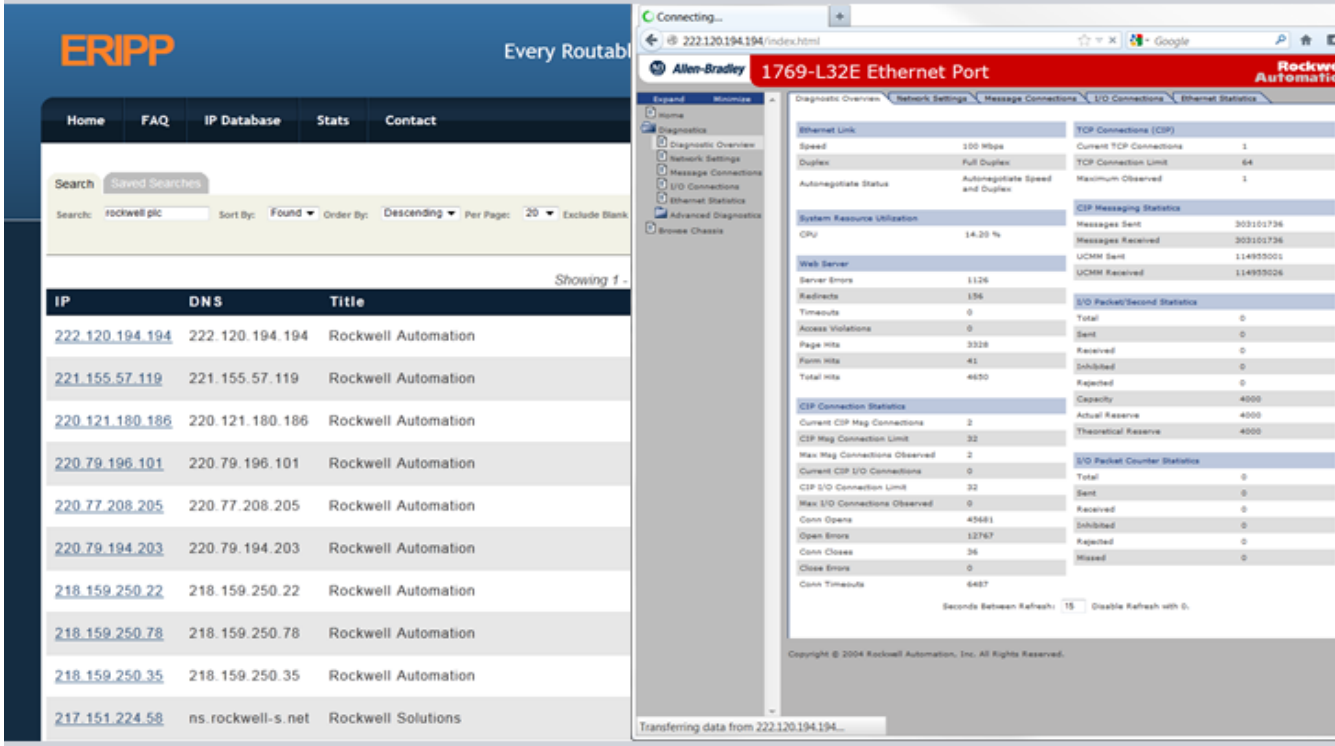
通过互联网搜索引擎即可发现在公网上的工业控制设备

The search engines:

http://www.shodanhq.com/
http://eripp.com/

Search Results for "Simatic PLC"

Search Results for "Rockwell PLC"



主要内容

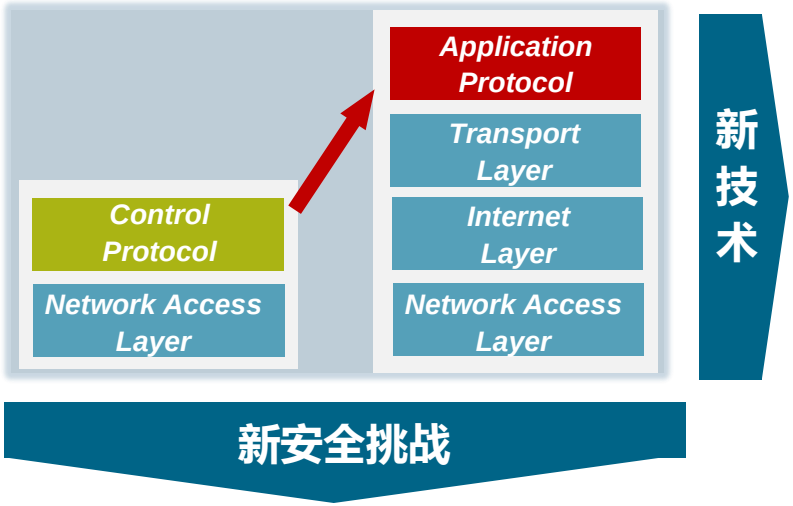
一 信息安全的新战场 - 工业基础设施

二 工业基础设施安全需求分析

三 工业信息安全解决方案：纵深防御

四 总结

工业基础设施领域面临全新的安全挑战



越来越多的基础设施工业领域开始采用最新的IT技术

- 将TCP/IP作为网络基础设施，将工业控制协议迁移到应用层
- 提供各种无线网络接入
- 广泛采用标准商用操作系统、设备、中间件与各种应用

从而，越来越多的工业控制网络正由封闭、私有转向开放、互联

在享受IT技术带来的益处的同时，针对工业控制网络的安全威胁也在与日俱增

- 设备/软件/应用的互联使得攻击能够很容易地借助于TCP/IP网扩展到其他系统
- 应用层安全成为了ICS系统的关键
- 传统的IT安全解决方案不足以应对工业基础设施领域的全新安全需求

工业控制网络技术演变趋势

以前与现在		现在与将来
▪ 封闭、专有系统	趋势	▪ 开放系统，并大规模采用IT技术
▪ 通信是以独立的解决方案提供给用户		▪ 集成化网络系统，并与IT基础设施充分互联，以实现远程控制和互操作性能
▪ 只有生产部门负责工业通信的运营		▪ IT部门与生产部门共同负责自动化网络运营
▪ 很少用到安全机制		▪ 综合全面的安全防范解决方案
▪ 面向产品的服务		▪ 面向解决方案的服务

工业控制网络需要一种最优化的安全概念和解决方案！

工业控制网络安全首要目标

商业信息网络

“确保信息的保密性”

可以容许服务中断

过程控制系统

“不可中断的连续运行和实时系统可用性”

服务中断可能造成巨大的生产损失

工业基础设施的典型脆弱性

管理制度缺陷
- 移动设备滥用
- 高危敏感操作
- 远程控制与破坏

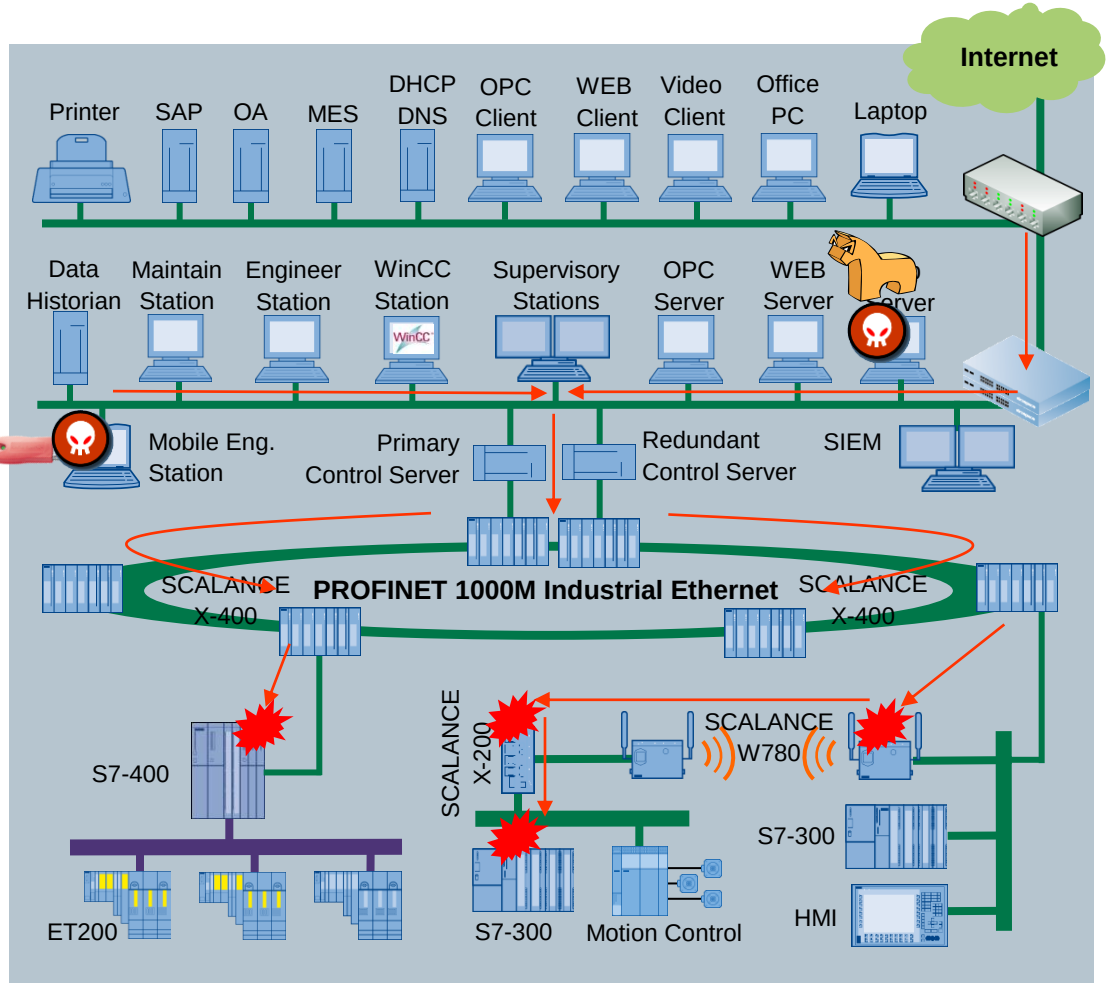
平台缺陷
- 老旧系统
- 软硬件缺陷
- 病毒木马攻击

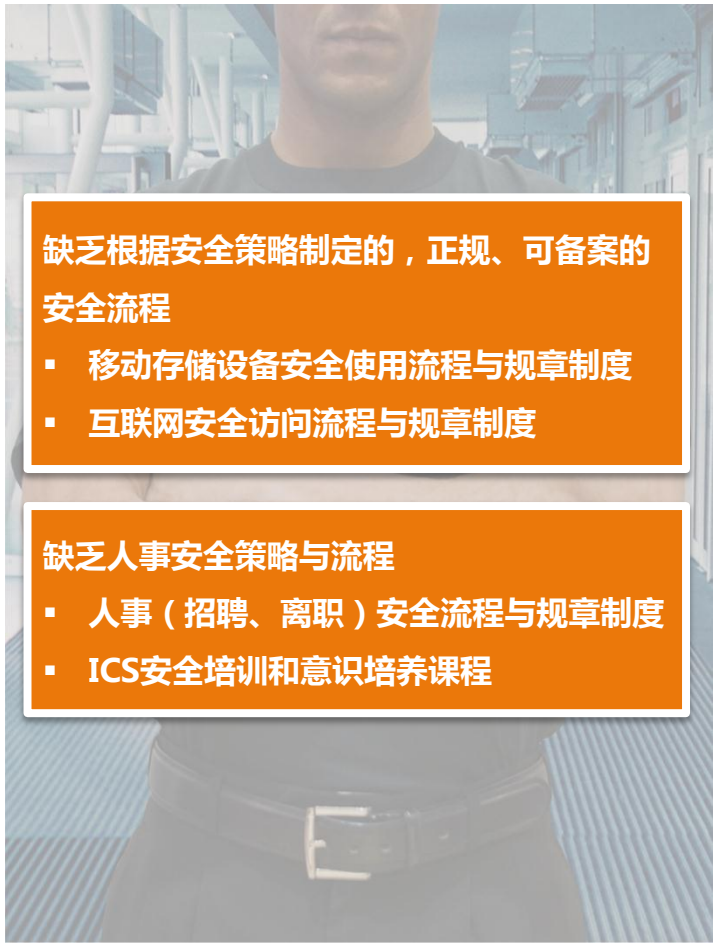
不安全的网络
- OPC安全攻击
- 网络拓扑不合理
- 无线网络

不安全的配置
- 弱口令，账号共用
- 开放不必要的服务与端口
- 不安全的版本

安全威胁危及工控系统的可用性，甚至导致严重的安全事故

案例： 移动存储介质与系统滥用





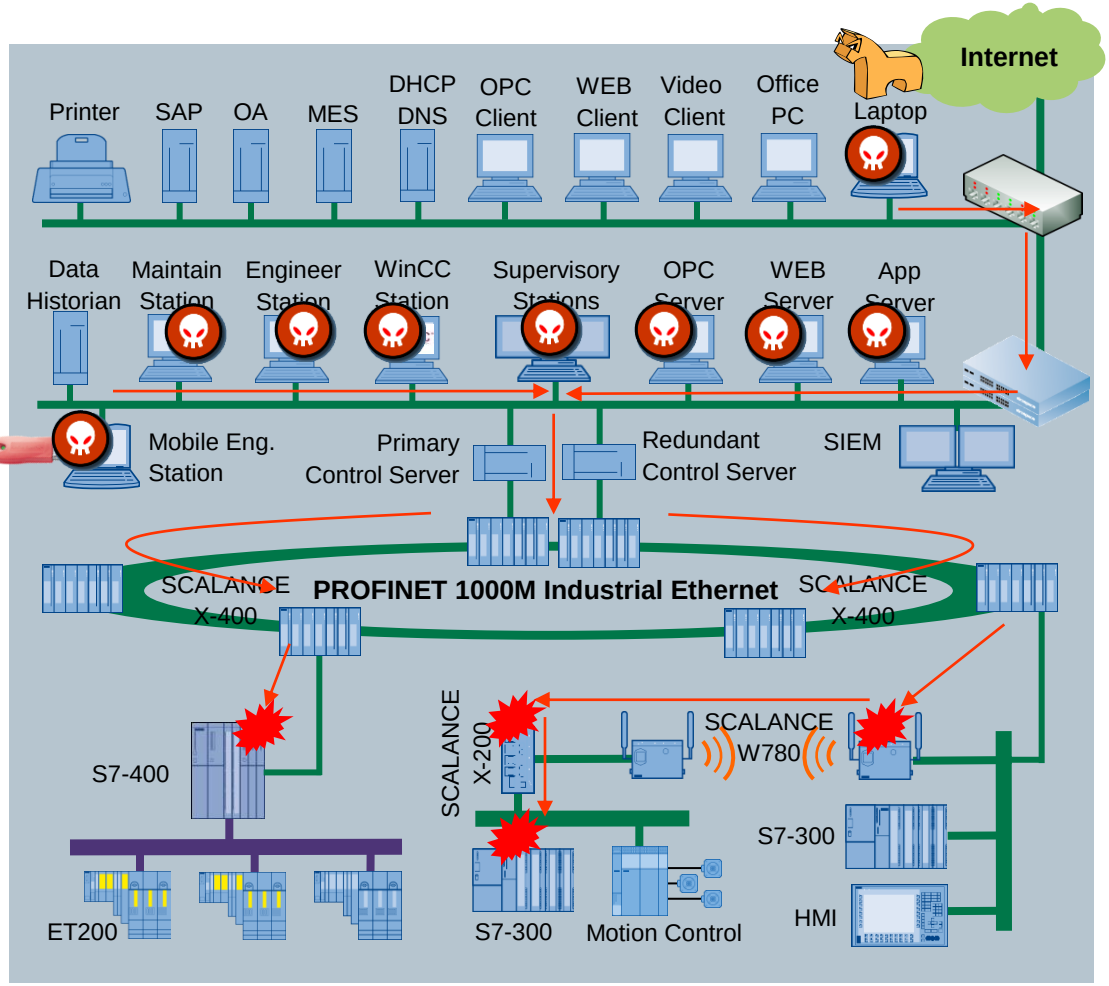
缺乏根据安全策略制定的，正规、可备案的安全流程

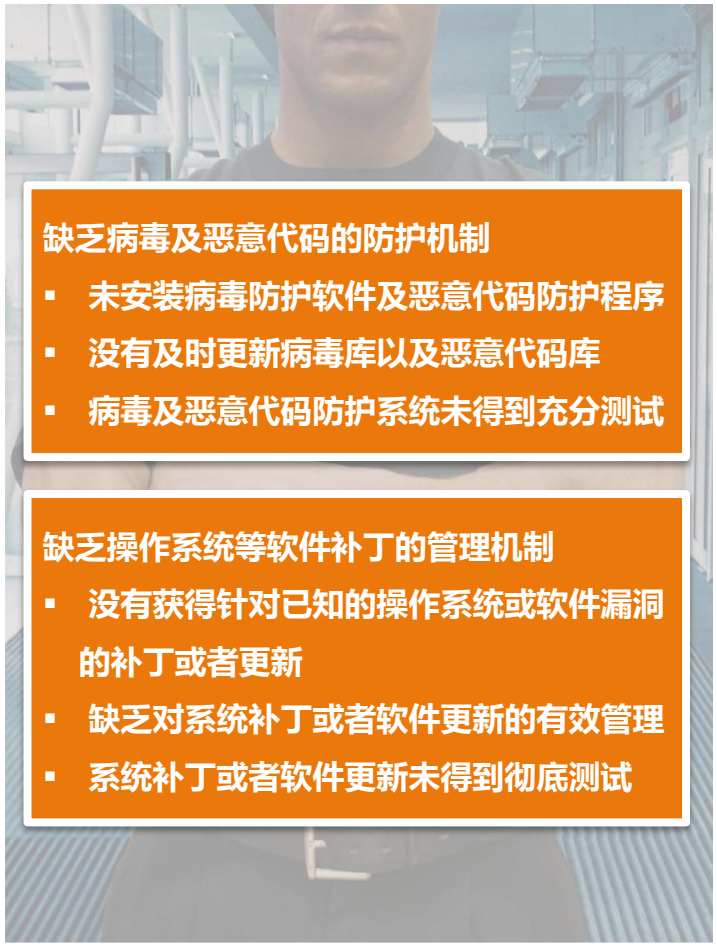
- 移动存储设备安全使用流程与规章制度
- 互联网安全访问流程与规章制度

缺乏人事安全策略与流程

- 人事（招聘、离职）安全流程与规章制度
- ICS安全培训和意识培养课程

案例:病毒、恶意软件与补丁管理





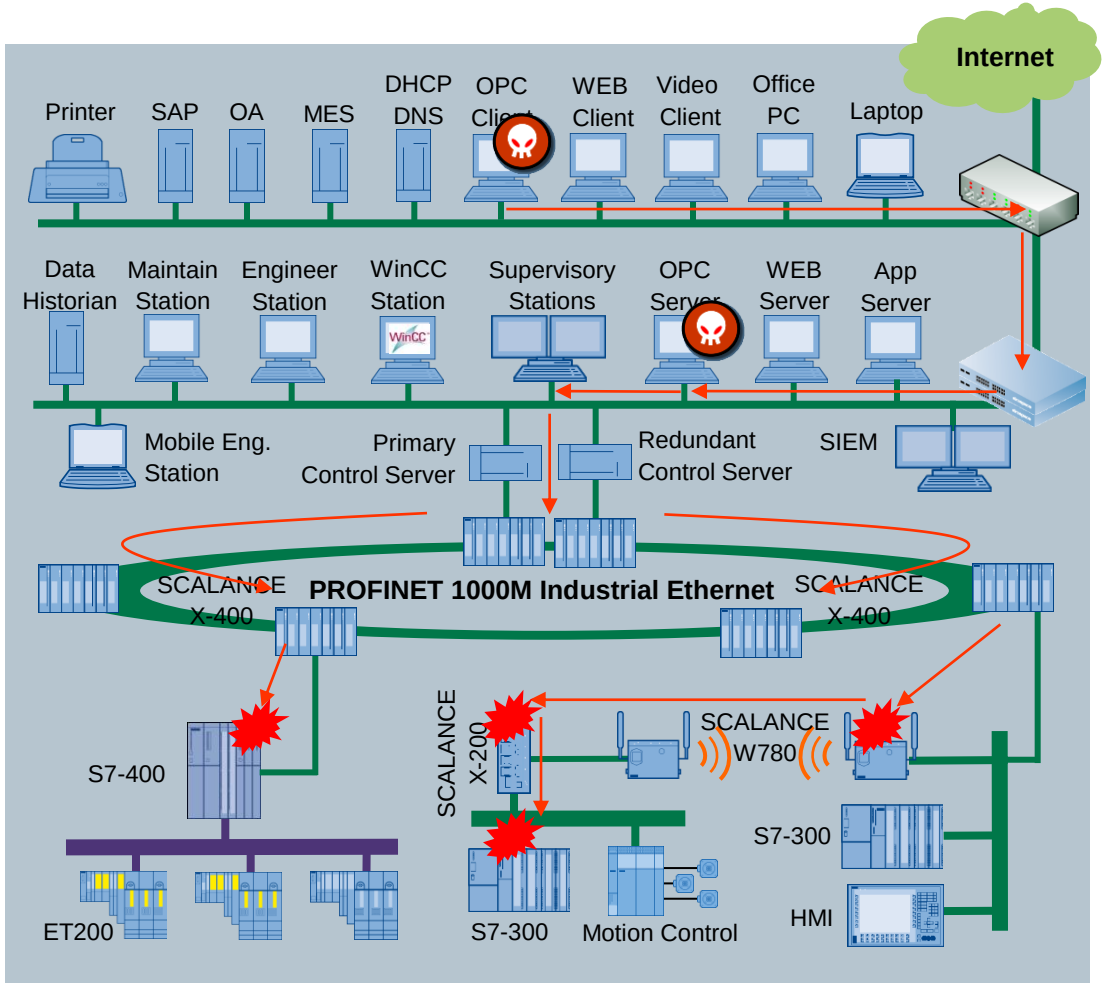
缺乏病毒及恶意代码的防护机制

- 未安装病毒防护软件及恶意代码防护程序
- 没有及时更新病毒库以及恶意代码库
- 病毒及恶意代码防护系统未得到充分测试

缺乏操作系统等软件补丁的管理机制

- 没有获得针对已知的操作系统或软件漏洞的补丁或者更新
- 缺乏对系统补丁或者软件更新的有效管理
- 系统补丁或者软件更新未得到彻底测试

案例：OPC通信安全



OPC服务器采取动态端口分配机制

- 通讯端口在会话中协商，无固定端口，因此无法使用传统防火墙进行防护
- 所有端口默认处于打开状态，给病毒木马、恶意代码和黑客入侵提供可趁之机

OPC的访问权限控制开放、繁琐

- 各个OPC厂商对访问权限要求不一，开放给用户配置，暴露出严重安全隐患
- 配置步骤繁琐，易于出错，且检查难度大

RPC\DCOM安全漏洞频发，易被病毒利用

- 不同的OPC厂商采取不同的
- 配置繁琐，检查难度大，易于出错
- RPC\DCOM安全漏洞频发，易被病毒利用

工信部：关于加强工业控制系统信息安全管理的通知

SIEMENS

2011年，工业与信息化部发布“**关于加强工业控制系统信息安全管理的通知**”，明确了重点领域工业控制系统信息安全管理要求，并强调了“谁主管谁负责、谁运营谁负责、谁使用谁负责”的原则

（一）连接管理要求

- 断开工控系统与公共网络间的不必要的连接
- 对必要的连接，部署防火墙等进行防护，并定期评估
- 严格控制移动存储介质

（二）组网管理要求

- 同步规划、同步建设、同步运行安全防护措施
- 采取VPN、数据加密等措施，保护工控远程通信
- 对无线组网采取严格的身份认证、安全监测等防护措施

（三）配置管理要求

- 建立安全配置与审计制度
- 严格账户管理，合理分类设置账户权限
- 严格口令管理
- 定期对账户、口令、端口、服务等进行检查

（四）设备选择与升级管理要求

- 慎重选择工业控制系统设备
- 加强对技术服务的信息安全管理
- 密切关注产品漏洞和补丁发布

（五）数据管理要求

- 对国家基础数据以及其他重要敏感数据，采取访问权限控制、数据加密、安全审计、灾难备份等措施加以保护

（六）应急管理要求

- 制定工业控制系统信息安全应急预案，明确应急处置流程和临机处置权限，落实应急技术支撑队伍，采取必要的容灾备份措施

主要内容

一 信息安全的新战场 - 工业基础设施

二 工业基础设施安全需求分析

三 工业信息安全解决方案：纵深防御

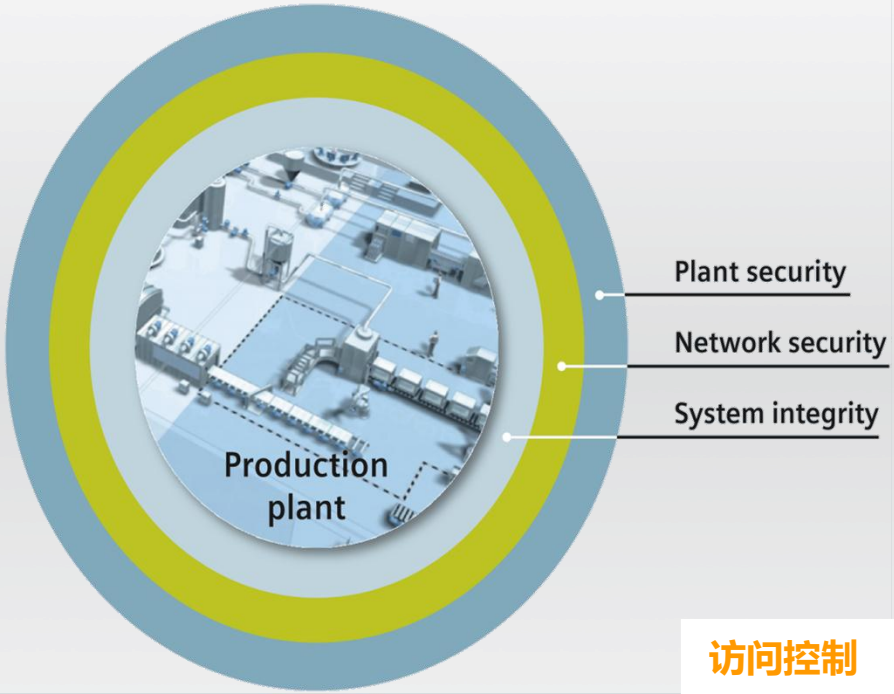
四 总结

西门子工业信息安全：从检测到防护

组件		工业信息安全服务
	**风险评估与安全管理咨询**	**提供建议与实施支持**
	**模块化的安全解决方案** 认证与访问控制 / 防火墙、VPN 补丁与配置管理 / 防病毒与软件白名单 工控协议安全网关 / 安全事件监控与管理	**模块化的解决方案**
	**安全培训、加固、监控、优化**	**可管理的服务**

工业控制安全：基本的工业安全防护层次

工业控制场景下的安全解决方案必须考虑所有层次的安全防护



工厂安全

- 对未经授权的人员阻止其访问
- 物理上防止对关键部件的访问

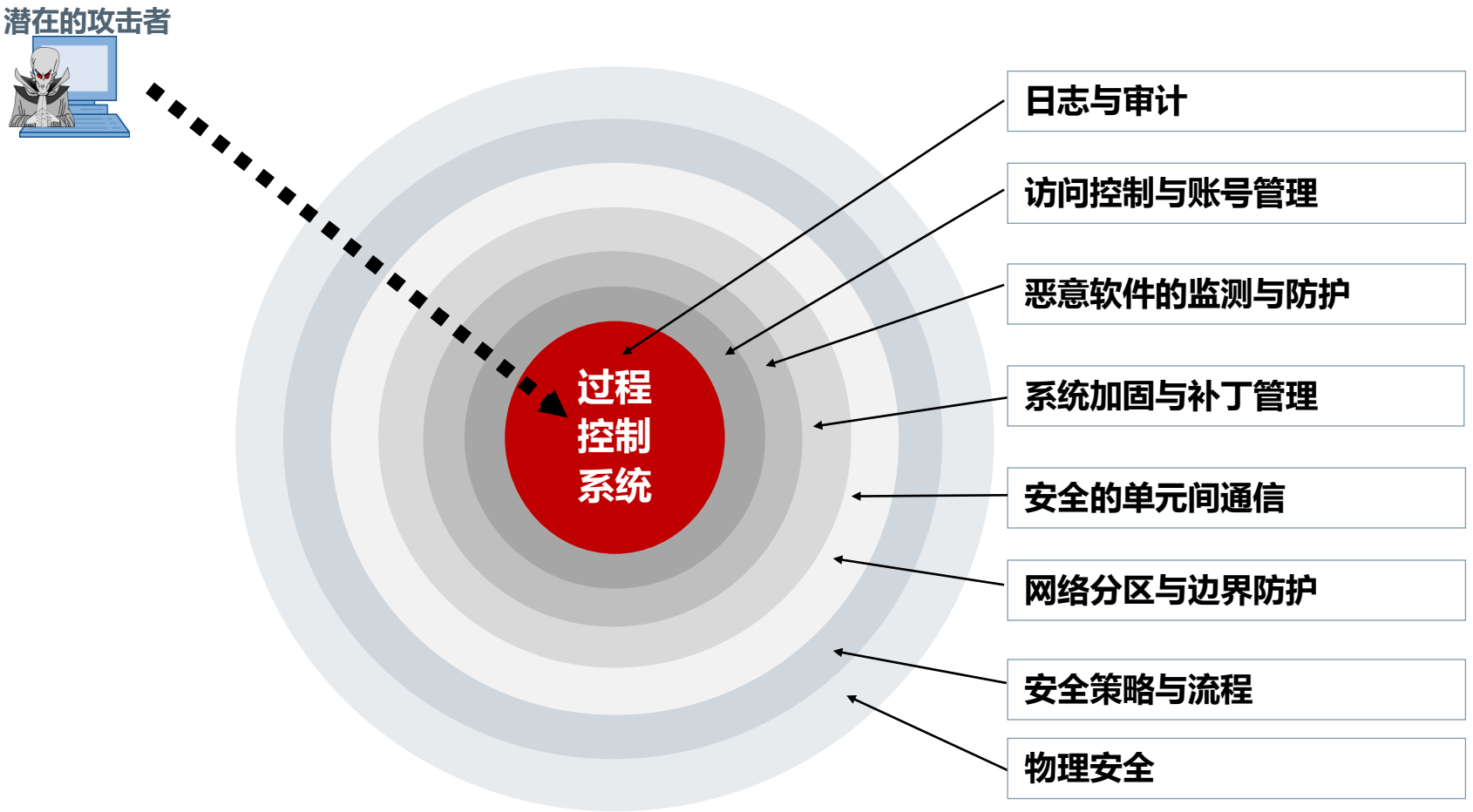
工厂IT安全

- 采用防火墙等技术对办公网与自动化控制网络之间的接口进行控制
- 进一步对自动化控制网络进行分区与隔离
- 部署反病毒措施，并在软件中采用白名单机制
- 定义维护与更新的流程

访问控制

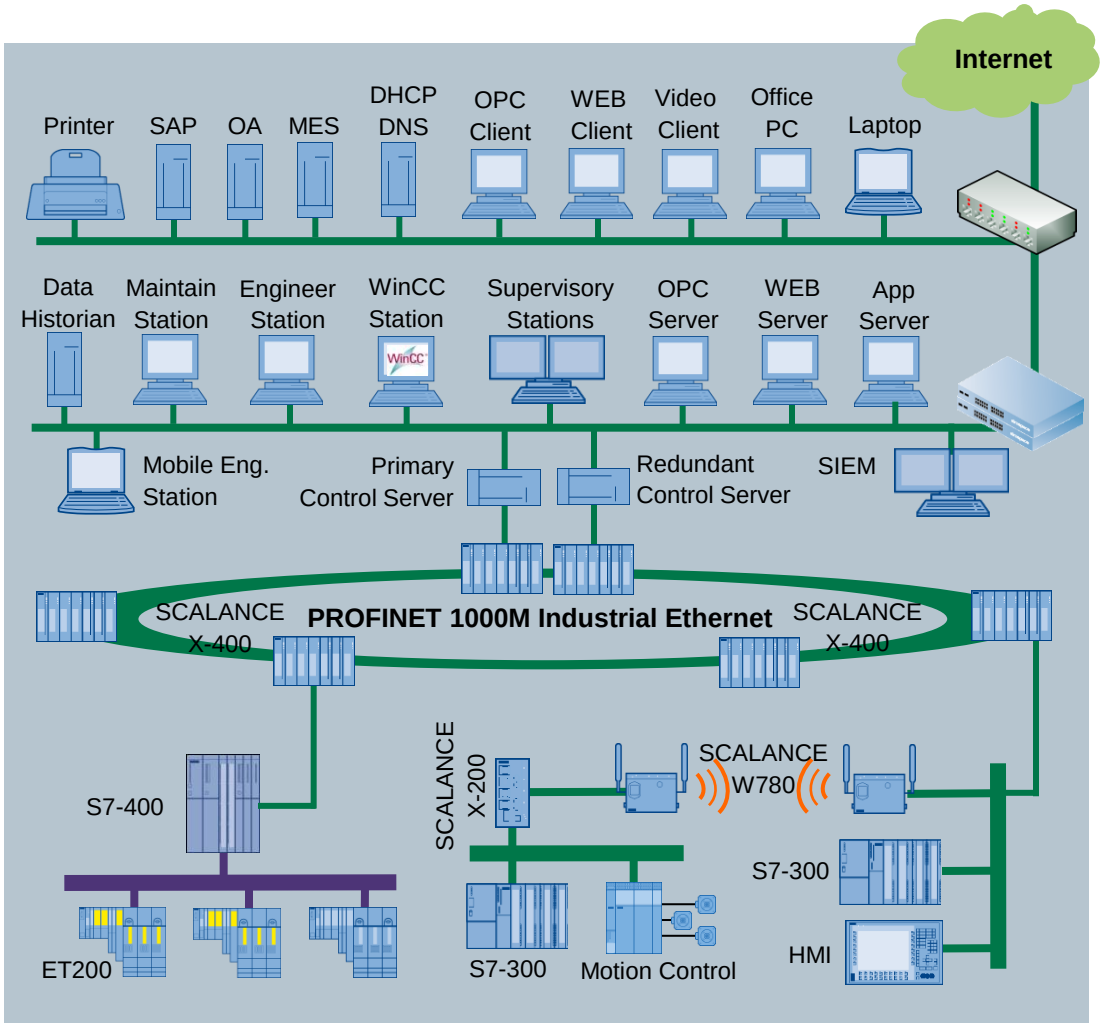
- 对自动化控制设备与网络操作员进行认证
- 在自动化控制组件中集成访问控制机制

工业网络纵深防御体系框架



将“纵深防御”引入过程控制系统的信息安全解决方案 ：在外部世界的威胁和工控网络之间建立**尽可能多层次的**保护。

建立工业网络纵深防御



第一阶段：评估

风险评估

第二阶段：规划

安全规划

第三阶段：执行

按照纵深防御理念构建安全防护体系，包括网络分区与隔离，访问控制，系统加固、补丁管理等

第四阶段：改进

持续改进的安全管理

基于IEC 62443工控安全评估规范的评估

评估分为管理评估和系统能力（技术）评估

- 管理评估宜对照风险接受准则和组织机构相关目标，识别、量化并区分风险的优先次序

工业控制系统信息安全评估规范&验收规范

表A.1 信息安全管理评估列表

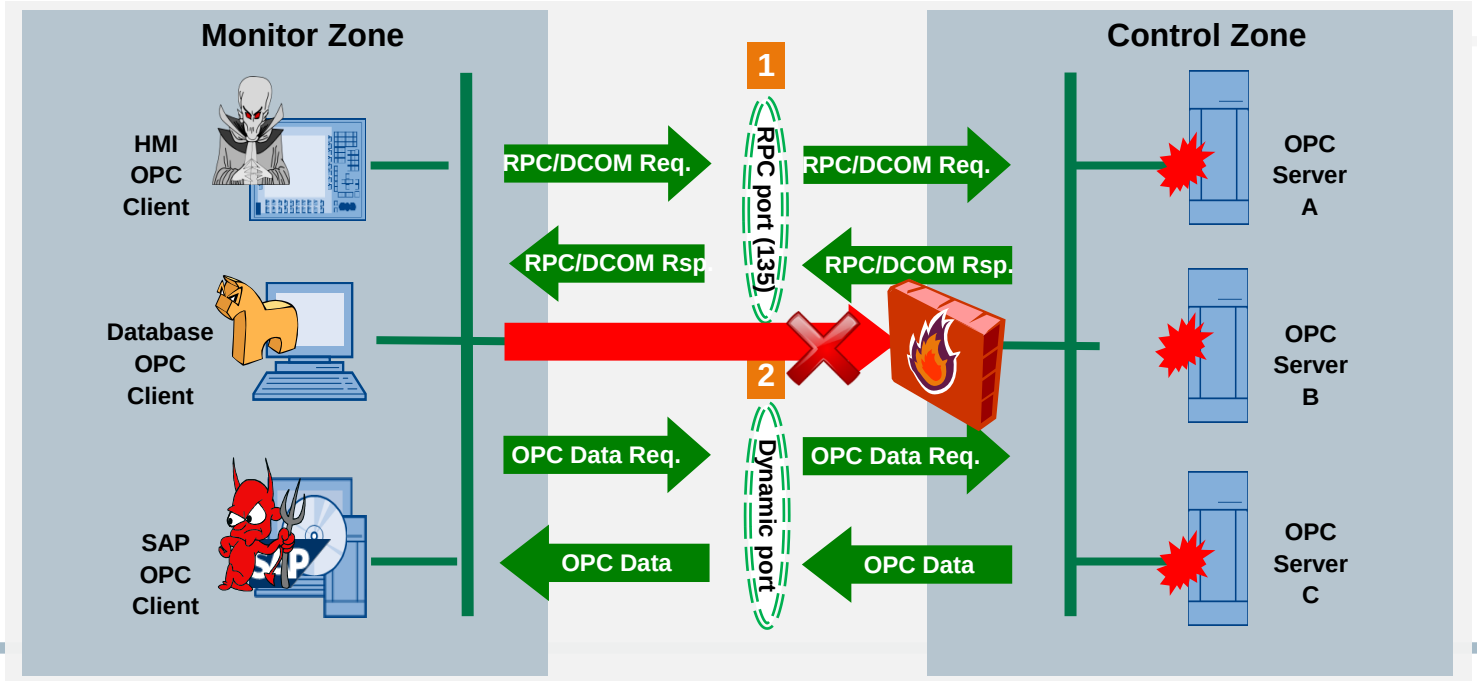
	BL 1	BL 2	BL 3
5.1 安全方针			
5.1.1 信息安全方针			
要求：依据业务要求和相关法律法规提供管理指导并支持信息安全			
5.1.1.1 信息安全方针文件	✓	✓	✓
5.1.1.2 信息安全方针的评审	✓	✓	✓
5.2 信息安全组织机构			

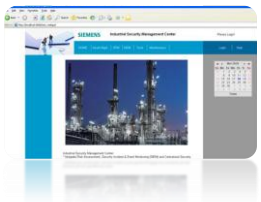
表A.1 系统要求和增强要求与安全等级的映射 （打对勾表示为该等级必须满足项）

RE (2)不可信网络的多因子认证			√	√	否
RE (3) 对所有网络的多因子认证				√	否
SR 1.2 – 账号管理	√	√	√	√	是
SR 1.3 – 标识符管理	√	√	√	√	是
RE (1) 用户不活跃时间超限时禁用该用户身份		√	√	√	是
SR 1.4 认证码管理	√	√	√	√	是
RE (1)软件进程身份凭证的硬件安全			√	√	否
SR 1.5 口令认证的加强		√	√	√	是
RE (1) 口令生成限制			√	√	是
RE (2) 口令生命周期限制				√	是
SR 1.6 公钥认证加强		√	√	√	否
SR 1.7 认证反馈	√	√	√	√	是
SR 1.8 失败的登陆尝试	√	√	√	√	是
SR 1.9 系统使用通知	√	√	√	√	是
SR 1.10 经由不可信网络的访问	√	√	√	√	是
RE (1) 默认拒绝所有原则			√	√	是
SR 1.11 设备认证		√	√	√	否

评估列表&等级映射示例

工业信息安全：OPC安全防护 -Janus



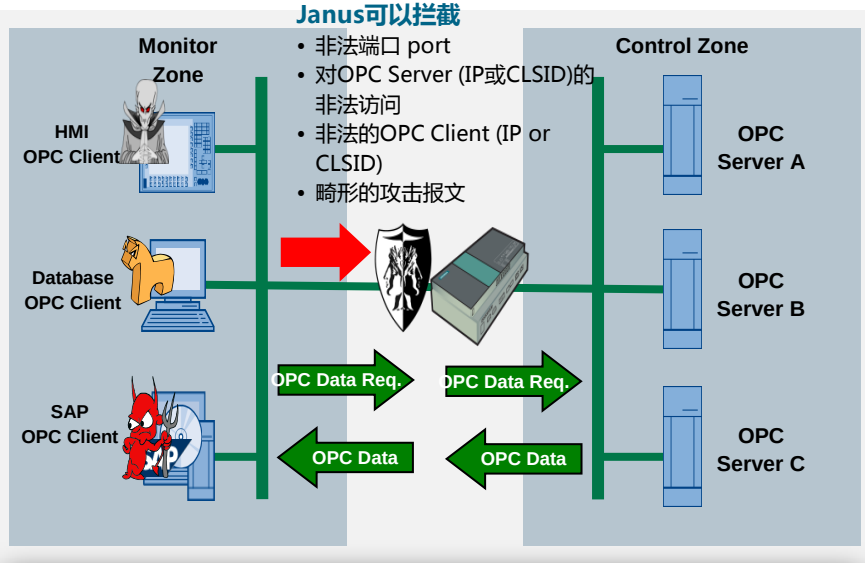


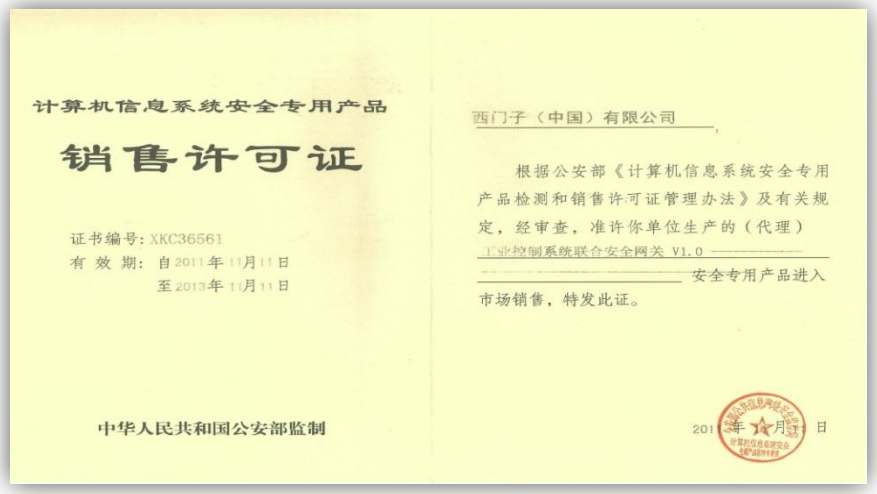
Janus对OPC的安全防护

•不同于传统防火墙，Janus可以动态知晓正常OPC通信所需端口，做到随用随开，通信结束后自动关闭

•Janus把安全防护从IP/端口进一步提升到应用级，它还通过应用ID来识别访问请求是否合法，实现细粒度的访问控制

工业信息安全：OPC安全防护 –Janus（续）




计算机信息系统安全专用产品

销售许可证

证书编号：XKC36561

有 效 期：自2011年11月11日

至2013年11月11日

西门子（中国）有限公司

根据公安部《计算机信息系统安全专用产品检测和销售许可证管理办法》及有关规定，经审查，准许你单位生产的（代理）工业控制系统联合安全网关 V1.0 安全专用产品进入市场销售，特发此证。

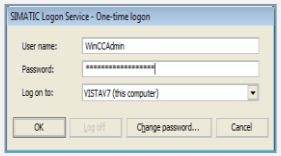
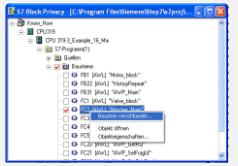
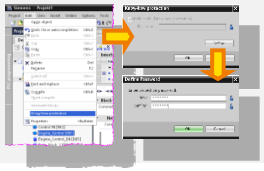
中华人民共和国公安部监制

2011年11月11日

Janus–工业自动化控制系统联合安全网关

- 基于西门子高性能工业级硬件平台SIMATIC Box ，具有极强的环境适应能力
- 应对病毒木马、网络入侵以及恶意软件等多种安全威胁，为工业控制系统提供联合、可灵活定制的安全防护
- 提供基于状态的工业级专用防火墙
- 支持应用层工业协议深度报文检测技术，将安全防护由网络层扩展至应用层
- 提供OPC网络增强式防护，阻断非法的数据通讯 ，确保OPC系统安全可靠运行
- 全中文集中式管理控制平台统一管理网络中的所有工业安全设备，易于配置及管理
- 提供特有的可视化安全统计报表，工业网络整体安全现状及风险一目了然
- 通过公安部信息安全产品检测并颁发销售许可

工业信息安全：访问控制

西门子解决方案	描述	
SIMATIC Logon	基于SIMATIC Logon提供用户管理与安全认证，支持Windows domain与Work Group	
反病毒与白名单	抵御病毒、蠕虫、木马的攻击，阻止未授权的应用及恶意软件	TREND MICRO, McAfee virusscan, symantec.
STEP 7 V5	提供改进的知识产权（控制程序）保护与拷贝保护	
WinCC V7	提供安全的SCADA，支持用户管理、变更控制、审计等	
STEP 7 V11	提供改进的知识产权（控制程序）保护与拷贝保护	

工业信息安全： 防火墙、VPN

防护自动化单元

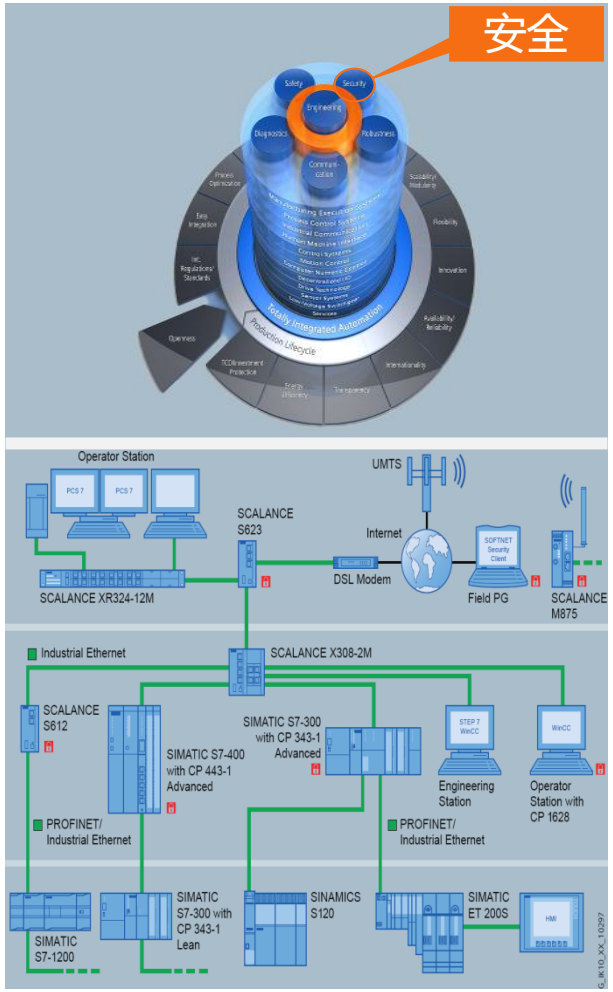
基于微软的TMG，一般部署在ERP与MES，及MES与DCS之间

- 应用层防火墙
- URL过滤，web防护
- 防病毒
- VPN功能

工业防火墙、VPN SCALANCE S，CP

一般部署在控制单元边界

- SCALANCE S
- Softnet安全客户端
- 最新的CP 343-1 Advanced 与CP 443-1 Advanced通信处理器集成了VPN与防火墙，为工业控制设备提供安全防护
- CP 1628通信处理器可以向工业PC提供防火墙与VPN防护



工业信息安全：配置管理

配置安全

- 未打补丁的系统、产品
- 错误的配置
- 不恰当的系统架构与网络拓扑

合规性

- ISA 99，NERC CIP等等
- 本地法规（等级保护）
- 企业安全规范
- 行业安全最佳实践

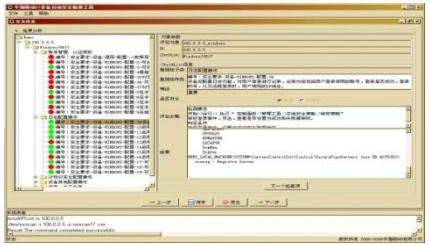
需求

- 高度自动化
- 支持不同的系统与设备
- 易于使用

功能	西门子工业安全基线检查工具
支持的系统与平台	**Industry applications**: WinCC, PCS7, etc. **OS**: Windows, Solaris, AIX, HP-UX, Linux, etc. **Database**: SQLServer, Oracle , DB2, etc. **Network Device**: Cisco, Juniper, Huawei, etc. **Middleware**: IIS, Weblogic, Webshpere, Tomcat, etc.
使用方式	Local or remote checking
可配置性	All the item in checklists are configurable
报表	Support enterprises' templates, including word, excel, pdf, and html version
可扩展性	New checklists and items can be updated/customized
安全性	No impact to targets, the results is encrypted and protected
部署方式	Standalone version for laptop & workstation, B/S version

工业安全基线检查工具

覆盖整个工业系统配置安全，包括网络、操作系统、中间件与控制应用等。



工业安全培训服务

培训形式包括专家面授、安全课件、演示和操作平台等

西门子工业技术培训中心

工业信息安全培训课程 ICS- Security Training
（A 7413）

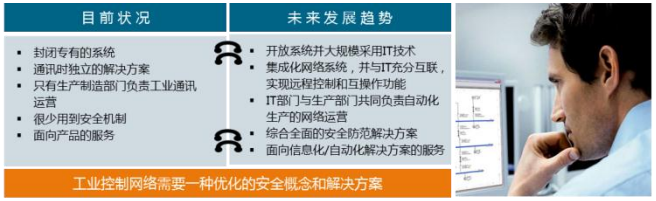
课程长度：2天

在信息化与工业化融合的大背景下，工业控制系统正面临前所未有的安全挑战与威胁，典型的有针对伊朗核设施的“震网”病毒，阿拉伯产油国的“火焰”病毒等。这些安全事件表明工业领域的信息安全已经成为新的战场。

工业信息安全对生产企业的重要性，已经显得越来越重要。如何保护我们的生产安全，如何保护我们的设备安全，如何保护我们的信息安全？

西门子，给您专业的解答！

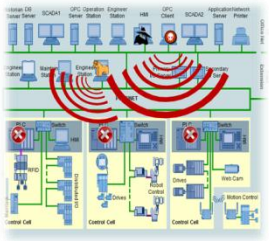
扫描二维码，快速访问西门子工业技术培训中心网站



课程目标

- 在本课程中，您将通过案例分析与攻击演示实地感受工控网络面临的安全威胁与风险，挖掘典型需求，学习国内外工业信息安全相关标准与前沿技术，熟悉西门子信息安全相关产品功能与配置操作，最后通过大量实践，获得如何通过纵深防御理念来构建工业信息安全防护体系的有关知识。
- 完成课程后，您将了解工业信息安全领域常见的威胁、风险、需求等，并掌握如何结合自身实际情况，设计并实施工业安全纵深防御体系，保护关键基础设施的安全。

采用案例式教学，逐项分析每一项工业安全威胁的处理方式



培训内容

- 工业信息安全背景、案例及攻击演示
- 工业信息安全需求分析，相关标准规范
- 西门子工业信息安全解决方案
- 西门子工业安全产品功能与配置操作（防火墙、安全网关、防病毒等）
- 典型工业控制网络纵深防御部署方案设计与实施

提供从威胁检测到安全防护的全面知识，并涉及主要服务和产品

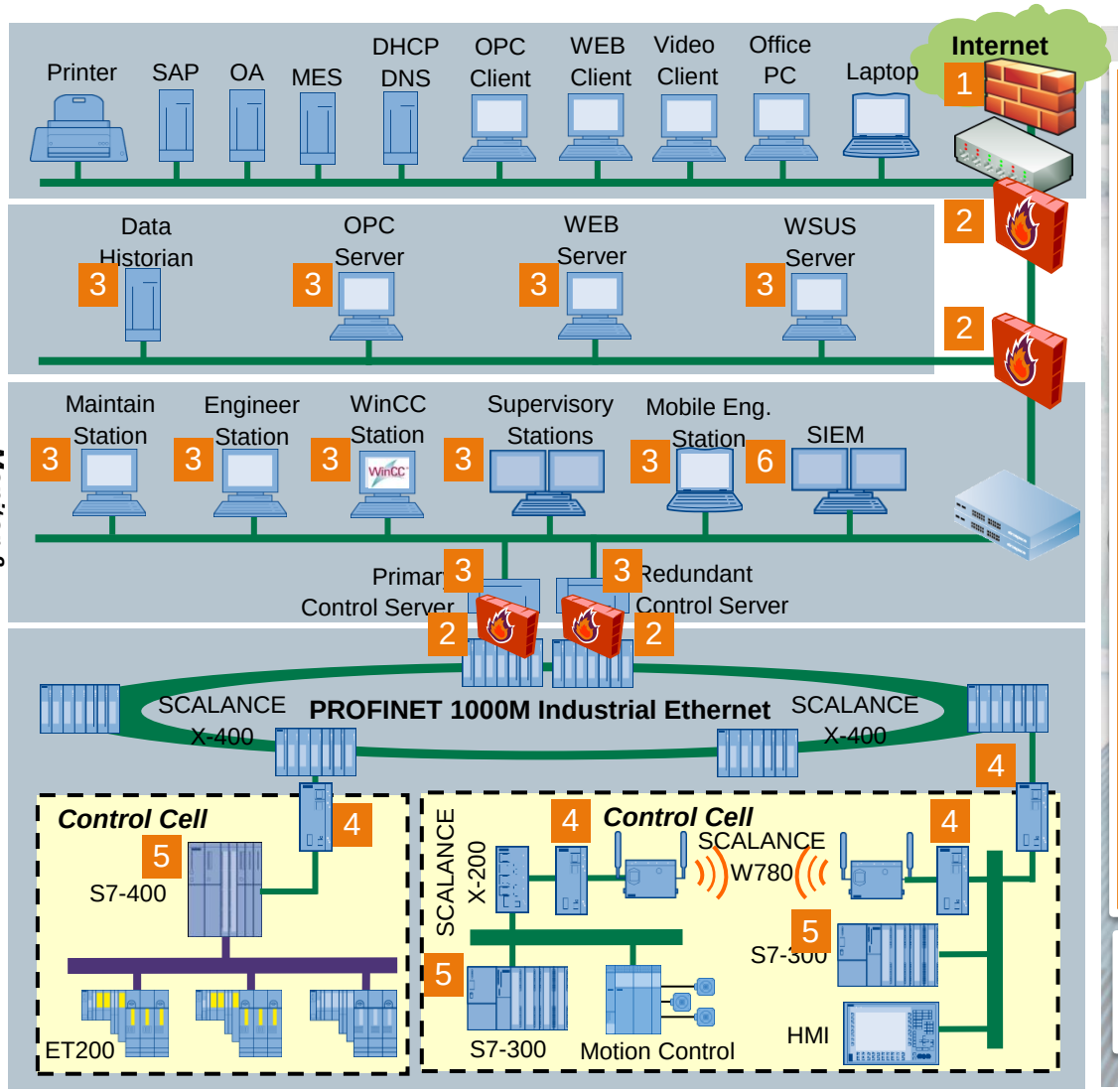
©工业安全培训课程由
西门子工业技术培训中心
西门子中国研究院
联合开发

培训中心网站
www.siemens.com.cn/sitrain

西门子（中国）有限公司
工业业务领域
客户服务集团
2013年8月

Sitrain
西门子工业技术培训中心
北京 | 上海 | 广州 | 沈阳 | 武汉 | 重庆

愿景：工业网络纵深防御



风险评估与工业自动化控制安全管理咨询

第一道防线

商用（IT）防火墙

第二道防线

抵御多种威胁的联合安全网关

第三道防线

工业PC的安全防护，如病毒扫描、白名单、配置安全、RBAC

第四道防线

现场设备的近身防护，例如SCALANCE S、CP Advanced等

第五道防线

安全可靠的现场设备

安全事故和事件监测SIEM

- 简易的配置与无缝透明的部署
- 全面的防护与持续改进的管理

主要内容

一 信息安全的新战场 - 工业基础设施

二 工业基础设施安全需求分析

三 工业信息安全解决方案：纵深防御

四 总结

总结：工业信息安全

1. 随着越来越多的安全事件的发生，我国的工业基础设施面临着前所未有的安全挑战
2. 工业信息安全不是一个单纯的技术问题，而是一个从意识培养开始，涉及到管理、流程、架构、技术、产品等各方面的系统工程
3. 工业信息安全需要工控系统的管理方、运营方、集成商与组件提供商的共同参与，协同工作
4. 目前，部署纵深防御是工业领域应对安全挑战的现实方法
5. 工业信息安全是一个动态过程，需要在整个工业基础设施生命周期的各个阶段中持续实施，不断改进

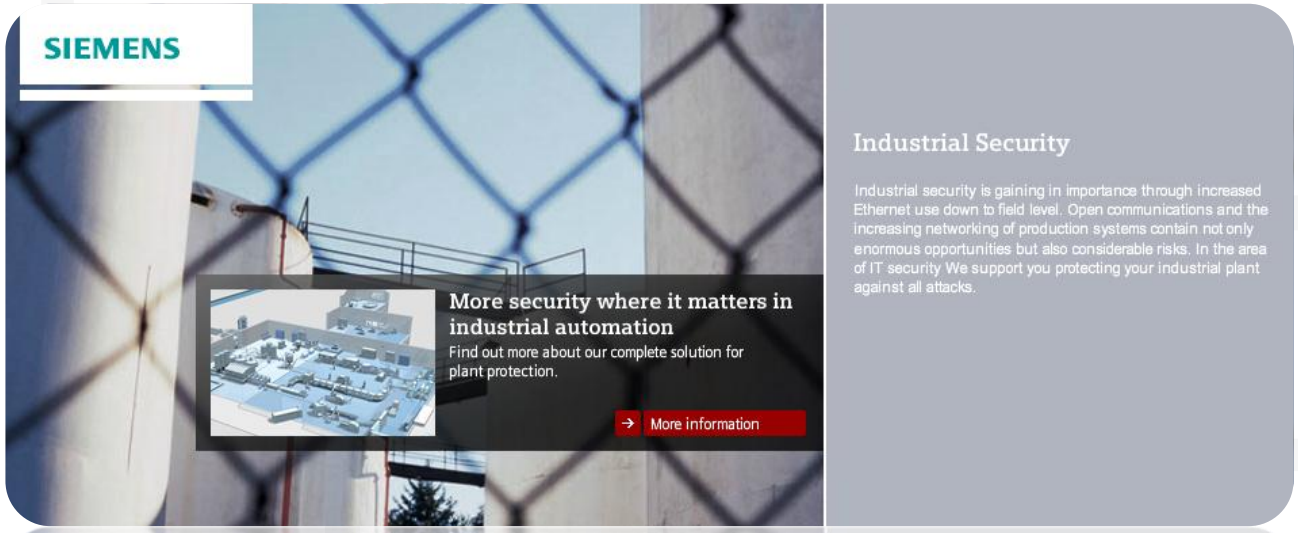
西门子内部的工业安全建设

系统测试	▪ IP协议栈加固 ▪ 通过系统的测试提高产品健壮性
安全事件的处理流程	▪ 建立并开始实行安全事件处理流程及其升级步骤
组织机构	▪ 在产品线管理流程中设立产品安全官及安全专家
研发过程改进	▪ 在研发中推行安全编码规范，进行静态代码审计等 ▪ 实施产品安全风险管理
标准与法规	▪ 与相关标准化组织密切合作 ▪ 产品获得了Achilles Level 2证书，目标是ISA 证书
提高安全意识与能力	▪ 专题讨论会、基于Web的培训、公告、专题报告 ▪ 安全培训

西门子工业安全信息的发布渠道

www.siemens.com/industrialsecurity

及时地提供工业安全信息（已知的安全漏洞与相应的补丁信息）



并通过通讯简报提供更进一步的信息

与CN CERT的合作

工业安全实验室@CT China

SIEMENS

获得安全证书与资质

- 信息安全服务资质
- 恶意软件控制产品销售资质
- 反网络病毒联盟

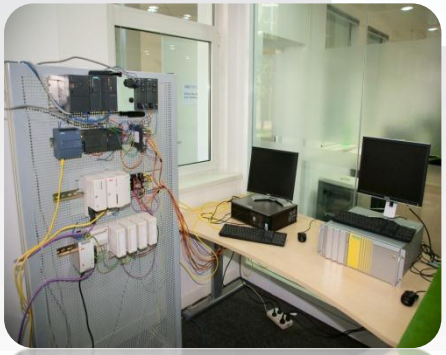
提供信息安全咨询与服务

Industry Security Lab

Innovated Research

R&D Expert | *Toolbox & Solutions* | *Consultant*

实验、演示与培训



开展针对中国本地需求的创新研发