工业控制系统信息安全技术现状与发展

上海工业自动化仪表研究院　王英

副总工程师

2014年9月24日

内 容

- 工业控制系统ICS面临的形势
- 工业控制系统信息安全的要求
- 信息安全相关的标准化工作
- 工业控制系统信息安全案例分析
- 国内外ICS信息安全发展趋势

控制系统的演变—新型控制系统

以太网无处不在

无线设备

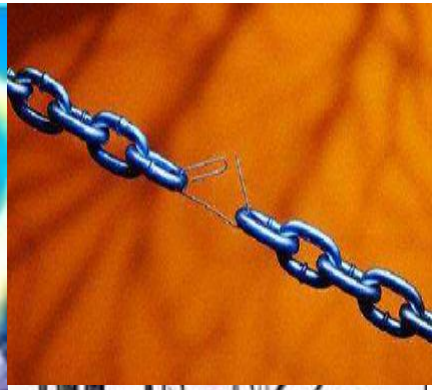
远程配置

Windows和Linux操作系统

从信息安全的角度来看，这一系统“有巨大的挑战，很容易被利用”

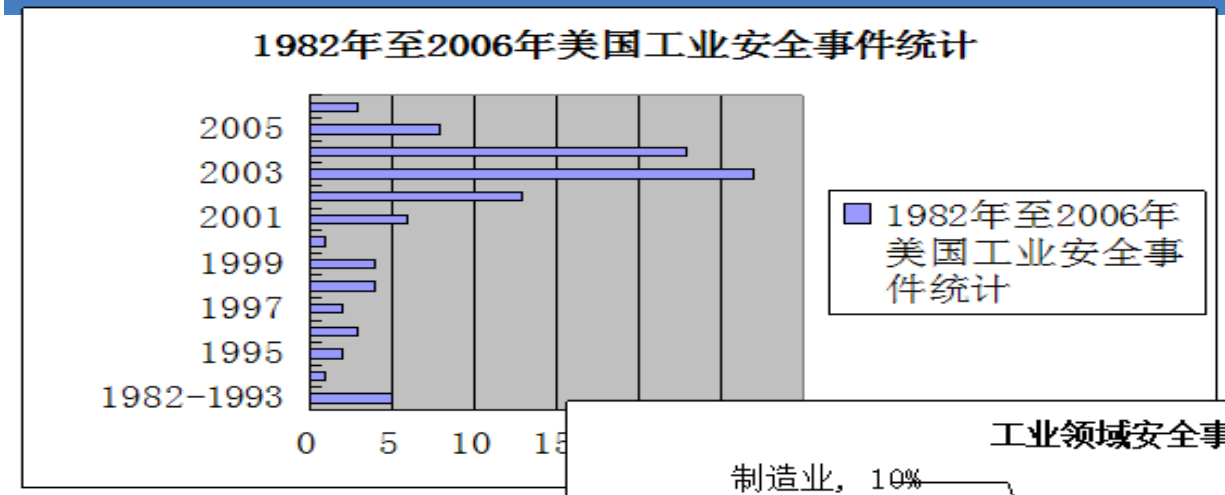
ICS面临安全的威胁

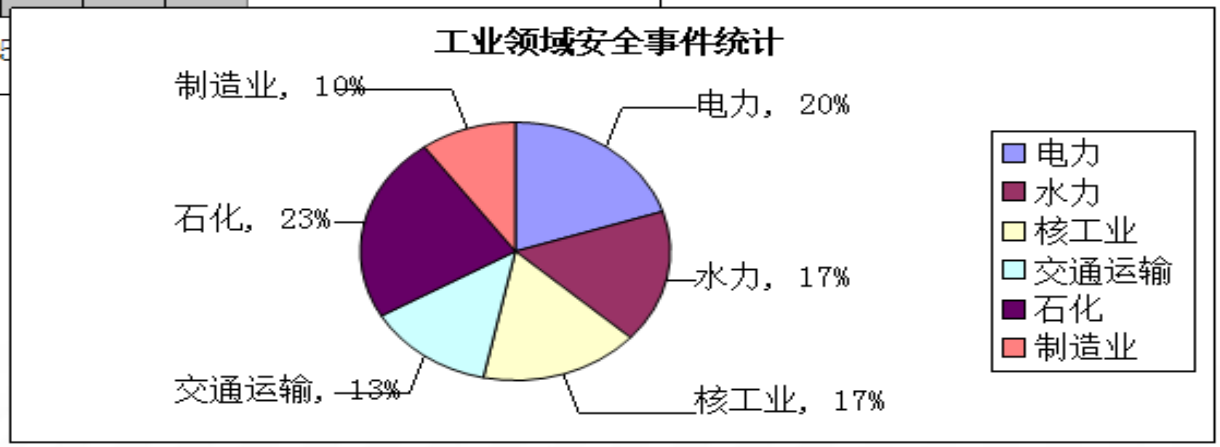
- 目前，工业基础设施面临的安全威胁包括：
  - 窃取数据、配方等
  - 破坏制造工厂
  - 由于病毒、恶意软件等导致的工厂停产
  - 操纵数据或应用软件
  - 对系统功能的未经授权的访问



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，在信息战的背景下，如何保障工业基础设施的安全





针对ICS的攻击

2010年6月出现的Stuxnet病毒，是世界上首个专门针对工业控制系统编写的席卷全球工业界破坏性病毒，它同时利用7个最新漏洞进行攻击。这7个漏洞中，有5个是针对windows系统，2个针对西门子SIMATIC WinCC系统。

内 容

- 工业控制系统ICS面临的形势
- 工业控制系统信息安全的要求
- 信息安全相关的标准化工作
- 工业控制系统信息安全案例分析
- 国内外ICS信息安全发展趋势

工业安全的新概念


风险评估
防护体系
测评体系
信息安全
功能安全
物理安全
安全?
安全?
产品
信息安全
网络
通信安全
信息辨识
处理安全
系统
功能安全
硬件
功能安全
软件
功能安全
防爆安全
电磁兼容
电气安全
环境适应性
工业控制系统的信息安全技术

IT系统与ICS的信息安全要求

	IT系统	工业控制系统
可用性	允许短时间/周期性的间断或维护	要求24h/7d/365d模式的可用性
时间敏感性	允许一定时延	要求实时响应
系统生命周期	3-5年	5-20年
信息安全意识及准备	较好	没有基础
保密性	较高	要求较低
设备类型	较少	较多
无线技术应用	很多	刚刚起步

传统信息系统：保密性—完整性—可用性

工业控制系统：可用性—完整性—保密性

内 容

- 工业控制系统ICS面临的形势
- 工业控制系统信息安全的要求
- 信息安全相关的标准化工作
- 工业控制系统信息安全案例分析
- 国内外ICS信息安全发展趋势

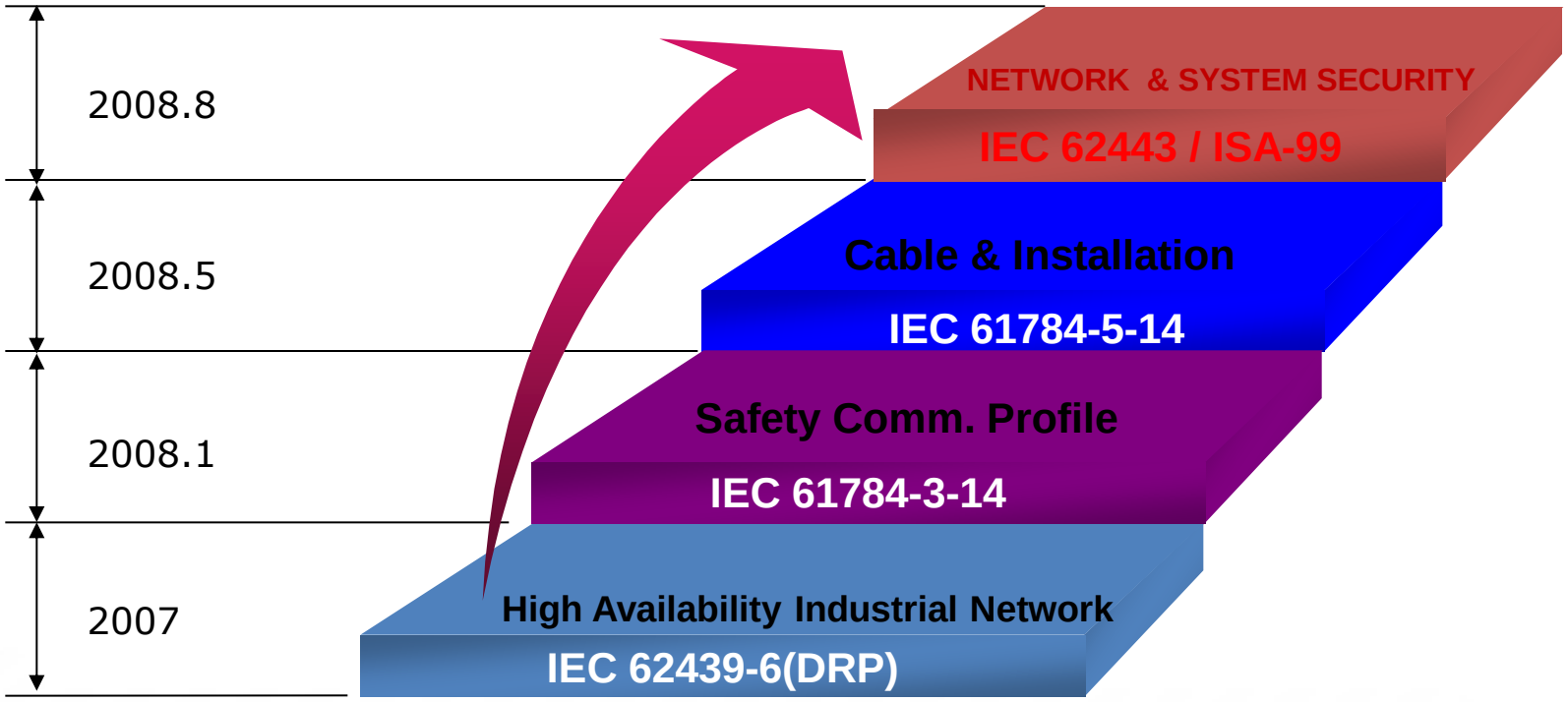
信息安全标准

GB 17859

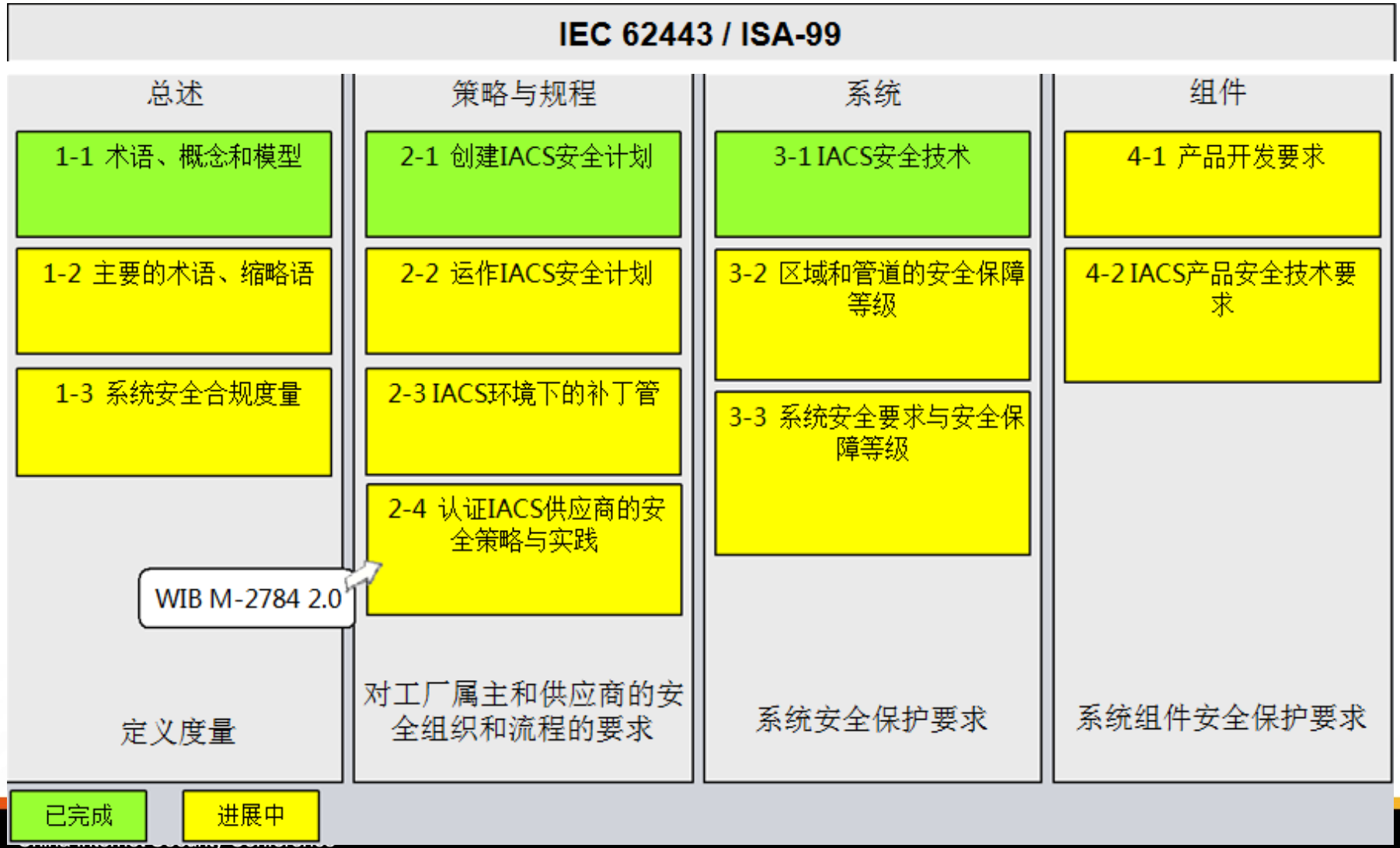
计算机信息系统安全保护能力等级

- 第一级:用户自主保护级
- 第二级:系统审计保护级
- 第三级:安全标记保护级
- 第四级:结构化保护级
- 第五级:访问验证保护级

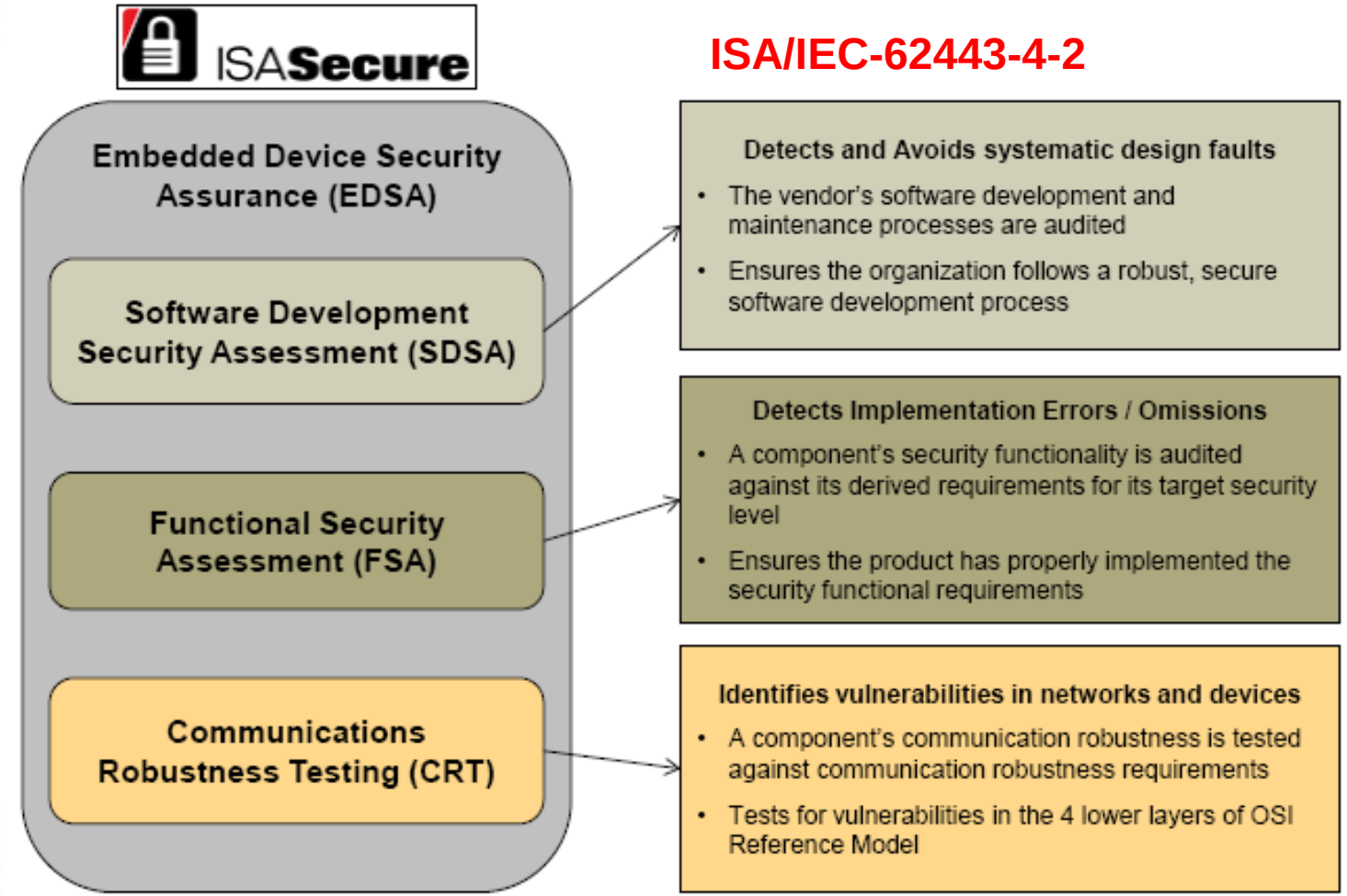
IEC标准化工作


2008.8
2008.5
2008.1
2007
NETWORK & SYSTEM SECURITY
IEC 62443 / ISA-99
Cable & Installation
IEC 61784-5-14
Safety Comm. Profile
IEC 61784-3-14
High Availability Industrial Network
IEC 62439-6(DRP)

IEC 62443 / ISA-99 架构



ISASecure EDSA Certification Program



ISASecure™ Security Development Lifecycle Assurance (SDLA)

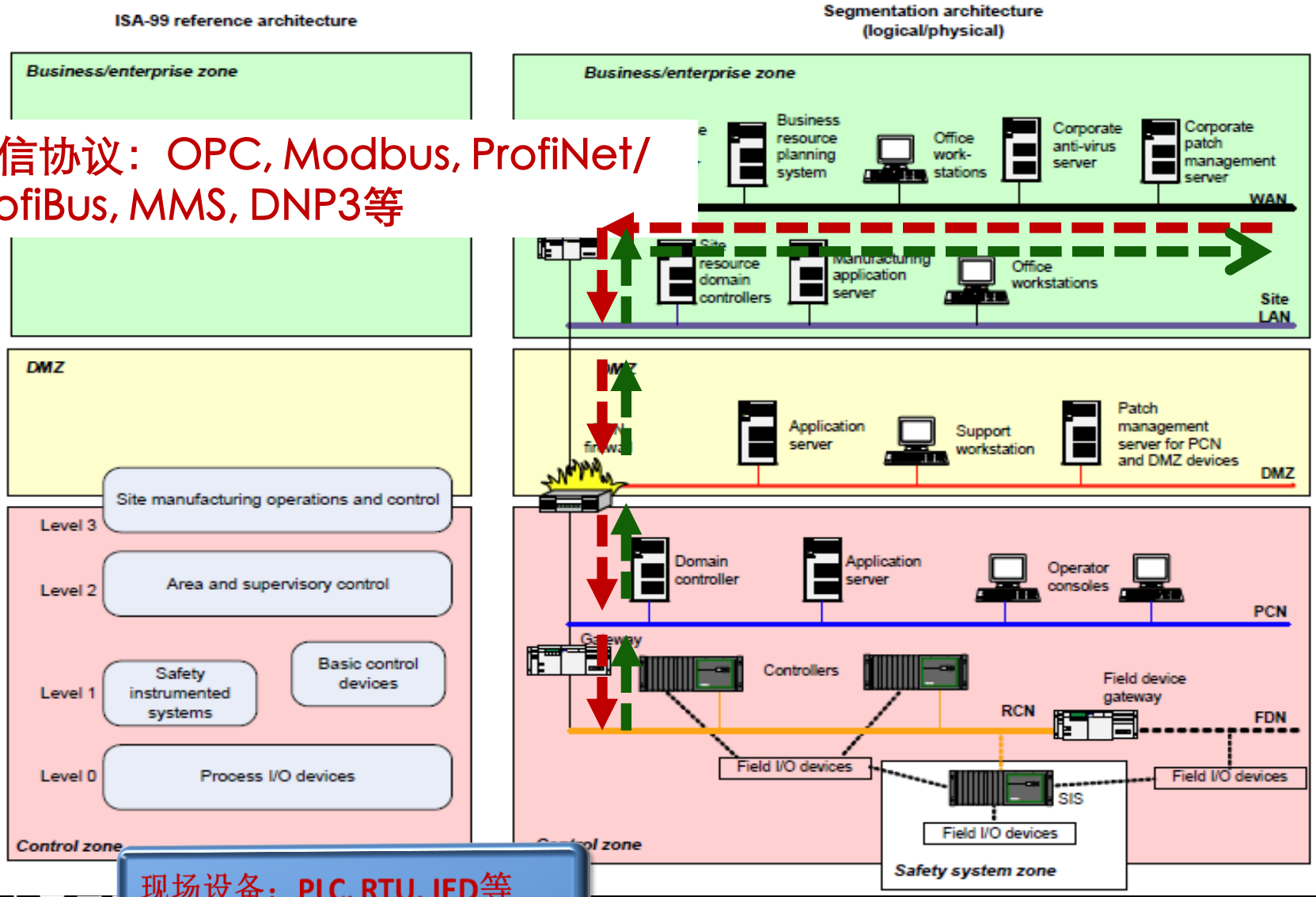
- Security Management Process
- Security Requirements Specification
- Security Architecture Design
- Security Risk Assessment (Threat Model)
- Detailed Software Design
- Document Security Guidelines
- Module Implementation & Verification
- Security Integration Testing
- Security Process Verification
- Security Response Planning
- Security Validation Testing
- Security Response Execution

ISA/IEC-62443-4-1

内 容

- 工业控制系统ICS面临的形势
- 工业控制系统信息安全的要求
- 信息安全相关的标准化工作
- 工业控制系统信息安全案例分析
- 国内外ICS信息安全发展趋势

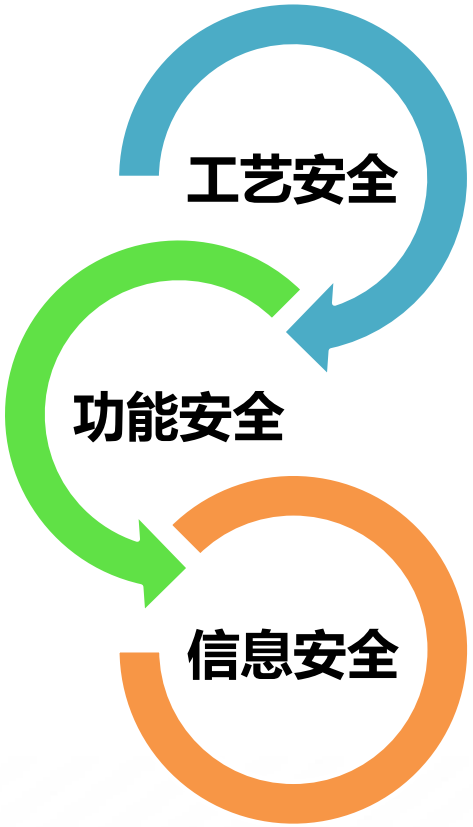
工业控制系统信息安全模型

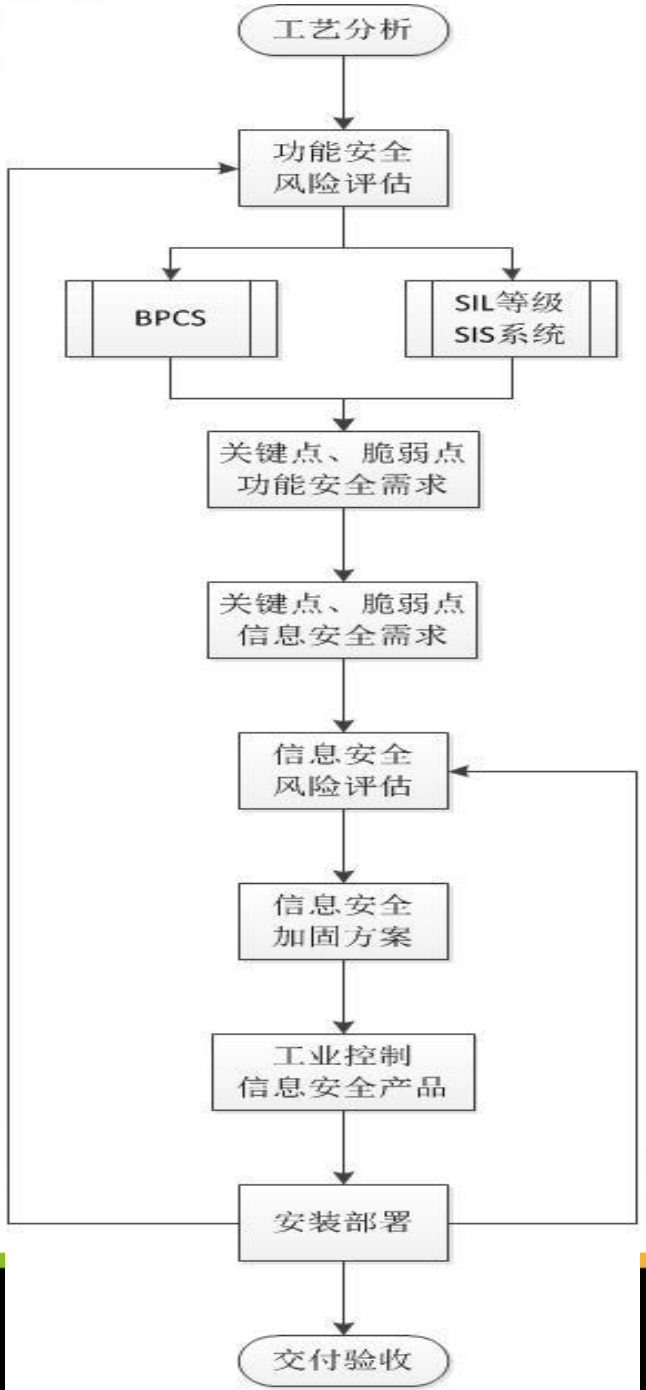


通信协议：OPC, Modbus, ProfiNet/ ProfiBus, MMS, DNP3等

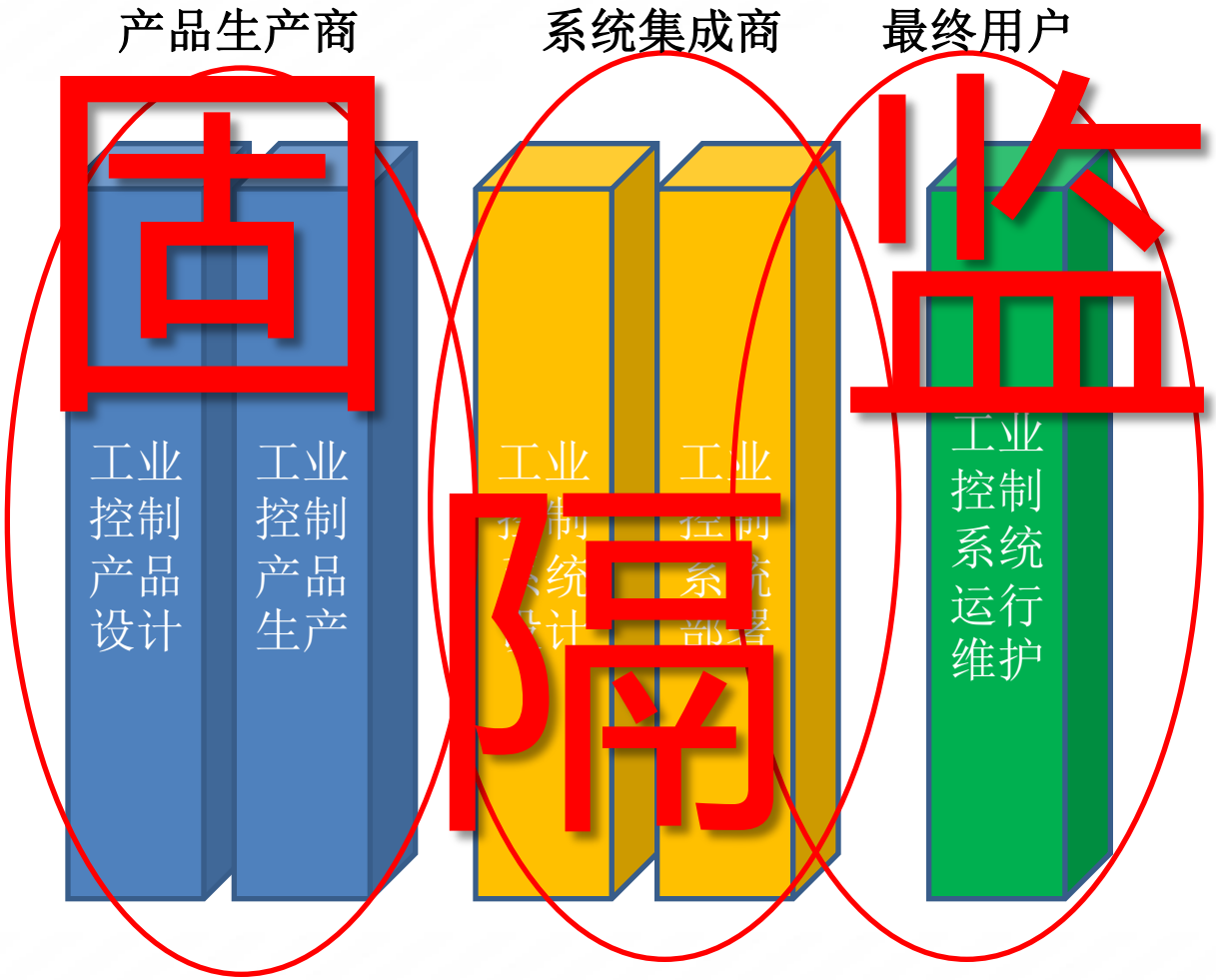
现场设备：PLC, RTU, IED等

ICS信息安全流程

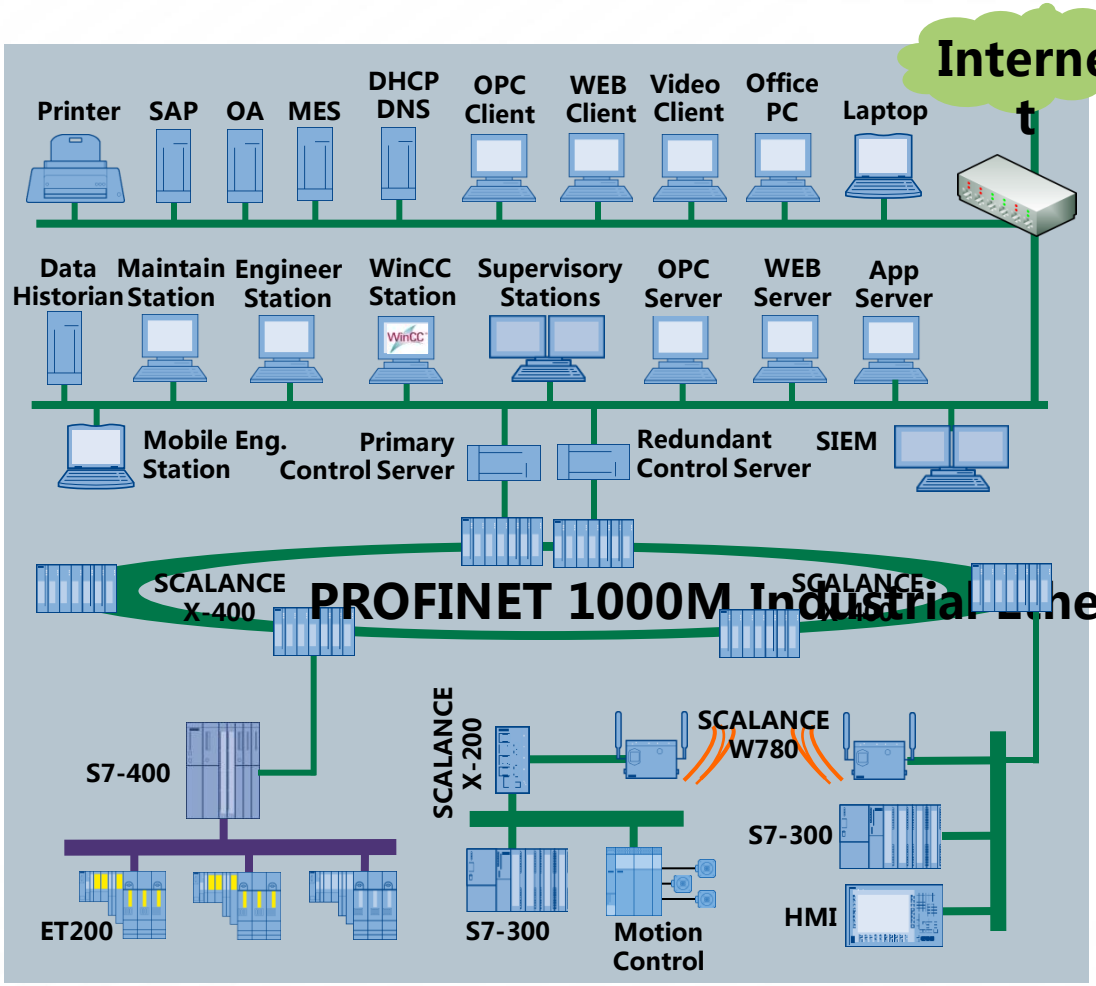

工艺安全
功能安全
信息安全


工艺分析
功能安全
风险评估
BPCS
SIL等级
SIS系统
关键点、脆弱点
功能安全需求
关键点、脆弱点
信息安全需求
信息安全
风险评估
信息安全
加固方案
工业控制
信息安全产品
安装部署
交付验收

自控系统信息安全工程实现



自控系统信息安全工程实现



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，包括配置SIS系统报警监控系统，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

石化控制系统信息安全风险分析

脆弱点名称	技术处置建议	管理处置建议
缺乏有效的身份鉴别机制	增强口令的审核和验证，部署“工程师站审计系统”对系统账号进行身份鉴别	严格管理终端用户帐号口令，禁止多用户共同使用administrator情况，加强用户初始口令更改，以及口令定期变更。
缺乏有效的病毒管控措施	部署工控信息安全监控系统检测病毒传播事件以便及时提醒现场管理人员进行处理	禁止混用U盘、带USB接口的存储设备等移动介质。
缺乏有效的应用系统监控措施	部署工控信息安全监控系统、对应用系统以及主机的状态进行监控	
缺乏有效的日志保存和审计措施	增强日志的收集及审计	
对连接系统的设备缺乏有效识别措施	部署工控信息安全监控系统对非法接入设备进行识别及报警	
缺乏漏洞管理机制	开展定期漏洞检测并及时漏洞修复	
缺乏系统升级机制	建立测试环境，并及时进行系统升级	
未对远程登陆进行安全控制	部署“工程师站审计系统”对远程登陆行为进行集中管理	增强远程登陆管理
未设置完善的日志策略	在设备上完善日志策略	
缺乏有效的账户安全策略设置	部署“工程师站审计系统”对系统账号进行集中管理	
未禁用不需要的端口或服务	部署边界防火墙、阻断不需要的端口或服务，增强控制网边界安全	

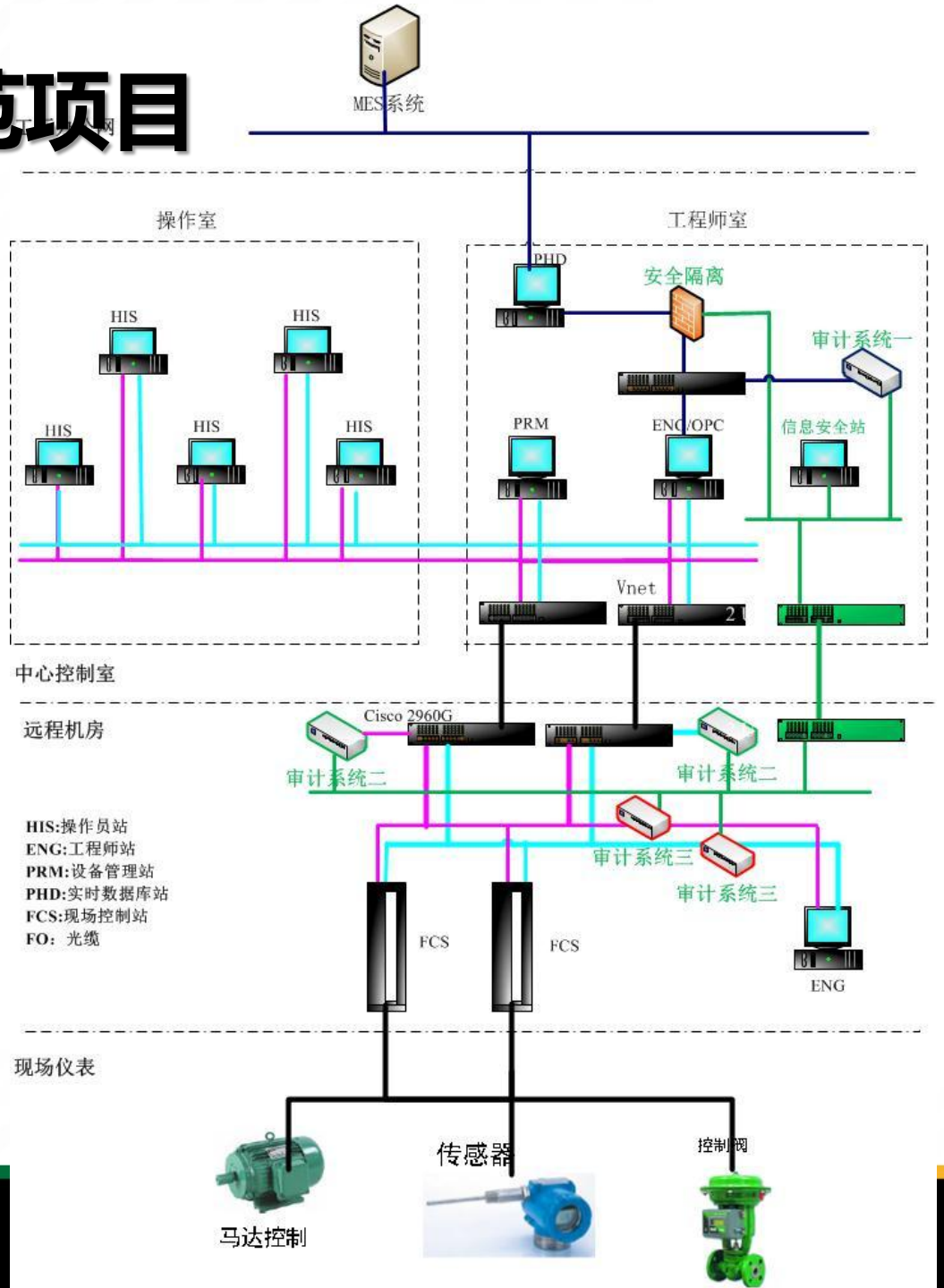
工控信息安全示范项目

纵深防御（IATF）

四层分区

安全专网

隔离与监控



内 容

- 工业控制系统ICS面临的形势
- 工业控制系统信息安全的要求
- 信息安全相关的标准化工作
- 工业控制系统信息安全案例分析
- 国内外ICS信息安全发展趋势

国内外控制系统安全研究现状

美国国土安全部和世界多家知名工业控制领域企业展开合作，建立“工业控制系统安全评估实验室”，并启动了“控制系统安全项目(CSSP)”将工业控制系统安全已经提高到了国家安全层面。

国内外控制系统信息安全发展趋势

2008年，美国商务部制定《工业控制系统安全的指导书》(**Guide to Industrial Control Systems Security**)，监管工业控制产品(**SCADA**、**DCS**、**PLC**等)的安全性

ISA(工业自动化协会) 分别于2007年和2009年制定了工业自动化与控制系统安全标准ISA99的第一部分和第二部分，提出了相关概念、模型，并对“如何建立安全的工业控制系统”进行了探讨。

国内外控制系统信息安全发展趋势

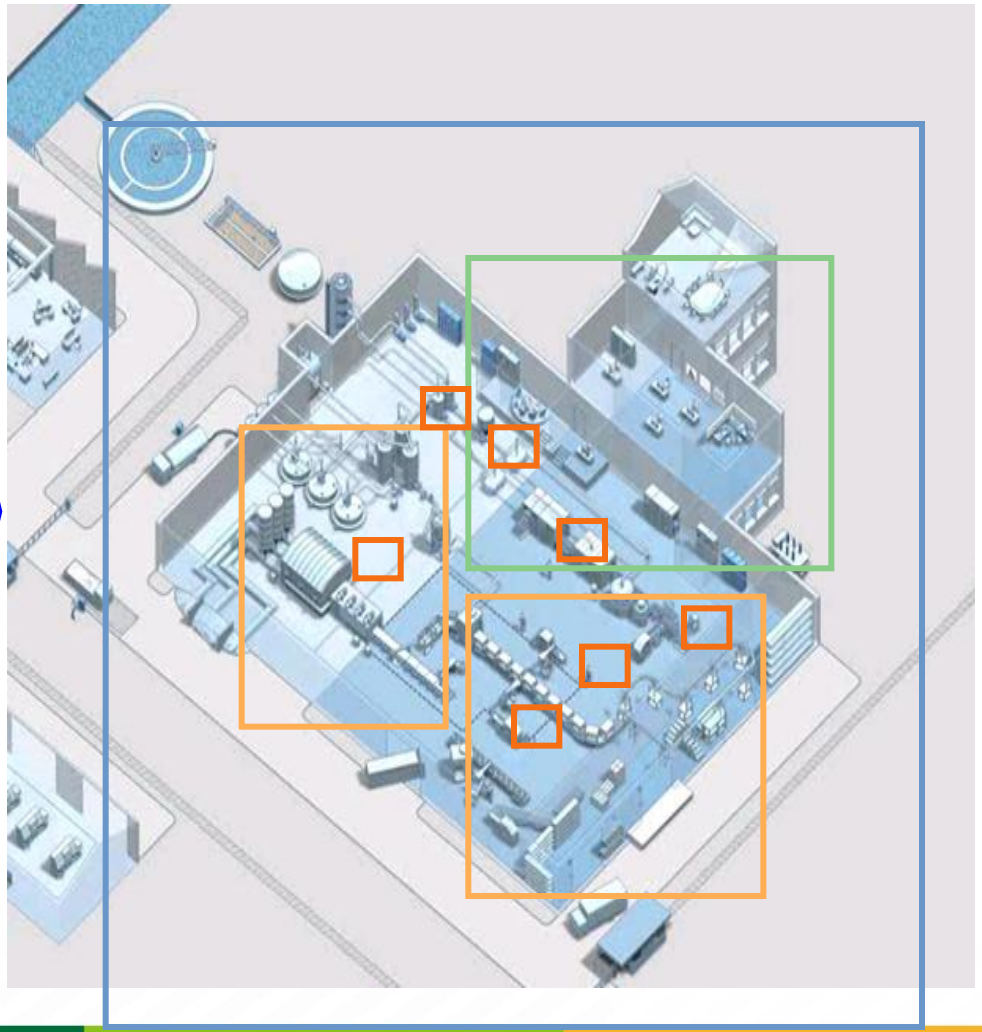
工业网络信息安全逐渐转向硬件解决方案，各大自动化公司和安全设备厂商都推出了工业控制系统安全产品，如物理隔离网闸、安全网关等安全接入设备。

工控系统安全实现

- 国家要求和企业自身管理需求的紧密结合
- 工艺安全、功能安全、信息安全的有效结合
- 完善的纵深防御体系
- 科学的ICS信息安全流程
- 有效的工业信息安全防御产品

工业安全：需要多方的积极参与

管理者	▪ 采取措施与流程防止对工厂的未经授权的访问 ▪ 对关键自动化组件物理访问的防护，等等
运营者	对运营者需的安全需求： ▪ 安全指南与流程规范 ▪ 安全风险管理 ▪ 信息与文档管理 ▪ 等等
OEM/系统集成商	系统层次的安全需求 ▪ 访问控制，用户控制 ▪ 数据完整性与机密性 ▪ 可控的数据流，等等
组件提供商	对自动化系统组件的安全需求： ▪ 产品开发流程 ▪ 产品功能 ▪ 等等



总结：工业安全

工业信息安全

- 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
- 工业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
- 工业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
- 目前，部署纵深防御是工业领域应对安全挑战的现实方法
- 工业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

Thanks!