工业控制系统面临的安全风险与对策

工业控制系统的安全需求

—— 工控系统为什么需要信息安全

当工业化遇到信息化

Industrial control system (ICS) is a general term that encompasses several types of control systems used in industrial production, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other smaller control system configurations such as programmable logic controllers (PLC) often found in the industrial sectors and critical infrastructures

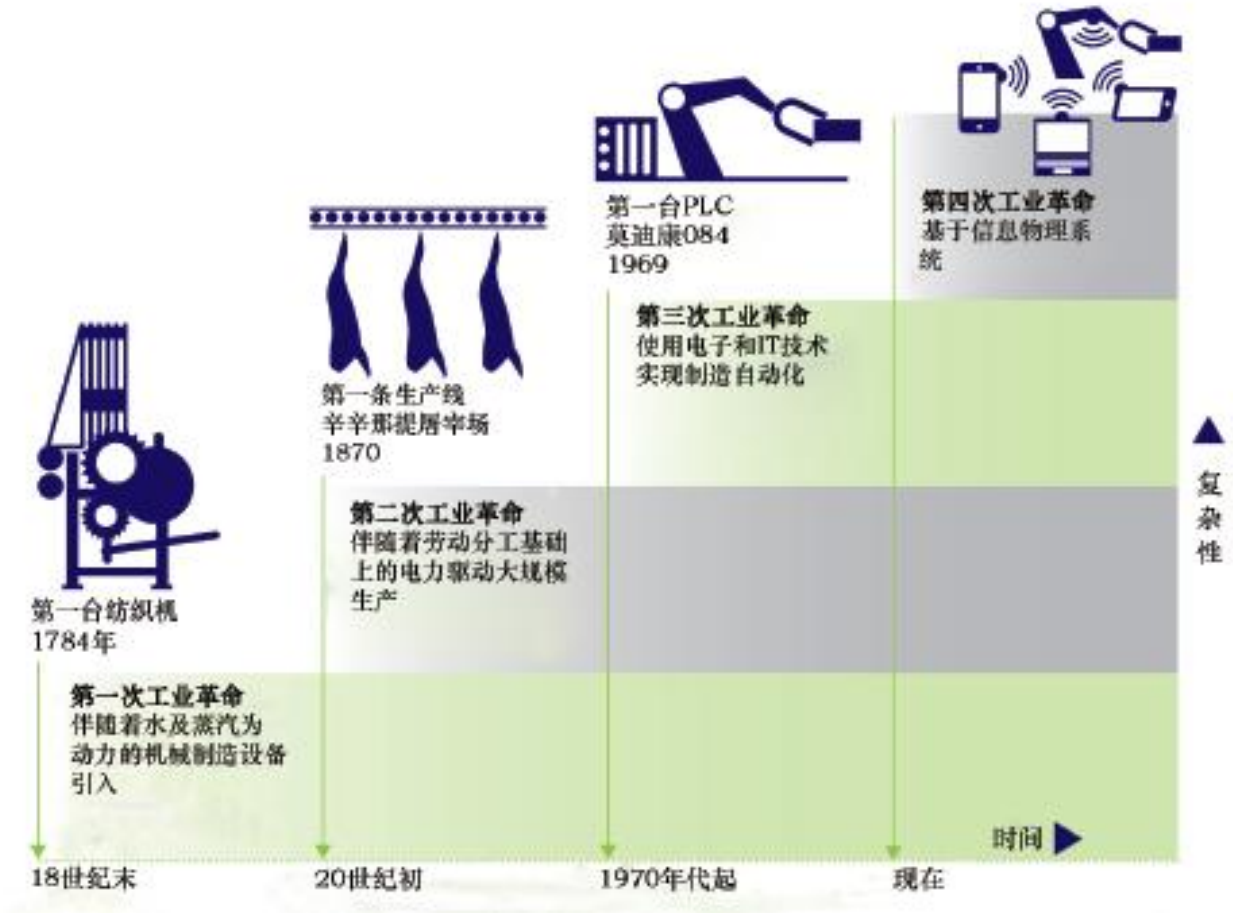
国务院政府工作报告强调积极推动两化融合

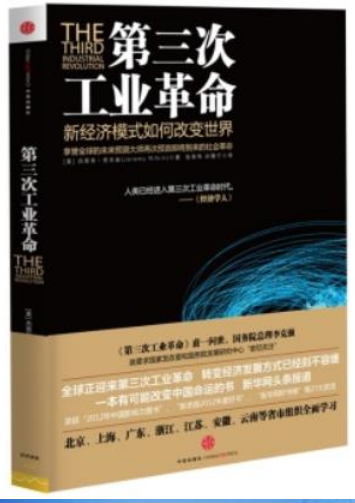
发布时间：2013-04-10　信息来源：信息化推进处　字体：大 中 小

2013年国务院政府工作报告强调要“积极推动信息化和工业化融合，加快建设新一代信息基础设施，促进信息网络技术广泛应用”，并将其列入加快转变经济发展方式、促进经济持续健康发展的重要内容。报告在回顾五年来的工作及特点中还提到，“新一代信息技术等一批战略性新兴产业快速发展”，“坚持在工业化、信息化、城镇化深入发展中同步推进农业现代化”。

提请十二届全国人大一次会议审议的《关于2012年国民经济和社会发展计划执行情况与2013年国民经济和社会发展计划草案的报告》中明确提出，推进“宽带中国”等重大信息化工程，强化信息安全等基础设施建设；“着力扩大国内需求”部分还特别强调，发展信息消费，加快培育新的消费增长点；优化消费环境，加强宽带网络等消费基础设施建设，鼓励发展电子商务、网络购物新型消费业态。

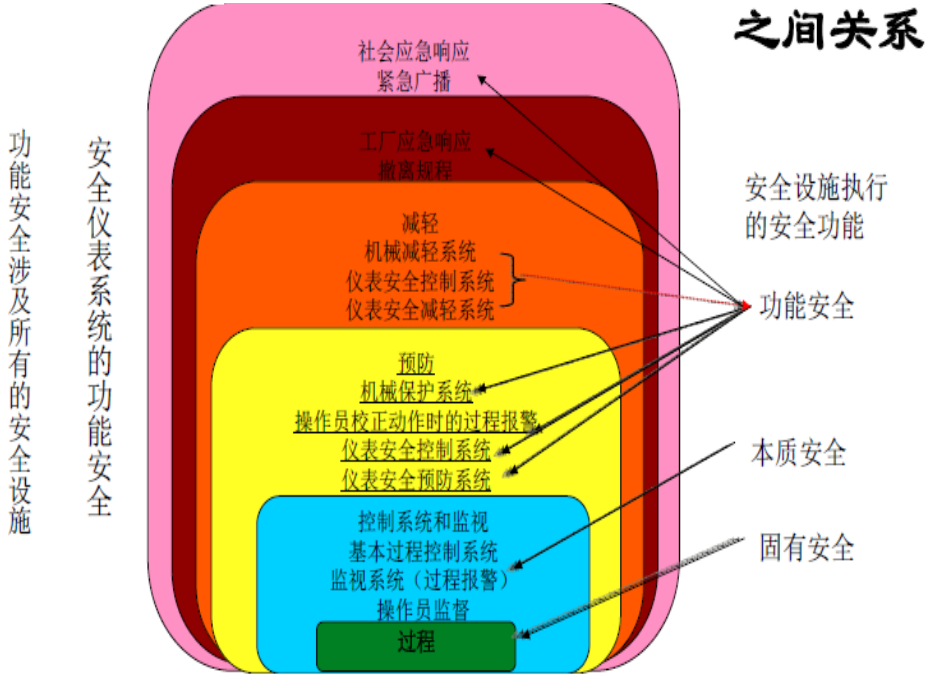
根据国家统一部署，我省今后一个时期应加快建立健全信息资源共享、信息普遍服务和网络信息安全保障机制，推动信息化“融合”工业化；工业化“互动”城镇化；城镇化“协调”农业现代化，实现“四化协同”发展。

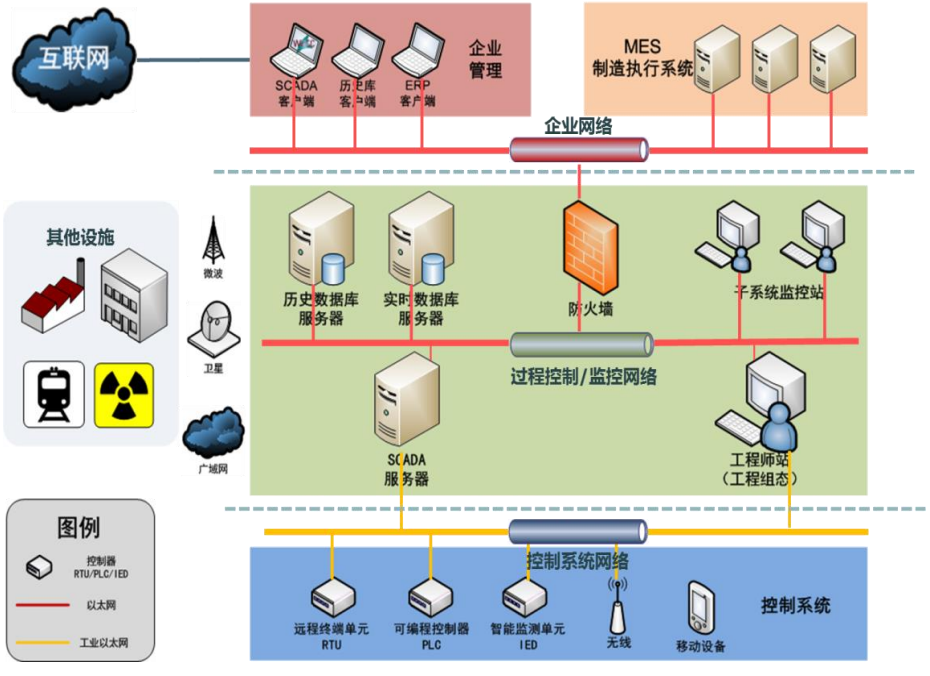




单体的能源形式，向多元化能源形式发展，能源之间的互连、互通、互相支撑的关系也越来越明显。
智能电网——电网2.0——能源互联网

当工业安全遇到信息安全



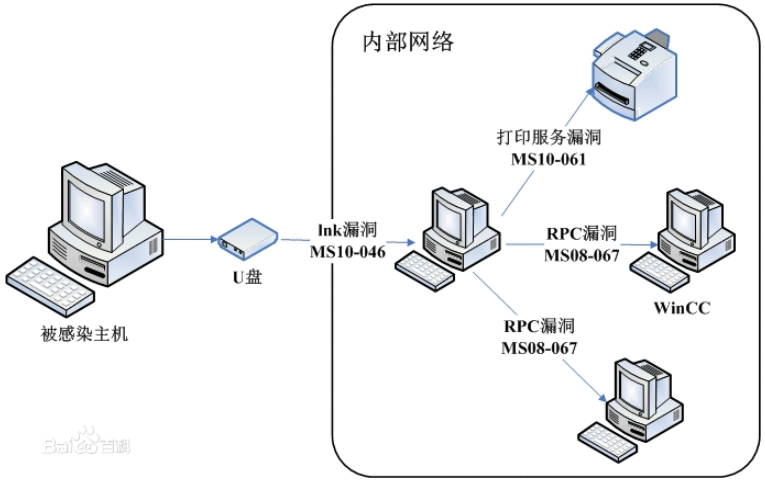


功能安全：针对特定的危险事件，为达到或保持过程的安全状态，由安全仪表系统、其它技术安全相关系统或外部风险降低设施实现的功能。
FROM:IEC 61508

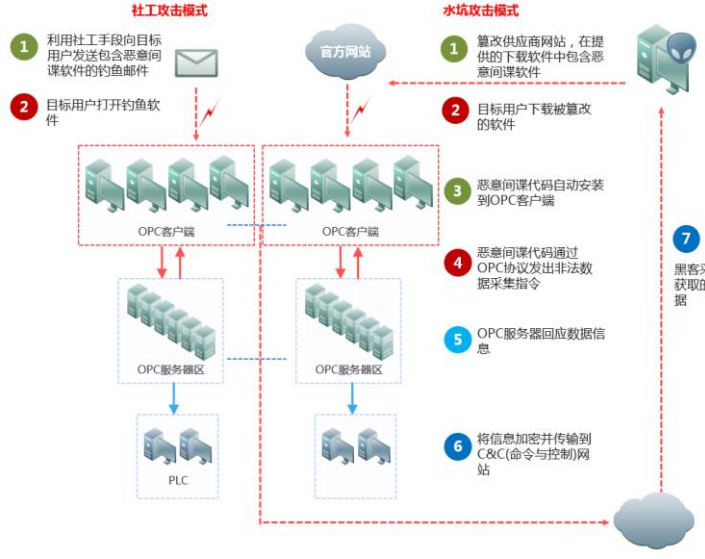
信息安全：保持信息的保密性、完整性、可用性；另外也可包括例如真实性、可核查性、不可否认性和可靠性等。
FROM:ISO 27001

OT安全&IT安全已经成为新形式下安全发展的一个新的趋势

威胁已渗入到工控系统

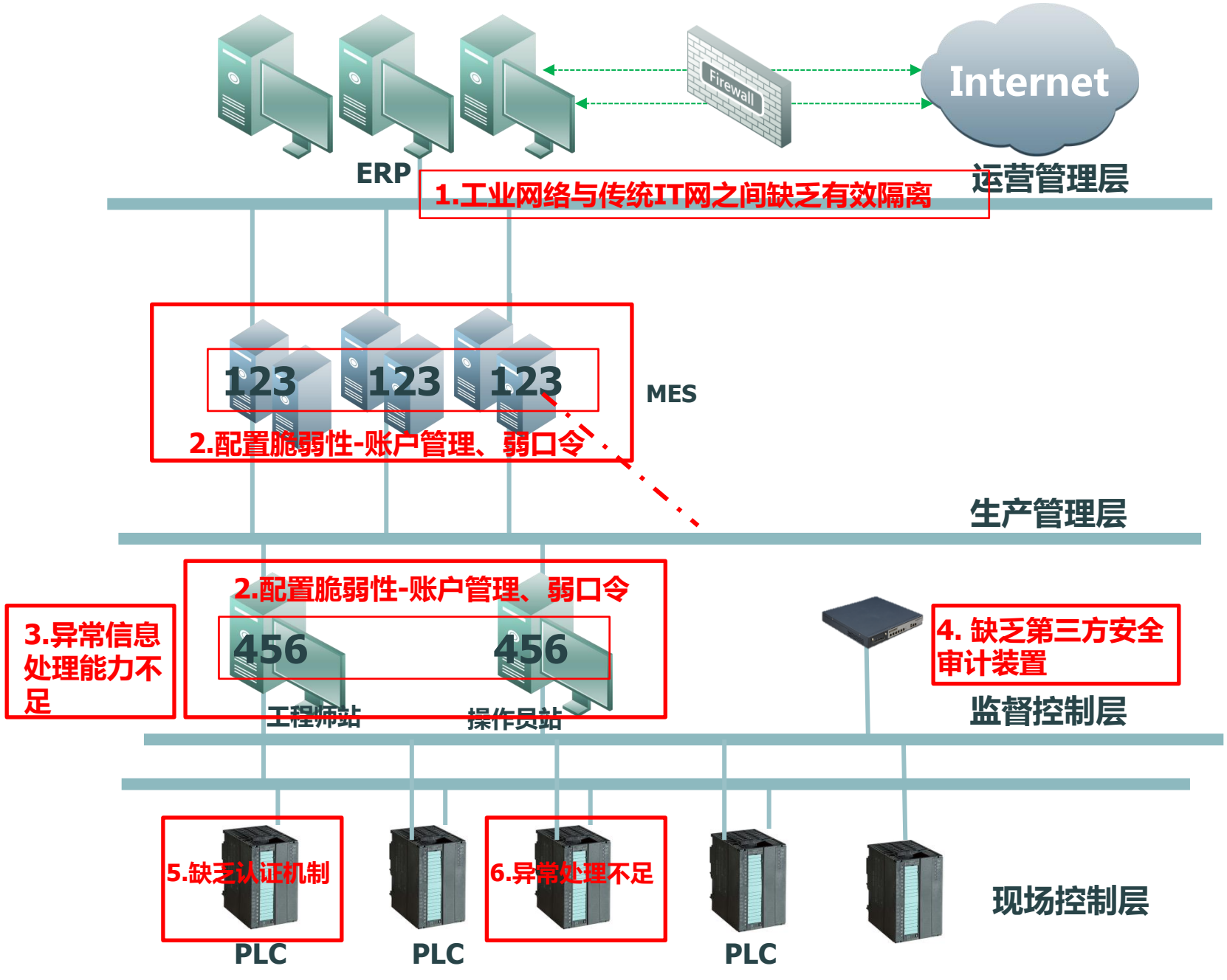

内部网络
打印服务漏洞
MS10-061
lnk漏洞
MS10-046
RPC漏洞
MS08-067
RPC漏洞
MS08-067
U盘
WinCC
被感染主机


TURKISH HACKER TEAM HACKS
POWER ADMINISTRATION SYSTEM
DELETES 1.5 MILLION LIRAS OF DEBT
REDHACK
KIZILHACKERLAR

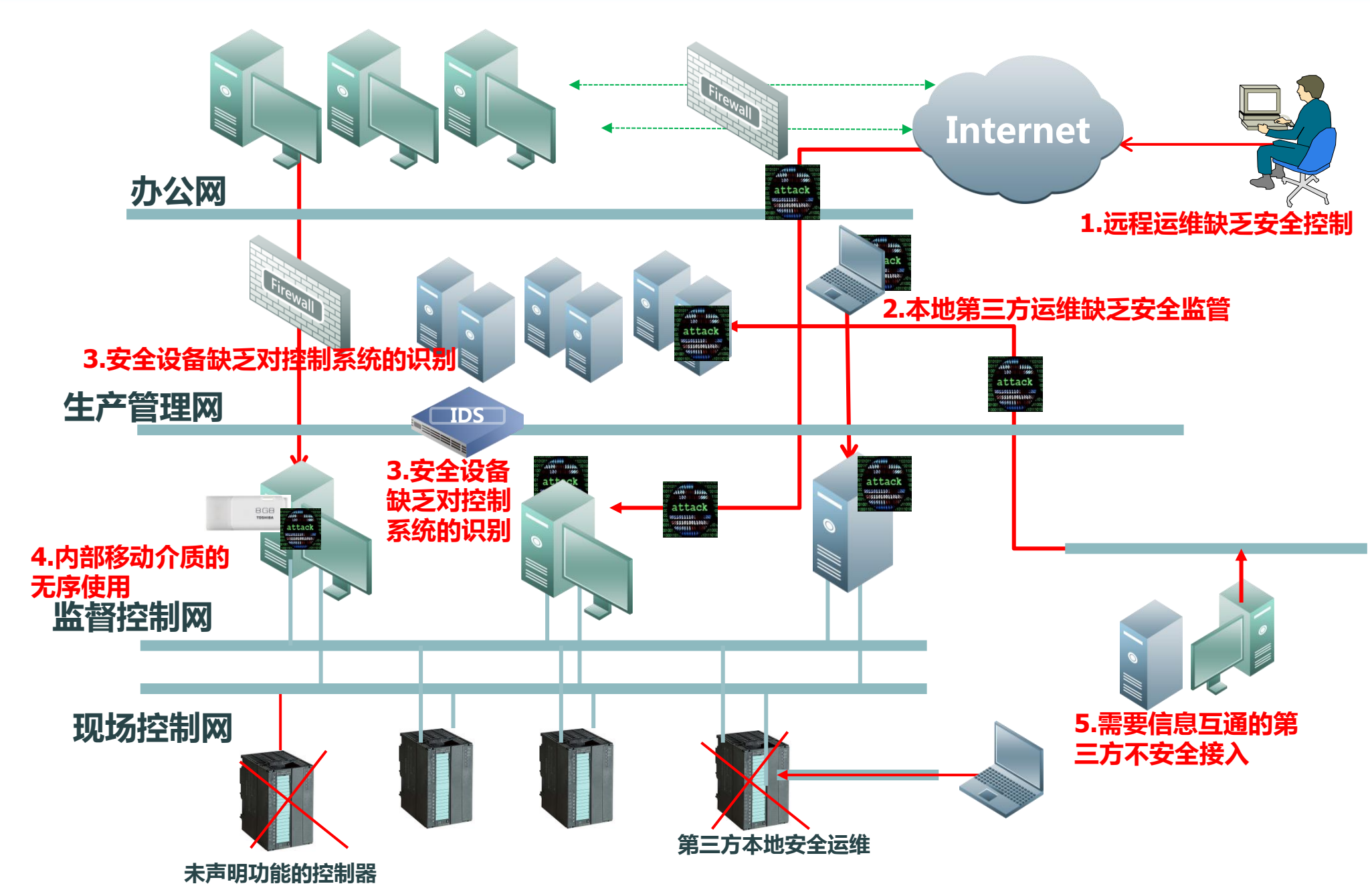

社工攻击模式
1 利用社工手段向目标用户发送包含恶意间谍软件的钓鱼邮件
2 目标用户打开钓鱼软件
官方网站
OPC客户端
OPC客户端
OPC服务器区
OPC服务器区
PLC
水坑攻击模式
1 篡改供应商网站，在提供的下载软件中包含恶意间谍软件
2 目标用户下载被篡改的软件
3 恶意间谍代码自动安装到OPC客户端
4 恶意间谍代码通过OPC协议发出非法数据采集指令
5 OPC服务器回应数据信息
6 将信息加密并传输到C&C(命令与控制)网站
7 黑客采集获取的数据


Duqu: 盗空一切
Duqu是一种复杂的木马，有迹象表明其编写者与先前制造臭名昭著的Stuxnet蠕虫的编写者同为一人。与Stuxnet不同的是，Stuxnet的主要目的是造成工业破坏，而Duqu则被用来收集与其攻击目标有关的各种情报。
可以说，Duqu能盗取目标系统中的所有信息。然而，从其发动的攻击情况来看，它似乎只对收集密码、抓取桌面截图（暗中监视用户的操作）、盗取各类文件感兴趣。这些行为预示着网络罪犯使用的技术将开启一个新的时代，网络罪犯将有足够的能力成功执行工业间谍活动，甚至绑架与勒索。

工控系统脆弱性


Firewall
Internet
ERP
1.工业网络与传统IT网之间缺乏有效隔离
运营管理层
123
123
123
MES
2.配置脆弱性-账户管理、弱口令
生产管理层
2.配置脆弱性-账户管理、弱口令
3.异常信息处理能力不足
456
456
工程师站
操作员站
4. 缺乏第三方安全审计装置
监督控制层
5.缺乏认证机制
6.异常处理不足
PLC
PLC
PLC
现场控制层

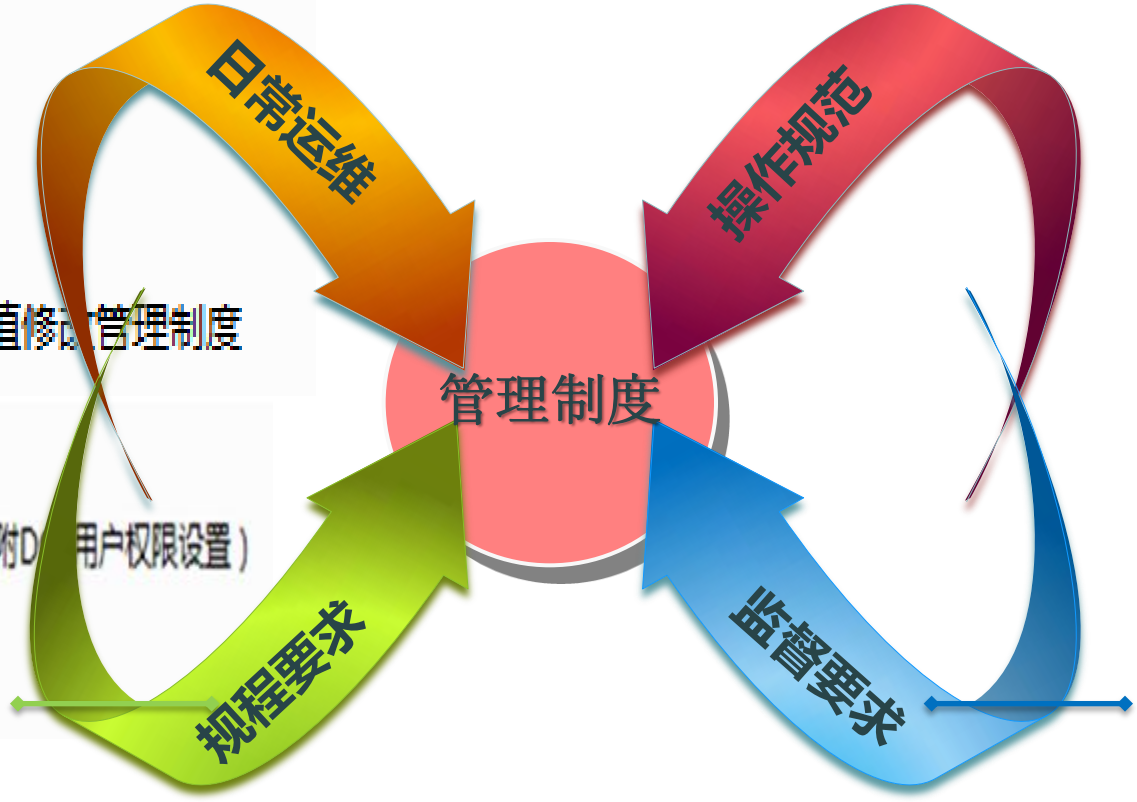
工控系统所面临的安全威胁



缺乏信息安全有效管理

- 工程师站管理考核细则
- 热控DCS软件管理制度
- 热控保护系统定期试验管理制度
- 热控保护运行管理制度
- 热控工程师站管理制度
- 热控自动、联锁和保护投退及逻辑、定值修改管理制度

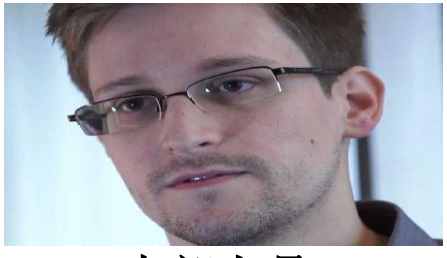
- 设备异常报警机制
- 误操作制度（通过工程师站、DCS的管理制度实现，另附D 用户权限设置）
- DL_T838-2003发电企业检修导则
- 电气二次班安全管理制度



缺乏信息安全意识培训

松耦合机制，信息安全与日常信息维护和生产维护没有有机的结合

工业系统威胁源分析

威胁源	描述
 敌对国家	在空间安全（Cyber security）和信息战的思维下，境外机构发展其对我国国家基础设施进行信息窃取、状态干扰的能力，其后果可能对我国工业基础设施产生严重影响，甚至可能危及人民生命
 内部人员	由于利益或者不满情绪的驱使，利用其对工业控制系统环境相关系统的了解，将在不具备大量计算机入侵知识的前提下造成系统损坏或者信息失窃；同时人员误操作也可能造成一定程度上的风险
 恐怖分子	恐怖分子尝试通过对工业控制系统进行干扰、破坏从而威胁国家关键基础设施的安全
 工业间谍	获取工业控制网络的相关核心技术和敏感信息

安全需求总结

合规性需求

- 原电监会5号令
- 工信部451号令
- 烟草生产网与信息网隔离要求
- 发改委14号令
- 发布国标：**GB/T 30976-2014**

业务安全需求

- 恶意代码感染正常业务运行
- 外部运维影响业务运行
- 人员意识不足，引入威胁
- 生产网络永远是黑盒

工控安全

—— 安全建设面临的挑战

国家电力监管委员会令

第 5 号

《电力二次系统安全防护规定》已经国家电力监管委员会主席办公会议通过，现予公布，自 2005 年 2 月 1 日起施行。

主　席　柴松岳

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

安全分区、网络专用、横向隔离、纵向认证

修订：引入安全接入区；边界防护→纵深防护发展

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：

客户的顾虑

隔离的网络安全性一定是有保障的？

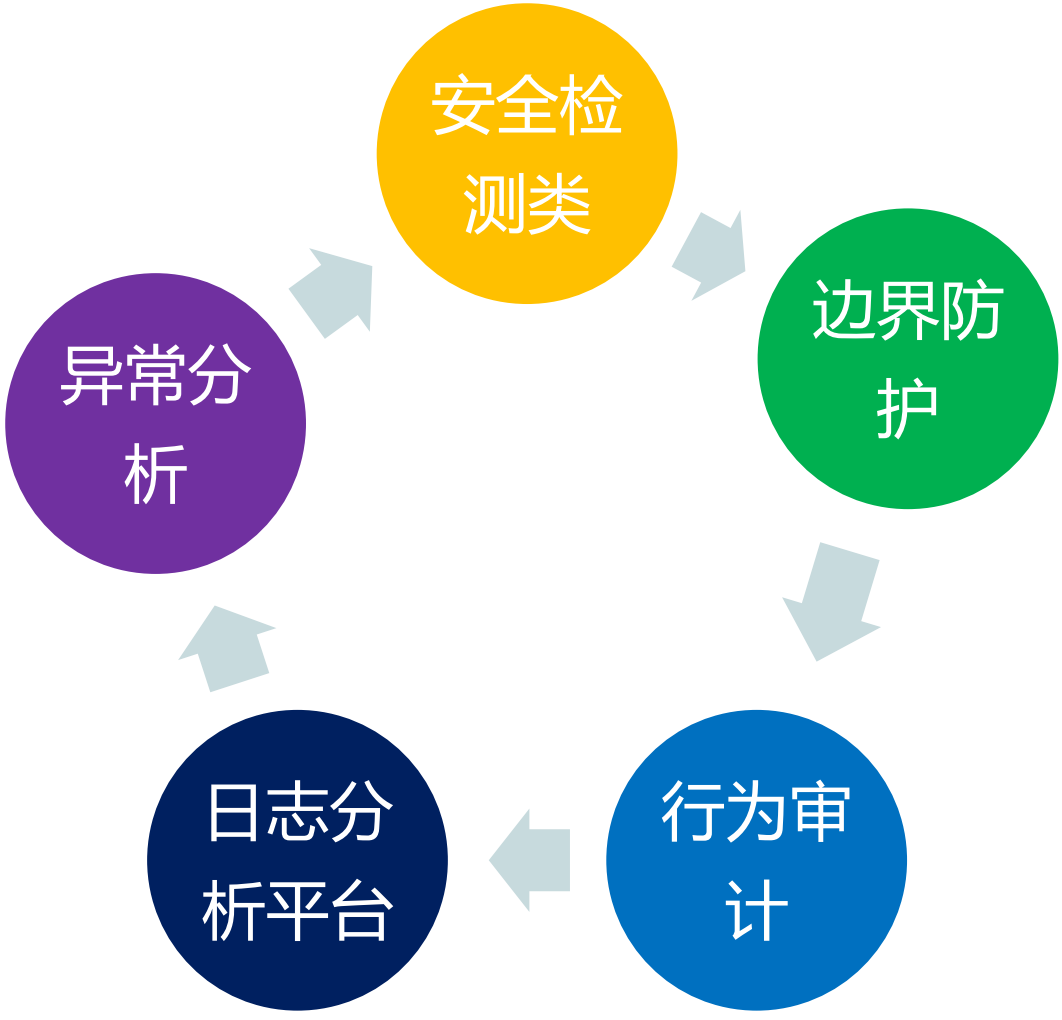
设备可适应于工控系统吗？

工控安全设备对系统没有影响吗？

工控有什么漏洞？

漏洞可解决吗？

主流技术特性



客户的期望

合规性需求：满足合规性要求为基础

业务安全能力提升为主要方向

工业企业在建设以满足合规性为主

以安全能力提升为主要的方向

安全能力趋势

全生命周期的安全管控

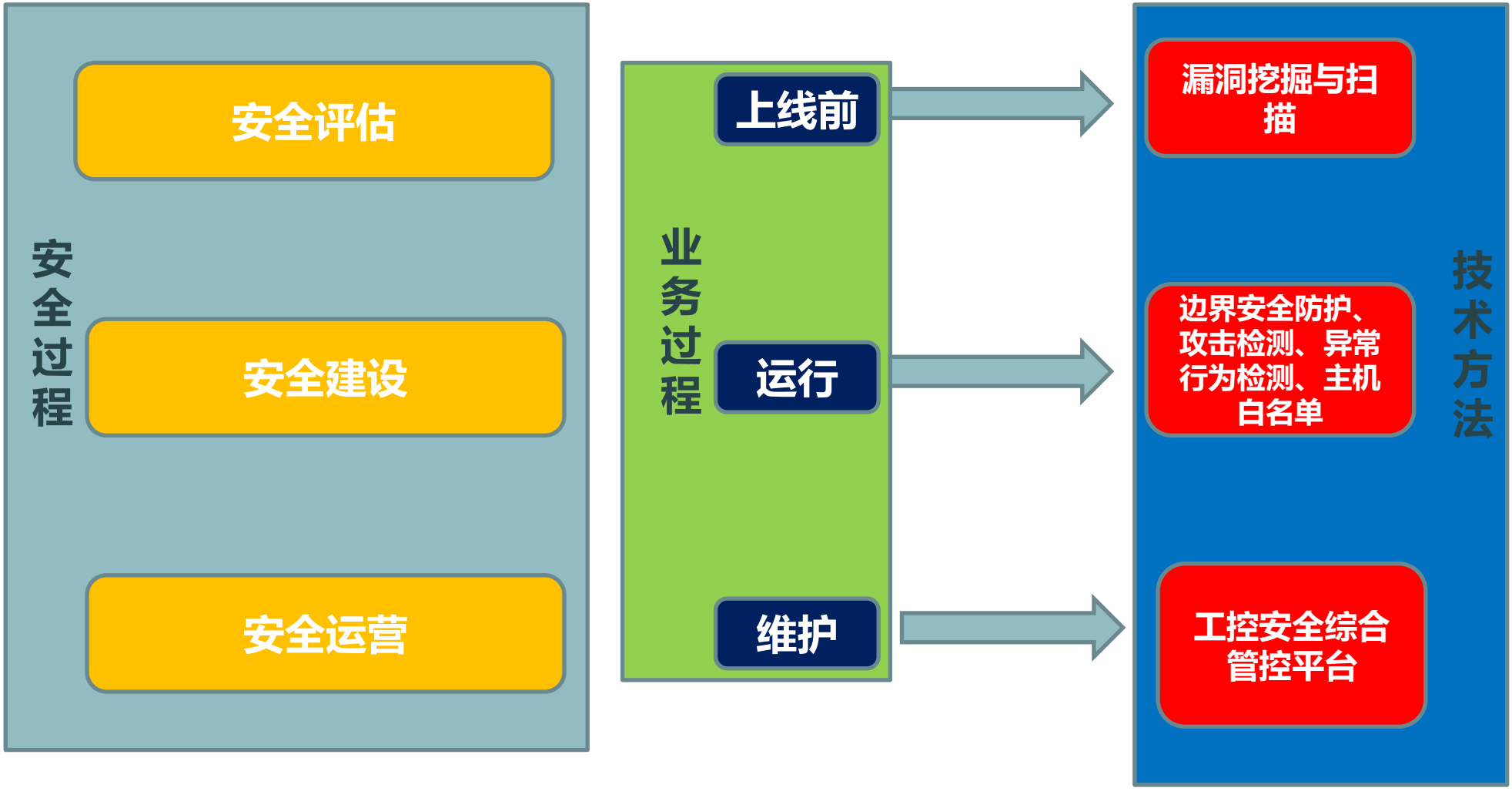
—— 系统不同节点的安全防护

系统生命周期安全管控


设计系统中的信息安全
产品上线前的安全检测
系统运行中的安全防护
运检阶段的安全检查
ICS Security


系统设计
系统上线
运行
检修
管理
技术
P D C A

安全技术保障


安全过程
安全评估
安全建设
安全运营
业务过程
上线前
运行
维护
技术方法
漏洞挖掘与扫描
边界安全防护、攻击检测、异常行为检测、主机白名单
工控安全综合管控平台

安全评估-上线前

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

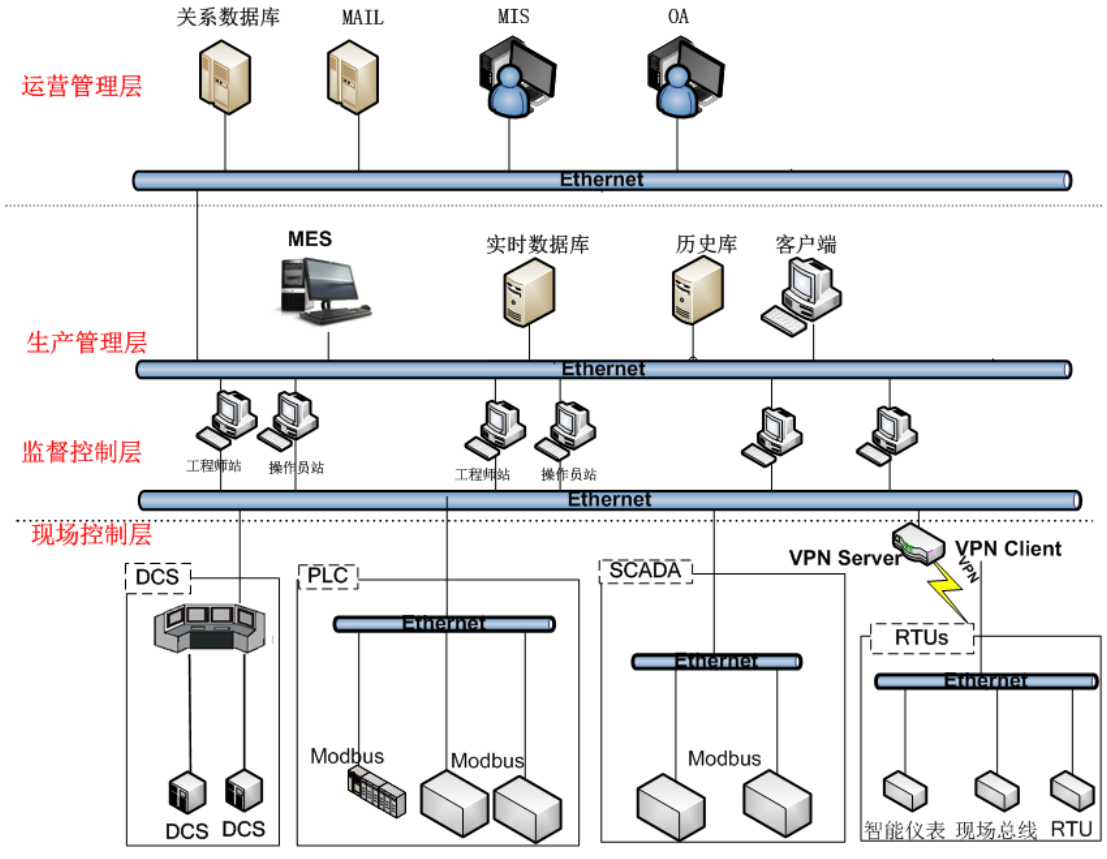
modbus	60870-5-1-4
512	2404

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

安全评估-在线运行



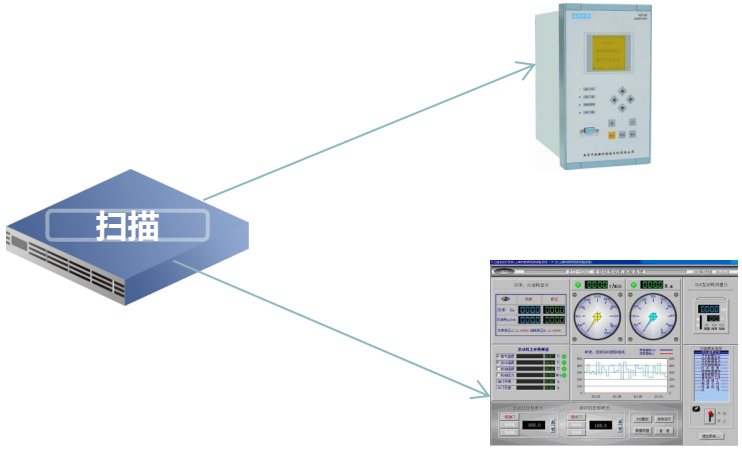
传统IT系统涵盖：

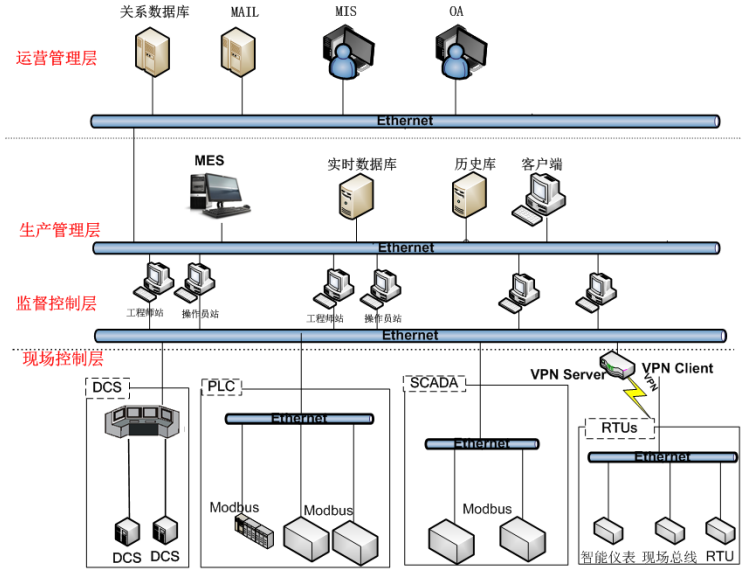
工程师站、操作员站、数据库服务器、交换机等。

工业控制器：

工控漏扫、组态软件

智能补丁

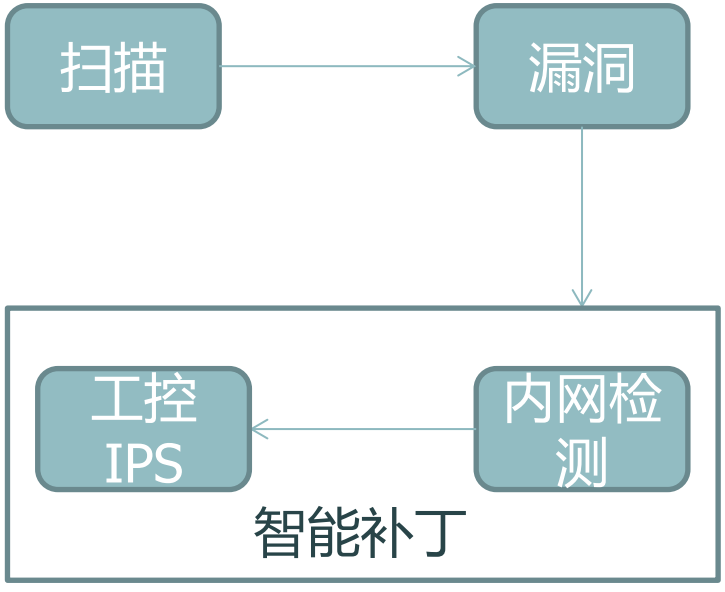


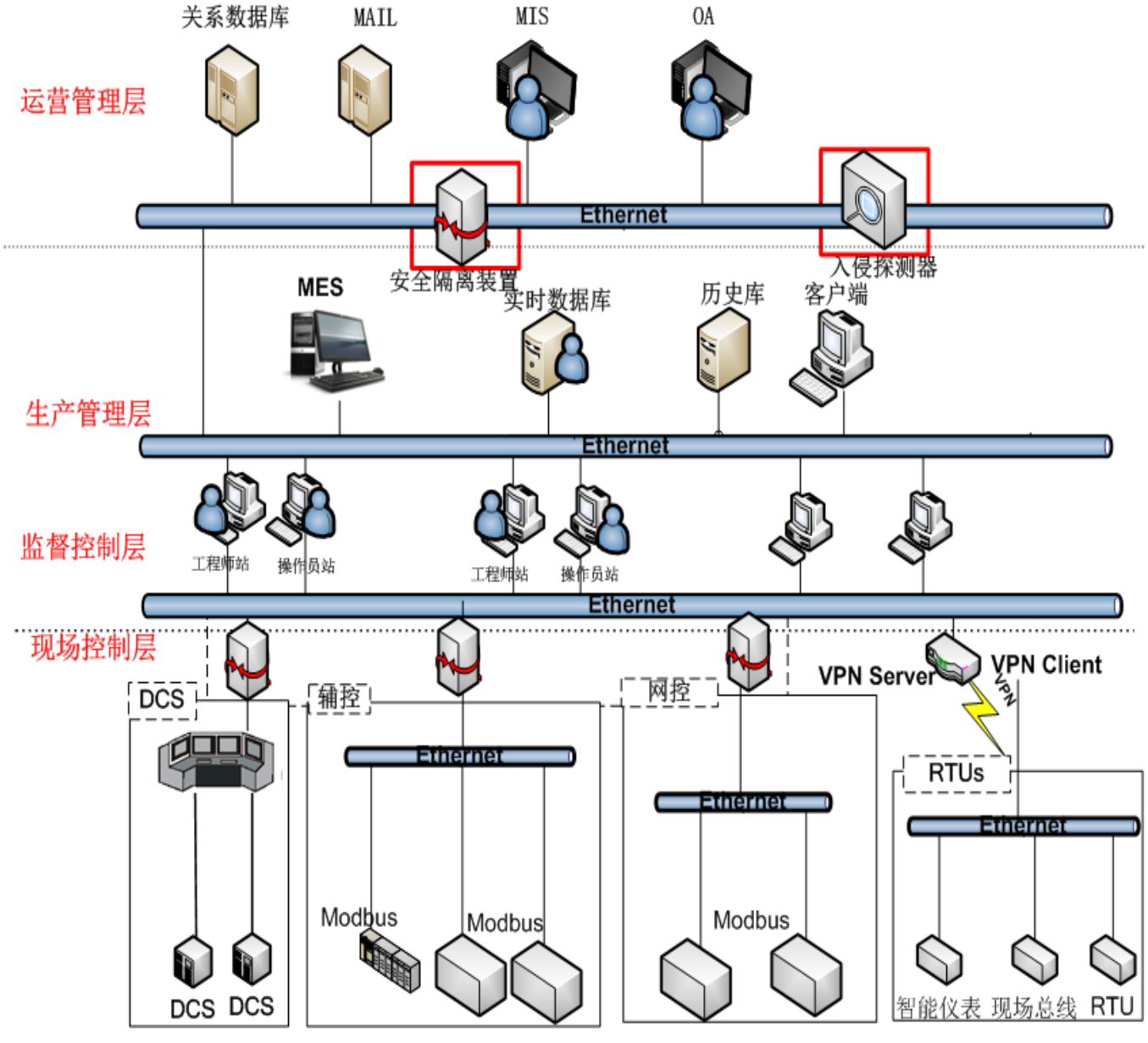


4.1漏洞分布

漏洞类别：高风险[11] 中危险[8] 低风险[7]

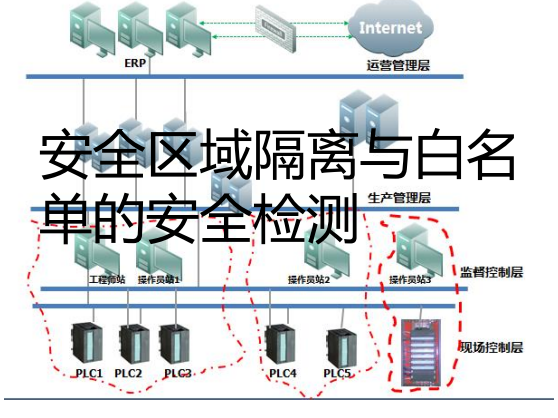
序号	漏洞名称	影响主机个数	影响主机百分比	出现次数
1	Ecava IntegraXor ActiveX save函数缓冲区溢出漏洞(CVE-2010-4597)	1/1	100%	1
2	WellinTech KingSCADA栈缓冲区溢出漏洞(CVE-2014-0787)	1/1	100%	1
3	Ecava IntegraXor < 4.00.4283 ActiveX 远程缓冲区溢出(CVE-2012-4700)	1/1	100%	1
4	Ecava IntegraXor igcom.dll Traversal 任意文件改写漏洞(CVE-2012-0246)	1/1	100%	1
5	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





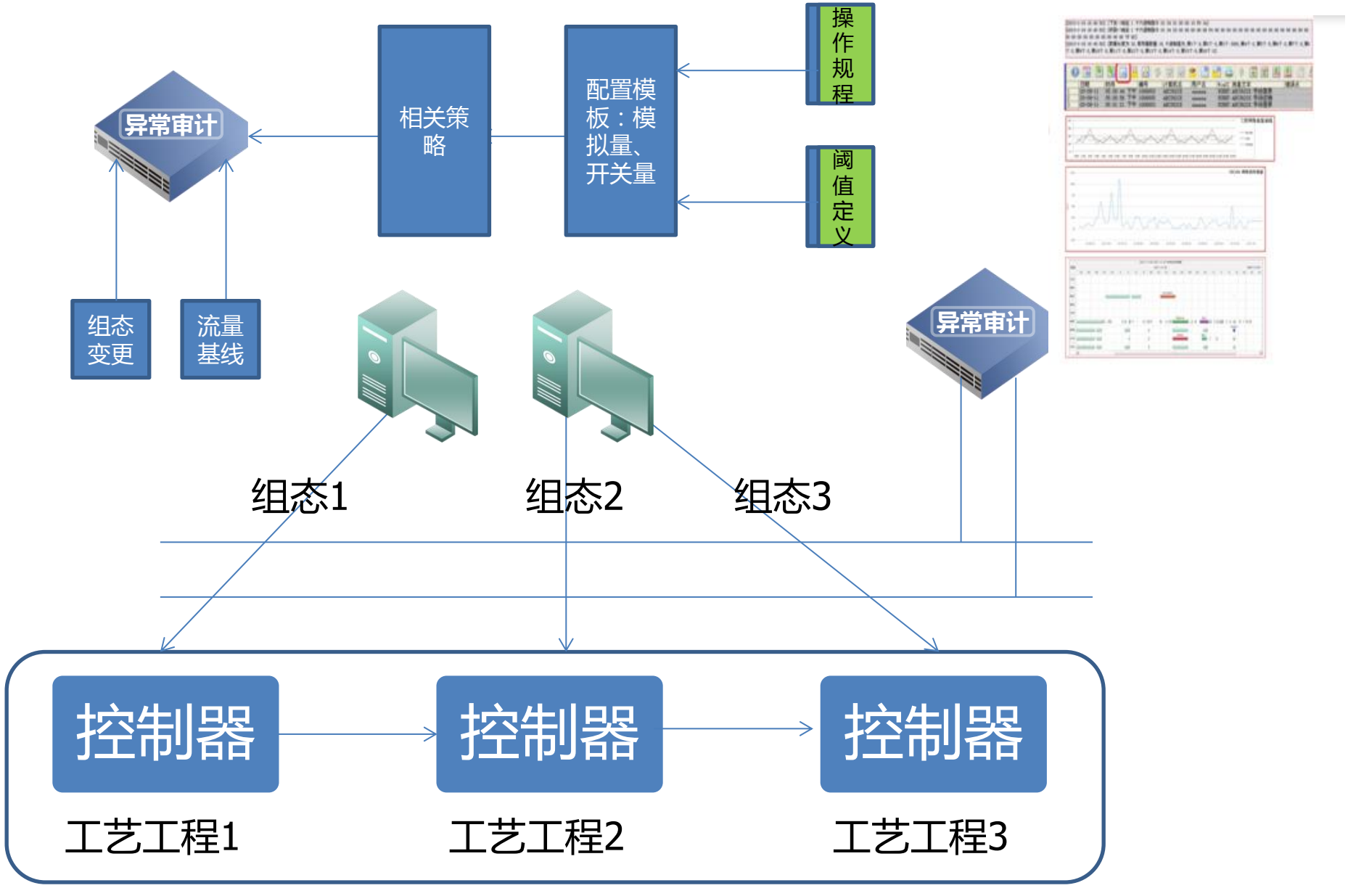
设备资产与攻击行为匹配

操作站白名单机制

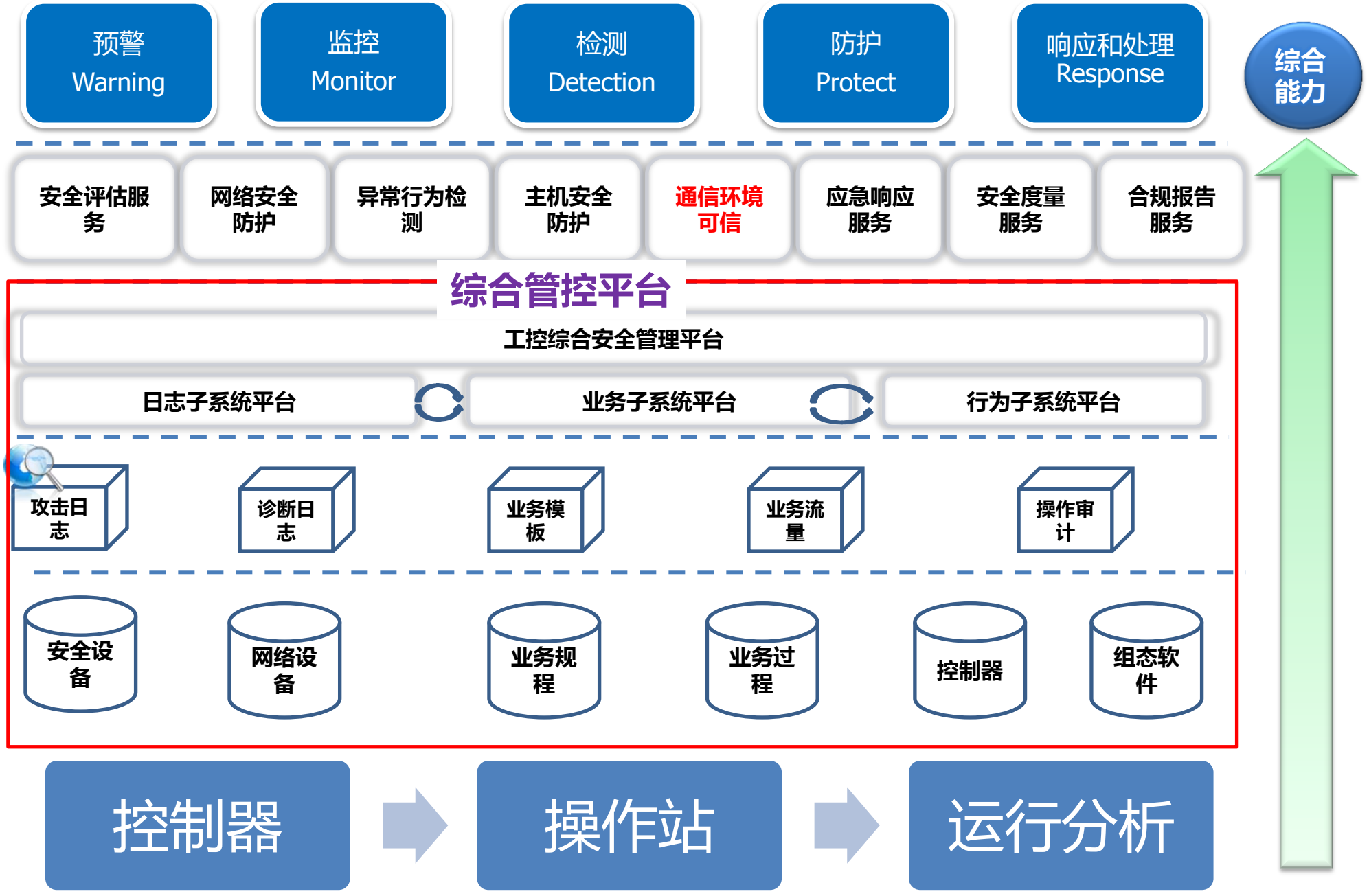


安全区域隔离与白名单的安全检测

异常审计


异常审计
相关策略
配置模板：模拟量、开关量
操作规程
阈值定义
组态变更
流量基线
异常审计
组态1
组态2
组态3
控制器
控制器
控制器
工艺工程1
工艺工程2
工艺工程3

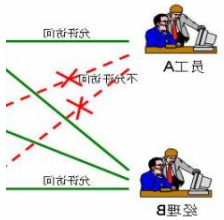
综合安全分析平台


预警
Warning
监控
Monitor
检测
Detection
防护
Protect
响应和处理
Response
综合能力
安全评估服务
网络安全防护
异常行为检测
主机安全防护
通信环境可信
应急响应服务
安全度量服务
合规报告服务
综合管控平台
工控综合安全管理平台
日志子系统平台
业务子系统平台
行为子系统平台
攻击日志
诊断日志
业务模板
业务流量
操作审计
安全设备
网络设备
业务规程
业务过程
控制器
组态软件
控制器
操作站
运行分析

信息安全与生产安全的结合

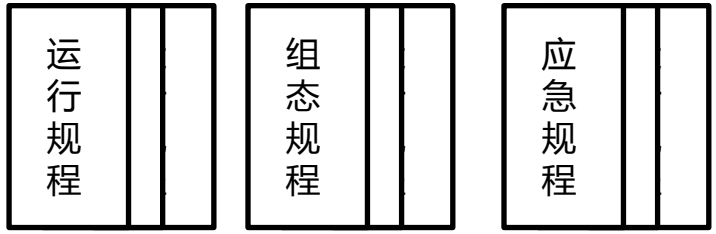
- 人员

岗位职责、 意识培训、权限划分



- 制度

运行规程、组态规程、应急规程

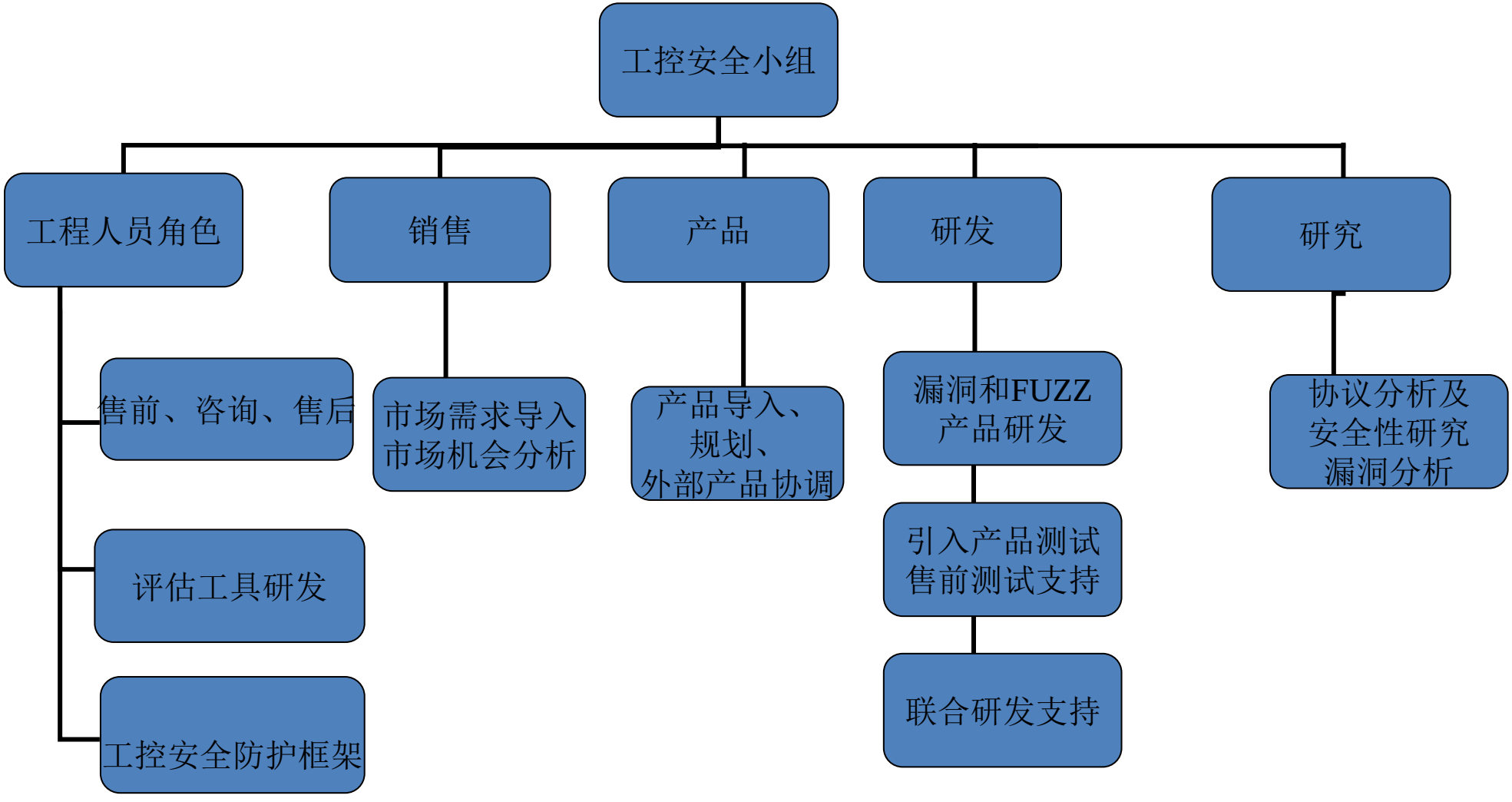


- 组织

信息安全的归口、管理架构

明确IT系统生产系统信息安全的归口

生产信息安全责任主体与信息主管部门的关系


工控安全小组
工程人员角色
销售
产品
研发
研究
售前、咨询、售后
评估工具研发
工控安全防护框架
市场需求导入
市场机会分析
产品导入、
规划、
外部产品协调
漏洞和FUZZ
产品研发
引入产品测试
售前测试支持
联合研发支持
协议分析及
安全性研究
漏洞分析

以无厚入有间，恢恢乎其于游刃必有余地矣

《南华经》

一把利剑、一场硬仗、杀出血路