工业控制系统安全认识和思考

中国软件评测中心

2016-5-21

目录 CONTENTS

一、安全事件


安全事件
前苏联油气管网爆炸-自主可控
伊朗核电站遭震网袭击-敌对攻击
美国棱镜监控计划曝光-敌对监视
乌克兰电网遭受网络袭击-恐怖网袭

一、安全事件-前苏联油气管网爆炸

1982年夏天，前苏联西伯利亚一条天然气输送管道发生了大爆炸

这场爆炸可谓是迄今为止最为严重的非核弹爆炸，爆炸引起的熊熊大火甚至可以从太空中观测到

一、安全事件-前苏联油气管网爆炸

管道基建有西欧和日本贷款，但当时尚未掌握相关SCADA软件技术，向美国购买又很快遭到拒绝，前苏联政府决心用克格勃“T局”下属“X线”间谍解决问题。

1970年，苏联新设了一个克格勃部门，名字叫做“科技理事会（T局）”，下属“X线”执行操作，目的是从西方窃取最有用的高科技研究成果

1970年，在法国居住了5年的维特洛夫被“X线”吸收，他的职责是评估特工获取的技术情报价值。

世事变化，维特洛夫对苏联渐渐开始失望，最后他决定叛变

上世纪70年代末，维特洛夫通过汤姆森公司普利福斯特向法国领土监护局(DST)正式“效忠”

从1981年春到1982年春，他向法国提供超过4000份秘密文件

导致来自克格勃的超过250名驻扎在全球工业间谍暴露

法国人欣喜若狂，他们还给了维特洛夫一个带有不详意味的代号“再会”

一、安全事件-前苏联油气管网爆炸

1981 → 1982 → 1983

1981年7月，在渥太华举行的**七国峰会**上，法国总统密特朗向里根分享了“维特洛夫文件”中的部分关键内容，该特工的档案资料还披露了苏联谋求的天然气管道控制技术。里根当时对密特朗披露的内容表示出了极大的兴趣

1982年1月，中情局专家威斯向中央情报局局长威廉凯西建议，可以在克格勃需要的技术名录里挑选出几种软件或硬件设备，将这些软硬件进行适当修改，然后再将其作为最新技术泄密给克格勃间谍

这些被修改的软件事实上已经隐藏了漏洞——即“逻辑炸弹”，这些软件可以正常工作一段时间，但随后会在特定的时间引发灾难

一、安全事件-前苏联油气管网爆炸

软件应用一段时间之后，重新调整了油泵的速度和阀门的设置，产生大大超过天然气接头和焊接承受的压力（8.4MPa），最终破坏整个管道系统。虽然这次管道爆炸未造成人员伤亡，但却对苏联的经济造成了巨大的破坏

灾难后果

在不到一年的时间里，美国向克格勃送出了众多的软硬件技术，但是前苏联人根本无法知道哪些技术是真的，哪些是假的。

一、安全事件-伊朗核电站遭震网袭击

2010年9月25日，伊朗的第一座核电站“布什尔核电站”遭受了“Stuxnet”病毒的攻击，浓缩铀离心机遭到破坏，全球超过45000个网络受到感染。

一、安全事件-伊朗核电站遭震网袭击

传播过程

首先感染外部主机；**然后感染U盘**，利用快捷方式文件解析漏洞，传播到内部网络；**在内网中实现管理网到控制网的跳转**，通过快捷方式解析漏洞、RPC远程执行漏洞、打印机后台程序服务漏洞，实现联网主机之间的传播；**最后抵达安装了WinCC软件的主机，展开攻击。**

攻击机理

获取PLC的访问控制权，拦截其他软件对PLC的访问命令，**修改发送至PLC 或从PLC返回的数据**；用被挂钩的导出命令修改这些发现或被破坏请求以保证Stuxnet的PLC 代码不会被发现或被破坏；对PLC代码的修改，使用“代码插入”的方式感染代码，感染OB1和OB35模块，并在其中注入恶意代码模块。

一、安全事件-伊朗核电站遭震网袭击

SW70-002：DLL加载策略缺陷漏洞
目的：实现对查询、读取函数的Hook，保证Stuxnet 的PLC代码不会被发现或被破坏

SW70-001：硬编码漏洞
目的：尝试访问该系统的SQL数据库，修改上传和下达的数据

MSXX-XXX：尚未公开的提升权限漏洞
目的：在利用MS08-067漏洞失败的情况下提升自身权限，再次尝试攻击

MS10-046：快捷方式文件解析漏洞
目的：使系统启动时加载攻击者指定的DLL文件，从而触发攻击和“摆渡”渗透

MS08-067：RPC远程执行漏洞
目的：以允许远程执行代码，获取完整权限，实现在内部局域网中的传播

MS10-061：打印机后台程序服务漏洞
目的：以系统权限执行任意代码，实现在内部局域网中的传播

一、安全事件-美国棱镜监控计划曝光

英国《卫报》和美国《华盛顿邮报》2013年6月6日报道，美国国家安全局（NSA）和联邦调查局（FBI）于2007年启动了一个代号为“棱镜”的绝密监控计划（ 代号US-984XN ），本计划允许NSA接入美国9个主要网络公司的中央服务器（中心服务器），直接提取电话记录、聊天日志、电子邮件、照片、语音通信、网络社交、视频、文件传输、存储数据、搜索记录等10类信息。

Microsoft YAHOO! skype Google facebook

paltalk.com QUALCOMM America Online YouTube

棱镜任务流程

NSA分析员将监听目标输入统一目标工具（UTT）

提交审查

审查存储的通讯信息

一级审查

每个产品线的S2 FAA审查官
监听目标审查/ 批准

专门的外国情报监听法监管和处理
（SV4）通讯信息的审查/批准

提交审查

审查存储的通讯信息

二级审查

目标和行动管理部门S343
监听目标的最终审查/批准

统一目标工具（UTT）

PRINTAURA;Web选择、分发管理员

对于存储的通信记录(非实时监控)，FBI会查询其数据库，确保筛选器不会匹配任何知名美国人。

FBI使用装在私人公司(例如微软、雅虎)的政府设备检索匹配的信息，不经进一步审查便交给NSA。

审查存储的通讯信息

FBI电子通讯监控局
调查和确认不是知名美国人士

提交 监听

发布存储的通讯信息

供货商
（谷歌，雅虎等）

监听目标
目标信息收集

FBI
数据拦截技术单元（DITU）

收集

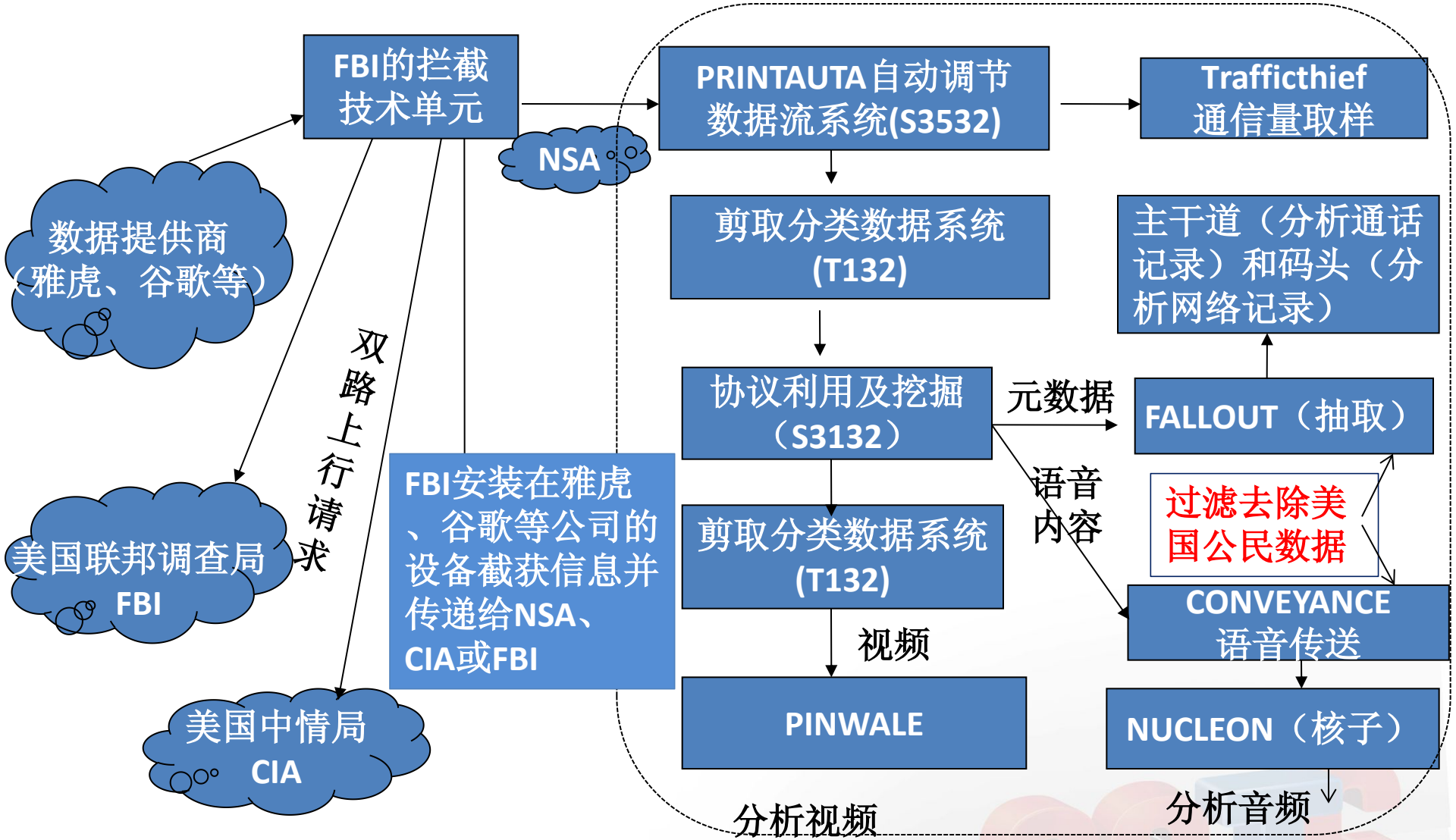
PINWALE项目、
核子等项目

外国情报监视法院不会审查任何个人信息收集请求

1、从新目标获取数据

这张幻灯片描述了NSA的分析人员通过“棱镜”系统监控新目标的整个流程。新的搜索请求会有人审核，如果诉求合理将获得通过。监控目标为外国公民，搜集信息期间身在国外。

棱镜数据流收集



2、分析从私人公司收集到的信息

“棱镜”系统获取通信信息后，由专门的系统处理语音、文字、视频以及地理位置、监控目标的设备特征等“数字网络信息”。

(TS//SI//NF)

棱镜监听案例（项目）编号注释

P2ESQC120001234

数据来源

- P1:微软
- P2:雅虎
- P3:谷歌
- P4:脸谱
- P5:Paltalk
- P6:YouTube
- P7:Skype
- P8:高通
- P9:苹果

固定的三个字母，表示收集信息的来源

内容类型
A: 通讯数据（搜索）
B: 即时通讯（聊天）
C: 电邮实时通知
D: 聊天实时通知
E: 电子邮件
F: 网络通话
G: 全文（网络论坛）
H: 社交网络信息
I: 社交网络基本用户资料
J:视频
. : 其他

表示对该监听目标建立的时间

序列号 #

TS/SI/NF:
Top Secret/Special Intelligence / No Foreigners

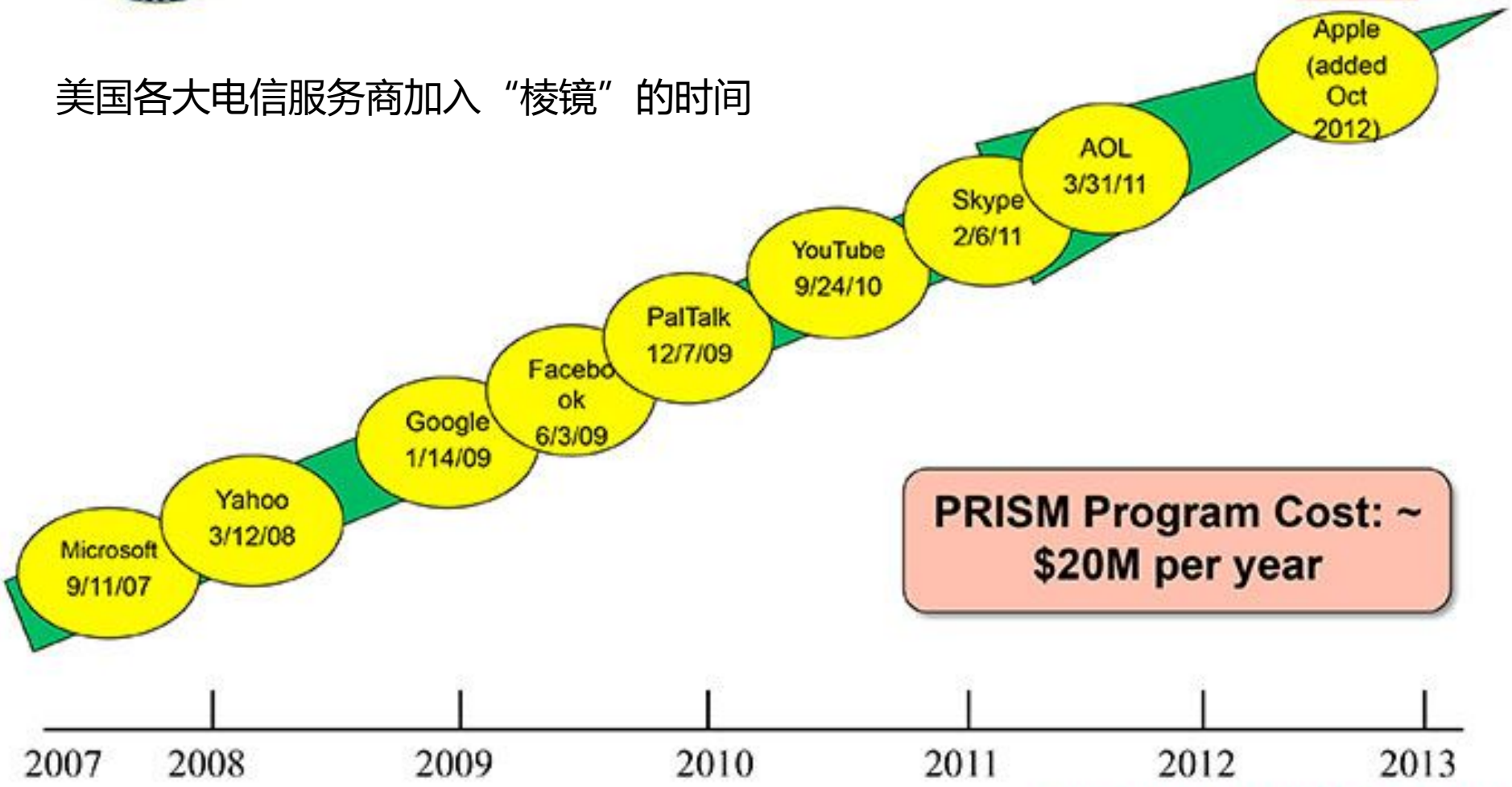
绝密/特殊情报/没有外国人

3、目标编号

每个被“棱镜”系统追踪的目标都会有一个编号，编号的不同部分各具含义。

(TS//SI//NF) Dates When PRISM Collection Began For Each Provider

美国各大电信服务商加入“棱镜”的时间



一、安全事件-美国棱镜监控计划曝光

其他监视项目

1.美国星际风监视计划概述

1.1棱镜监视项目

1.2核子监视项目

1.3主干道监视项目

1.4码头监视项目

2.美国野战行动

3.英国的时代（Tempora）监听计划

4.法国的 DGSE监视项目

5.德国“Xkeyscore”监控系统

6.澳洲的监听设施

7.“五只眼睛”监视组织（美国、英国、澳大利亚、加拿大和新西兰的情报机构组成）

一、安全事件-乌克兰电网遭受网络袭击

2015 年12 月23 日，乌克兰电力部门遭受到恶意代码攻击，乌克兰新闻媒体TSN 在24 日报道称：

“至少有**三个电力区域被攻击**，并于当地时间*15* 时左右导致了**数小时的停电事故**”；“攻击者入侵了监控管理系统，超过一半的地区和部分伊万诺-弗兰科夫斯克地区断电几个小时。”

Kyivoblenergo 电力公司发布公告称：“公司因遭到入侵，导致*7* 个*110KV* 的变电站和*23* 个*35KV* 的变电站出现故障，导致*80000* 用户断电。”

一、安全事件-乌克兰电网遭受网络袭击

以BlackEnergy等相关恶意代码为主要攻击工具，通过BOTNET体系进行前期的资料采集和环境预置

以邮件发送恶意代码载荷为攻击的直接突破入口

通过远程控制SCADA节点下达指令

摧毁破坏SCADA 系统实现迟滞恢复和状态致盲

以DDoS 电话作为干扰，最后达成长时间停电并制造整个社会混乱

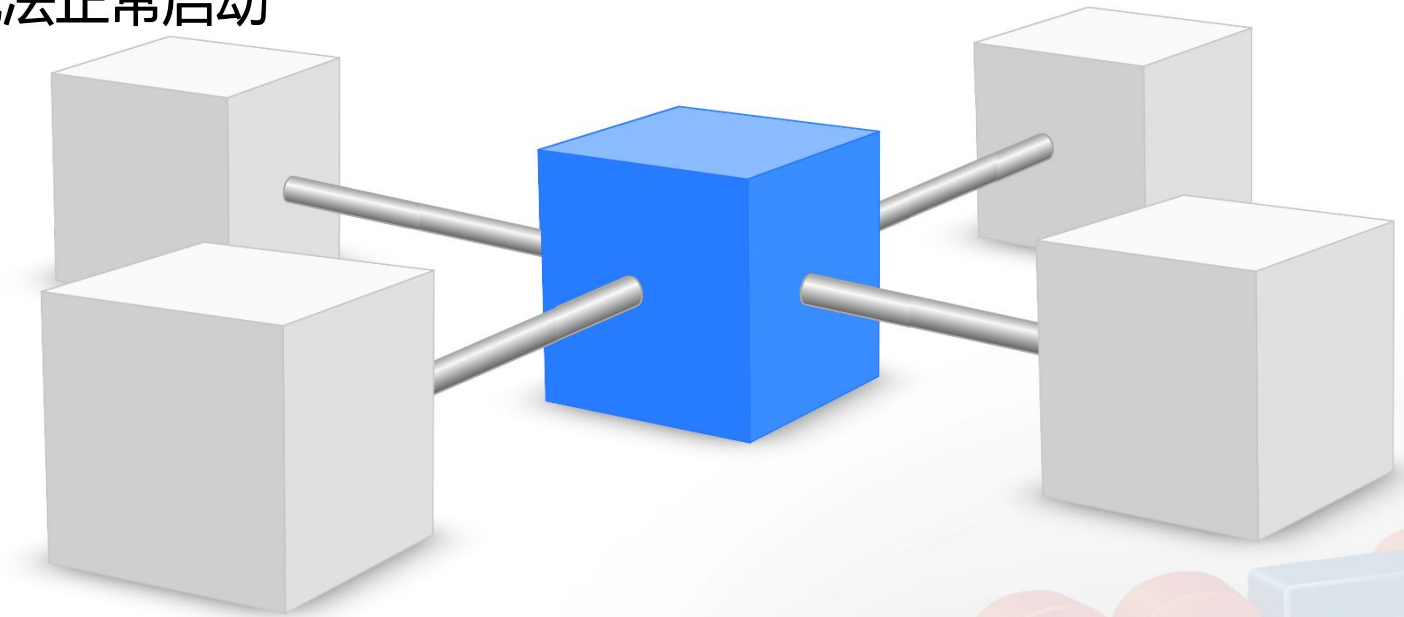
该事件是一起具有信息战水准的网络攻击事件

一、安全事件-乌克兰电网遭受网络袭击

攻击者通过鱼叉式钓鱼邮件或其他手段，首先向“**跳板机**”植入BlackEnergy恶意代码，通过BlackEnergy 建立据点进行横向渗透，之后通过攻陷监控装置区的关键主机，获取SCADA的控制权

KillDisk擦写包括主引导扇区（MBR）的前256 个磁盘扇区，导致系统无法正常启动

采用清除系统日志的方式提升事件后续分析难度



除对变电站进行攻击外，同时对电力客服中心进行电话DDoS 攻击，两组“火力”共同配合，发起攻击

采用覆盖文档文件和其他重要格式文件的方式，导致实质性的数据损失

目录 CONTENTS

二、基本认识-主要内容


基本认识
工业控制系统与信息系统边界
工业控制系统与信息系统差异
工控信息安全与功能安全差异
工业控制系统的基本安全要求

二、基本认识-ICS与IT边界-定义

工业控制系统（Industrial Control System ,ICS)

IEC 62443 Industrial communication networks - Network and system security 定义：工业自动化和控制系统（industrial automation and control system）**影响或改变工业过程的安全、信息安全和可靠操作的人员、硬件和软件的集合。**（广义工业控制系统）

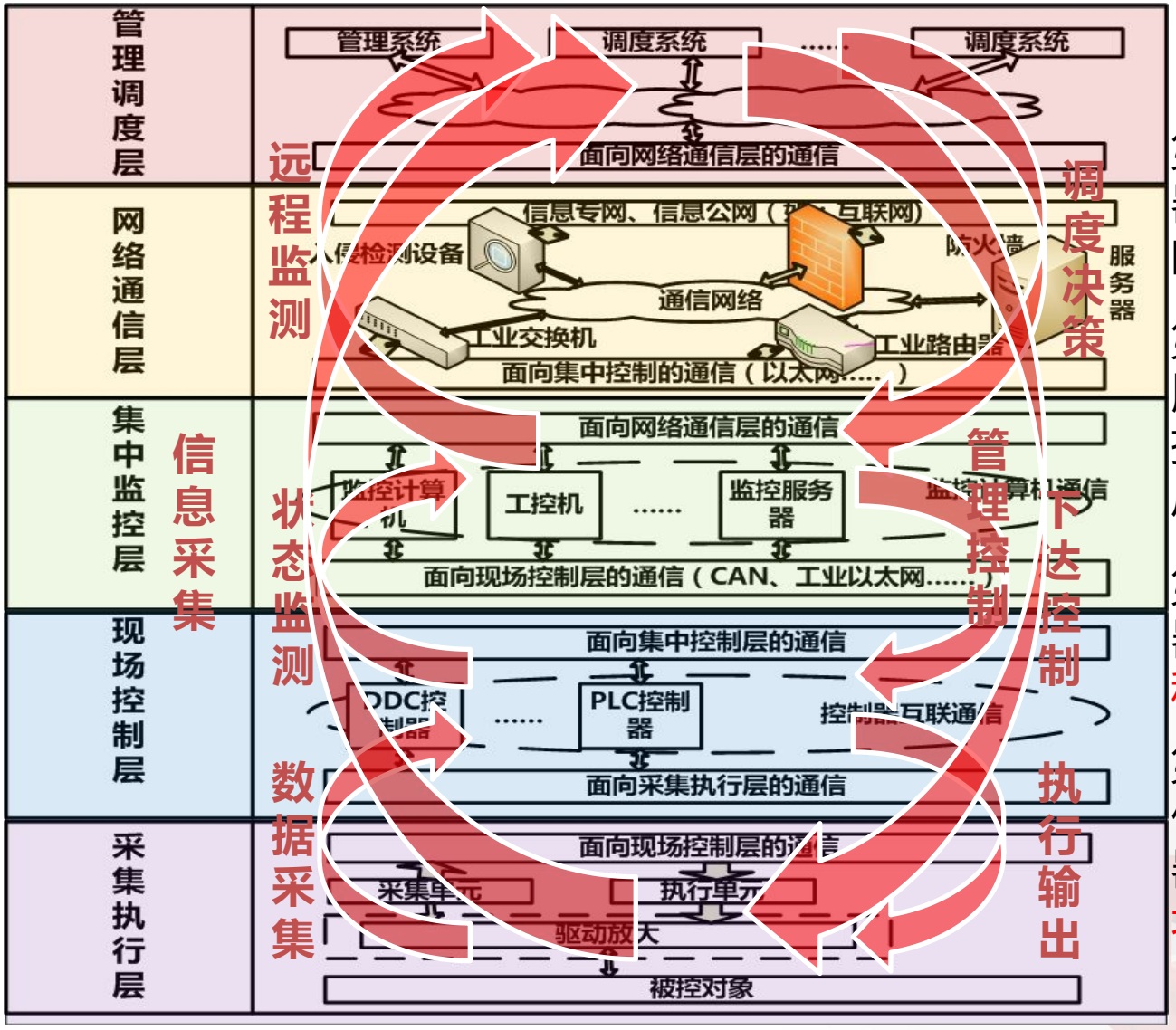
注：系统包括，但不限于：

1、**工业控制系统**包括分布式控制系统（**DCS**）、可编程序控制器（**PLC**）、远程终端单元（**RTU**），智能电子设备、监控和数据采集（**SCADA**），网络电子传感和控制，监视和诊断系统；

2、相关的**信息系统**，例如先进控制或者多变量控制、在线优化器、专用设备监视器、图形界面、过程历史记录、制造执行系统和工厂信息管理系统；

3、相关的内部、人员、网络或机器**接口**，为连续的、批处理、离散的和其他过程提供控制、安全和制造操作功能。

二、基本认识-ICS与IT边界-架构



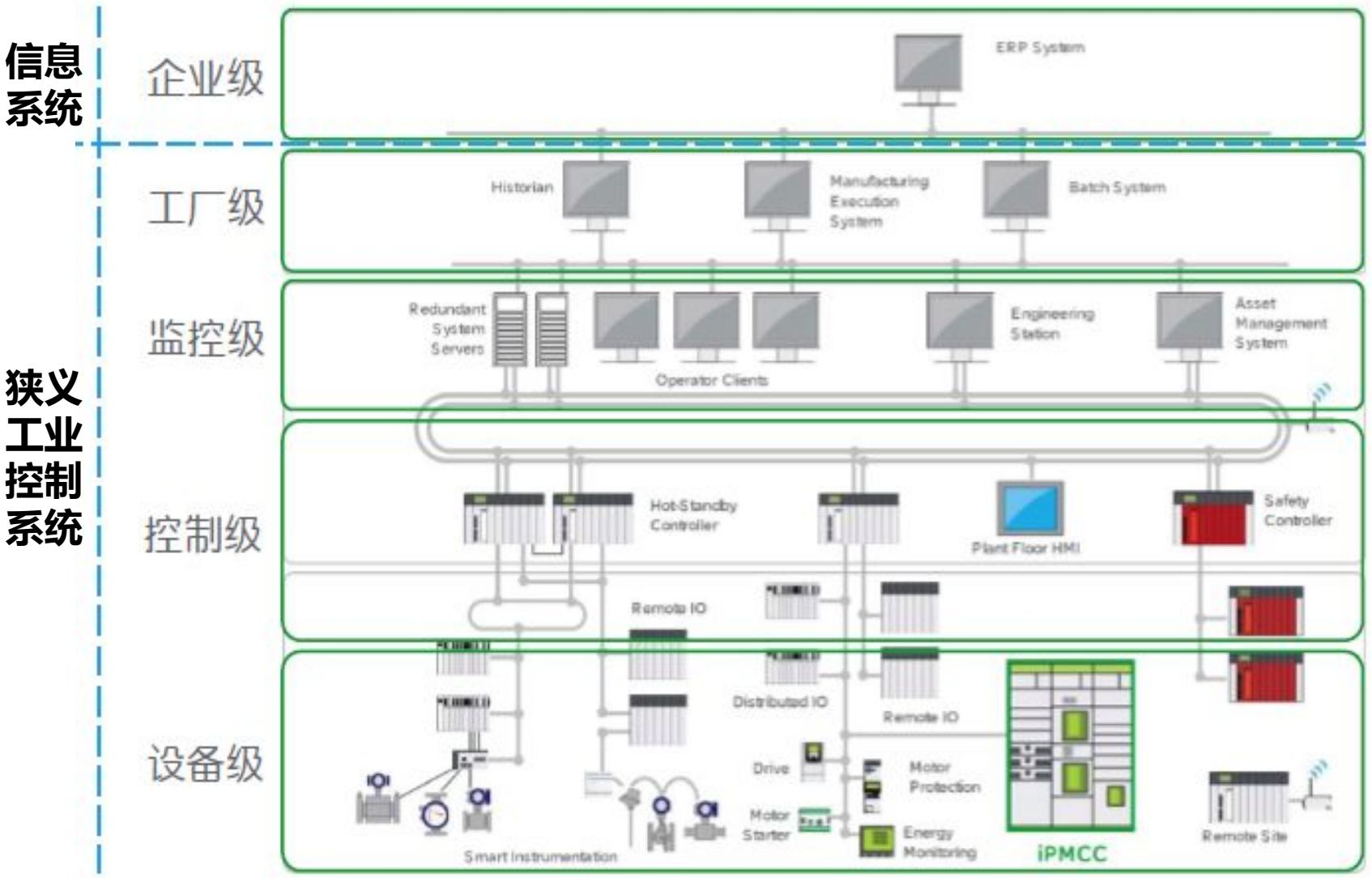
第三个闭环：管理服务器、调度服务器等构成的管理调度环

第四个闭环：管理调度服务器、监控服务器、控制器、被控设备等构成的**管理控制环**

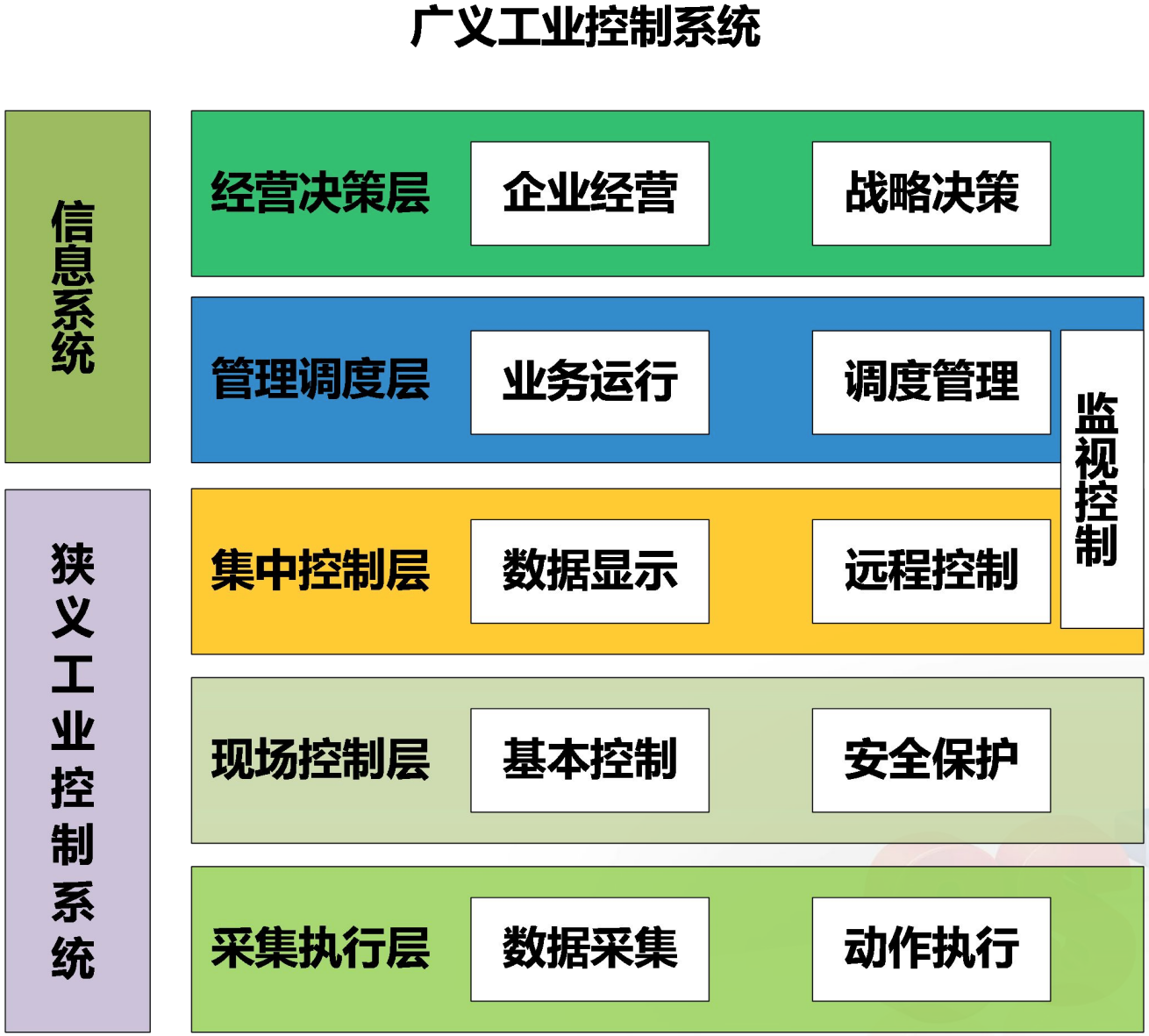
第二个闭环：监控服务器、工控机等构成的**远程控制环**

第一个闭环：控制站、传感器、控制器、执行器和被控对象构成的**现场控制环**

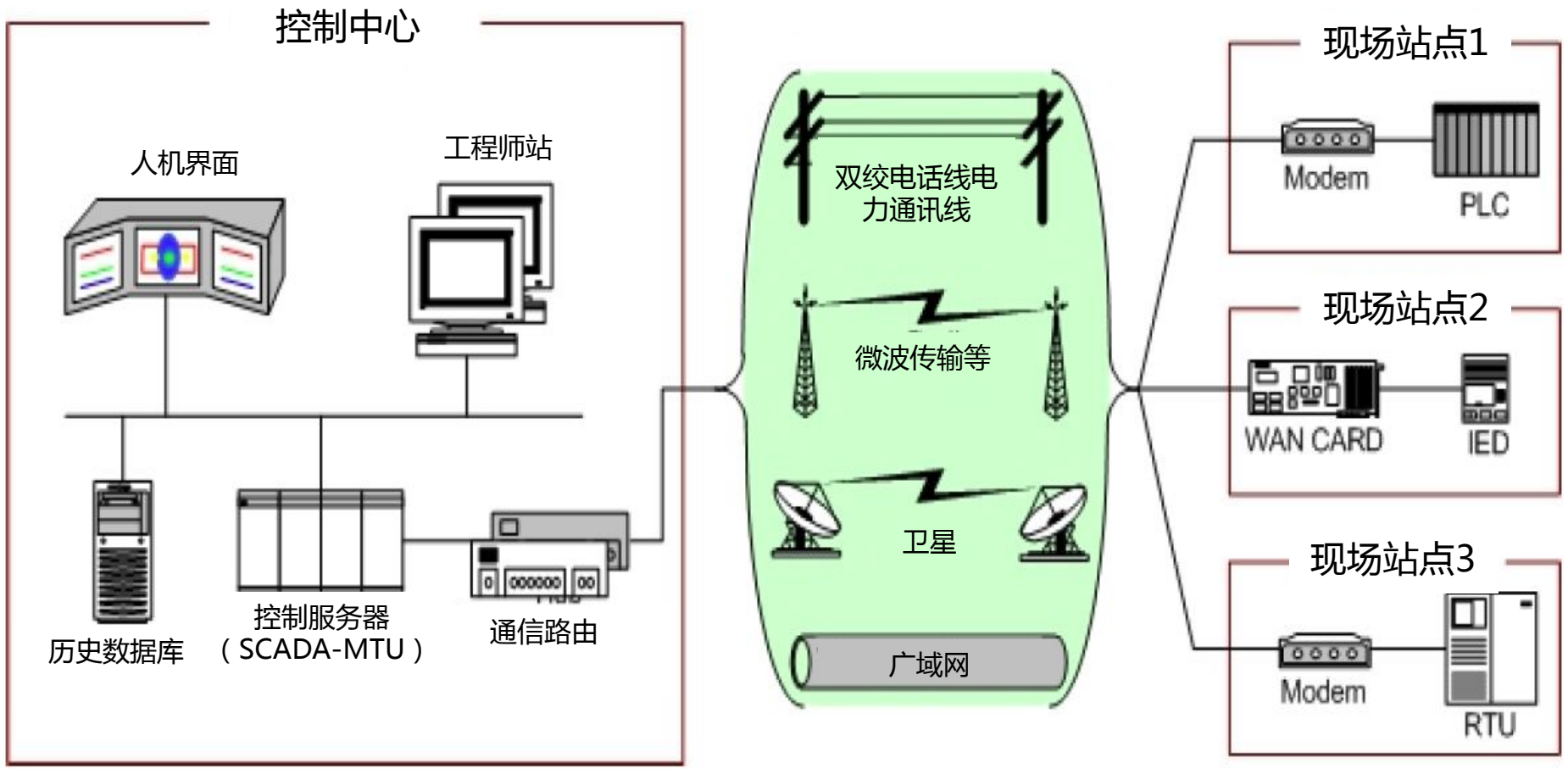
二、基本认识-ICS与IT边界-界定



二、基本认识-ICS与IT边界-界定

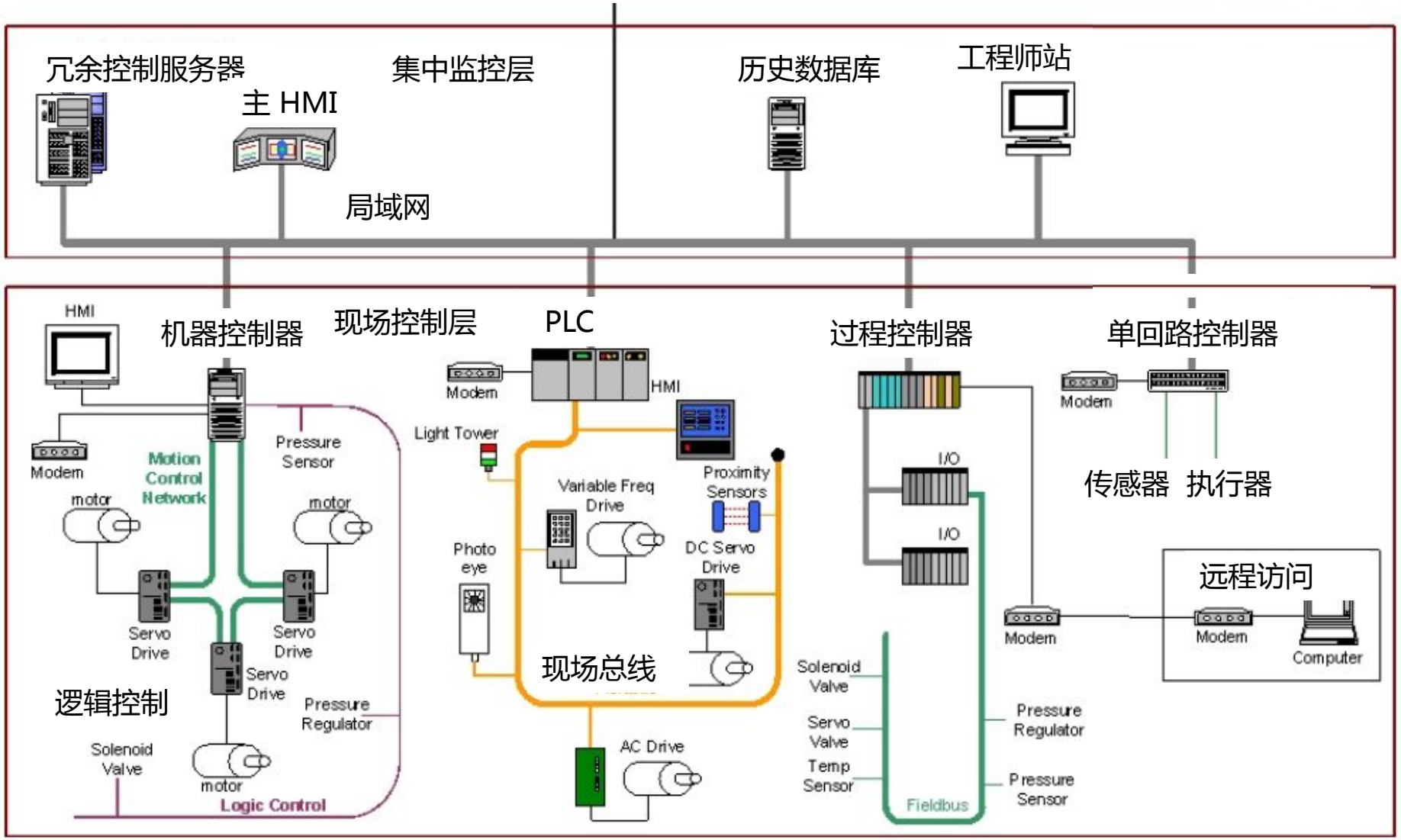


二、基本认识-ICS与IT边界-SCADA架构

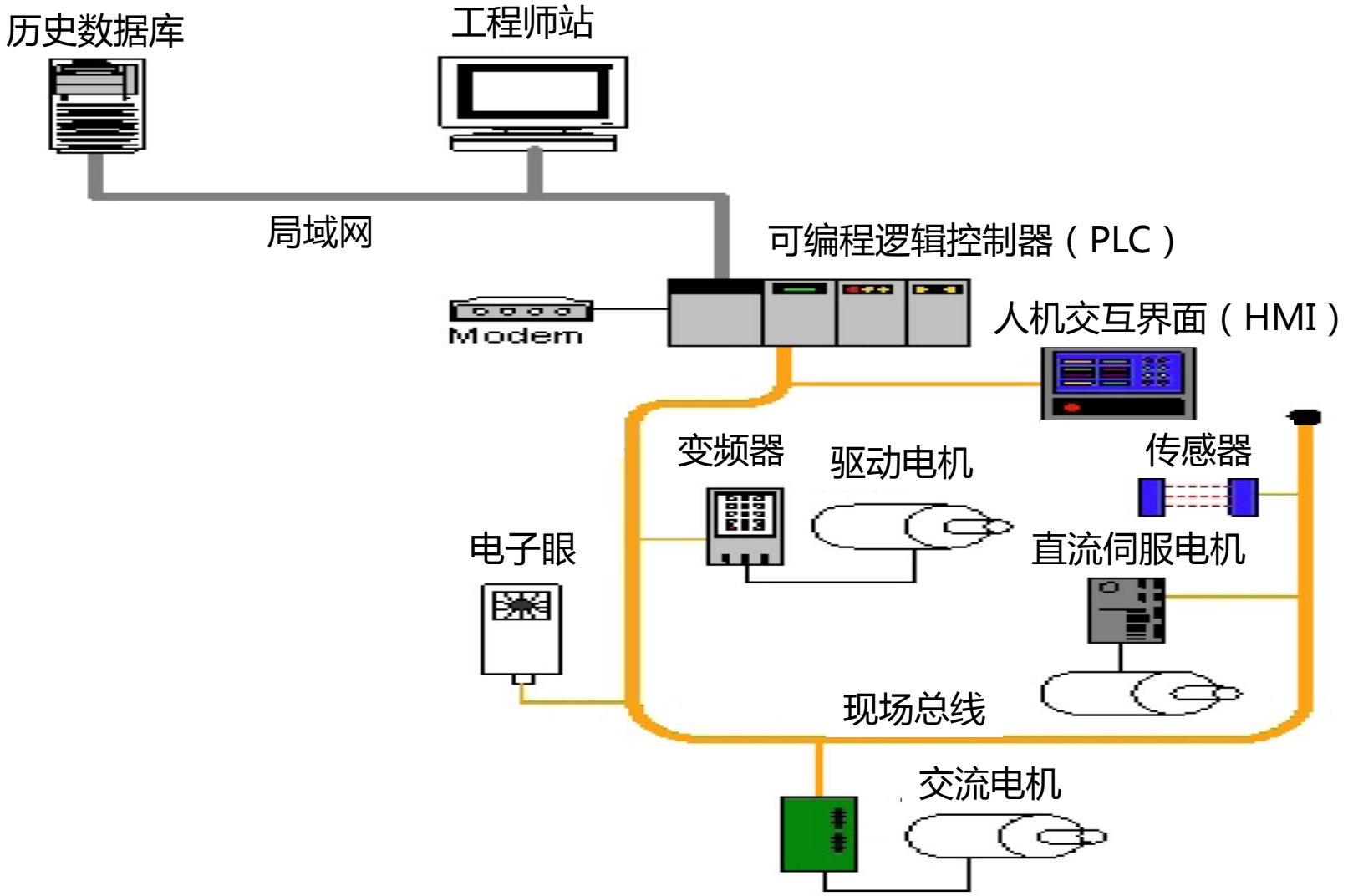


二、基本认识-ICS与IT边界-DCS架构

MES制造执行系统、MIS管理信息系统、ERP企业资源计划、……



二、基本认识-ICS与IT边界-PLC架构



二、基本认识-ICS与IT差异

用途	•ICS属于工业生产领域的生产过程运行控制系统，重点是**生产过程的采集、控制和执行** •信息系统通常是信息化领域的管理运行系统，重点在于**信息管理**
目标	•ICS以**生产过程的控制**为中心 •信息系统的目的是**人使用信息进行管理**
安全三要素	•传统IT系统的安全三要素**机密性、完整性、可用性**按**CIA原则**排序，即机密性最重要，完整性次之，可用性排在最后 •ICS系统的安全目标应符合**AIC原则**，即可用性排在第一位，完整性次之，机密性排在最后
后果	•ICS系统受到攻击后会直接对人民生命财产安全造成威胁 •传统IT系统失效后对物理环境无直接影响

二、基本认识-ICS与IT差异-对比

类别	IT系统	ICS
运行	非实时，可延迟，高数据量	实时，不可延迟，中数据量
实用性	可重启，实用性要求不高	不可重启，高实用性要求
侧重点	机密性、完整性和可用性	人身安全，进程安全最高
结构安全	关注信息安全和中心安全	关注边缘设备和中心安全
意外后果	可多种安全方案	必须测试后才能上线安全方案
时间准则	紧急要求不高	紧急要求高
系统处理	可用典型操作系统	系统往往没有安全防护
资源限制	系统有足够资源给安全方案	系统不一定有资源给安全方案
通信	标准通信协议	专有通信协议
变化管理	可自动更新软件	软件变动必须测试才能上线
管理支持	可以多样化支持	通常单一服务商支持
组件寿命	3-5年	15-20年
访问组件	可以随时访问本地组件	组件可能被遥控，难以访问

二、基本认识-ICS与IT差异-对比

类别	IT系统	ICS
性能需求	● 通信非实时 ● 响应一致性 ● 高吞吐量 ● **允许存在延迟和抖动**	● 通信实时 ● 响应时间关键性 ● 中等吞吐量 ● **不允许存在延迟和抖动**
可用性需求	● 允许重启系统 ● 以系统的**功能需求为主**，可用性居其次	● 不允许重启系统 ● **高可用性需求**，部署前需详尽测试 ● 需要冗余系统 ● 中断操作需要提前计划
风险管理需求	● **数据**的保密性和完整性是第一位的 ● **容错性是次要**的—短暂停机不是主要风险 ● 主要风险是商业运作的延迟影响	● 首先**人身**安全，其次**过程**安全，核心是进程安全 ● 容错是必不可少的，任何**停机都是不能接受**的 ● 主要风险是经常性的不合规定操作、环境影响

二、基本认识-Security与Safety差异

功能安全和信息安全

功能安全(Safety)聚焦保护BPCS外围人物环，考虑随机硬件失效对生命、健康、设施或环境的伤害或影响，SIS紧急处置BPCS内外所导致事故导火索，强调故障导向安全
偏向生产安全、物理安全

信息安全(Security)聚焦保护BPCS本身可用、完整和机密，而非健康、安全和环境(HSE)，防止技术、管理脆弱性和外在威胁的结合，规避BPCS弱点、威胁所导致的风险
偏向数据安全和网络安全

对工业控制系统安全内涵的理解

工业控制系统安全是Security和Safety的融合，不仅要研究设备、工艺过程的危险性，还要进一步综合考虑黑客、有组织犯罪等人为因素的威胁，还要进一步考虑安全对企业自身、对社会公众甚至对国家安全所造成的影响和后果。
工业控制系统安全分析技术手段有：失效模式、影响及其诊断分析(FMEDA)，故障树、事故树分析(FTA)，保护层分析(LOPA)、危险与可操作性分析(HAZOP)、风险评估(GB/T27921/ 20984)、渗透测试等等

二、基本认识-安全要求-标准规范

国内外主要的工业控制系统安全标准规范

《NIST SP800-82 工业控制系统信息安全指南》，是2011年6月美国国家标准与技术研究院（NIST）制定的、旨在指导开发商、集成商**建立安全工业控制系统的指南。**

《IEC62443 工业自动化和控制系统信息安全》，是2009年IEC/TC65/WG10（国际电工协会工业过程测量、控制与自动化/网络与系统信息安全工作组）与国际自动化协会ISA99成立联合工作组组织制定、**旨在应对工业自动化和控制系统信息安全挑战的系列标准，以规避工业控制系统在信息安全方面的风险。**

《工业控制系统信息安全等级保护规范标准草案》，是2013年国家公安部组织制定、旨在强化工业控制系统领域的信息安全等级保护工作的系列标准。

二、基本认识-安全要求-标准规范

国内外主要的工业控制系统安全标准规范

《GBT 26333-2010 工业控制网络安全风险评估规范》，是2010年全国工业测量和控制标准化委员会制定的、旨在发现工业网络安全隐患、增强工业控制网络安全的风险评估规范。

《GBT 30976.1-2014工业控制系统信息安全 第1部分：评估规范》，是2014年全国工业过程测量和控制标准化技术委员会制定的、**旨在对工业控制系统的信息安全进行评估，以规避工业控制系统在信息安全方面的风险。**

《GBT 30976.2-2014 工业控制系统信息安全 第2部分：验收规范》，是2014年全国工业过程测量和控制标准化技术委员会组织制定的、旨在证明工业控制系统在增加安全解决方案后满足对安全性的要求。

二、基本认识-安全要求-注意点

1.连接管理要求

- **断开**工业控制系统同公共网络之间的所有**不必要连接**
- 对确实需要的连接，系统运营单位要**逐一进行登记**，采取设置防火墙、单向隔离等措施加以防护，并定期进行风险评估，不断**完善防范措施**
- **严格控制**在工业控制系统和公共网络之间**交叉使用移动存储介质以及便携式计算机**

2.组网管理要求

- 工业控制系统组网时要**同步规划、同步建设、同步运行**安全防护措施
- 采取虚拟专用网络、线路冗余备份、数据加密等措施，加强对关键工业控制系统远程通信的保护
- 对无线组网采取严格的身份认证、安全监测等防护措施，防止经无线网络进行恶意入侵，尤其要**防止通过侵入远程终端单元（RTU）进而控制部分或整个工业控制系统**

二、基本认识-安全要求-注意点

3.配置管理要求

- 建立控制服务器等工业控制系统关键设备**安全配置**和**审计制度**
- 严格账户管理，根据工作需要**合理分类设置账户权限**
- 严格口令管理，及时**更改**产品安装时的**预设口令**，**杜绝弱口令、空口令**
- 定期对账户、口令、端口、服务等进行检查，及时**清理不必要的用户和管理员账户，停止无用的后台程序和进程，关闭无关的端口和服务**

4.运维管理要求

- **慎重**选择工业控制系统设备，在供货合同中或以其他方式明确供应商应承担的**信息安全责任**和**义务**，确保产品**安全可控**
- 加强对技术服务的**信息安全管理**，在安全得不到保证的情况下禁止采取远程在线服务
- 密切关注产品漏洞和补丁发布，严防病毒、木马等恶意代码侵入。**关键工业控制系统软件**升级、补丁安装前要请专业技术机构进行**安全评估**和**验证**

二、基本认识-安全要求-注意点

5.数据管理要求

- 国家基础数据以及其他重要敏感数据的采集、传输、存储、利用等，要采取**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，切实维护个人权益、企业利益和国家信息资源安全

6.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，根据实际情况采取必要的**备机备件**等**容灾备份**措施

二、基本认识-安全要求-注意点

7.白名单要求

- 建立网络设备、控制设备、计算机设备等所有**联网设备的白名单**，非白名单设备无法进入
- 建立并启用**应用程序白名单**，只允许预先经认可的应用程序来执行
- 建立**数据存取、指令执行白名单**，只允许符合特定规则的数据操作，只允许符合工艺规则的指令运行

8.密码应用要求

- 新建的重要工业控制系统应使用**国产密码产品**，已建的重要工业控制系统开展国产密码改造
- 定期比对应用程序的**数字摘要**，防止对程序的非预期修改
- 对RTU和SCADA之间的数据**通信进行加密**，并对敏感信息进行加密
- 对用户进行身份**认证和鉴别**，采用双因素认证

二、基本认识-安全要求-注意点

9.分层分域要求

- 坚持“管控分设、光电隔离、纵向分层、横向分区、层间隔离、区间认证、网络专用”的原则开展防护
- 具备网络架构拓扑图和资产清单，并及时更新，对不同区域之间的安全防护进行优化

10.自主可控要求

- 在设备选型和采购过程中优先选择国产工业控制设备
- 选择国内设计单位、集成单位和供货商，并在设备及系统的全生命周期内对其负责，具备系统的二次开发能力

目录 CONTENTS

三、应对策略

1. 完善工业控制系统安全法规及标准
2. 建立工业控制系统分类分级监管机制
3. 健全企业工业控制系统安全责任制
4. 统筹推进工业控制系统多角度防护
5. 推行工业自动化工程测试管控体系
6. 开展工业控制系统安全测试、检查和评估

三、应对策略

1.完善工业控制系统安全法规及标准

应结合实际制定并完善相关法规制度，并参考《IEC 62443工业通讯网络网络和系统安全》、《NIST SP800-82 工业控制系统安全指南》、《GB/T 26333-2010工业控制网络安全风险评估规范》、《GB/T 30976.1-2014 工业控制系统信息安全 第1部分：评估规范》、《GB/T 30976.2-2014工业控制系统信息安全 第2部分：验收规范》、《GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求》制定适用于各行业领域的工业控制系统安全标准

部分企业对推荐性标准的执行力度不够，有必要出台强制性标准

三、应对策略

2.建立工业控制系统分类分级监管机制

按照行业领域或设施工艺分类，将工业控制系统作为电子基础设施分级监管，分为战略级、关键级、重大级、重要级和一般级，分别由国家、省、市、县负责，开展工业控制系统基数、资产基数和风险基数摸底，按照级别要求组织开展安全技术防护，建立相应的安全监测、信息共享、信息通报与事故预警体系。

三、应对策略

3.健全企业工业控制系统安全责任制

要按照谁主管按照谁负责、谁运营谁负责、谁使用谁负责的原则建立健全信息安全责任制，建立信息安全领导机构和专职部门，配备工业控制系统安全专职技术人员，统筹工业控制系统和信息系统安全工作，建立工业控制系统安全管理制度和应急预案，保证充足的信息安全投入，系统性开展安全管理和技术防护

三、应对策略

4.统筹推进工业控制系统多角度防护

结合生产安全、功能安全、信息安全等多方面要求统筹开展工业控制系统安全防护，提升工业控制系统设计人员、建设人员、使用人员、运维人员和管理人员的信息安全意识，避免杀毒等传统防护手段不适用导致工业控制系统未进行有效防护、工业控制系统遭受外界攻击而发生瘫痪、工业控制系统安全可靠性不足导致停机事故、工业控制系统重要信息失窃密等风险

三、应对策略

5.推行工业自动化工程测试管控体系

要在系统需求设计、选型、招标、建设、验收、运维、扩建等阶段强化厂商内部测试、出厂测试、选型测试、试运行测试、验收测试、安全测试、入网测试、上线或版本变更测试等测试管控手段，减少需求、设计、开发、运维过程中的问题，提升系统安全可靠性

三、应对策略

6.开展工业控制系统安全测试、检查和评估

要定期开展工业控制系统的安全测试、风险评估、安全检查和安全评估，以便及时发现网络安全隐患和薄弱环节，有针对性地采取管理和技术防护措施，促进安全防范水平和安全可控能力提升，预防和减少重大网络安全事件的发生。同时要加强对工业领域工业控制系统信息安全工作的指导监督，加强安全自查、检查和抽查，确保信息安全落到实处