股票代码：002439

启明星辰

工业控制系统安全理念及其解决方案

启明星辰—张晔

zhangye@venustech.com.cn

Mobile：13466787338

纲要

工业控制系统的演进过程

- 工业控制系统技术由专用性向通用性演进
  - **工控系统伴随着IT技术的发展而发展，且大量采用IT通用软硬件，如PC、操作系统、数据库系统、以太网、TCP/IP协议等；**
- 工业控制系统由封闭性向开发性演进：
  - **互联网、物联网技术的发展，工业化与信息化的深度融合，使工控系统不再是一个独立的系统。**
- 工业控制系统由硬到软演进：
  - **工业控制系统由机械化、电气化、电子化、软件智能化方向不断演进。即工控控制系统不断的由硬到软在演进。**

1、工控系统的安全问题是IT系统安全问题的延伸与放大！

工控安全事件（1）

- **2010年11月16日**，伊朗布什尔核电站遭到‘震网病毒’攻击，造成 **1000台离心机被摧毁，浓缩铀被毁**
- **2008 年，攻击者入侵波兰某城市的地铁系统，通过电视遥控器改变轨道扳道器，导致4节车厢脱轨**
- **2011 年，黑客通过入侵数据采集与监控系统SCADA，使得美国伊利诺伊州城市供水系统的供水泵遭到破坏。**

工控安全事件（2）

- 2008年，华中（河南）电网因继电保护误动作、安全稳定控制装置拒动等原因引发一起重大电网事故，导致华中东部电网与川渝电网解列，华中电网与西北电网直流闭锁、与华北电网解列。
- 2007年，法国电力公司全资企业广西来宾B电厂（2台36万千瓦燃煤机组）因江边水泵房设备的控制和通讯完全中断，造成两台机组停运，全厂对外停电。
- 2006年，清华同方环境有限责任公司在中国华能集团公司德州电厂二期3号机组脱硫装置试运行过程中，旁路门突然非受控性关闭，致使工作间内7人被埋，其中4人经抢救无效死亡。

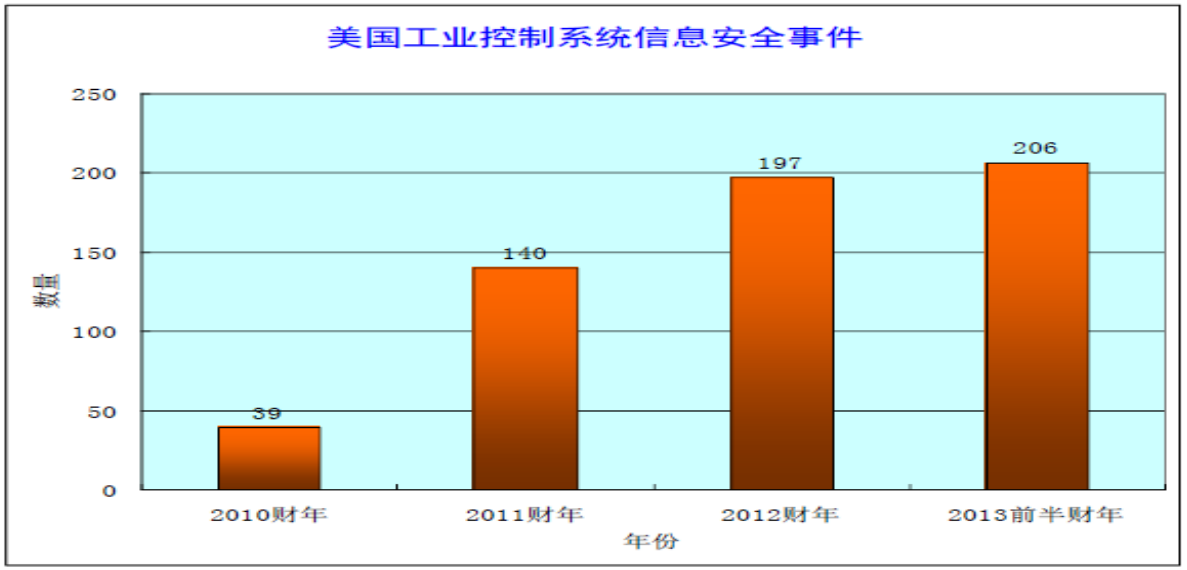
某行业行业工控安全事件（3）

- 移动存储设备的随意接入，把病毒代入工控系统。
- 工控系统运维人员笔记本接入工控网络，把病毒带入到工控系统。
- 维护工控系统疏忽导致网线插错，造成工控网形成网络风暴，造成生产停车。
- 固定IP地址与DHCP共存造成的IP地址冲突，影响生产作业。
- 工业交换机损坏，工艺控制失效，导致生产线上的原材料报废。
- 生产网与管理网隔离失效，导致病毒几乎感染整改车间，对生产造成重大影响。
- 工艺配方数据泄露事件。

工控系统面临的威胁

- 台湾ICST在几个月时间，通过检测31厂家的67个产品，挖掘出50个可以被利用的漏洞。
- 从2007年起，每年的黑客大会都有关于工控系统安全的报告。
- 美国ICS-CERT报告，2012年工控安全事件197起，2013上半年工控安全事件206起。排在前三位的行业分别是：能源、关键制造业、交通。

数据来源： 美国ICS-CERT



工控系统标政策与标准

- 2011年9月，工信部发布《关于加强工业控制系统信息安全管理的通知》（工信部协[2011]451号）
  - **1.连接管理要求。2.组网管理要求。3.配置管理要求。4.设备选择与升级管理要求。5.数据管理要求；6.应急管理要求；7.连续性管理要求。**
- 2012年6月，国务院又发布了《关于大力推进信息化发展和切实保障信息安全的若干意见》（国发〔2012〕23号），明确提出要“保障工业控制系统安全”。
- 国际电工委员会制定IEC 62443工控安全标准。
- 美国国家标准技术研究院NIST于2010年10月发布SP800-82，2013年5月推出了第一版本，2014年第一季度将推出第二版本。
- 全国信息安全标准化技术委员会正在制定工业控制系统安全相关标准。
- 国家发改委《关于组织实施2013年国家信息安全专项有关事项的通知》中，工控安全成为四大安全专项之一，国家在政策层面给予工控安全大力的支持。

纲要

（一）工业控制系统技术上的脆弱性

- 工控系统从相对独立的环境中发展而来，在设计过程中主要考虑系统可用性，实时性问题。对工控系统的安全性，考虑不足；工控系统通信协议缺乏授权和加密、缺乏对用户身份的鉴别和认证等安全机制。
- 考虑到兼容性和连续性生产的问题，工控系统无法及时安装系统补丁，无法有效使用杀毒软件。
- 工控系统的安全防护落后于IT系统，但IT系统的安全问题却延伸到工控系统，并得以放大。

2、先天的不足，后天的无耐，导致工控系统相当脆弱！

（二）工控控制系统管理上的脆弱性

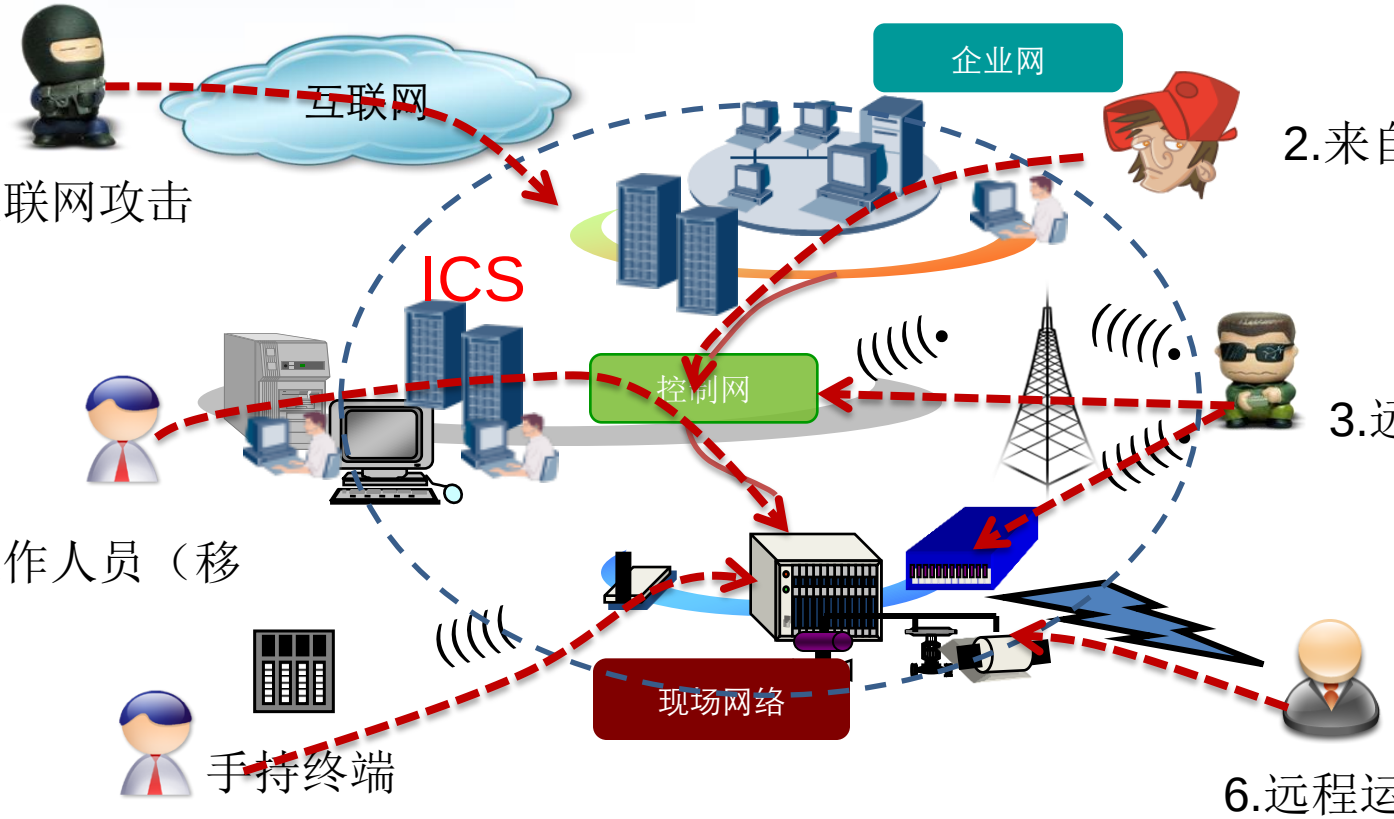
- 工业控制系统安全不仅是一个技术问题，更是一个管理问题，需要完善的工业控制系统安全政策、标准、制度和安全意识来支撑。
- 工控系统的安全管理，与IT安全管理有许多不同，易用性是工控系统安全管理考虑的第一要素。
- 相对信息系统用户来说，工控系统用户安全意识更加薄弱！

3、安全管理与安全意识不强！

工业控制系统的威胁源

威胁源			描述	威胁能力
内部威胁	员工		1.员工有意或无意的错误操作，对工控系统造成的威胁。 2.维护人员携带移动计算机或移动存储设备随意接入工控系统带来的威胁。	非常高
	厂商维护人员			非常高
外部威胁	工业间谍		通过互联网，以管理网作为跳板，入侵工控网络，从而获取工控系统中的涉密配方与工艺数据。	低
	病毒	工控病毒	针对工业控制系统的特定病毒（如震网、Duqu等），通过管理网或其他移动存储设备，进入工控网络，对工控系统进行破坏。	高
		非工控病毒	工控系统大量采用IT技术，病毒很容易被引入工控系统，从而对工控系统的正常运行造成影响。	高
	异常行为与流量		病毒、木马、软硬件故障，都可能产生异常行为或异常流量，从而对工控系统造成影响。	中
可用性	系统的可用性		工控系统由于CPU、内存、硬盘、端口流量等性能问题，造成工控系统产生故障。	中

工业控制系统风险引入的途径



1.来自互联网攻击

2.来自企业网攻击

3.远程网络劫持

4.现场操作人员（移动介质）

手持终端

5.现场运维人员

6.远程运维人员

工业控制系统风险分析（一）

- 来自IT管理网的风险
  - 工业以太网一网到底，工业协议承载在TCP/IP协议之上，导致恶意的入侵，病毒、木马感染，网络风暴扩散。
- 运维人员带来的风险
  - 远程运维带来的风险。通过Internet的运维、以及来自其他国家远程运维。
  - 本地运维带来的风险。带有病毒的移动运维设备给脆弱的工控网带来的风险、恶意运维操作带来的风险。

工业控制系统风险分析（二）

- **移动存储介质带来的风险**
  - 移动介质是生产网与管理网进行数据交换的主要方式之一。
  - 移动介质是“震网”传播的主要途径。
  - 移动介质也是病毒、木马传播的主要途径之一。
- **工业无线带来的风险**
  - 工业无线技术在给生产控制、生产监控带来了便利，但也带来了风险。
  - 802.11n Wi-Fi无线；
  - 蓝牙短距离无线通信；
  - 3G移动通信技术（CDMA2000，WCDMA，TD-SCDMA）。

纲要

I 工控系统安全背景

II 工控系统安全特点

III 工控系统安全理念

IV 工控系统安全解决方案

V 启明星辰与工控系统安全

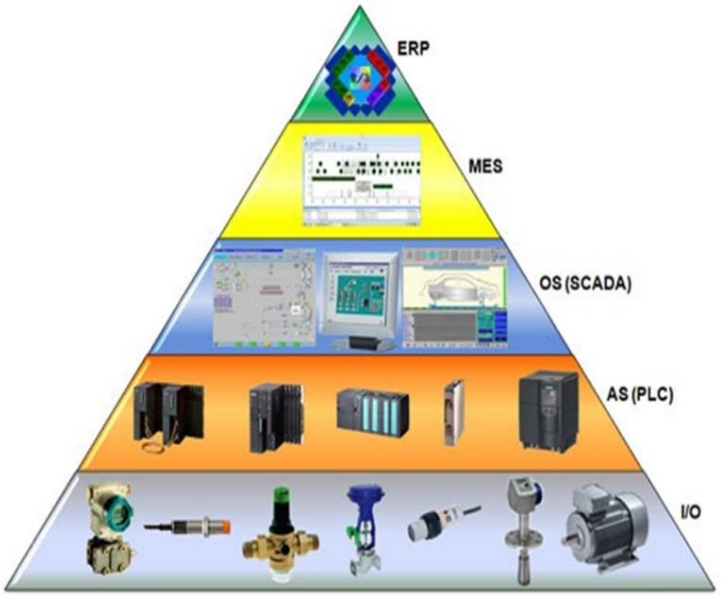
（一）工控系统安全理念-白名单化

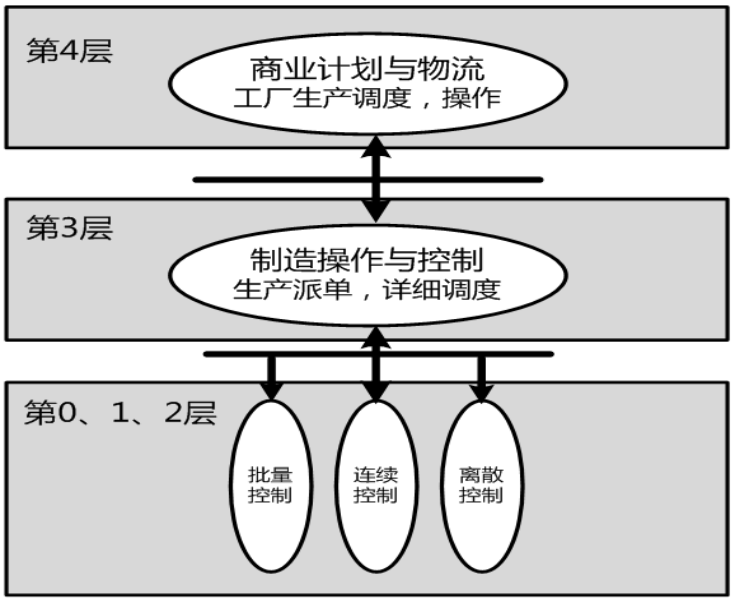
- 工控PC、服务器的进程、服务的“白名单化”
  - 操作员站、工程师站、HMI、WEB服务器、数据库服务器；
- 工控系统访问控制列表“白名单化”
  - IT防火墙、工业交换机、工业防火墙等；
- 工控系统资产“白名单化”
  - 能够实时识别非法设备进入工控系统。

实现工控系统的可信，网络的可信！

（二）工控系统安全理念-层次化

- “层次化”
  - 针对工业控制系统的特点，我们提出了“**三层架构，二层防护**”的方案。在实现的过程中进一步细化为“**分层、分域、分等级**”。





（三）工控系统安全理念-边缘化

“边缘化”

- 从工控系统演变过程可以看到，工控系统最初是独立的自动控制系统，但随着信息化的发展，以及智能控制的要求，不断的引入IT技术、互联网技术，从而使工控系统不再独立。
- 工控系统安全，需要加强工控系统周边信息化系统的安全。例如：SCADA、MES、ERP安全。

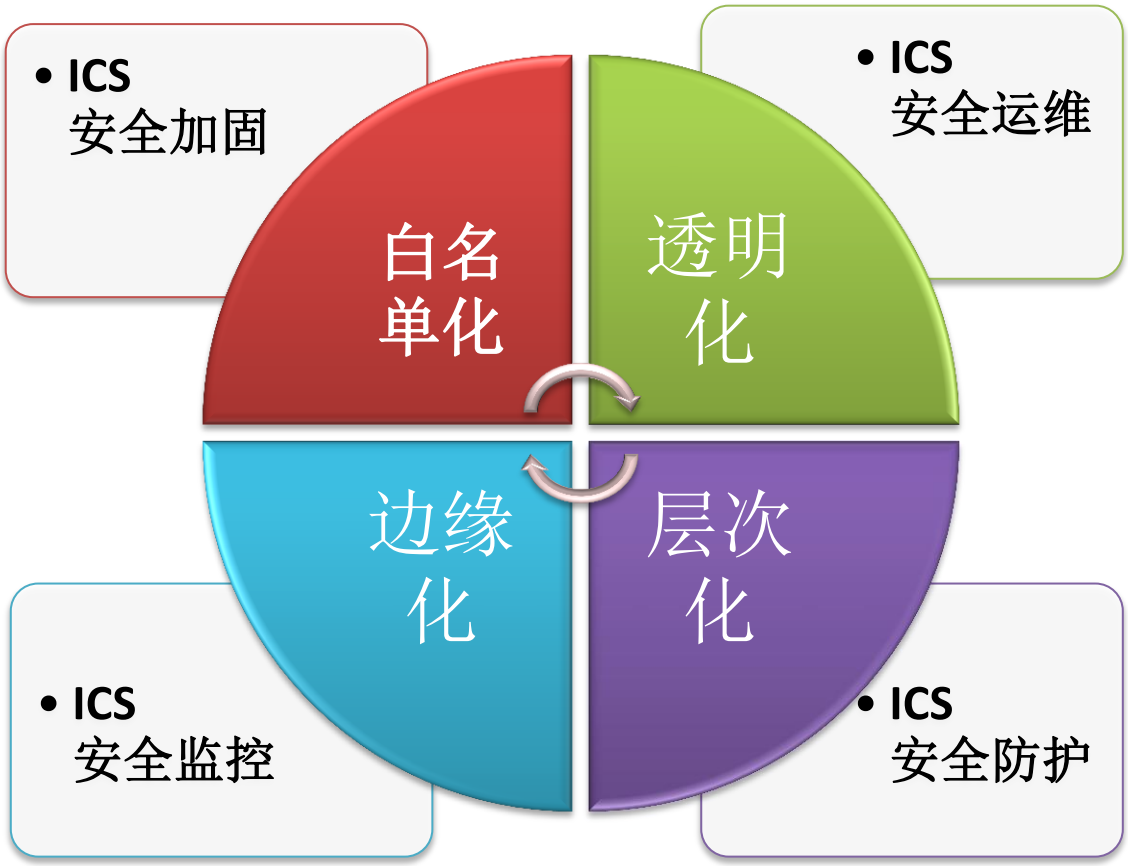
（四）工控系统安全理念-透明化

- “透明化”
  - 工控系统安全采取的技术措施、管理措施，不能够降低系统使用者的易用性，安全措施对使用者来说是透明的。
  - 工控系统安全解决方案，不能够降低系统的可用性、尽可能避免系统的延时（如果有延时，必须在可接受的范围之内）。

纲要

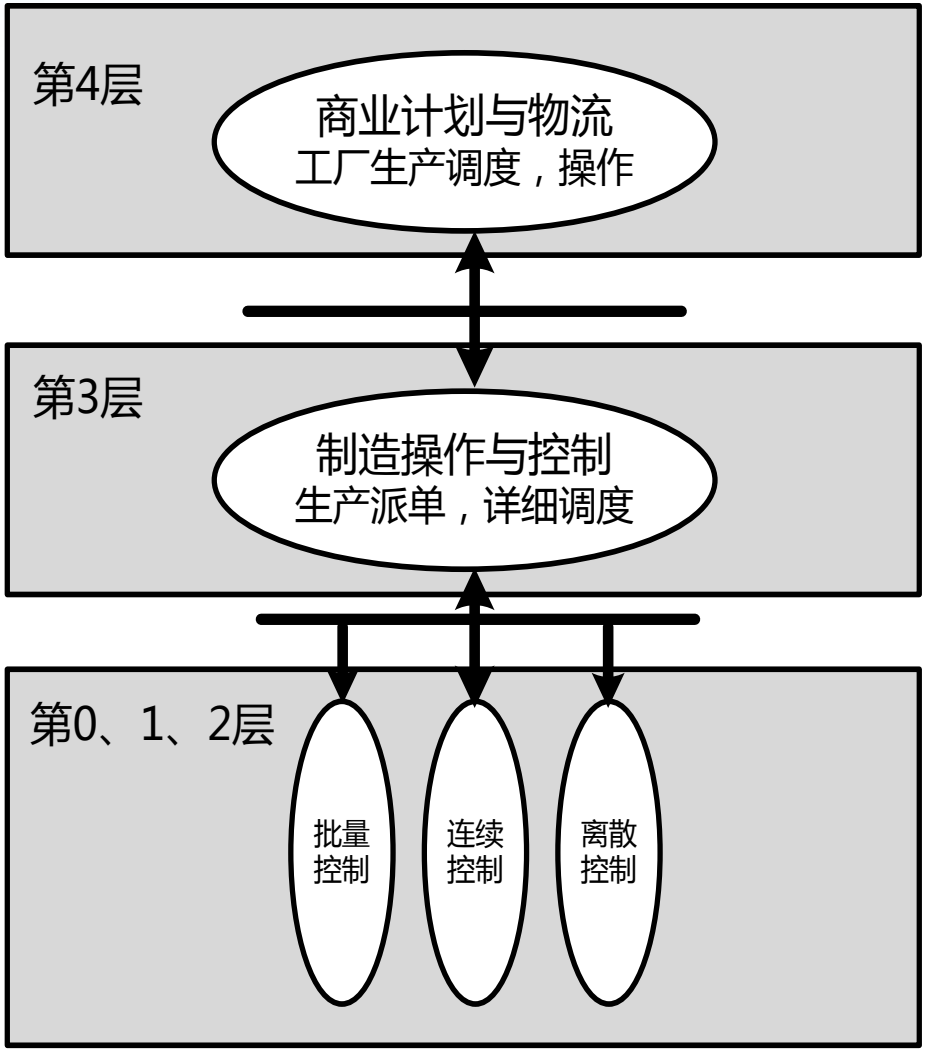
工控系统安全解决方案思路

- 基于工控系统安全防护理念，从四个维度，解决工控系统安全问题。



工控系统安全防护（一）

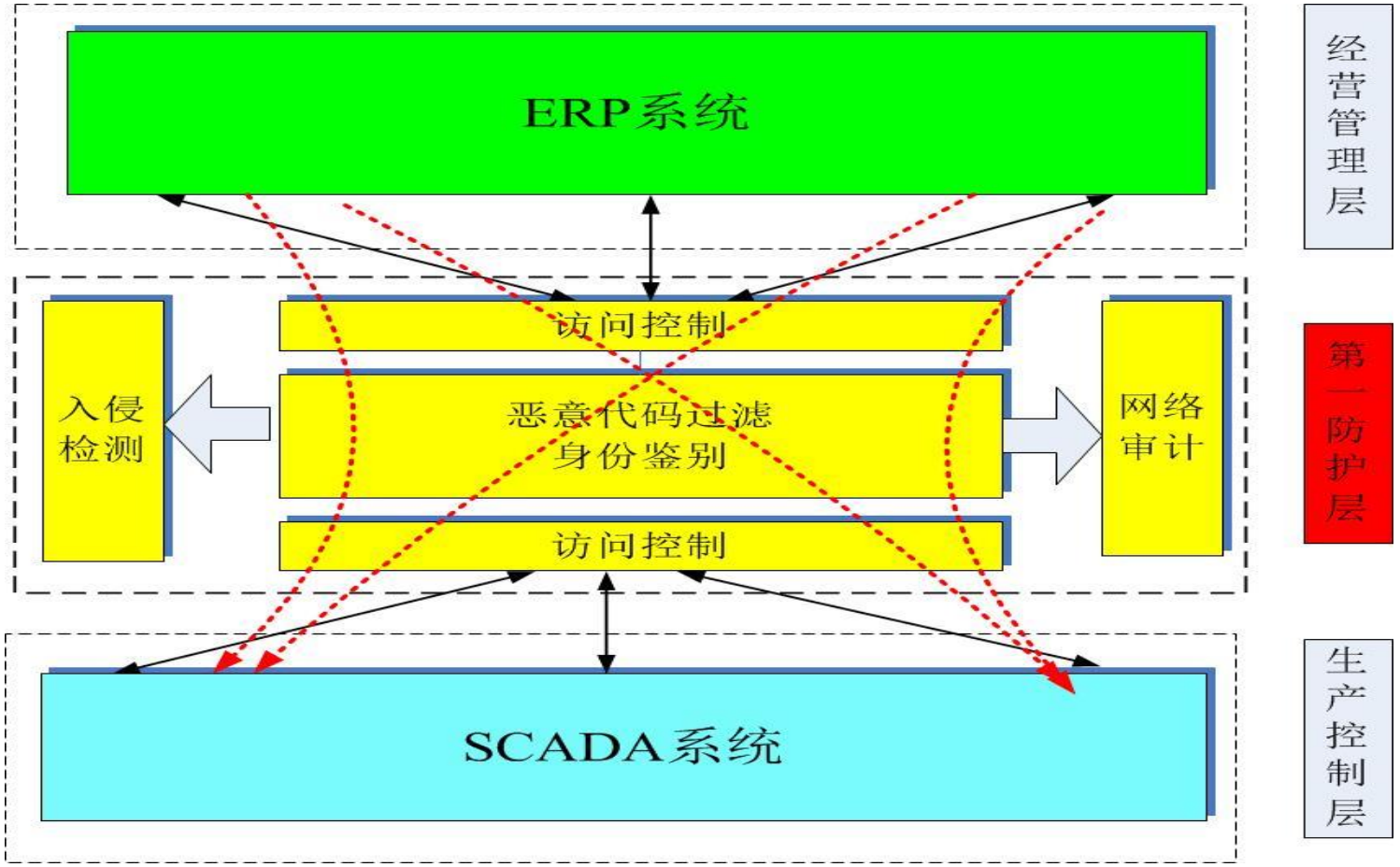
- 纵向分层：三层架构，二层防护。经营管理层、生产控制层、过程控制层。
- 横向分域：不同的车间、不同的生产线进行逻辑隔离。
- 分层分域的目的就是进行安全隔离防护。



GB/T20720-1

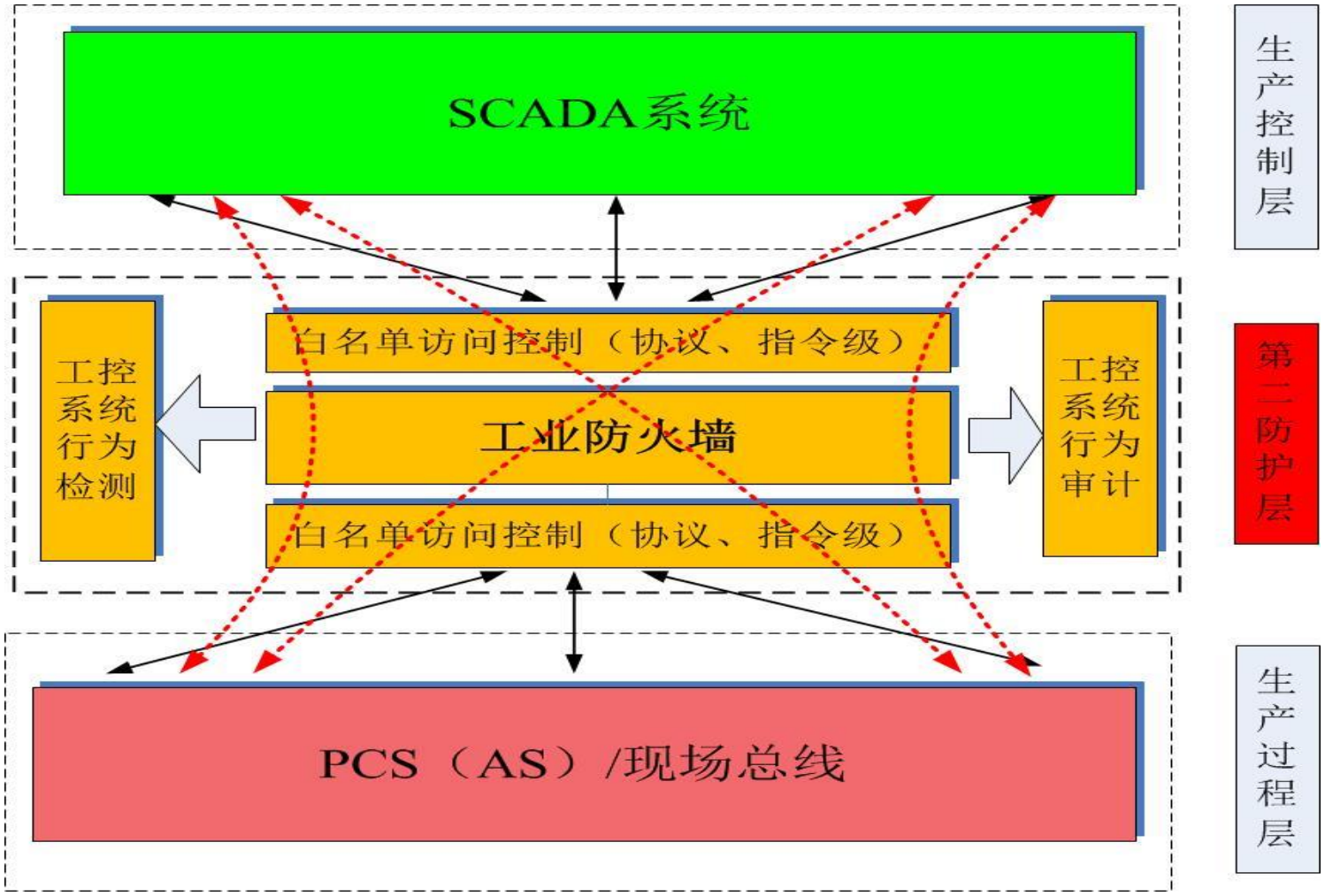
（一）工控系统安全防护-1

- 经营管理层与生产控制层之间的防护



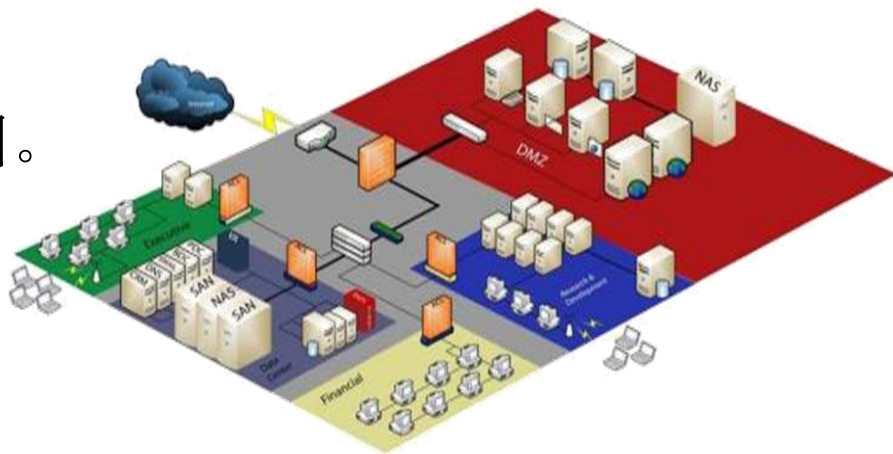
（一）工控系统安全防护-2

- 生产控制层与生产过程层之间的防护



（二）工控系统安全加固

- **经营管理层-系统安全加固**
  - 对ERP、MIS等与生产控制层交互的终端、服务器以及交换设备进行安全加固。
- **生产控制层-系统安全加固**
  - 对SCADA、MES系统中工控计算机（IPC）、服务器进行白名单式安全加固，同时对工业交换机进行加固。
- **生产过程层-系统安全加固**
  - 对PLC、RTU等进行安全加固。



（三）工控系统安全监控-1

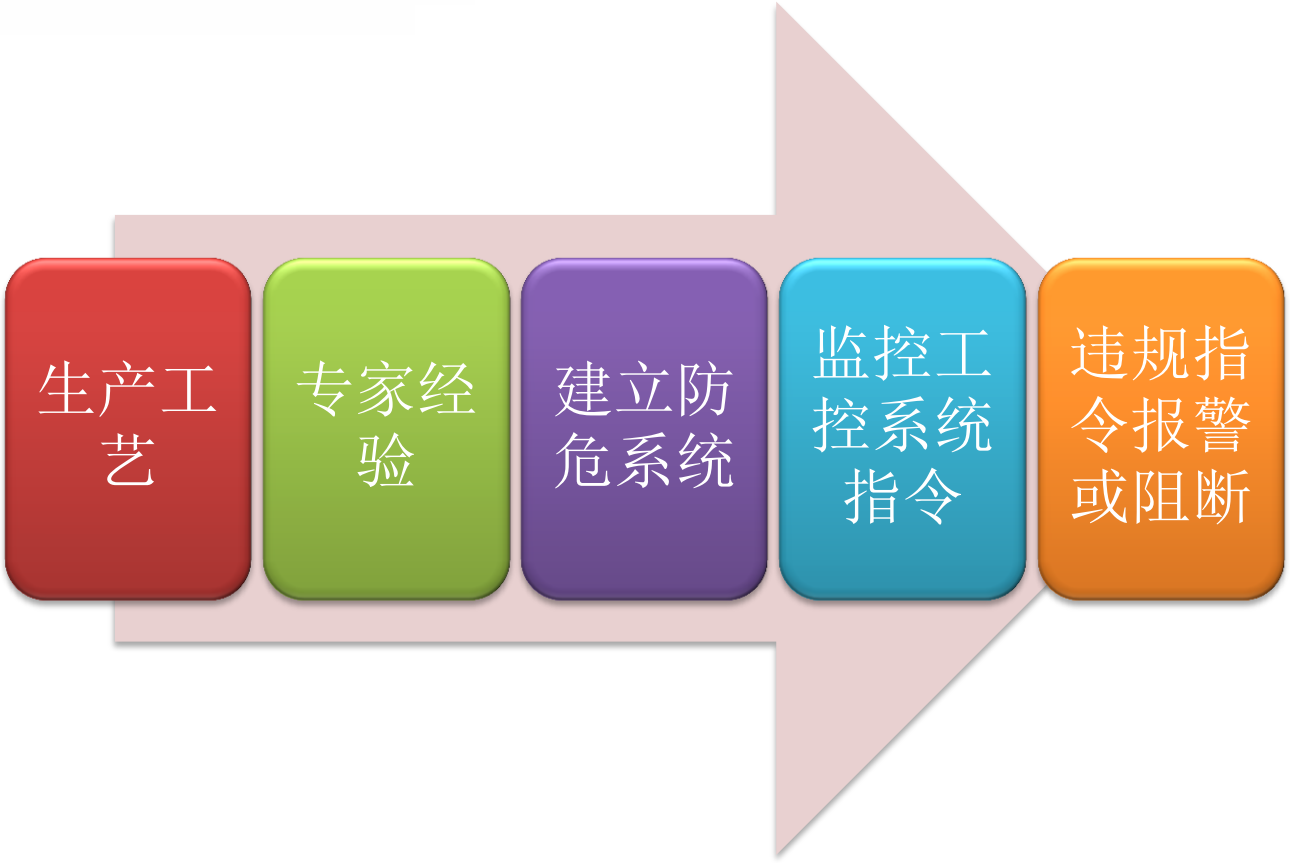
- 工控系统的可用性监控

（三）工控系统安全监控-2

- 工控系统网络行为监控

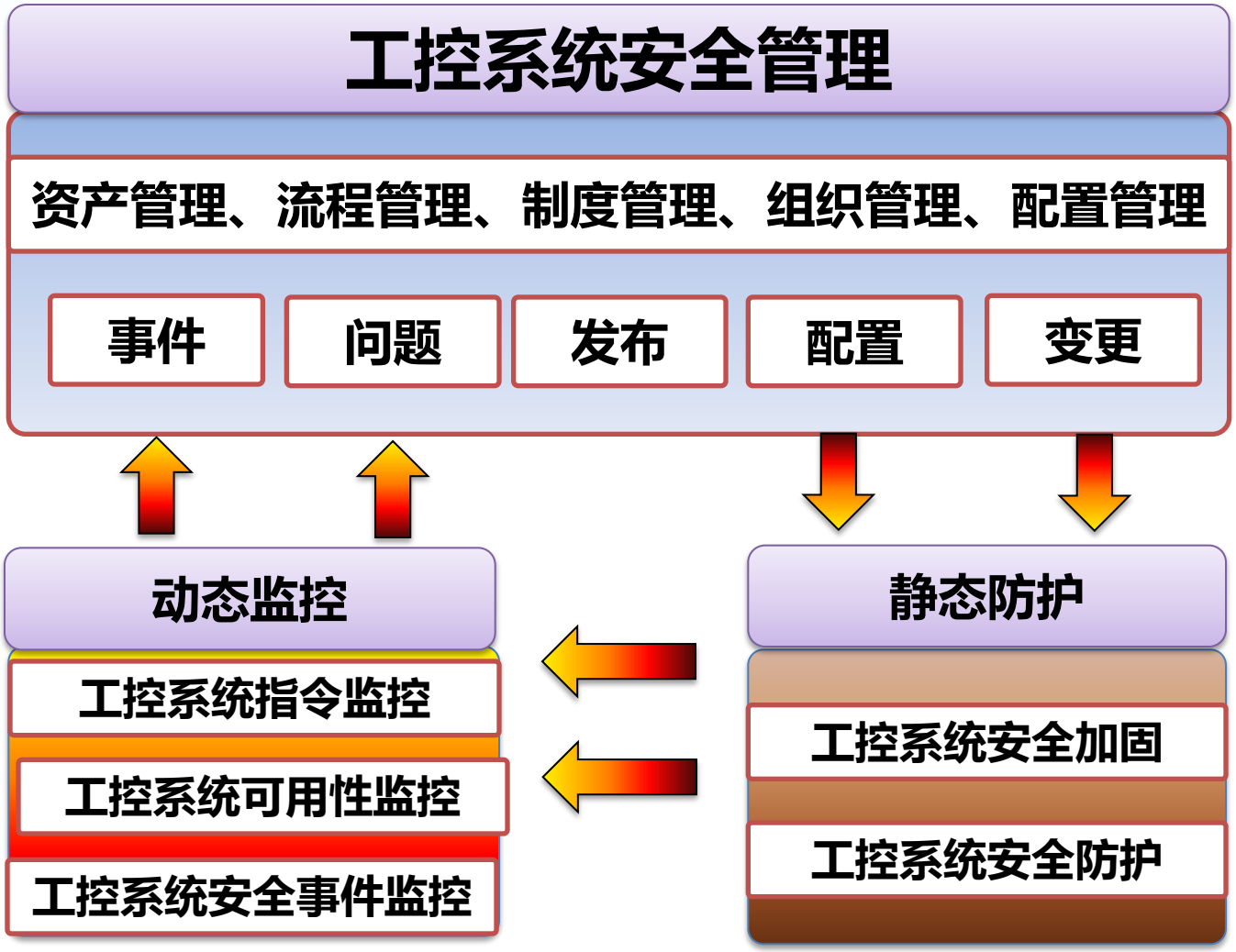
（三）工控系统安全监控-3

- 工控系统指令监控

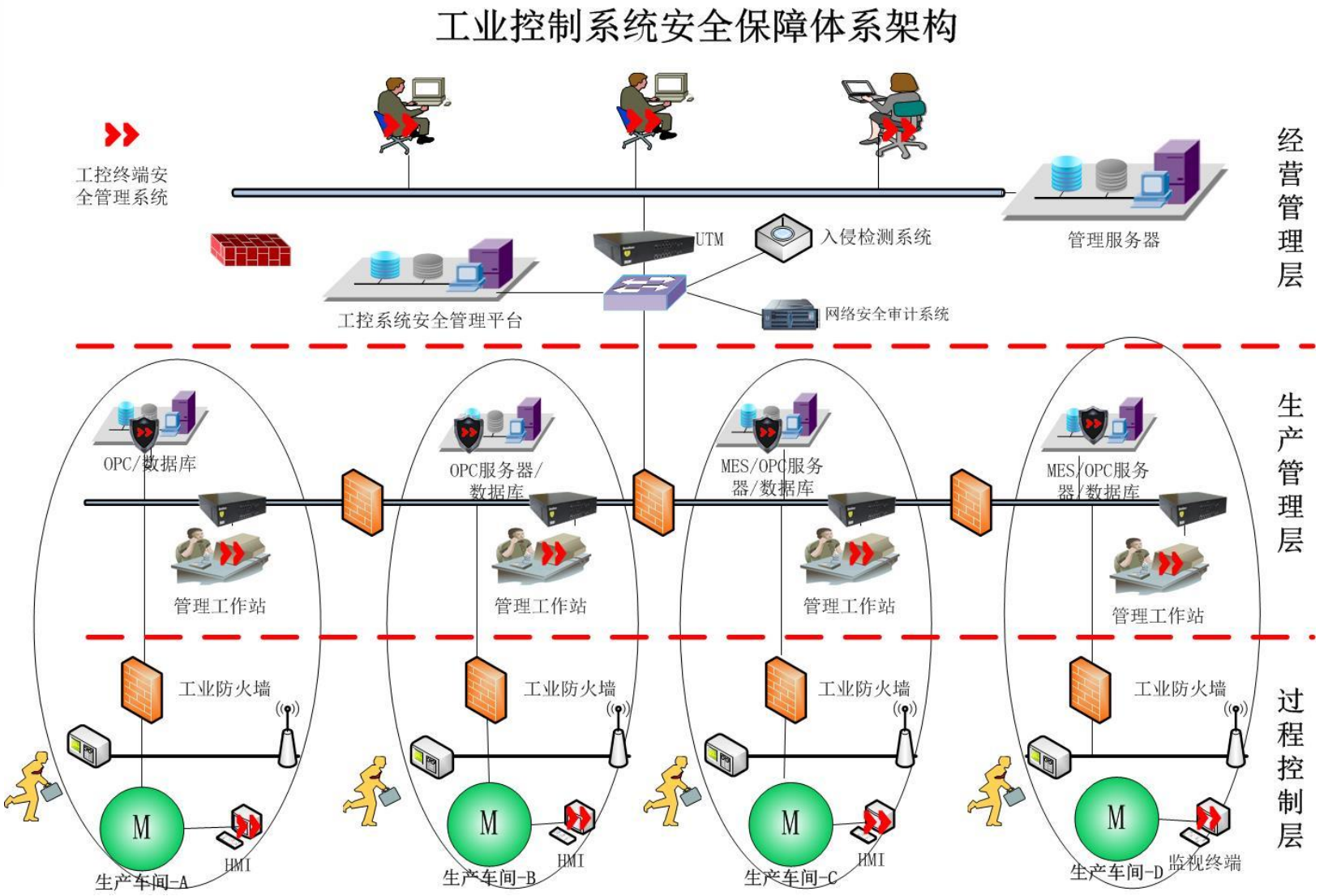


（四）工控系统安全运维管理

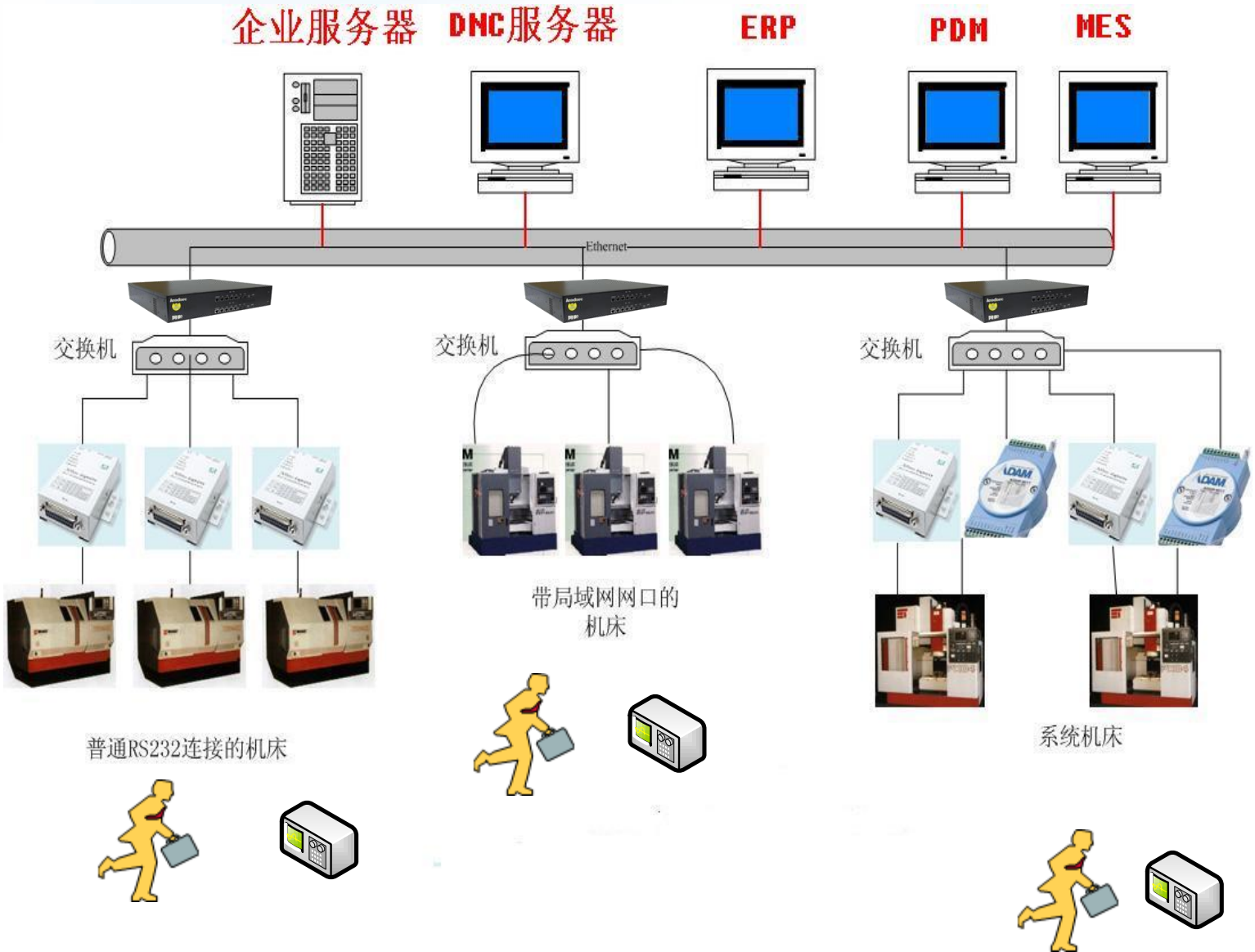
- 工控系统安全运维管理



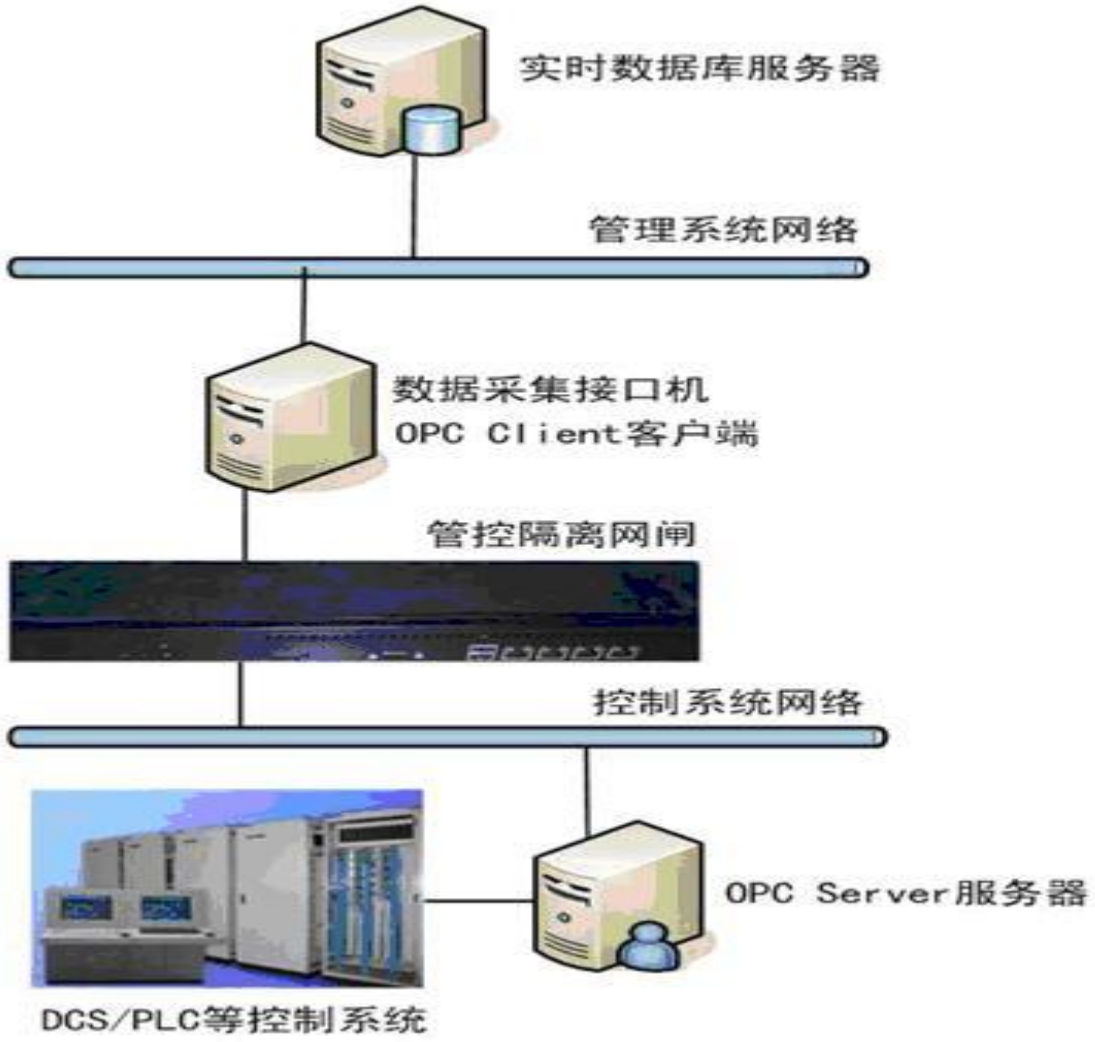
工控系统安全解决方案整体框架



数控机床DNC联网安全



石油石化数据采集安全


实时数据库服务器
管理系统网络
数据采集接口机
OPC Client客户端
管控隔离网闸
控制系统网络
OPC Server服务器
DCS/PLC等控制系统

工业控制系统安全隔离网闸

- **GAP-6600BD**
  - 内外接口最大支持4个电口和1个光口（万兆）。
  - 标准2U机箱，双冗余电源；设备健康监控声光报警装置。
  - 支持OPC协议。

工业控制系统防火墙

产品硬件形态

- 2网口、2-4现场总线接口、可选bypass、无风扇
- 导轨式、适应环境温度-40-75。

产品功能

- 实现工控网络的逻辑隔离
- 只允许工业协议指令通过
- 隔绝病毒和任何非法指令与流量
- 对进出流量进行限制，防止广播风暴的影响
- 防止对组态文件的非法修改
- 具备数字量输入输出功能，可与PLC交互
- 选用逻辑隔离的主要原因后续维护比较简单

解决方案给予用户的收益

- 工控机（IPC）操作系统的加固（进程、服务白名单）
- 工控机（IPC）外设管理，如USB接口，光驱，网卡，串口。
- 工控机（IPC）强口令认证。
- 工控系统与管理系统的安全隔离控制。
- 工控系统的无线安全接入。
- 工控系统远程安全接入。
- 工控系统的设备准入控制。
- 工控系统的可用性、异常事件以及流量监控、。
- 工控系统病毒的查杀。

纲要

关于启明星辰公司

- 启明星辰公司由留美博士严望佳女士创建于1996年；
- 2010年6月23日，启明星辰在深交所挂牌上市；
- 启明星辰是国内最具实力的安全产品、安全管理平台、安全服务和解决方案的提供商；
- 启明星辰位于中关村软件园启明星辰大厦，占地40 余亩
- 启明星辰在全国各地拥有三十多个分公司、子公司和办事处。

启明星辰的荣誉

2000年1月24日，江泽民、李岚清、曾庆红等党和国家领导人亲切视察启明星辰公司

2003年1月24日，胡锦涛总书记亲切接见启明星辰公司CEO严望佳博士

启明星辰工控安全动态

- 2013年3月，启明星辰被中国工业软件产业发展联盟聘为理事单位，成为联盟中唯一的安全厂商。


聘　书

LETTER OF APPOINTMENT

兹聘任　北京启明星辰信息安全技术有限公司

为中国工业软件产业发展联盟

理事　单位，聘期1年。

CISPA 中国工业软件产业发展联盟

2013年3月

工控安全产业联盟理事会成员

- 2014成为工业控制系统信息安全产业联盟理事会成员。
- 公司参与安全标准委员会组织的《工业控制系统安全管理标准》起草工作。

ICSISIA 工业控制系统信息安全产业联盟
Industrial Control Systems Information Security Industry Alliance

加强合作，携手共进

- 工业信息化提高了工业系统生产效率，实现了集约化生产和精细化管理；但带来的工控系统安全问题，涉及到国计民生和生命财产。“震网”病毒为工控系统安全敲响了警钟，工控安全已经引起了国家、重要行业的重视。
- 启明星辰作为国内最大的信息系统安全厂商，愿意和各行业、相关厂商加强合作，携手共进，为国家的工业控制系统安全做出自己的贡献。

欢迎大家交流探讨！

启明星辰 Venus
www.venustech.com.cn
信息安全 领航