股票代码：002439

启明星辰

# 工控系统安全理念及解决方案

启明星辰—张晔

领航 信息安全

# 纲要

# （一）工控系统的演进

- 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服务器、工控PC、操作系统、数据库系统、以太网、TCP/IP协议等；
- 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。

1、工控系统的安全问题是77系统安全问题的延伸与放大！

# （二）工控系统的脆弱性

- 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。

**2、先天的不足，后天的无耐，导致工控系统相当脆弱！**

# （三）工控系统安全管理的不足

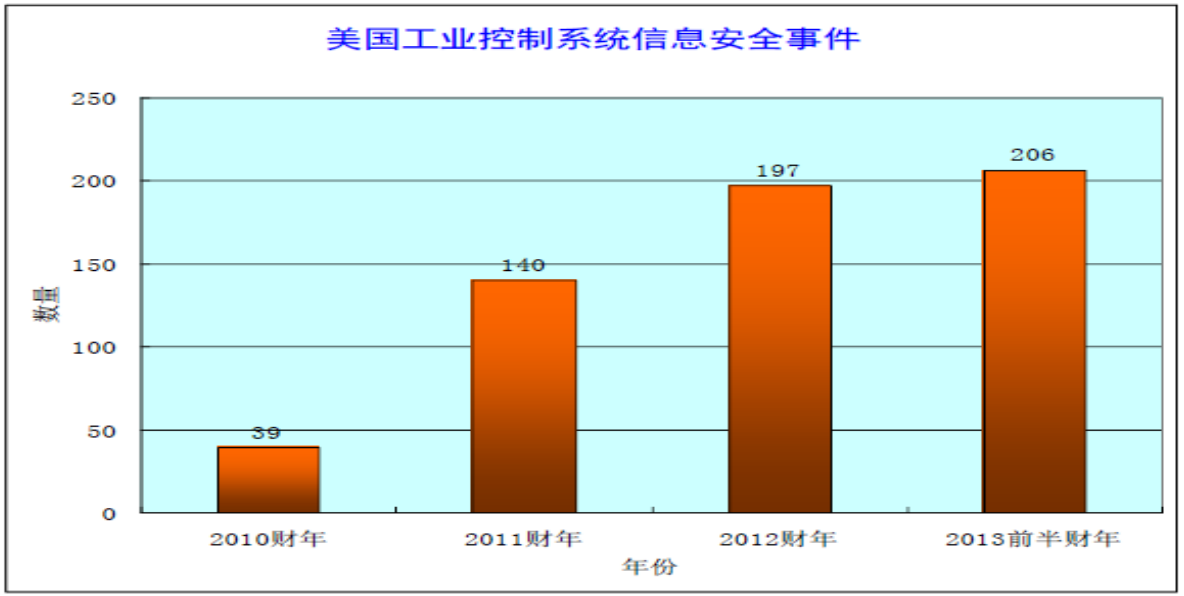
- 工业控制系统安全不仅是一个技术问题，更是一个管理问题，需要完善的工业控制系统安全政策、标准、制度和安全意识来支撑。
- 工控系统的安全管理，与IT安全管理有许多不同，易用性是工控系统安全管理考虑的第一要素。
- 相对信息系统用户来说，工控系统用户安全意识更加薄弱！

3、安全管理与安全意识不强！

# （四）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



# （五）工控系统标政策与标准

- 2011年9月，（工信部协〔2011〕451号）
- 2012年6月，（国发〔2012〕23号）
- 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

# 工控系统的特点（一）

- 可用性，实时性对工控系统尤其重要。
- 工控系统存在两种不同类型的协议，即TCP/IP协议和工控通信协议；
- 工控系统持续运行周期长，工控系统上线生产以后，很长周期内不会进行调整。
- 很多工控系统安全管理上隶属于生产单位，但工控系统安全管理和IT安全管理有很大的不同。

# 工控系统的特点（二）

- 工控系统要求封闭性比较强。
- 工控系统中承载着一些需要保密的工艺数据。
- 工控系统是国家重要的基础设施，工控系统安全会影响到生命安全、重大财产损失以及产生环境问题。
- 加强工控系统的物理安全，会达到事半功倍的效果
- 无线安全问题会成为工控系统安全的热点问题。

# 纲要

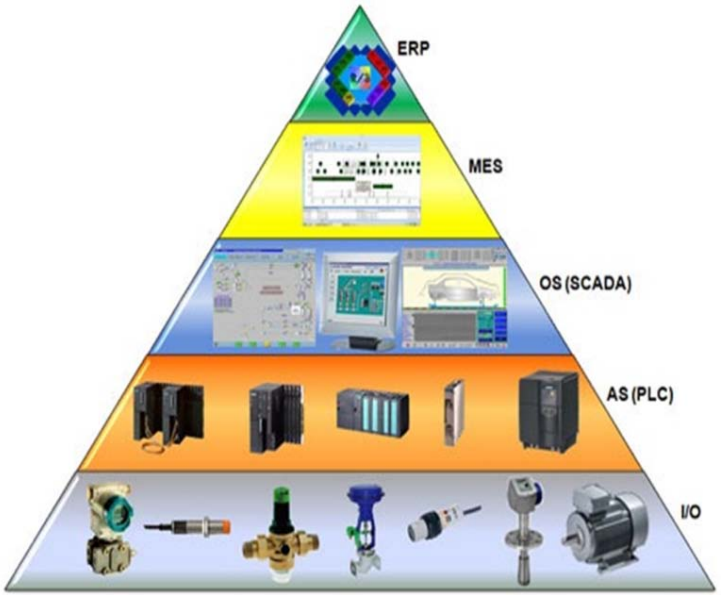
# （一）工控系统安全理念-白名单化

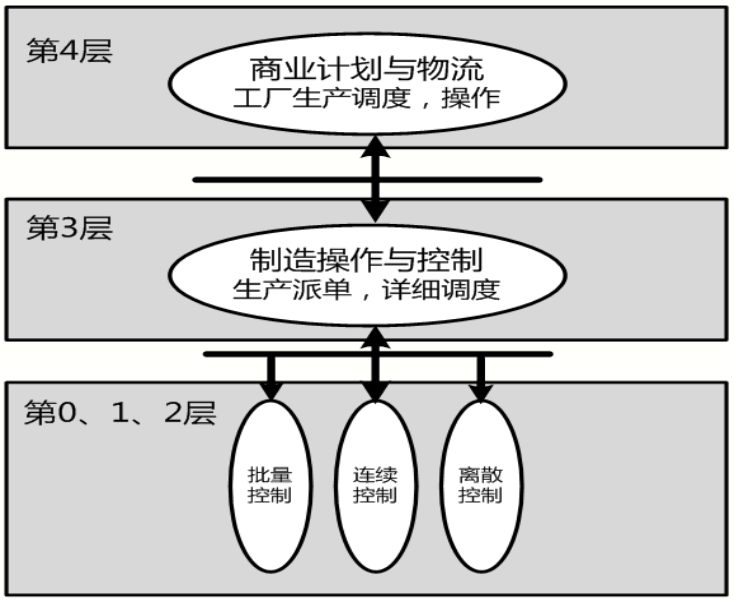
- 工控PC、服务器的进程、服务的“白名单化”
  - 操作员站、工程师站、HMI、WEB服务器、数据库服务器；
- 工控系统访问控制列表“白名单化”
  - IT防火墙、工业交换机、工业防火墙等；
- 工控系统资产“白名单化”
  - 能够实时识别非法设备进入工控系统。

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”
  - 根据工控系统功能的不同，对工控系统进行纵向分层、横向分域，域分等级，目的是进行安全隔离防护。
  - 针对工控系统的特点，我们提出了“三层架构，二层发防护”的方案。



# （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。

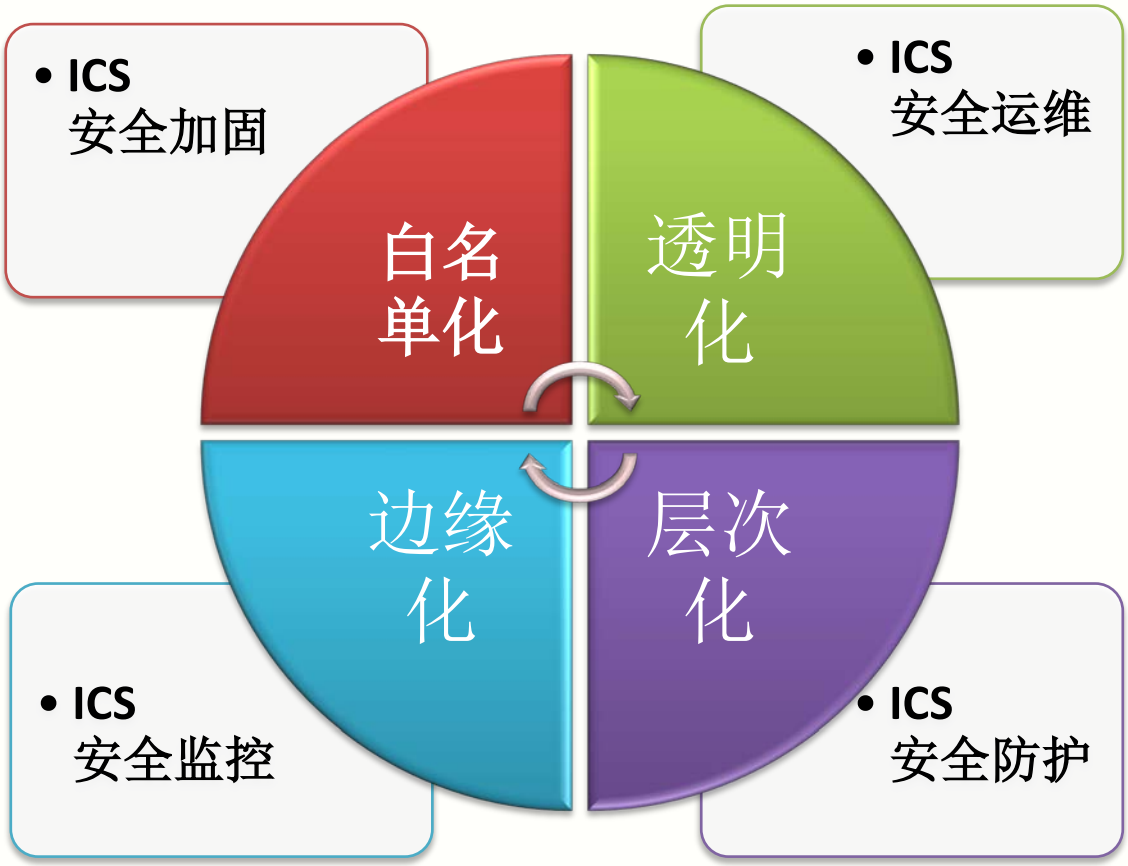
# （四）工控系统安全理念-透明化

- “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

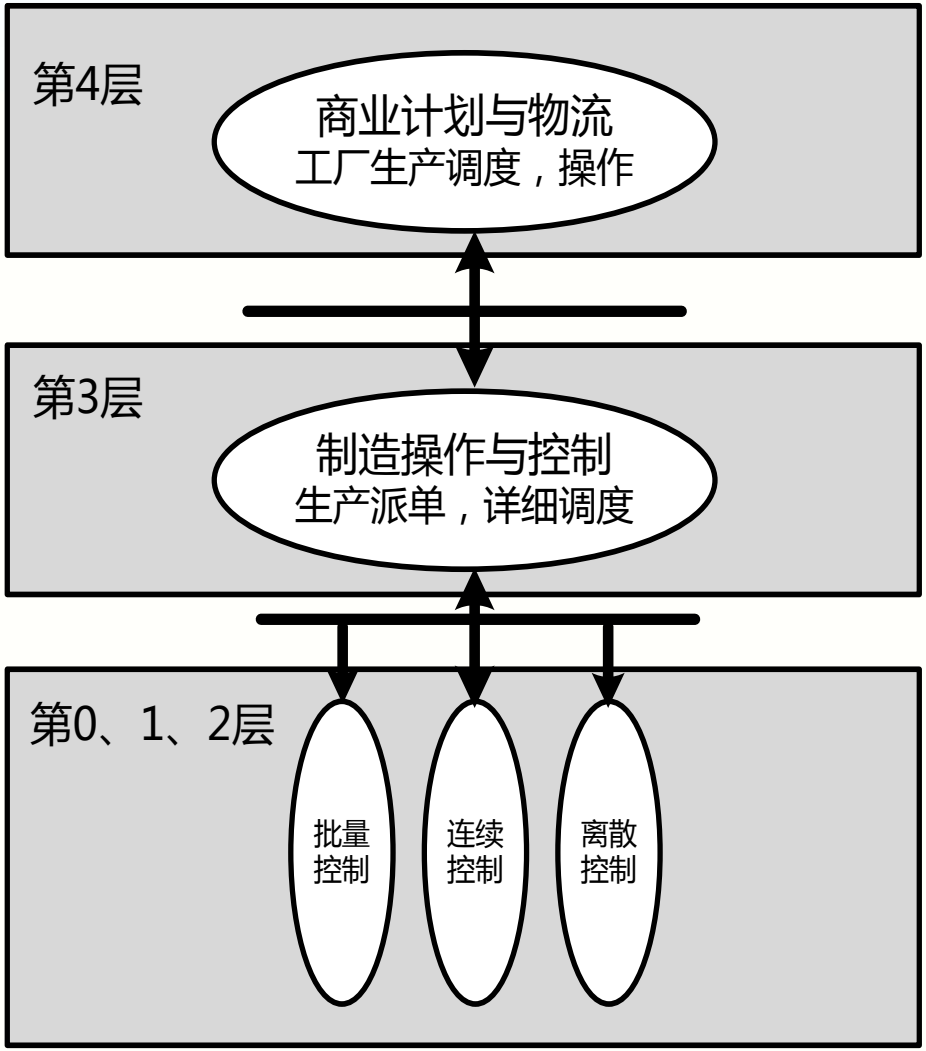
# 工控系统安全解决方案思路

- 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）

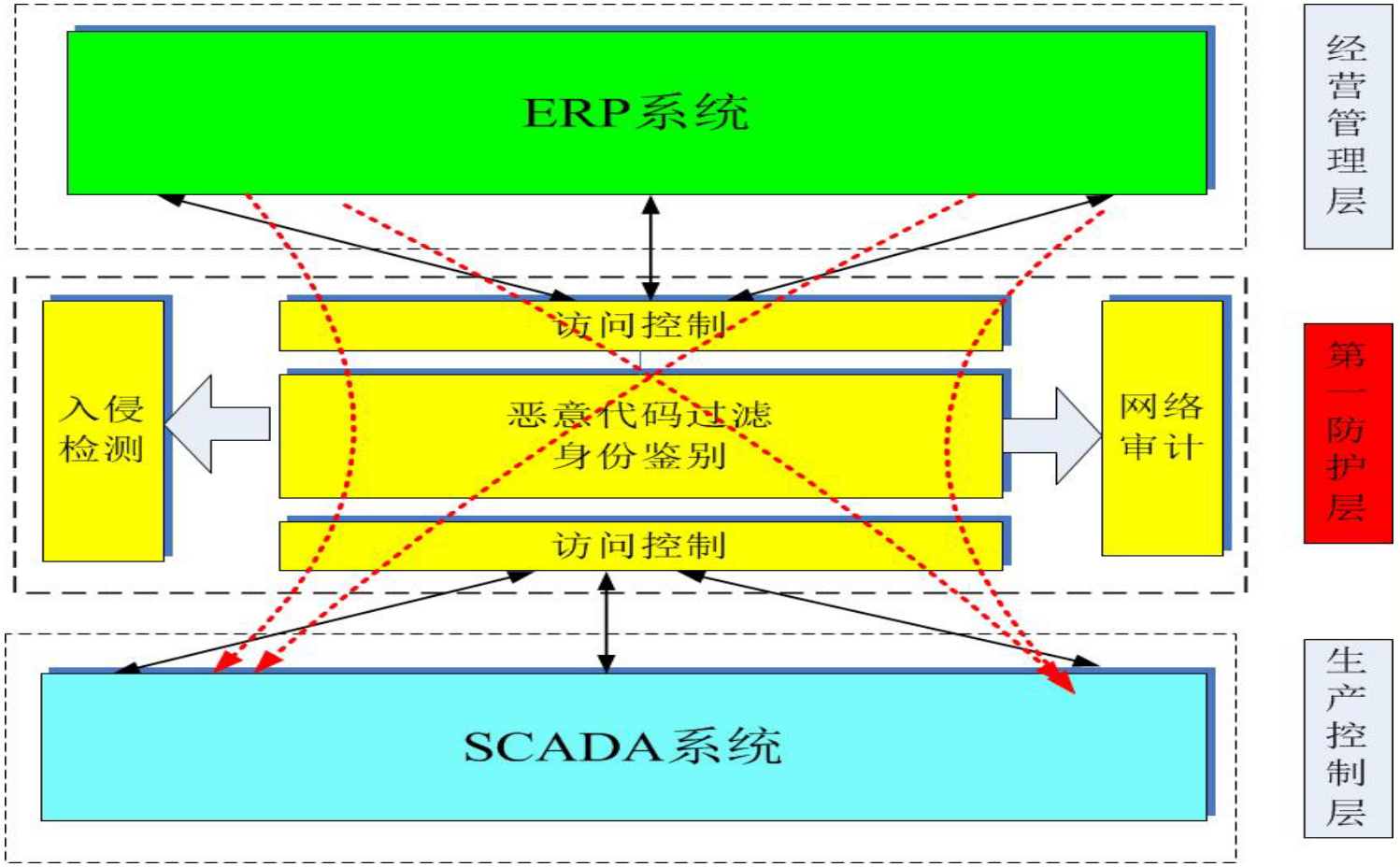
- 纵向分层：三层架构，二层防护。经营管理层、生产控制层、过程控制层。
- 横向分域：不同的车间、不同的生产线进行逻辑隔离。
- 分层分域的目的就是进行安全隔离防护。




GB/T20720-1

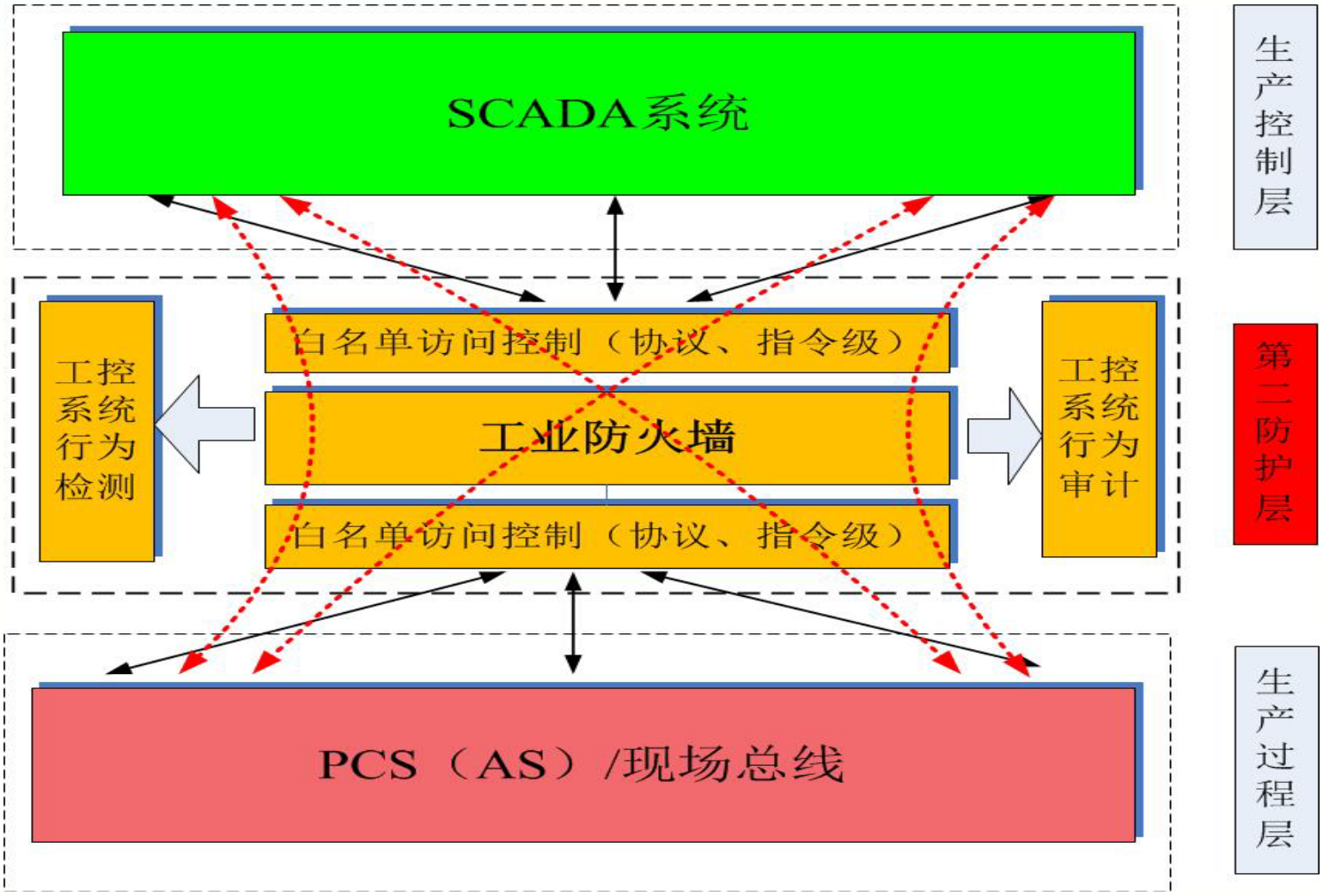
# （一）工控系统安全防护-1

- 经营管理层与生产控制层之间的防护



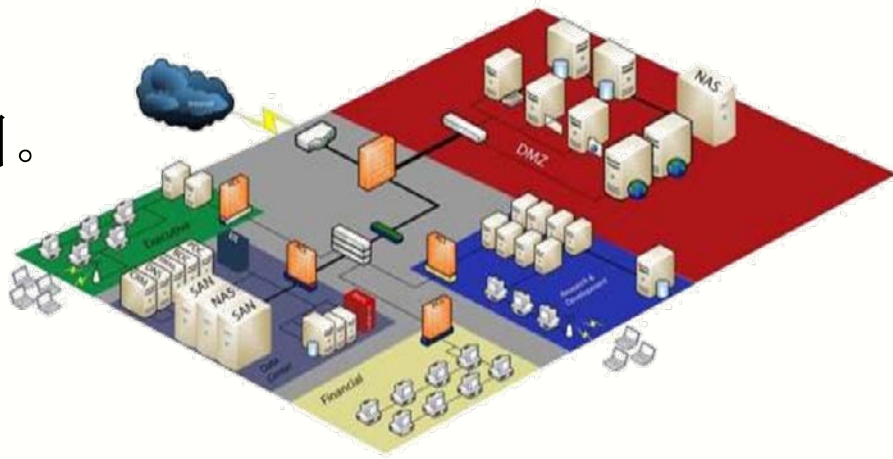
# （一）工控系统安全防护-2

- 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。

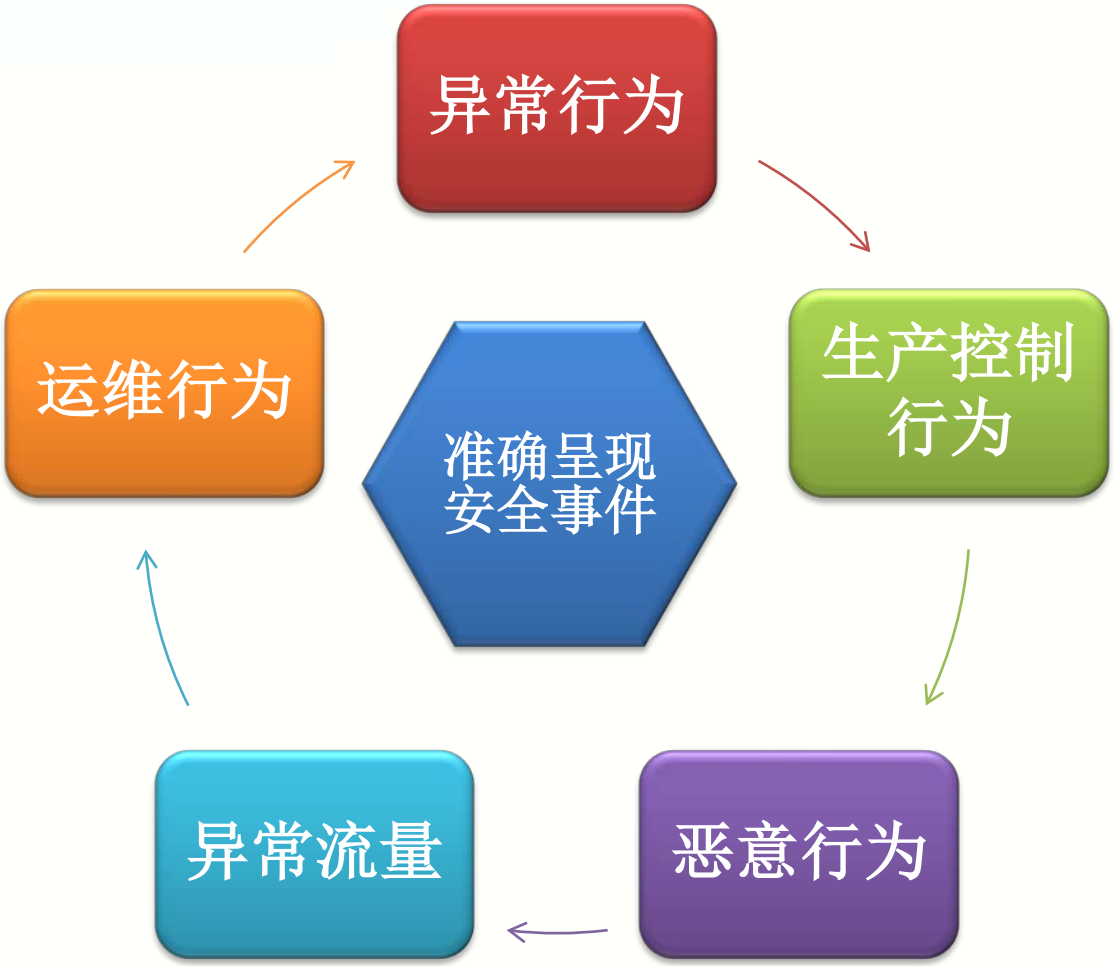


# （三）工控系统安全监控-1

- 工控系统的可用性监控

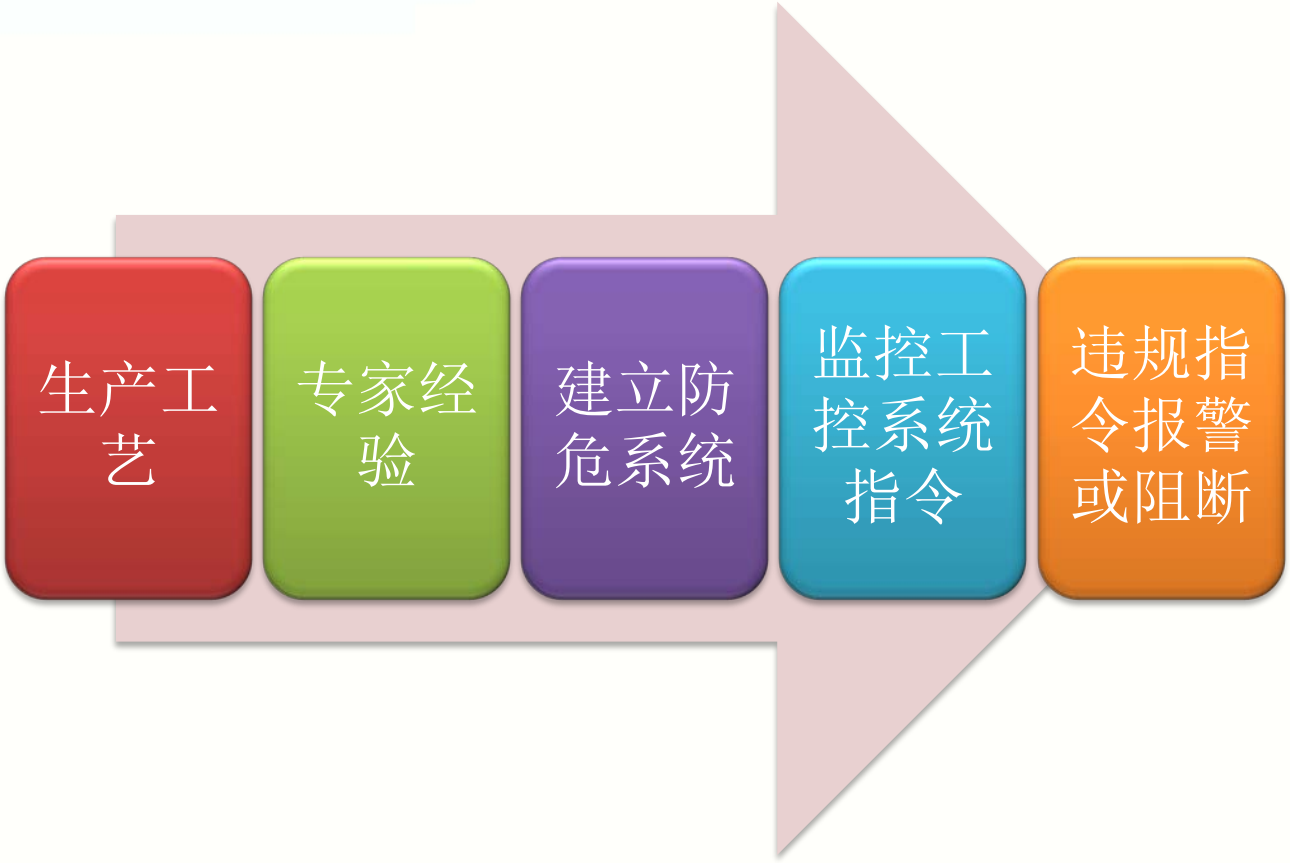
# （三）工控系统安全监控-2

- 工控系统网络行为监控



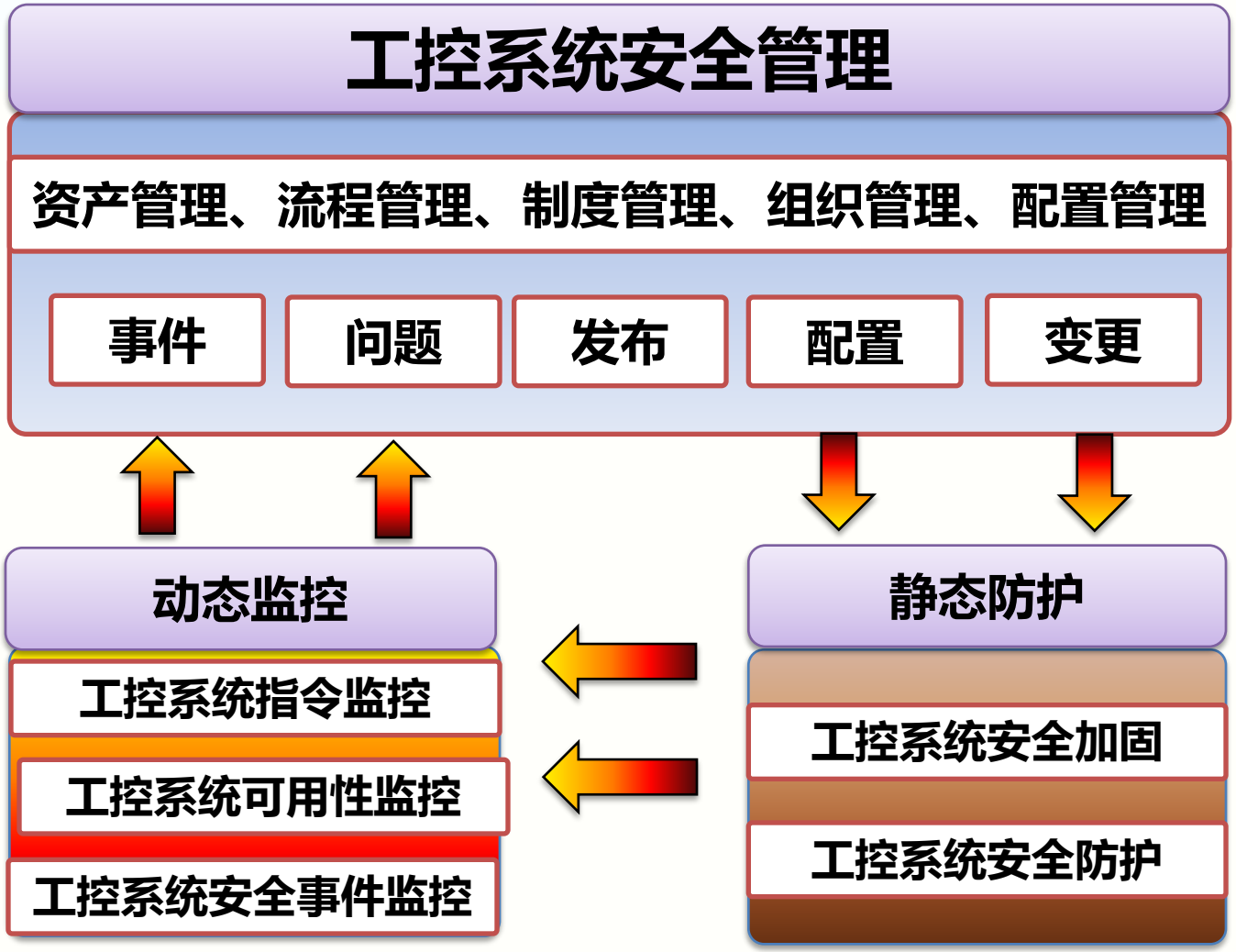
# （三）工控系统安全监控-3

- 工控系统指令监控

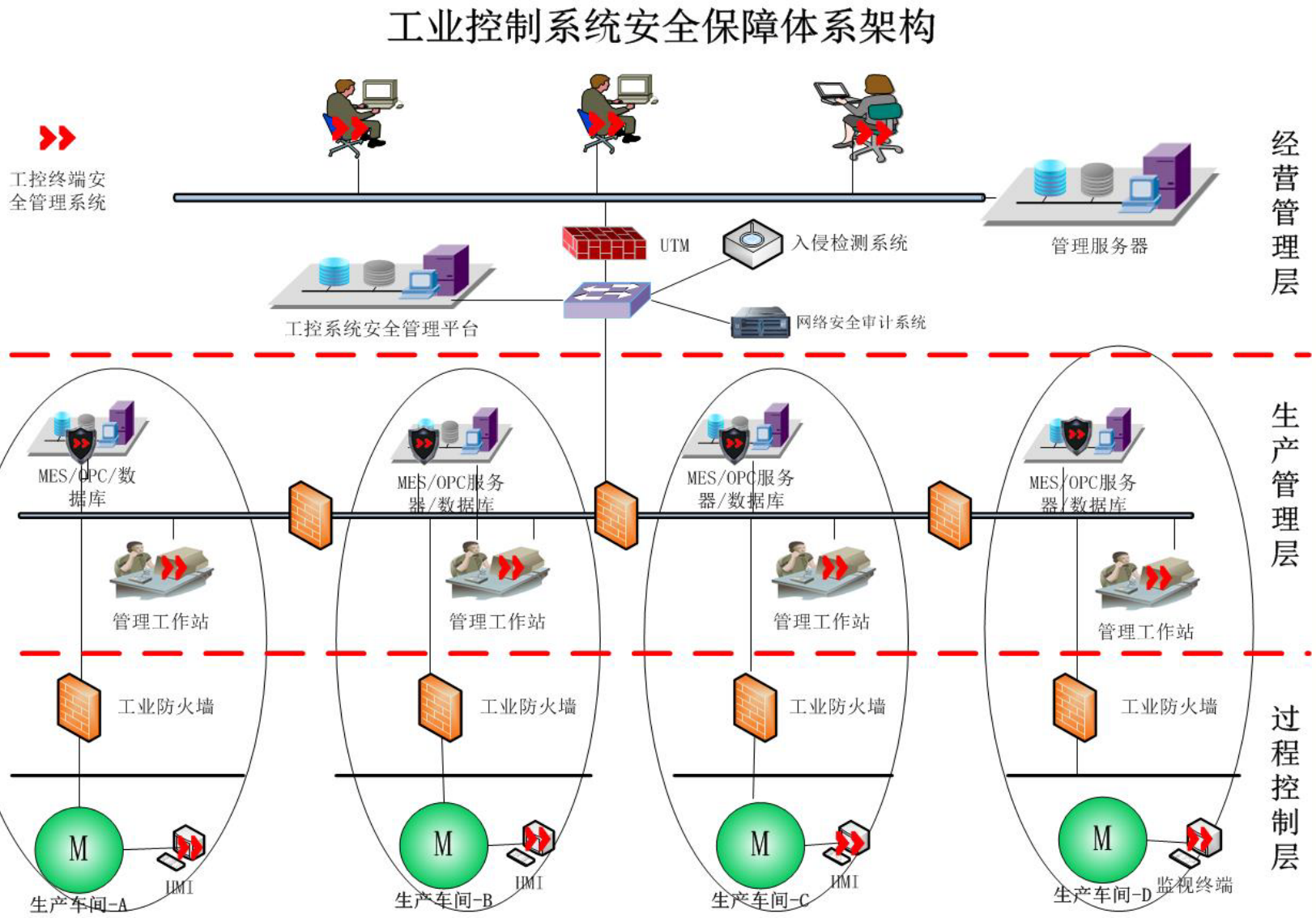


# （四）工控系统安全运维管理

- 工控系统安全运维管理



# 工控系统安全解决方案整体框架



# 解决方案解决的主要问题

- 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

# 加强合作，携手共进

- 工业信息化提高了工业系统生产效率，实现了生产的精细化控制；
- 工业控制系统安全涉及到环境灾难、生命财产的问题，目前已经引起了国家、各行业、各相关厂商的重视。
- 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 www.venustech.com.cn Venus 领航 信息安全