工业控制系统三层网络的信息安全检测与认证

顾健　沈清泓
公安部第三研究所
公安部信息系统安全产品质量监督检验中心

工控信息安全方面国家政策：

- 《关于加强工业与控制系统信息安全管理的通知》工信部协[2011]451号
  - 切实加强工业控制系统信息安全管理，以保障工业生产运行安全、国家经济安全和人民生命财产安全
  - 点明了我国工业控制领域信息安全工作的问题和不足
  - 明确重点领域工业控制系统信息安全管理要求
  - 建立工业控制系统安全测评检查和漏洞发布制度

工控信息安全方面国家政策：

- 《国家发展改革委办公厅关于组织实施2012年国家信息安全专项有关事项的通知》（发改办高技[2012]2091号）
  - 适用于工业控制系统的防火墙
  - 面向工业控制系统的异常行为审计产品
  - 工业控制网络安全管控平台
  - 工控信息安全专业化服务

工控信息安全方面国家政策：

- 《国家发展改革委办公厅关于组织实施2013年国家信息安全专项有关事项的通知》（发改办高技[2013]1965号）
  - 面向现场设备环境的边界安全专用网关产品
  - 面向集散控制系统（DCS）的异常监测产品
  - 面向工业控制信息安全领域的可控试点示范

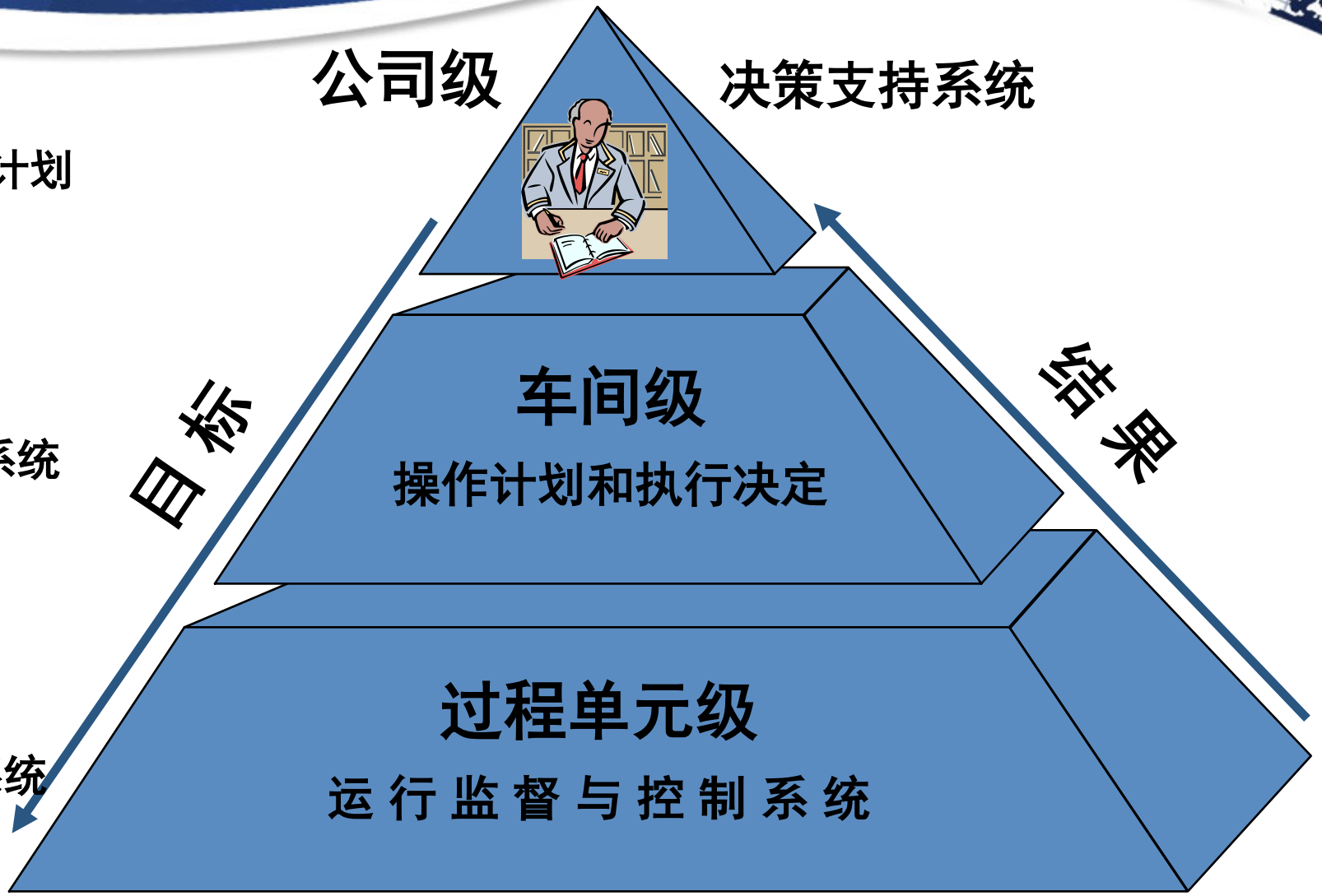
工业控制系统：

- 由各种**自动化控制组件**以及对实时数据进行采集、监测的**过程控制组件**，共同构成的确保工业基础设施自动化运行、过程控制与监控的**业务流程管控系统**
- 核心组件：
  - SCADA
  - PCS
  - DCS
  - PLC
  - RTU
  - IED
  - 通信接口

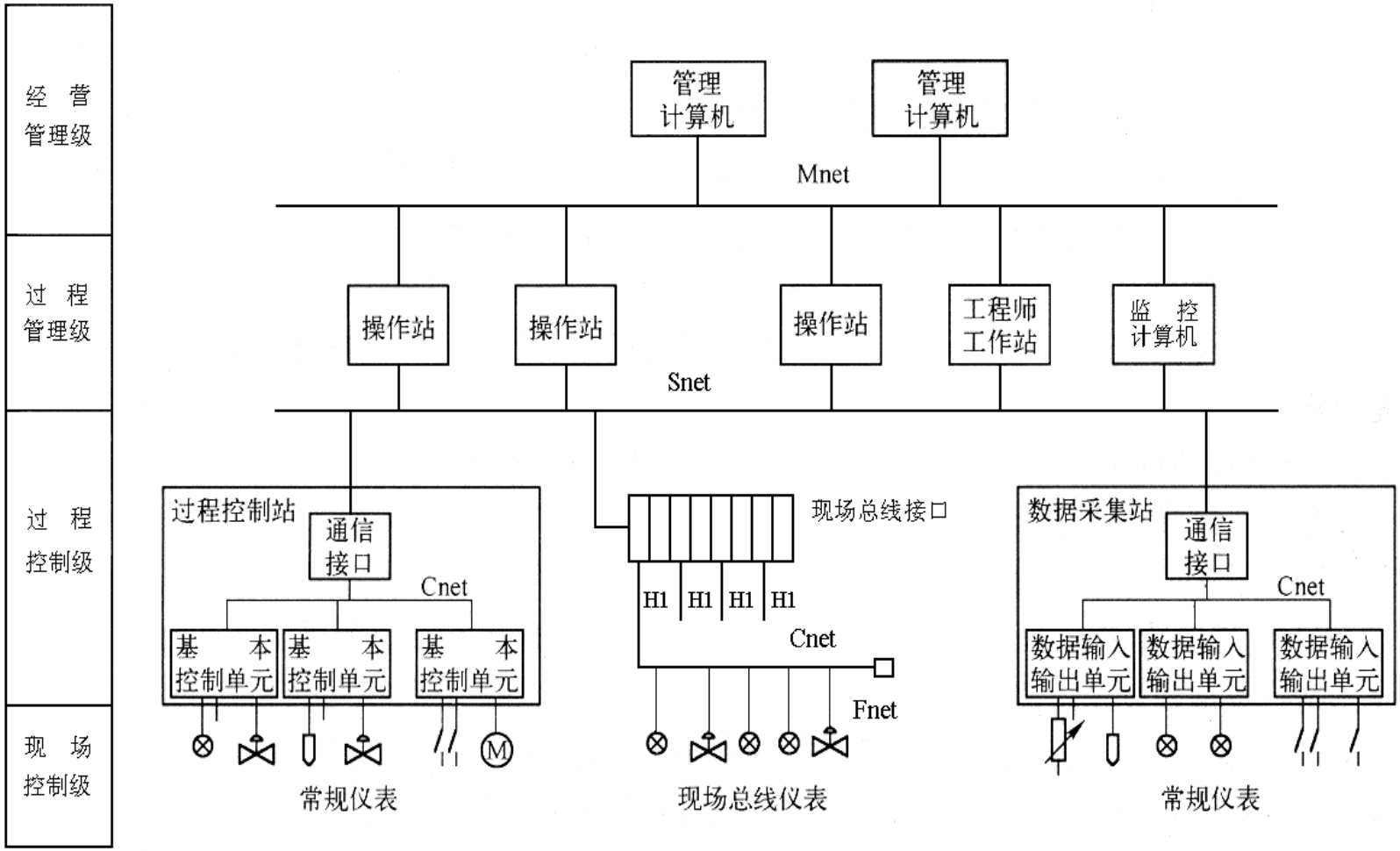
ERP
企业资源计划

MES
制造执行系统

PCS
过程控制系统



工业控制系统网络层次：


经营管理级
过程管理级
过程控制级
现场控制级
管理计算机
管理计算机
Mnet
操作站
操作站
操作站
工程师工作站
监控计算机
Snet
过程控制站
通信接口
Cnet
基本控制单元
基本控制单元
基本控制单元
常规仪表
现场总线接口
H1
H1
H1
H1
Cnet
Fnet
现场总线仪表
数据采集站
通信接口
Cnet
数据输入输出单元
数据输入输出单元
数据输入输出单元
常规仪表

管理网：

即办公网

- 主要涉及企业级应用
- 互联网通信边界
  - 威胁：不安全的远程支持
  - 防护措施：防火墙、身份认证、准入控制
- 监控网通信边界
  - 威胁：无基本访问控制及认证机制
  - 防护措施：防火墙、网闸、安全管理平台

监控网：

- 主要部署关键工业控制组件
- 威胁：
  - 非授权接入
  - 不安全通信
  - 第三方外联网络带来的攻击
  - 专用工业控制协议漏洞
- 防护措施：
  - 工控防火墙、工控安全审计

控制网：

- 工业以太网、总线网
- 信息处理的现场化
- 威胁：
  - 接入技术繁杂
  - 不安全维护
  - 操作系统漏洞、防病毒手段缺乏
  - 指令越权/越限下达
- 防护措施：
  - 工控防火墙、主机安全防护产品

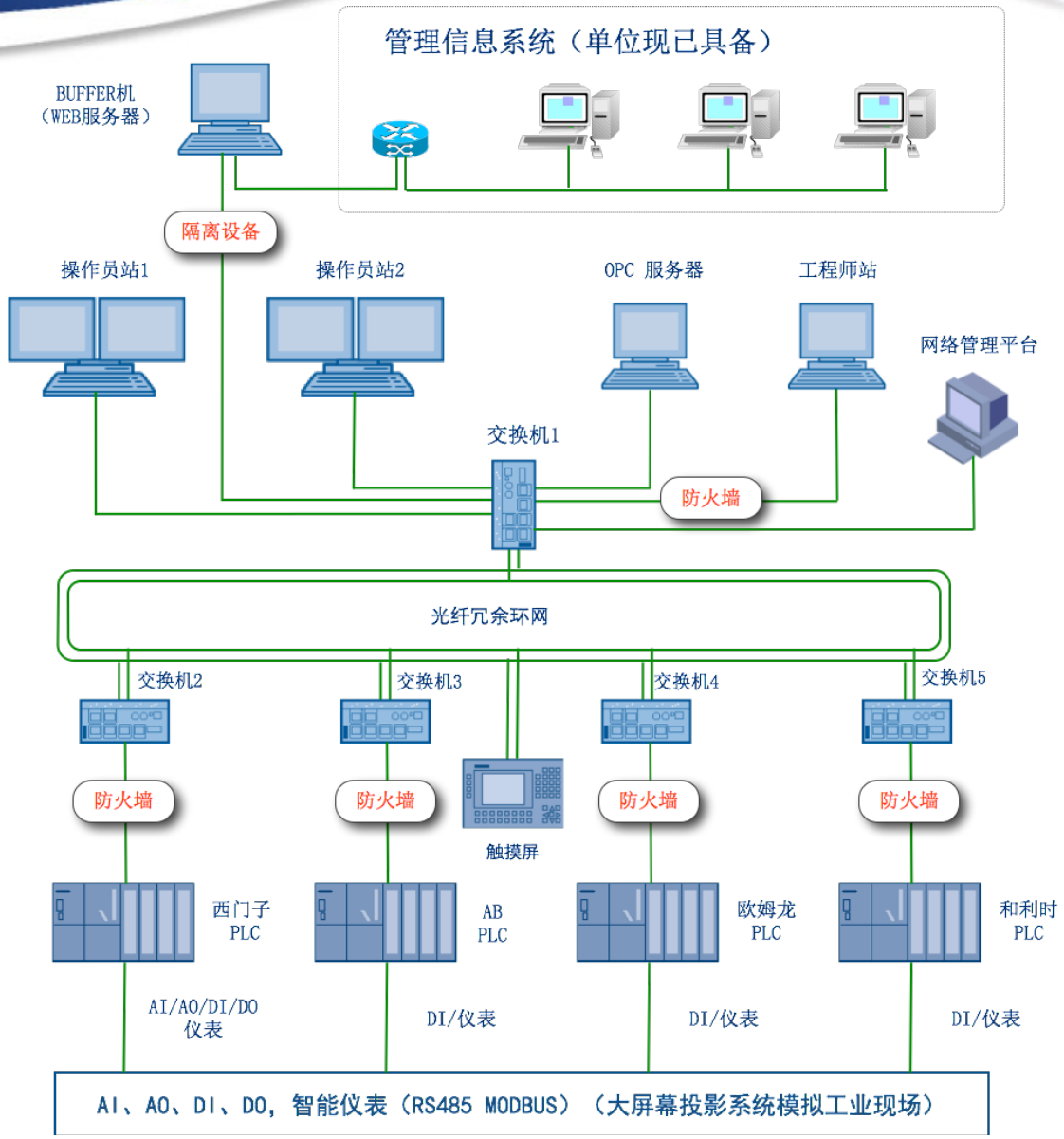
三层网络，二级防护：

- 管理网和监控网之间：
  - 避免非授权访问和滥用
  - 对操作失误、篡改数据，抵赖行为的可控制、可追溯
  - 避免终端违规操作
  - 及时发现非法入侵行为
  - 过滤恶意代码
- 防护措施：
  - 身份鉴别、访问控制、检测审计、链路冗余、内容检测

三层网络，二级防护：

- 监控网和控制网之间：
  - 阻止来自企业信息层的病毒传播
  - 阻挡来自企业信息层的非法入侵
  - 管控OPC客户端与服务器的通讯
  - 区域隔离及通信管控
  - 实时报警
- 防护措施：
  - 工控防火墙、工控安全审计、工控IDS、工控安全管理平台

分区域防护：


管理信息系统（单位现已具备）
BUFFER机
（WEB服务器）
隔离设备
操作员站1
操作员站2
OPC 服务器
工程师站
网络管理平台
交换机1
防火墙
光纤冗余环网
交换机2
交换机3
交换机4
交换机5
防火墙
防火墙
防火墙
防火墙
触摸屏
西门子
PLC
AB
PLC
欧姆龙
PLC
和利时
PLC
AI/AO/DI/DO
仪表
DI/仪表
DI/仪表
DI/仪表
AI、AO、DI、DO，智能仪表（RS485 MODBUS）（大屏幕投影系统模拟工业现场）

工控信息安全防护：

- 工控设备和组件的信息安全
  - 防病毒、抗攻击
- 专用工控信息安全防护产品
  - 工控防火墙、工控主机防护产品
- 工控系统的信息安全
  - 工控系统等级保护

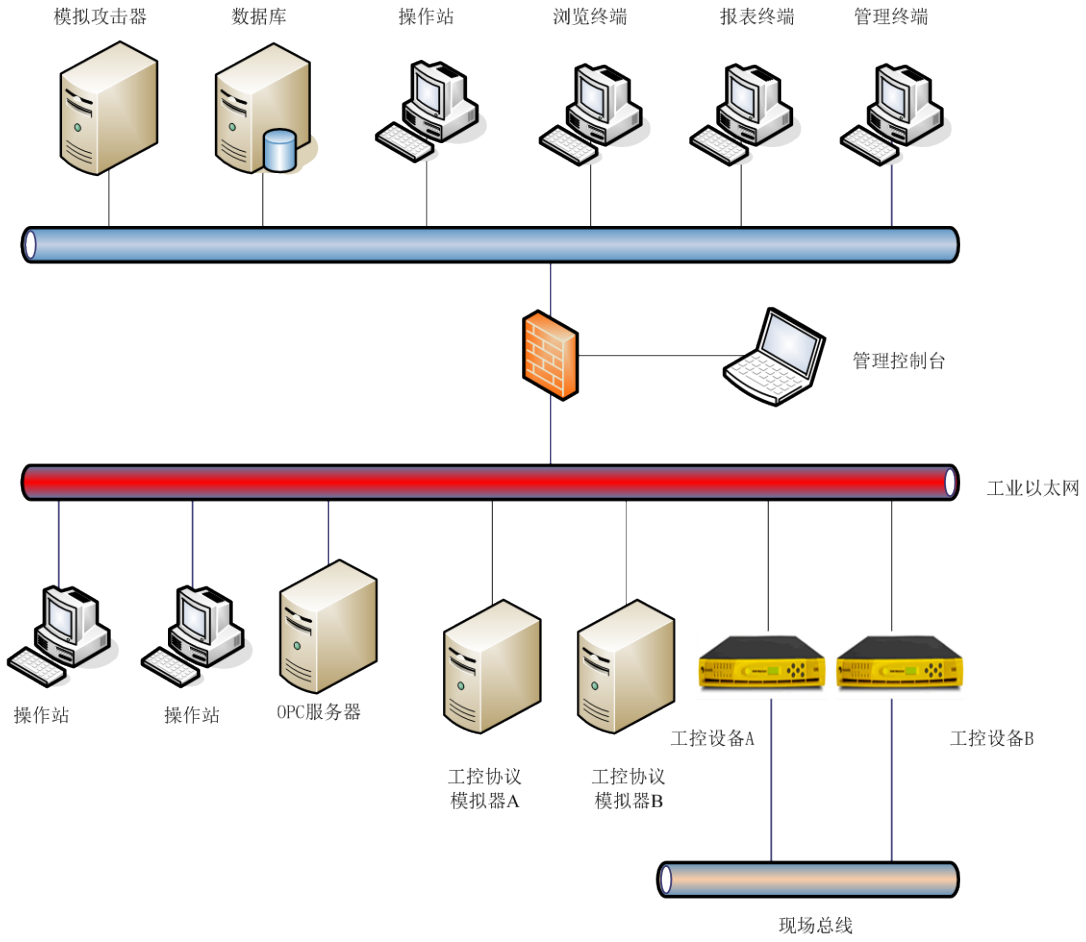
专用工控信息安全产品测试流程：

- 测试依据
  - 发布的相关产品测试标准
  - 工控环境适应性
- 通过测试
  - 申请销售许可证

专用工控信息安全防护产品：

- 适用于工业控制的防火墙
  - 传统防火墙要求的适用性
  - 白名单策略
  - 主流工控协议过滤：ModeBus TCP、OPC、Profinet、DNP3.0等
  - 动态开放OPC端口
  - 多工作模式
  - 高可靠性

适用于工业控制的防火墙测试环境：



专用工控信息安全防护产品：

- 工控主机防护产品
  - 铠甲式外挂
  - 人员审核与访问控制
  - 操作行为审计与监控
  - 数据安全交换与杀毒

工业控制系统安全测评：

- 借鉴计算机等级保护制度
- 技术要求
  - 物理安全、网络安全、工业控制设备安全、应用安全、数据安全
- 管理要求
  - 安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理

工控信息安全标准：

- 国际标准
  - ISA、IEC：IEC 62443《工业过程测量、控制和自动化 网络与系统信息安全》（ISA SP99）
  - NIST：SP 800-82《工业控制系统安全指南》
- 国家标准
  - SAC TC124、TC260
- 行业标准
  - 电力、公安（GA）

总结：

- 工控信息安全重要性
- 三层网络、二级防护机制
- 工控信息安全产品的研制、检测和标准化
- 工控系统等级保护