工业控制系统信息安全业务发展思路

和利时集团
朱毅明

工控系统信息安全市场现状

- **商业模式不成熟，生态环境不完整；**
  - 行业政策：尚未出现强制性法规、规范和标准；
  - 参与者：工控系统产品厂家、IT行业的信息安全产品厂家、IT行业的测试检测单位、科研机构和高校；
  - 最终用户：
    - 既有工控系统用户：信息安全升级改造对既有系统的正常运行影响最小；
    - 新建工控系统用户：一次性投入？长期维护？降低总拥有成本
  - 商业模式：服务？产品？
    - 产品销售
    - 系统集成
    - 长期维护性服务
    - 检测检验服务
- **在役工控系统信息安全改造升级和新建工控系统信息安全采用的策略不尽相同；**
- **工控行业产品利润空间较小，信息安全产品价格要合理；**
- **工控信息安全市场尚处于培育阶段，长期的盈利模式不够清晰；**
- **仅仅依靠政策是很难保证工控系统信息安全市场的健康持续成长。**

来自最终用户的声音

- **恶意攻击的最终目标是实际的工业设施或工艺装备，应该面向具体的工业应用开展信息安全风险评估和安全分级，而不是面向工业控制系统设备本身；**
  - 由于化工、石油、火电、核电、冶金等行业连续过程工艺的特点，一旦中断运行，经济损失大，甚至可能造成严重环境污染和人员伤亡，危险性大，信息安全风险较大；
  - 由于交通、电网、市政设施和管线、长输油气管线、水利设施、矿山等行业采用的工业监控系统地理分布广泛，大部分设备无人值守自动运行，采用公网或无线传输，容易遭到攻击，且直接影响社会安定，信息安全风险较大；
  - 离散制造业在受到恶意攻击主要是停产和废品率升高造成的经济损失；
  - 大型数控加工中心存储的秘密数据存在泄漏的风险；
  - 危险的工业设施大多保留手动或非数字化的后备保护系统，如果受到攻击，经济损失不可避免，但恶性事故发生的风险不大；
- **缺少信息安全专业人员，维护能力弱；**
- **缺少维护经费，特别是长期的服务采购费用；**
- **没有工控系统信息安全标准和设计规范；**
- **缺少权威的认证检测机构；**

工控系统信息安全产品

- **信息安全系统在线升级，整个工控系统不允许停机；**
- **网络安全增强型产品：外挂式，不需要修改现有工控系统的网络协议、软件和硬件，增加网络信息安全设备，对于既有工控系统是透明的。**
  - 外部边界网关、防火墙等
  - 网络安全审计系统
  - 网络过滤设备
  - 加密传输设备
  - 病毒查杀、漏洞探查修复等
- **本质信息安全型产品：嵌入式，修改工控系统的网络协议、软件和硬件，从本质上提升工控系统的信息安全性能。**
  - 信息安全的工业实时网络协议
  - 可信工业控制系统开发环境
    - IEC61131-3编译器
    - 下装身份验证
    - 代码加密
  - 信息安全的工控系统控制单元：安全计算？

工控系统网络的特点

- 工控系统对外的网络多采用标准的以太网、TCP/IP协议和开放的工业控制系统网络协议；
- 部分在役工控系统没有采用以太网，而是采用令牌总线、令牌环、FDDI、CAN、Controlnet或基于RS232/485串口的通讯协议；
- 工控系统内部网络多采用私有协议，甚至不是TCP/IP，但数据流量相对稳定，网络行为模式固定；
- Profinet（IRT）、EtherCAT、POWERLINK等工业实时网络协议是基于以太网，但大多在标准的IEEE802.3以太网的基础上进行了修改，而且由于网络循环周期ms级别，对网络保护装置造成的报文延迟非常敏感；
- 工控系统网络大多采用双重冗余的结构；

工控信息安全产品

- **工控系统边界防护产品：单向网闸、网关、防火墙等；**
  - 支持OPC、MODBUS-TCP、IEC60870-5-104、IEC61850、DNP等开放的协议；
  - 访问控制：数据对象？寄存器？命令码？
  - 攻击检测：主动？被动？升级？
  - 漏洞检测？
  - 白名单？黑名单？
  - 支持远程管理？
  - 提供升级服务？

工控信息安全产品

- **工控系统内部网络防护产品：**
  - 网络安全审计产品：
    - 已知网络协议：工控系统差异较大，需要支持非信息安全专业人员的现场配置方式，如图形化配置、脚本、配置表等等；
    - 未知网络协议：自学习？
    - 已知漏洞探查
    - 已知威胁检测报警
    - 远程管理和升级
  - 网络安全过滤产品：协议深度解析
    - 单端口？多端口？
    - 限制MAC、IP？
    - 限制命令码？
    - 限制可访问数据对象？
    - 延迟？

“本质信息安全”的工控系统

- 工控系统要求分散部署，采用分布式控制模式，每一个控制节点具备独立工作的能力，采用的信息安全手段要支持去中心化设计，集中的信息安全管理设备可能不适用。
- 由于工作环境恶劣，工控系统采用的嵌入式处理器性能远低于IT系统，很难支持基于软件的加密、解密、数字签名等复杂的操作；
- 工业现场在线升级困难，要考虑试运行和回退措施，清晰分离工控系统的信息安全保护和控制部分，尽量避免对控制部分的修改；
- 由于PLC、DCS等工控系统大多提供面向工艺用户的可视化控制逻辑描述语言（梯形图、功能块图、SAMA图等），用户可以自己编写控制逻辑代码，需要对从编辑、编译、下装、加载运行的全过程进行信息安全控制。
  - 数字签名
  - 可信编译
  - 下装身份认证
  - 建立可信链，安全启动；
  - 控制器虚拟化

工控系统信息安全服务

- **降低最终用户的一次性投资，提供长期的工控系统信息安全服务；**
- **基于云计算技术的远程服务**
  - 历史数据云存储
  - 运行状态判断
  - 异常事件分析
  - 漏洞探查和修补
  - 防护策略升级
  - 远程故障处理
- **存在问题**
  - 公网网络流量费用？
  - 如何保证远程端口的安全？
  - 用户数据的安全？
  - 初期建设费用高，后期的盈利模式不够清晰。

HollySys

谢谢！

Automation for Better Life