

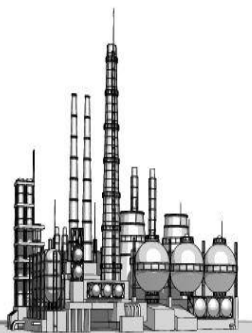


工业控制系统信息安全产品现状及标准情况介绍

邹春明

公安部第三研究所

国家网络与信息系统安全产品质量监督检验中心



目 录

- 工业控制信息安全产品情况
- 工业控制信息安全产品标准
- 检测中心的主要工作（工控）



1

工业控制信息安全产品情况

工业控制信息安全现状

缺乏信息安全基础：

- 工控设备/工控协议缺少信息安全方面设计
- 系统建设之初较少考虑信息安全
- 信息安全意识比较淡薄
- 标准体系缺乏

与互联网的融合增加风险：

- 随着互联网的发展，工控设备广泛的支持互联网协议
- 业务上、效率上的需要，不得不融入互联网



工业控制信息安全防护

工控信息安全防护

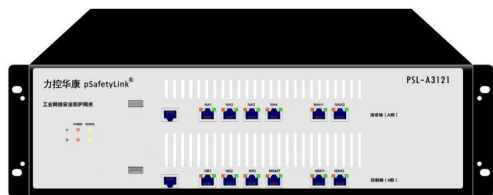
1. 加强政策引导
2. 完善工控信息安全标准体系
3. 工控设备的自身加固、开发安全的工控协议
4. 通过**工业控制信息安全专用产品**进行防护



工业控制信息安全产品

基本定义

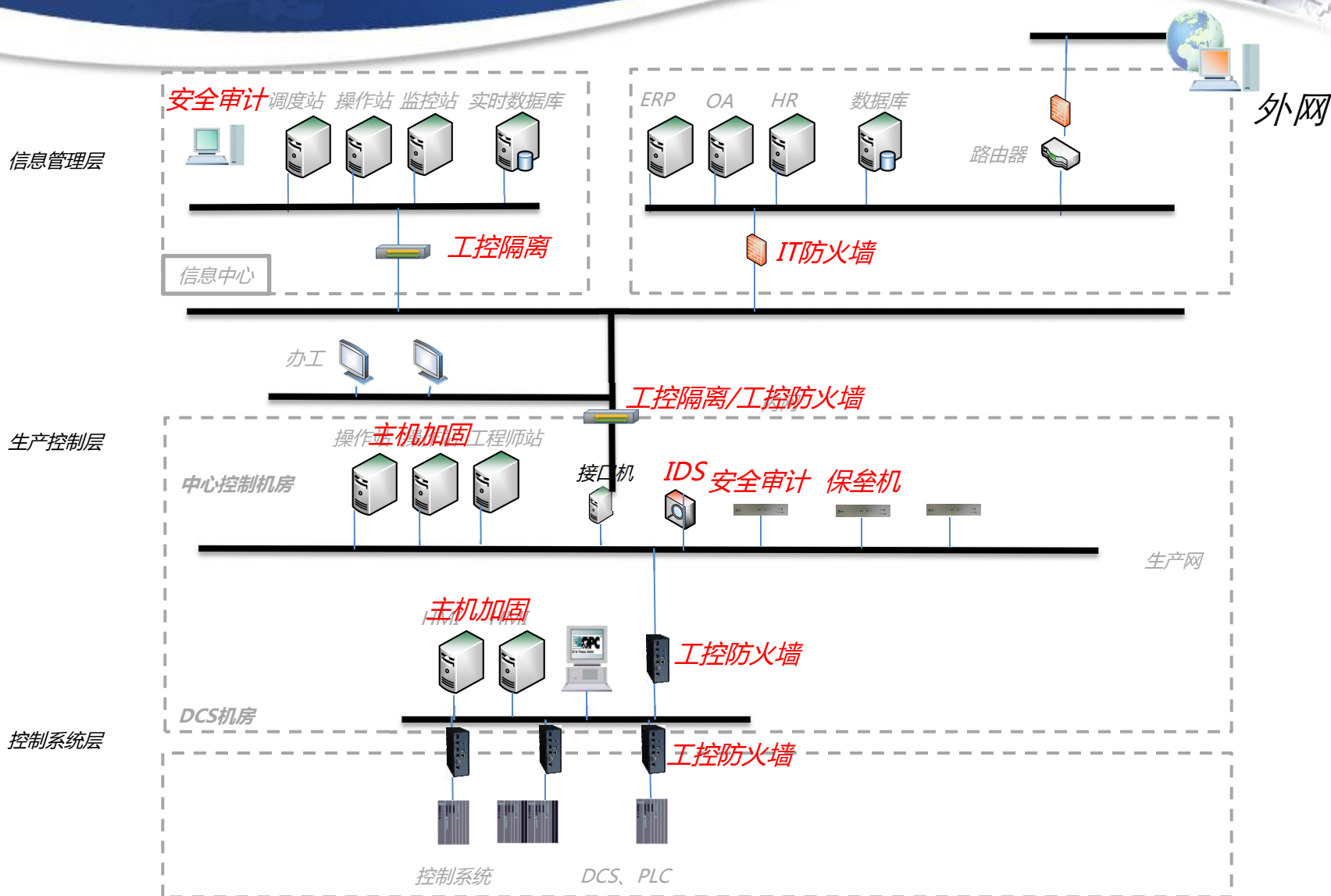
适用于工业控制系统，对工业控制系统及系统中的计算机设备、工业控制设备进行安全防护的专用硬件和软件产品。



设备 + 网络版25222 out, 11335, en



工业控制信息安全产品



工业控制信息安全产品



主要分类：

- 边界防护类
- 审计监控类
- 主机防护类
- 其它类

边界防护类产品：

以串接方式工作，部署在工控以太网与企业管理网络之间、工厂的不同区域之间、控制层与现场设备层之间。通过一定的访问控制策略，对工控系统边界、工控系统内部区域边界进行保护。

主要产品：工控防火墙、工控隔离（网闸、协议隔离、单向导入）

由于这类产品串接方式部署，同时具有阻断功能，产品的稳定可靠、功能安全要求较高，产品的异常将会对工控系统的正常运行带来直接影响。

总体安全性：**单向导入>工控隔离>工控防火墙**

边界防护类产品：

➤ 工控隔离类产品

主要部署在工控系统中控制网与管理网之间。

- 工控网络隔离：采用双机或者2+1架构，协议剥离与重组，两机之间私有协议传输。典型产品：**OPC网闸**、**电力网闸**、**通用网闸**等。
- 单向导入：采用双机架构，物理上单向保障（单向光纤、VGA视频传输）

边界防护类产品：

➤ 工控防火墙

通常用于各层级之间、各区域之间的访问控制，以及部署在单个或一组控制器前方提供保护。（域间防火墙、现场防火墙）

- 支持传统的五元组访问控制，工业控制协议的深度分析及过滤（实现OPC动态端口开放支持、工业控制协议格式检查、命令及参数的白名单方式控制等）。
- 实现上：传统IT防火墙上增加工控协议的分析与控制；参考多芬诺工业防火墙及工控设备模式来实现

审计监控类产品：

主要以旁路方式工作，被动方式对网络流量进行审计分析，或以主动方式对主机及设备安全性进行探测获取。

当前主要产品：工控安全审计产品、工控安全监测/管理平台。
存在有工控漏扫、工控入侵检测。

由于这类产品主要以旁路方式部署，产品自身的故障之类不会对工控系统带来直接危害，用户更容易接受。

审计监控类产品：

➤ 工控审计产品

通常旁路监听方式，主要目的包括事后的分析，事中监测报警。

- 对各协议(包括工控协议)进行深度解析，获取必要的内容进行记录。包括网络层信息及应用层信息。
- 不足：目前主要还是对通信进行审计记录，对事后的分析方面工作较少。

审计监控类产品：

➤ 工控漏洞扫描产品

集成了传统的网络漏洞扫描功能；增加了工业控制漏洞扫描，基于设备厂商、类型、固件版本等进行分析，可能还具有基于协议fuzzing的漏洞探测。

需求：工控等保标准即将发布，工控等保工作稳步推进中，漏洞扫描是必不可少的工具。

问题：在线生产系统通常不允许扫描；漏洞库的完备性欠缺。

主机防护类产品：

工控系统部署有一定数量的计算机主机设备，如工程师站、操作员站、数据库服务器等。这些设备往往是工控系统的重要风险点之一，病毒的入侵、人为攻击等威胁主要都是通过主机设备进入工控系统。

主要产品：ICS主机安全防护、文件加载执行控制（白名单）

工业控制信息安全产品

近年工业控制信息安全产品销售许可检测情况：

主要产品类型：

- 工控防火墙
- 协议隔离
- 工控审计
- 网闸
- 单向导入
- 文件加载执行控制
- 其它产品

测评依据：

对应的IT信息安全标准

+工业控制安全补充要求

工业控制信息安全产品

近年工业控制信息安全产品销售许可检测情况：

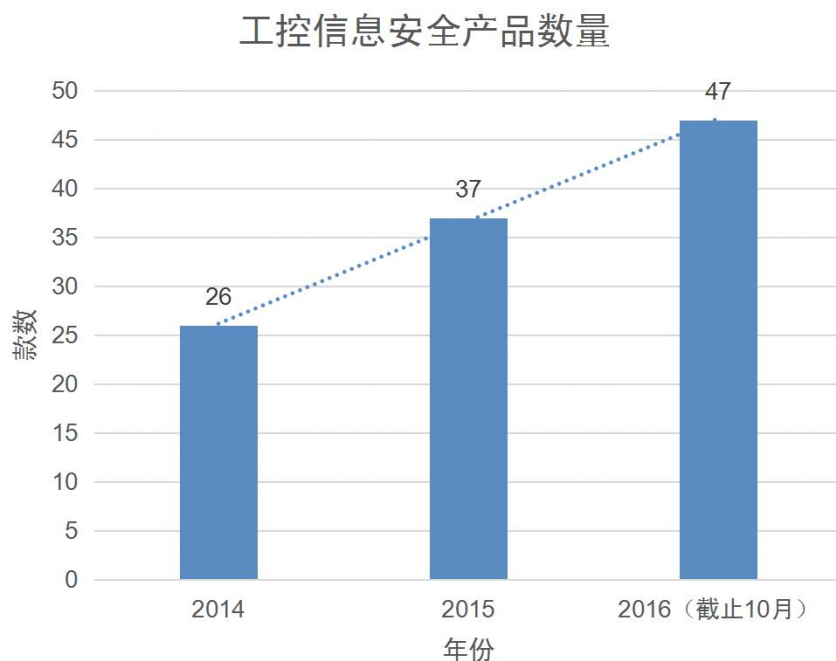
根据统计结果：

市场上产品总数：约80款

隔离类产品：28款

工控防火墙：33款

工控审计：11款



工业控制信息安全产品



生产厂商：

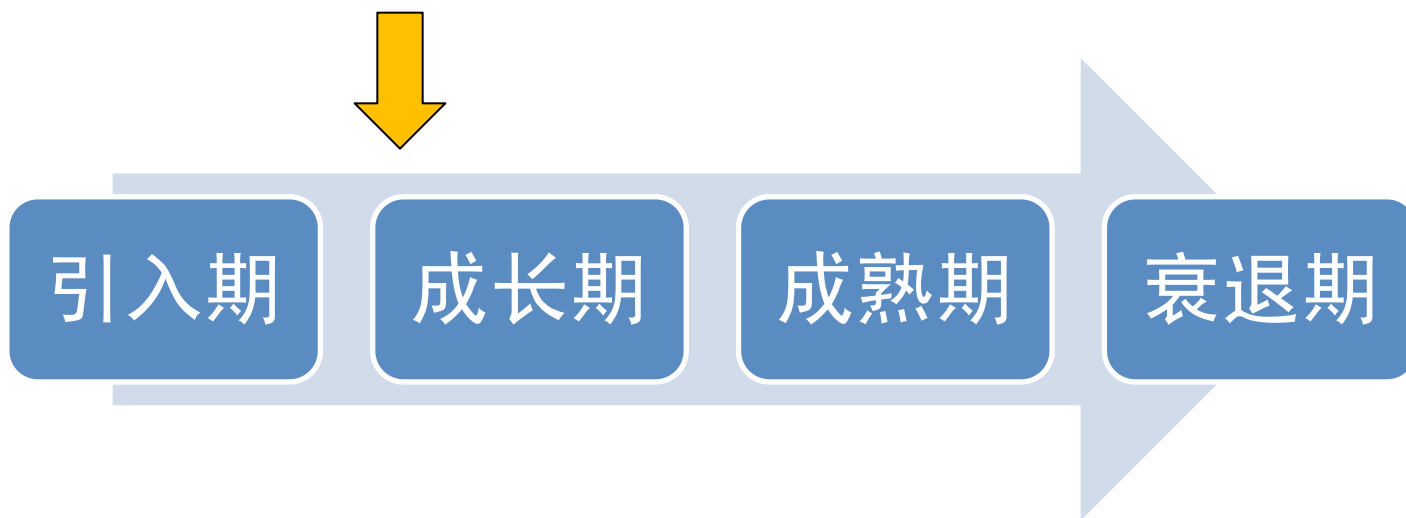
原来IT信息安全产品厂商

原工业控制厂商

部分工业控制信息安全厂商

工业控制信息安全产品

产品生命周期：



发展与期望：

进一步完善产品的安全功能

关注产品自身的稳定性、可靠性、环境适应性

自主可控



2

工业控制信息安全产品标准

工控信息安全相关标准现状：

- 总体还不够完善
- 各研究机构、公司在努力完善过程中
- 编制难度较大，行业差异

工控信息安全产品相关标准-国标：

- ① 《信息安全技术 工业控制网络安全隔离与信息交换系统安全技术要求》
- ② 《信息安全技术 工业控制系统网络审计产品安全技术要求》
- ③ 《信息安全技术 工业控制系统专业防火墙技术要求》



工控信息安全产品相关标准-公共安全行标：

- ① 《信息安全技术 工业控制安全管理平台安全技术要求》
- ② 《信息安全技术 工业控制系统入侵检测产品安全技术要求》
- ③ 《信息安全技术 安全采集远程终端单元(RTU)安全技术要求》
- ④ 《信息安全技术 工业控制系统边界安全专用网关产品安全技术要求》
- ⑤ 《信息安全技术 工业控制系统软件脆弱性扫描产品安全技术要求》
- ⑥ 《信息安全技术 ICS主机安全防护与审计监控产品安全技术要求》



3

检测中心的主要工作（工控）

检测中心的主要工作



- 工业控制信息安全产品检测
- 工业控制设备（PLC等）安全性测试
- 工业控制系统的安全评估
- 工业控制信息安全相关的科研工作

谢谢！