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

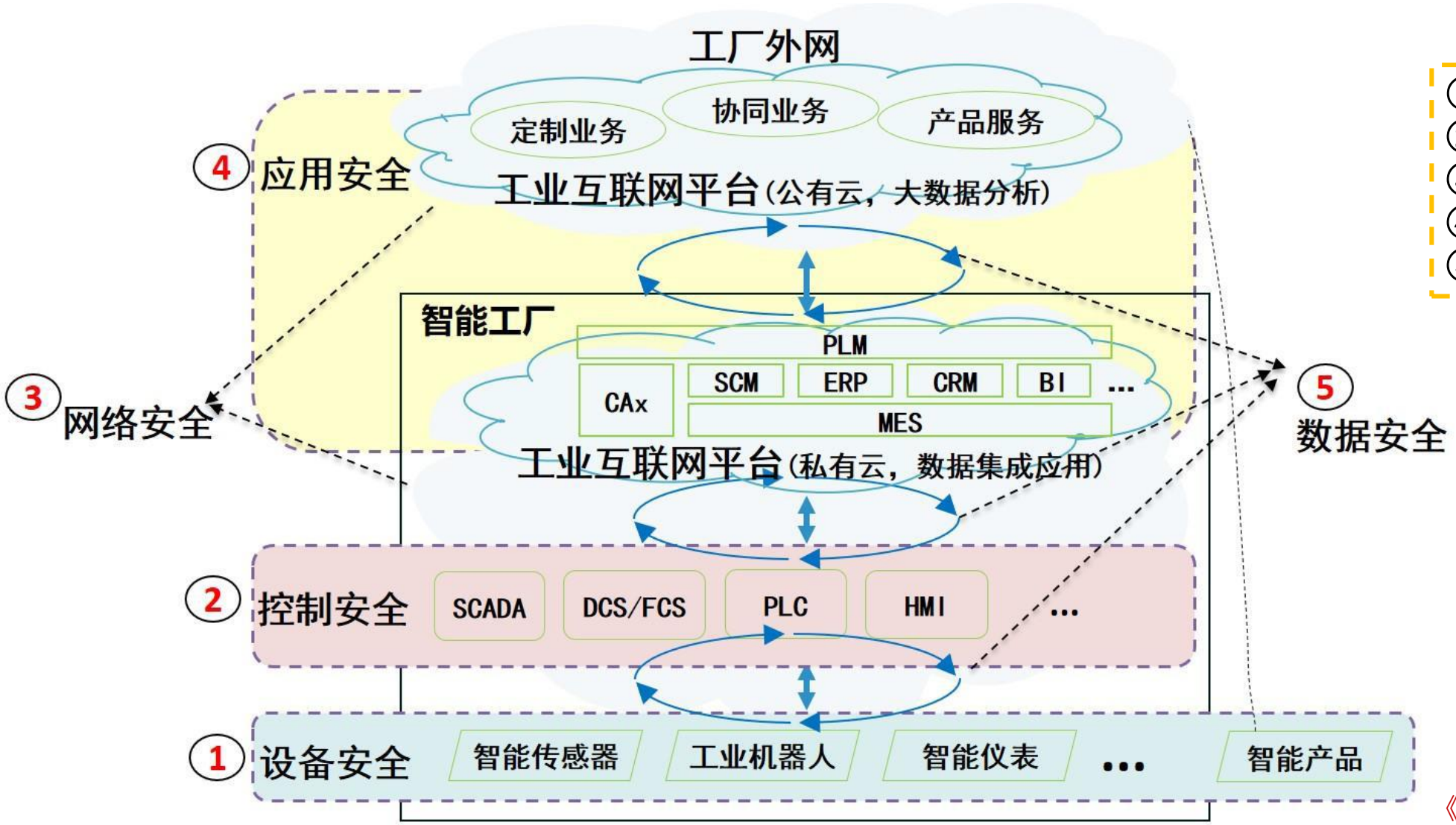
工业互联网热潮中工控安全的落地点

汇报人：启明星辰集团 原真

汇报日期： 2019年5月9日

- 2016.10月 《工业和信息化部关于印发《工业控制系统信息安全防护指南》的通知》
- 2017.11月《 国务院关于深化“互联网+先进制造业”发展工业互联网的指导意见》
- 2017.12月 《工业和信息化部关于印发《工业控制系统信息安全行动计划（2018-2020年）》的通知》
- 2018.6月 《关于印发《工业互联网发展行动计划（2018-2020年）》和《工业互联网专项工作组2018年工作计划》的通知》
- 2019.4月 工信部《关于加强工业互联网安全工作的指导意见（征求意见稿）》

工业互联网发展的政策推动力



① 设备安全
② 控制安全
③ 网络安全
④ 应用安全
⑤ 数据安全

《工业互联网 安全总体要求》

工业互联网安全防护场景

工业互联网网络安全体系框架

2018年第二季度网络安全威胁态势分析与工作综述

（二）工业互联网平台和智能设备成为网络威胁的重要目标。据国家工业信息安全发展研究中心监测，第二季度我国境内共有22个工业互联网平台提供服务，针对这些工业互联网平台的、来源于境外的网络攻击事件共有656起，涉及北京、重庆、湖南、内蒙古等地区；新增工业控制系统漏洞115个，涉及罗克韦尔、西门子、施耐德电气等品牌的71款产品；我国境内感染工业互联网智能设备恶意程序的受控IP地址共有52.7万余个，受控IP地址数量在1万个以上的僵尸网络共有13个。

2018年第四季度网络安全威胁态势分析与工作综述

（二）工业互联网安全问题不容忽视。第四季度，对54个工业互联网平台、200多万个联网工业控制设备进行持续监测，**发现疑似弱口令、SQL注入、信息泄露等风险2433个**。同时，监测发现针对工业互联网平台的SQL注入、跨站脚本等网络攻击1000余起。

2018年第三季度网络安全威胁态势分析与工作综述

一、网络安全威胁总体态势

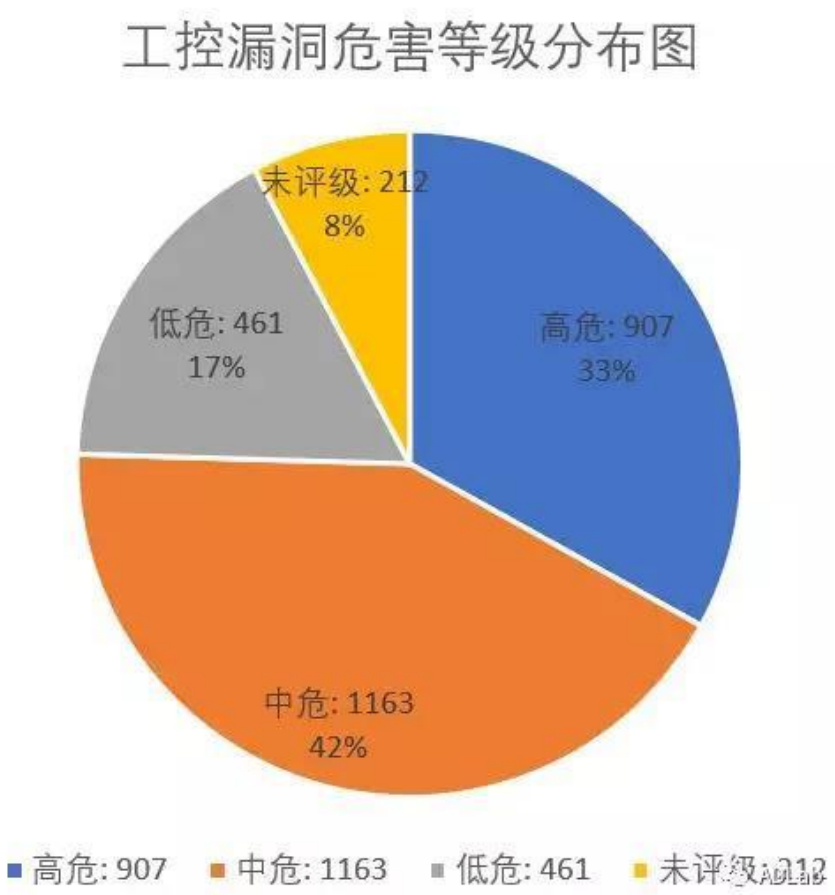
（二）云计算平台相继发生故障，其安全性仍待加强。 近年来，“企业上云”已成为发展趋势，公有云计算平台承载着越来越多的关键业务和重要数据，其安全问题也成为各方关注的焦点。第三季度前后，国内外多家云计算平台相继发生故障，出现大规模用户访问异常、用户数据丢失等问题，暴露出云计算平台在管理、运维、防护等方面仍存在诸多不足。

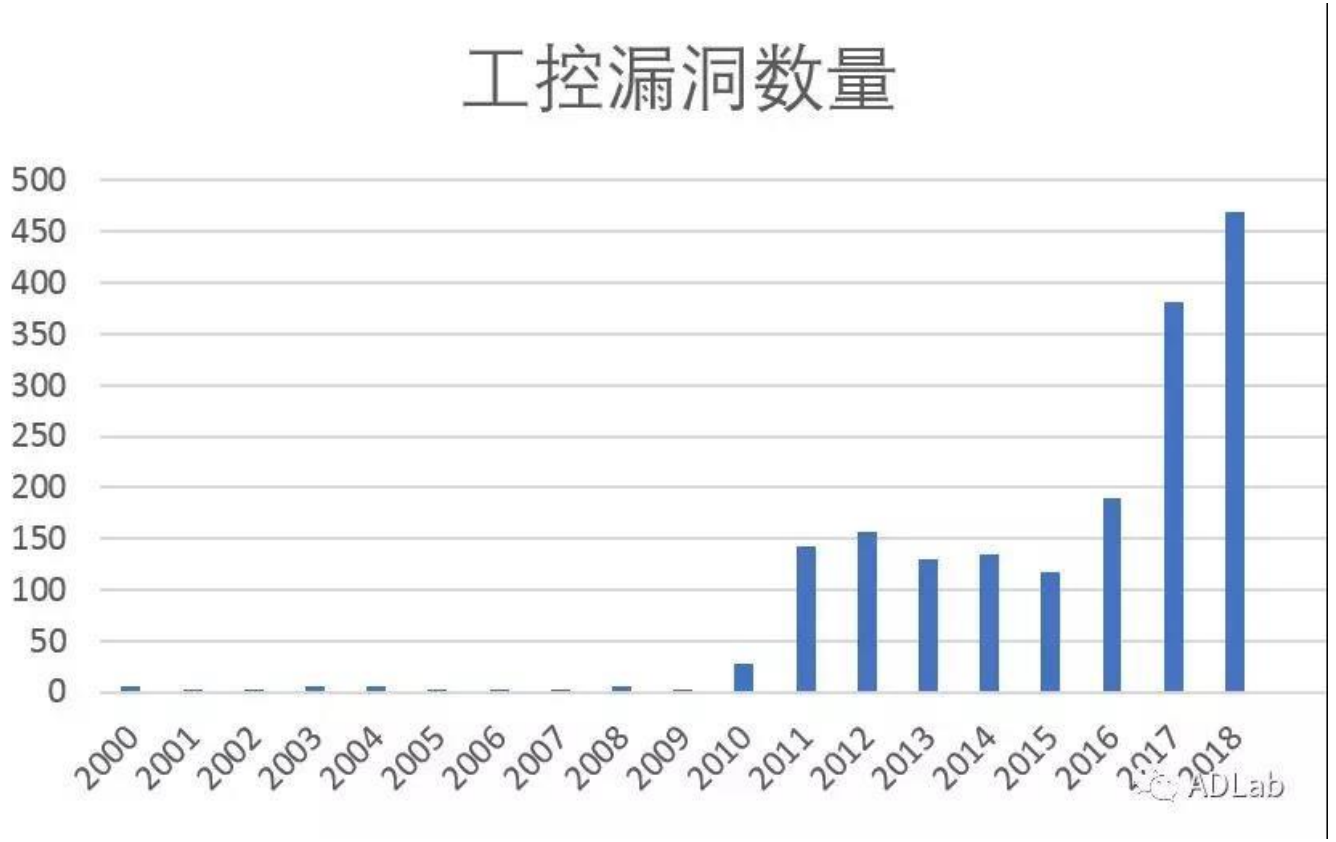
（三）勒索病毒严重危害网络用户合法权益。多家单位持续关注勒索病毒威胁，监测到多地发生Globelmposter勒索病毒攻击事件，同时对已爆发近17个月的WannaCry勒索病毒在国内的感染情况进行了统计，本季度每天仍有约6000至14000的感染量；根据阿里云统计，阿里云平台在第三季度共拦截约836亿次攻击，其中利用永恒之蓝漏洞（WannaCry勒索病毒利用的漏洞）进行攻击的数量占到近三分之一。

（四）网络安全漏洞仍然是工业互联网面临的主要安全威胁之一。第三季度，国家工业信息安全发展研究中心监测发现新增工业控制、智能设备、物联网等相关漏洞105个；中国信息通信研究院对31个工业互联网平台的126个域名、近170万个IP地址持续进行监测，发现疑似风险2600余个，并开展风险核实工作，目前相关工作正在进行中；中国软件评测中心监测发现45个联网工控系统漏洞，涉及多个品牌的58个产品。

三、开展的其他主要工作

（五）启动勒索病毒威胁专项治理行动。9月初，组织基础电信企业、网络安全专业机构、互联网企业和网络安全企业等召开恶意程序专项治理工作讨论会，重点对勒索病毒的工作原理、传播渠道、防范与处置措施等方面进行了研究讨论。在研讨会基础上，进一步研究分析并制定工作方案，于9月底印发**《关于开展勒索病毒专项治理工作的通知》**，组织各地通信管理局、电信和互联网行业企业、网络安全专业机构等针对勒索病毒的传播渠道开展监测与处置。

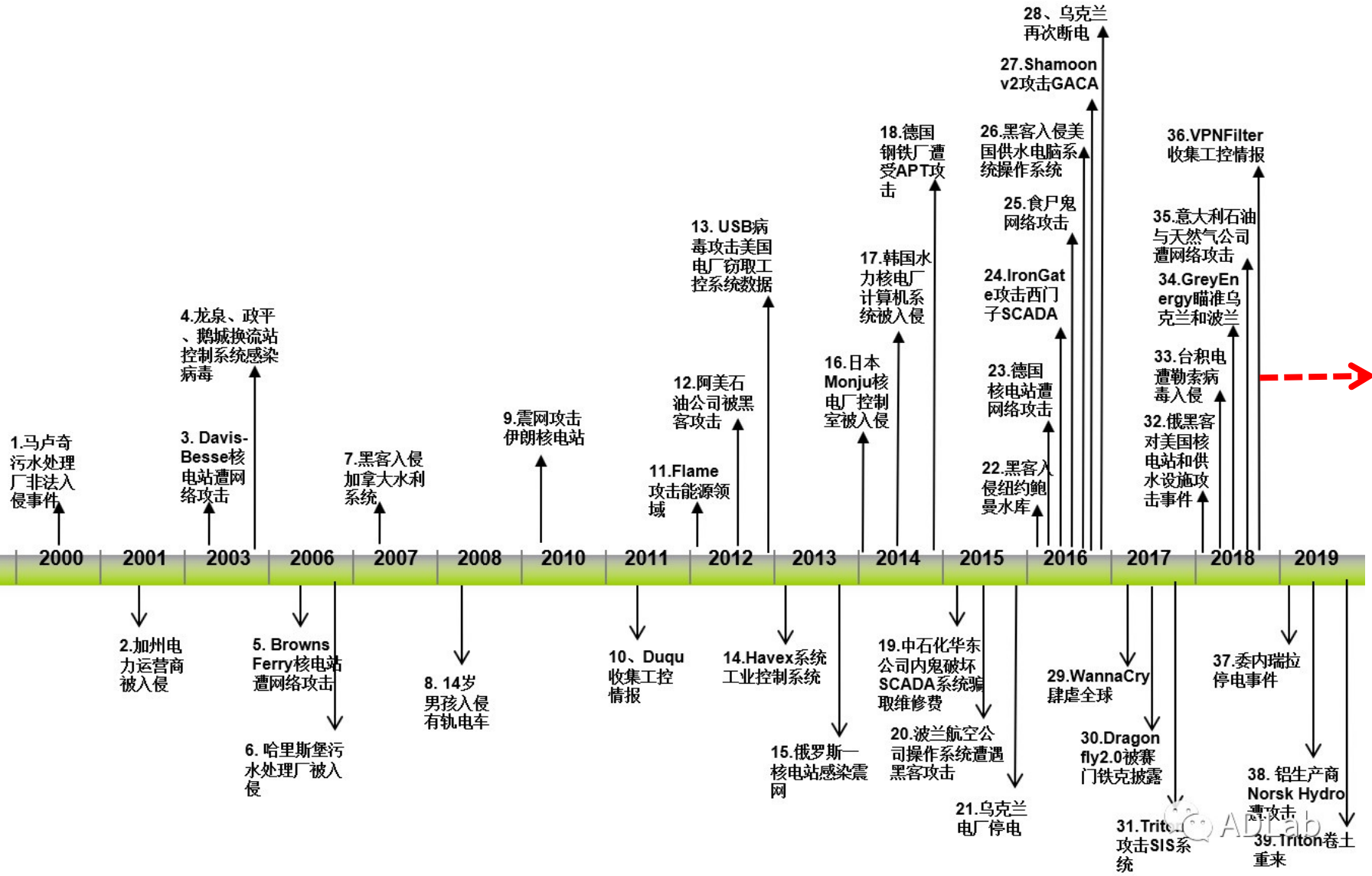




通过对CNVD公开披露的工控漏洞数据的统计分析发现(如图1-1)，截至目前有2743个工控漏洞，其中高危漏洞占比为33%，有907个，中危漏洞占比为42%，达1163个，大大高于传统行业的高中危漏洞比例。其中部分硬件级别的漏洞修复极为困难，只能进行硬件更新。

——《启明星辰ADLab：工控十大网络攻击武器分析报告》

面临的工控安全威胁态势



2018年8月3日~6日台积电晶圆厂遭到勒索病毒攻击，造成高达18亿的经济损失。

● ● ● ● ● ● ? ? ?

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

面临的工控安全威胁态势

《启明星辰ADLab：工控十大网络攻击武器分析报告》

一、工控安全现状
二、工控类攻击事件汇总
三、十大工控网络武器分析
3.1 Stuxnet：工控网络攻击的里程碑
3.2 Duqu-Stuxnet之子
3.3 Flame
3.4 Havex
3.5 Dragonfly2.0
3.6 BlackEnergy
3.7 Industroyer
3.8 GreyEnergy
3.9 VPNFilter
3.10 Triton
四、结语

面临的工控安全威胁态势

启明星辰 | ADLab

adlab.venustech.com.cn

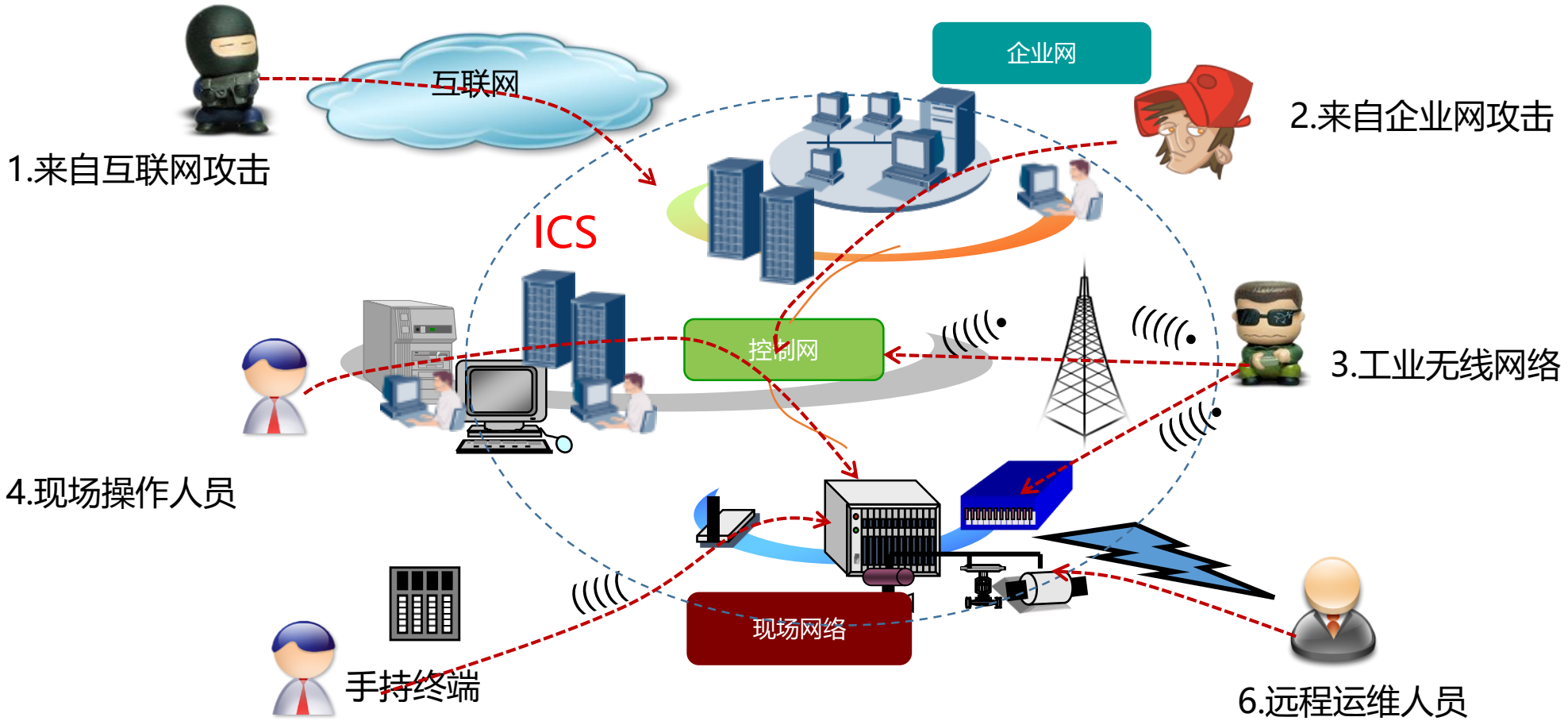
《启明星辰ADLab：工控十大网络攻击武器分析报告》

《启明星辰ADLab：乌克兰电力系统恶意破坏组件分析》

《启明星辰ADLab：乌克兰电力系统攻击过程深度分析》

《【深度分析】VPNFilter：危及全球工控设备和办公网络的物联网高级威胁》

面临的工控安全威胁态势



面临的工控安全威胁分析

◆OS普遍采用Windows 平台
◆一般不会对Windows平台安装任何补丁
◆微软停止对Windows XP/7的技术服务

操作系统

◆应用软件多种多样，很难形成统一的防范规范
◆开放应用端口，常规IT防火墙很难保障其安全性
◆利用一些应用软件的安全漏洞获取设备的控制权

应用软件

通信协议

◆普遍采用TCP/IP 协议和OPC 协议等通信，通信协议存在潜在威胁
◆使用FTP服务
◆G代码明文传输，容易读取到网络上传输的消息，也可以冒充其它的结点

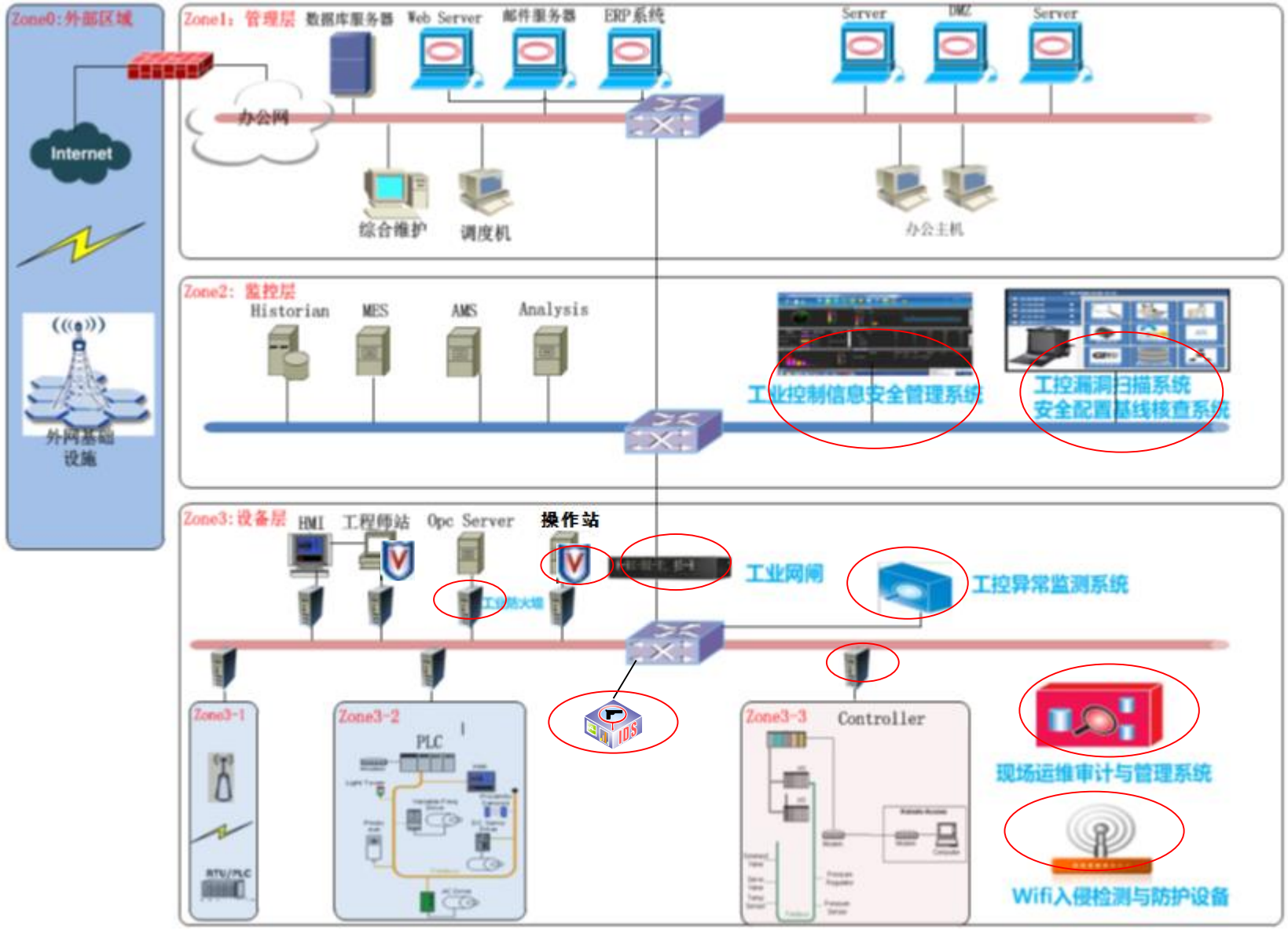
端口与数据

◆外设端口缺乏管控，存在滥用风险
◆G代码在CF卡上有临时备份，可通过非法拷贝等方式对加工数据进行获取
◆生产加工数据明文存放于PCU上，缺少必要的安全增加及保护措施。

135__TCP__msrpc

序号	危险级别	漏洞编号	漏洞名称	返回信息
1	高危险	00010111	RPCSS Dcom接口报文长度域堆缓冲区溢出漏洞(MS03-039)	
2	高危险	0001010F	Windows RPC Dcom接口缓冲区溢出漏洞	
3	高危险	00010110	RPCSS Dcom接口长文件名堆缓冲区溢出漏洞(MS03-039)	

面临的工控安全威胁分析



- 工业防火墙
- 工业网闸
- 工业入侵检测
- 生产网互联关系管理
- 工业主机安全管理系统
- 工业主机病毒监测系统
- 工控运维/数据库审计
- 无线入侵检测与防御
- 物联网安全网关
- 工控漏洞扫描系统/管理平台
- 工控等保检查工具箱
- 工控信息安全管理平台

工控安全建设方案

1.**针对工控网络的风险评估。**通过风险评估对自身工控网络做全面的了解，确定风险和安全缺失项，并根据当前的互联网安全形势和所在行业要求确定整改优先顺序。同时对发现的未知资产或已经被恶意程序攻击（木马后门）的资产进行问题确认和处置。

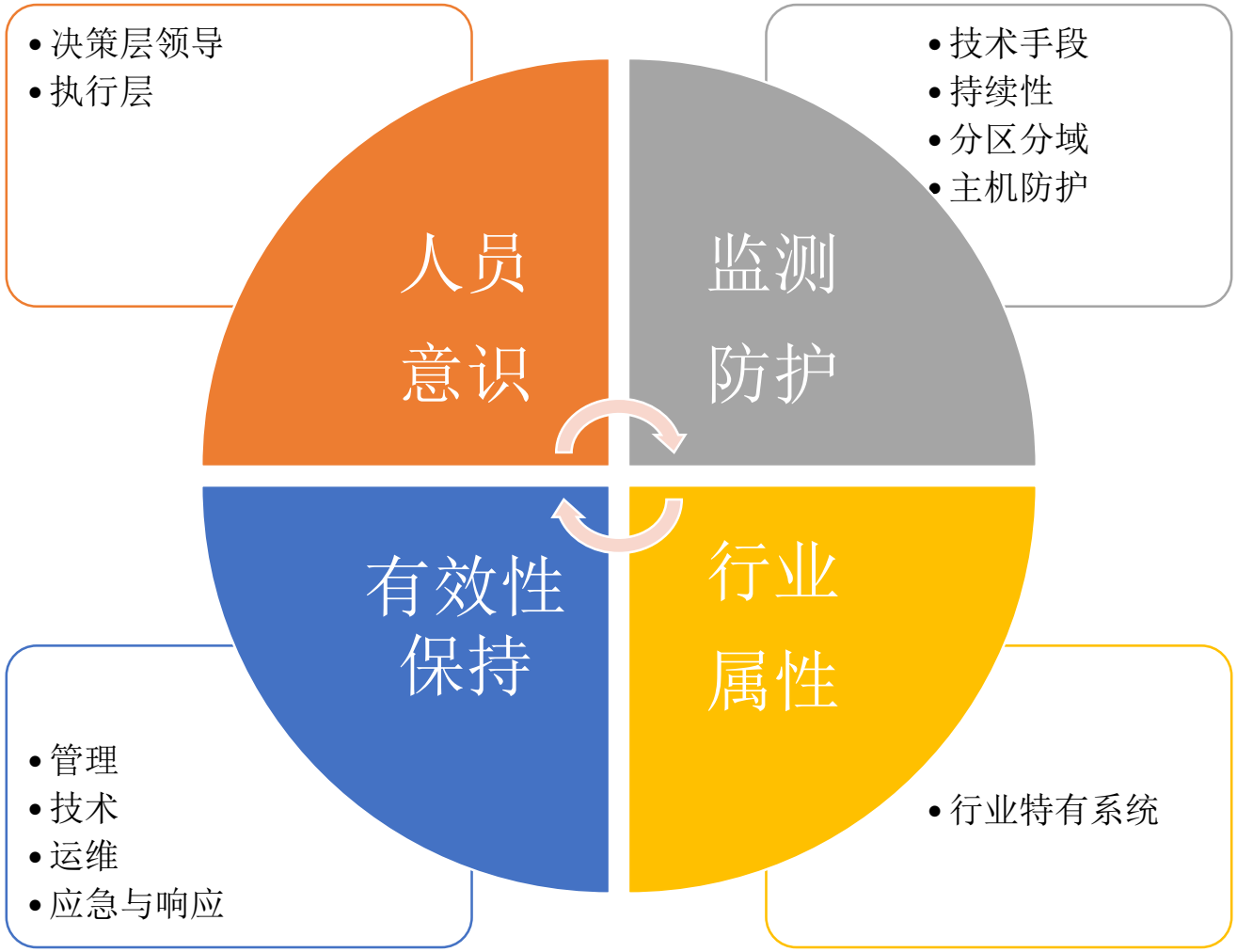
2.**两网隔离防护建设。**优先进行生产网和管理网的逻辑隔离和访问控制，可根据两网接口实际流量协议，通过部署传统多功能安全网关/工业防火墙/工业隔离网闸进行边界检测和防护。

3.**工控网络异常检测和监测。**鉴于生产网的特性，优先针对生产网进行异常流量、入侵攻击、病毒等的检测和设备之间业务访问关系监控，为攻击、异常、故障定位处置提供分析呈现的原始依据。

4.**生产网安全域边界检测和防护。**针对生产网内明确的安全域，通过在域边界部署工业防火墙，进行基本的安全域边界逻辑隔离和访问控制，实现基本的工控域防护和降低安全事件爆发时影响范围。

5.**生产网内部安全建设。**通过在工程师站、操作员站部署工作站安全管理系统，关键PLC前端部署导轨式工业防火墙、无线入侵检测与审计系统、中控室部署运维审计/数据库审计、工控安全管理平台等安全措施，实现生产网内部的安全检测、防护、审计、运维、管理。

工业控制安全建设开展步骤建议



工控安全建设中涉及的突出难点

1.网络安全是人与人的对抗，PDCA螺旋上升是基本需要

2.网络安全需要系统化的规划、分步实施过程中问题导向

3.生产业务与网络安全的三同步问题（同步规划、同步建设、同步运行）

4.安全管理中的人性弱点

5.工控安全投入的经济可行性标准

共同的思考？

Thanks

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