工业互联网产业联盟
Alliance of Industrial Internet

航天云网工业互联网安全保障思考

主讲人：穆森

智联赋能　　融通创新

2019工业互联网峰会
INDUSTRIAL INTERNET SUMMIT 2019

目录
Contents

新的安全挑战

	设备	控制	网络	数据	应用
需求变化	大量智能设备出现，集成通用嵌入式操作系统及应用软件，可实现感知，决策，控制等功能	高度融合IT技术的工业控制系统使控制环境更开放。	生产网络将统一为以IP为核心的物理网络，并与办公网络，互联网等互联互通。	数据在IT、OT，以及生产网络外流动，打破了企业内部各环节和企业间的连接壁垒。	网络化协同、服务化转型、个性化定制等新应用模式不断涌现，企业将越来越多应用部署在云端，并采用大量工业APP
安全挑战	设备弱口令、漏洞、大量开放端口；设备网络协议多样，存在大量漏洞；设备众多，存在违规接入的风险	软件、硬件、协议的风险；现场与远程运维带来的风险；无线通讯带来的风险协议的风险；系统漏洞无法经常更新	“两网连接”带来的风险身份验证问题，凭证被盗；攻击面加大；恶意内部人士；APT攻击；DDOS攻击	数据泄露 永久的数据丢失 共享数据导致共享风险	内部泄密行为 各类系统存在的安全漏洞；恶意、垃圾邮件的威胁；WannaCry等恶意代码的威胁

工业互联网安全问题

漏洞

工控系统曝光的漏洞数量从2010年的55个发展到当前的1061个
半数以上为高危漏洞。
（数据来源：NVD、CVE、CNVD及CNNVD等主流数据库）

攻击

针对工业控制系统的攻击事件也一直处于高位，2011年200余起，
2012年248起，2013年248起，最近五年每年约300起
(数据来源：美国工控应急响应中心ICS-CERT）

病毒

2018年8月3日，台积电遭遇病毒袭击，直接经济损失2.5亿美元；2017年“Wanna Cry”勒索病毒入侵全球150个国家，多国能源、通信等重要行业损失惨重。2010年伊朗核设施遭受“震网病毒”攻击

设备暴露

截止2018年5月，国内范围内，暴露在互联网上的工业控制系统设备数量达97625个

工业互联网基础设施缺芯少魂

工控系统/操作系统

全国5000多个重要的工业控制系统中
95%以上的工控系统操作系统均采用国外产品
（数据来源：中国产业信息研究网调查统计结果）

工控系统/PLC

逻辑控制器PLC95%是来自施耐德（法国）、
西门子（德国）、发那科（日本）等的国外品牌。

基础软件

中间件国外产品超过70%
PC端和服务器端操作系统，微软超过90%
数据库，甲骨文，微软，国际商业机器等国外产品超过90%

芯片

国产化率低于1%。

工业互联网安全保障体系总体建设内容

自主可控 安全可靠	工业现场安全防护	工控防火墙	工业审计	工业主机防护
		工业网闸	工业安全态势感知	
	云平台安全防护	云数据库安全	云应用安全	云主机安全
		虚拟网络安全	云资源安全	物理资源安全
	云基础设施安全	虚拟智能化	云操作系统	数据库云平台
		超级服务器	负载均衡	分布式存储
	安全服务	安全评测	安全风险评估	安全咨询
		安全培训	攻防演练	

01 工业互联网实现了设备、工厂、人、产品的全方位连接，因此工业互联网安全建设必须从云基础设施安全，安全防护（设备与云平台），安全运维（制度），安全服务（服务）的整体视角统筹规划

02 构建工业互联网安全保障体系需要从自主可控开始，各个层面都要围绕着自主可控，安全可靠开展

云基础设施安全

超级服务器	国内首款高性能安全可靠超融合系统，采用2路ARM64 Hi616处理器，具有高性能、低功耗、高兼容、灵活扩展等特点
数据库云平台	具有事务强一致性、灵活横向扩展能力，具备超大规模单一实例，无须分库分表可高度兼容 Oracle,去IOE
分布式存储	提供基于通用硬件平台的、低成本的、具有高度可伸缩性的云存储解决方案。
负载均街系统	具有丰富的功能、卓越的处理性能和系统稳定性。果用航天天域负载均衡系统整体解决方案，使企业部署数据中心和云计算的成本降低三分之一，可用性提升五倍，效率提升三倍，以及高度安全
虚拟智能化平台	基于裸金属架构，采用高性能的虚拟化内核，真正实现计算、网络、存储、安全虚拟化的全面融合。
云操作系统	提供包括云资源、云用户、云服务、云运营、云运维在内的多种云管理功能。

自主可控、安全可靠是云基础设施安全的保障

云平台安全和云租户安全服务

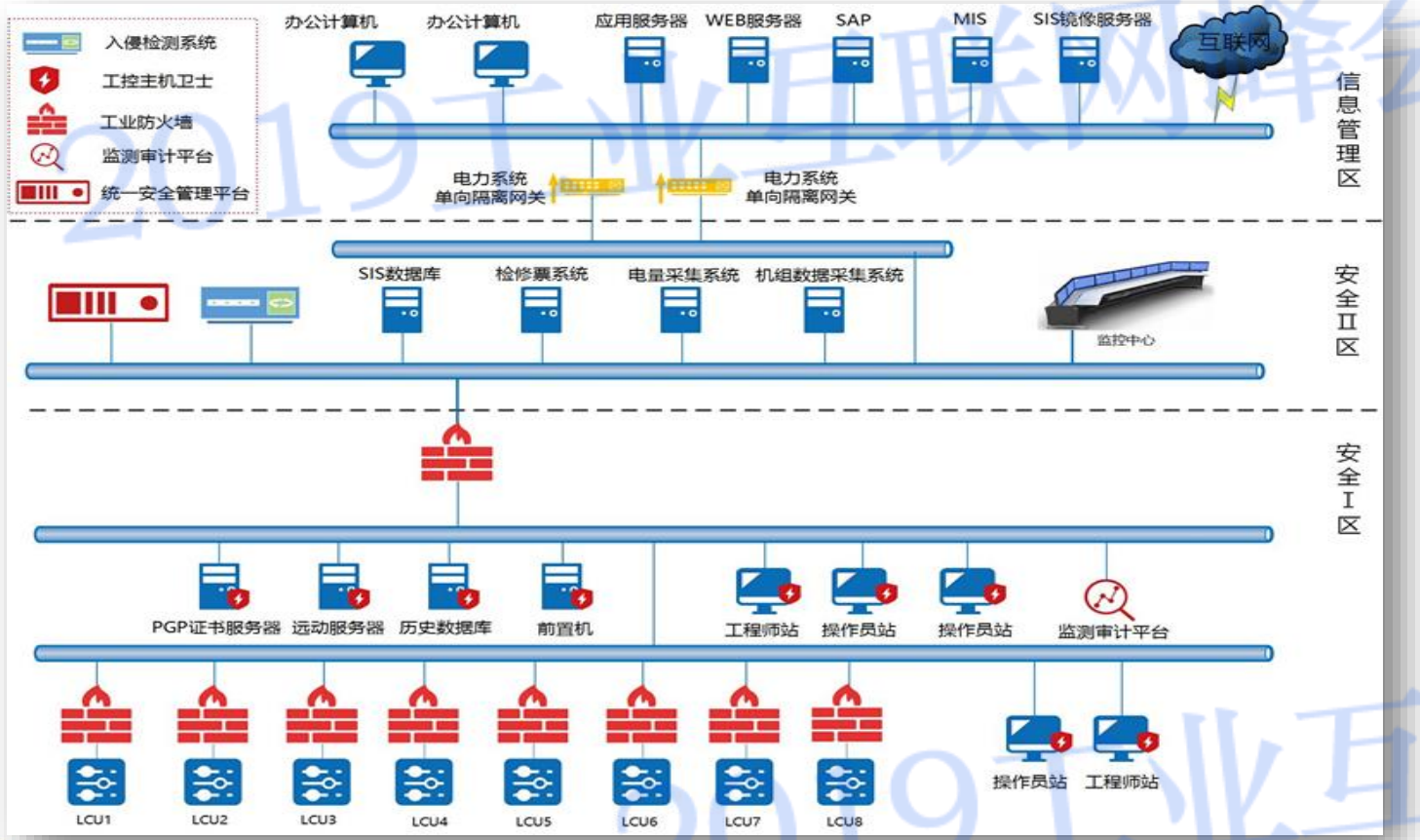
云租户安全服务	数据安全服务	DB扫漏	DB防火墙	DB审计	数据库加密	数据备份与恢复		安全运维体系		
	应用安全服务	Web扫漏		WAF		Web审计安全				
	网络安全服务	网络扫漏	主机微隔离	DDOS防护		网络安全审计				
	主机安全服务	系统扫漏	主机EDR	虚拟防病毒		主机安全服务				
云平台基础安全	云资源安全	态势感知		综合安全管理平台		统一身份认证		运维监控	应急响应	
		DDOS防护	防火墙	IPS/IDS	网络日志审计	WAF	数据库防火墙	防病毒		
	物理资源安全	宿主机和物理网络安全	边界NGFW	边界IPS	堡垒机	宿主机IPS	DPI			
		机房与环境安全	机房位置	防火	防潮	防雷	防盗	电力安全		

云平台自身安全和租户业务安全缺一不可

云平台安全以**云安全防护、云安全运维、云安全监测、云安全服务**为闭环解决思路，向用户提供**合法合规**、防护有效、简单易用、灵活扩展的云安全方案；

云租户安全服务(Security as a Service)可以以**按需使用，按使用量付费**的方式向云平台的租户提供安全服务。

工业现场安全



1. 自主可控
2. 纵向分层，横向分区
   做好隔离与边界防护
3. 基于白名单的权限设置
4. 信息管理区要做好
   病毒防护和人员安全管理
5. 故障备份和恢复软件

工业互联网安全保障体系迭代过程

安全保障体系建设不是一次建设，安枕无忧，而是持续分析，迭代改进的过程

工业互联网安全需要从被动防护到主动防护，定期做好风险评估，对攻击做好预测与预案

工业互联网安全保障体系体系生态建设

航天云网与业内专业厂商形成了长期的合作伙伴关系，共同建设工业互联网安全保障体系

工业互联网产业联盟
Alliance of Industrial Internet

Thanks

主讲人：穆森

2019年2月22日

智联赋能　融通创新

2019工业互联网峰会
INDUSTRIAL INTERNET SUMMIT 2019