

工业互联网安全攻防战

策划编辑 | 孟圆

随着“新基建”战略的发布和“两会”的召开，“工业互联网”在产业界的热度持续攀升，也引起了更多的讨论。《2020年国务院政府工作报告》提出，重点支持“两新一重”（新型基础设施建设，新型城镇化建设，交通、水利等重大工程建设）建设，对于“新基建”、工业互联网建设也作出重要指示：推动制造业升级和新兴产业发展。支持制造业高质量发展。大幅增加制造业中长期贷款。发展工业互联网，推进智能制造，培育新兴产业集群。

中国信息通信研究院副院长、工业互联网产业联盟秘书长余晓晖表示：“随着我国工业互联网创新发展战略深入推进，从中央到地方持续掀起工业互联网建设及推广热潮，工业互联网三大体系基本建成，新兴产业持续壮大，行业应用水平持续提升，具体体现在四个方面：一是网络基础设施建设初见成效，互联互通水平持续提升；二是各类主体积极开展平台建设，典型平台实力逐步提升；三是安全实践不断深入，安全产业蓬勃发展；四是融合应用体系初步建成，行业赋能作用逐步显现。

工业互联网安全

工业领域的安全一般分为三类，信息安全（Security）、功能安全（Functional Safety）和物理安全（Physical Safety）。传统工业控制系统安全最初多关注功能安全与物理安全。与传统的工控系统安全和互联网安全相比，工业互联网安全打破了以往相对明晰的责任边界，其范围、复杂度和风险度更大，其中工业互联网平台安全、数据安全和联网智能设备安全等问题越发突出。

工业互联网安全是工业信息安全的核心，与传统的信息安全保护企业信息资产与数据资产不同，工业互联网安全直接决定工业生产安全，更关乎经济发展、社会稳定乃至国家安全。

从核心要素的角度来看，工业互联网安全包括智能设备安全、智能系统安全和智能决策安全。其中智能决策安全主要体现在工业互联网平台安全。随着智能制造以及工业互联

网的发展,工业控制系统正朝着高度信息化方向发展,越来越多的工控系统及设备接入互联网,让更多的网络攻击手段有了可乘之机,网络空间中的安全问题开始延伸到工控系统中。网络、平台和安全是工业互联网三大功能体系,而工业互联网安全是工业互联网业务目标达成、功能正常运行和建设顺利实施的重要保障。

新一代信息技术在加速信息化与工业化深度融合发展的同时,也带来了日趋严峻的信息安全问题。工业信息化、自动化、网络化和智能化等基础设施是工业的核心组成部分,是各行业、企业的神经中枢。工业互联网安全的核心任务就是要确保这些工业神经中枢的安全。工业互联网安全事关经济发展、社会稳定和国家安全,是网络安全的重要组成部分。从内容来看,工业互联网安全涉及工业领域各个环节,包括工业控制系统信息安全(简称工控安全)、工业大数据安全、工业云安全和工业电子商务安全等内容。

随着 IT 与 OT 加速融合一体化,工业互联网的快速发展为工业信息系统的整体安全防护带来更大的挑战。工业和信息化部网络安全管理局副局长杨宇燕表示:“互联网和工业的深度融合,打破了传统工业领域相对封闭可信的环境,将互联网的安全威胁渗透进工业领域。网络攻击直达生产一线。目前,工业互联网平台安全、工业网络基础设施安全、工业数据安全以及 IT 和 OT 的融合安全等领域的技术研究和产品应用均处于起步阶段,但随着防护对象保障需求的变化,工业信息安全产业的边界也将不断延伸扩展。”

工业互联网安全相关政策

◎ 《关于深化“互联网+先进制造业”发展工业互联网的指导意见》

◎ 《工业互联网发展行动计划(2018~2020年)》

◎ 《加强工业互联网安全工作的指导意见》

◎ 《工业互联网企业网络安全分类分级指南(试行)》

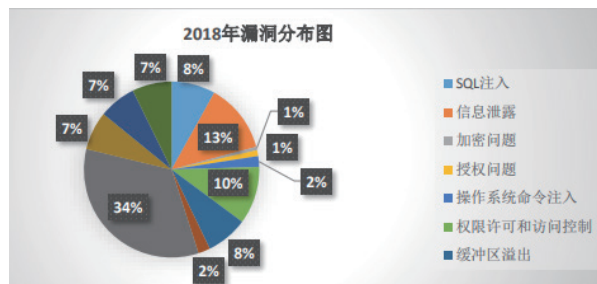
2019年8月,工信部等十部门联合印发《加强工业互联网安全工作的指导意见》,明确了工业互联网安全的指导方针和总体目标,到2020年底工业互联网安全保障体系初步建立;到2025年,制度机制健全完善,技术手段能力显著提升,安全产业形成规模,基本建立起较为完备的工业互联网安全保障体系。

为结合我国具体情况与国际形势进一步落实《指导意见》,工信部明确了推动工业互联网安全责任落实、构建工业互联网安全管理体系、提升企业工业互联网安全防护水平、强化工业互联网数据安全保护能力、建设国家工业互联网安全技术手段、加强工业互联网安全公共服务能力和推动工业互联网安全科技创新与产业发展七方面主要任务。

工业和信息化部总经济师王新哲指出,加强工业互联网安全工作,是落实国家总体安全观、保障“两个强国”建设的关键举措,是抢占新一轮工业革命发展制高点、加强网络安全工作的重要基石,是应对日益复杂网络安全形势、筑牢网络安全防线的必然要求。

工业互联网安全发展现状

工业互联网安全产业潜力巨大。根据工信部测算,我国工业互联网安全产业存量规模由2017年的13.4亿元增长至2019年的27.2亿元,年复合增长率高达42.3%,远高于传统安全市场。



2018年漏洞分部图

来源:《中国网络安全态势报告》

从产业层面看,工业互联网厂商开始入局工业互联网安全领域。微软以1.6亿美元收购以色列工业网络安全初创公司CyberX。而传统安全厂商,如fortinet、veritas和卡巴斯基等纷纷推出针对工业互联网的解决方案。



以色列工业网络安全初创公司 CyberX

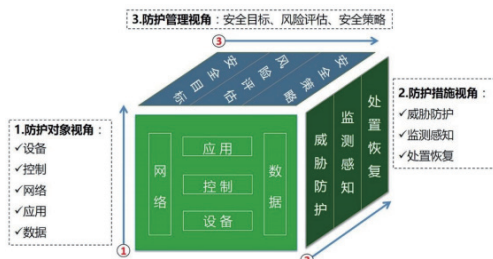
工业互联网安全参考构架

工业互联网安全工作需要从制度建设、国家能力和产业支持等更全局的视野来统筹安排,目前很多企业还没有意识到安全部署的必要性与紧迫性,安全管理与风险防范控制工作亟需加强。

六方云结合自身对工业互联网以及工业信息安全的深刻理解和当前工业互联网安全的普遍需求,参考中国工业互联网产业联盟发布的《工业互联网体系架构(版本2.0)》、《工业互联网安全架构》、美国工业互联网安全参考架构(IIRA G4)和美国国土安全部发布《物联网安全指导原则》,于2020年5月26日正式发布六方云《工业互联网安全架构白皮书V1.0》。



六方云《工业互联网安全架构白皮书 V1.0》

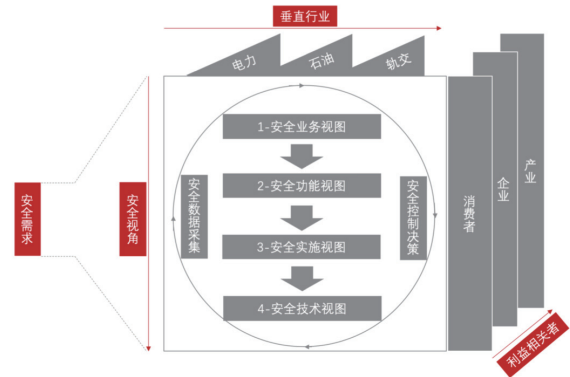


工业互联网安全框架

来源:《中国工业互联网安全态势报告(2018)》

此白皮书给出了具有前瞻性的工业互联网安全定义及内涵,从安全需求、安全视角、相关者及垂直行业应用四个方面阐述了工业互联网安全的体系结构及应用场景,创造性地抽象出指引未来工业互联网安全建设的五维安全视图架构,即安全业务、安全功能、安全实施、安全技术和数据安全,并系统地阐述了工业人工智能安全如何赋能工业互联网安全建设以及工业5G安全需求与技术实现路线。

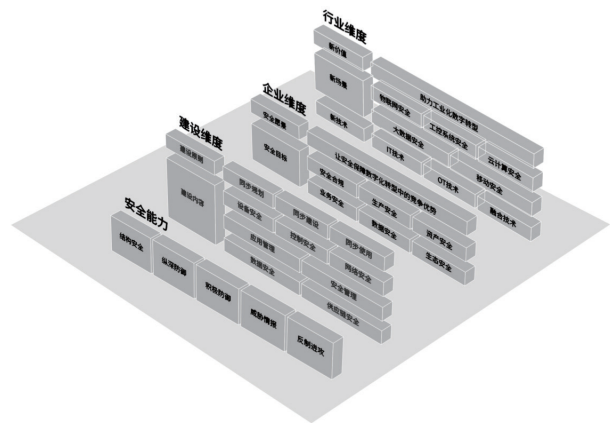
白皮书从三个工业互联网安全现状出发,提出七大工业互联网技术发展趋势,最终得出工业互联网安全五大核心需求:工业企业的资产安全、业务安全、生产安全、生态安全



六方云工业互联网安全架构

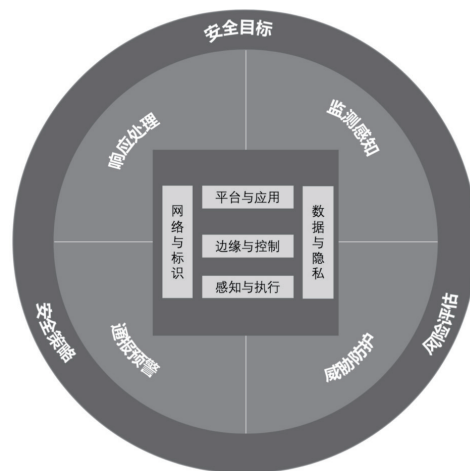
和数据安全;安全业务视角从五个维度进行了阐述:

1. 业务视图: 从产业、企业、建设和能力四个维度阐述。



业务视图

2. 安全功能视图: 从防护对象、防护措施和安全管理三个维度阐述了工业互联网建设要实现的功能



安全功能视图

工业互联网平台架构图展示了从设备层到产业工业层的完整架构。该图分为五个主要层级：产业工业层、企业信息层、边缘层、设备层以及工业互联网平台层。在产业工业层，骨干网络与国家安全防护中心相连。企业信息层包含企业/园区网络和省/行业级安全平台。边缘层则包括边缘控制设备和边缘系统。设备层列出了PLC、传感器、执行器和通信设备等。工业互联网平台层作为核心，包含国家级平台、企业级平台和边缘系统。图中还详细标注了标识解析的各级节点，从国家级节点到企业级节点，再到标识解析中间件和标识数据采集设备，体现了标识解析体系的全覆盖。

- 21 -

六方云工业互联网安全体系



六方云工业互联网安全体系

致力于提供关键信息基础设施保护、工业互联网安全产品和解决方案。

六方云工业互联网安全体系基于“AI基因、威胁免疫”的安全理念，首先设定建立了“可信连接、智能防护、安全互动”的主动防御安全体系总体目标，包括主动检测、主动保护、主动预测和主动响应四个子目标；其次从规划体系、管理体系、技术体系和产品体系四大维度进行应用实践。六方云拥有四大核心技术：OT与IT融合安全技术、工控安全虚拟补丁技术、工业企业上云安全技术和人工智能安全。

工业互联网安全态势监测与感知将成为重要技术手段

2019年12月9日，在2019年中国网络安全产业高峰论坛上，国家工业互联网安全态势感知与风险预警平台正式发布。该平台通过主动探测与流量分析相结合的方式，充分利用行业监管数据资源优势，实现多维感知安全态势、及时预警风险信息、多元汇聚基础资源等功能，依托“国家-省-企业”三级架构，形成“全国一盘棋”的工业互联网安全风险实时监测、动态感知和快速预警的监测保障体系。

当前，工业互联网蓬勃兴起，安全技术防护体系亟待

同步构建，需要发挥政府、市场和企业力量，加大资金投入和统筹设计，鼓励创新，推动工业互联网安全防护整体能力的提升，防范化解网络安全风险。IM