中国工业信息安全
产业发展白皮书
（公开版）

工业信息安全产业发展联盟（NISIA）
二〇一八年五月

前言

工业信息安全产业肩负着为我国工业自动化和信息化基础设施和信息系统的安全保障提供安全产品和服务的重要任务，是制造强国和网络强国建设的重要支撑，是保障国家网络安全的重要基础。当前，日益复杂严峻的工业信息安全形势引发全球关注，世界各国政府与产业界高度重视工业信息安全，不断加大安全投入，工业信息安全产业迎来发展机遇。

“十三五”以来，党中央、国务院科学构建工业信息安全战略布局，以《网络安全法》为基础，出台了一系列法规政策、战略规划和指导意见，强化企业的安全主体责任，明确工业信息安全工作的方向和目标，工业信息安全产业发展环境不断优化。2017 年，我国工业信息安全市场规模达 5.57 亿元，较 2016 年增长 53.6%，工业信息安全产业发展进入“快车道”。在工业互联网、工业云、工业大数据等产业发展需求的带动下，工业信息安全领域的技术和产品创新升级，威胁情报、态势感知、安全可视化、虚拟化等新技术不断涌现，以边界安全、监测审计为代表的工业信息安全产品市场增长迅猛，工业信息安全企业加速布局，市场竞争格局逐渐形成。

放眼全球工业信息安全形势，立足我国工业信息安全产

业发展现状，国家工业信息安全发展研究中心联合 360 企业安全集团、启明星辰、威努特、烽台科技、天地和兴等企业共同编写了《中国工业信息安全产业发展白皮书》。该白皮书是国内首份全面系统深入研究分析我国工业信息安全产业发展的报告，在梳理了 2017 年全球和我国工业信息安全产业发展状况的基础上，重点对产业规模结构、政策环境、技术发展、行业应用及市场竞争格局等进行深入分析，剖析我国工业信息安全产业发展面临的挑战，并对产业发展趋势进行了展望。由于时间关系，报告尚有不足之处，敬请指正。

工业信息安全产业发展白皮书编写组

2018 年 5 月

目录

第一章 工业信息安全产业的范畴

一、工业信息安全的内涵和产业范畴

当前，以移动互联网、云计算、大数据、物联网和人工智能等为代表的新一代信息技术与制造技术加速融合，推动着制造业向数字化、网络化、智能化、服务化方向发展，成为推动经济转型升级、新旧发展动能接续转换的强劲引擎。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、智能化等基础设施是工业的核心组成部分，是工业各行业、企业的神经中枢。工业信息安全的核心任务就是要确保这些工业神经中枢的安全。工业信息安全事关经济发展、社会稳定和国家安全，是网络安全的重要组成。

从内容来看，工业信息安全泛指工业运行过程中的信息安全，涉及工业领域各个环节，包括工业控制系统信息安全（以下简称工控安全）、工业互联网安全、工业大数据安全、工业云安全、工业电子商务安全等内容。

根据普渡参考模型，工业企业信息系统架构可以分为企业网络层、信息管理层、生产管理层、过程监控层、现场控制层、现场仪表/设备层（图 1.1）。从安全防御技术成熟度来看，工业领域各行业在信息管理层的信息安全防护发展较早，

技术和产品上都相对成熟。

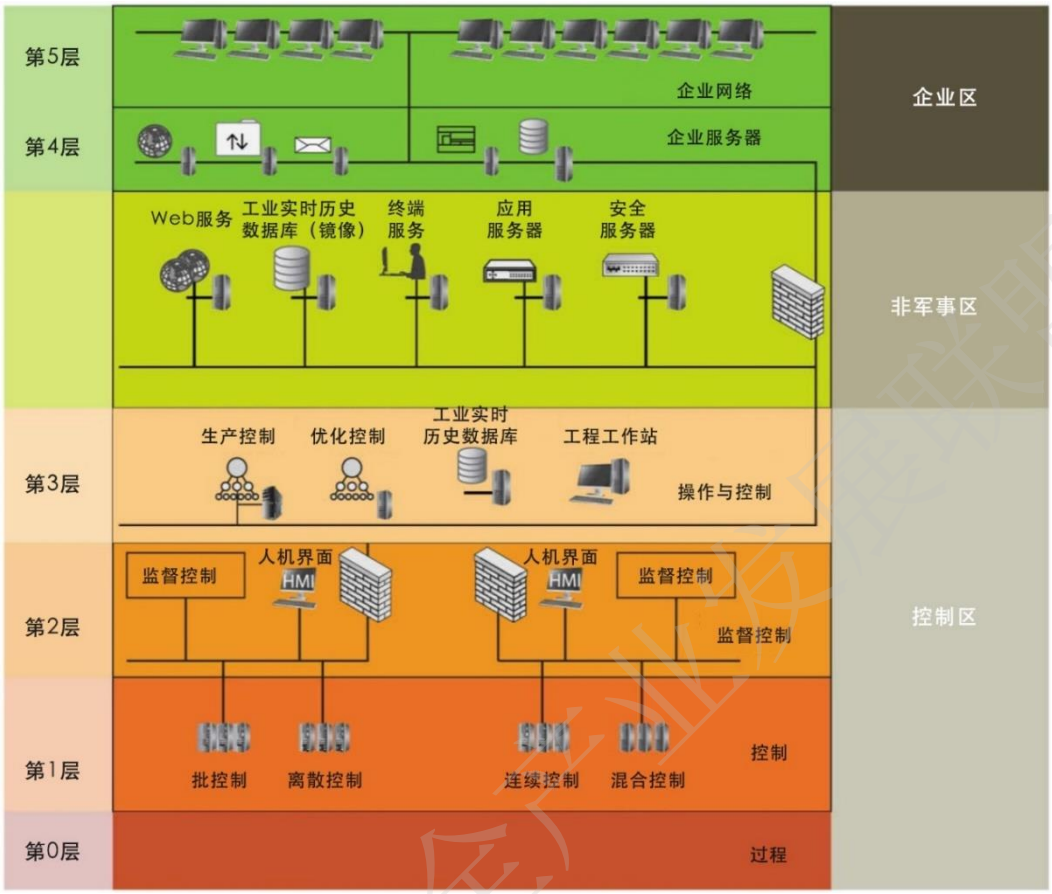

图 1.1 工业企业普度参考模型（Purdue Model）

资料来源：工业信息安全产业发展联盟综合分析

工控安全或以资产为中心的操作技术（OT, Operational Technology）安全主要指生产管理层、工业控制层及现场设备层所涉及的信息安全防护。Gartner 在 2017 年的《OT 安全市场指南》中，指出工业信息安全市场重点关注的操作运行系统包括数据采集与监控系统（SCADA）、过程控制网络（PCN）、离散控制系统（DCS）、制造执行系统（MES）、远程信息处理、机器人、设施管理、建筑自动化系统（BAS）、交通运输管理系统等。据 Gartner 于 2017 年发表的 OT 技术成熟度曲

线（图 1.2），全球 OT 安全目前正处于泡沫化的底谷期，距离市场的广泛应用将有 2-5 年的时间。

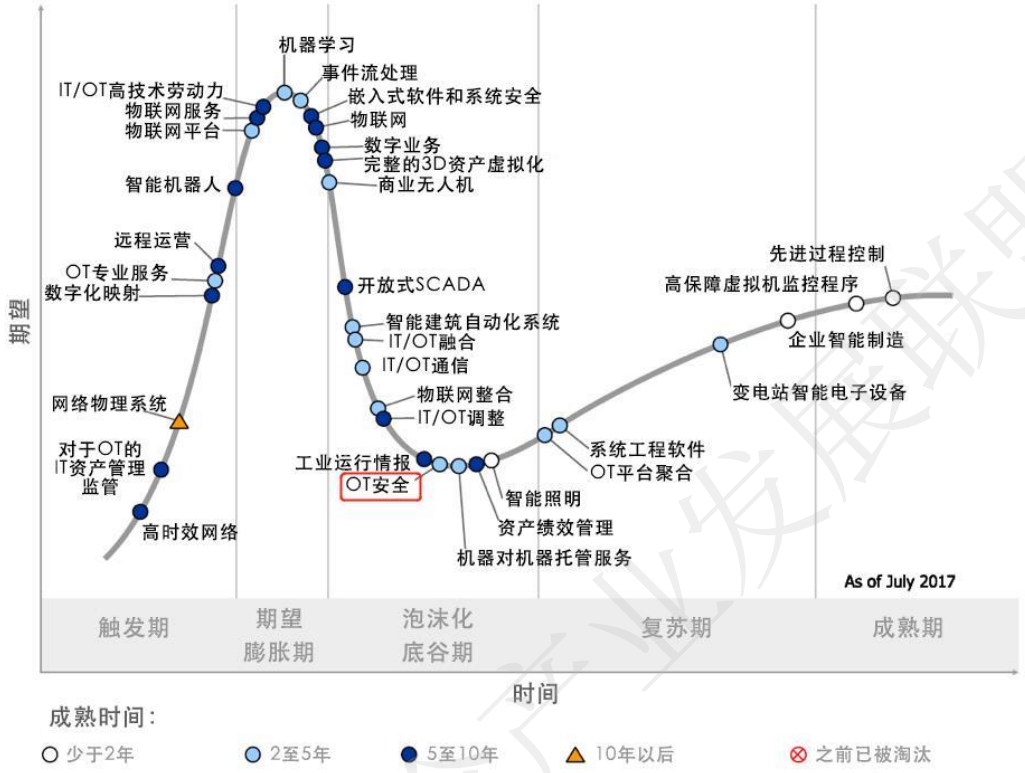

图 1.2 Gartner 的 OT 管理技术成熟度曲线（2017）

资料来源：Gartner，工业信息安全产业发展联盟综合分析

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。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/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。

结合工业信息安全的内涵和传统信息安全产业的范围，工业信息安全产业主要是指从事工业运行过程中的信息安

全技术研究开发、产品生产经营和提供相关服务的经济活动。其中，以满足工业企业安全生产需求为核心、自身含有工业信息安全功能的工业控制系统的技术研究开发及产品生产销售也在工业信息安全产业范畴中，但不包含在本报告产业测算范围内。

二、工业信息安全产业结构分类

随着新一代信息技术的快速发展，工业信息安全产业结构不断变化，软硬件产品的界限越发模糊，产品和服务的联系愈加紧密。在借鉴 Gartner 和 ARC 咨询公司对市场主要产品和服务的分类的基础上，结合我国实际，工业信息安全产业发展联盟基于自身对产业结构的理解，依据市场主流应用将工业信息安全产业结构分为产品和服务两大类，如图 1.3 所示。

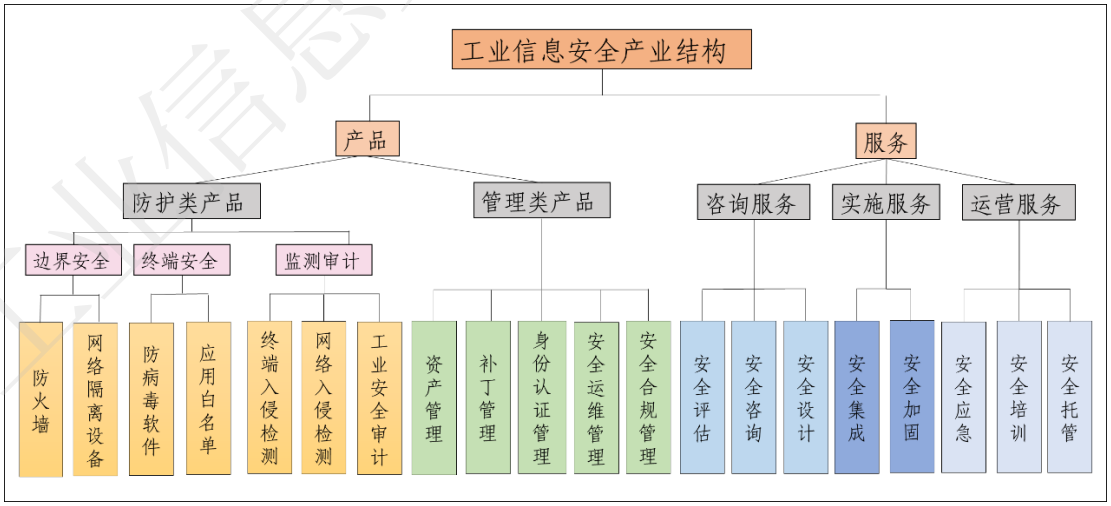

图 1.3 工业信息安全产业结构

资料来源：工业信息安全产业发展联盟综合分析

（一）产品类

与传统计算机网络安全相比，工业信息安全在保障对象、安全需求、网络和设备环境、通信协议等方面具有特殊性。识别工业企业信息系统存在的风险与安全隐患，并对应实施相应的安全技术与管理保障策略是确保工业信息安全的重要手段。从市场发展来看，针对工业企业用户的信息安全需求，工业信息安全产品类市场主要分为两类：防护类产品与管理类产品。

从技术防护的角度，工业信息安全防护类产品包括边界安全产品、终端安全产品及监测审计类产品。其中，边界安全产品以工业防火墙和网络隔离设备为代表，主要用于保护工业网络边界并提供区域隔离；终端安全产品涵盖了能够在工业信息安全环境下，防护所有终端设备的安全产品，如防病毒软件、应用白名单、端口设备控制、主机加固等；监测审计类产品主要用于监控和评估工业控制系统的完整性，典型产品包括终端入侵检测、网络入侵检测和工业安全审计等。

从安全策略和管理流程的角度，工业信息安全管理类产品包括资产管理、补丁管理、身份认证管理、安全运维管理和安全合规管理几大类，旨在帮助企业管理和维护工业资产和设备安全态势。由于工业企业用户的安全需求侧重于生产或运行过程的可靠性，工业信息安全管理产品结合了传统 IT 网络安全管理产品和解决方案，但限制了会对工业生产环境

造成影响的功能模块。同时，工业信息安全管理产品还将覆盖范围扩展到其他工业资产和控制协议。

（二）服务类

工业信息安全服务主要指工业企业购买的第三方安全服务。通过对工业信息安全服务市场发展驱动因素的分析，根据安全服务对象及企业用户项目管理生命周期，安全服务可以分为三大类。一类是以安全评估、安全咨询、安全设计为代表的咨询服务，该类服务主要依托专家的知识体系和行业经验并依据国内外标准和行业监管规范，建立工业信息安全管理体系，为用户提供决策依据和优化方案。第二类是以安全集成和安全加固为代表的实施服务，该类服务主要采取适当的管理过程和控制措施，通过产品和解决方案将工业信息安全管理体系落地实施。最后一类是以安全应急、安全培训和安全托管为代表的运营服务，旨在为工业企业提供满足其全生命周期安全运营和管理需求的服务。

第二章 全球工业信息安全产业概况

一、全球工业信息安全市场规模稳定增长

随着工业信息系统的不断开放和互联互通，工业控制系统及工业物联网设备的安全脆弱性逐渐凸显。日趋频繁的网络威胁和攻击、对智能制造安全防护投资的增加以及各国政府对工控安全的持续关注等多种因素都对全球工业信息安全市场的快速增长起到了推动作用。据市场研究公司 Markets and Markets 分析，2017 年工业信息安全市场规模达 138.1 亿美元，预计在 2023 年增长至 227.9 亿美元，年复合增长率达 8.6%。其中，全球工业控制系统信息安全市场规模为 102.4 亿美元，预计未来五年的年复合增长率为 6.3%，占全球工业控制及自动化市场规模的 7%。

从区域分布来看，据 Markets and Markets 预测，由于化工行业和制造业需求的激升，北美地区工业信息安全市场规模在 2017 年仍保持全球领先地位。另据市场研究公司 Research and Markets 预测，未来五年，中东和非洲地区的工业信息安全市场规模将快速增长，年复合增长率达 8.4%；欧洲和北美地区的工业信息安全市场规模将进一步扩大，年复合增长率分别为 7.7%和 4.5%。2017 年，弗若斯特沙利文公司（Frost&Sullivan）通过工业控制系统网络协议检测发现，亚太地区与工业控制系统相关的联网设备有 83929 个，其网

络安全保护需求日益明显。该公司预测，亚太地区的整体工控安全市场规模将从 2015 年的 3.84 亿美元激升至 2020 年的 16.3 亿美元，涨幅超 4 倍，其中，日本和大中华地区（Greater China）年复合增长率都达 50%以上（图 2.1）。

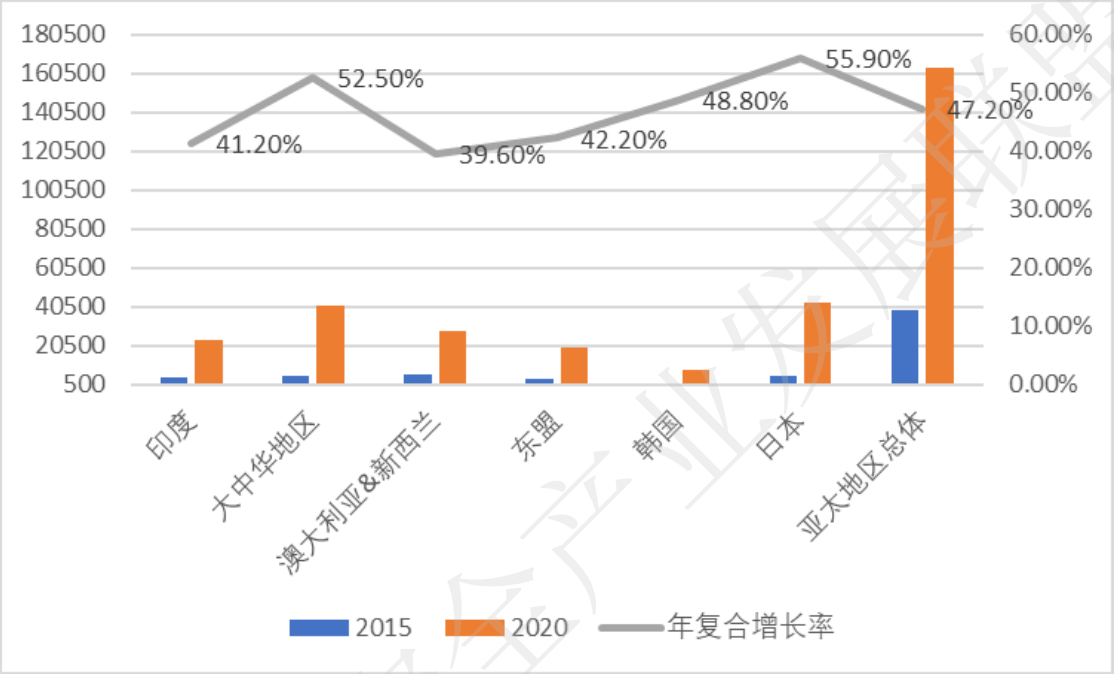

图 2.1 亚太地区工控安全市场规模和增长情况（2015-2020）

数据来源：Frost & Sullivan，工业信息安全产业发展联盟综合分析

从行业应用来看，工业领域知名咨询公司 ARC 认为，电力行业、石油天然气行业以及化工和石化行业 2017 年在工业信息安全市场的投入仍将保持市场领先地位（图 2.2）。其中，受《大型电力系统的网络安全标准》（NERC-CIP）等合规标准影响，电力行业工业信息安全市场将以年复合增长率 13.38%保持强劲增长。同时，全球对基础设施安全问题的不断关注也是驱动水处理行业的工业信息安全市场投入的主要动力，其年复合增长率达 12.76%。另据 Markets and Markets

预测，在交通运输关键基础设施中，由于航空与海运部门的工业控制系统近两年来频繁受到网络安全威胁，其工业信息安全需求将快速增长，预计未来五年，交通运输行业的工业信息安全市场规模将不断扩大。

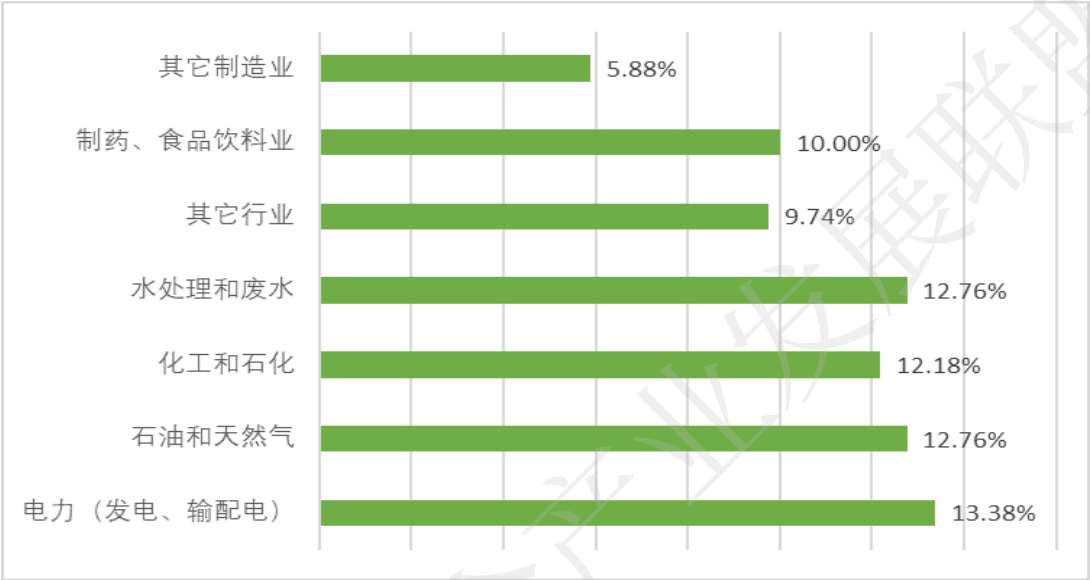

图 2.2 各行业工业信息安全投入年复合增长率（2015-2020）

数据来源：ARC 公司，工业信息安全产业发展联盟综合分析

从产业结构来看，2017 年终端安全领跑全球工业信息安全市场，市场份额达 47%；以工业防火墙、路由器、工业以太网交换机为代表的网络安全类排名第二，市场占有率为 33%，预计在未来五年里增速最快；应用安全、数据安全及工业云安全市场占有率为 20%。其中，由于下一代防火墙技术具有综合网络入侵防御、应用感知和深度包检测等功能，工业防火墙产品及相关解决方案在未来五年将占据工业信息安全市场主导地位。

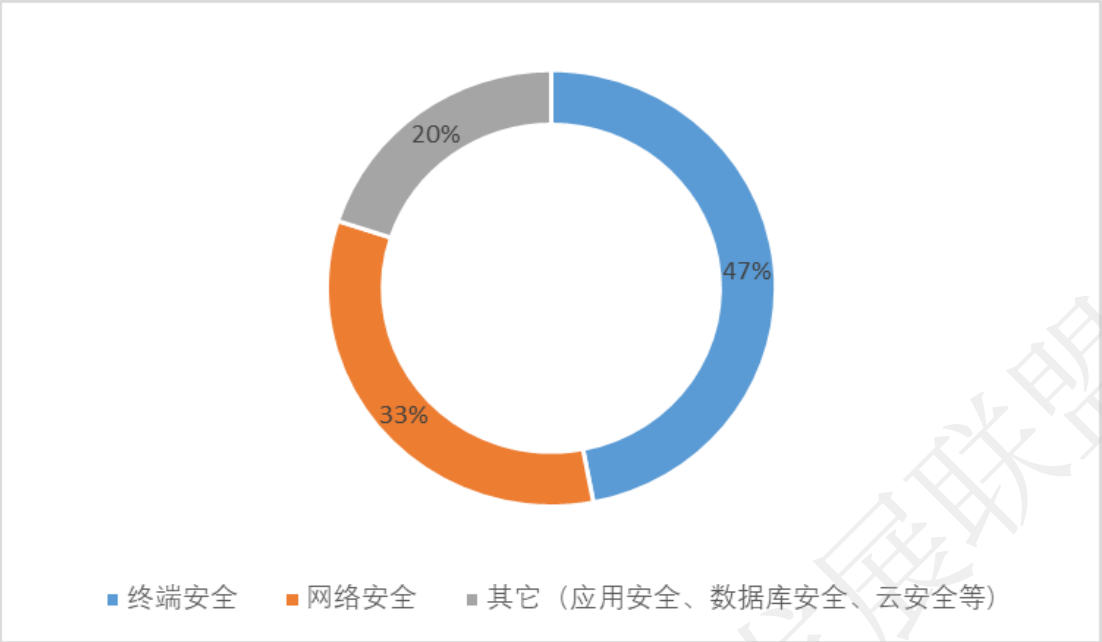

图 2.3 2017 年全球工业信息安全市场产业结构情况

数据来源：Markets and markets，工业信息安全产业发展联盟综合分析

二、主要国家产业政策向好，战略性投入升级

作为网络安全产业的领导者，美国在工业信息安全领域布局较早。美国政府高度重视工业信息安全顶层战略设计，并且已经形成分工明确、相互协作的管理组织机构。美国国土安全部（DHS）、美国国防部（DoD）及美国司法部（DOJ）作为三个最主要的联邦网络安全机构，于 2014 年合作成立了网络响应小组，并从行政管理、执法调查、国防情报等多个方面对 ICS/SCADA 的网络安全形成保障。国土安全部还专门设立了工业控制系统网络应急响应小组（ICS-CERT），着力解决工业控制系统网络安全领域的态势感知、脆弱性协调、事件响应和公私合营等问题。

相比美国而言，欧洲在工业信息安全领域的管理组织和相关政策制定方面起步较晚。2011 年，欧盟网络与信息安全局（ENISA）发布《保护工业控制系统—对欧洲及其成员国的建议》，正式开启对工业信息安全领域的系列研究。2017 年 2 月，ENISA 公布了《ICS-SCADA 系统通信网络依赖》报告，旨在提升欧盟各成员国关键基础设施领域 ICS/SCADA 系统和通信网络功能的安全水平及弹性。

与西方发达国家不同，以色列地处战乱不断的中东地区，常年不间断的网络攻击促使以色列政府大力发展网络安全防御技术，在短短二十多年内成功跻身网络安全强国。近年来，以色列在工业信息安全领域表现尤为亮眼，不仅拥有多家世界领先的工业信息安全厂商，在工业信息安全产业政策和生态环境上也不断创新升级。以色列创新的军民融合机制和长期的网络安全技术储备，使以军事信号情报组织 8200 部队（Unit 8200）和以色列国防部（IDF）经营网络安全部门为代表的军方成为工业信息安全企业的孵化器和加速器。此外，以色列的资本市场在工业信息安全领域的活跃度高，也推动了企业的快速发展。

三、全球工业信息安全技术创新升级

IT 信息安全领域经过多年的发展，形成的新理念和新成果为工业信息安全的技术发展提供了重要借鉴和参考。同时，

安全威胁的复杂化和多样化以及工业企业用户不断升级的安全需求也驱动了全球工业信息安全技术的迭代和创新。积极防御、威胁情报、态势感知、数据驱动安全、安全可视化等新理念在工业信息安全领域不断推广应用，大数据、人工智能等新技术从概念走向落地。

从国际工业信息安全企业技术和产品的布局上，全球工业信息安全技术主要聚焦在主动防御、安全自动化、新兴互联网技术在工业信息安全领域的融合应用以及内嵌安全设计等方面，呈现如下发展特征:

（一）持续监测需求促进主动防御技术发展

由合规需求驱动的工业信息安全产品和服务投入在近年来增长迅速，被动防御技术得到广泛应用。但面对非传统且针对性更强的网络攻击时，单纯依靠被动防御技术已不能满足需求，采用更为专业的持续监测和异常管理等积极防御手段将至关重要。ARC 在 2017 年开发了“工业控制系统网络安全模型”，将工控安全分解为单个设备的安全防护、外部攻击防御、访问控制、监控可疑活动和主动管理复杂的威胁和网络事件等一系列步骤（图 2.4）。该模型强调了基于环境的异常检测和威胁情报驱动的积极防御技术在工业信息安全应用中的重要性。以 Dragos 公司为代表的厂商，已经开始采

用情报驱动的积极防御技术来检测和分析工业信息安全威胁，为客户提供事件响应措施。

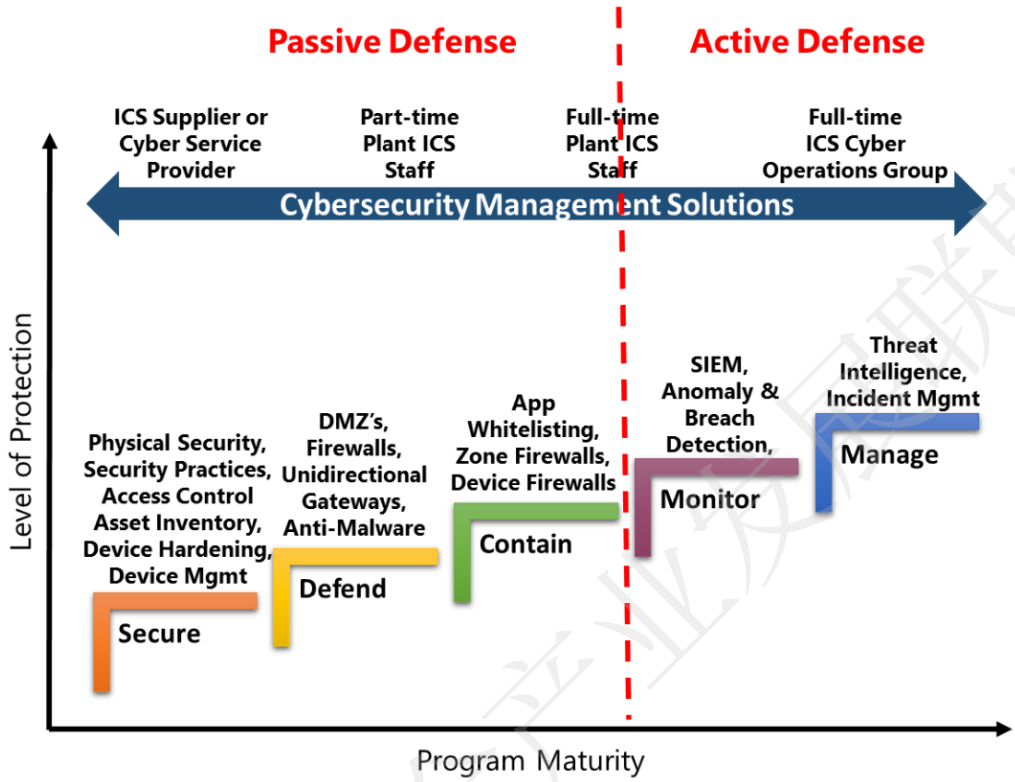

图 2.4　工业控制系统网络安全成熟度模型

数据来源：ARC 公司，工业信息安全产业发展联盟综合分析

（二）人才短缺大幅推动安全自动化技术

当前，全球工业信息安全市场人才紧缺的问题正加速推动人工智能（AI）技术在网络安全领域从概念走向落地，工业企业用户将更广泛的采用含有 AI 技术的工业信息安全解决方案来实现安全和生产力目标。含有 AI 功能的工业信息安全监测工具可以自动化发现工控环境中的违规行为、提供补救信息。以 US-CERT 对“Dragonfly 2”的建议为例，安全措施包括检查 17 个不同的日志库和存储库来识别恶意软件

的迹象，使用自动化威胁检测解决方案将大幅提升检查时间。

（三）新兴互联网技术与安全技术融合应用

传统的安全防护手段正在不断被黑客进行挑战，机器学习算法和区块链等新兴互联网技术的出现为工业信息安全领域提供了新的防护理念和新视角。以色列工业信息安全公司 SIGA 使用机器学习算法和预测分析技术来实时检测由网络攻击或技术故障导致的异常情况，并与外部网络和通信完全隔离，消除了攻击者操纵机器学习算法的风险并提供了弹性。美国初创公司 Xage Security 使用区块链技术在设备网络中批量分发隐私数据并进行身份验证，防止入侵活动通过网络传播。Xage 的平台利用区块链的分权化原则，网络入侵需要破解每一个分类账和设备，加大了网络攻击的难度。

（四）用户需求加快内嵌安全设计工控系统研发

工业信息安全风险的一个主要因素即工业控制系统在设计之初未考虑安全性，随着工业企业用户安全意识的提高，安全性已逐渐成为新的自动化设备采购的必要条件之一。主要的自动化和工业控制系统供应商已开展对其产品进行 ISA Secure 的网络安全认证测试，确保其安全性。此外，埃克森美孚、杜邦公司以及洛克希德马丁在内的 120 多家企业正在开展一项合作，旨在开发出内嵌安全功能且成本更低的

SCADA 工控系统。

四、全球工业信息安全市场竞争格局逐渐形成

全球工业信息安全市场在过去多年一直保持较平稳低速增长，但自 2016 年以来，由于工业互联网、工业物联网、工业云等创新应用深入发展，市场开始逐渐进入快速成长期。工业企业用户对工业信息安全风险的认识明显提高，在工业信息安全方面的预算投入稳中有增；不同类型的工业信息安全产品供应商开始根据自身优势角逐发力；专业的工业信息安全服务领域不断发展，供应商显著增多；产业链上下游企业通过资本整合加快工业信息安全市场布局。

（一）用户安全投资意愿增强

近年来频频爆出的工业信息安全事件为工业企业用户敲响了警钟。2017 年，“WannaCry”和“Petya”勒索病毒大规模感染等事件对工业信息安全造成重大影响，导致汽车制造商本田（Honda）、巧克力生产厂商吉百利（Cadbury）工厂受到影响而关停等。据安全研究机构 SANS 的最新研究报告《保障工业控制系统——2017》统计，2017 年有接近七成的工业企业安全管理人员认为企业面临严重或很高的安全威胁。

面对日益严峻的安全挑战，工业企业用户趋向于使用多种防护产品和服务来保障其自身的工业信息安全。据 SANS

的调查显示（图 2.5），有 81%的工业企业正在使用反恶意软件或防病毒的终端安全产品，而正在使用访问控制的工业企业占 71%。与 2016 年相比，工业企业在漏洞扫描、安全意识培训、工业入侵防御等产品和服务的使用方面均有不同程度的提高。此外，工控系统配置管理成为工业企业在未来 18 个月中计划使用的首要解决方案。

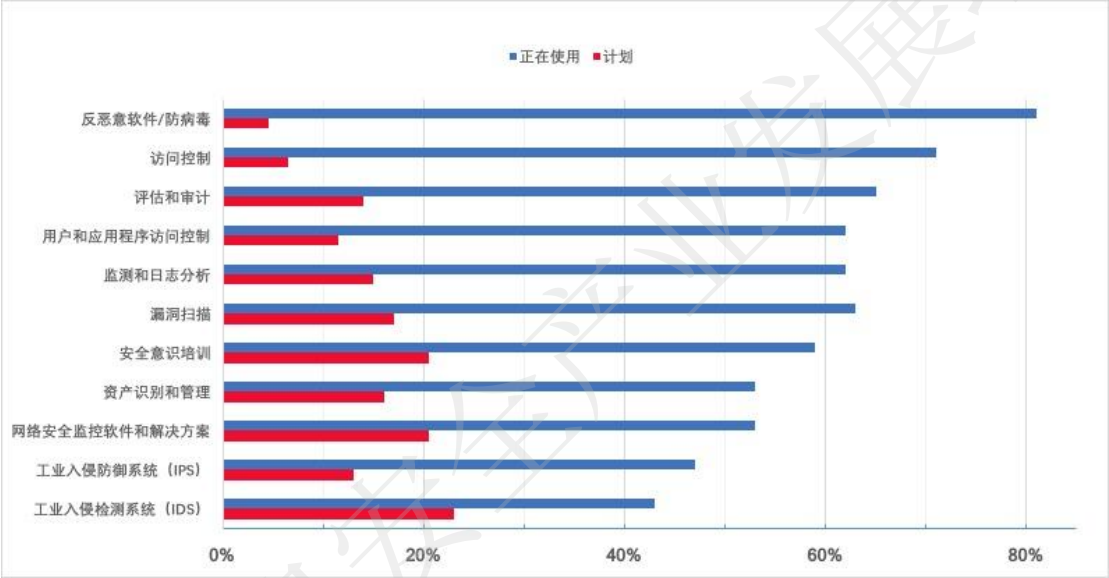

图 2.5　企业 2017 年正在使用和未来 18 个月计划使用的工业信息安全技术产品/服务/解决方案

数据来源：SANS 公司，工业信息安全产业发展联盟整理

SANS 的调查还表明，企业在 2017 年的工业信息安全投入较为可观，分别有 46%的工业企业表示会保持稳定的工业信息安全预算或增加其预算。大型企业在 2017 年的工业信息安全预算整体较高，而小微型企业在工业信息安全的预算方面较低，有 9.4%的小型企业表示 2017 年没有相关预算。

表 2.1 2017 年度企业的工业信息安全预算

	少于 1000 人	1000-10000 人	超过 10000 人
没有预算	9.4%	3.4%	2.6%
<10 万美元	3.4%	2.6%	0.0%
10 万-49 万美元	**6.0%**	**3.4%**	**3.4%**
50-99 万美元	0.0%	1.7%	4.3%
100 万-249 万美元	**0.9%**	**6.8%**	**4.3%**
250 万-999 万美元	0.0%	4.3%	1.7%
超过 1000 万美元	0.0%	0.9%	2.6%

数据来源：SANS 公司，工业信息安全产业发展联盟整理

（二）产品类厂商竞争激烈

工业信息安全产业发展联盟选取了全球 57 家工业信息安全典型厂商，并对其边界安全、终端安全、监测审计防护产品进行统计分析。其中，美国企业数量最多，共 29 家，占整体统计对象的半数以上；以色列作为网络安全强国，共有 14 家企业在近年来涉足工业信息安全领域，并在产品类市场具有较大影响力；欧洲地区也有 14 家企业开展了工业信息安全产品类业务。

工业信息安全防护产品细分市场供应商数量众多，竞争较激烈，市场尚未形成寡头垄断。目前，工业信息安全防护类产品厂商主要可以分为四大类，一是以思科（Cisco）、飞

塔（Fortinet）以及帕洛阿尔托网络（Palo Alto Networks）等为代表的传统网络产品供应商。该类厂商在传统 IT 领域基础深厚，拥有成熟的 IT 系统网络安全产品，工业信息安全市场仅为其垂直行业应用的一个分支，因此，该类厂商的产品仍集中于工业防火墙等边界安全产品。

二是以通用电气（GE/Wurldtech）、霍尼韦尔（Honeywell）、罗克韦尔（Rockwell Automation）为代表的自动化供应商。这类厂商有大量的用户群体作为基础，对于用户的工业信息安全选择具有较大话语权。该类厂商在工业信息安全市场的业绩仍以防护其自身的自动化产品为主。

三是以卡巴斯基（Kaspersky Lab）、迈克菲（McAfee）、赛门铁克（Symantec）为代表的传统安全软件供应商。该类厂商在传统 IT 领域上拥有广泛的安全产品，其工业信息安全产品以防病毒和应用白名单等终端安全产品为主。除个别厂商拥有专门的工业信息安全产品线，大部分厂商的终端安全产品与传统 IT 领域的安全产品区别较小。

四是以 Claroty、Indegy、Radiflow 等为代表的专注于工业信息安全市场的厂商。这类供应商通常为初创型企业，其工业信息安全领域的产品以监测审计产品为主。该类供应商有丰富的工业信息安全知识，为工业信息安全市场定制化开发产品，近年来增长势头迅猛。但由于用户在采购工业信息

安全产品时往往倾向于选择大型供应商和综合解决方案，因此该类厂商目前其市场份额仍相对较小。

（三）服务类厂商蓄势待发

工业生产环境的特殊要求和工控系统特有的安全管理约束使得工业信息安全服务愈发重要。工业信息安全服务供应商除了需要掌握工控系统的专业知识，还需要深入了解如何在工业环境中实施安全部署和维护网络安全技术。Gartner 在 2017 年的《OT 安全市场指南》中指出，工业信息安全服务市场正处在发展期，且增势强劲。工业信息安全产业发展联盟对全球 28 家工业信息安全服务类典型厂商深入分析，其中美国厂商 18 家，占总数的近 2/3。

全球工业信息安全服务市场的快速增长吸引了一大批不同类型的供应商，主要可以分为四大类。一是以埃森哲（Accenture）和德勤（Deloitte）为代表的国际知名咨询机构，通过收购和合作的方式进入工业信息安全市场，这类厂商通常以提供安全托管服务为主。二是以 ABB、艾默生（Emerson）、施耐德电气（Schineider Electric）、西门子（Siemens）和横河电机（Yokogawa）为代表的全球性自动化企业。这类厂商的服务通常以为其自身的自动化控制产品和使用的第三方网络安全产品提供全方位工业信息安全服务为主。服务内容包括安全评估、安全设计和实施以及安全托管等。三是以

aeSolutions、地平线控制集团（Horizon Controls Group）和 Verve Industrial Protection 为代表的控制系统集成商。该类厂商已经将其原有的工控系统服务，扩展至工业信息安全服务业务。通过其积累的丰富的工控系统知识和现有客户关系，该类厂商可以实现快速转型，为工业企业用户提供安全评估服务和后续的设计实施服务。四是以 FoxGuard Solutions 和 Red Trident 等为代表的专业工业信息安全服务供应商。该类厂商的行业用户广泛，并且拥有丰富的工业信息安全服务经验和行业合规标准知识，其工业信息安全服务内容也较全面。

（四）产业链上下游企业资本整合加速

随着工业信息安全市场的快速发展，产业链上下游企业通过资本整合或战略合作加快工业信息安全市场布局。2016 年至 2017 年，跨国自动化企业、国际咨询机构开始以收购和合作的方式拓展工业信息安全产品和服务业务。其中，以色列的工业信息安全初创企业 Claroty 在 2017 年表现亮眼，分别与罗克韦尔、施耐德和雷多斯合作，推进其工业信息安全异常和入侵检测产品和解决方案。

2016 年至 2017 年，专业的工业信息安全初创企业也愈发受到资本市场青睐（如表 2.2 所示）。以色列有 5 家初创企业在近两年获得 A 轮融资，分别为 Indegy、 Cyber X、Claroty、Scadafence 和 Cylus。美国工业信息安全企业 PAS、

Dragos 和 Nozomi Networks 也分别在 2017 年获得投资。其中，有 23 年历史的工业信息安全解决方案公司 PAS，于 2017 年获得由 Tinicum 领投的 4000 万美元投资，并将投资用于开展工控安全业务。英国安全公司 Darktrace 凭借其在网络威胁情报自动检测上的出色表现，于 2017 年 7 月完成 D 轮 7500 万美元的融资。

表 2.2 2016 至 2017 年工业信息安全市场企业融资情况

序号	时间	厂商	融资金额（万美元）	融资阶段	投资方
1	2016 年 7 月	Indegy	1800	A 轮	以色列本土风投 Vertex Venture（领投）
2	2016 年 8 月	Cyber X	900	A 轮	弗林特资本(领投)
3	2016 年 9 月	Claroty	3200	A 轮	柏尚风险投资（BVP）领投
4	2017 年 4 月	PAS	4000	-	Tinicum 领投

5	2017 年 7 月	Darktrace	7500	D 轮	洞见创投（Insight Venture Partners）领投
6	2017 年 8 月	Dragos	1000	A 轮	Energy Impact Partners （EIP）、艾利安(Allegis)资本
7	2017 年 11 月	SCADAf-ence	1000	A 轮	31Ventures Global Innovation Fund 领投
8	2017 年 12 月	Nozomi Networks	1500	B 轮	Invenergy 未来基金领投
9	2018 年 1 月	Cylus	470	种子轮	Zohar Zisapel 领投

数据来源：工业信息安全产业发展联盟整理

第三章 我国工业信息安全产业发展总览

一、我国工业信息安全产业发展环境日益优化

（一）我国工业信息安全产业政策充分利好

近年来，我国加强网络安全相关法规政策制定。2016 年 11 月，十二届全国人大常委会第二十四次会议表决通过了《中华人民共和国网络安全法》(以下简称《网络安全法》), 并于 2017 年 6 月 1 日起正式施行。工业信息安全是网络安全的重要组成部分，随着“两个强国”战略加快落实，信息化和工业化融合不断深入，工业信息化、自动化、网络化、智能化系统在提升效率的同时，对安全的需求日益提高。工业和信息化部围绕落实《网络安全法》《中国制造 2025》《关于深化制造业与互联网融合发展的指导意见》(国发〔2016〕28 号), 相继出台了一系列政策、指南，从宏观、中观、微观层面不断细化完善工业信息安全政策体系。

2016 年,《工业控制系统信息安全防护指南》从管理、技术两方面提出了工业安全软件选择与管理、配置和补丁管理、边界安全防护等 11 项工控安全防护要求,为工控安全防护工作提供了基本依据。

2017 年，我国工业信息安全政策体系得到进一步完善。6 月，工业和信息化部印发《工业控制系统信息安全事件应

急管理工作指南》，明确了工控安全事件概念，对工控安全风险监测、信息报送与通报、应急处置、敏感时期应急管理等工作提出了细化管理要求。8 月，为检验《工业控制系统信息安全防护指南》的实践效果，综合评价工业企业工控安全防护能力，工业和信息化部选取了电力、化工、汽车、有色、石化、烟草等行业的 10 家典型工业企业开展了防护能力评估工作，并编制发布了《工业控制系统信息安全防护能力评估工作管理办法》。该办法明确了工控安全防护能力评估工作的管理组织机构设置，详细规定了评估的基本要求、工作程序、工作方法和监督管理方式，为下一步开展全生命周期评估，进一步发挥管理实效提供了政策依据。

11 月，国务院发布《关于深化“互联网+先进制造业”发展工业互联网的指导意见》。该意见围绕打造网络、平台、安全三大体系，推进大型企业集成创新和中小企业应用普及两类应用，构筑产业、生态、国际化三大支撑，提出了工业互联网发展的 7 项主要任务。在安全保障方面，文件提出要着力提升安全防护能力、建立数据安全保护体系、推动安全技术手段建设，全面强化工业互联网安全保障能力。12 月 29 日，工业和信息化部发布了《工业控制系统信息安全行动计划（2018-2020）》（以下简称《行动计划》），旨在进一步落实国家工业信息安全相关战略规划，满足在工业信息化快速发展条件下对工业生产安全性不断提升的需求。表 3.1 列出了

近年来我国发布的工业信息安全顶层设计相关政策。

表 3.1 近年来我国发布的工业信息安全相关主要法规政策

序号	法规政策名称	发布时间	主要内容
1	中国制造 2025（国发〔2015〕28 号）	2015 年 5 月	以五大重点工程建设、十大领域关键技术、产品产业化突破为重点，通过“三步走”战略实现制造强国战略目标。
2	关于深化制造业与互联网融合发展的指导意见（国发〔2016〕28 号）	2016 年 5 月	围绕一条主线、建设两类平台、培育三种模式、提升三个能力、加强七项保障，推动制造业与互联网融合发展。
3	国家信息化发展战略纲要	2016 年 7 月	从安全和发展辩证关系、信息技术战略目标、网络安全内在规律和防御威慑网络能力四个方面，对我国未来网络安全工作做出顶层设计。
4	网络安全法	2016 年 11 月	提出制定网络安全战略，网络空间治理目标，政府各部门及网络运营者的职责权限和义务责任，关键信息基础设施保护制度，个人信息保护要求，将监测预警与应急处置措施制度化、法制化。
5	国家网络空间安全战略	2016 年 12 月	阐明我国网络空间的重大立场和主张，指明重要利益和底线，明确了我国网络安全工作重点并作出战略部署，维护我国在网络空间的主权、安全、发展利益。
6	“十三五”国家信息化规划	2016 年 12 月	“十三五”规划纲要和《国家信息化发展战略纲要》关于信息化任务的细化落实，将“健全网络安全保障体系”列为重要任务。

7	国家网络安全事件应急预案（中网办发文〔2017〕4号）	2017年1月	为国家层面组织应对涉及多部门、跨地区、跨行业的特别重大网络安全事件的应急处置提供政策性、指导性和可操作性方案。
8	网络产品和服务安全审查办法（试行）	2017年5月	从审查范围、审查内容、审查机构等方面搭建了网络安全审查工作的基本制度框架。
9	关于发布<关键设备和网络安全专用产品目录（第一批）>的公告	2017年6月	规定了网络关键设备与网络安全专用产品的范围、符合法律的方式，以及网络关键设备与网络安全专用产品提供商的义务。
10	关键信息基础设施安全保护条例（征求意见稿）	2017年7月	从关键信息基础设施范围、运营者安全保护、产品和服务安全、监测预警、应急处置和检测评估等方面作了相关规定。
11	深化“互联网+先进制造业”发展工业互联网的指导意见	2017年11月	明确开展网络基础、平台体系、安全保障、融合应用和制度保障等五个方面的工作，打造网络、平台、安全三大体系，推进大型企业集成创新和中小企业应用普及两类应用，构筑产业、生态、国际化三大支撑任务。
12	工业控制系统信息安全行动计划（2018-2020年）	2017年12月	突出落实企业主体责任，提出建立“一网一库三平台”的主要目标，部署五大能力提升行动，促进工业信息安全产业发展，加快工业控制系统信息安全（以下简称工控安全）保障体系建设。

数据来源：工业信息安全产业发展联盟整理

（二）我国工业信息安全标准体系逐步形成

工业信息安全标准化是工业信息安全保障体系建设的重要内容，在构建安全的网络空间、推动网络治理体系变革方面发挥着基础性、规范性、引领性作用。从总体上看，我国工业信息安全标准化工作正积极稳步推进，目前主要工作成果聚焦于工业控制系统安全。

工业控制系统安全标准化工作推进相对较快，目前已发布的工业控制系统安全标准有三项，主要包括《GB/T 32919-2016 信息安全技术 工业控制系统安全控制应用指南》、《GB/T 30976.1-2014 工业控制系统信息安全 第 1 部分：评估规范》和《GB/T 30976.2-2014 工业控制系统信息安全 第 2 部分：验收规范》。目前，《信息安全技术 工业控制系统风险评估实施指南》《信息安全技术 工业控制系统漏洞检测技术要求及测试评价方法》等 20 余项工业控制系统安全相关标准已完成立项。我国正逐步形成涵盖安全管理、系统安全防护、产品安全评估的工控信息安全标准体系，但绝大多数标准正处于草案或征求意见阶段。工业互联网安全、工业大数据安全等工业信息安全标准研制正处于筹划、酝酿阶段。

目前，我国工控系统信息安全标准体系按照安全等级、安全要求、安全实施和安全测评四方面展开，具体情况如表 3.2 所示。

表 3.2 我国工控系统信息安全标准体系工作开展情况

标准体系分类	标准状态	标准名称
安全等级	在研	《信息安全技术 工业控制系统安全分级指南》
安全要求	在研	《信息安全技术 工业控制系统安全管理基本要求》
		《信息安全技术 工业控制系统测控终端安全要求》
		《信息安全技术 工业控制系统漏洞检测产品技术要求及测试评价方法》
		《信息安全技术 工业控制网络监测安全技术要求及测试评价方法》
		《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》
		《信息安全技术 工业控制系统网络审计产品安全技术要求》
		《信息安全技术 工业控制系统产品信息安全技术要求》
安全实施	已发布	《信息安全技术 工业控制系统安全控制应用指南》
	在研	《信息安全技术 工业控制系统风险评估实施指南》
安全测评	已发布	《工业控制系统信息安全 第 1 部分:评估规范》
		《工业控制系统信息安全 第 2 部分:验收规范》
	在研	《信息安全技术 工业控制系统安全检查指南》

		《信息安全技术 工控系统信息安全防护要求与测试测评方法》
		《信息安全技术 工业控制系统信息安全防护能力评价方法》

数据来源：工业信息安全产业发展联盟整理

二、我国工业信息安全产业规模高速增长

（一）我国信息安全产业规模增速稳定

随着习近平总书记“4.19”（在网络安全和信息化工作座谈会上的讲话）和“10.9”（习近平总书记在主持第三十六次中共中央政治局集体学习时讲话）等系列关于网络安全的重要讲话的发表，以及《网络安全法》、《国家网络空间安全战略》等一系列信息和网络安全相关政策文件的出台，我国信息安全市场环境得到明显改善。在政策环境与市场需求的共同作用下，信息安全产业迎来快速增长期。

2012-2017 年，我国信息安全产业年均复合增长率约为 20.83%，远高于全球信息安全产业平均增长速度。2017 年，我国信息安全市场增长步伐虽较 2016 年增长率略有放缓，但仍保持了 23%左右的增速，市场规模达到 419.1 亿元人民币。

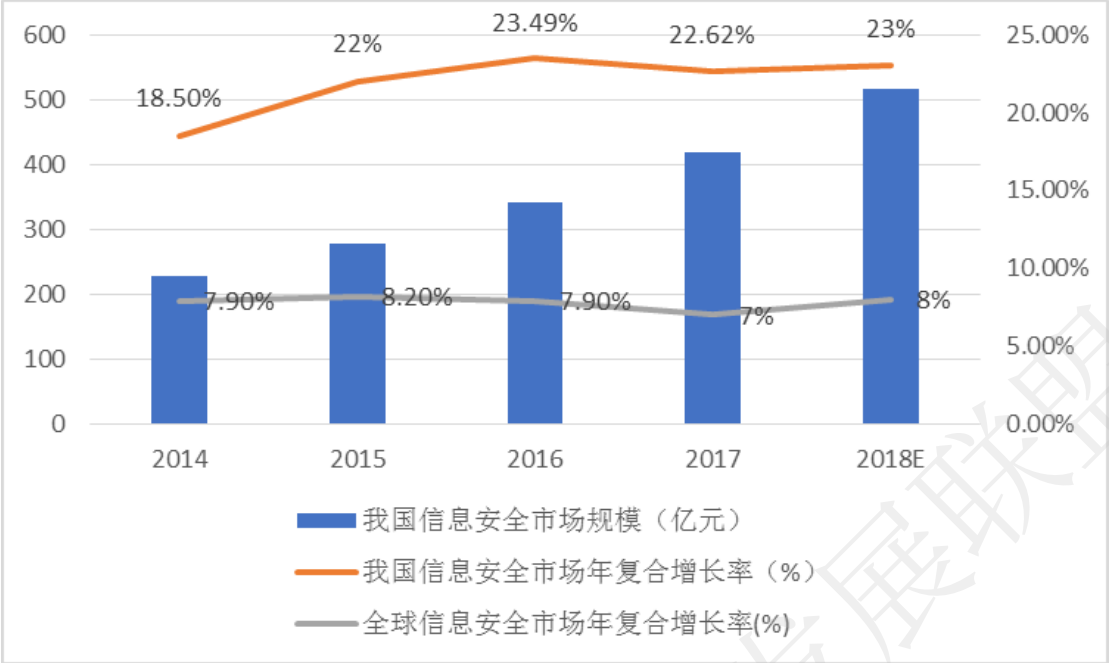

图 3.1　2014-2018 年中国信息安全市场规模及增长率

数据来源：　工业信息安全产业发展联盟整理

从行业应用来看，2017 年政府部门在信息安全领域的投入保持领先，占市场总量的 28%。电信行业和金融行业在信息安全领域发展较早，在信息安全方面的投入有小幅下降，但市场占比分别位居二、三位。

2017 年，工业[1]领域信息安全的市场规模约为 54.5 亿元，占整体的 13%。但目前工业领域在信息安全方面的投入仍以传统 IT 信息安全为主，在以工控安全为主的工业信息安全投入仅约 10%。

[1] 本报告中工业领域的定义参考国家标准《国民经济行业分类》（GB/T4754-2017），包括采矿业、制造业和电力、热力、燃气及水生产和供应业的 41 个大类

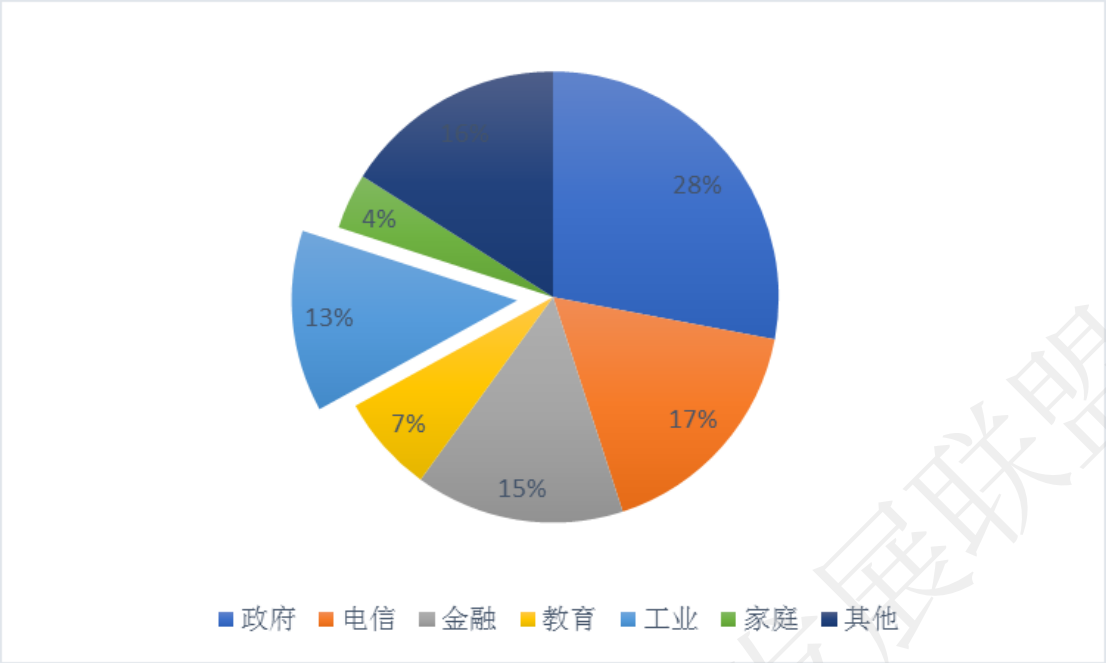

图 3.2　2017 年中国信息安全市场行业应用情况

数据来源：工业信息安全产业发展联盟整理

（二）我国工业信息安全产业进入快速增长期

近年来，日益复杂严峻的工业信息安全形势引发我国政府与产业界的高度关注，各行业不断加大安全投入，工业信息安全迎来发展机遇。工业信息安全产业发展联盟对联盟内成员单位 2017 年业绩进行了调研，结合国内工业信息安全市场公开招标情况、企业年报、其他相关产业报告等材料，对我国工业信息安全产业进行多维度分析和预测。

据工业信息安全产业发展联盟统计与调研结果显示，2017 年我国工业信息安全市场规模为 5.57 亿元，较 2016 年市场增长率达 53.6%，工业信息安全产业发展进入“快车道”。

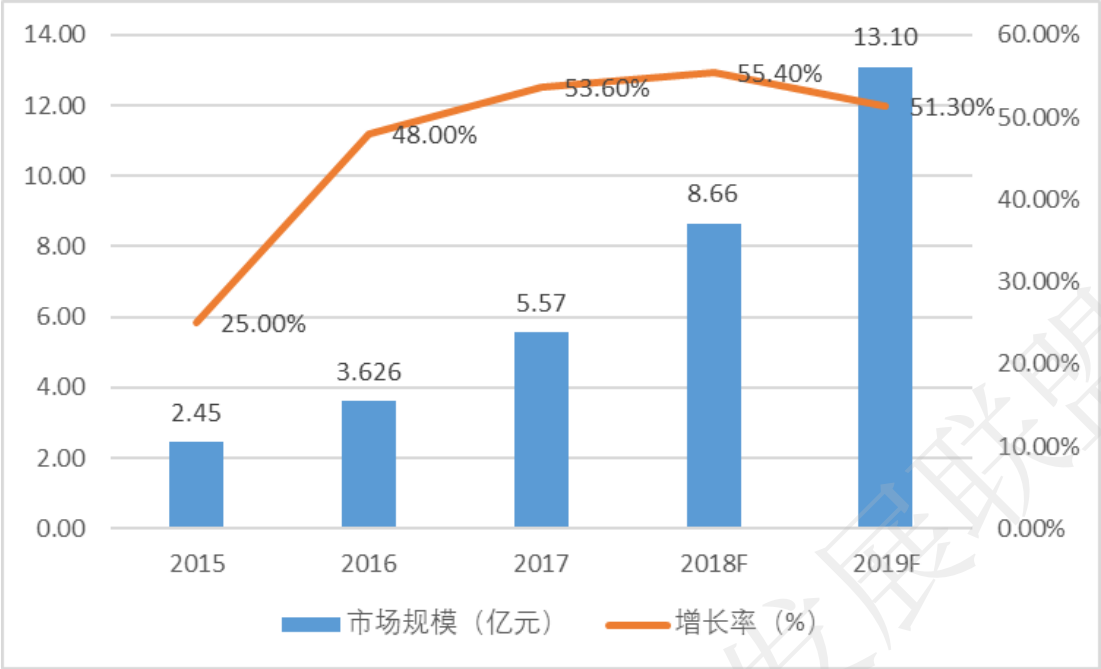

图 3.3　2015 至 2019 年我国工业信息安全市场规模及增长率

资料来源：工业信息安全产业发展联盟综合分析

与传统 IT 信息安全产业相比，以工控安全为核心的工业信息安全产业发展起步较晚。工业企业用户长期以来对于工控安全缺乏足够的重视，工控安全市场缺少相关标准、认证和防护规范，产业主要驱动力来自于工控安全厂商。据工控网数据显示，2012 年至 2015 年，我国工业信息安全产业整体处于起步阶段，发展较为平稳，年复合增长率约为 10%左右，2015 年我国工业信息安全市场整体规模仅为 2.45 亿元。

“十三五”以来，中央网信办、工业和信息化部等国家部门以《网络安全法》为基础，出台了一系列法规政策、战略规划、指导意见，从测试、评估、监测、应急、技术、产业、服务等方面提出工作要求，进一步明确工业信息安全主

体责任，工业信息安全正式进入落地实施阶段。2017 年，在工业互联网、工业云、工业大数据等产业发展需求的带动下，我国工业信息安全产业快速发展、市场规模显著提升。

综合考虑工业互联网加速发展、工业信息安全已成为国家安全体系的有机组成、工业企业安全意识不断增强等因素，我国工业信息安全产业开始进入快速增长期，预计 2018 年我国工业信息安全市场年增长率将接近 55.4%，市场整体规模将增长至 8.66 亿元。

三、我国工业信息安全产品类市场持续升温

我国工业信息安全产业的产品类市场和服务类市场均有不同程度的发展，产业结构不断完善。2017 年，工业信息安全防护类产品市场规模达 2.47 亿元，占总额的 44%，且受到技术成熟度差异等因素影响，未来一段时间内工业信息安全产品类市场规模仍将保持主导地位。与全球产业有所区别的是，我国工业信息安全管理类产品市场规模增长更加迅速，2017 年达 2.18 亿元，占比高达 39%。

目前，工业信息安全服务类市场整体规模仍较小，仅占整体市场份额的 17%。其中，安全咨询服务是服务类市场增长的主要动力，未来随着工业企业用户意识的增强，市场增速将逐渐加快。除安全培训外，其他工业信息安全实施和运营类服务目前仍发展较慢。一方面是因为我国工业信息安全

产业处于在成长期，工业企业用户对安全运营服务的需求不明确，市场尚不成熟；另一方面是由于我国许多工业信息安全厂商将运营服务与管理类产品进行了整合。

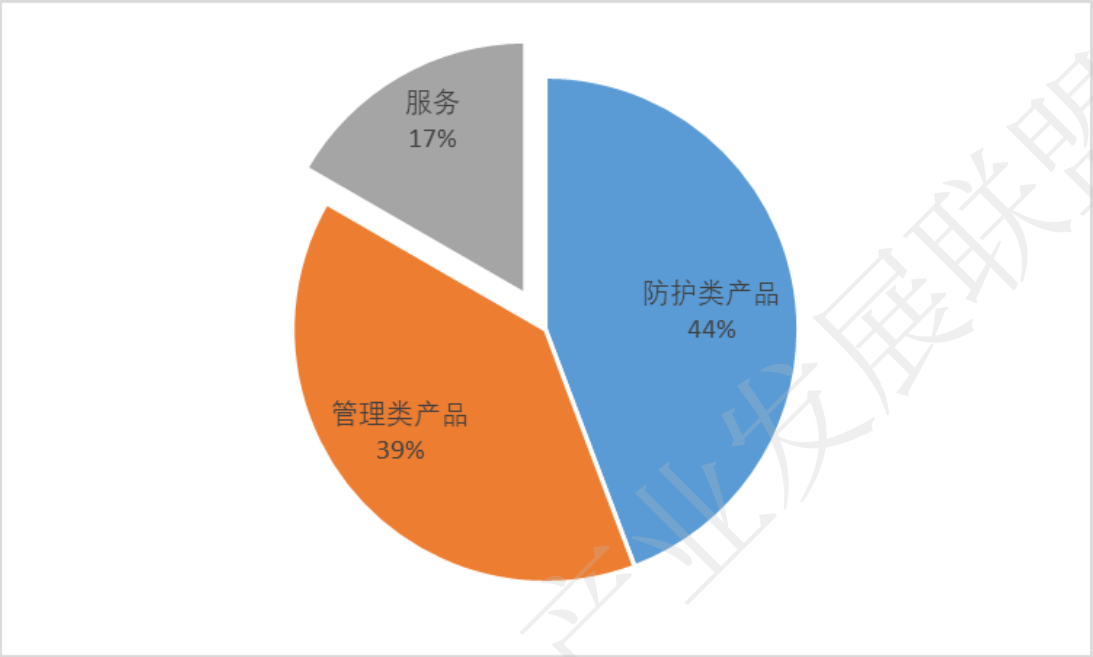

图 3.4　2017 年我国工业信息安全产业结构

资料来源：工业信息安全产业发展联盟综合分析

据工业信息安全产业发展联盟调研结果表明，目前我国工业信息安全防护类产品市场仍以边界安全和终端安全为主，工业防火墙、工业网络隔离设备和应用白名单产品发展相对成熟，市场占有率较大。监测审计类产品市场规模较小，但发展速度较快，多家厂商以不同形式布局监测审计类防护产品。

管理类产品方面，工业企业用户对安全运维管理和安全合规管理产品接受度较高，市场增长较快。但目前我国工业信息市场上的资产管理与补丁管理类产品较少，未来受政策

标准等合规性需求影响，将有更多厂商布局该类产品。据工业信息安全产业发展联盟对我国工业信息安全典型厂商深入调研分析，防护类产品和管理类产品的分布如表 3.3 和表 3.4 所示。

表 3.3 我国工业信息安全典型防护类产品

序号	厂商名称	边界安全		终端安全		监测审计		
		防火墙	网络隔离设备	防病毒软件	应用白名单	终端入侵检测	网络入侵检测	工业安全审计
1	360 企业安全	工业安全网关	工业安全网闸		工业主机防护系统		工业安全审计（带 IDS 功能）	工业安全审计
2	启明星辰	工业防火墙；工业物联网安全防护网关	工业网闸；wifi 入侵检测与防护设备		操作站安全系统		工业控制系统异常监测系统	日志审计、数据库审计、流秩型分析诊断系统
3	绿盟	绿盟 NF 防火墙系统	绿盟工业安全隔离装置；绿盟工业安全网关				绿盟工控安全入侵检测系统	
4	威努特	工业防火墙	单向隔离网闸；安全隔离与信息交换系统		工控主机卫士		入侵检测系统	监测审计平台
5	天地和兴	工控防火墙	安全隔离与信息交换系统		主机安全防护系统		工控安全威胁检测系统；入侵检测系	工控安全审计平台

							统;	
6	烽台科技						烽台入侵检测系统	
7	安点科技	工业防火墙	工业网闸				网络威胁感知系统	工业安全审计系统;
8	网藤科技		工业安全隔离网关	网御高级持续性威胁预警系统			工控安全行为追溯系统; 工控安全防护系统;	工控安全审计系统
9	长扬科技	工业防火墙	工业网闸; 安全隔离与信息单向导入系统		工控主机卫士			工业监测审计系统
10	海天炜业	Guard 工业防火墙	UniFace 安全数采网关		InTrust 可信芯片工控安全平台		工控安全审计与异常监测系统	
11	力控华康	工业防火墙	工业安全防护网关; 嵌入式工业通信网关					
12	立思辰	工业防火墙	内外网隔离设备		终端防护应用程序白名单系统		工业控制系统网络安全监控系统	

13	中京天裕		工业安全网关;工业安全隔离与信息导入装置;				工业入侵检测系统;工业异常监测审计装置	
14	中科物安	工业防火墙	安全隔离与信息单向导入系统		主机安全防护系统			工业安全监测审计系统
15	三零卫士	工业防火墙						
16	中科网威	超级下一代防火墙、中科网威防火墙	安全隔离与单向导入系统				入侵检测系统；异常感知系统	
17	江苏博智	工控防火墙						
18	九略智能				工业主机智能防护系统		工业网络智能防护系统；工业网络智能监测系统	
19	华创网安				工业控制网络安全主机防护产品			工业控制网络安全监测审计平台
20	中电瑞铠	工业防火墙				安全防护与审计监控系统		网络审计与监控系统

资料来源：工业信息安全产业发展联盟综合分析

表 3.4 我国工业信息安全典型管理类产品

		资产管理	补丁管理	合规管理	身份认证管理	安全运维管理
1	360 企业安全	工业态势感知、工业安全运营中心、工业安全管理系统		工业安全检查评估工具、工业主机威胁评估工具	工业无线入侵防御系统	运维安全审计与管理系统
2	启明星辰	工业控制信息安全管理系统		工控漏洞扫描系统		工控态势感知平台；工业控制系统信息安全管理系统；现场运维审计与管理系统
3	绿盟			绿盟工控漏洞扫描系统		绿盟工控安全审计系统
4	威努特	工业互联网雷达		工控漏洞挖掘平台；工控漏洞扫描平台		统一安全管理平台；安全运维管理系统
5	天地和兴				账号管理及运维审计系统	工业控制系统信息安全监管与分析平台
6	烽台科技	工控安全信息与事件管理系统；态势感知平台		标准符合性工具；工控脆弱性评估工具		工控安全信息与事件管理系统
7	安点科技				可信环境认证系统	工业信息安全运营平台；工业安全生产流程管理系统
8	网藤科技			USB 安全隔离装置	网藤账号集中管理与审计系统	

9	长扬科技			工控等保检查工具箱；工控安全评估系统		统一安全管理平台
10	海天炜业					工控网络安全管理平台
11	立思辰				工控运维审计平台	
12	中京天裕	SSMC 工业安全监控预警平台		工业设备通信加密装置；工业安全配置核查工具；工业协议漏洞挖掘平台；ICS 安全性验证工具		工业设备运维审计装置
13	三零卫士			风险评估套件		监控系统
14	中科物安	物联网安全态势感知平台、物联网安全风险探知平台		风险评估系统		安全管理平台
15	中科网威	集中管理平台		漏洞扫描系统		
16	江苏博智	工控网络安全态势感知分析系统		工控漏洞挖掘平台		
17	九略智能			工业主机智能防护系统		

18	华创网安			工业控制网络漏洞评估系统；工业控制网络安全主机防护产品		工业控制网络安全监测审计平台
19	中电瑞铠			网络安全管理平台		
20	匡恩	威胁感知平台		漏洞挖掘检测平台；威胁评估平台		安全监管平台

资料来源：工业信息安全产业发展联盟综合分析

随着国内工业信息安全厂商在软硬件一体化产品研发、安全服务提供等方面加快布局，IT 与 OT 之间寻求互补、融合发展的需求将更为迫切，安全应急、安全培训、安全托管等运营类服务将迎来发展机遇期，工业信息安全产业结构将有望得到优化。

第四章 我国工业信息安全行业应用情况

从行业应用来看，我国工业信息安全市场整体格局有所调整。地方政府及科研机构在工业信息安全领域的投入有显著提高，2017 年达 1.79 亿元，占市场总量的 32%。这主要得益于近年来国家的一系列相关政策的推动，如工业和信息化部于 2016 年发布的《工业控制系统信息安全防护指南》。此外， 2017 年组织开展的工控安全检查和防护能力评估工作，推动了地方政府对工业信息安全的重视，也加快了科研机构对工业信息安全研究的投入。

电力行业在工业信息安全领域的投入稳中有增，市场规模在 2017 年达 1.43 亿元，市场占比位居第二。与前几年相比，电力行业工业信息安全产品和服务应用已不仅局限于电网端，发电端企业工业信息安全产品和服务的应用明显增多。2017 年，中国华能集团针对发电企业的工业信息安全防护问题，在火电、水电和新能源三个方向开展生产控制系统信息安全监管与预警平台试点项目。中国国电集团下属的多家热电公司在 2017 年也相继开展了生产监控系统信息安全防护技改项目。

石油石化行业 2017 年工业信息安全市场规模达 1.16 亿元，市场占有率排在第三位。石油石化行业是工控系统普及度较高的行业之一，对工业信息安全的重视程度较高。2015

年以来，中石油、中石化、中海油等多次组织研讨会，加强论证和探讨工业信息安全在行业的实际应用和推广方案优化。2017 年，中国石油和化工集团针对其所属的油田企业、炼化企业等新建、改扩建及在用的工控系统的安全保障工作，发布了《关于加强工控系统安全防护的指导意见》，推进石化行业工业信息安全的应用。

此外，轨道交通行业、烟草和制造业的工业信息安全市场均较 2016 年有所增长，但目前市场份额仍较小。随着中国制造 2025 的不断推进，工业信息安全在这些行业的应用将会更加广泛。

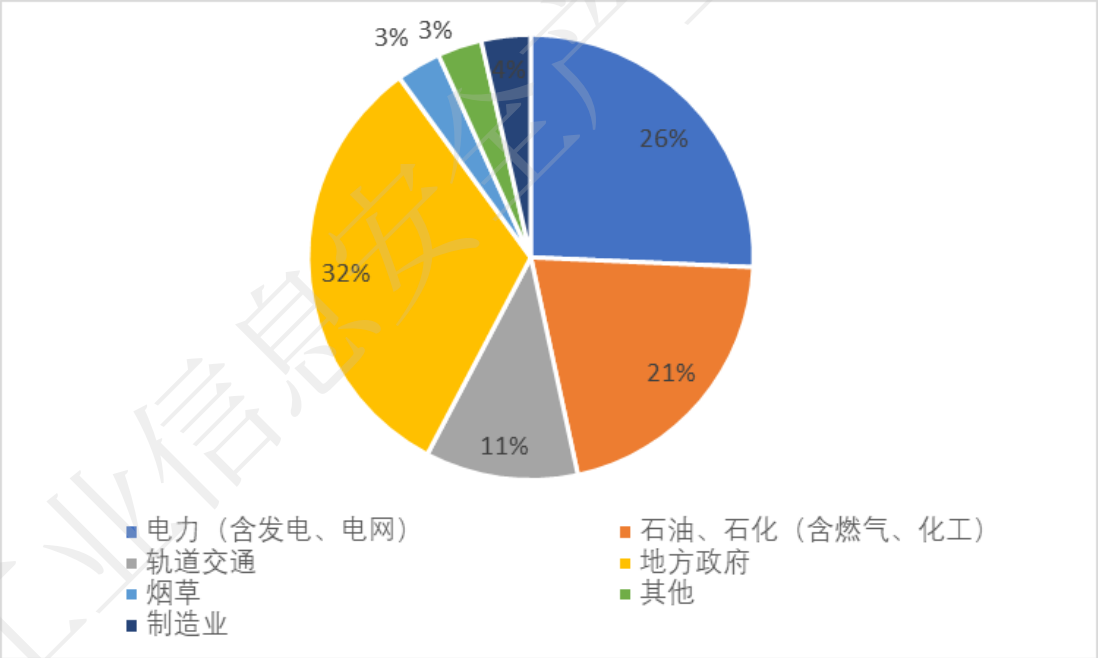

图 4.1　2017 年我国工业信息安全市场行业应用情况

资料来源：国家工业信息安全发展研究中心综合分析

第五章 我国工业信息安全技术发展现状

一、基于“应用程序白名单”的主机防护技术

目前针对工控主机的安全防护主要采用“应用程序白名单”技术。“应用程序白名单”技术主要指一组应用程序名单列表，只有在此列表中的应用程序是被允许在系统中运行，之外的任何程序都不被允许运行。通过数据采集和分析，智能学习模块自动生成的工业控制软件正常行为模式的白名单，与工业主机要运行的进程进行比较、匹配、判断。如果发现其特征不符合白名单中的记录，则将会对此行为进行阻断或告警，以此避免工业控制网络受到未知漏洞威胁，同时还可以有效的阻止操作人员异常操作带来的危害。

二、基于可靠性提升和专有协议识别的工控网络防护技术

工控网络防护技术能够有效检测到工控网络中的通信异常和协议异常并加以阻止，对工控网络专有协议进行深度分析，层层拆解数据包，深入剖析结构，帮助用户实现对工控网络进行深层次的安全管理和控制进而避免工控系统的意外事故。工控网络防护技术相对传统 IT 网络防护主要在可靠性方面进行了增强并增加了工控专有协议的识别。该技术用于生产控制网与监控网、监控网与管理信息网的边界，隔离生产控制网和监控网以及保护工控网络安全区域的安

全，阻止来自监控网、管理信息网和其他区域的安全威胁，提供工控协议深度解析、工控指令访问控制、攻击防护、日志审计等综合安全功能，保证生产的安全有序进行。

三、基于镜像流量的工控网络威胁检查技术

基于镜像流量的网络威胁检查技术主要用来检测工控网络安全区域的网络流量，发现来自监控网、信息网和其他区域的安全威胁。对工业控制协议的通信报文进行深度解析，能够实时检测针对工业协议的网络攻击、用户误操作、用户违规操作、非法设备接入以及蠕虫、病毒等恶意软件的传播并实时报警，同时详实记录一切网络通信行为，包括指令级的工业控制协议通信记录，为工业控制系统的安全事故调查提供坚实的基础。

四、基于模糊测试的工控设备漏洞挖掘技术

模糊测试主要是通过生成相应的报文，变换协议字段进行安全测试从而挖掘工控设备中的未知漏洞，提高工控设备的安全等级。基于模糊测试的工控设备漏洞挖掘技术可以支持工业控制系统中的主流工控协议以及私有协议进行深度挖掘。帮助工控企业有效审核风险控制策略，对工业控制系统设备中存在的漏洞进行全面安全评估，提升工控系统的安全性。

五、基于指纹识别和漏洞库的工控设备漏洞扫描技术

基于指纹识别和漏洞库的工控漏洞扫描技术主要是检测已知的安全漏洞，采用基于被动方式接收流量扫描，与指纹识别库和工控漏洞库进行特征匹配，发现工控设备漏洞。在工业应用环境中，漏洞扫描建议采用被动的、非破坏性的办法对工控系统、工控设备、工控网络进行检查检测，及时发现漏洞，发现威胁，避免影响正常的生产业务。在工业控制系统中，生产业务的稳定性、可靠性、连续性是至关重要的，尤其是对一些核心的生产系统、控制设备，因此，对其进行漏洞扫描时也需要做到“无害”、“无损”。把扫描融入到正常的业务中的思路，也就是说，扫描行为与正常的业务行为是一致的，这样就能避免非正常的操作而造成对系统的影响。通过这种成熟的技术，以实现对工业控制系统的无损漏洞扫描。

第六章 我国工业信息安全市场竞争格局

一、企业积极布局工业信息安全业务

据国家工业信息安全发展研究中心数据统计，目前国内约有 138 家企业涉足工业信息安全业务，较 2012 年时有显著增长。目前，国内工业信息安全厂商可根据业务发展背景分为四种类型：自动化背景厂商、传统信息安全背景厂商、IT 系统集成商及专注工业信息安全的厂商。

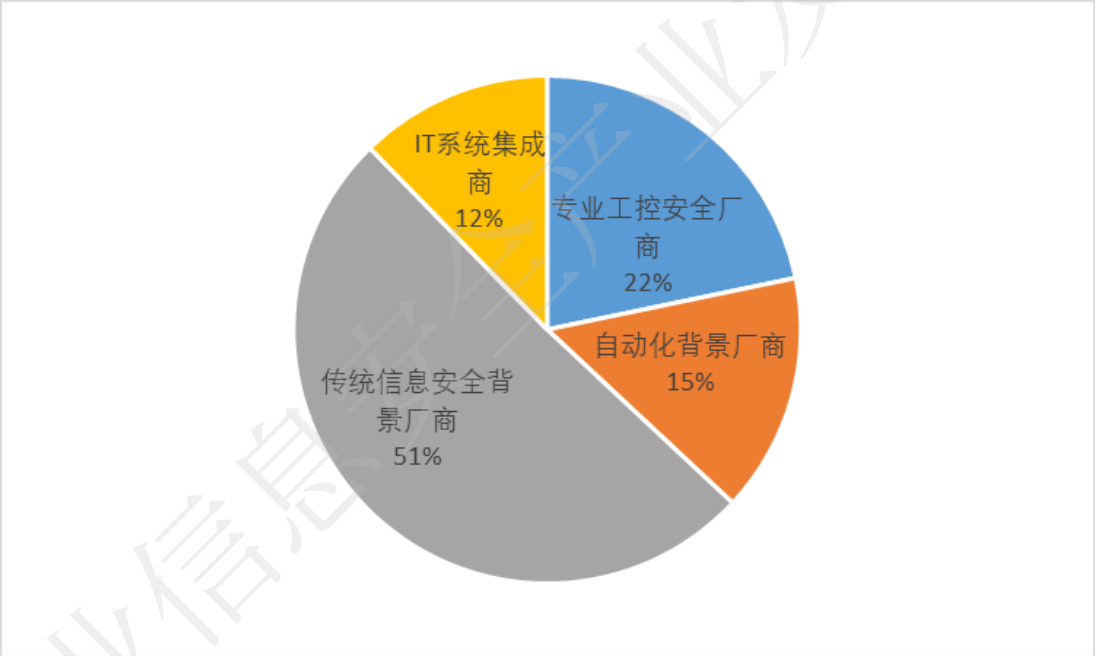

图 6.1　2017 年中国工业信息安全厂商分布

数据来源：国家工业信息安全发展研究中心分析整理

自动化背景的厂商，主要指原来从事自动化控制相关业务的公司，通过成立子公司或工控安全部门进入工业信息安全市场领域，如浙江中控、和利时、三维力控等公司。

传统信息安全背景的厂商是指主要从事信息安全业务，

将工业信息安全作为其安全业务的一个分支，这类公司主要通过成立工控安全部门或投资有工控安全业务的企业进入工业信息安全领域，如启明星辰、绿盟、立思辰等公司。

IT 系统集成商，是指具备系统集成资质、能对行业用户实施系统集成的企业。这类公司拥有深厚的行业用户基础，主要通过与专业的工业信息安全公司合作进入工业信息安全领域，如石化盈科、中油瑞飞、南瑞信通等公司。

专注工业信息安全的厂商是指通过整合信息安全和自动化控制方面的人才，专注于开展工业信息安全领域业务的企业，如威努特、天地和兴、安点科技等公司。

二、资本助力工业信息安全市场

据东方财富旗下的金融数据平台 Choice 统计，目前国内 A 股市场已有启明星辰、绿盟科技、卫士通、北信源、南洋股份、立思辰、蓝盾股份等多家上市公司有工控安全相关板块，初步形成主营业务方向。同时，天融信、海天炜业、华创网安、珠海鸿瑞等中小微型工控安全企业近年业绩快速增长，已在新三板实现挂牌上市。

表 6.1　A 股上市公司开展工控安全板块情况

上市公司	上市板块	上市时间	相关主营业务
启明星辰	中小板	2010 年 6 月	工控安全防火墙、工控安全漏洞扫描、工控安全异

			常检测
绿盟科技	创业板	2014 年 1 月	工控安全漏洞扫描
卫士通	中小板	2008 年 7 月	旗下三零卫士子业务专营工控安全防火墙、工控安全审计
北信源	创业板	2012 年 9 月	与匡恩网络合资主营工控安全防火墙、工控安全审计、工控安全漏洞挖掘
南洋股份	中小板	2008 年 2 月	收购天融信涉足工控安全产业，业务包括工业防火墙、入侵检测与防御、企业终端安全等
立思辰	创业板	2009 年 10 月	战略投资谷神星，主营工控安全防火墙、主机白名单、工控安全漏洞扫描、工控安全堡垒机
蓝盾股份	创业板	2012 年 3 月	子公司满泰科技专营水利行业自动化和工控安全解决方案

资料来源：Choice、国家工业信息安全发展研究中心综合分析

2017 年工业信息安全初创企业引发投融资市场关注。主营工控安全业务的安点科技于 8 月完成第二轮融资，融

资规模达 4500 万元。天地和兴、网藤科技也于 2017 年分别完成 A 轮融资，融资规模均超过千万，预计未来还将有更多工业信息安全初创企业将借助产业发展东风，成为信息安全投融资市场的新星。

第七章 我国工业信息安全产业发展面临的挑战与趋势展望

一、我国工业信息安全产业发展面临的挑战

（一）工业企业安全主体责任落实不到位问题仍然存在

工业信息安全的建设和产业发展在过去几年主要受合规需求驱动，工业企业对工业信息安全的重视程度有限，普遍存在重发展、轻安全的现象，安全投入不持续、主体责任落实不到位等问题十分突出，造成工业信息安全能力建设滞后于形势发展、产业低价竞争等不良局面。当前，工业企业的安全意识虽有所提升，但是包括机制建立、制度建设、责任定岗、安全部署等方面在内的企业安全主体责任仍需强化。

（二）工业信息安全产品和服务缺乏认证机制，大规模应用进程缓慢

目前，市场上工业信息安全产品和服务的种类繁多，但与之对应的认证和市场准入机制尚不完善，有针对性的检测认证标准规范和技术手段还很缺乏，大多数工业信息安全产品和服务仍然使用传统信息安全检测认证标准和方法。这种缺乏统一的标准和认证机制的问题，将会导致工业信息安全产品和服务的认证缺乏权威性，难以快速广泛地推向市场，

产业化生产、规模化应用更是步履维艰。

（三）安全服务市场发展缓慢，产业结构有待进一步优化

近年来，我国工业防火墙、工业网闸等工业信息安全防护类产品市场发展较快，但安全运维、安全评估、安全设计与实施等服务能力不足，安全服务市场占有率较低。目前，用户对工业信息安全产品的配置和运维缺乏持续学习的渠道和经验，安全服务市场已无法满足快速增长的用户需求，导致一些安全产品无法发挥最大效果，市场对运营类安全服务等服务型产业需求迫切。

（四）工业信息安全产业集中度不足，缺乏龙头企业引领

目前，我国专注工业信息安全领域的厂商普遍规模较小，而布局工业信息安全业务的传统信息安全厂商、自动化厂商和 IT 系统集成商进入市场的时间多数不足五年。现有的工业信息安全企业普遍缺乏具有市场竞争力的核心产品，技术实力和创新能力都显不足，尚未形成产品竞争力强、行业影响力大、引领产业发展的骨干龙头企业，产业集聚效应不明显，整体工业信息安全产业发展规模还处于低位。

二、我国工业信息安全产业前景展望

（一）工业信息安全产业政策红利将进一步释放

工业信息安全是落实党的“十九大”关于建设制造强国和网络强国、坚持国家总体安全观等要求的关键抓手，《网络安全法》等政策的落地实施将进一步提升工业企业的安全意识，落实企业主体责任，促进工业信息安全产业的内需增长。同时，《工业控制系统信息安全行动计划（2018-2020 年）》明确指出将培育龙头骨干企业、创建国家新型工业化产业示范基地（工业信息安全）作为主要任务。未来随着各项国家法规政策的稳步推进，工业信息安全产业环境将持续优化，产业聚集效应将逐渐形成。

（二）工业信息安全产业规模将保持高速增长

产业环境的日益优化，为我国工业信息安全技术创新、工业信息安全企业做大做强提供了前所未有的机遇。在工业互联网、工业云、工业大数据等产业发展需求的带动下，综合考虑工业信息安全已成为国家安全体系的有机组成、工业企业安全意识不断增强等因素，我国工业信息安全产业将保持高速增长，预计 2018 年国内工业信息安全市场年增长率将接近 55.4%，市场整体规模将增长至 8.66 亿元。

（三）新一代信息技术促进新兴业态安全技术研发

以移动互联网、物联网、云计算、大数据、人工智能等为代表的新一代信息技术风起云涌，加速 IT 和 OT 技术全方位的融合发展。与此同时，工业互联网等新兴业态的安全环境复杂多样，安全风险呈现多元化特征，安全隐患发现难度更高，安全形势进一步加剧。这一系列的技术和形势的变化，将促进威胁情报、态势感知、安全可视化、大数据处理等新技术在工业信息安全领域的创新突破。

（四）工业信息安全产业链上下游加速协同互动

工业信息安全保障工作的重要性、复杂性和及时性需要工业企业、工控系统厂商、安全企业、研究机构、行业主管部门等参与方进行紧密配合。未来工业信息安全厂商与工控系统厂商、IT 系统集成商将针对工业领域各行业的生产运营特征，加快开展多层次、多维度的合作，形成有效的业务安全实践，共同打造协同发展的生态系统。