行业研究报告\信息安全行业研究

2017 年度信息安全行业研究

受益信息安全产业政策 工控安全市场强势启动

研究要点

- 工控安全事件频发，工控安全危害频出，安全防护进入高速发展期；
- 我国将成工控安全市场热土。世界各国都对工控安全空前重视，纷纷加大力度。我国政策支持力度空前；
- 工控安全处于市场发展早期。工控安全厂商及产品逐年增加，但市场仍处于早期，未来发展空间巨大。

基石基金 CORNERSTONE CAPITAL

基石基金投资部

康苏宾

电话：15699766683

电子邮件：ksb@bjjsfund.com.cn

相关研究

1. 工业信息化部网站
2. 方正证券
3. 国家工业信息安全发展研究中心
4. 工控网
5. Wind 资讯

目录

一、 工控安全是什么

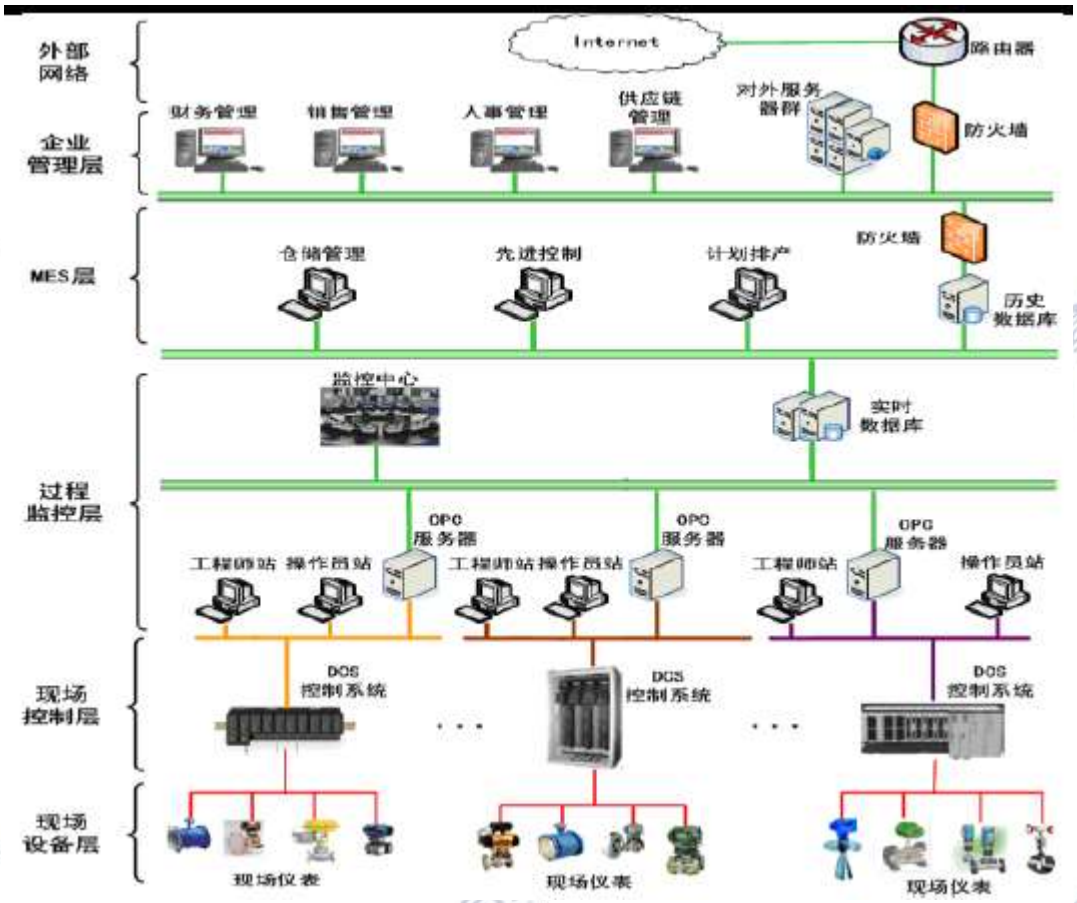
1.1 工业控制系统是什么

工业控制系统，即 ICS（也称工业自动化与控制系统），是由计算机设备与工业过程控制部件组成的自动控制系统。经典的工业控制系统通常具有测量、比较、计算、矫正四个功能，通过传感器、转换器、发射器、控制器与执行器五个部件实现。

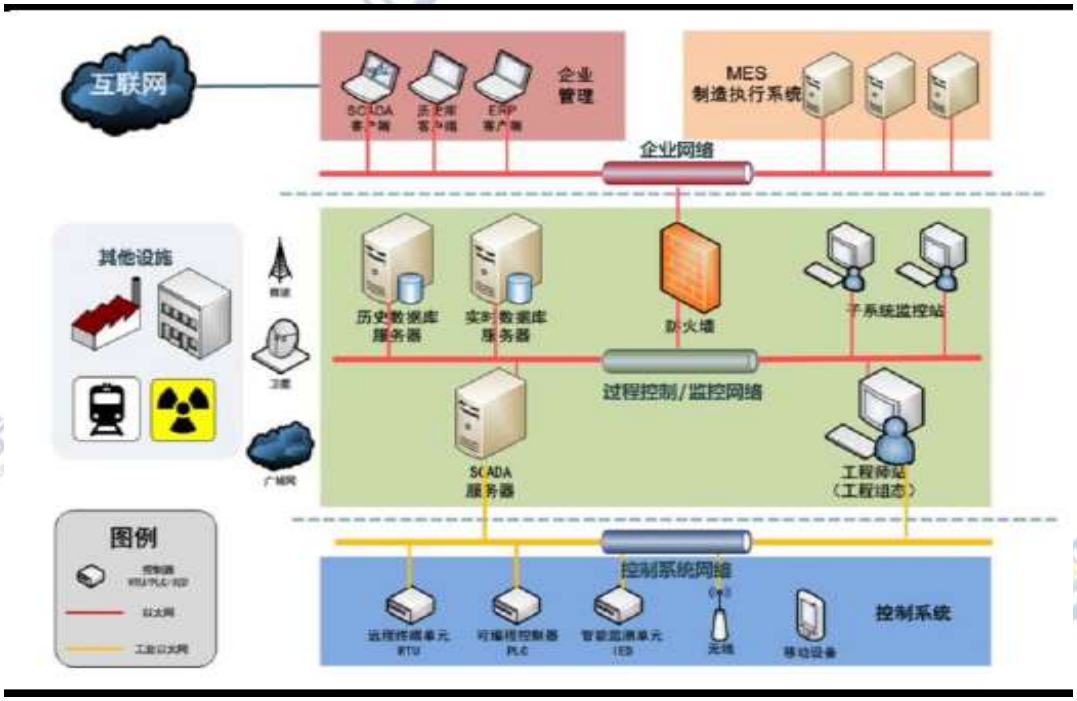
图表 1 经典工业控制系统四个功能

图表 2 工业控制系统五个部件

工业控制系统的层级较为复杂，自下而上包括现场设备层、现场控制层、过程监控层、MES 层、企业管理层和外部网络层，通过各层级配合实现工厂设备的智能化管理操作。这些复杂的层级可分为三个业务区：业务区一是由实际的工业控制系统资产组成，包括物理资产、数字资产、逻辑资产和人力资产等；业务区二由定制的设备系统构成，它是工业控制的核心系统设施，包括 SCADA 系统、DCS 系统、PLC 系统等；业务区三是上层 IT 业务区，除了一般的业务操作，这样的 IT 业务区一般来说会为了更好得统计和监控而连接到其他业务区中。



图表 3 工业控制系统层级



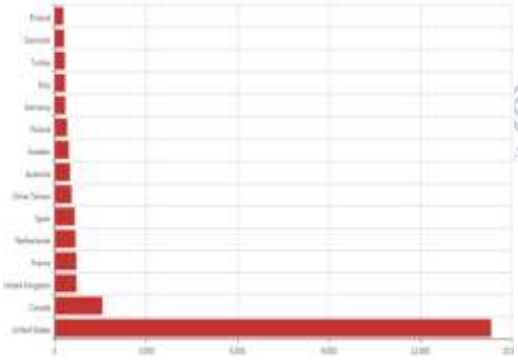
图表 4 制系统的三个业务区

工业控制系统广泛运用于工业、能源、交通、水利以及市政等，重点领域包括许多与国际民生紧密相关的领域。例如：核设施、钢铁、有色、化工、石油石化、电力、天然气、先进制造、水利枢纽、环境保护、

铁路、城市轨道交通、民航、城市供水供气供热等。

工控系统的分布数量与工业的发达程度正相关。美国的工业控制系统数量最多，紧跟其后的是加拿大，欧盟各成员国也都居于世界前列，俄罗斯、非洲和南美的一些国家数量相应较少。

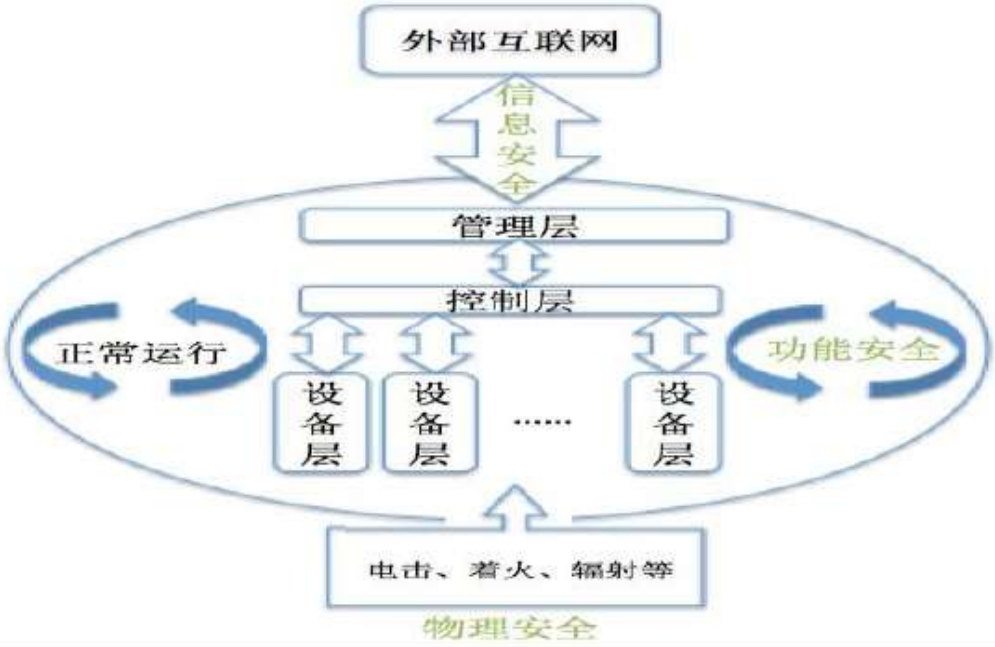
图表 5 全球工控系统数量分布图



图表 6 全球工控系统数量排名

1.2 工控安全是什么

工业控制安全的定义为：①保护系统所采取的措施；②由建立和维护系统的措施所得到的系统状态；③能够避免对系统资源的非授权访问和意外的变更、破坏或损失；④基于计算机系统的能力，能够保证授权人员和系统的合法操作权限，避免非授权人员和系统修改软件及其数据或访问系统功能；⑤防止对工控系统非法、有害的入侵，或者对其正常操作的干扰。工业控制系统的安全通常可分为功能安全、物理安全和信息安全三类。功能安全是为实现设备和工厂的安全功能；物理安全是减少由于电击、着火、机械危险、幅射、化学危险等因素造成的危害；信息安全是保持信息的保密性、完整性、可用性，另外还有真实性、可核查性、不可否认性和可靠性等。



图表 7 工控安全三种安全子类关系

工控系统与 IT 信息系统安全防护存在本质区别。IT 信息系统更多关注信息安全，而工业控制系统通常关注更多的是物理安全与功能安全，尤其是功能安全，该系统的安全运行由相关的生产部门负责，信息部门仅处于从属的地位。在信息安全的三个属性（机密性、完整性、可用性）中，IT 信息系统的优先顺序是机密性、完整性、可用性，而工业控制系统则是可用性、完整性、机密性。

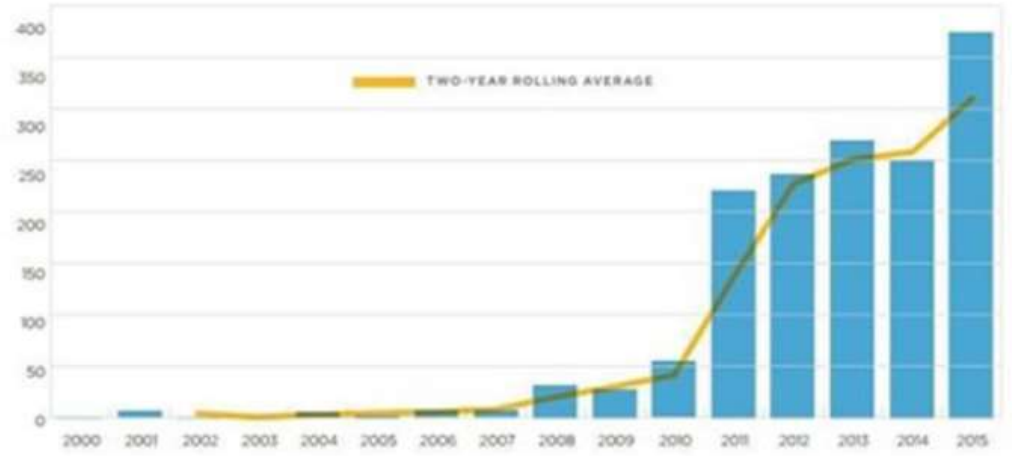
随着信息化与工业化技术的紧密结合以及潜在网络战威胁的影响，工业控制系统也将从传统模式转向更为关注信息安全。

总的来说，工控安全是针对工业领域中除物理安全外的功能安全、信息安全的一系列防护策略和手段的总称。其要解决的问题就是通过防攻击、防篡改、防病毒、防瘫痪、防窃密等手段来保证工控系统网络的合理运行，达到保障工业生产安全的目的。

二、 工控安全危害频出，安全防护进入高速发展期

2.1 工控安全态势愈发严重

公开披露的工业控制系统相关漏洞数量在 2011 年之前相当少，但在 2011 年出现快速增长，原因可能是 2010 年的 Stuxnet 蠕虫事件之后，人们对工业控制系统安全问题持续关注以及工业控制系统厂商，也在分析解决历史遗留安全问题。随着各方面对工业控制系统的安全重视度越来越高其相关公开漏洞数量仍将保持一个快速增长的总体趋势。美国国土安全部工业控制系统网络应急响应小组(ICS-CERT)提供周期性的事件报告《2015 事件响应统计》显示，美国 2015 年共报告了 295 起涉及关键基础设施的事件，而 2014 年仅有 245 起。大多数安全事件影响到了制造业和能源业。



图表 8 工控安全事件数量统计

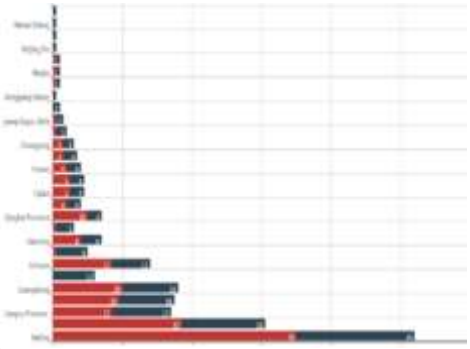
公开漏洞所涉及的工业控制系统厂商排名前五为：西门子（Siemens）、施耐德电气（Schneider）、研华科技（Advantech）、通用电气（GE）与罗克韦尔（Rockwell），仍然是以国际著名的工业控制系统厂商为主。

用户的工控系统使用情况调研结果表明，在国内市场上，这些国际著名工控系统厂商的产品占据极大的优势地位，甚至某些产品在一些行业中处于明显的垄断地位。这种情况也就导致了这些厂商的产品更易受到系统攻防双方的重视和关注，而且想要获得研究分析用户的产品也比较容易，这很可能就是公开漏洞涉及到的工控系统厂商总是以国际厂商为主的主要原因。

国际范围内工控安全事件的分布，主要发生在欧美等经济发达地区，在经济发达地区制造工控安全事件能够牟取更多的经济利益，其工控系统在受到攻击后往往损失惨重，因此对于工控系统安全防护的需求更为迫切。

我国工控安全事件也同样发生在经济发达地区，主要集中在北京、江苏、广东等地。

图表 9 国际工控安全事件分布图



图表 10 我国工控系统暴露事件地区分布图

2.2 工控安全威胁引发严重后果

工业基础设施构成了我国现代社会国民经济以及国家安全的重要基础，而工业基础设施的核心是其工业控制系统（ICS）。工业基础设施中关键 ICS 系统的安全事件与传统的 IT 信息安全不同，一旦发生，则可能会导致影响系统可用性、关键控制数据被篡改或丧失、失去控制、环境灾难、破坏基础设施、经济损失、惨重人员伤亡、危及公众生活及国家安全等严重后果。更为重要的是，近年来更多针对工业网络的攻击已上升至国家安全层面，保护工控安全迫在眉睫。

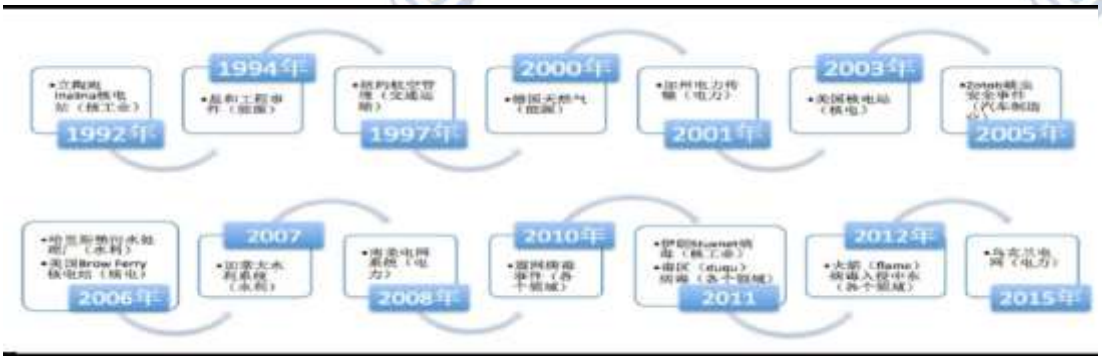
图表 11 2010-2016 年国家安全事件

自从 2010 年震网病毒、Flame、Duqu 以及 2014 年“蜻蜓组织”相关的可能大规模影响欧洲能源企业 SCADA 系统的安全事件对工业界的影响巨大，针对工控系统攻击的恶意代码一直层出不穷，并可能在攻击活

动的背后具有国家支持的潜在因素。因而，工控系统所面临的安全威胁日益严峻。

2.3 典型工控安全事件

自 20 世纪 90 年代以来，工业控制系统安全事件时有发生，近年来，针对工业控制系统的各种网络攻击事件日益增多，且安全威胁已经从能源领域向各领域延伸，呈现多领域攻击的态势，暴露出工业控制系统在安全防护方面的严重不足。



图表 12 工控安全事件概览

三、 工控安全下一个热土在中国

自从 2010 年震网事件之后，世界各国对工控系统的安全问题的关注度日益提升，工控安全更成为备受工业和信息安全领域研究机构关注的研究热点。近年来，世界各国都在政策、标准、技术、方案等方面展开了积极应对，其中美国是工控安全建设领域的领头者。

3.1 各国把工控安全提升至国家安全战略高度

作为信息产业发展的领导者，自 2003 年起美国就开始重视工控系统的安全，并于 2009 年率先颁布响应战略政策。就全球范围来看，自 2011 年以来工控安全领域在国际范围内得到了高度重视，各国相继制定战略颁布法律，在国家层面的支持下，各国的工控安全领域正迎来利好的发展。

国家/地区	时间	主要政策
美国	2003 年	将工控安全视为国家安全优先事项
	2008 年	列入国家需重点保护的关键基础设施范畴
	2009 年	颁布《保护工业控制系统战略》：在 CERT 组织下面成立工业控制系统网络应急相应小组（ICS-CERT）
	2015 年 1 月	总统奥巴马拜访美国国土安全部国家网络安全与通信集成中心（NCCIC），提出针对网络安全信息共享的立法提案
	2015 年 4 月	国防部发布第二版网络战略报告，指导美国网络力量的发展，加强网络防御建设与网络威慑力量
德国	2011 年 2 月	公布《德国网络安全战略》，作为指导网络安全建设的纲领性文件
	2015 年 7 月	立法要求关键基础设施企业和机构实施更强大的信息安全标准，同时联邦机构将扩展至国际安全网络中心，提升其访问与恶意攻击相关的外部数据权限
英国	2014 年 10 月	工程和物理科学研究委员会（EPSRC）总投资 250 万英镑资助大学开展对国家重要工业控制系统（ICS）的网络安全开展新研究
法国	2013 年 2 月	在全国安全系统信息机构（ANSSI）的引领下，各行业相关机构和法国政府机构联手成立一个信息安全工作组，旨在在提高关键基础设施的网络安全方面巩固具体和实操的计划
欧洲	2014 年 12 月	欧洲网络与信息安全局(ENISA)针对工业控制 系统发布了《对网络安全的 ICS / SCADA 专业技能认证》
	2015 年 8 月	欧洲委员会跟欧洲网络安全组织（ECSO）签订了促进网络信息安全解决方案研究和发展的协议。在这个合作关系下，欧盟委员会声明将投资 4.5 亿欧元于 Horizon2020 研究创新项目，ECSO 将在 2020 年之前持续投资 13 亿欧元在其联盟国家内提高网络安全解决方案的研究与发展
日本	2015 年 5 月	举行网络安全战略本部会议，制定了新的《网络安全战略》，提出了"信息自由流通"、"法治"、"对使用者的开放性"、"主动遏制恶意行为的自律性"、"政府和民间等多方面的合作"等 5 项原则

国际上标准化组织针对工业控制系统的信息安全标准化一系列研究主要包括 NIST、IEC 以及美国行业规范为主的各类标准等。IEC62443 是专门针对工业自动化和工业安全的系列标准。NIST 制定工控安全主要标准，标准可跨行业，并且标准不停的滚动发布。从标准成果还可以看出，美国针对 SCADA 控制系统的安全标准比较多，主要因为 SCADA 的安全问题在控制系统中尤为突出。

此外，美国能源部于 2011 年发布《实现能源供应系统信息安全路线图》，是对 2006 年《能源行业防护控制系统路线图》的更新完善，该路线图由能源领域控制系统工作组起草完成。该路线图对能源输送系统的前景进行分析展望，确定 2020 年前美国能源输送系统网络安

全目标。同时向相关政府部门和私营企业提出了 5 项战略，相关规范措施还包括美国能源部发布的《中小规模能源设施风险管理核查事项》、美国核管理委员会发布的《核设施网络安全措施》等。

3.1.1 美国

美国政府早在 21 世纪 90 年代初便开始关注工业控制系统安全问题。自从 1998 年首次提出了信息安全的概念，便更将工控安全视为国家间战略制衡的重要手段。

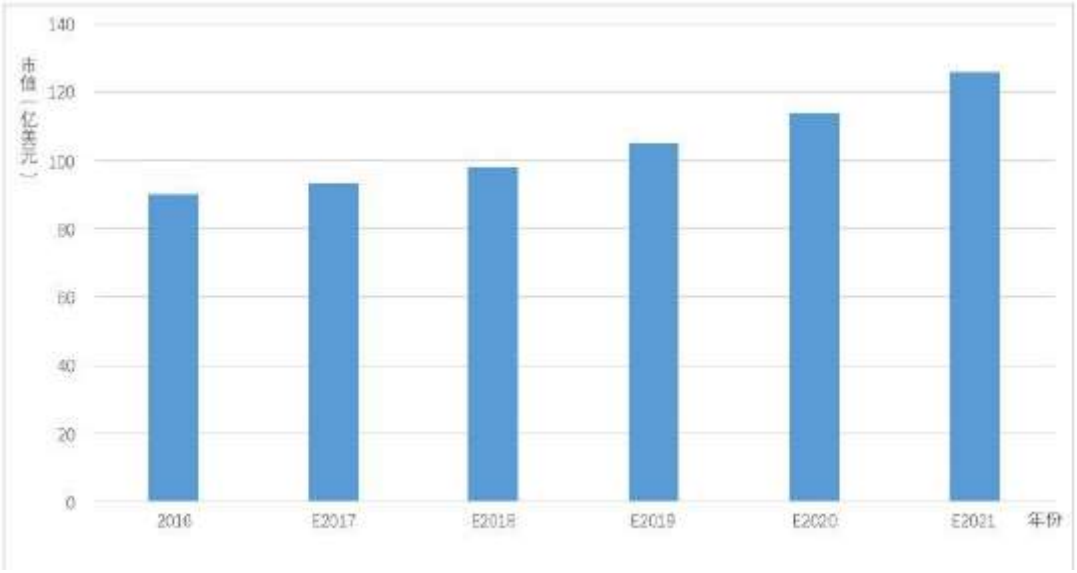
图表 13 美国推进工控安全建设进程

美国在工控安全保障领域保持着技术领先，突出体现在工业控制系统安全研究重点实验室的建设方面，六家国家实验室对工业控制系统安全开展了系统、全面的研究，范围涵盖工业控制系统安全标准、协议制定、工业控制安全威胁研究、安全控制研发等。

实验室	实验室简介	工控安全研究概况
爱达荷国家实验室（INL）	1949 年成立 研究领域：核能、国土安全、能源与环境 运营 SCADA 安全中心	主持国家 SCADA 测试床（NSTB）项目 在通信协议、系统评估漏洞削减和系统防御有多项研究成果 当前研究重点为开发控制系统态势感知技术的相关工具
阿贡国家实验室（ANL）	1946 年成立 研究领域：科学设施、能源资源、环境	已开展 SCADA 系统调查和评估研究 为天然气管道运输系统设计 SCADA 整合远程设施控制方案
西北太平洋国家实验室（PNNL）	1965 年成立 研究领域：环境、卫生、能源、计算机、科学与安全	提出 SSCP 概念（安全 SCADA 通信协议） 当前研究为构建能源行业安全通信架构、开发现场设备管理软件应用、开发加密信任管理软件应用、开发协议分析器
桑迪亚国家实验室（SNL）	1949 年成立 研究领域：核武器防扩散和材料控制、能源和关键基础设施以及国家安全	建立 SCADA 安全发展实验室和研究中心 发布一系列控制系统研究报告，涵盖控制系统设备安全、电力供应和能源可靠性、控制系统安全标准、基础设施控制系统等
橡树林国家实验室（ORNL）	1943 年成立 研究领域：中子科学、化学与放射化学技术、复杂生物系统、能源科学等	正进行通过便携式验收测试仪和协议进行 SCADA 系统网络安全测试项目 开发下一代安全的、可扩展的智能电网通信网络
洛斯阿拉莫斯国家实验室（LANL）	1943 年成立 研究领域：国家安全、空间探索、可再生能源、医药、纳米技术、超级计算机	当前研究 SCADA 通信领域 致力于开发效益建模工具

图表 14 美国 6 大工控安全国家实验室概况

除此之外，美国进一步加大工控安全能力建设，凭借其雄厚的信息技术基础和创新能力，率先建设形成了多位一体的工控安全保障体系。美国工控安全保障体系由管理体系、技术体系、产业体系构成。在管理方面，政府给予高度重视，设置有专门的组织机构提供保障，并在政策、法规、规划等方面均有大力支持。在技术方面，拥有许多世界一流的研发实验室，进行一系列世界范围内工业控制系统相关安全标准的研制，庞大的研制工作强有力支撑着美国的工控安全保障体系。在产业方面，拥有强大的研发和产业化力量，诸如爱默生、霍尼韦尔、罗克韦尔、通用电气等，且与相关管理机构、技术机构等形成有效配合，成为美国工控安全保障体系中不可或缺的后盾。



图表 15 全球工控安全市场规模

根据 M&M（MarketandMarket）市场调研报告，全球的工业控制系统安全的市场规模预计从 2016 年的 90 亿美元市值增长到 2021 年的 126 亿美元市值，年复合增长率为 7%。预计在这五年期间，北美地区的工控系统安全市场占有最大的全球市场份额，占全球市场份额达 39%，主要得益于该地区的众多领先的工控系统安全提供商如赛门铁克，IBM，CSC，思科，McAfee 等。该地区预计在 SCADA 和信息安全技术上持续投资超过 40 亿美金。在全球的范围内，工控系统安全的主要提供商包括了德国西门子，法国施耐德，美国的霍尼韦尔国际集团、IBM、思科系统、赛门铁克等，这些领先的供应商主要集中在美国。

从垂直领域来看，当前的数据表明无论在投资和开发方面，电力能源和公关事业这领域将继续成为工控系统安全占比最大的应用领域。其次是商业，通信系统和制造业领域。报告预测，能源市场和新兴国家的工控系统安全基础设施布局将会很大程度上促进工控安全市场的发展。

排名	厂商	总营收（百万美元）
1	通用电气公司（GENERAL ELECTRIC）	140,389.00
2	西门子（SIEMENS）	87,660.00
3	日立（HITACHI）	83,583.50
4	博世公司（ROBERT BOSCH）	78,322.70
5	松下（PANASONIC）	62,920.80
6	霍尼韦尔国际公司（HONEYWELL INTERNATIONAL）	38,581.00
7	三菱电机股份有限公司（MITSUBISHI ELECTRIC）	36,604.00
8	瑞士 ABB 集团（ABB）	35,481.00
9	施耐德电气（SCHNEIDER ELECTRIC）	29,551.10
10	艾默生电气（EMERSON ELECTRIC）	22,304.00

图表 16 2016 年全球十大工业自动化企业排行榜

以发达国家为例，国外的一些著名的工控提供商和信息安全厂商都在工控安全方面展开深入研究，

不断提高相应产品的技术和完善信息安全的解决方案，目前相关的技术日趋完善。

美国在工控安全技术的研发上一直处于领先地位，其背后是由传统信息安全厂商、传统的工控厂商以及一些新兴的专业工控安全厂商联合推动的。传统的信息安全厂商有赛门铁克、MCAFEE、思科，这些厂商在工控安全领域展开了深入研究，为工控信息安全方面提供了众多成熟的技术。不仅是传统工控厂商罗克韦尔、通用电气或是一些新兴的专业工控安全厂商，均为工控系统的安全防护及产品服务做出了很大贡献。

技术厂商	技术优势
赛门铁克	两大防护：威胁防护＋信息防护 统一安全分析平台搭配全球智能情报网对行为与威胁进行全方位实时分析
McAfee	全面的解决方案（网络防火墙，防恶意软件，数据丢失防护，变更控制，安全 SaaS 等） 利用与关键基础设施高度相关的产品技术： 动态白名单，安全信息和事件管理（SIEM），入侵防御系统（IPS），数据库活动监视（DAM）以 面对客户的四个主要需求，即态势感知，多区域保护，对 SCADA 和 ICS 解决方案的本地支持， 以及持续合规
思科	攻击发生前：ASA 防火墙技术，ASA 下一代防火墙技术，ISE 身份认证引擎技术和 VPN 技术 攻击发生时：下一代入侵防御技术，邮件安全技术，Web 安全技术 攻击发生后：恶意软件防护技术和异常流量分析技术。

图表 17 美国工控安全厂商的技术优势

3.1.2 欧洲

在欧洲则以德国西门子、法国施耐德电气为代表的工业控制系统提供商为主，这两家企业的市场和技术优势也将在未来很长一段时间内奠定其在工控安全领域的领先地位。

技术厂商	技术优势
西门子	“纵深防御”：在外部世界的威胁和工控网络之间建立尽可能多层次的防护。 工业安全解决方案包括物理环境安全、安全策略与流程、划分安全单元与 DMZ、部署防火墙与 VPN，进行系统加固、管理用户账号、部署补订管理、监测与防护恶意软件 提供贯穿整个生命周期的支持，包括咨询服务、安全分析、客户培训和托管服务等
施耐德	致力于提升自身产品的安全性，并助力全行业广大用户提升整体信息安全水平和风险防范能力 针对工业用户的实际需求，首创“自下而上”的三级纵深防御体系，使更多的用户得以灵活、务实 地满足其工业信息安全需求

图表 18 欧洲工控安全厂商的技术优势

3.1.3 加拿大

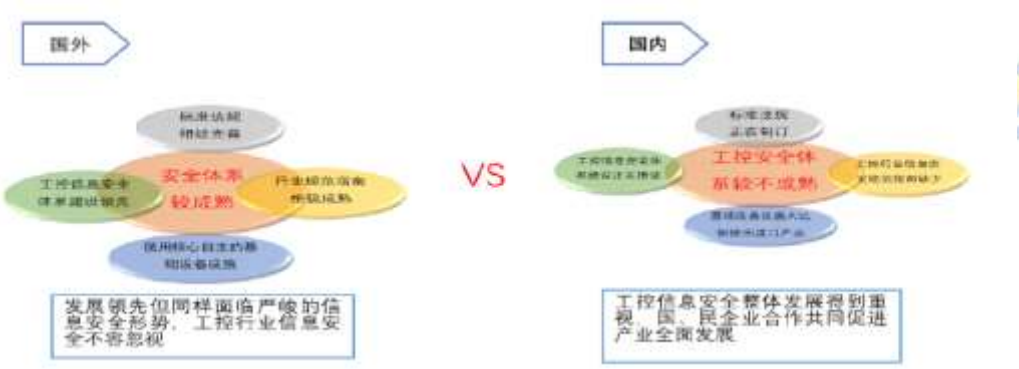
在专业的工控安全厂商方面，加拿大 Tofino（多芬诺）公司曾以其业内著名的工控系统防火墙成为业内领先的工控系统安全的专业厂商，芬兰的科诺康公司（Codenomicon）是以其用于漏洞发现的 fuzzing（基于缺陷注入的自动软件测试技术）测试工具而在工控系统安全领域拥有重要的地位。

技术厂商	技术优势
Tofino 多芬诺	以工控系统防火墙成为业内领先的工控系统安全的专业厂商，产品在石化等多个行业应用广泛 Tofino 防火墙基于内置工业通讯协议的防护模式，不仅是在端口上的防护，更是基于应用层上数据包的深度检查、协议分析，属于新一代工业通讯协议防火墙。
Codenomicon 科诺康	其 Defensics 测试解决方案能够重点对测试目标的响应进行分析，并且通过自动分析定位那些虽然不会导致系统崩溃，但会影响系统安全的敏感安全弱点。 Defensics 测试解决方案采用能完全识别协议或被测文件格式的 fuzzing 技术，当没有测试方案适用于 fuzzing 网路协议或文件格式时，科诺康也会提供适用于 IP 网络协议和文件格式的样板 fuzz 测试技术。

图表 19 多芬诺和科诺康的技术优势

3.2 我国工控安全整体情况不容乐观

在我国，尽管工控信息安全的整体发展得到了重视，国民企业也共同合作促进产业发展，但是我国的工控安全体系还处于不成熟阶段，与国外发达国家相比有一定的差距。具体表现在于以下几个方面：1）工控系统产品大比例使用进口产品，自主可控无从实现；2）标准和安全体系还不够完善；3)我国工控系统安全防护问题频出。



图表 20 国内外工控安全对比

3.2.1 我国防御工控安全存在先天不足

对于我国而言，工业控制系统安全所面临的重要问题就是自主可控的问题，我国在工控领域对国外设备和技术的依赖程度强。据中国产业信息研究网调查统计结果显示，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；在我国的工控系统产品上，国外产品已经占领了大部分市场，如 PLC 国内产品的市场占有率不到 1%，工业中用到的逻辑控制器 95%是来自施耐德（法国）、西门子（德国）、发那科（日本）等的国外品牌。

重要工业控制系统基本情况调查，统计显示，全市 24 个企业共计 1213 个重点工业控制系统，主要分属

化工、电力行业和城市公用事业服务领域。德国西门子公司生产的可编程控制器（PLC）和我国浙江浙大中控公司生产的分布式控制系统（DCS）在扬州市工业企业应用广泛，其中德国西门子公司生产的可编程控制器占全部调查企业工业控制系统总数的 87%，占全部调查企业可编程控制器应用总数的 95%以上。

3.2.2 工控系统安全的可控的缺失将会带来巨大的安全隐患

我国大部分工控系统核心控制模块从国外引进，而国外工业控制芯片、工业控制系统产品设计和配置等都可能存在漏洞。这些漏洞的存在将有可能给予不法分子利用病毒进行网络攻击的机会，从而造成严重后果。另外，国家层面的威胁也有可能由于我国工业控制系统被硬件设备生产国操控而加剧，标准和安全体系尚未完善。

早期，我国发布了《工业控制系统信息安全》的评估规范和验收规范两个标准，作为我国工控安全最先发布的两个有内容的国家标准，解决了我国工控安全无标准可依的窘境以及验收有标准可依的困境。在行业方面，电力、石化、核电及烟草行业也有相应标准。我国目前在研的工控安全标准有 19 项之多，其中工控安全管理标准 4 项，工控产品及系统信息安全标准 9 项，工控安全评估标准 1 项，工控安全防护及检测技术标准 5 项。尽管如此，从国外工控安全标准优势方面对比来看，我国的工控安全标准还有以下差距：1）我国还未发布成熟的工控安全基本标准；2）我国还未有像美国的 ISCI 这类对工控安全标准符合性检测及授权的组织；3）我国已发布的几个标准，缺乏标准宣贯的手段，或者没有持续性的进行宣贯；4）在行业的标准上，我国的行业标准的覆盖面不如美国全面，仅仅主要集中在电力、石化、核电这类重点领域。因此，为了做到工控安全真正有标准可依，需要加快标准研制过程。

3.2.3 我国工控安全防护仍然面临诸多问题

1） 我国网络安全专业人才紧缺

根据《2015 年中国工业控制系统信息安全蓝皮书》，我国重要行业信息系统和信息基础设施需要各类网络空间安全人才 70 万，但预

计到 2020 年，需要各类网络空间安全人才约 140 万，而我国高校每

年培养的信息安全相关人才不足 1.5 万人，远远不能满足网络空间安全的需要。

2） 大多数工控系统运营企业负责人的信息安全意识不足

由于工控系统信息安全的相关工作的参与者大多来自于各级主管部门、行业协会及信息安全公司，而作为实际使用者的运营企业明显缺乏参与度，对在工业现场的应用需求、应用场景的了解不明确。另外，一些

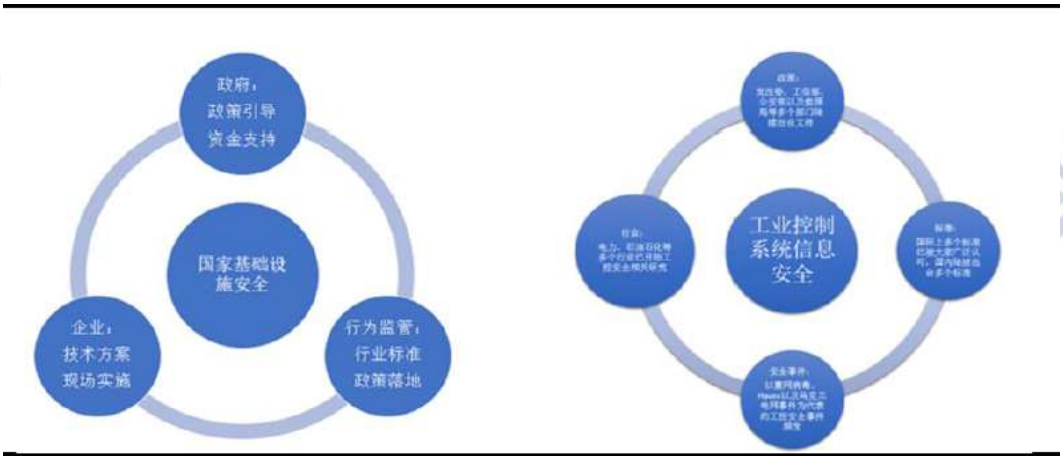
用户对于信息安全存在严重的侥幸心理，企业普遍认为工控系统只有对外联网时，才需要进行信息安全防护，而工控系统病毒入侵才是导致信息安全事故发生的主要方式。认知与实际的偏差导致我国工控安全事件时有发生。

3） 工控系统信息防护解决方案成本仍然较高

当前大部分工控系统信息安全产品价格昂贵，如按照纵深防御理念，每台控制器都需要一个工业防火墙，解决方案的总体成本价格不菲。况且工控安全产品对运营或业务的表现没有带来明显的影响，导致大部分公司对安全预算和支出的决策变得困难。当市场不景气时，用户将精力和关注度更多地转向于如何提升销售额和压缩成本的经营层面，降低了用户对于 ICS 信息安全的投入，从而阻碍了工控系统信息安全发展的步伐。

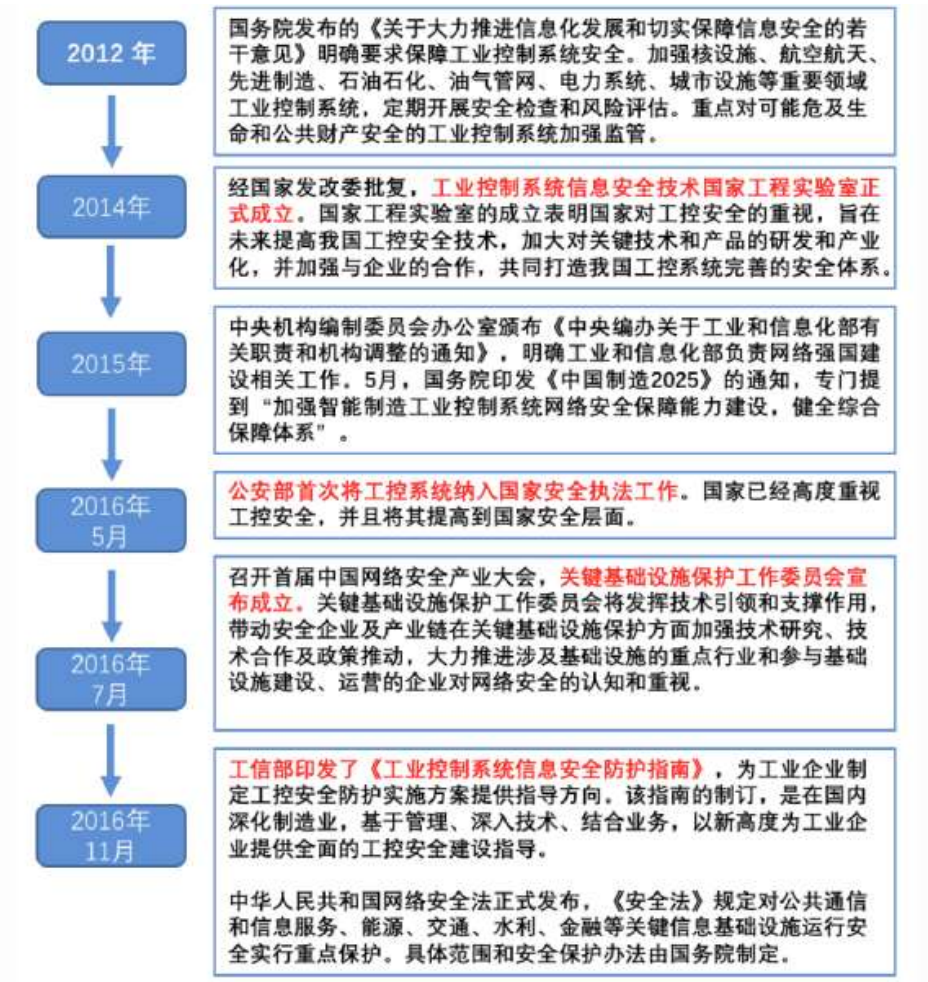
3.3 加快推进信息基础设施安全保障体系，工控安全发展爆发在即

3.3.1 政策支持力度空前



图表 21 政府企业合力推进国家基础设施安全

早在 2011 年，工信部发表了《关于加强工业控制系统信息安全管理的通知》，强调加强工业信息安全的重要性、紧迫性，并明确了重点领域工业控制系统信息安全的管理要求，其中特别提到了与国计民生紧密相关领域的控制系统，如核设施、钢铁、石油石化、电力等。自此，工控安全开始受到政府的高度重视，国家发改委开展工业控制系统信息安全专项的工控安全试点。



相关政策的出台标志着我国已经将工控安全问题提升到了国家战略高度，特别是其中关乎到国计民生的基础设施行业，在鼓励两化融合和向工业 4.0 发展的同时，加强对工控领域的投入和重视。国家政策对于工控安全的重视，将会对工控网络安全市场带来实现爆发式。未来工业控制网络安全领域将存在巨大的市场潜力和需求。在 2016 年实施的《工业控制系统信息安全防护指南》基础上，2017 年工信部将会加快出台《工业控制系统信息安全保障行动计划》《工业控制系统信息安全防护能力评估方法》等系列规范标准，同时，《网络安全法》将于 2017 年 6 月起施行，工控安全被纳入信息安全等级保护也正在推进，一旦落实，将有望复制特定信息安全领域的发展模式，比如内网安全终端，在未来形成新的市场爆发点。

3.3.2 等级保护制度推动我国信息安全市场大发展

信息安全等级保护制度是我国信息安全保障工作的一项基本制度和基本国策，也是开展信息安全工作的基本方法和促进信息化、维护国家信息安全的根本保障。等级保护的主要工作是对信息系统进行定级，根据不同等级进行安全保护和监管，同时也对信息安全产品分等级使用和管理，对信息安全事件分等级响应和处置。

受侵害客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

图表 22 信息安全等级保护分级

信息安全等级保护的基本安全要求分有两个方面：一是技术要求，二是管理要求。

图表 23 国家等级保护基本安全要求

信息系统的安全等级保护评测包括：系统定级、系统备案、安全建设整改、等级保护评测和定期安全检查五个环节，其中安全建设整改对厂商在信息安全的建设方面有更高的要求，是推动信息安全防护需求的至关重要的环节。

自从 2007 年发布了《信息安全等级保护管理办法》之后，信息安全等级保护在全国范围内开展评级工作，信息安全在我国国家安全战略和政策的等级保护下早已迎来了蓬勃的发展机遇，行业的市场机会不断扩大。

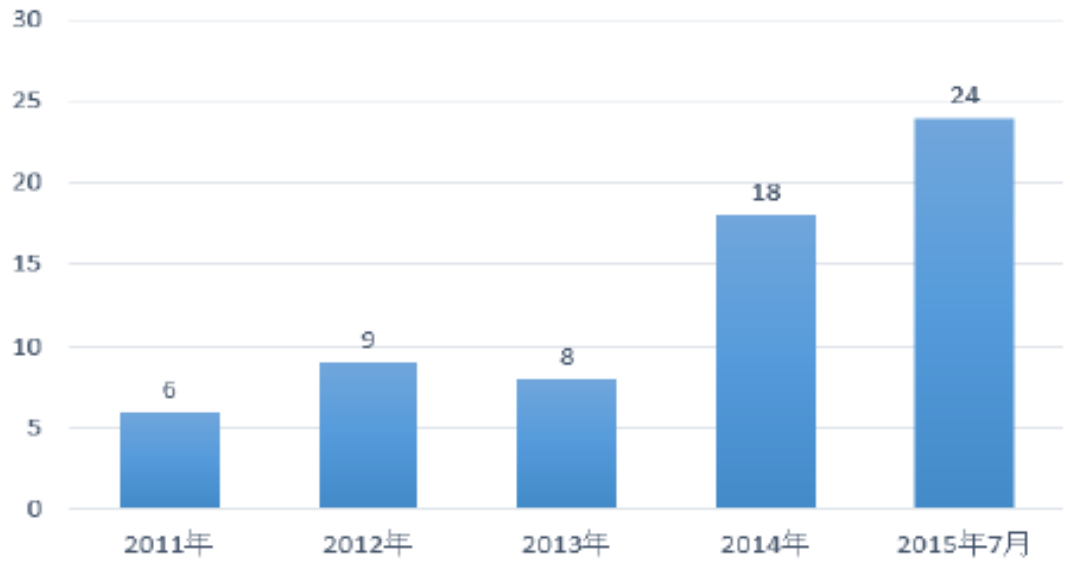
综上，我国工控系统安全在信息安全等级保护下将迎来值得期待的发展前景，主要原因有两个：首先，工控安全被信息安全等级保护所涵盖，信息安全等级保护适用于工控安全领域，工控安全的发展在信息安全等级保护的国家高级重视层面下将得到支持；其次，工控安全在信息安全等级保护下有望复制信息安全的发展模式。目前，国家正在加强网络安全等级保护标准的制定工作，包括云计算、移动互联、物联网、工业控制和大数据等新技术的标准。原先的基础要求变成了系列标准，变成了六个部分，包括通用要求、云计算、移动互联、物联网、工业控制和大数据六个部分。因此，随着等级保护标准的完善，工业控制系统未来的安

全防护技术要求将会大大提高，工控安全领域有望实现突破性发展。

四、 工控安全处于市场发展早期，空间巨大

4.1 工控安全产品方兴未艾

随着工业系统信息安全产业近几年的蓬勃发展，我国专业从事工控系统信息安全工作的企事业单位逐年增多，设计研发的产品也越来越多。总体来看，从 2011 年开始，我国通过公安部销售许可认证的工控信息安全产品逐年增长，尤其是 2014、2015 年两年，更多呈现出井喷式发展趋势。截止 2015 年 7 月，通过认证的产品数量已达 24 个之多。



图表 24 我国历年通过认证的工控安全产品数量

随着工业控制系统信息安全产品数量不断攀升，我国工业控制系统信息安全的种类也不断多样化，产品线也不断完善。统计我国近年来通过公安部销售许可认证的工业控制系统信息安全主要产品，产品类型及名称列于下表，主要包括工业网匣、工业防火墙、工业防火墙、工业防护网关、工业安全交换机、工业安全网关等。

目前，工控防护主要是在不改变工控系统基础架构的前提下，通过增加与工控系统高度集成的信息安全组件达到工控系统的信息安全目标。产品主要包括防护类产品、检测类产品以及管理服务平台三大类。目前主要以隔离网关（装置）和防火墙类等硬件产品为主，两者的市场份额共达到整体 ICS 信息安全市场的 71%，占主导地位；安全管理平台、安全审计、安全监测等出现一定提升。安全培训和服务被越来越多机构和用户接受。

近年来恶性工控安全事件频发，一些大型攻击行为甚至上升到国家层面，人们对工业控制系统安全的重视程度日益提高，也正是从这一时期开始，大多数安全组织特别是国家力量开始对工业控制系统的安全性进行研究。整体来看工业控制系统网络安全防护理念经历了四个阶段的演变：强调隔离、纵深防御、持续性防御、以攻为守。

目前市场上工控安全技术理念主要以监、评、防、融四大核心功能为主：

（1）监测预警：对接入互联网的工业控制系统面临的威胁态势进行监视，并对工业控制网内部进行全时段、全流量及多业务分析，构建早期异常行为和攻击前兆特征发现预警能力，提供工控信息安全事件的追溯能力。

（2）攻防评估：以高逼真度工业控制系统攻防演示仿真环境为基础，分析工控设备、网络、协议、系统、应用、软件及工艺流程等方面存在的漏洞，同时评估其存在的风险，并开展合规性检查，并利用演示环境评估安全方案的可行性、稳定性等。

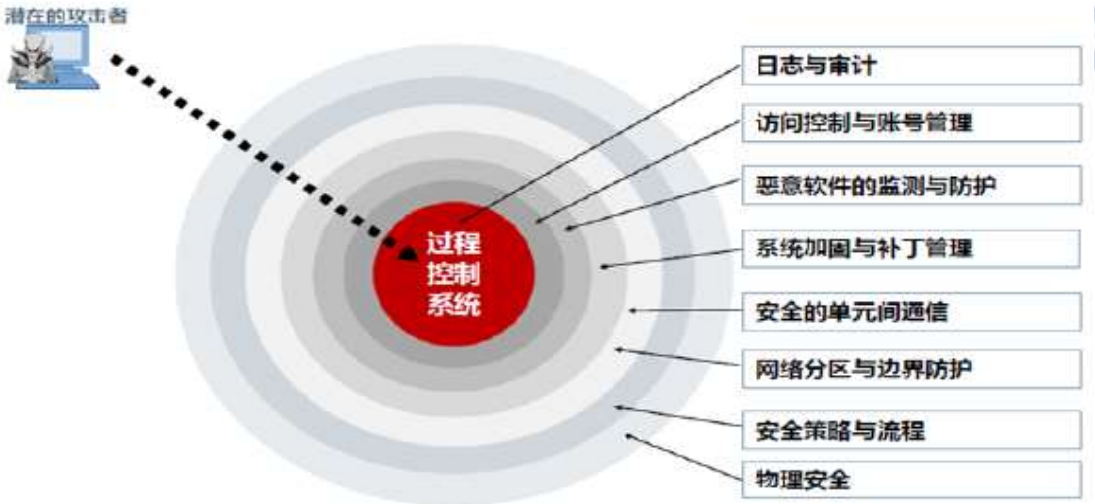
（3）体系防御：以工业控制安全生产为前提，通过安全分域、边界防护、密码保护、流量监控等手段，提供工控信息安全解决方案和服务，强化工控信息安全管理能力，保障工控信息系统的运行安全。

（4）融安于用：以围绕军工、核工业、石油石化、轨交、烟草、冶金等行业的安全需求，促进信息安全与行业应用的深度融合，确保工控系统应用安全，提升工控安全产品的可靠性，满足客户定制化需求，增强用户“敢用”、“会用”、“管用”的最佳实践。

图表 25 工控安全技术防护体系

目前市场上的防护技术主要还是以边界防护为主，其主要产品为针对工控安全问题设计的的工业防火墙。

其不仅具有普通防护墙的访问控制功能，更重要的是它提供针对工业协议的数据级深度过滤然而，近年来工控安全事件的频频爆发表明，依赖于传统边界安全防护的工控安全技术已经无法解决工业控制系统面临的诸多问题，相关的防护技术已经向纵深防护的方向发展，从工业控制系统的安全生命周期的角度来考虑工业控制系统的安全。从漏洞扫描、安全审计、态势感知、综合管理平台的方向发展工控安全技术，以及综合应用相关技术来应对工业控制系统所面临的安全威胁已成为新的趋势。



图表 26 工业网络纵深防御体系框架

随着两化融合、互联网+、中国制造 2025 的出现，各行业新体态形式渐渐兴起，如智能发电、虚拟电站、智能风电、智能工厂、云工厂等出现，使业务系统之间的交叉和连接关系变得更加复杂。传统控制系统的边界已经开始变得不那清晰，原有的以边界防护为主手段的防护体系必将面临的重大挑战。融合工控安全技术、虚拟化安全技术、云安全技术、大数据等技术的防护体系会成为未来工控安全发展的一个重要方向。

4.2 市场仍处于早期体量偏小，成长空间巨大

4.2.1 全球工控安全行业整体市场规模

根据 M&M（MarketandMarket）市场调研报告，全球的工业控制系统安全的市场规模预计从 2016 年的 90 亿美元市值增长到 2021 年的 126 亿美元市值，年复合增长率为 7%。预计在这五年期间，北美地区的工控系统安全市场占有最大的全球市场份额，占全球市场份额达 39%，主要得益于该地区的众多领先的工控系统安全提供商如赛门铁克，IBM，CSC，思科，McAfee 等。该地区预计在 SCADA 和信息安全技术上持续投资超过 40 亿美金。在全球的范围内，工控系统安全的主要提供商包括了德国西门子，法国施耐德，美国的霍尼韦尔国际集团、IBM、思科系统、赛门铁克等，这些领先的供应商主要集中在美国。

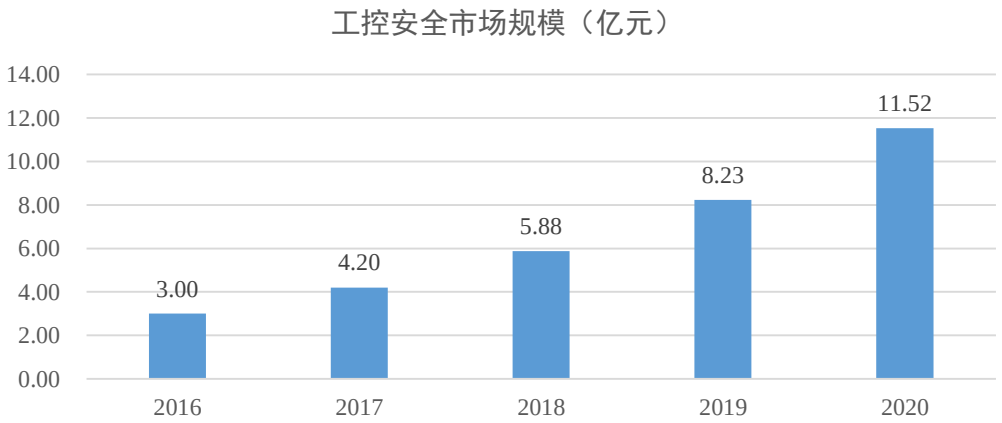
4.2.2 我国工控安全市场规模

工业和信息化部电子科学技术情报研究所与中国工控网共同发布《2016 年工业控制行业市场规模及发展趋势分析》显示：20 世纪 90 年代以来，中国工业自动化行业的产量一直保持在年增长 20%以上。中国已成为世界最大的自动化控制设备市场，自动化技术正在向智能化、网络化和集成化方向发展。2014 年中国国工业自动控制系统装置制造行业销售收入 3,304 亿元，2015 年的规模达到 3,550 亿元，同比增长 11.78%。在国家大力发展高端装备、智能制造、产业升级、人力成本上升和替代进口等众多因素的推动下，未来中国自动化控制市场依然将保持增长，预计 2020 年中国工业自动控制系统装置制造行业销售收入将达 4,800 亿元。

图表 27 中国工业自动控制系统装置制造行业销售收入（亿元）

根据工控网络安全在工业控制网络中支出占比 2%-3%的预测，我国的工控网络安全市场将在 2020 年达到市场潜力在 100-200 亿人民币市场预期规模，未来的市场潜力巨大。但由于市场渗透率现阶段还较低，此数据预测还是较为乐观，

根据现阶段的市场状态，保守测算：按照 2016 年市场规模在 3 个亿左右（数据来源：方正证券），假设年复合增长率在 40%（假设依据：北信源作为内网安全的龙头企业，在内网安全等保制度出台期间，2011 年至 2015 年期间其业绩维持了年均 37.89%的年均复合增速），可以预计未来 2020 年将达到将近 12 亿的市场规模，如下图：



图表 28 工控安全市场规模（亿元）

相比于工控安全全球市场的繁荣，国内工控安全市场的现阶段的市场容量还较小，主要是由于市场的渗透率较低所导致的，渗透率低主要是由于企业负责人对于工控安全的认知和重视有限，以及企业对工控安全方面的经费预算和法律政策没有明确要求所致。2016 年被业内称为工控安全的元年，是由于产业政策阶级引导及“工业 4.0”，企业对于工控安全的需求日益增大；对于工控安全的导向越来越明确，企业对于工控安全的认知和预算的增加，促使市场将会在接下来的几年内快速增长。市场渗透率会逐年快速增长。市场容量将会随着市场渗透率的提高而快速增长。