IT/OT一体化的工业信息安全态势报告（2018）

工业控制系统安全国家地方联合工程实验室**2019.3**

主要观点

* 工业互联网安全是一个新战场，黑客组织有目的的向高价值目标投放勒索病毒、恶意软件等，严重威胁到国家安全；
* 勒索病毒攻击已经成为工业企业面临的最大安全问题之一，勒索病毒导致工业互联网企业停产的事件频繁发生。系统暴露，系统漏洞，远程维护成为勒索病毒入侵的主要原因。勒索病毒的流行彻底打破了“一般互联网安全威胁对工业系统是无害的”这个传统认知；
* 将近一半工业企业遭受过生产设备安全故障、电脑蓝屏、重启等安全问题，但确有69.4%的企业表示没有发生过网络安全事件。当企业内部电脑出现大量蓝屏、重启等现象时，往往意味着企业已经遭到了攻击，但企业管理者未作为安全事件来进行响应和调查，错过处置最佳时机；
* 国内76.1%的被调研工业企业非常重视工业互联网安全，工业互联网安全市场将有巨大的需求；梳理工业资产，80%的防御工作可以放到工业主机防护.；
* 目前看不到收益、人才缺乏是阻碍安全投资建设的重要因素。工业互联网安全建设最大的难处在于没有造成安全事故，企业高层较难理解安全建设短时间内给企业带来的收益，工业互联网安全建设不被工业企业理解；
* 工业互联网安全防护体系还没有完全建立起来，工业安全产品和服务的部署率不足、安全管理水平较低、相关人才缺乏；
* 工业互联网安全已经逐步引起社会各界的广泛重视，政府主管部门出台一系列法律法规、政策和指导意见。同时，工业企业正在投入更多的资金进行安全建设，信息安全企业也推出了更多的安全产品和服务。

摘要

* 全球工控系统联网组件总数量为175632个，主要集中在美洲和欧洲国家，中国联网组件总数量为6223个，超出意大利365个，排名全球第五；
* 在所有的工控系统组件中，工控设备的暴露是最为危险的。工控设备的暴露意味着攻击者有可能直接对设备本身发动攻击。
* 工业互联网安全漏洞数量快速增长，类型多样化特性明显，且高危漏洞占比较高；漏洞涉及行业广泛，以制造业、能源行业为主；漏洞涉及厂商以国际厂商为主；
* 工业企业对自身安全建设程度普遍“自我感觉良好”，实际上是一种过度乐观的状态。绝大多数工业企业的实际安全状况都让人十分堪忧；
* 国内53.1%的企业遭受过生产设备安全故障、电脑蓝屏、重启等安全问题，仅有不足25%的企业没有出现过蓝屏、重启现象，我国工业互联网安全建设情况并不乐观；
* 将近有1/4的被调研企业表示对生产车间设备、电脑是否出现过蓝屏、重启现象表示“不掌握”。“不掌握”也就意味着企业其实并没有部署足够的网络安全监测措施以实时了解其工业系统的网络安全状况；
* 多数工业企业过低的估计了自身遭受网络攻击风险的可能性；
* 工业互联网存在安全管理不到位、安全责任模糊、工业主机几乎“裸奔”等问题，造成安全风险突出；
* 工业主机投入运行后，一般较少打补丁，同时老旧操作系统难以安装杀毒软件，几乎处于“裸奔”状态，这是“永恒之蓝”爆发一年多以后，工业主机仍然频频遭受勒索软件攻击的最主要原因；工业互联网安全事件发生后，应急响应的处置能力至关重要；
* 在工业互联网信息安全领域，传统的安全防御产品已逐渐乏力、无法有效应对越来越严重的安全威胁，构建层次清晰、定位明确、融合联动的工业互联网信息安全产品体系将成为产业未来发展的重要趋势；
* 国内76.1%的工业用户非常重视工业互联网安全的建设；将近49.1%的工业企业在安全方面的投入有明显增加趋势；超过1/4的企业对安全的投资金额在10-100万之间；国内43.9%的被调查者认为工业互联网安全投入应该占工业互联网投入金额的5%-10%；
* 人才的缺乏是影响工业互联网建设的首要因素，看不到收益仍然是阻碍安全投资建设的最主要因素；
* 国内69.1%的工业企业有专门的人员/部门负责安全，但负责安全的人数差距较大；
* 八成以上的国内工业企业有意愿部署工业互联网安全服务，39%的企业能够接受的采购费用低于20万；
* 安全问题发生后，国内51.8%以上的企业愿意选择一家综合能力强的规模较大的安全厂商解决安全问题；
* 工业企业安全安全服务市场显著增多；多方协作趋势明显；防护类产品需求较高，网络安全关注点居多，非防护类产品比例相当，呈现多样化趋势；
* 针对第三方服务供应商的攻击同样会影响到工业互联网安全，应加强工业互联网供应链的安全；
* 梳理工业资产，重点关注工业主机资产；做好工业主机防护；持续监控生产风险。
* 统筹规划，合力发展；顶层设计，标准推动；重视人才，培养高端。

目 录

[研究背景 1](#_Toc2005551)

[第一章 工业互联网安全风险态势 2](#_Toc2005552)

[一、 工控系统互联网暴露情况 2](#_Toc2005553)

[二、 工业互联网安全漏洞分析 3](#_Toc2005554)

[（一） 安全漏洞数量快速增长，安全形式日益严峻 3](#_Toc2005555)

[（二） 安全漏洞类型多样化特性明显 4](#_Toc2005556)

[（三） 高危漏洞占比较高 5](#_Toc2005557)

[（四） 漏洞涉及厂商以国际厂商为主 5](#_Toc2005558)

[（五） 漏洞涉及行业广泛，以制造业、能源行业为主 6](#_Toc2005559)

[三、 工业企业网络安全感知 6](#_Toc2005560)

[（一） 工业企业对自身安全建设水平的认知 6](#_Toc2005561)

[（二） 工业企业对自身面临安全风险的感知 7](#_Toc2005562)

[（三） 工业企业对网络安全事件影响的认知 9](#_Toc2005563)

[四、 工业互联网安全威胁 9](#_Toc2005564)

[第二章 2018工业互联网安全工作进展 11](#_Toc2005565)

[一、 国外工业互联网安全重要文件 11](#_Toc2005566)

[二、 国内工业互联网安全重要文件 12](#_Toc2005567)

[三、 工业信息安全标准体系建设 15](#_Toc2005568)

[第三章 工业互联网安全产业态势 18](#_Toc2005569)

[一、 工业互联网安全产业结构 18](#_Toc2005570)

[（一） 高中低位能力安全产品体系 18](#_Toc2005571)

[（二） 防护监测层产品 18](#_Toc2005572)

[（三） 安全运营层产品 18](#_Toc2005573)

[（四） 安全态势感知层产品 19](#_Toc2005574)

[二、 Gartner关于OT市场的分析 19](#_Toc2005575)

[三、 工业企业网络安全投入分析 20](#_Toc2005576)

[（一） 工业互联网用户对工业互联网安全的重视程度 20](#_Toc2005577)

[（二） 工业互联网用户每年在工业互联网网络安全中的资金投入分析 21](#_Toc2005578)

[（三） 阻碍工业互联网安全投资建设的主要因素 23](#_Toc2005579)

[（四） 工业互联网安全团队现状 24](#_Toc2005580)

[四、 工业企业网络安全采购需求 25](#_Toc2005581)

[（一） 工业互联网安全产品需求 25](#_Toc2005582)

[（二） 工业互联网安全服务需求 26](#_Toc2005583)

[（三） 工业互联网安全应急响应需求 27](#_Toc2005584)

[第四章 工业互联网安全发展趋势 29](#_Toc2005585)

[一、 工业互联网安全建设发展趋势 29](#_Toc2005586)

[二、 工业互联网安全技术发展趋势 30](#_Toc2005587)

[（一） 引入数据驱动安全的技术理念 30](#_Toc2005588)

[（二） 基于威胁情报的工业威胁监测技术 30](#_Toc2005589)

[（三） 基于大数据的工业态势感知技术 31](#_Toc2005590)

[（四） 网络安全、功能安全、可靠性融合技术 31](#_Toc2005591)

[（五） 应用工业大数据进行异常发现和实体行为分析 31](#_Toc2005592)

[（六） 构建产业协同的联合防御体系 31](#_Toc2005593)

[第五章 工业互联网安全发展建议 33](#_Toc2005594)

[一、 对工业企业的建议 33](#_Toc2005595)

[二、 对安全服务机构的建议 33](#_Toc2005596)

[三、 对政府主管部门的建议 34](#_Toc2005597)

[第六章 工业互联网安全应急响应典型案例 35](#_Toc2005598)

[一、 某知名汽车零部件生产企业遭受“永恒之蓝”勒索病毒攻击 35](#_Toc2005599)

[二、 某大型炼钢厂遭受挖矿蠕虫病毒攻击 35](#_Toc2005600)

[三、 某卷烟厂遭受蠕虫病毒攻击 36](#_Toc2005601)

[四、 某半导体制造企业遭勒索软件攻击 37](#_Toc2005602)

[附录一 工业控制系统安全国家地方联合工程实验室 38](#_Toc2005603)

[附录二 工业互联网安全事件 39](#_Toc2005604)

[（一） 美国通报“熔断”和“幽灵”高危漏洞 39](#_Toc2005605)

[（二） 台积电三大基地疑遭勒索软件攻击停摆 39](#_Toc2005606)

[（三） 英国2700 万能源智能电表存在安全漏洞 39](#_Toc2005607)

[（四） 美国天然气输气管道电子系统遭受供应链攻击 40](#_Toc2005608)

[（五） 伊朗机场显示屏幕遭受黑客攻击 40](#_Toc2005609)

[（六） 俄罗斯400多家工业企业遭遇网络钓鱼攻击 40](#_Toc2005610)

[（七） 乌克兰国防系统密码竟为初始密码“123456” 40](#_Toc2005611)

[（八） 洛阳市北控水务集团远程数据监测平台遭到黑客攻击 41](#_Toc2005612)

研究背景

在政策与技术的双轮驱动下，工业控制系统正在越来越多地与企业内网和互联网相连接，并与新型服务模式相结合，逐步形成了工业互联网架构。工业互联网是数字浪潮下，工业体系和互联网体系的深度融合的产物，是新一轮工业革命的关键支撑。工业互联网的发展一方面极大的促进了生产效率和服务水平的提高，另一方面也使原本封闭的系统变得越来越开放，致使系统安全风险和入侵威胁不断增加，网络安全问题日益突出。

工业互联网目前已经广泛应用于电力、交通、石油、取暖、制造业等关键信息基础设施领域，一旦发生安全事件，往往会造成巨大的损失和广泛的影响。但是，由于工业互联网环境的特殊性，传统的IT信息安全技术并不能完全有效的保护工业系统的安全，甚至很多常用的安全技术都不能直接应用于工业网络的安全防护。对于工业互联网安全的分析与防护，需要使用一些专门的方法和专用的技术。

工业控制系统安全国家地方联合工程实验室（以下简称“联合实验室”）于2017年发布《IT/OT一体化的工业信息安全态势报告（2017）》，总结分析IT/OT融合带来的新挑战，给出工业信息安全建议和展望。

为给政府部门、科研机构和工业企业提供参考和借鉴，工业控制系统安全国家地方联合工程实验室（以下简称联合实验室）继续编撰了《IT/OT一体化的工业信息安全态势报告（2018）》。本报旨在总结全年的工业互联网安全进展从在市场、技术、产业、用户、事件的维度给读者对全年的安全发展状态有一个概要性的了解，并对未来的发展趋势有一个初步的预测，供合作伙伴及企业客户决策参考使用。

本报告对工业互联网安全漏洞的分析，采用了一种新型漏洞评分系统，将可见性、可控性、漏洞利用目标服役情况等体现工控安全特性的指标纳入量化评估范围。报告以联合实验室漏洞库收录的工业控制系统相关的漏洞信息为基础，综合参考CVE、NVD、CNVD、CNNVD四大公开漏洞平台发布的漏洞信息，分析工业互联网安全态势。

以往的很多工业安全研究报告缺乏对工业企业本身的深入研究，而工业互联网安全的建设发展离不开对工业企业需求的探讨。为了更真实的了解工业企业的安全需求，本报告特别对近400家工业企业进行了问卷调查，对工业企业的安全现状和安全认知进行了深入的分析。此外，本次报告还以360工业安全应急响应中心2018年处置的工业安全事件为基础，分析了4个典型案例。

最后，本次报告还总结了工业互联网安全发展趋势，分析了国内外政策法规及Gartner市场研究；对工业企业、安全服务机构、上级主管部门提出安全发展建议，希望能够帮助读者对工业互联网安全有一个更加全面、前沿的认识。

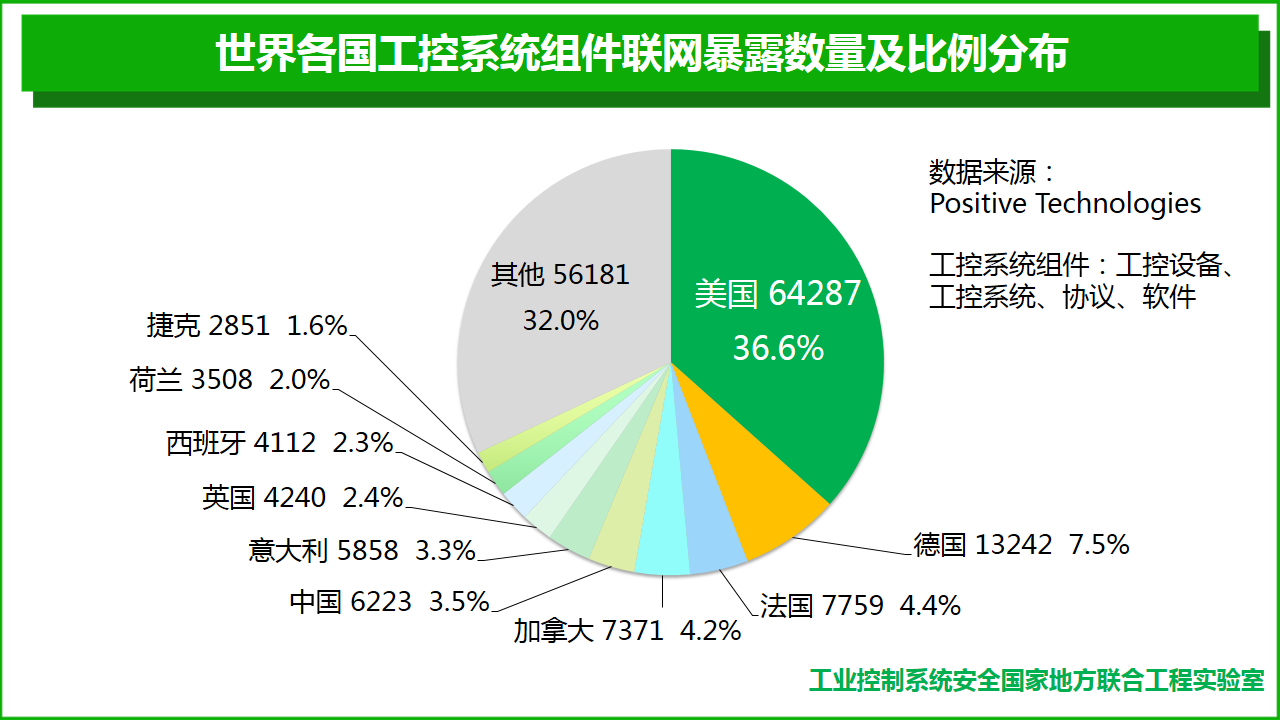
1. 工业互联网安全风险态势
2. 工控系统互联网暴露情况

工控系统在互联网上的暴露问题是工业互联网安全的一个基本问题。所谓“暴露，是指我们可以通过互联网直接对某些与工控系统相关的工业组件，如工控设备、协议、软件、系统等，进行远程访问或查询。

造成工控系统暴露的主要原因之一是“商业网络（IT）”与“工业网络（OT）”的不断融合。IT与OT网络的连通在拓展了工业控制系统发展空间的同时，也带来了工业控制系统网络安全问题。近年来，企业为了管理与控制的一体化，实现生产和管理的高效率、高效益，普遍推进生产执行系统，实现管理信息网络与控制网络之间的数据交换，实现工业控制系统和管理信息系统的集成。如此一来，如果未能做好必要的分隔管控工作，就会导致原本封闭的OT系统，通过管理系统与互联网互通、互联后，面临从互联网侧传播进来的各类网络攻击风险。

工控系统的直接连接到互联网，也称为“暴露”在互联网上，这个问题要一分为二的来看待：一方面，某地区工控系统在互联网上暴露的越多，往往说明该地区工业系统的信息化程度越高，工业互联网越发达；而另一方面，因为绝大多数的工业组件其实并不需要通过互联网进行远程操作，因此，暴露的比例越大，也往往意味着工业系统在信息化的同时，没有充分的做好必要的隔离工作，系统遭遇攻击和入侵的风险也越大。

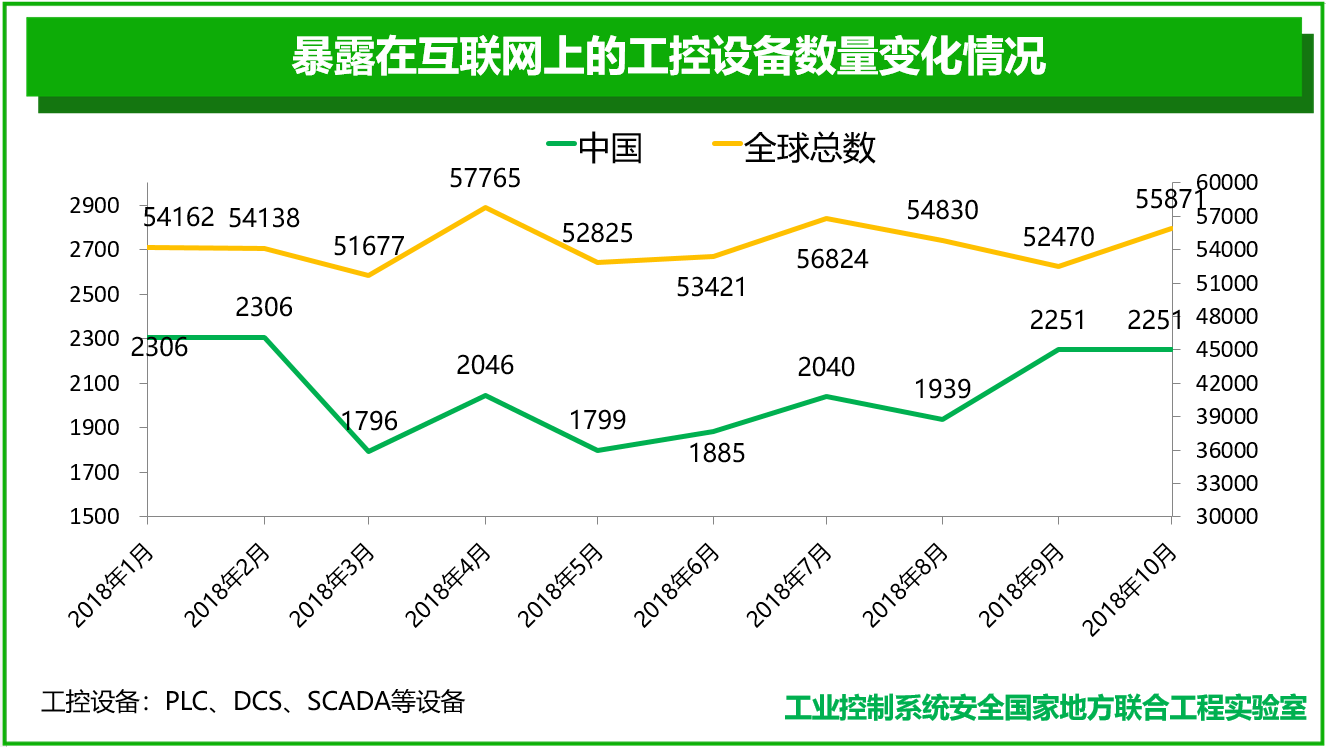
美国安全公司Positive technologies的监测数据较好的反映了全球范围内，工业组件在互联网上的暴露情况。为了收集在互联网上具有可访问性的工业控制系统站点及组件， Positive technologies采用被动方式，使用可公开访问的引擎：Google、Shodan（shodan. io）、 Censys（censys. io）对全球工业系统进行了搜索。其中，Shodan 和Censys可搜索工业服务器、路由器、专用摄像头等设备的联网情况。



根据Positive Technologies2018研究数据显示：当前全球工控系统联网暴露组件总数量约为17.6万个。从这些工业组件的国家和地域分布来看，联网的工控组件主要集中在美洲和欧洲国家，其中美洲占比达到40%以上。这也是为什么工业互联网安全事件多集中在欧洲和美洲等发达国家的主要原因。从具体国家来看，美国的工控系统组件联网暴露情况最为严重，达到64287个；其次是德国， 13242个；法国排名第三，7759个。中国排名全球第五，位列加拿大之后，为6223个。全球各国工控系统联网组件暴露数量及分布情况如下图。

在所有的工控系统组件中，工控设备的暴露是最为危险的。工控设备的暴露意味着攻击者有可能直接对设备本身发动攻击。基于全国全球的主动探测，360工业互联网安全大数据分析平台 ——哈勃平台收录了2018国内以及全球范围内，暴露在互联网上的工业控制系统设备数量。该平台统计的工控设备主要包括PLC、DCS、DTU、SCADA等设备。

统计显示，2018年全年，中国和全球的工控设备暴露数量基本处于稳定状态，2018年末比2018年初有稍微增长，在2018年4月份中国和全球的工控设备有稍微增长趋势。暴露的工控设备数量折线图如下所示。



1. 工业互联网安全漏洞分析

安全漏洞问题是工业互联网面临的又一个顽疾。特别的，与一般的IT系统不同，受到生产环境的约束，很多的工业系统安全漏洞即便已知，也未必能有条件进行修复。

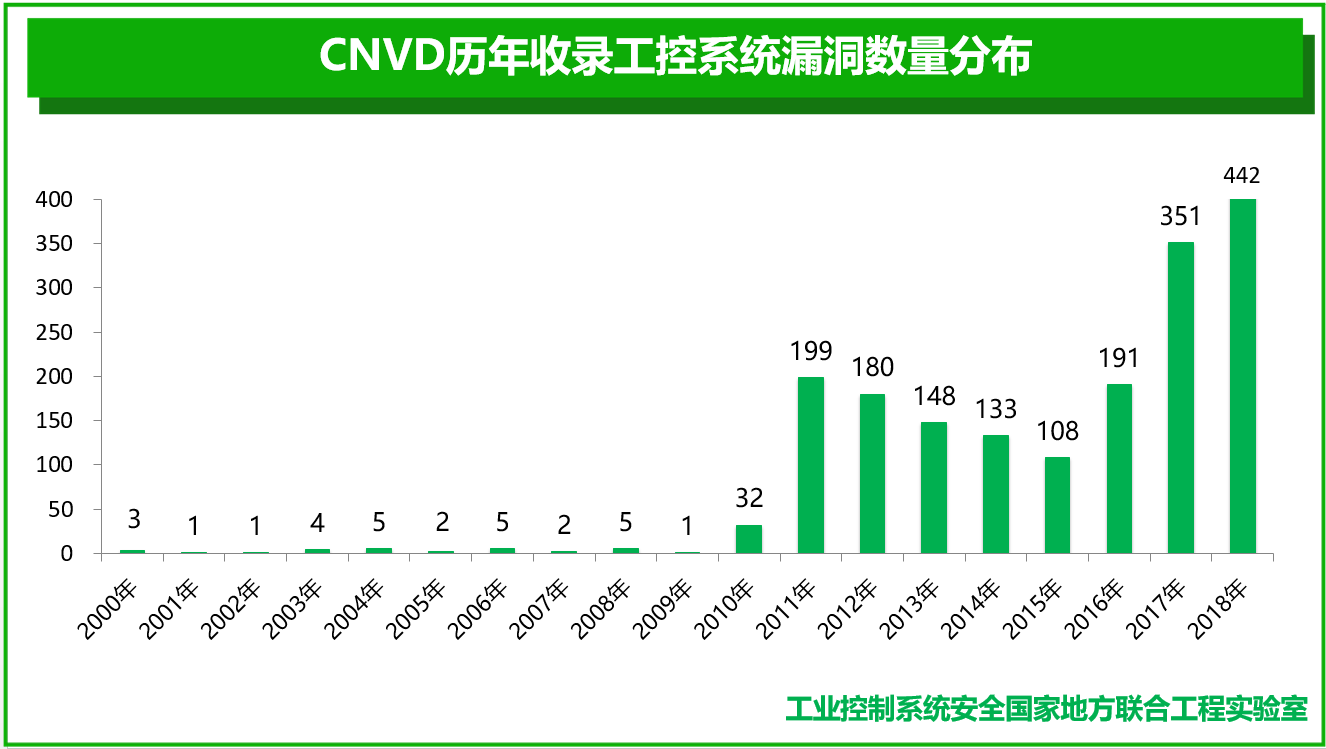
本节主要以联合实验室漏洞库收录的工业控制系统相关的漏洞信息为基础，综合参考了Common Vulnerabilities & Exposures（CVE）、National Vulnerability Database（NVD）、中国国家信息安全漏洞共享平台（CNVD）及国家信息安全漏洞库（CNNVD）所发布的漏洞信息，从工控漏洞的年度变化趋势、等级危害、漏洞类型、漏洞涉及行业、漏洞设备类型等方面分析工业控制系统的安全威胁态势及脆弱性。

本报告中的工控漏洞风险评估方法，基于通用漏洞评分系统，将可见性、可控性、漏洞利用目标服役情况等体现工控安全特性的指标纳入量化评估范围。该方法使用改进的工控漏洞风险评估算法，既可以生成工控漏洞的基础评分、生命周期评分，也可以用于安全人员结合实际工控安全场景的具体需求以生成环境评分。

### 安全漏洞数量快速增长，安全形式日益严峻

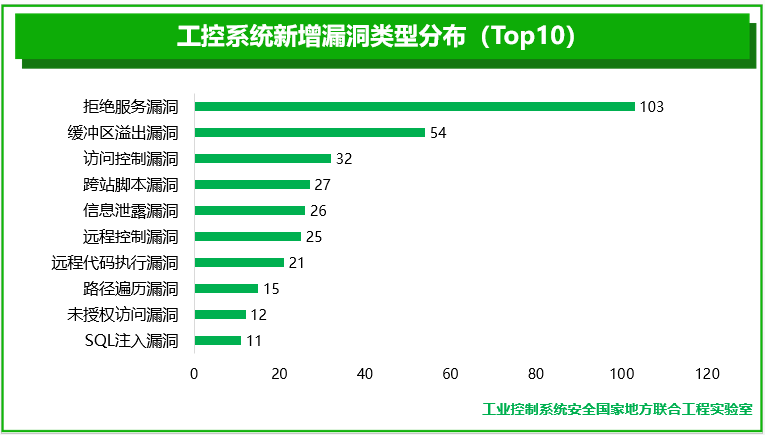
根据中国国家信息安全漏洞共享平台（CNVD）最新统计数据显示，自2000年-2009年， CNVD每年收录的工控系统漏洞数量一直保持在个位数。但到了2010年，该数字一下子攀升到32个，次年又跃升到190个。这和情况的发生与2010年发现的[Stuxnet蠕虫病毒](https://baike.baidu.com/item/Stuxnet%E8%A0%95%E8%99%AB%E7%97%85%E6%AF%92)（震网病毒）有直接关系。[Stuxnet病毒](https://baike.baidu.com/item/Stuxnet%E8%A0%95%E8%99%AB%E7%97%85%E6%AF%92" \t "_blank)是世界上第一个专门针对工业控制系统编写的破坏性病毒，自此业界对工业控制系统的安全性普遍关注，工业控制系统的安全漏洞数量增长迅速。

不过，从2011年-2015年，CNVD收录的工控系统漏洞数量，又呈现了一个持续的稳中有降的态势。直到2015年底至2016年初的乌克兰大停电事件之后，工控系统漏洞的发现再次进入高速增长期：2016年191个；2017年351个；而到了2018年，增长到了442个。



### 安全漏洞类型多样化特性明显

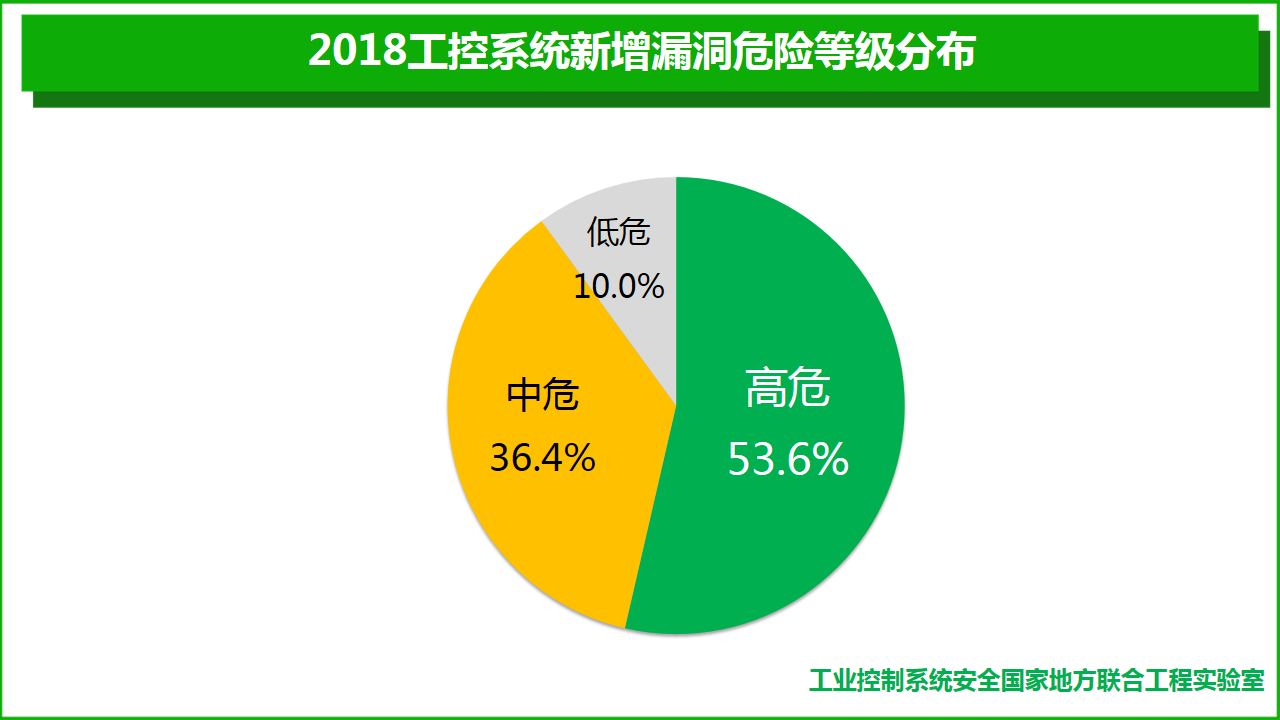
在2018年四大漏洞平台收录的工业控系统漏洞中，漏洞成因多样化特征明显，技术类型多达30种以上。其中，拒绝服务漏洞（103）、缓冲区溢出漏洞（54）和访问控制漏洞(32)数量最多，最为常见。



攻击者可以利用多样化的漏洞获取非法控制权、通过遍历的方式绕过验证机制、发送大量请求造成资源过载等安全事故。实际上，无论攻击者无论利用何种漏洞造成生产厂区的异常运行，均会影响工控系统组件及设备的灵敏性和可靠性，造成严重的安全问题。

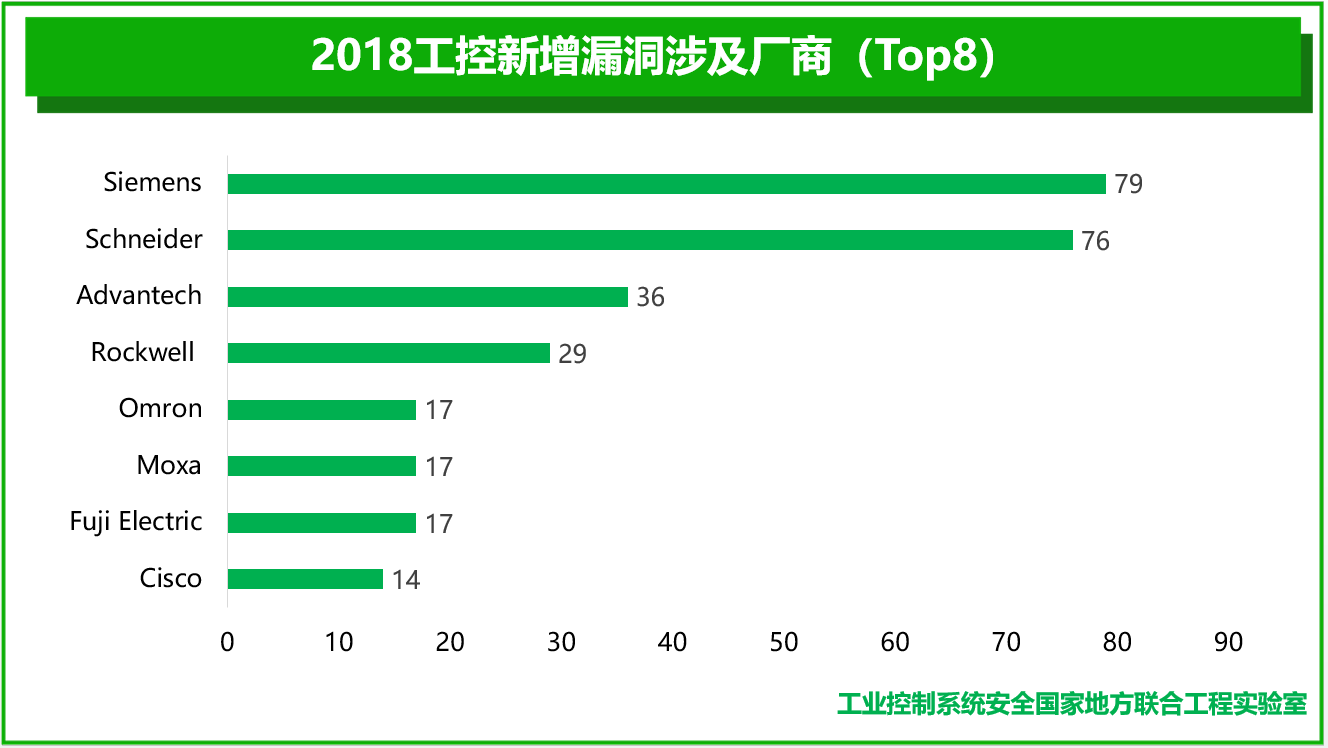
### 高危漏洞占比较高

在2018年四大漏洞平台收录的工业控系统漏洞中，高危漏洞占比53.6%，中危漏洞占比为36.4%，中高危漏洞占比达到90%。漏洞危害等级分布如下：



### 漏洞涉及厂商以国际厂商为主

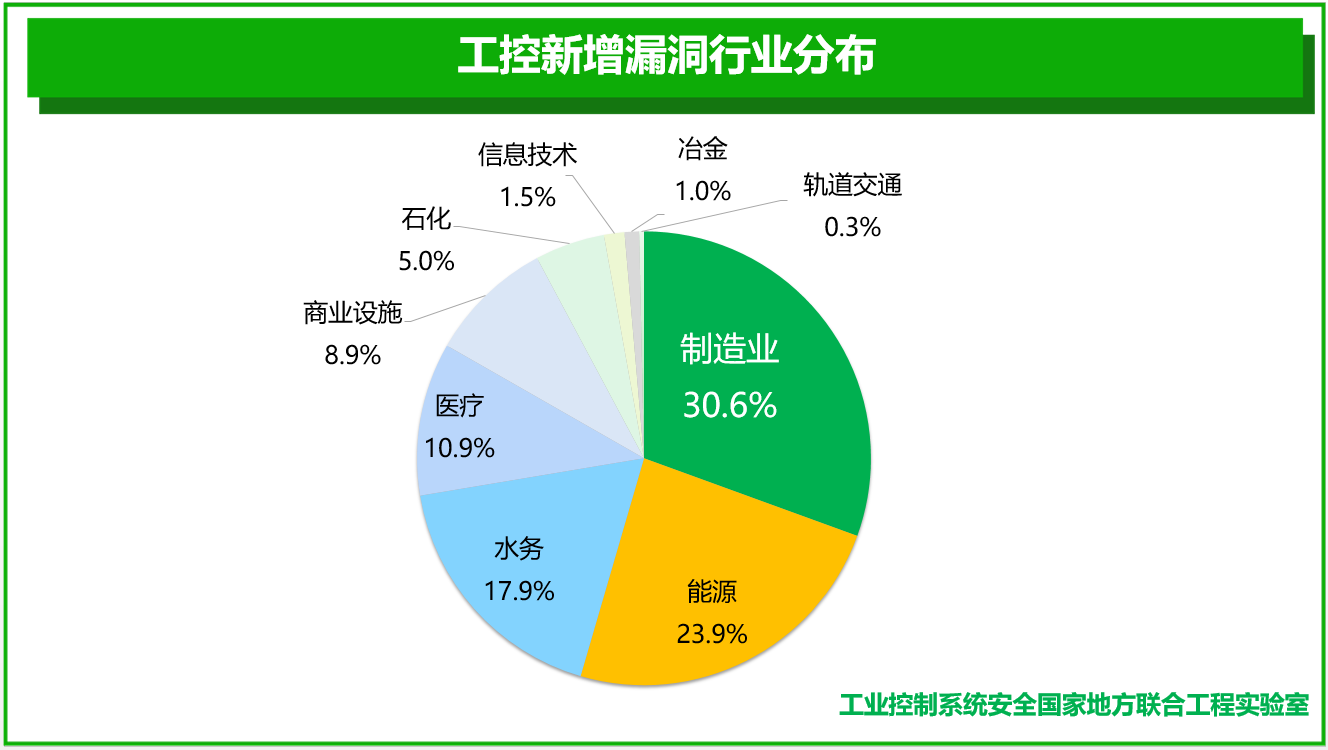
在2018年四大平台新收录的工业控制系统漏洞中，涉及到的前八大工控厂商中有七个为国际厂商，一个为中国台湾厂商。这些厂商分别为西门子（Siemens）、施耐德（Schneider）、研华（Advantech）、罗克韦尔（Rockwell）、欧姆龙（Omron）、摩莎（Moxa）、富士电机（Fuji Electric）和思科（Cisco）。漏洞涉及主要厂商情况如下图所示：



需要说明的事，虽然安全漏洞在一定程度上反映了工控系统的脆弱性，但不能仅通过被报告的厂商安全漏洞数量来片面判断比较厂商产品的安全性。因为一般来说，一个厂商的产品越是使用广泛，越会受到更多安全研究者的关注，因此被发现安全漏洞的可能性也越大。某种程度上来说，安全漏洞报告的厂商分布，更多程度上反映的是研究者的关注度。

### 漏洞涉及行业广泛，以制造业、能源行业为主

在2018年四大平台新收录工业控制系统安全漏洞中，多数分布在制造业、能源、水务、医疗、食品、石化、轨道交通、冶金、市政、信息技术等关键基础设施行业。制造业占比最高，涉及的相关漏洞数量占比达到30.6%，打破了近几年能源行业稳居第一的局面，能源行业涉及的相关洞数量为23.9%。漏洞行业分布图如下：



1. 工业企业网络安全感知

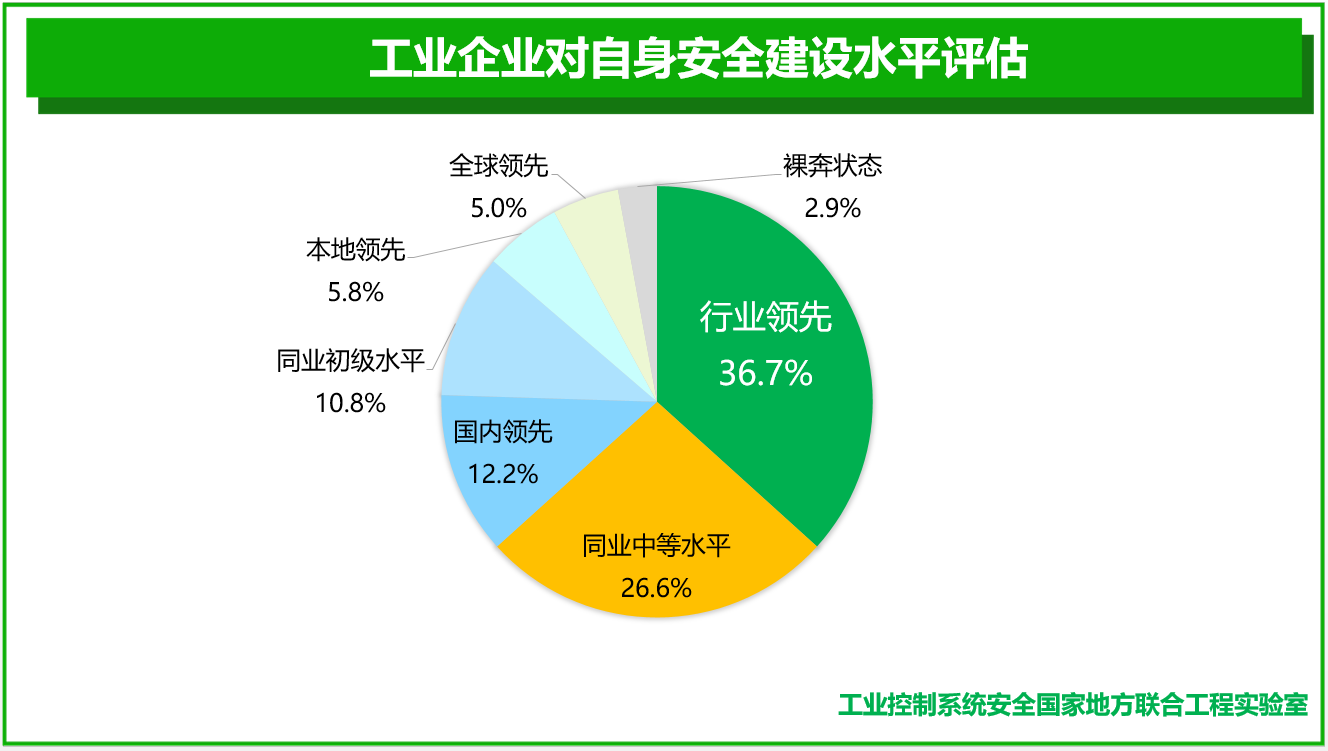
本小节将主要从工业企业对自身网络安全状况的认知和感知情况，来分析工业企业的安全态势。

### 工业企业对自身安全建设水平的认知

2018年，联合实验室在全国范围内对工业企业用户进行了一次系统的深入调研。根据参与行业的单位属性将制造业、市政/交通、通信/网络、石油石化/化工、能源电力用户填写的问卷作为有效数据进行分析。关于本次调研的详细情况，可参见本报告“研究背景”一节的相关介绍。

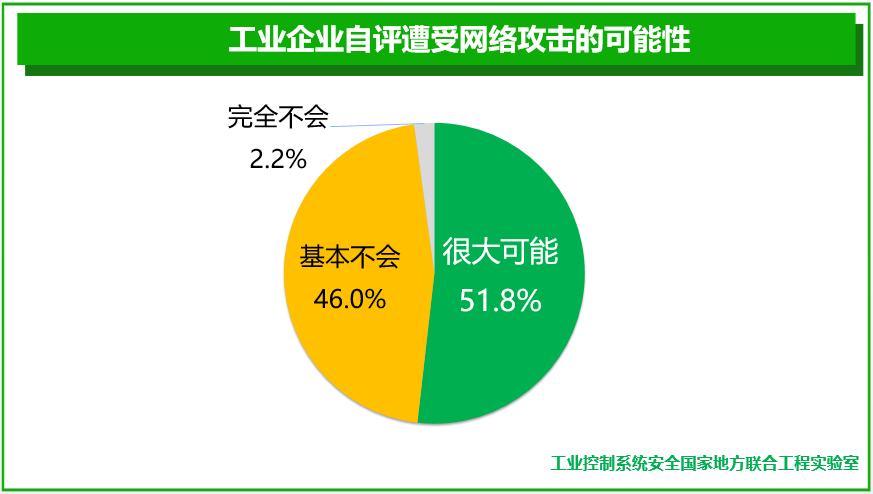
调查显示，工业企业对自身企业安全建设水平普遍有较高的认识，**36.7%的被调查者认为自己所在企业网络安全建设水平达到行业领先**；，仅有2.9%的被调查者认为，自己所在的企业网络安全建设水平处于“裸奔”状态。

需要说明的是，根据联合实验室在全国各地工业企业的实地考察情况来看，工业企业对自身安全建设程度普遍“自我感觉良好”，实际上是一种过度乐观的状态。绝大多数工业企业的实际安全状况都让人十分堪忧。



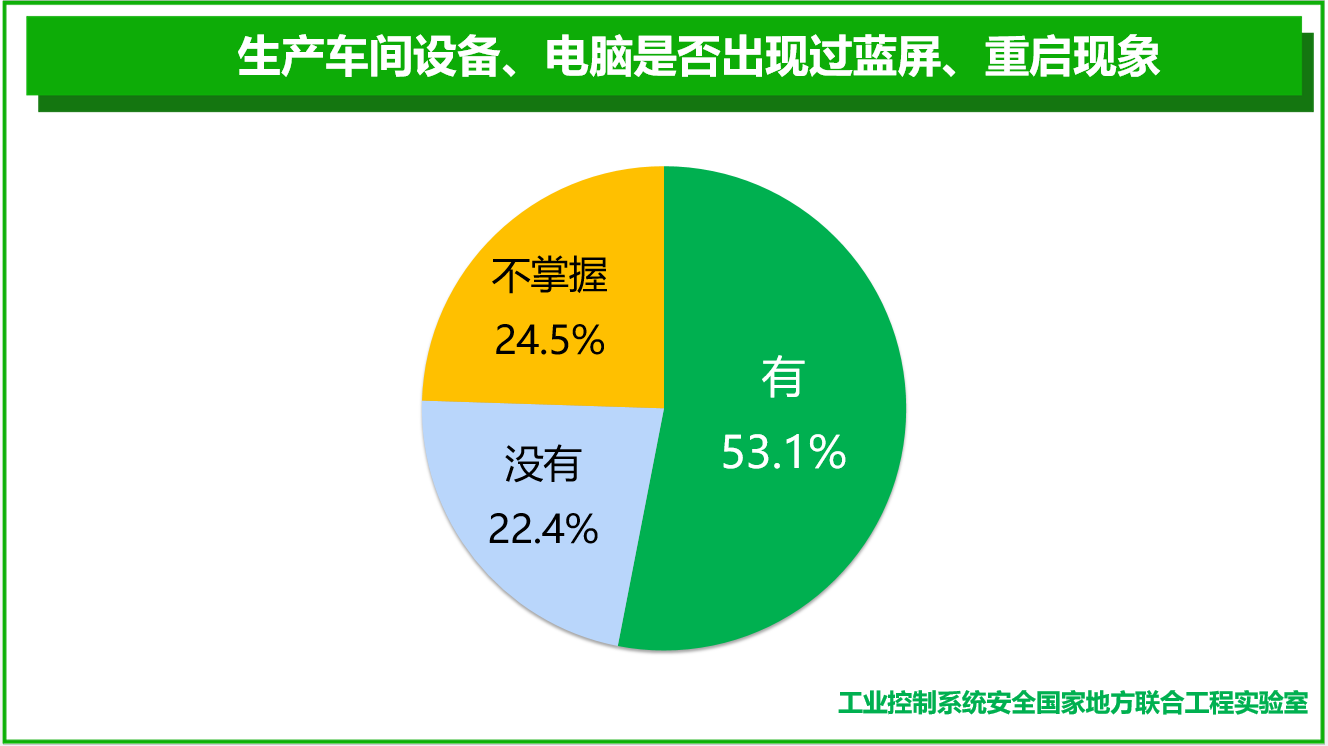
### 工业企业对自身面临安全风险的感知

调查还显示，在被问及自己所在的工业企业是否会遭受网络攻击时，认为会遭到攻击的人和认为不会遭到攻击的人几乎各占一半。

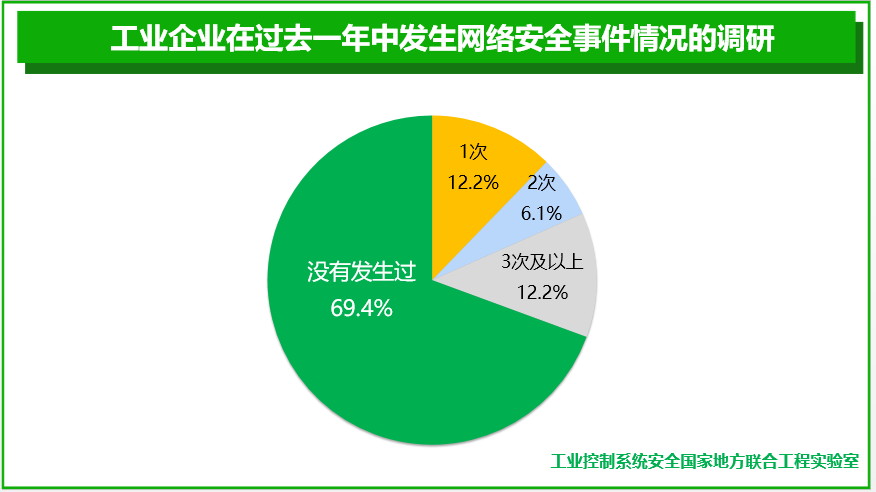


针对生产车间设备、电脑出现蓝屏、重启现象进行调研分析发现，超过50%的企业遭受过生产设备安全故障问题，仅有不足1/4的企业没有出现过这些现象；另有约1/4的企业对此问题表示 “不掌握”相关情况。详见下图。

其实“不掌握”，这一结果可能是最可怕的一种风险。因为“不掌握”也就意味着企业其实并没有部署足够的网络安全监控措施以实时了解其工业系统的网络安全状况。这也说明，很多工业企业对自身网络安全建设水平处于业内领先地位的评估可能是过于乐观。



在被问及过去一年中，是否发生过网络安全事件时，69.4%的被调查企业表示没有发生过；表示发生过1次的有12.2%；2次的6.1%；3次及以上的占比12.2%。



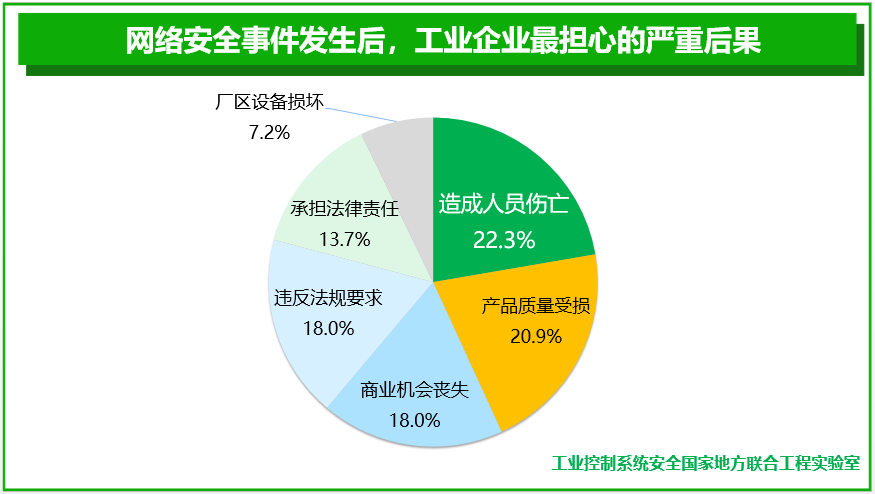
将上述三组数据的结果进行对比分析，我们就会发现：**多数企业确实过低的估计了自身遭到网络攻击风险的可能性**。事实上，当企业内部电脑出现大量蓝屏、重启等现象时，往往意味着企业已经遭到了攻击，只是很多企业的管理者并没有把这些事件作为安全事件来进行响应和调查，而只是当作一般的系统故障而已，从而可能导致其错过发现问题的最佳时机。

一句话，企业认为自己没有遭到过攻击，但实际上有迹象表明他们可能已经遭到了攻击，只是自己不知情或没有意识到这些现象可能与攻击有关。

此外，从应急响应或现场处置过的大量事件看，绝大多数自认为没有安全问题的工业企业，往往都存在着巨大的安全漏洞，他们对于安全事件只是处于“不知情”的状态。

### 工业企业对网络安全事件影响的认知

调查显示，一旦遭遇网络安全事件，22.3%的工业企业最为担心的严重后果是造成人员伤亡；其次为产品质量受损，占比20.9%，接下来是商业机会丧失、违反法规要求、承担法律责任、厂区设备损失等。需要特别说明的是，**人员伤亡和产品质量受损，是工业企业遭遇网络安全事件时所需面对的特殊风险**，一般的政府机构、企业，或IT、互联网公司都无需面对此类风险。



1. 工业互联网安全威胁

联合实验室在对工业企业进行广泛、深入的研究的过程中，总结出了当前国内工业企业在工业互联网领域面临的8个主要安全威胁。

1. OT安全管理不到位

在很多大中型工业企业中，IT安全管理一般措施比较到位，但OT安全管理措施却有显著疏失。尽管企业大小不同，但一般其IT安全由企业的信息中心或专门团队管理。其中，制造业、石油石化、天然气，公用事业等行业的IT安全管理比其他行业更成熟。但一般来说，这些工业企业的安全管理和策略没有为OT做针对性定制，OT网络和资产及其网络安全影响多年未被覆盖和管理。

1. IT和OT安全责任模糊

很多工业企业的信息中心会去管理OT网络和服务器的连接性和安全性，但往往对于OT网络上的生产设备与控制系统的连接性没有管辖权限；而这些设备、控制系统也是互联的，有些就是基于IT技术实现的。如：操作员站、工程师站等。因此，常见的IT威胁对OT系统也有影响。反过来说，OT的运维团队一般会对生产有效性负责，但往往并不对网络安全负责。对于很多工业企业来说，生产有效性通常都比网络安全性更重要。

1. IT安全控制在OT领域无效

很多工业企业在OT设置中使用IT安全控制，但没有考虑其对OT的影响。 例如，国内某汽车企业，IT安全团队按照IT安全要求主动扫描OT网络，结果导致汽车生产线PLC出现故障，引起停产。

从实践来看，很多工业企业要么不做OT安全评估，要么OT安全评估由IT安全服务商执行。而IT安全评估通常不包括OT网络的过程层和控制层，即使对这两层进行评估，也只能采用问卷方式而不能使用工具。执行这些评估的人员通常是IT安全专家，对OT领域也不甚了解。

1. 缺乏OT资产和漏洞的可见性

工业企业的IT团队一般不负责OT的资产，而是由OT团队负责OT资产。但因为生产线系统是历经多年由多个自动化集成商持续建设的，因此OT团队对OT资产的可见性一般十分有限，甚至没有完整的OT资产清单，关于OT资产的漏洞基本上无人负责和收集。

1. 工业主机几乎“裸奔”

工业企业的OT网络中存在着大量工业主机，如：操作员站、工程师站、历史数据服务器、备份服务器等。这些PC或服务器上运行的实时数据库、监视系统、操作编程系统等，向上对IT网络提供数据，向下对OT中的控制设备及执行器进行监视和控制，它们是连接信息世界和物理世界的“关键之门”。

但在实际系统中，这些工业主机上面要么没有任何安全防护措施，要么防护措施因没有进行更新已经失效，工业主机几乎处在“裸奔”状态。近年来不断发生的各类工业安全事件中，首先遭到攻击或受影响往往都是工业主机。

1. IT和OT网络混杂缺防护

很多工业企业的IT和OT网络并没有进行有效的隔离；部分工业企业虽然进行了分隔，并设置了访问策略，但总有员工为方便，私自设置各类双网卡机器，使得IT、OT网络中存在有许多不安全、也不被掌握的通信通道。

OT系统往往由不同集成商在不同时间建设，使用不同的安全标准。因此，当需要集成商进行维修维护时，工作人员经常会开放远程维护端口，而且这些端口往往不采用任何安全防护措施，甚至还常见端口打开后忘记关闭的情况发生，从而增加工业互联网的攻击剖面。

国内某冷轧厂就曾因为工程师远程运维，结果导致勒索病毒传入生产网络影响生产。

1. OT缺乏安全响应预案和恢复机制

IT工作计划和OT工作计划往往是两张皮，IT安全事件响应计划与OT之间的协调往往十分有限。很多OT网络在制定生产事故应对计划时，都没有考虑过网络安全事件的处理。同时，由于缺乏备份和恢复机制，OT中发生的网络安全事件，恢复速度往往很慢。

1. IT和OT人员安全培训普遍缺失

很多工业企业虽然有IT组织负责IT网络安全，但其在安全意识和培训计划中，往往会忽视IT和OT之间的文化差异；IT安全人员很少会对OT人员进行安全培训，OT人员的信息安全培训普遍缺失。

1. 2018工业互联网安全工作进展
2. 国外工业互联网安全重要文件

2018年，美国先后制定并出台了一系列与工业互联网安全相关的法案、战略和规划，值得我们借鉴和参考。

1. 4月的4项法案

2018年4月，美国众议院能源和商业小组委员会通过4项能源安全法案，旨在提升美国能源部的网络响应能力和参与度，并制定新计划解决电网和管道的安全问题。其四项法案分别为：

《管道与液化天然气设施网络安全准备法案》：该法案要求美国能源部长里克·佩里制定计划提高美国能源管道和液化天然气设施的物理安全与网络安全。

《能源应急领导法案》：该法案提出将美国能源部的应急响应和网络安全工作领导权力提至助理部长一级。

《2018网络感知法案》：该法案制定计划帮助私营公共事业公司识别并使用网络安全功能强大的产品。

《公私合作加强电网安全法案》：该法案提出加强公私合作确保电力设施安全。

1. 网络安全战略

2018年5月，美国国土安全部发布首个《网络安全战略》（以下简称《战略》）。《战略》将“网络空间”定义为信息基础设施相互依赖的网络，包括互联网、电信网络、计算机、信息与通信系统，以及嵌入式处理器和控制器。

《战略》重点阐述了美国土安全部面临的网络威胁环境、未来五年愿景、发展目标、实现途径等，指导美国国家层面的网络安全风险管理。《战略》基于美国土安全部“网络空间可以安全且富有弹性”的理念，采取整体风险管理的思路和方法，以实现更好的国家网络安全风险管理。其理念、思路和方法对于我国网络安全管理工作具有重要借鉴参考作用。

1. 能源行业网络安全多年计划

2018年5月，美国能源部发布美国《能源行业网络安全多年计划》（以下简称《计划》）。

《计划》概述了网络风险管理实践的颠覆性变革；强调了网络威胁的频率、规模和复杂程度不断上升，发动网络攻击也变得更加容易，强调了网络威胁的频率、规模和复杂程度不断上升，发动网络攻击也变得更加容易。《计划》指出了美国能源部应履行网络安全责任的举措，以解决能源所有者和运营商不断变化的安全需求等问题，力图在应对网络威胁方面占据先决优势。

《计划》侧重于关注美国能源部各部门协调确定的高优先级举措，并支持美国联邦政府和能源行业的战略和计划，以此降低美国能源行业的网络安全风险。

1. 网络安全与基础设施安全局法案

2018年10月，美国网络安全与基础设施安全局法案获得参议院通过。该法案将国家保护与计划局（简称NPPD）重组为网络安全与基础设施安全局（简称CISA），并由CISA负责网络与物理基础设施安全。

据NPPD保护司副司长克里斯托弗·克雷布斯（Christopher Krebs）称：“经国会通过的CISA法案代表国家为提升网络安全所作的诸多工作取得了真正的进展。强化美国国土安全局的网络安全任务、精兵简政以及使NPPD名副其实，反映了目前所作的工作能够切实地帮助国家更好地保护关键基础设施与网络平台。这些变化还能提升国土局的工作能力，有助于其更好地与行业及政府利益相关人合作、招募网络安全顶尖人才。”

CISA的通过建立了一个致力于捍卫基础设施安全的网络安全机构，也表明了美国安全局对网络安全问题的高度重视。

1. 国内工业互联网安全重要文件
2. 2018年，国内也先后发布了一系列与工业互联网相关的政策和法规。中华人民共和国核安全法

2018年5月，为贯彻落实党中央、国务院关于安全高效发展核电工作的重要决策部署，宣贯实施《中华人民共和国核安全法》。该法案按照《中共中央国务院关于推进安全生产领域改革发展的意见》等有关要求，在总结核电行业安全管理经验和“核电安全管理提升年”专项行动工作基础上，聚焦核电运行关键环节，进一步加强安全管理，保障核电机组安全稳定运行，促进核电安全高效发展。

1. 关于进一步加强核电运行安全管理的指导意见

2018年5月，中国核工业集团有限公司、中国广核集团有限公司、国家电力投资集团有限公司、华能集团有限公司共同发布《关于进一步加强核电运行安全管理的指导意见（发改能源[2018]765号）》。

该指导意见第八条明确规定：加强核电厂网络安全管理。将网络安全纳入核电安全管理体系，加强能力建设，保障核电厂网络安全。其主要包括：开展网络安全能力建设；做好网络等级保护测评；开展网络安全培训及评估工作。

1. 工业互联网APP培育工程实施方案

2018年5月，为落实《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》，推动工业互联网应用生态加快发展，工信部印发《工业互联网APP培育工程实施方案（2018-2020年）》的通知。

该方案以习近平新时代中国特色社会主义思想为指导，深入贯彻落实党的十九大和十九届二中、三中全会精神，牢固树立新发展理念，围绕制造业提质增效和转型升级实际需求，以企业为主体，以发展和繁荣工业互联网平台应用生态为目标，推动软件技术与工业技术深度融合，工业APP培育与工业互联网平台建设协同推进，着力突破共性关键技术，夯实工业APP发展基础，着力提高工业APP发展质量，提升价值和应用效果，着力构建开放共享和流通交易机制，推动工业APP向工业互联网平台汇聚，形成建平台和用平台双向迭代、互促共进的制造业新生态。

工业互联网APP是基于工业互联网，承载工业知识和经验，满足特定需求的工业应用软件，是工业技术软件化的重要成果。实施工业APP培育工程离不开工业APP安全的部署和落实。

1. 网络安全等级保护条例（征求意见稿）

2018年6月，公安部关于《网络安全等级保护条例（征求意见稿）》，公开征求意见。

征求意见稿显示：为加强网络安全等级保护工作，提高网络安全防范能力和水平，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，依据《中华人民共和国网络安全法》、《中华人民共和国保守国家秘密法》等法律，制定本条例。

网络安全等级保护工作应当按照突出重点、主动防御、综合防控的原则，建立健全网络安全防护体系，重点保护涉及国家安全、国计民生、社会公共利益的网络的基础设施安全、运行安全和数据安全。

1. 工信部关于工业互联网发展的计划

根据《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》（以下简称《指导意见》），2018-2020年是我国工业互联网建设起步阶段，对未来发展影响深远。

为贯彻落实《指导意见》要求，深入实施工业互联网创新发展战略，推动实体经济与数字经济深度融合，2018年6月，工信部发布《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》。两项加护提出，到2020年底，我国将实现“初步建成工业互联网基础设施和产业体系”的发展目标，具体包括建成5个左右标识解析国家顶级节点、遴选10个左右跨行业跨领域平台、推动30万家以上工业企业上云、培育超过30万个工业APP等内容。

行动计划中第七条明确规定：安全保障水平增强行动。行为内容只要包括：健全安全管理制度机制；初步建立工业互联网全产业链数据安全管理体系；指导督促企业强化自身网络安全技术防护。

1. 工信部制定“推广指南”与“评价方法”

2018年7月，为贯彻落实《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》，加快发展工业互联网平台，工业和信息化部印发《工业互联网平台建设及推广指南》（以下简称《指南》）。同时，为规范和促进我国工业互联网平台发展，支撑开展工业互联网平台评价与遴选，工业和信息化部印发《工业互联网平台评价方法》（以下简称《评价方法》）。

《指南》中第十八条明确规定：完善平台安全保障体系。制定完善工业信息安全管理等政策法规，明确安全防护要求。建设国家工业信息安全综合保障平台，实时分析平台安全态势。强化企业平台安全主体责任，引导平台强化安全防护意识，提升漏洞发现、安全防护和应急处置能力。

《评价方法》平台应用服务能力中明确指出：部署安全防护功能模块或组件，建立安全防护机制，确保平台数据、应用安全。平台安全可靠能力中强调工控系统安全可靠、关键零部件安全可靠、软件应用安全可靠。

1. 推动企业上云实施指南（2018-2020年）

2018年7月，为贯彻落实《国务院关于促进云计算创新发展培育信息产业新业态的意见》、《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》、《云计算发展三年行动计划（2017-2019年）》等部署要求，推动企业利用云计算加快数字化、网络化、智能化转型，推进互联网、大数据、人工智能与实体经济深度融合，工业和信息化部印发《推动企业上云实施指南（2018-2020年）》的通知。

云计算是信息技术发展和服务模式创新的集中体现，是信息化发展的重大变革和必然趋势。支持企业上云，有利于推动企业加快数字化、网络化、智能化转型，提高创新能力、业务实力和发展水平；有利于加快软件和信息技术服务业发展，深化供给侧结构性改革，促进互联网、大数据、人工智能与实体经济深度融合，加快现代化经济体系建设。

该实施指南第二十七条明确规定：落实《中华人民共和国网络安全法》相关要求，推动建立健全云计算相关安全管理制度，完善云计算网络安全防护标准。指导督促云平台服务商切实落实主体责任，保障用户信息安全和商业秘密。

1. 国家智能制造标准体系建设指南（2018年版）

2018年8月，为加快推进智能制造发展，指导智能制造标准化工作的开展，工业和信息化部、国家标准化管理委员会共同组织制定了《国家智能制造标准体系建设指南（2018年版）》。

该建设指南按照《国家智能制造标准体系建设指南（2015年版）》中提出的“统筹规划，分类施策，跨界融合，急用先行，立足国情，开放合作”原则，进一步完善智能制造标准体系，全面开展基础共性标准、关键技术标准、行业应用标准研究，加快标准制（修）订，在制造业各个领域全面推广。

该建设指南中建设内容明确了安全标准，主要包括**功能安全**、**信息安全**和**人因安全**三个部分。其中信息安全标准用于保证智能制造领域相关信息系统及其数据不被破坏、更改、泄露，从而确保系统能连续可靠地运行，包括软件安全、设备信息安全、网络信息安全、数据安全、信息安全防护及评估等标准。

1. 关于加强电力行业网络安全工作的指导意见

2018年9月，为深入贯彻习近平总书记关于网络强国战略的重要论述，全面落实党中央、国务院关于网络安全工作的决策部署，国家能源局印发《关于加强电力行业网络安全工作的指导意见》（以下简称《意见》），从电力行业全局的角度指导、推进网络安全工作。

《意见》围绕进一步落实电力企业网络安全主体责任，完善网络安全监督管理体制机制，加强全方位网络安全管理，强化关键信息基础设施安全保护，加强行业网络安全基础设施建设，加强电力企业数据安全保护，提高网络安全态势感知、预警及应急处置能力，支持网络安全自主创新与安全可控；积极推动电力行业网络安全产业健康发展，推进网络安全军民融合深度发展，加强网络安全人才队伍建设，拓展网络安全国际合作等12方面提出30条具体要求。

1. 公安机关互联网安全监督检查规定

2018年10月，公安部发布《公安机关互联网安全监督检查规定》。该规定自11月1日起施行。根据规定，公安机关根据网络安全防范需要和网络安全风险隐患的具体情况，可以进入互联网服务提供者和联网使用单位的营业场所、机房、工作场所监督检查，对其是否存在网络安全漏洞进行远程监控。规定明确，公安机关在互联网安全监督检查中，发现互联网服务提供者和联网使用单位有违法行为的，公安机关可以依法予以行政处罚：构成违反治安管理行为的，依法予以治安管理处罚；构成犯罪的，依法追究刑事责任。

我国2018年发布的工业互联网安全政策如表1所示：

|  |  |  |
| --- | --- | --- |
| **时间** | **组织** | **文件** |
| 2018.5 | 中国核工业集团有限公司等四家大型能源企业 | 《关于进一步加强核电运行安全管理的指导意见（发改能源[2018]765号）》 |
| 2018.5 | 工业和信息化部 | 《工业互联网APP培育工程实施方案（2018-2020年）》 |
| 2018.6 | 公安部 | 《网络安全等级保护条例（征求意见稿）》 |
| 2018.6 | 工业和信息化部 | 《工业互联网发展行动计划(2018-2020年)》  《工业互联网专项工作组2018年工作计划》 |
| 2018.7 | 工业和信息化部 | 《工业互联网平台建设及推广指南》  《工业互联网平台评价方法》 |
| 2018.7 | 工业和信息化部 | 《推动企业上云实施指南（2018-2020年）》 |
| 2018.8 | 工业和信息化部 | 《国家智能制造标准体系建设指南（2018年版）》 |
| 2018.9 | 国家能源局 | 《关于加强电力行业网络安全工作的指导意见》 |
| 2018.10 | 公安部 | 《公安机关互联网安全监督检查规定》 |

表1 2018年工业互联网安全政策一览表

1. 工业信息安全标准体系建设

建立健全工业控制系统[信息安全](https://www.baidu.com/s?wd=%E4%BF%A1%E6%81%AF%E5%AE%89%E5%85%A8&tn=SE_PcZhidaonwhc_ngpagmjz&rsv_dl=gh_pc_zhidao)标准体系对工业信息安全建设具有重要的指导意义。通过工业信息安全标准体系的建设，可有效提高对工业信息安全风险的管控能力，通过与等级保护等工作接续起来，使得工业信息安全管理更加科学有效。同时，信息安全标准体系的建立将使得企业安全实施水平与国际先进水平接轨，从而加快工业控制系统信息安全的落实。

为了充分发挥生产、管理、科研、应用等各方面在各个行业、产业、企业、组织、机构的标准化工作中的作用，广泛开展信息安全领域的标准化工作，2002年，中国通信标准化协会（CCSA）成立。2016年，经国家标准化管理委员会批准成立全国信息安全标准化技术委员会（以下简称“信安标委”，TC260）。

信安标委是在信息安全专业领域内，从事全国标准化工作的技术工作组织，负责全国信息安全标准化的技术归口工作。另有全国电力系统管理及其信息交换标准化技术委员会（TC82）、全国电力监管标准化技术委员会（TC296）、全国工业过程测量和控制标准化技术委员会（TC124）共同推动工业控制系统信息安全标准工作。

2018年2月，**行业标准2018-1396T-YD《工业互联网平台安全防护要求》正式发布**。标准针对工业互联网平台对于安全防护方面的需求，规定了工业互联网平台安全防护的总体要求，主要包括边缘层安全、平台IaaS层安全、平台PaaS层安全、平台SaaS层安全等。

2018年3月，为规范电力信息系统安全的检查流程、内容和方法，防范网络与信息安全攻击对电力信息系统造成的侵害，保障电力信息系统的安全稳定运行，保护国家关键信息基础设施的安全，依据国家有关信息安全和电力行业信息系统安全的规定和要求，**国家标准GB/T 36047-2018《电力信息系统安全检查规范》正式发布，该标准2018年10月1号起开始实施**。本标准规定了电力信息安全检查工作的流程、方法和内容等。本标准适用于行业网络与信息安全主管部门开展电力信息系统安全的检查工作和电力企业在本集团（系统）范围内开展相关信息系统安全的自查工作。

2018年6月，**国家标准GB/T 36323-2018《信息安全技术 工业控制系统安全管理基本要求》正式发布，该标准2019年01月01日开始实施。**本标准规定了工业控制系统安全管理基本框架及该框架包含的各关键活动，并提出为实现该安全管理基本框架所需的工业控制系统安全管理基本控制措施，在此基础上，给出了各级工业控制系统安全管理基本控制措施对应表，用于对各级工业控制系统安全管理提出安全管理基本控制要求。

2018年6月，**国家标准GB/T 36324-2018《信息安全技术 工业控制系统信息安全分级规范》正式发布，该标准2019年01月01日开始实施。**本标准规定了基于风险评估的工业控制系统信息安全等级划分规则和定级方法，提出了等级划分模型和定级要素，包括工业控制系统资产重要程度、存在的潜在风险影响程度和需抵御的信息安全威胁程度，并提出了工业控制系统信息安全四个等级的特征。

2018年6月，**国家标准GB/T 36466-2018《信息安全技术 工业控制系统风险评估实施指南》正式发布，该标准2019年01月01日开始实施。**本标准在对工业控制系统的资产进行整理分析的基础上，从其资产的安全特性出发，分析工业控制系统的威胁来源与自身脆弱性，归纳出工业控制系统面临的信息安全风险，并给出实施工业控制系统风险评估的指导性建议。本标准主要为第三方安全检测评估机构在工业控制系统现场实施风险评估提供指南，也可供工业控制系统业主单位进行自评估时参考。

2018年6月，**国家标准GB/T 36470-2018《信息安全技术 工业控制系统现场测控设备通用安全功能要求》正式发布，该标准2019年01月01日开始实施。**本标准规定了工业控制系统现场测控设备的用户标识与鉴别、使用控制、数据完整性、数据保密性、数据流限制、资源可用性6类通用的安全功能要求。为提高现场设备的信息安全能力，本标准提出针对现场测控设备的通用安全功能要求，用于设备的安全设计、开发、测试与评估。使用者应根据实际或计划使用环境的安全风险分析结果，选择设备应满足的安全功能要求。

2018年11月，**国家标准《信息安全技术 关键信息基础设施安全检查评估指南（报批稿）》试点工作正式启动**。本次试点工作旨在验证《检查评估指南》标准内容的合理性和可操作性，为关键信息基础设施安全检查评估工作摸索经验。《检查评估指南》结合了国际先进理念和国内高水平专业队伍多年的检查评估经验，此次试点又集中了一线运营单位、国家级测评队伍、熟悉检查沿革、行业需求和地方实际的专家等多方面力量，参与试点的单位、专家和队伍不仅全面评估了此项标准，也对安全技术产业发展、对增强安全防护体系提出宝贵建议。

我国2018年发布的工业互联网安全标准如表2所示：

|  |  |  |
| --- | --- | --- |
| **时间** | **组织** | **文件** |
| 2018.2 | 工业互联网平台安全防护要求 | 正式发布 |
| 2018.3 | 电力信息系统安全检查规范 | 正式发布 |
| 2018.6 | 信息安全技术 工业控制系统安全管理基本要求 | 正式发布 |
| 2018.6 | 信息安全技术 工业控制系统信息安全分级规范 | 正式发布 |
| 2018.6 | 信息安全技术 工业控制系统风险评估实施指南 | 正式发布 |
| 2018.6 | 信息安全技术 工业控制系统现场测控设备通用安全功能要求 | 正式发布 |
| 2018.11 | 信息安全技术 关键信息基础设施安全检查评估指南 | 报批稿 |

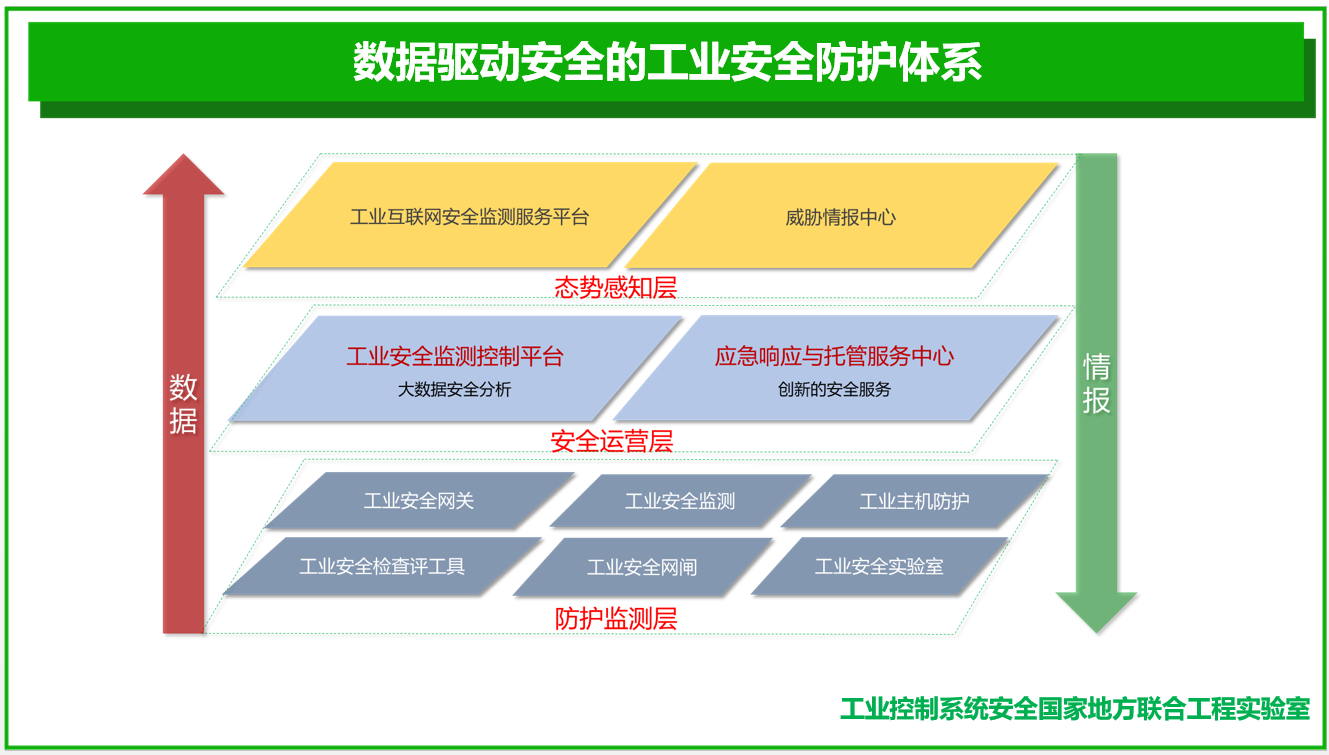
表2 2018年工业互联网安全标准一览表

1. 工业互联网安全产业态势
2. 工业互联网安全产业结构

### 高中低位能力安全产品体系

随着大数据、人工智能等新技术的广泛应用，积极防御、威胁情报、态势感知、安全可视化等创新理念和新产品的出现推动了传统信息安全产业的变革。在工业互联网信息安全领域，传统的安全防御产品已逐渐乏力、无法有效应对越来越严重的安全威胁，构建层次清晰、定位明确、融合联动的工业互联网信息安全产品体系将成为产业未来发展的重要趋势。

根据功能层级和数据、威胁情报流向，应当建立低位、中位、高位能力“三位一体”的安全防护体系。具体来说：工业互联网信息安全市场产品结构可从低到高分为三层：防护监测层、安全运营层、态势感知层。这三层产品分别实现不同的安全功能，三层产品进行数据、指令、威胁情报的流动，实现协同联动的整体防护效果。其中数据从低到高流动，威胁情报从高到低赋能。工业互联网信息安全市场产品结构如下图所示。



### 防护监测层产品

防护监测层产品处于产品体系功能层级的最低层，主要包括工业安全网关（工控防火墙）、工业安全审计、工业主机防护软件、工业安全网闸、工业安全检查评估工具、工业漏洞扫描、工业无线入侵防御、工业云安全防护等产品。此类产品进行数据采集，在发现威胁或接到上层安全运营类产品命令时实施处置，具备简单的分析功能。

### 安全运营层产品

安全运营层产品处于产品体系功能层级的中层，主要部署在工业企业内部，作为工业信息安全的威胁感知、集中管控和应急响应平台在企业内部发挥核心作用。此类产品主要包括工业安全监测系统、工业安全监测控制平台等产品，其技术核心是威胁情报利用、安全可视化、大数据处理技术。

### 安全态势感知层产品

安全态势感知层产品处于产品体系功能层级的最高层，其核心能力是情报搜集、威胁请报库和数据高级分析。此类产品包括工业互联网安全监测服务平台、威胁情报库等，主要部署在政府主管部门或大型企业集团总部，负责对辖区和主管范围内的主要工业企业进行态势感知和安全监管。

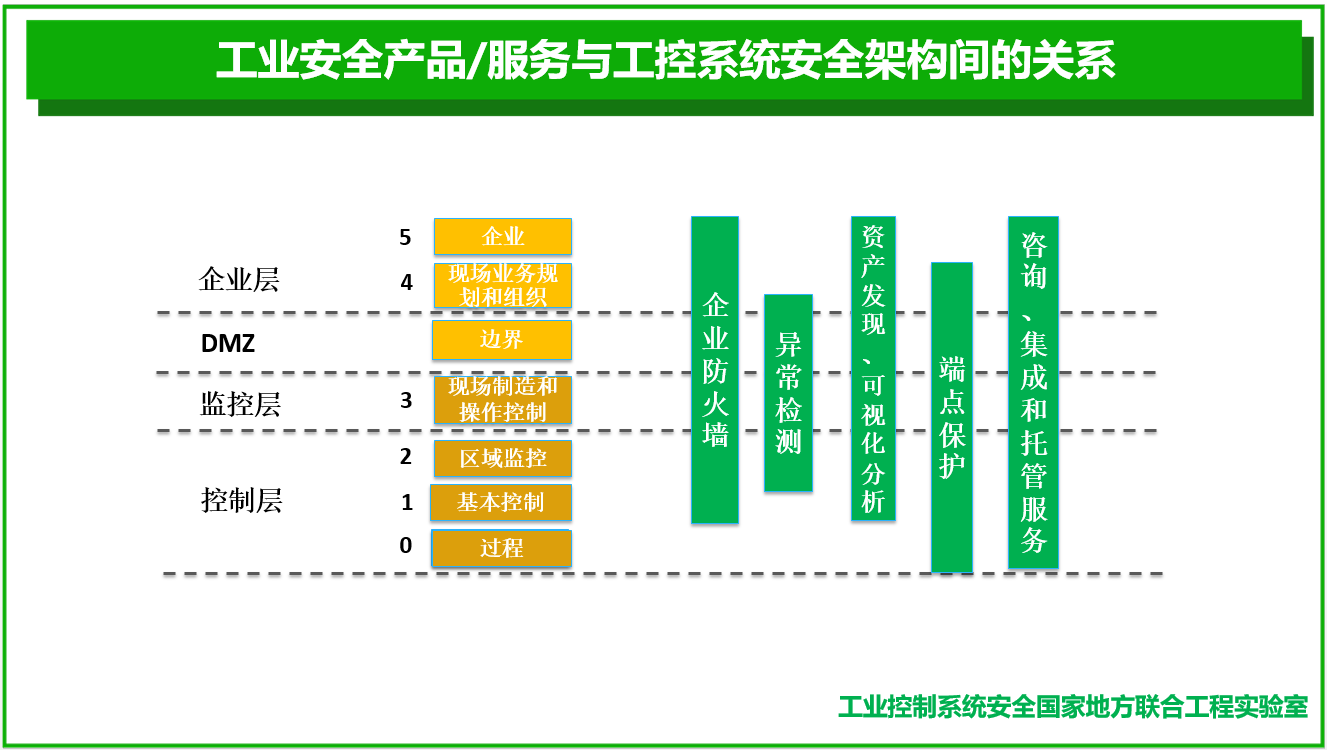
1. Gartner关于OT市场的分析

工业互联网包含了工业控制系统、工业网络，同时也包含了大数据存储分析、云计算、商业系统、客户网络等商业网络基础设施。本节讨论的工业互联网安全市场更强调以资产为中心的操作技术（Operational Technology，OT）安全。

Gartner在2018年7月发布的《OT 安全市场指南》中，明确了操作技术（OT）安全的定义，指出OT安全性指用于保护参与监测和（或）控制物理设备、过程和事件的人员、资产和信息的实践和技术。

与以往不同的是，在该市场指南中，Gartner 扩展了OT安全性的范畴，将OT安全服务也纳入其中。同时，Gartner认为工业互联网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）。

传统的IT系统网络安全按重要性排列顺序为：保密性、完整性、可用性。OT安全按重要性排列顺序为：可用性、完整性、保密性。信息安全目标重要性排序不同造成了OT与IT系统在风险评估、安全需求、标准要求、实现方案、部署实现、安全运维整个安全生命周期过程都有很大不同。因此，传统的IT信息系统的网络安全技术并不能直接应用于工业控制系统，要解决工业控制系统网络安全问题应当充分考虑工业应用场景的特点。Gartner强调，尽管物联网设备和软件，如传感器、移动设备等应用于OT环境中，通常被称为工业物联网（IIOT），但是相对而言，OT安全市场更加成熟。工业物联网是OT的一部分。OT安全市场中的大多数解决方案都集中在下图中。



Gartner根据用于工控系统的普渡参考模型总结工业安全产品/服务与工控系统安全架构间的关系，在L1-L5每层部署企业防火墙设备，同时全面掌握每一层内的工控资产，进行可视化分析；L1-L4每层之间进行异常检测，对于L0-L4进行端点防护，对整个普渡参考模型进行咨询、集成和托管服务。

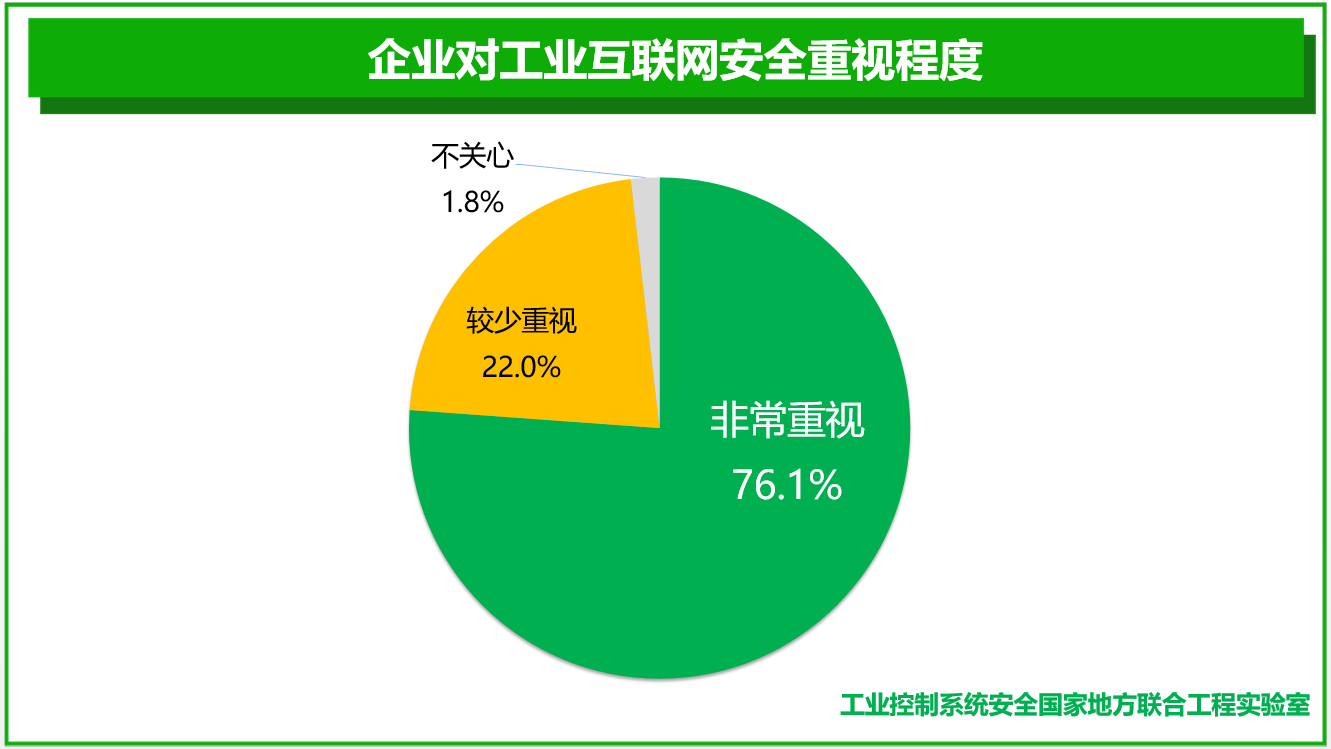
同时，Gartner市场趋势预测：到2019年，65%的企业OT安全将有CIO（首席信息官）负责。到2020年，新部署的工业物联网IIOT（Industrial Internet of Things）或OT系统将支持时间敏感网络TSN；到2020年，25%的数字孪生将以服务的形式提供；到2020年，50%的OT服务供应商将于IT供应商建立合作伙伴关系。

1. 工业企业网络安全投入分析

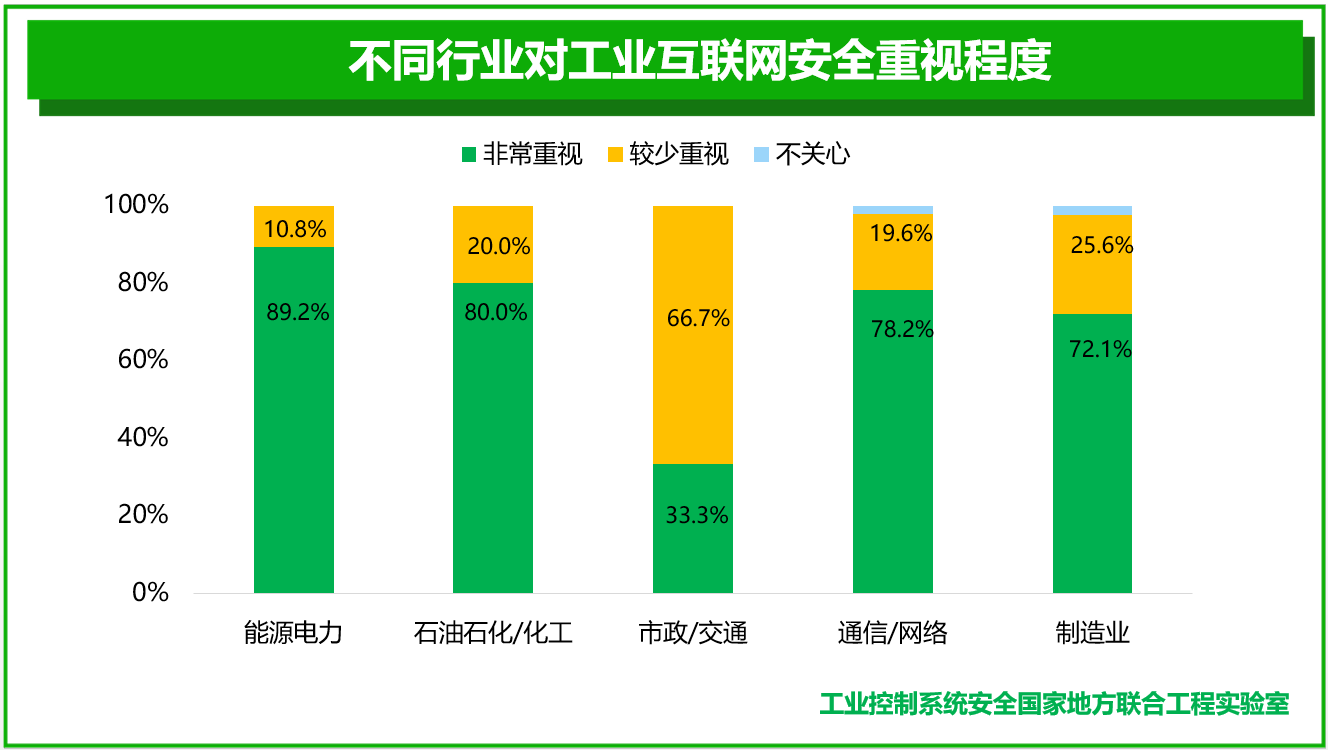
联合实验室在全国范围内对工业企业用户进行问卷调查。为了更真实的了解工业企业的安全需求，根据参与行业的单位属性将制造业、市政/交通、通信/网络、石油石化/化工、能源电力用户填写的问卷作为有效数据进行分析。

### 工业互联网用户对工业互联网安全的重视程度

通过对问卷调查数据统计发现，2018年工业互联网行业用户对安全的重视程度较高，有**76.1%的工业用户非常重视工业互联网安全的建设**，根据卡巴斯基《2018工业网络安全现状》中统计结果，77%的受访者认为网络安全是重中之重。国内外的工业企业都已经非常关注工业互联网安全的建设和部署。

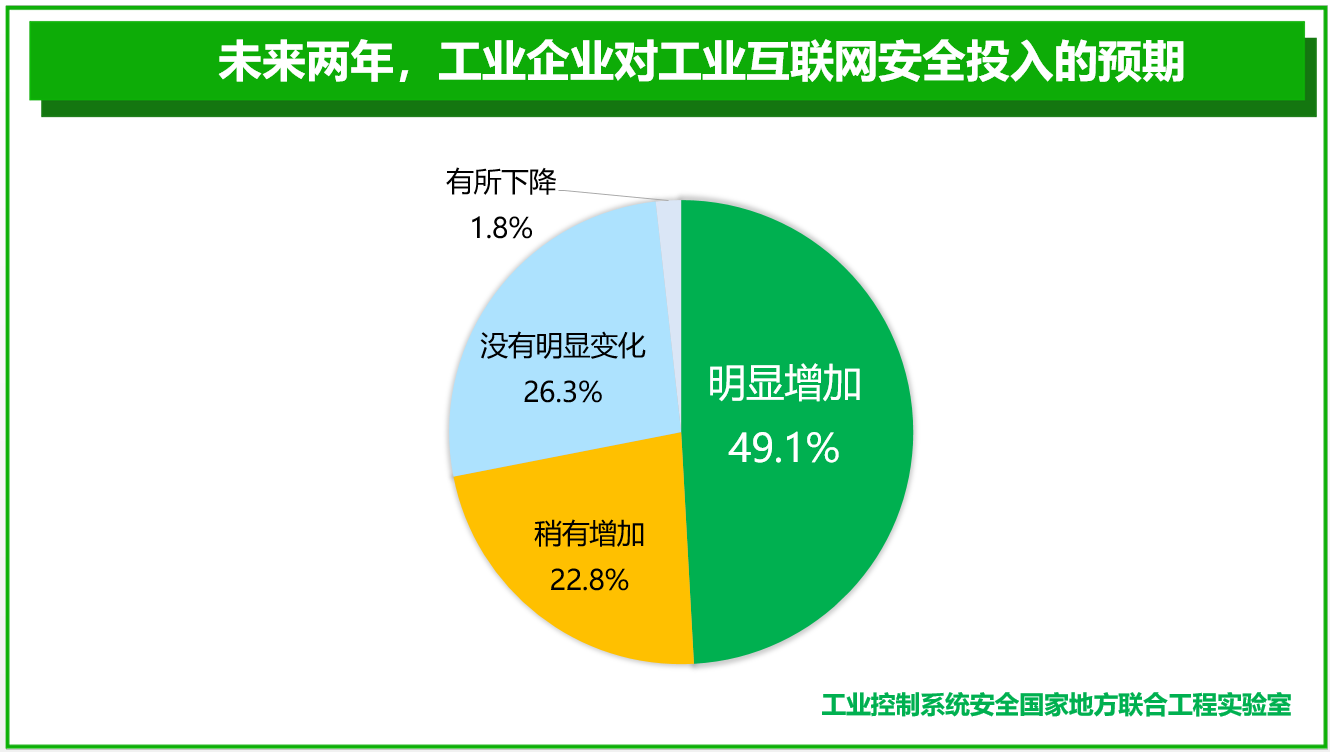


针对不同行业对工业互联网安全重视程度进行分析，统计结果发现，**市政/交通行业、制造业对工业互联网安全重视程度相对较低**，，其中市政/交通行业重视程度最低。



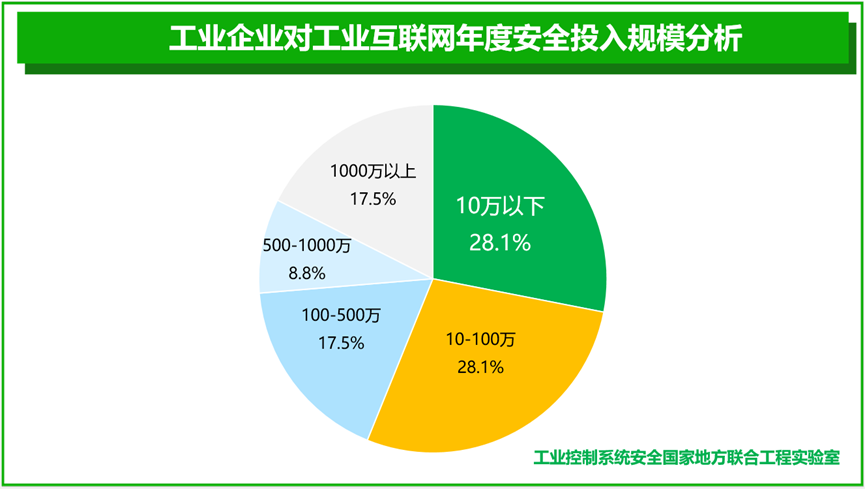
### 工业互联网用户每年在工业互联网网络安全中的资金投入分析

未来两年，有49.1%的被调查工业企业在安全方面的投入有明显增加趋势，22.8%的企业投入的资金稍有增加。总体来看，工业互联网企业对安全的投入有一个良好的趋势，也充分说明了工业互联网用户对工业互联网安全的重视程度越来越高。

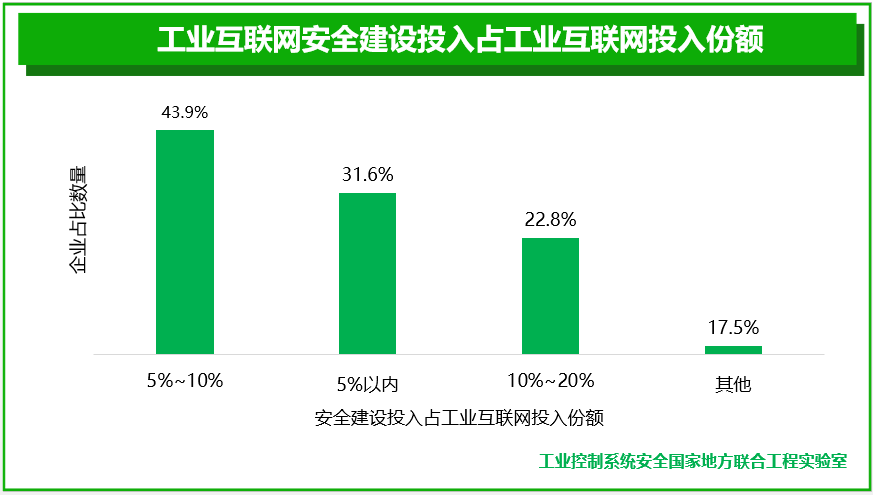


被调查的工业互联网企业计划在工业互联网网络安全方面投入的资金规模集中在10万以下或者10-100万之间，占比均为28.1%。**超过1/2的被调查企业对安全的投资金额集中在此范围内**。由此可见，工业互联网安全市场还有较大的提升空间。

值得关注的是，大型制造企业和通信/网络对安全投入规模较大，其中17.5%的被调查企业年度安全投入超过1000万，呈现一个跨越式进阶投资，一部分企业已经非常重视工业互联网安全的建设，纷纷开始布局。

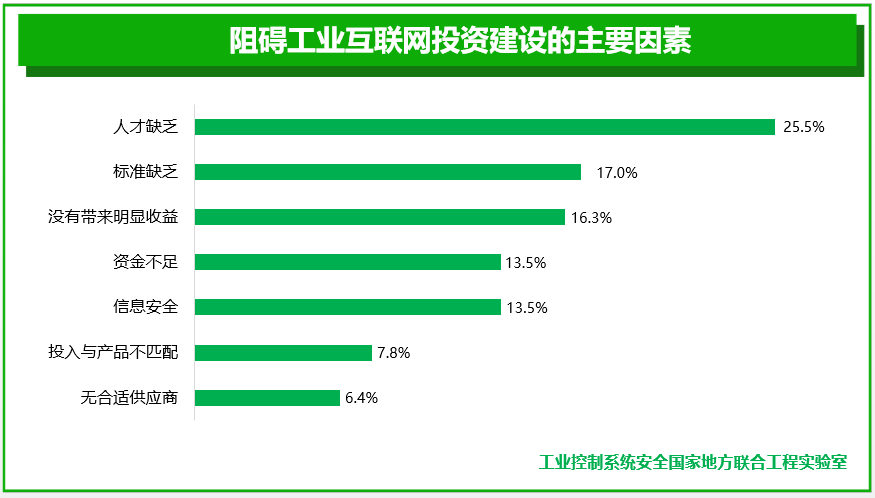


针对工业互联网安全建设费用占工业互联网投入份额进行统计分析发现，43.9%的被调查者认为应该占工业互联网投入金额的5%-10%之间，投入份额在10%以下的企业达到3/4以上。可见，**针对工业互联网安全建设的投入金额比例总体还是偏低的**。虽然工业企业对工业互联网安全的重视程度相对提高，但总体资金投入仍不足。

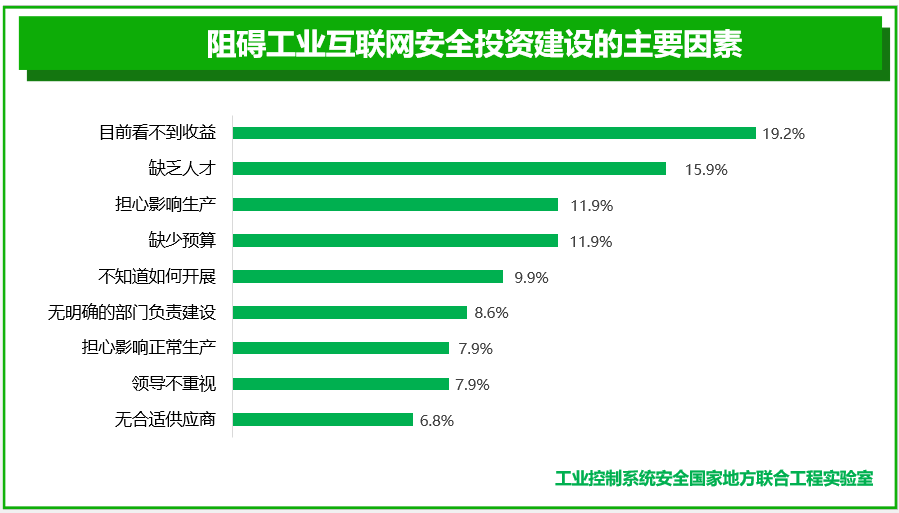


### 阻碍工业互联网安全投资建设的主要因素

为了更全面的了解总体资金投入不足的影响因素，首先分析阻碍工业互联网投资建设的原因。经过统计分析发现，**人才缺乏是影响工业互联网建设的首要因素**，值得注意的是信息安全和资金不足占据相同的比例。可见信息安全在工业互联网投资建设中影响越来越大。



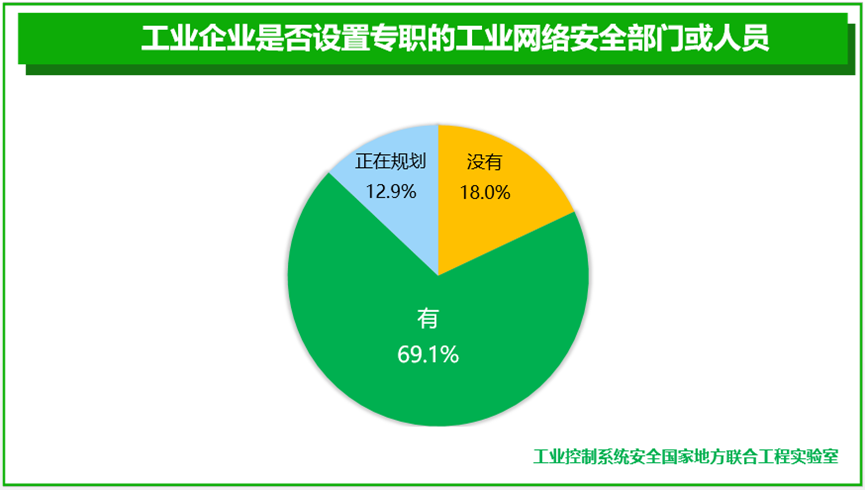
针对工业互联网安全投资建设的影响因素分析发现，**目前“看不到收益”仍然是阻碍安全投资建设的最主要因素**。工业互联网安全建设最大的难处在于没有造成安全事故，企业高层较难理解安全建设短时间内给企业带来的收益，工业互联网安全建设不被工业企业理解。



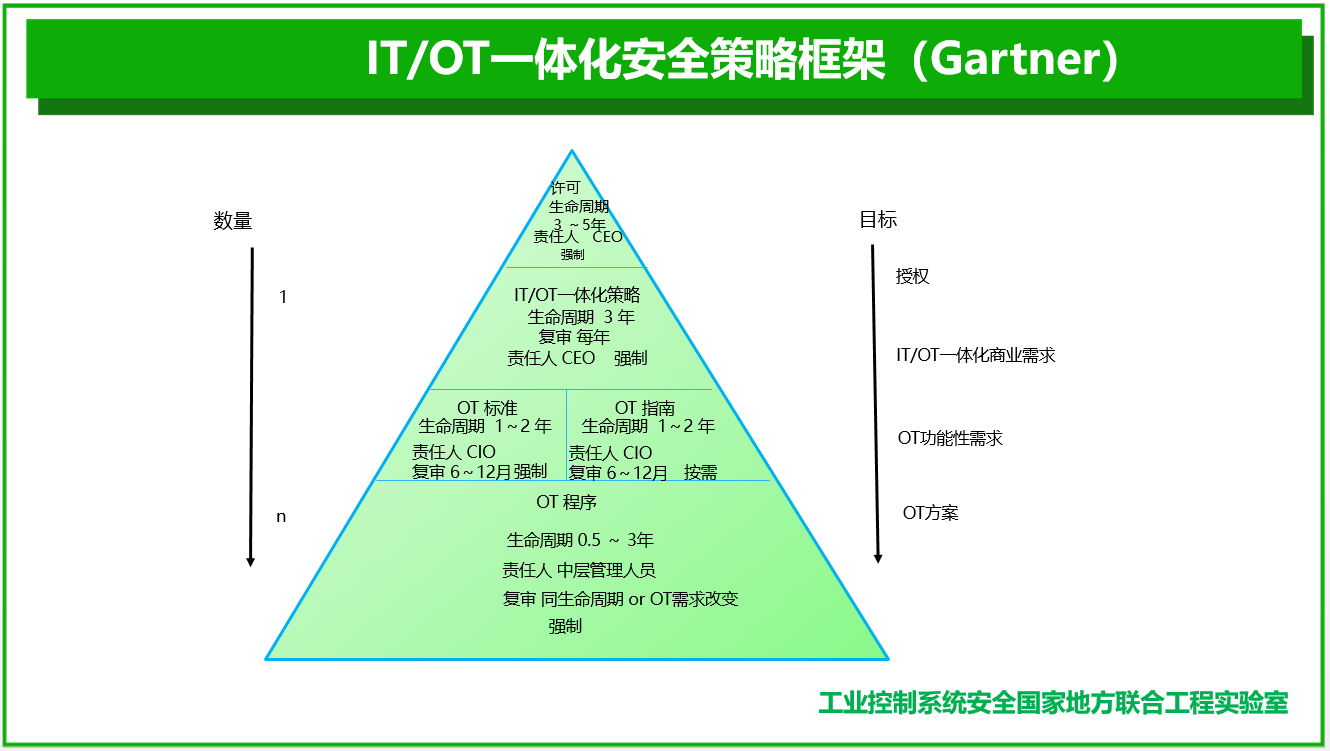
无论是工业互联网建设还是工业互联网安全建设，人才的缺乏都是阻碍发展的重要因素。根据国际非盈利会员学会（ISC）2 2018年网络安全劳动力研究表明，北美、拉丁美洲、亚太地区以及欧洲、中东和非洲的**全球网络安全人才缺口已扩大至近300万**。根据360互联网安全中心和智联招聘联合发布的《2018网络安全人才研究状况研究报告》统计，2018年上半年，网络安全人才需求规模指数较2017年上半年同比增长了44.9%，与2017年下半年相比环比增长了9.4%。可见，对网络安全人才的强劲需求还将持续较长时间。

### 工业互联网安全团队现状

是否设置专职的工业网络安全部门或人员在一定程度上反映出工业企业自身网络安全建设水平。对工业企业是否设置专职的工业网络安全部门和人员进行统计分析发现，**69.1%的工业企业有专门的人员/部门负责安全**，12.9%的企业正在规划，可见多数企业已设置或者正准备设置安全部门或人员。



**除了工业网络安全团队外，在工业网络安全建设方面，IT部门参与程度最高，达到37%**。董事长或高级管理人员的参与程度相对较低，仅占到10%。根据Gartner发布的IT/OT一体化安全策略框架，从上层到下层，其都有企业高层或者管理人员参与，高层领导对工业互联网安全的重视程度在一定程度上能够促进工业安全的落实与发展。



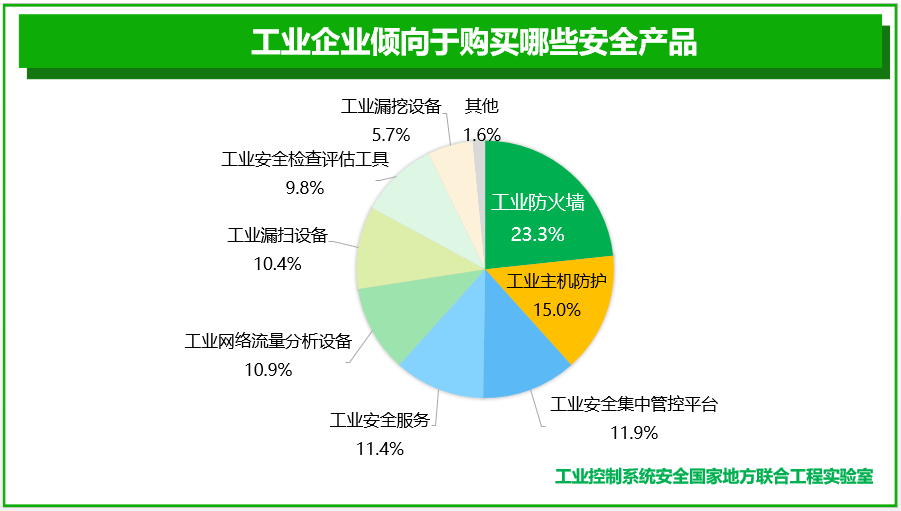
1. 工业企业网络安全市场需求分析

### 工业互联网安全产品需求

**防护类产品需求较高，网络安全关注度高。**工业防火墙、工业主机防护、工业安全集中管控平台三个产品所占比例高达50.2%，占据工业安全产品比例的一半，工业安全集中管控平台主要为防护类产品做管控，将其归为防护类。由统计结果可见，防护类产品需求总体较高，工业防火墙占比23.3%，在工业安全产品体系中所占比重最高，可见工业企业的首要关注点在工业企业的网络安全建设方面。

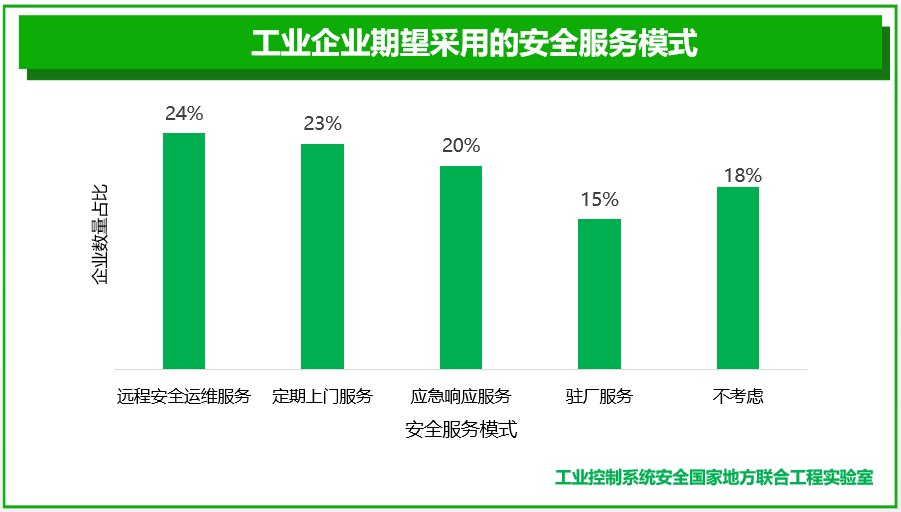
其次为工业主机防护，工业主机老旧操作系统较多，工业主机在投运后会运行很多年，硬件资源受限，同时存在老旧操作系统，往往难以安装杀毒等IT安全防护软件。因此，工业主机目前基本处于没有任何安全防护软件的裸奔状态，而且运行时间较长存在众多的漏洞，因此工业主机的安全防护也是势在必行。

**非防护类产品比例相当，呈现多样化趋势。**工业网络流量分析设备占比10.9%、工业安全服务占比11.4%、 工业漏扫设备占比10.4%、工业安全检查评估工具占比9.8%、工业漏挖设备占比5.7%。相对来说，各产品所占比例相当，呈现多样化趋势。安全检测类、安全评估类、安全服务类、安全研究类产品发展平衡，工业安全产品和服务体系日益完善。

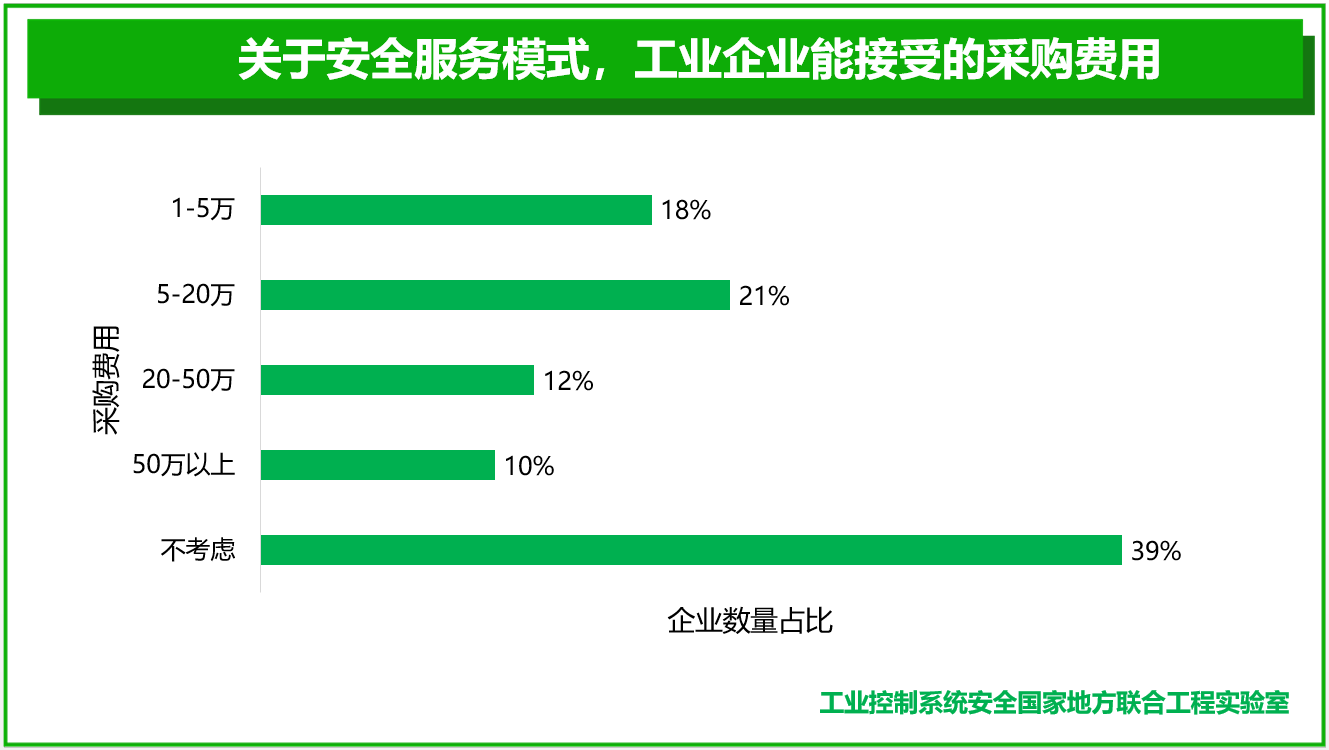


### 工业互联网安全服务需求

对被采访者进行工业互联网安全服务的调查分析，82%的被采访者企业考虑采用“工业互联网安全托管服务”，仅有18%的企业不考虑。其中远程安全运维服务占比最高，达到24%，驻场服务相对较少，占比15%。远程安全运维服务相对而言，所需成本较低，驻场服务成本偏高。企业所选择的工业互联网安全服务随着各服务成本的增多，其选择的比例相对较少。不管是选择何种安全服务，**总体有意愿部署工业互联网安全服务的企业达到4/5以上**，安全服务市场总体形式较乐观。

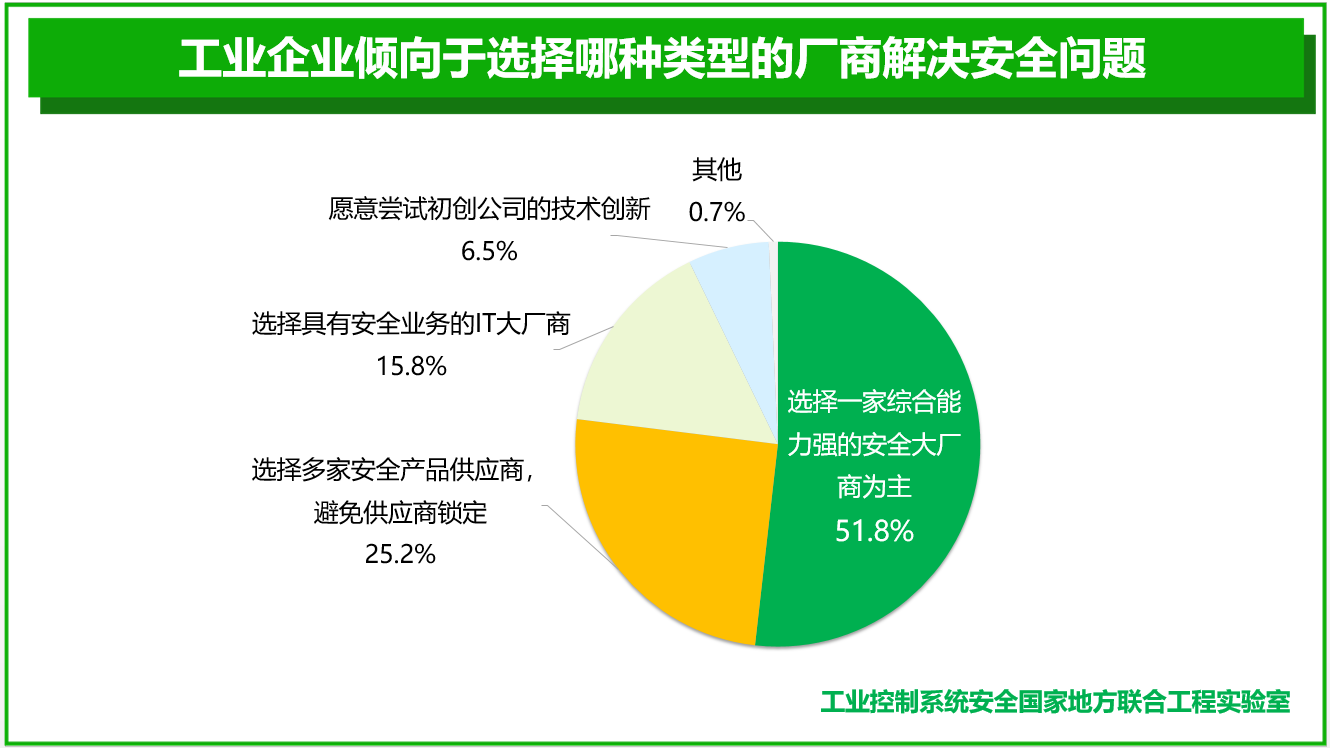


针对工业互联网安全服务所能接受的采购费用进行分析，**低于20万的企业占比达到39%，**从采购费用的占比上也一定程度反映出企业选择相对费用较低的安全服务模式的原因。



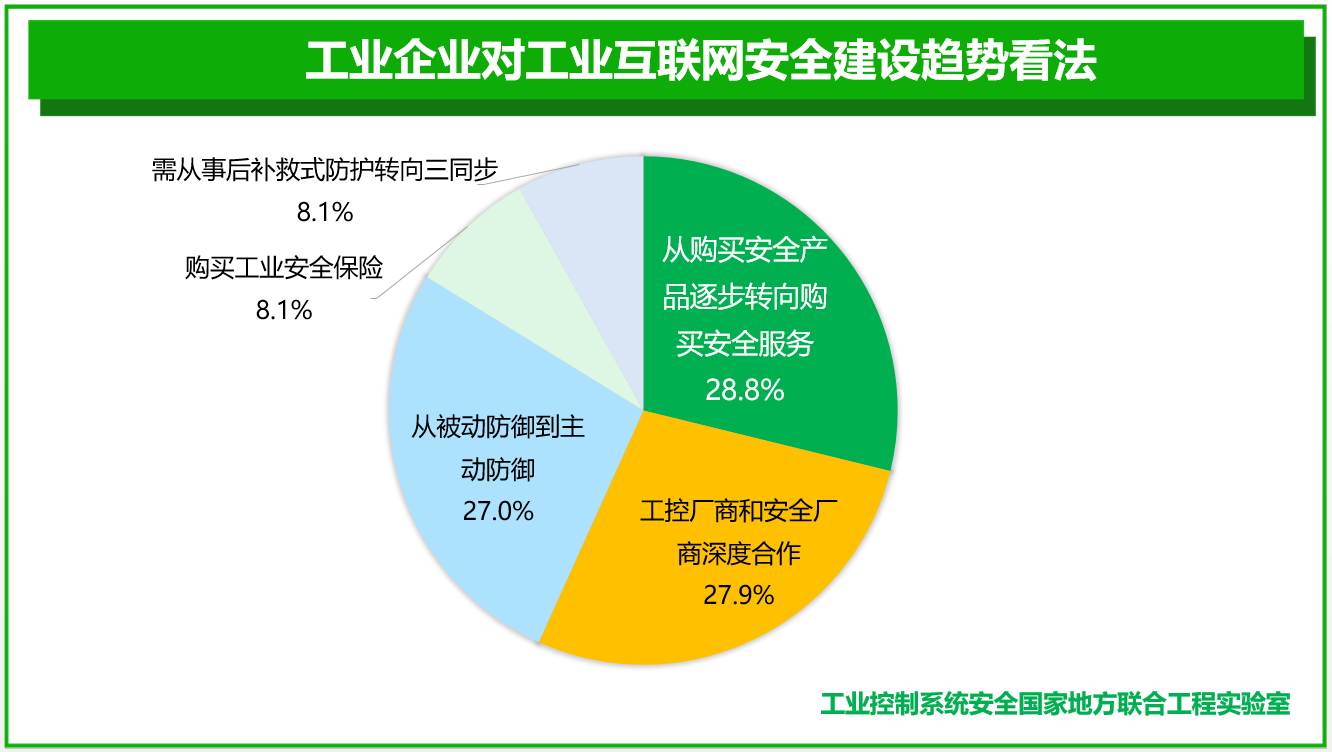
### 工业互联网安全应急响应需求

针对安全问题应急响应解决方案，超过一半的被调查企业愿意选择一家综合能力强而且规模较大的安全厂商解决安全问题，25.2%的企业愿意选择多家安全产品供应商，避免供应商锁定现象，仅有6.5%的企业愿意尝试初创公司的技术创新。



1. 工业互联网安全发展趋势
2. 工业互联网安全建设发展趋势

针对工业互联网安全建设进行调研分析，我们发现如下几点趋势：



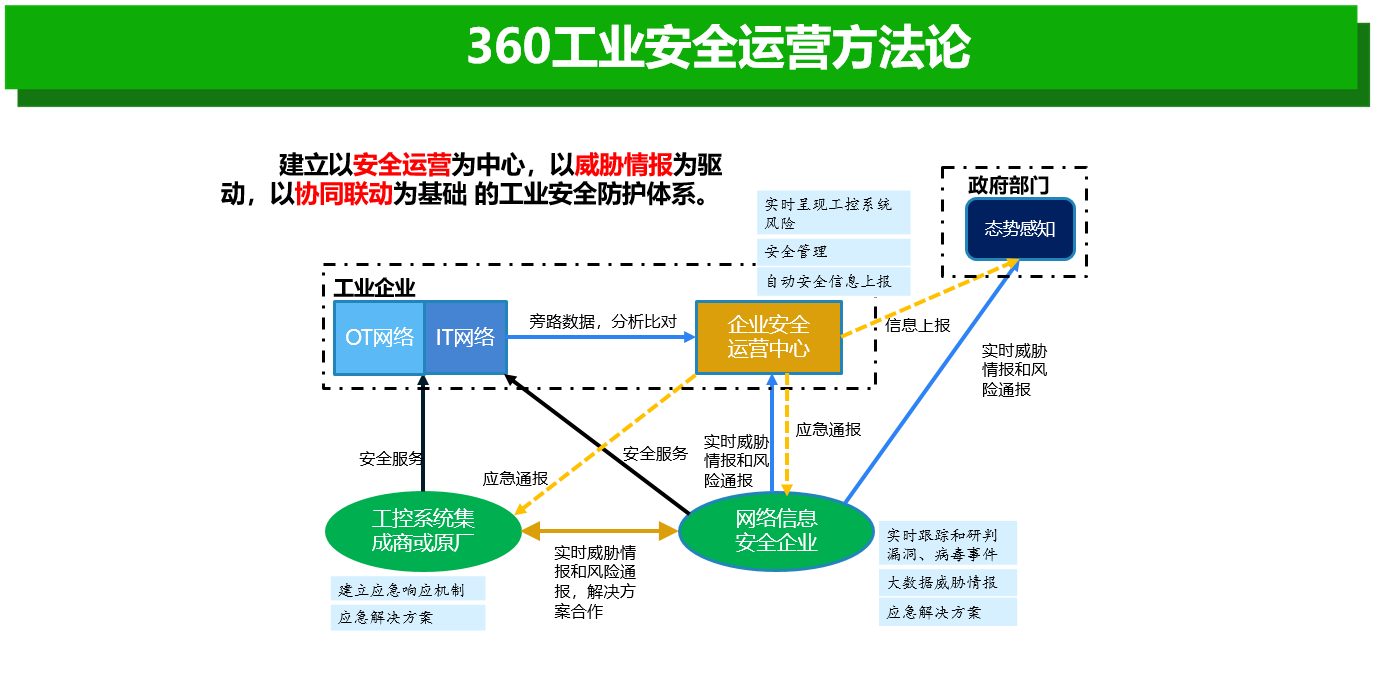
**趋势一：工业企业安全意识有所提高，安全服务市场扩大**

从购买安全产品逐步转向购买安全服务占比达到28.8%，可见工业企业已不完全满足于工业安全产品的部署，安全服务的购买更有效的保障工业企业的安全，提供工业生产的信息安全整体保障。提供产品+服务的整体性解决方案是工业互联网安全发展的主要趋势。Gartner在《2018工业安全市场指南》中也扩展了OT安全性的概念，将OT安全服务纳入OT安全范围内，安全厂商在深度挖掘工业企业安全需求做好工业安全产品的同时，也需考虑安全服务的建设。

**趋势二：多方协作趋势明显，构建产业协同的联合防御体系**

工控厂商和安全厂商深度合作占比达到27.9%。工业互联网是工业互联网是互联网和新一代信息技术（IT）与操作技术（OT）全方位深度融合所行成的产业和应用生态，工业互联网安全的建设发展首先需要熟悉工控背景，无论是做软件、硬件、系统集成都需要深入具体的应用场景，因此需要多方的通力协作。

此调研趋势和360工业安全运营方法论如出一辙，360工业互联网安全建设倡导以安全运营为中心，以威胁情报为驱动，以协同联动为基础的工业安全防护体系。



安全企业需要不断深入与更多的工业企业、工控系统集成商、安全厂商进行生态合作与交流，为工业企业客户提供更加优质的工业互联网安全解决方案。

**趋势三：技术层面深度创新**

从被动防御到主动防御占比27.0%，需从事后补救式防护转向三同步（同步建设/规划/运营）占比8.1%，两者均可以归为从技术层面创新来解决工业互联网安全问题。

工业安全信息安全目标重要性排序不同造成了工控系统与IT系统在风险评估、安全需求、标准要求、实现方案、部署实现、安全运维整个安全生命周期过程都有很大不同。因此，传统的IT信息系统的网络安全技术并不能直接应用于工业控制系统，从以“黑名单”为主的被动防御体系到以“白名单”为主的主动防御体系的转变从技术层面打破壁垒，强化工业互联网安全防护能力。

1. 工业互联网安全技术发展趋势

### 引入数据驱动安全的技术理念

目前国际上公认的，解决网络安全攻防不对称问题的方法之一，就是数据驱动安全。对于工业互联网企业来说，对某一行业中某一家企业的攻击，如果被发现，攻击方法和攻击目标被辨析，则一方面可以结合全网的安全大数据和企业自身的安全大数据进行分析，另一方面可以形成有效的威胁情报，提升整个行业的防御能力。

### 基于威胁情报的工业威胁监测技术

威胁情报依托于云端的海量工业数据，经过数据收集、数据清洗、数据关联、数据验证、上下文、优先级、格式化、情报分发等过程生成。威胁情报通过统一的规范化格式将攻击中出现的多种攻击特征进行标准化。

基于威胁情报的工业威胁检测技术能够对工业互联网攻击中出现的特点进行识别、背景信息关联和可视化展现。该技术不仅可以更早地发现威胁和进行响应处理，还可以实现从点到面的协同防护，极大地压缩攻击者进行攻击的时间并提升其成本。该技术可对受害目标及攻击源头进行精准定位，最终达到对入侵途径及攻击者背景的研判与溯源，帮助企业从源头上解决安全问题。

### 基于大数据的工业态势感知技术

大数据时代的到来为工控企业安全提供了新的技术手段，工业领域传统的数据资产、设备物联数据、外部数据进行统一管理，将工业大数据技术和工业云相结合，实现对云端数据、本地数据的采集、分析并从功能维度进行汇总、查看、统计及处置。

在工控企业研发设计、生产过程、需求预测、供应链优化等环节利用大数据技术进行持续监控收集、实时探测，在云端判断、取证、溯源、修复从而建立可信任的设备、信息、和软件。基于大数据处理的工业态势感知技术成为工业大数据采集、存储、处理和呈现的有力武器，能够对标识态势、攻击源、攻击事件和工控资产的态势进行可视化展示，并通过可视化界面进行数据关联查询，及时对工控环境中未来风险进行预测、预防。

### 网络安全、功能安全、可靠性融合技术

工业互联网系统因其对人身安全、环境、社会经济效益的巨大影响，相对于一般电子信息系统更加强调它的RAMS属性，即：R可靠性（Reliability）、A 可用性（Availability）、M 可维修性（Maintainability）、S 安全性（Safety、Security）。所以只强调工业互联网的网络安全，不考虑其它RAMS属性，不能统筹考虑工业互联网网络安全、功能安全和可靠性，将难以满足行业、客户的全部需求。

工业领域涉及行业较多，包括能源、电力、通信、交通、金融等关键信息基础设施，然而不同行业之间的工业控制系统生产工艺、供应链等应用特点差距较大，利用统一的技术标准、安全体系无法解决企业的安全问题。同时预防性维修、柔性生产等新业务的需求也面临着新的网络安全威胁。因此，在不断加强工业互联网网络安全建设中，如何将各行业之间的特点相融合，形成有效的业务安全建设的最佳实践，是工业互联网安全的发展方向之一。

### 应用工业大数据进行异常发现和实体行为分析

对生产故障的预测性维护，找出生产环节的异常，已经成为目前工业大数据的主要应用方向之一。工业生产设备损坏或衰退的预测与发现，生产流程停机的预测与发现，其实就是一种工业生产的异常发现。而对工业互联网的攻击也可以产生类似异常。因此，可利用工业大数据发现工业生产异常的能力，为安全大数据的分析提供触发条件或关键线索，这将成为数据驱动安全的最值得实践的方法之一

另外安全大数据还可以被用于工业互联网中的用户和实体行为分析，对用户的行为和设备的行为用大数据的方法建立行为基线，基线偏离将触发异常，这也将成为安全大数据重要应用手段之一。

### 构建产业协同的联合防御体系

我国目前暴露在公共互联网上的工业设备，约在千台左右。但是美国暴露在公共互联网上的工业设备则多达数万台。随着我国工业互联网的发展，将有大量的工业企业接入公共互联网。在这种情况下，受到人才、设备、数据、情报等方面的限制，任何一个企业都很难进行单独的防御。

所以，未来的工业互联网企业，与其设备提供商、安全服务商、监管机构等都需要建立协同机制，共同应对来自工业、互联网、网络安全等跨领域、跨行业的挑战。网络安全的能力，将变成一种可定制的服务，工业互联网企业可以根据自己的威胁、成本、人才和运行阶段按需使用。

1. 工业互联网安全发展建议
2. 对工业企业的建议

网络化发展是工业企业不可阻挡的发展趋势，特别是消费类产品的生产加工企业。应该充分注意到网络安全的高风险性，同时意识到远离网络连接并不等于远离网络攻击，而远离网络所造成的技术落后将导致竞争力的实质性落后，因此面对网络技术，充分评估网络安全风险，加强网络安全防护措施，才是正确发展思路。“不能只要发展，不顾安全问题，也不能因安全风险，而不努力发展”

在大力推进我国企业由传统生产方式向数字化、网络化、智能化转型过程中，企业应积极进行工业控制网络安全升级改造，对接国家相关政策，加大研发和管理投入。应积极推进与安全服务企业协同开展行业系统的安全解决方案应用试点示范，从理论和实践中构建工业控制网络安全技术与管理保障体系，具备对工业互联网的网络安全防护、应急响应等保障能力。

值得关注的是，近一年来国内在汽车、电子制造、钢铁冶炼、机械加工、微电子等行业发生的数起工业安全事件，八成首先攻击或影响的是工业主机，只有二成是其他原因，利用好这个二八定律，从工业主机开始构建工业互联网安全防护体系。

如果理解了工业互联网安全“二八定律”，优先保护好引起80%工业安全事件的20%防护目标，将取得“最高费效比”实现“事半功倍”。具体的操作建议如下：

**梳理工业资产，重点关注工业主机资产。**对生产网中工业资产和工业主机进行全面梳理，通过定义网络IP段分组，对指定的网络分组进行周期性地发现与统计网络中的终端数量及类型，从而了解生产线上工业主机数量，测算出工业主机安全防护系统终端的需要安装的数量，为工业主机防护的实施、管理和安全运维提供有效的参考，有利于实现资产统计和分析。

**做好工业主机防护。**对生产网中“裸奔”的工业主机实现了“白名单”技术安全防护，并结合“永恒之蓝”漏洞防御进行现在对工业企业影响最大的勒索病毒的“超前防御”，从而形成多层关卡层层拦截，对病毒进行入口拦截、运行拦截、扩散拦截。同时对移动U盘进行了有效管控，防止恶意程序攻击，保障生产稳定运行。

**持续监控生产风险。**通过已安装工业主机防护的监控和管理能力，对生产网中的已联网工业主机进行全面风险监控和集中管理，第一时间发现工业主机白名单告警、异常登录、移动介质违规使用等安全风险。对已经部署的工业主机，应当部署工业主机防护软件进行全面防护；在新建工业系统时，应要求供应商配置工业主机防护软件；在系统改造升级时，新增的主机也都应当安装工业主机安全防护软件，从而做到实时监测，保护泛终端安全。

1. 对安全服务机构的建议

安全服务机构除了以监督管控为主的国家有关管理机构外，更多的安全服务要靠商业化企业提供。当安全服务质量与利润直接挂钩时，提高服务质量才是竞争实力的体现。因此安全服务机构应该以具有前瞻性的眼光部署安全防护措施，提供高质量持续性的安全服务，为企业和社会提供服务的同时，给自身企业带来丰厚的利润回报。

安全服务机构应以高标准的技术水平为基础，建设工业控制网络安全态势感知及共享平台。《工业控制系统信息安全行动计划（2018-2020年）》提出围绕工控安全态势感知、安全防护和应急处置能力提升，提出建成“全国在线监测网络、应急资源库以及仿真测试、信息共享、信息通报平台（一网一库三平台）”。安全服务机构对此项工作的推进承担重要责任，同时也给自己的服务水平和市场认可度带来很大的提升。

1. 对政府主管部门的建议

政府主管部门对工业企业和安全服务企业的管理是安全生产的底线，是保障生产安全和社会稳定不可或缺的组成部分。

为了工业互联网的安全健康发展，政府主管部门应进一步强化工业互联网安全技术发展顶层设计，瞄准工业网络安全基础技术、共性关键技术和前沿技术以及重点工业行业的网络安全解决方案，研究出台政府指导性文件，为突破关键核心技术与产品、培育骨干企业、优化产业生态环境提供有力指引，着力构建安全可控的工业互联网体系机构，并使其推进工业生产的智能化发展。

考虑到工业企业对网络安全问题的重视不够和工业互联网面临严峻网络安全威胁这一现状，对政府主管部门提出如下建议：

**统筹规划，合力发展。**充分发挥财政资金的引导作用，吸引社会资金积极参与，加大引导资金投入，支持企业、研究机构等联合攻关，共同承担具有自主知识产权的工业互联网安全核心技术攻关，构建包括安全架构、基础软硬件、网络和安全设备、网络安全服务等一体化自主可控技术体系，推动安全产品和服务的示范应用。同时积极培育国内工控互联网领域的安全解决方案服务商，重点扶持推广自主可控的工业互联网产品和服务。

**顶层设计，标准推动。**加强工业控制网络安全技术标准顶层设计和统筹协调，研究制定工业互联网设备、平台、控制、数据等层面的安全防护、测试、评估规范，加快制定工控安全防护能力评价方法、工控设备产品级安全测试方法、工业互联网平台系统安全要求等急需标准研制，搭建重点标准的综合测试验证平台，开展相关标准试点工作。利用国际标准化交流平台，推进我国自主知识产权工控安全技术标准成为国际标准，实质性参与工控安全国际标准化工作，提升我国影响力。充分发挥国家工业网络安全产业发展联盟等行业组织的作用，加强国家技术标准宣贯，建立行业技术标准体系，编制技术与产品推荐目录，推广通用安全框架及技术解决方案。

**重视人才，培养高端。**加大专业人才培养和使用力度。加强工业互联网安全相关学科建设，鼓励工业企业加强与院校合作，联合培养既掌握工业控制知识又熟悉安全防护技术的复合型人才，为构建以企业为主体、产学研相结合的工业控制网络安全技术创新体制和技术与产品方案落地实施提供人才队伍支撑；推动高端人才开展国际交流与合作，加强与国外知名院校及工控网络安全企业的交流合作，培养具备国际视野和水平的工控网络安全技术人才，广揽海外留学回国优秀专业人才加入到核心关键技术的研发队伍；发挥国家工业网络安全产业发展联盟的资源优势，打造国家级工业网络安全高端智库，为工业网络安全战略部署、规划制定、决策咨询、重大问题提供智力支持和技术支撑。

1. 工业互联网安全应急响应典型案例及总结
2. 某知名汽车零部件生产企业遭受“永恒之蓝”勒索病毒攻击

**场景回顾**

2018年7月17日，某知名汽车零部件生产企业工业生产网络遭受“永恒之蓝”勒索病毒的攻击，酸轧生产线一台Windows Server08 R2主机出现蓝屏、重启现象。当日晚上，4台服务器出现重启，现场工程师通过查阅资料，对病毒进行了手动处理。9月10日开始各条生产线出现大量蓝屏和重启现象，除重卷、连退生产线外，其他酸轧、包装、镀锌生产线全部出现病毒感染、蓝屏/重启现象。此时，病毒已对正常生产造成严重影响。9月12日，该汽车板厂求助360工业互联网安全应急响应中心，360工业安全应急响应中心高度重视，对事件进行全面处置。

**问题研判**

经过对各生产线的实地查看和网络分析可知，当前网络中存在的主要问题有：

1）网络中的交换机未进行基本安全配置，未划分VLAN，各条生产线互通互联，无明显边界和基本隔离；

2）生产线为了远程维护方便，分别开通了3个运营商ADSL拨号，控制网络中的主机在无安全措施下访问外网；

3）控制网中提供网线接入，工程师可随意使用自己的便携机接入网络；

4）U盘随意插拔，无制度及管控措施；

5）安全意识不高；

6）IT、OT的职责权限划分不清晰。

**处置方案**

攻击目标是经过精心选择的，承载了核心业务系统，客户一旦中招须缴纳赎金或者自行解密，否则业务瘫痪。镀锌生产线处于停产状态，以“处置不对工业生造成影响或最小影响”为原则，首先检查镀锌生产线服务器。然后进行病毒提取；停止病毒服务；手动删除病毒；对于在线终端，第一时间推送病毒库更新和漏洞补丁库并及时采取封端口、打补丁等措施，避免再次感染。

1. 某大型炼钢厂遭受挖矿蠕虫病毒攻击

**场景回顾**

2018年10月31日，360工业安全应急响应中心接到该炼钢厂电话求助，称其工业生产网络自10月起各流程工艺主机遭受了蠕虫病毒的攻击，出现不同程度蓝屏、重启现象。早期在其他分厂区曾出现过类似现象，10月18日该炼钢分工厂出现主机蓝屏重启，10月30日晚间蓝屏重启主机数量增多，达到十几台。意识到病毒在L1生产网络有爆发的趋势，厂区紧急配置了趋势杀毒服务器，并在各现场工控主机终端安装趋势杀毒网络版本进行杀毒，部分机器配合打补丁进行应急处置。

**问题研判**

通过360工业安全应急响应人员近两天的情况了解、现场处置，可以确认L1网络中感染了利用“永恒之蓝”漏洞传播的挖矿蠕虫病毒（Wannamine），OA/MES网络主机既感染了挖矿蠕虫病毒，又感染了“永恒之蓝”勒索蠕虫变种。由于网络未做好隔离与最小访问控制，关键补丁未安装（或安装未重启生效），蠕虫病毒通过网络大肆快速传播与感染，导致蓝屏、重启事件。网内主机感染时间有先后，网络规模庞大，因业务需要，外网主机可远程通过VPN访问生产网中主机，进而访问现场PLC；网络中存在多个双网卡主机，横跨L1、L2网络，进而造成整个L1 、L2、L3实质上为互联互通；同时传播感染有一定的时间跨度，被感染的主机亦可以攻击网络中其他目标，无全网全流量监控。由分析可知，挖矿蠕虫病毒、“永恒之蓝”勒索蠕虫变种通过某种网络途径，采用系统漏洞利用的方式传入，由于内部网络无基本安全防护措施且互联互通，进而导致了病毒迅速蔓延扩散。

**处置方案**

对该炼钢厂L1生产网络中的多个流程工艺，包括转炉、异型坯、地面料仓、精炼、倒灌站等操作站主机进行处置，当前病毒传播、蓝屏重启现象已得到基本控制，部分主机已做过处理。对于其他主机建议做如下处理：确认主机是否存在挖矿蠕虫病毒或“永恒之蓝”勒索病毒；挖矿蠕虫病毒处置方式： 安装微软补丁： 建立完善的工业安全防护制度和统一方案，确保生产安全、连续、稳定。

1. 某卷烟厂遭受蠕虫病毒攻击

**场景回顾**

2018年11月12日，某大型卷烟厂卷包车间主机出现不同程度蓝屏、重启现象，运维人员通过安装免费版本杀毒软件及关闭445端口暂时解决了问题，但是在11月19日，卷包车间工业生产网络（包括数采、物流和生产）较多数量工控机出现蓝屏、重启现象，意识到病毒在生成网络有爆发的趋势，该卷烟厂相关负责人紧急联系了360工业安全应急响应中心，同步现场情况，360工业安全应急响应中心对事件高度重视，对该卷烟厂工业主机蓝屏问题进行全面处置。

**问题研判**

经过情况了解、现场处置，360工业安全应急响应人员可以确认工业生产网络中感染了“永恒之蓝”勒索蠕虫变种。由于网络未做好隔离与最小访问控制，关键补丁未安装（由于系统原因部分无法安装），蠕虫病毒通过网络大肆快速传播与感染，导致蓝屏、重启事件。工业生产网络中存在大量双三网卡主机，车间多个接入交换机、汇聚交换机直至核心交换进行串行级联，无基本逻辑隔离，加之多网卡主机的存在，导致网络边界模糊，生产网与办公室网络连通，办公室主机遭蠕虫感染之后，通过网络迅速传入生产网中，网络中暂无全网全流量监控、工业级防火墙和主机安全防护。由分析可知，“永恒之蓝”勒索蠕虫变种通过某种网络途径，利用操作系统漏洞的方式传入，先感染车间办公室主机，进一步通过网络感染内网中的工控机。

**处置方案**

经过基本处理，对卷包车间的10台工控机进行了处置：手动进行病毒检测样本抓取，创建阻止445端口数据传播的组策略，当前病毒传播、蓝屏重启现象已得到基本控制，对于其他主机，建议做如下处理：确认主机是否存在 “永恒之蓝”勒索病毒；安装微软补丁；建立完善的工业安全防护制度和统一方案，确保生产安全、连续、稳定。

1. 某半导体制造企业遭勒索软件攻击

**场景回顾**

2018年12月5日，国内某半导体制造企业遭受勒索病毒攻击，其核心生产网络和办公业务网络被加密，导致生产停工，被加密的主机被要求支付0.1个比特币的赎金。

**问题研判**

360 企业安全应急响应安全专家通过对现场终端进行初步排查，发现客户终端主机被植入勒索病毒，导致无法进入操作系统。修复 MBR 后使用数据恢复软件恢复部分文件，在部分机器上对日志进行分析，发现其存在域控管理员登入记录。经过排查，初步判断此次攻击事件由黑客入侵企业的备用域控，获得其账号密码，并在bat脚本中批量使用cmdkey命令来保存远程主机凭据到当前会话，随后调用psexec远程执行命令，向域中机器下发攻击文件进行勒索。360 企业安全的同事在客户现场共提取了三个样本， update3.exe、 update.exe、 update2.exe，其功能分别为：将勒索病毒写入主机 MBR、使用类似 TEA 的对称加密算法加密文件、使用 libsodium-file-crypter 开源项目开源代码加密文件。因目前已有多家工控企业遭受该勒索病毒，且攻击者通过人工渗透的方式释放病毒，不排除攻击者会对其他已经控制的内网系统下手， 360 安全监测与响应中心提醒广大用户及时做好安全防护工作。

**处置方案**

使用 PE 系统登入服务器，使用磁盘工具搜索磁盘，并使用安全工具恢复MBR 即可解决系统无法启动的问题。对于已中招服务器下线隔离。对于未中招服务器在网络边界防火墙上全局关闭 3389 端口或 3389 端口只对特定 IP 开放；开启 Windows 防火墙，尽量关闭 3389、 445、 139、 135 等不用的高危端口；每台服务器设置唯一口令，且复杂度要求采用大小写字母、数字、特殊符号混合的组合结构，口令位数足够长（15 位、两种组合以上；安装终端安全防护软件。

1. 工业互联网安全应急响应案例总结

以上所述仅为2018年360工业安全应急响应中心完成的近二十起应急响应任务中的四个典型案例。对所有应急响应处置进行综合分析、总结，不难得出以下基本结论：

1）从问题和现象上看：企业遭受攻击后的现象多为蓝屏、重启、勒索；病毒多为“永恒之蓝”蠕虫变种、挖矿蠕虫；蠕虫病毒普遍利用MS17-010漏洞进行大面积传播

2017 年 5 月 WannaCry（永恒之蓝勒索蠕虫）在全球范围内大规模爆发，而2018年度蠕虫变种在工业环境中感染、传播呈现爆发的趋势。“永恒之蓝”勒索蠕虫存在多个变种，“永恒之蓝”挖矿也从WannaMine1.0、WannaMine2.0到WannaMine3.0不断更新，传播速度和感染面积惊人。当前企业内网中任然存在大量未安装“永恒之蓝”补丁的主机，工业环境中主机处于裸奔现象更是普遍，病毒在漏洞利用传播的过程中，不同操作系统平台存在不稳定现象，存在引起主机蓝屏、重启几率，挖矿病毒更是利用目标进行挖矿活动，大量消耗主机资源，对连续、稳定、安全生产构成了巨大威胁。

2）从行业分布上看：当前感染蠕虫病毒的企业多为智能制造、钢铁、烟草等行业的企业；

3）从根本原因分析上看：工业环境缺乏基本的安全防护为最主要原因

病毒攻击的目标为主机，而工业主机基本处于裸奔状态；其次网络结构划分不当，缺乏边界防护和网络流量监测手段；再次就是安全管理的问题，包括补丁管理、移动介质使用、第三方运维准入、网络资产台账、人员管理、安全意识提升等等多个方面。

附录一 工业互联网安全事件

1. 美国通报“熔断”和“幽灵”高危漏洞

2018年1月，美国谷歌（Google）公司安全团队Project Zero披露2组高危漏洞，分别是“熔断”“幽灵”漏洞，该漏洞影响英特尔（Intel）、美国超微半导体公司（AMD）等厂商生产的主流中央处理器（CPU）并导致用户敏感信息泄露。

“熔断” （Meltdown，漏洞编号为CVE-2017-5754）和“幽灵”（Spectre，漏洞编号为 CVE-2017-5753、CVE-2017-5715）漏洞会利用CPU芯片硬件层面乱序执行机制的缺陷，使得低权限的恶意访问者可以突破内存隔离，发动侧信道攻击。在未被许可的情况下读取同一系统中的其他进程或同一主机上其他虚拟机内存中的敏感信息，包括密码、帐户信息、加密密钥或理论上存储在内核内存中的任何内容。

此次事件告诫我们：工业企业、工业控制系统厂商及工业控制系统安全企业应该密切关注跟踪工业控制系统漏洞进展；按照《工业控制系统信息安全防护指南》要求，开展工业控制系统及工控主机的安全防护工作，及时修复安全漏洞。

1. 台积电三大基地疑遭勒索软件攻击停摆

2018年8月，台积电位于台湾新竹科学园区的12英寸晶圆厂和营运总部，遭遇勒索软件攻击且生产线全数停摆的消息。几个小时之内，台积电位于台中科学园区的Fab 15厂，以及台南科学园区的Fab 14厂也陆续传出同样消息，这代表台积电在台湾北、中、南三处重要生产基地，同步因为勒索软件入侵而导致生产线停摆。

去年“5.12”勒索软件爆发以来，工业企业已经成为勒索攻击的重灾区，罗马尼亚汽车企业(Dacia)、日产汽车桑德兰工厂、西班牙电厂和天然气企业等，国内外已经有多个行业的众多大型工业企业因为遭遇勒索软件攻击而停产，在国内仅仅360企业处理过的勒索软件感染事件，就涉及汽车生产、智能制造业、电子加工业、烟草等领域十余家单位。这些受害企业普遍遭遇的现象是工业生产网络的工业主机出现蓝屏，反复重启，存储重要生产信息的服务器被加密或文件丢失，从而影响生产，甚至造成停产。

此安全事件告诫我们：我国的工业系统普遍处于没有任何防护手段的“裸奔”状态，企业甚至不了解自己的工业系统信息资产，以及系统之间如何互联，对于当前的勒索软件危害与安全事件发展趋势和应对策略更是缺乏了解。工业企业应对工控网络中的IT资产和OT资产进行全面梳理；进行适当的网络分区和隔离，防止威胁扩散；建立或完善安全组织机构，实现安全运营。

1. 英国2700 万能源智能电表存在安全漏洞

2018年3月，英国情报机构政府通信总部 GCHQ 发现安装在 2700 万个家庭中的新型智能电表存在安全漏洞，可能会对数百万居民的物联网设备构成严重风险。

新型第二代智能电表解决了能源公司第一代仪表的各种问题。与旧的 第一代仪表不同，能源供应商可以使用第二代智能电表以电子方式远程接收仪表读数。攻击者能够窃取智能电表用户的个人信息，利用相同的软件攻击每一个计量器，并篡改账单来获取非法利益。此次事件告诫我们：随着物联网设备不断接入互联网，工业控制系统将面临更为严峻的安全挑战，在设计开发新型仪表过程中，就应该从初期将安全问题考虑在内。

1. 美国天然气输气管道电子系统遭受供应链攻击

2018年4月，美国4家输气管道Oneok公司、Energy Transfer Partners LP（简称ETP）、Boardwalk Pipeline Partners LP（简称BPP）和Chesapeake Utilities Corp（简称CUC）旗下的Eastern Shore Natural Gas（简称ESNG）与客户通信的电子系统被关闭，其中3家公司已证实是网络攻击所致。遭受攻击的电子系统通过计算机交换文件，以此帮助管道客户与运营商沟通需求。

ETP表示这是一起针对第三方服务提供商的攻击。美国律师事务所Jones Walker的高级合伙人Andy Lee指出，美国的管道公司有许多都依赖第三方公司的电子通信系统。此类系统日益引起黑客的关注，其原因在于这些系统易被攻破，能够让黑客有机会勒索，或者窃取信息在“暗网”兜售。此类安全事件告诫我们：工业企业应该加强供应链安全建设，《工业控制系统信息安全防护指南》中明确供应链管理，在选择工业控制系统规划、设计、建设、运维或评估等服务商时，优先考虑具备工控安全防护经验的企事业单位，以合同等方式明确服务商应承担的新安全责任和义务。

1. 伊朗机场显示屏幕遭受黑客攻击

2018年5月，伊朗东北部马什哈德市的机场遭到黑客的攻击。黑客攻破机场网络，在机场出入口的电子显示屏上显示一份抗议伊朗政府在中东地区军事行为的声明。该声明以波斯语呈现，指责伊朗伊斯兰革命卫队（Islamic Revolutionary Guard Corps，IRGC）给伊朗人造成的财政损失。该黑客组织鼓动乘客拍摄电子显示屏图像并通过社交媒体平台进行发布。据伊朗电台调查结果显示，数以百计的伊朗人通过Twitter发布了电子显示屏的照片。

黑客之所以能够挟持电子显示屏并发布图像，是因为他们成功攻破了马什哈德机场民用航空部负责人Mohsen Eidizadeh的电子邮箱。此安全事件告诫我们：随着IT/OT 的融合，生产网和办公网互通互联，且部署使用的邮件系统收发端口往往是企业内网唯一与互联网连接的网络端口，因而成为不法分子关注的重点和网络入侵窃密的主要目标。企业内应坚决禁止使用弱口令；按照相关法律法规、政策要求，落实网络安全等级保护制度和技术防护措施，组织开展邮件系统技术检测和渗透性攻击测试，查找安全漏洞，及时进行整改。

1. 俄罗斯400多家工业企业遭遇网络钓鱼攻击

2018年8月，卡巴斯基实验室（Kaspersky Lab）ICS CERT发现了一系列带有恶意附件的网络钓鱼电子邮件，其邮件伪装成合法的商业邀请函，主要发送给位于俄罗斯的工业企业，且每一封电子邮件的内容都与目标收件人所从事的工作有很大的相关性。攻击者主要是通过分析被攻击企业员工的通信来获取进行犯罪活动所需的信息，通过这些信息对企业进行攻击，不仅会造成企业业务中断，企业的敏感数据也会泄露。

该恶意软件现已造成俄罗斯400家工业企业遭受攻击，涉及行业包括制造业、冶金、工程、能源、矿业、物流、石油和天然气等。恶意软件造成的攻击涉及行业广泛，但均属于工业企业的系统。此安全事件告诫我们：近几年，随着信息技术和操作技术的不断融合，工控系统开放性与日俱增，网络犯罪份子更倾向于攻击工业企业网络，工控网络安全问题不容忽视。

1. 乌克兰国防系统密码竟为初始密码“123456”

2018年9月，乌克兰记者Alexander Dubinsky披露，乌克兰武装部队的自动控制系统（ACS）“Dnipro”长期使用密码“admin”和“123456”访问服务器。无需任何特殊的操作即可自由访问交换机、路由器、工作站、服务器、语音网关、打印机、扫描仪等，黑客可以分析乌克兰武装部队的大量机密信息，仅需要几天时间就可以扫描整个国防系统网络，建立所有网络的拓扑结构，包括部队的属种、结构单位等。

2017年，在“乌克兰女性黑客运动”中Berehynya就曾泄露过乌克兰海军信息与心理行动中心Cipso的个人数据信息。此安全事件告诫我们：网站系统绝不能使用初始密码及弱密码，且设置的密码不能使用纯数字或纯字母，密码最好包括大写字母、数字及特殊字符等，保障系统的安全。

1. 洛阳市北控水务集团远程数据监测平台遭到黑客攻击

2018年9月，河南省公安厅官网发布通告，洛阳市北控水务集团远程数据监测平台遭到黑客攻击，致使网页被纂改。洛阳警方第一时间派出网络安全应急处置小组到该中心网站所在地进行处置和调查。经查，洛阳市北控水务集团网络安全意识淡薄，网络安全管理制度不健全，网络安全技术措施落实不到位，未留存6个月以上的网络日志。

2017年6月1日，《网络安全法》正式实施，网络安全等级保护制度上升为法律规定的强制义务，根据《网络安全法》第21条规定，国家实行网络安全等级保护制度，网络运营者应当按照网络安全等级保护制度的要求，履行安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。

此安全事件告诫我们：工业企业应制定严格的内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任;采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施;采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；采取数据分类、重要数据备份和加密等措施以及法律、行政法规规定的其他义务。

附录二 工业控制系统安全国家地方联合工程实验室

工业控制系统安全国家地方联合工程实验室（简称：工业安全国家联合实验室）是由国家发展与改革委员会批准授牌成立，由360企业安全集团承建的对外开放的工业控制安全技术方面的公共研究平台。

实验室依托360企业安全的安全能力和大数据优势，同时联合了公安三所、信通院、国家工业信息安全发展研究中心、中科院沈阳自动化所、东北大学等科研院所及大学。实验室以对工业控制系统安全领域有重大影响的前沿性、战略性技术作为研究目标，建立以工程实验室为主，联合高等院校、科研院所和国家需求部门、企业共同参加的，产、学、研、用相结合的合作机制，发挥高等院校、科研院所在基础理论研究方面的力量和优势，发挥国家需求部门、企业在技术创新和应用方面的主体作用，共享科研成果。

实验室积极吸纳国内外优秀的科技人才，建立高水平专业人才培养基地。目前实验室已与北京大学、西安电子科大、吉林大学、武汉大学、北京理工、信息工程大学等均建立了人才联合培养机制。

实验室拥有软件著作权7项，专利16项，创新地提出了工业互联网自适应防护架构（PC4R），推出了工业主机防护、工业防火墙/网关、工业互联网安全监测预警系统、工业安全监测等工业安全领域完整解决方案及产品，并已经在众多央企和工业企业中进行应用。未来，工业安全国家联合实验室将充分利用科技资源，发挥产学研联盟作用，打造产业链合作，与产业链企业实现互利共赢，在合作中共同壮大，努力成为工业互联网安全产业创新的龙头。