IT/OT 一体化的工业信息安全态势报告（2017）

工业控制系统安全国家地方联合工程实验室

360 威胁情报中心

2018 年 2 月 1 日

主要观点

IT/OT 一体化融合带来的新挑战

- ✧ IT/OT 一体化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。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，普遍引入生产执行系统 MES，实现管理信息网络与控制网络之间的数据交换和工业控制系统和管理信息系统的集成。MES 不再是一个独立运行的系统，而要与管理系统甚至互联网互通、互联，从而在工业系统中引入了网络攻击风险。
- ✧ 对于传统 IT 网络安全，保密性优先级最高，其次是完整性、可用性。工业网络则有明显的不同，工业网络更为关注的是系统设备的可用性、实时性。在工业系统中，设备超期服役、带洞运行、带毒运行的状况非常普遍。而且有大量的内部系统和设备不必要的暴露在互联网上，进一步加大了工业系统的安全风险。
- ✧ 工业互联网的 IT/OT 融合会带来很多安全挑战。一方面是来自外部的挑战，如：暴露在外的攻击面越来越大；操作系统安全漏洞难以修补；软件漏洞容易被黑客利用；恶意代码不敢杀、不能杀；DDOS 攻击随时可能中断生产；高级持续性威胁时刻环伺等。另一方面是来自工业系统自身安全建设的不足，如：工业设备资产的可视性严重不足；很多工控设备缺乏安全设计；设备联网机制缺乏安全保障；IT 和 OT 系统安全管理相互独立互操作困难；生产数据面临丢失、泄露、篡改等安全威胁等。

工业信息安全建议与展望

- ✧ 建立网络安全滑动标尺动态安全模型，该标尺模型共包含五大类别，分别为架构安全（Architecture）、被动防御（Passive Defense）、积极防御（Action Defense）、威胁情报（Intelligence）和进攻反制（Offense）。这五大类别之间具有连续性关系，并有效展示了防御逐步提升的理念。
- ✧ 从安全运营的角度，建立企业的工业安全运营中心（IISOC）。在 IT 和 OT 一体化推进发展中，IT 技术在 OT 领域大量使用，IT 所面对的风险也跟随进入了 OT 网络，因此工业企业对这两个应用角度都要识别风险的切入点，列举相关的风险，并且要进行一体化的规划。
- ✧ 组建 IT&OT 融合的安全管理团队，对整个工业控制系统进行安全运营。
- ✧ 在技术层面提高防护能力，包括终端层面、网络层面和监管层面，以及数据和系统的可恢复性（备份层面）方面。

摘　要

- ✧ 工业控制系统(Industrial Control Systems, ICS)通常指由计算机设备和工业生产控制部件组成的系统。
- ✧ 根据美国工业控制系统网络紧急响应小组（ICS-CERT）最新统计报告，2015 年漏洞总数为 486 个，2016 年美国关键基础设施存在 492 个安全漏洞。
- ✧ ICS-CERT 的最新报告显示，相关漏洞涉及供水、能源和石油行业等关键基础设施。此外，ICS-CERT 安全研究专家指出，针对工业控制系统环境入侵的攻击者数量增长无疑意味着可利用的漏洞数量和类型也会同时增长。
- ✧ 2000 年 1 月截止到 2017 年 12 月，根据我国国家信息安全漏洞共享平台（CNVD）统计，所有的信息安全漏洞总数为 101734 个，其中工业控制系统漏洞总数为 1437 个。2017 年 CNVD 统计的新增信息安全漏洞 4798 个，工控系统新增漏洞数 351 个，均比去年同期有显著增长。
- ✧ CNVD 在 2017 年收录的工控相关漏洞中，高危漏洞占比最高，达到 53.6%。中危漏洞占比 42.4%，其余 4.0%为低危漏洞。
- ✧ CNVD 已收录的漏洞数量最多的五大工控厂商的安全漏洞数量中，Siemens 最多，为 197 个，其次是 Schneider117 个。
- ✧ 工业互联网安全监测公共服务平台收录了 2017 下半年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。从中分析可知，在八月份和九月中旬期间，国内和全球暴露的工控设备数均有一个明显上升趋势，且 2017 年末比 2017 年中旬暴露的工控设备数多。
- ✧ 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，普遍引入生产执行系统 MES，实现管理信息网络与控制网络之间的数据交换和工业控制系统和管理信息系统的集成。
- ✧ 工业网络则有明显的不同，工业网络更为关注的是系统设备的可用性、实时性，除此特点外，IT 系统和 OT 系统之间仍然存在很多差异性。
- ✧ 根据 ICS-CERT 的报告显示，在 2016 年，工业控制系统网络安全应急小组团队完成了对 290 起安全事件的处理。其中，对制造业的攻击比重最大，有 63 起，约占 22%，此外，通信部门攻击有 62 起，比重第二，有 59 起能源部门安全事件。
- ✧ 2017 年工业网络八大重点安全事件：永恒之蓝勒索病毒、新型物联网僵尸网络 HTTP81、类 Petya 勒索病毒席卷欧洲、美国供水设施网络瘫痪、印度 ISP 遭受 BrickerBot 攻击、瑞典交通机构遭受 DDOS 攻击、巴西银行发现恶意软件攻击、恶意软件 TRITON 攻击能源关键信息基础设施。
- ✧ 2017 年 2 月，美国纽约州金融服务部（DFS）颁布了新的网络安全监管规则，这意味着在纽约运营的主要金融机构迎来了相比过去更为严厉的网络安全防控义务。
- ✧ 2017 年 5 月，澳大利亚总理特恩布尔日前宣布，发布政府首次年度修订版《国家网络安全战略》。该战略于 2016 年 4 月推出，涵盖 33 个网络安全计划，投入资金达 2.31 亿

澳元（约合 12 亿人民币）。

- ✧ 2017 年 1 月，韩国政府向国会正式提交了《国家网络安全法案》。其旨在防止威胁国家安全的网络攻击，迅速积极应对网络危机，为保障国家安全及国民利益做出贡献。
- ✧ 2017 年 7 月，新加坡通信部与网络安全局共同发布了《网络安全法案 2017》（草案）征求公众意见，该草案是新加坡继去年 10 月宣传的旨在加强全球合作伙伴关系的“网络安全战略”之后又一网络安全举措。
- ✧ 2017 年 8 月，英国政府出台《智能汽车网络安全新指南》，指南的全称为《面向联网和自动驾驶汽车的网络安全关键原则》，目标是将之拓展到汽车制造和供应链上的每一方。
- ✧ 2017 年 1 月，工信部印发《信息通信网络与信息安全规划（2016-2020）》，规划》明确了以网络强国战略为统领。
- ✧ 2017 年 3 月，经中央网络安全和信息化领导小组批准，外交部和国家互联网信息办公室 1 日共同发布《网络空间国际合作战略》。
- ✧ 2017 年 4 月，工信部印发《云计算发展三年行动计划（2017-2019 年）》。
- ✧ 2017 年 5 月，国家互联网信息办公室发布《网络产品和服务安全审查办法（试行）》，于 6 月 1 日起实施。
- ✧ 2017 年 5 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》。
- ✧ 2017 年 6 月，《中华人民共和国网络安全法》正式实施，这是我国网络领域的基础性法律，其中明确规定要加强对个人信息保护。
- ✧ 2017 年 7 月，国家互联网信息办公室发布《关键信息基础设施安全保护条例（征求意见稿）》。
- ✧ 2017 年 8 月，工信部印发《工业控制系统信息安全防护能力评估工作管理办法》。
- ✧ 2017 年 11 月，工信部印发《公共互联网网络安全突发事件应急预案》。
- ✧ 2017 年 12 月，工业和信息化部制定了《工业控制系统信息安全行动计划（2018-2020 年）》。
- ✧ 对比 2016 年和 2017 年 Gartner 技术成熟度曲线：OT 安全进入底谷期，估计会在 2018 年进入稳步爬升的光明期。

关键词：工业信息、ICS

目　　录

第一章　概述

一、　研究背景及意义

工业控制系统(Industrial Control Systems, ICS)通常指由计算机设备和工业生产控制部件组成的系统,主要包括五大部分：数据采集与监测控制系统(SCADA)、分布式控制系统(DCS)、过程控制系统(PCS)、可编程逻辑控制器(PLC)及现场总线控制系统(FCS)等。工业控制系统已经广泛应用于工业、能源、交通及市政等领域，是我国国民经济、现代社会以及国家安全的重要基础设施的核心系统。

在工业互联网、“中国制造 2025”、“工业 4.0”等政策驱动下，信息技术（IT, Information Technology）和操作技术(OT, Operational Technology)一体化已成为必然趋势。随着 IT/OT 一体化的迅速发展，工业控制系统越来越多的采用通用硬件和通用软件，工控系统的开放性与日俱增，系统安全漏洞和缺陷容易被病毒所利用，然而工业控制系统又涉及我国电力、水利、冶金、石油化工、核能、交通运输、制药以及大型制造行业，一旦遭受攻击会带来巨大的损失。事实上，对于电力、水利、能源、制造业等领域的工业控制系统的入侵事件，在此之前就已经层出不穷。

2000 年，澳大利亚的一个污水处理控制系统被恶意攻击，造成了该公司的污水处理泵站进行非正常操作，导致超过 1000 立方米的污水没有进行净化直接排放到附近的河流，造成严重的环境污染。

2003 年，美国 CSX 运输公司的计算机系统被病毒所感染，导致华盛顿所有的客运和货运全部中断。

2005 年，尽管在 Internet 和企业网、控制网之间部署了防火墙，13 家汽车厂还是被 Zorob 蠕虫病毒感染迫使停业，造成 50000 生产线工人停工，经济损失达到 140 万美元。

2008 年，波兰 Lodz 的城铁系统被恶意攻击，攻击者通过远程操纵改变铁路系统的铁轨扳道器，直接导致 4 节车厢脱离正常轨道。

2010 年，“震网”病毒（Stuxnet）攻击了伊朗的核设施，具有极强的破坏力，推迟了伊朗铀浓缩的进程，并且截止到 2010 年 9 月，全球已有十万台主计算机受到感染。

2014 年，美国的知名电子商务企业 eBay 被黑客入侵，全球 1.28 亿用户的个人信息被泄露。

2016 年，乌克兰电网遭遇黑客攻击，造成大范围停电，以及伊斯兰教的大赦之夜（Lailat al Qadr），包括 GACA（沙特国家民航总局）在内的至少 6 家沙特重要机构遭到了严重的网络攻击，更是让全球目光再次聚焦在工控网络信息安全问题上。

工控系统网络安全与IT系统网络安全有很大区别。网络安全有三个目标，也称安全三元组，即保密性（confidentiality），完整性（integrity）和可用性（availability）。保密性是指未经授权的个人，实体或进程，不能利用和获取信息。完整性确保防止不合适的修改或破坏信息。可用性是授权的用户可以按需求，及时、可靠地访问和使用信息的特征。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。工控系统网络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，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。工业网络安全是一个动态的过程，需要在整个工业控制系统生命周期的各个阶段持续实施，不断改进。

二、 研究内容与结构

随着 IT/OT 一体化的逐步推进，工业控制系统越来越多地与企业网和互联网相连接，形成了一个开放式的网络环境。工控系统网络化发展导致了系统安全风险和入侵威胁不断增加，面临的网络安全问题也更加突出。由于工控网络系统环境的特殊性，传统的 IT 信息安全技术不能直接应用于工业控制网络的安全防护。然而，工业控制系统又应用于国家的电力、交通、石油、取暖、制药等多种大型制造行业，一旦遭受攻击会带来巨大的损失，因此需要有效的方法确保工控系统的网络安全。

为给政府部门、科研机构和工业企业提供参考和借鉴，360 安全集团撰写和发布 IT/OT 一体化的工业网络安全态势报告。

本报告共分为五大章节：第一章为概述，主要讲解该报告的研究背景和意义，以及与传统 IT 网络安全的区别；第二章主要对工业信息的安全性进行了分析，统计了工控的漏洞，以及面临的挑战；第三章主要是对 2017 年的重要工控安全事件进行概述，并列举了八大重要安全事件，总结安全事件中存在的安全隐患；第四章主要对行业内信息安全标准和政策动向进行了分析，总结了国内外行业动态及发展趋势；第五章对工业网络安全提出改进建议，首先总结分析了工业网络安全中存在的问题，同时提出建议及展望，

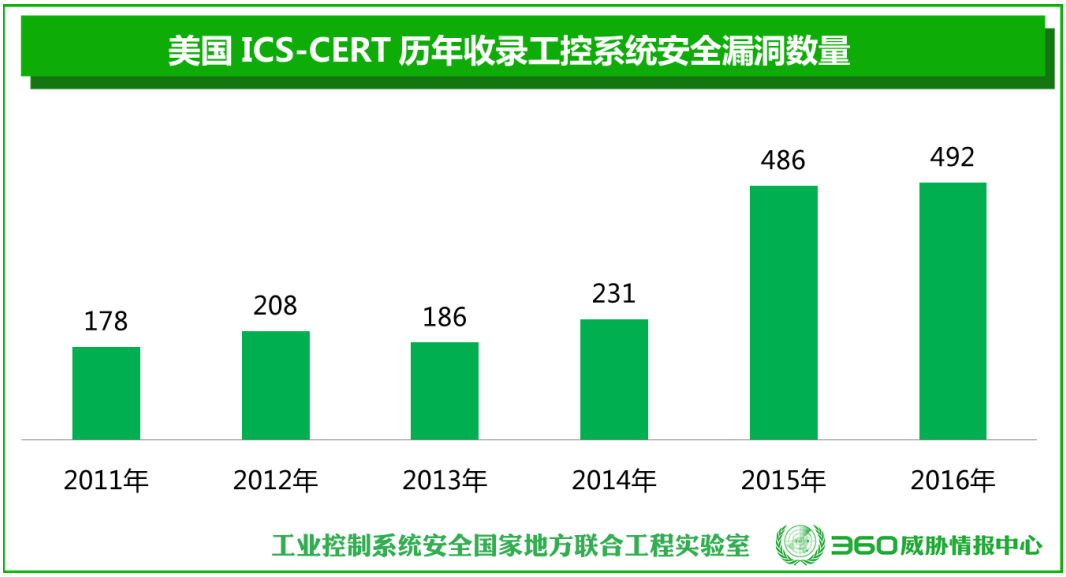
本报告可供合作伙伴及企业客户决策参考使用。

第二章　工业信息安全性现状分析

一、　工业控制系统漏洞现状

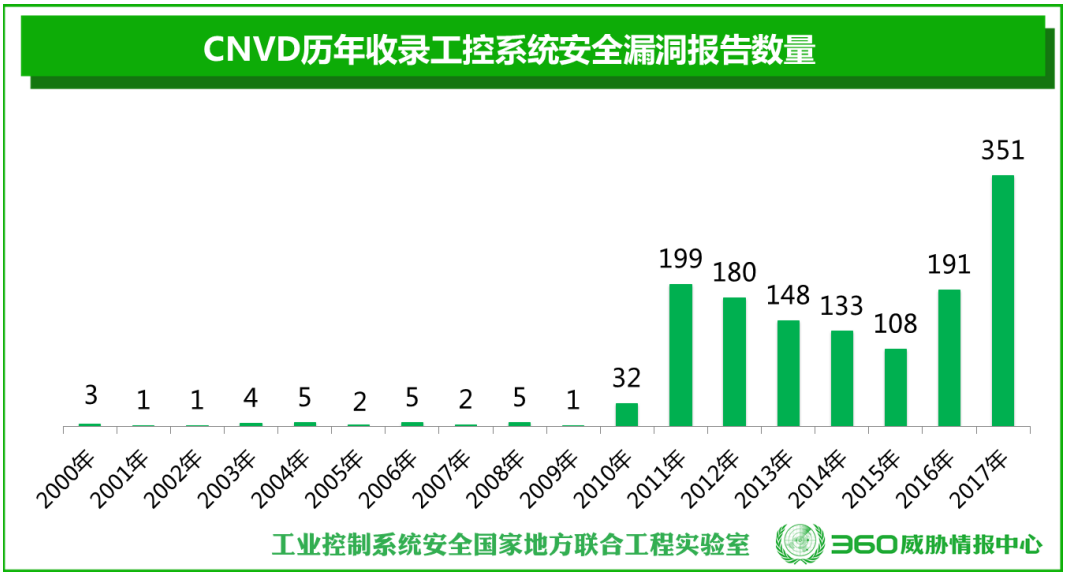
安全漏洞，是工业控制系统面临的首要安全问题。目前，全球最有名的工业控制系统漏洞收录机构是美国工业控制系统网络紧急响应小组（ICS-CERT），而国内最有名的官方漏洞收录机构是国家信息安全漏洞共享平台（CNVD），本小节将主要结合这两个机构的相关统计数据，分析工业控制系统安全漏洞近年来的报告与收录基本情况。

根据美国工业控制系统网络紧急响应小组（ICS-CERT）最新统计报告，2015 年漏洞总数为 486 个，2016 年美国关键基础设施存在 492 个安全漏洞。根据公开的 ICS 漏洞数的年度变化趋势来看，工控安全漏洞逐年增加，尽管目前 ICS-CERT 2017 年的工控漏洞收录数据还未公开，但很有可能再创新高。ICS-CERT 工控漏洞收录年度分布图如下所示。

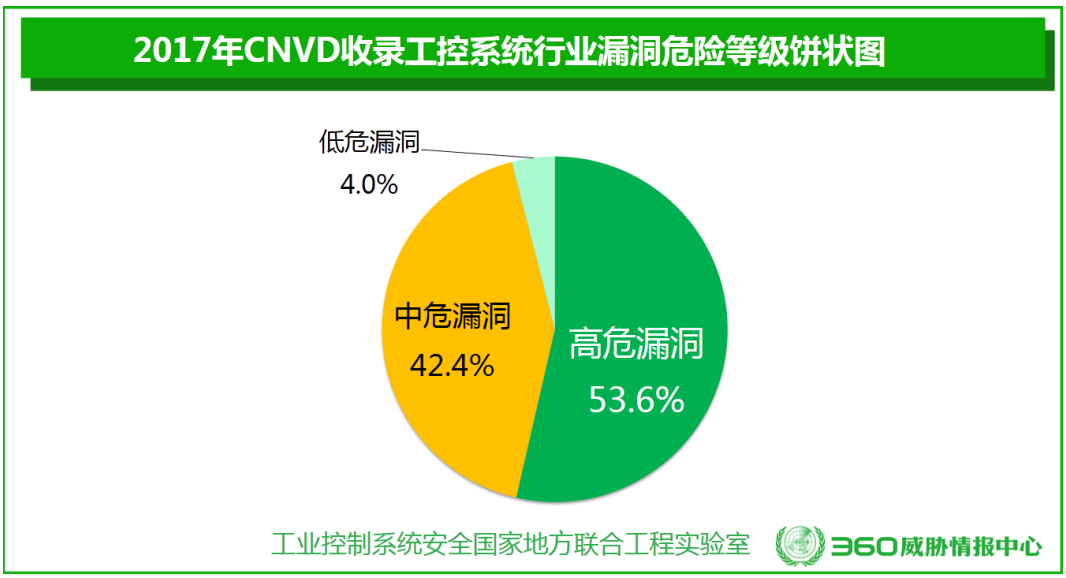


ICS-CERT 的最新报告显示，相关漏洞涉及供水、能源和石油行业等关键基础设施。此外，ICS-CERT 安全研究专家指出，针对工业控制系统环境入侵的攻击者数量增长无疑意味着可利用的漏洞数量和类型也会同时增长。工业控制系统的信息安全问题仍然需要亟待解决。

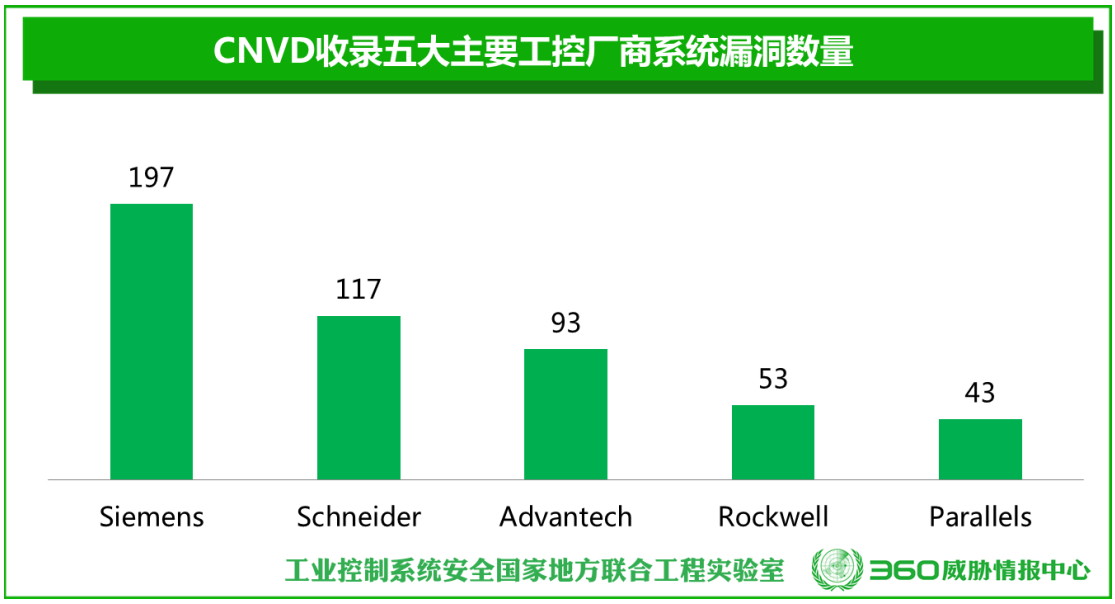
自 2000 年 1 月截止到 2017 年 12 月，根据我国国家信息安全漏洞共享平台（CNVD）统计，所有的信息安全漏洞总数为 101734 个，其中工业控制系统漏洞总数为 1437 个。2017 年 CNVD 统计的新增信息安全漏洞 4798 个，工控系统新增漏洞数 351 个，均比去年同期有显著增长。本章主要分析工业网络安全，对工业控制系统漏洞进行了详细分析，如下图所示。



CNVD 在 2017 年收录的工控相关漏洞中，高危漏洞占比最高，达到 53.6%。中危漏洞占比 42.4%，其余 4.0%为低危漏洞。2017 年 CNVD 收录工控系统漏洞危险等级分布如下图。

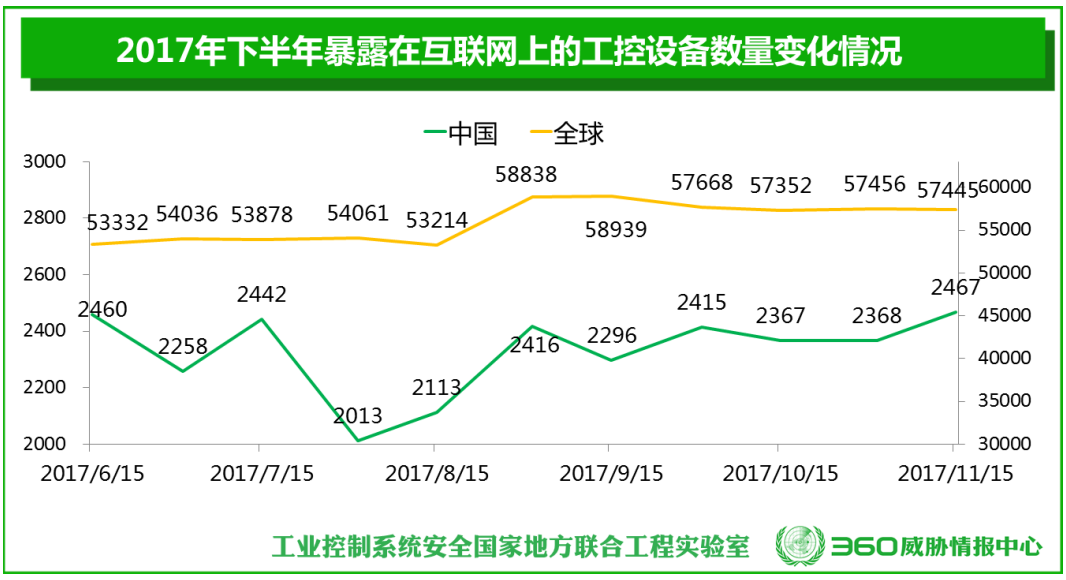


下图给出了目前 CNVD 已收录的漏洞数量最多的五大工控厂商的安全漏洞数量。其中，Siemens 最多，为 197 个，其次是 Schneider117 个。需要说明的是，收录的漏洞越多，不等于相关厂商的设备越不安全，因为往往是使用越广泛的系统，越受安全工作者的关注，所以被发现和披露的漏洞往往也越多。



二、 工控系统暴露情况

工业互联网安全监测公共服务平台收录了 2017 下半年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。从表中分析可知，在八月份和九月中旬期间，国内和全球暴露的工控设备数均有一个明显上升趋势，且 2017 年末比 2017 年中旬暴露的工控设备数多。暴露的工控设备数量折线图如下所示。



三、 工业信息安全风险分析

工业控制系统安全是国家关键信息基础设施安全的重要组成部分。在工业互联网、“中国制造 2025”、“工业 4.0”等趋势驱动下，随着云计算、物联网、大数据技术的成熟，IT/OT 一体化已成为必然趋势。

IT/OT 一体化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，随着安全事件的频繁发生，工业信息安全越来越受到政府、工业用户、科研机构和工控系统厂商的重视。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，普遍引入生产执行系统 MES，实现管理信息网络与控制网络之间的数据交换和工业控制系统和管理信息系统的集成。MES 不再是一个独立运行的系统，而要与管理系统甚至互联网互通、互联，从而引入网络攻击风险。

对于传统 IT 网络安全，保密性优先级最高，其次是完整性、可用性。工业网络则有明显的不同，工业网络更为关注的是系统设备的可用性、实时性， 除此特点外，IT 系统和 OT 系统之间仍然存在很多差异性，如表 1 所示。

表 1 IT 系统和 OT 系统的差异性

分类	IT 系统	OT 系统
可用性需求	可重启、热切换	高可用（不能重启）、计划性中断、重要系统冗余
管理需求	保密性、完整性、有效性、隐私	人身安全、有效性、完整性、保密性、隐私
体系安全焦点	IT 资产及信息、中央服务器更重要	边缘设备与中央设备一样重要
未预期的后果	安全解决方案围绕典型的 IT 系统进行设计	安全工具必须先测试以确保不会影响 ICS 的正常运作
时间紧迫的交互	交互时效可有弹性 可实施严格限制的访问控制	实时性、紧急响应 访问控制不能妨碍必要人机交互
系统操作	典型的操作系统、自动部署、持续升级	专有的操作系统，无安全功能、软件变更须验证
资源限制	近 3-5 年主流硬件，有性能冗余	按需设计，可能 10-20 年前设备还可以使用
通信	标准通信协议、有线、无线	专有标准、异构、交互操作

由于 IT 系统和 OT 系统之间存在的众多差异，当工业互联网的 IT/OT 进行融合时会带来很多安全挑战。

首先是来自外部的安全挑战，

1） 暴露在外的攻击面越来越大

IT/OT 一体化后端点增加，给工业控制系统（ICS）、数据采集与监视控制系统（SCADA）等工业设施带来了更大的攻击面。与传统 IT 系统相比较，II/OT 一体化的安全问题往往把安全威胁从虚拟世界带到现实世界，可能会对人的生命安全和社会的安全稳定造成重大影响。

2） 操作系统安全漏洞难以修补

工业控制系统操作站普遍采用 PC+Windows 的技术架构，任何一个版本的 Windows 自发布以来都在不停的发布漏洞补丁，为保证过程控制系统的可靠性，现场工程师通常在系统开发后不会对 Windows 平台打任何补丁，更为重要的是即使打过补丁的操作系统也很少再经过工控系统原厂或自动化集成商商测试，存在可靠性风险。但是与之相矛盾的是，系统不打补丁就会存在被攻击的漏洞，即使是普通常见病毒也会遭受感染，可能造成 Windows 平台乃至控制网络的瘫痪。

3） 软件漏洞容易被黑客利用

黑客入侵和工控应用软件的自身漏洞通常发生在远程工控系统的应用上，另外，对于分布式的大型的工控网，人们为了控制监视方便，常常会开放 VPN tunnel 等方式接入甚至直接开放部分端口，这种情况下也不可避免的给黑客入侵带来了方便之门。

4） 恶意代码不敢杀、不能杀

基于 Windows 平台的 PC 广泛应用，病毒也随之而泛滥。全球范围内，每年都会发生数次大规模的病毒爆发。目前全球已发现数万种病毒，并且还在以每天数十余种的速度增长。这些恶意代码具有更强的传播能力和破坏性。

例如蠕虫病毒死灰复燃。与一般的木马病毒不同，这种病毒随着第三方打补丁工具和安全软件的普及，近些年来本已几乎绝迹。但随着永恒之蓝、永恒之石等网军武器的泄露，蠕虫病毒又重新获得了生存空间，死灰复燃。其最为显性的代表就是 WannaCry 病毒。基于工控软件与杀毒软件的兼容性，在操作站（HMI）上通常不安装杀毒软件，即使是有防病毒产品，其基于病毒库查杀的机制在工控领域使用也有局限性，主要是网络的隔离性和保证系统的稳定性要求导致病毒库对新病毒的处理总是滞后的，这样，工控系统每年都会大规模地爆发病毒，特别是新病毒。在操作站上，即插即用的 U 盘等存储设备滥用，更给这类病毒带来了泛滥传播的机会。

5） DDOS 攻击随时可能中断生产

拒绝服务攻击是一种危害极大的安全隐患，它可以人为操纵也可以由病毒自动执行，常见的流量型攻击如 Ping Flooding、UDP Flooding 等，以及常见的连接型攻击如 SYN Flooding、ACK Flooding 等，通过消耗系统的资源，如网络带宽、连接数、CPU 处理能力、缓冲内存等使得正常的服务功能无法进行。拒绝服务攻击非常难以防范，原因是它的攻击对象非常普遍，从服务器到各种网络设备如路由器、防火墙、IT 防火墙等都可以被拒绝服务攻击。控制网络一旦遭受严重的拒绝服务攻击就会导致严重后果，轻则控制系统的通信完全中断，重则可导致控制器死机等。目前这种现象已经在多家工控系统中已经出现

网络风暴经常是由于 ARP 欺骗引起的 flood 攻击，或者因工控信息网络因环路故障造成的网络风暴，这种攻击往往发生在同一网段的控制区域中，占用大量的带宽资源，工控系统疲于处理各种报文，将系统资源消耗殆尽，使工业系统报文无法正常传输。目前的工业总线设备终端对此类拒绝服务攻击和网络风暴基本没有防范能力，另外，传统的安全技术对这样的攻击也几乎不可避免，缺乏有效的手段来解决，往往造成严重后果。

6） 高级持续性威胁时刻环伺

高级持续性威胁的特点是：目的性非常强，攻击目标明确，持续时间长，不达目的不罢休，攻击方法经过巧妙地构造，攻击者往往会利用社会工程学的方法或利用技术手段对被动式防御进行躲避。而传统的安全技术手段大多是利用已知攻击的特征对行为数据进行简单的

模式匹配，只关注单次行为的识别和判断，并没有对长期的攻击行为链进行有效分析。因此对于高级持续性威胁，无论是在安全威胁的检测、发现还是响应、溯源等方面都存在严重不足。

另一方面是来自工业系统自身安全建设的不足。

1） 工业设备资产的可视性严重不足

工业设备可视性不足严重阻碍了安全策略的实施。要在工业互联网安全的战斗中取胜，“知己”是重要前提。许多工业协议、设备、系统在设计之初并没有考虑到在复杂网络环境中的安全性，而且这些系统的生命周期长、升级维护少也是巨大的安全隐患。

2） 很多工控设备缺乏安全设计

主要来自各类机床数控系统、PLC、运动控制器等所使用的控制协议、控制平台、控制软件等方面，其在设计之初可能未考虑完整性、身份校验等安全需求，存在输入验证，许可、授权与访问控制不严格，不当身份验证，配置维护不足，凭证管理不严，加密算法过时等安全挑战。例如：国产数控系统所采用的操作系统可能是基于某一版本 Linux 进行裁剪的，所使用的内核、文件系统、对外提供服务、一旦稳定均不再修改，可能持续使用多年，有的甚至超过十年，而这些内核、文件系统、服务多年所爆出的漏洞并未得到更新，安全隐患长期保留。

3） 设备联网机制缺乏安全保障

工业控制系统中越来也读的设备与网络相连。如各类数控系统、PLC、应用服务器通过有线网络或无线网络连接，形成工业网络；工业网络与办公网络连接形成企业内部网络；企业内部网络与外面的云平台连接、第三方供应链连接、客户的网络连接。由此产生的主要安全挑战包括：网络数据传递过程的常见网络威胁（如：拒绝服务、中间人攻击等），网络传输链路上的硬件和软件安全（如：软件漏洞、配置不合理等），无线网络技术使用带来的网络防护边界模糊等。

4） IT 和 OT 系统安全管理相互独立互操作困难

随着智能制造的网络化和数字化发展，工业与 IT 的高度融合，企业内部人员，如：工程师、管理人员、现场操作员、企业高层管理人员等，其“有意识”或“无意识”的行为，可能破坏工业系统、传播恶意软件、忽略工作异常等，因为网络的广泛使用，这些挑战的影响将会急剧放大；而针对人的社会工程学、钓鱼攻击、邮件扫描攻击等大量攻击都利用了员工无意泄露的敏感信息。因此，在智能制造+互联网中，人员管理也面临巨大的安全挑战。

5） 生产数据面临丢失、泄露、篡改等安全威胁

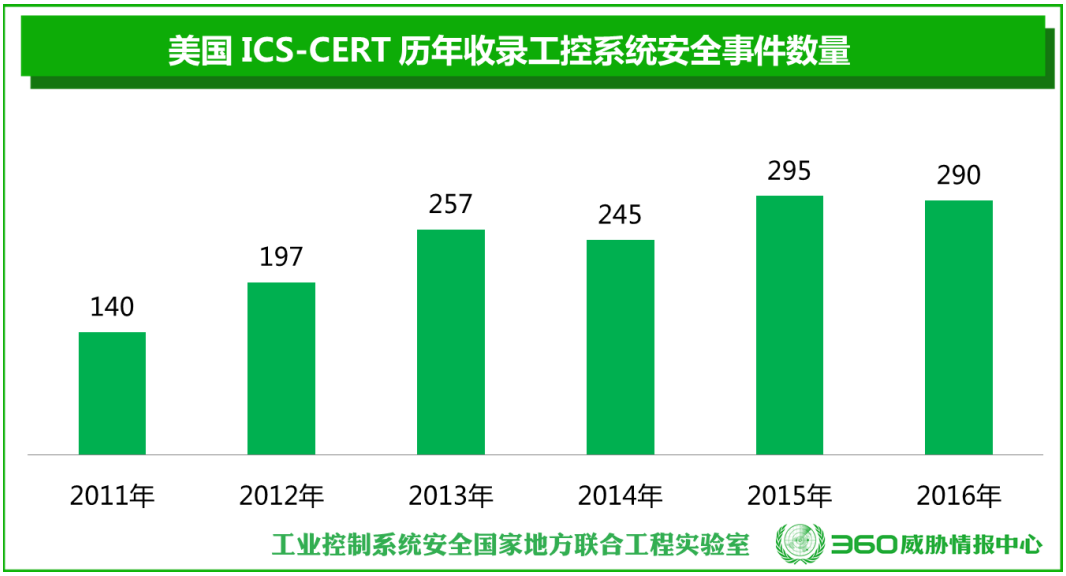
智能制造工厂内部生产管理数据、生产操作数据以及工厂外部数据等各类数据的安全问题，不管数据是通过大数据平台存储、还是分布在用户、生产终端、设计服务器等多种设备上，海量数据都将面临数据丢失、泄露、篡改等安全威胁。

第三章　2017 工业信息安全重大事件

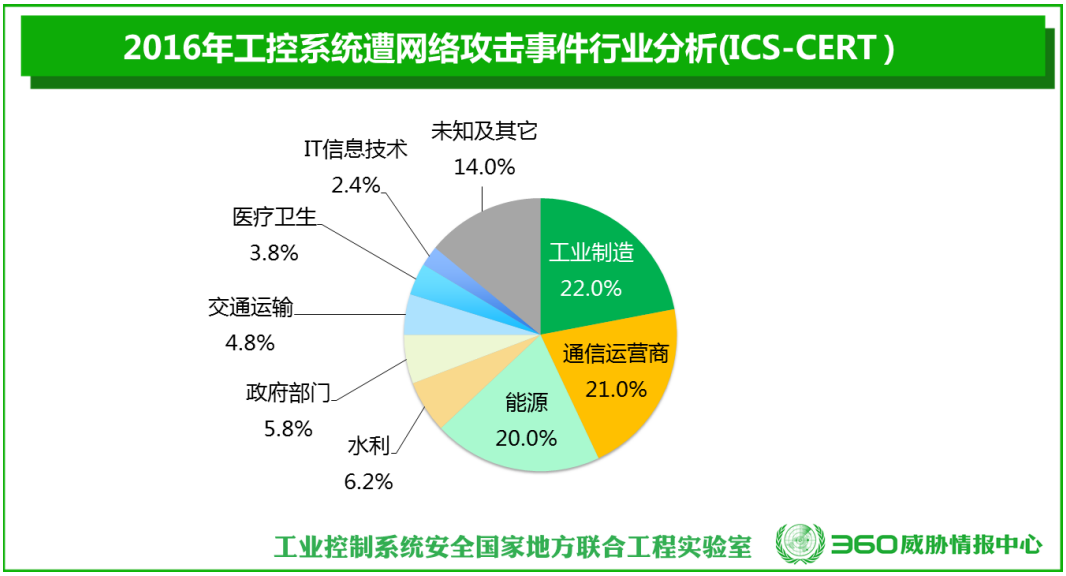
2017 年，针对工业控制系统的各种网络攻击事件日益增多，暴露出工业控制系统在安全防护方面的严重不足。本章汇总了国内外工控领域工业网络安全事件，希望能帮助读者进一步了解工业控制系统所面临的安全威胁，促进加大在工业控制网络安全方面的投入，加速推进相关技术和解决方案的完善以及相关政策标准的推出，促进工控网络安全事业不断发展。

一、　2017 安全事件概述

根据 ICS-CERT 的报告显示，在 2016 年，工业控制系统网络安全应急小组团队完成了对 290 起安全事件的处理，由于 IT/OT 的一体化，传统病毒和工控病毒的相互渗透以及 IT 技术和 OT 技术的融合，可利用的漏洞数量和类型同时增长，近几年的安全事件也会增多，工业控制系统安全事件如下所示。



在 2016 年发生的 290 起工控安全事件中，对制造业的攻击比重最大，有 63 起，约占 22%，此外，通信部门攻击有 62 起，比重第二，有 59 起能源部门安全事件，工业控制系统安全事件攻击类型如下所示。



随着我国工业互联网的发展，IT/OT 一体化进程的不断推进，工业控制系统不再是孤立的系统，单纯地进行网络隔离已经不能有效控制工业控制系统的安全，不断发生的工业控制系统信息安全事件充分说明了这点。此外，分析了安全事件攻击类型，希望本文对于致力于工业控制系统安全防护的同行有所借鉴和帮助。

二、 2017 工业网络八大重点安全事件

（一） 永恒之蓝（WannaCry）勒索病毒分析

5 月 12 日，不法分子利用据称是 NSA（National Security Agency，美国国家安全局）泄露的黑客数字武器库中“永恒之蓝”工具发起蠕虫病毒攻击进行勒索的恶性事件。WannaCry 利用 Windows 操作系统 445 端口存在的漏洞进行传播，无需用户任何操作，只要开机上网，不法分子就能在电脑和服务器中植入恶意代码加密用户数据实施数字勒索，并具有自我复制、主动传播的特性。仅仅几个小时，该勒索软件已经攻击了近百个国家，中国、英国、美国、德国、日本、土耳其、西班牙、意大利、葡萄牙、俄罗斯和乌克兰等国家的上千家企业及公共组织，超过 10 万台电脑遭到了勒索病毒攻击、感染。

工业企业也受到勒索病毒的感染而影响正常生产。根据公开报道，尼桑和本田均遭受停产。中国某大型能源企业的部分加油站正常运行受到波及。病毒导致加油站加油卡、银行卡、第三方支付等网络支付功能无法使用。Wannacry病毒严重影响英国NHS系统，NHS辖下48个医疗机构在此次网络攻击中受影响，占所有NHS机构的五分之一。医院的急症服务、手术服务等等都必须延迟甚至取消，受影响的病人数以千计。因此，相关部门需要加强对加强工控环境保护，提前做好对勒索软件的防护。

（二） 我国发现新型物联网僵尸网络 HTTP81

在去年Mirai僵尸网络攻击造成美国东海岸大面积断网事件之后，2017年5月，国内也出现了控制大量IoT设备的僵尸网络。该僵尸网络是由360网络安全研究院率先发布公告，披露了一个名为http81的新型IoT僵尸网络。

http81僵尸网络的幕后操控者远程入侵了大量没有及时修复漏洞的网络摄像头设备，在这些摄像头中植入恶意代码，只要发出指令就可以随时向任何目标实施DDoS攻击。由于网

络摄像头属于长期在线的设备，普遍拥有比较高的带宽，与由电脑组成的僵尸网络相比，具备更强的杀伤力。此外，http81僵尸网络借鉴了Mirai的端口嗅探手法和部分基础代码，但是对比僵尸网络的关键特性，http81在传播、C2通信协议、攻击向量等方面与Mirai完全不同，属于新的僵尸网络家族。

http81僵尸网络在中国已经感染控制了超过5万台网络摄像头。如果按照每个活跃IP拥有10Mbps上行带宽测算，http81僵尸网络可能拥有高达500Gbps的DDoS攻击能力，足以对国内互联网基础设施产生重大威胁。此安全事件告诫我们：国内的网络摄像头等设备大多缺乏安全更新维护，从事物联网行业的运维人员应该尽可能更新维护，及时清除恶意代码。

（三） 类 Petya 勒索病毒席卷欧洲

6 月 27 日，乌克兰、俄罗斯、印度、西班牙、法国、英国以及欧洲多国遭受大规模“类 Petya”勒索病毒袭击，该病毒远程锁定设备，然后索要赎金。其中，乌克兰地区受灾最为严重，政府、银行、电力系统、通讯系统、企业以及机场都不同程度的受到了影响，包括首都基辅的鲍里斯波尔国际机场（Boryspil International Airport）、乌克兰国家储蓄银行（Oschadbank）、船舶公司（AP Moller-Maersk）、俄罗斯石油公司（Rosneft）和乌克兰一些商业银行以及部分私人公司、零售企业和政府系统都遭到了攻击。

类 Petya 病毒是 2017 年全球流行并造成严重破坏的一类勒索软件。具体包括 Petya 病毒，NotPetya 病毒和 BadRabbit 病毒（坏兔子）三种。从纯粹的技术角度看，类 Petya 病毒的三个子类并不属于同一木马家族，但由于其攻击行为具有很多相似之处，因此有很多安全工作者将其归并为一类勒索软件，即类 Petya 病毒。Petya 病毒主要通过诱导用户下载的方式进行传播。病毒会修改中招机器的 MBR（主引导记录，Master Boot Record）并重启设备。重启后，被感染电脑中 MBR 区的恶意代码会删除磁盘文件索引（相当于删除所有文件），导致系统崩溃和文件丢失。

与 5 月爆发的勒索病毒相比，新病毒变种的攻击速度更快。它会利用“管理员共享”功能在内网自动化渗透，即使打全补丁的电脑也会被攻击。

（四） 美国供水设施网络瘫痪

6月中下旬，美国宾夕法尼亚Bala Cynwyd的亚当弗拉纳根（42岁）因破坏美国东海岸多个供水设施提供商的网络被判1年零1天的监禁。

2013年11月，该公司以非公开理由解雇了弗拉纳根。弗拉纳根于2007年11月至2013年11月在某智能水电气设备制造商担任工程师，他的工作职责之一是为客户（主要为供水设施网络）建立塔式网关基站（TGB）。

被解雇后的弗拉纳根此后决定报复公司，从而关闭了TGB，使该公司客户的供水设施网络陷入瘫痪，之后他用攻击性的语言修改了某些TGB上的密码。TGB是供水设施网络（由安装在民众家中与供水设施运营商系统交换数据的智能水表）的主要组成部分。这些网络允许供水设施运营商收集用水数据，并检查客户家中的安装情况。此安全事件导致美国东海岸5个城市的塔式网关基站受到影响，供水设施提供商不得不派遣员工到客户家中手工抄写每月的用水量。在2016年11月，美国当局对弗拉纳根提出指控，于2017年6月弗拉纳根被判刑。此安全事件告诫我们：对于企业内员工的管理，不仅要加强安全策略管理，还需要定期进行安全培训教育。

（五） 印度 ISP 遭受 BrickerBot 攻击

8月3日，印度多地发生网络攻击事件，影响了Bharat Sanchar Nigam Limited（BSNL）和Mahanagar Telephone Nigam Limited（MTNL）这两家印度国有电信服务提供商的机房内的调制调解器以及用户的路由器，事件导致印度东北部、北部和南部地区调制调解器丢失网络连接，预计6万台调制调解器掉线，影响了45%的宽带连接。

BrickerBot是一款影响Linux物联网和联网设备的恶意软件。与其它囤积设备组成僵尸网络实施DDoS攻击等恶意软件不同的是，BrickerBot重写Flash存储，使物联网设备变“砖”。大多数情况下，“砖化”效应可以逆转，但在某些情况下却会造成永久性的破坏。BSNL几万台调制调解器使用了不受保护的TR069（TR064）接口，允许任何人重新配置设备实施中间人攻击或DNS劫持。BSNL和MTNL遭遇这起网络攻击的原因，还在于这两大ISP允许他人通过7547端口连接到它们的网络。此安全事件告诫我们：应加强使用非安全设备ISP的注意，此外，设备所有者和互联网服务器提供商也需要谨慎保护设备安全。

（六） 瑞典交通机构遭受 DDOS 攻击

10月11日，黑客针对瑞典运输管理局（ Trafikverket ）展开 DDoS 攻击，导致该机构负责管理列车订单的 IT 系统瘫痪，以及电子邮件系统与网站宕机，从而影响了旅客预定或修改订单的情况。10月12日，瑞典交通运输局（Transportstyrelsen），以及公共交通运营商 Västtrafik 的 IT 系统遭到类似 DDoS 攻击。黑客发动的 DDoS 攻击主要针对服务提供商 TDC 和 DGC，其目的是影响机构的正常运营。

（七） 巴西银行发现恶意软件攻击

12月17日，趋势科技的安全研究人员于近期发现了一种名为PRILEX的ATM恶意软件，旨在瞄准巴西银行进行针对性攻击、窃取ATM用户的信息。10月份，卡巴斯基实验室发现了第一起PRILEX攻击，PRILEX 具有非典型的行为，因为 PRILEX 只会影响特定品牌的自动取款机，这种非典型行为表明恶意软件是为高度针对性的攻击而设计的。被发现的ATM恶意软件通过挂钩某些动态链接库（DLL）来工作，并将其替换为自己的应用程序屏幕。一旦感染ATM，PRILEX恶意软件就会kill掉银行应用进程、显示特定的虚假屏幕诱导用户提供帐户验证码。

从去年10月份，巴西银行36个银行域名、企业电子邮件和DNS都被黑客控制，攻击者利用伪造的HTTPS页面网络钓鱼获取用户凭证和访问行为，还向访问者分发恶意软件。此安全事件告诫我们：企业应加强HTTPS的配置，同时加强对DNS的控制和监督，尽量使用双因子身份验证。

（八） 恶意软件 TRITON 攻击能源关键信息基础设施

12月，黑客利用恶意软件Triton攻击了施耐德电气公司Triconex安全仪表系统（Triconex Safety Instrumented System，SIS），该系统广泛应用于能源行业，包括石油天然气和核设施的功能安全保护。该系统失效有可能造成极为严重的后果。美国国土安全部（DHS）的国家网络安全和通信集成中心（NCCIC）也对此攻击事件进行了调查分析。

调查显示，基于Python编写的HatMan恶意软件主要以施耐德电气的Triconex安全仪表系统（SIS）控制器为目标，旨在关停系统并尝试修改系统到危险失效状态。HatMan通过专有的TriStation协议与SIS控制器进行通信，允许攻击者通多添加新的梯形图修改SIS安全逻辑。NCCIC在其报告中指出，该恶意软件主要包括两部分组件：一部分是在受损的PC端运行后与安全控制器交互，另一块是在控制器上直接运行。这是第一起针对能源基础设施功能安全保护系统发起的攻击事件。此安全事件告诫我们：攻击者已不满足于攻击常规工控系统（DCS、

PLC等），造成停车或停产，而是开始攻击工业领域最核心的安全保护系统，尝试造成爆炸、有害物质泄漏等更严重的危害。

第四章　工业信息系统应急响应典型案例

在本章中，为叙述方便，“工业控制系统安全国家地方联合工程实验室”均简称为：“工控安全联合实验室”。

一、　工业系统遭勒索软件攻击典型案例

（一）　某大型能源机构遭 WannaCry 大规模攻击

场景回顾

2017 年 5 月 12 日 14:26，360 互联网安全中心发现安全态势异常，启动黄色应急响应程序，安全卫士在其官方微博上发布永恒之蓝紧急预警。5 月 13 日凌晨 1:23’，360 安全监测与响应中心接到某大型能源企业的求助，反映其内部生产设备发现大规模病毒感染迹象，部分生产系统已被迫停产。360 安全监测与响应中心的安全服务人员在接到求助信息后，立即赶往该单位总部了解实际感染情况。

疫情分析

初步诊断认为：WannaCry 病毒已在该机构全国范围内的生产系统中大面积传播和感染，短时间内病毒已在全国各地内迅速扩散，但仍处于病毒传播初期；其办公网环境、各地业务终端（专网环境）都未能幸免，系统面临崩溃，业务无法开展，事态非常严重。

进一步研究发现，该机构大规模感染 WannaCry 的原因与该机构业务系统架构存在一定的关联；用户系统虽然处于隔离网，但是存在隔离不彻底的问题；且存在某些设备、系统的协同机制通过 445 端口来完成的情况。

处置方案

安服人员第一时间建议全网断开 445 端口，迅速对中招电脑与全网机器进行隔离，形成初步处置措施。随后，针对该企业实际情况，制定了应急处置措施，提供企业级免疫工具并开始布防。该企业在全国范围内针对该病毒发送紧急通知，发布内部应急处理和避免感染病毒的终端扩大传播的公告。

5 月 16 日，病毒蔓延得到有效控制，染毒终端数量未继续增长，基本完成控制及防御工作。整个过程中，该企业和安全厂商全力协作配合，监控现场染毒情况、病毒查杀情况，最终使病毒得到有效控制。

（二）　某市视频监控系统服务器遭勒索软件锁定

场景回顾

5 月 13 日凌晨 3:00 许，360 安全监测与响应中心接到某单位（市级）电话求助，称其在全市范围内的的视频监控系统突然中断了服务，大量监控设备断开，系统基本瘫痪。安服人员第一时间进行了远程协助，初步判断：猜测可能是监控系统的服务器遭到攻击感染了勒索病毒，进而感染了终端电脑，建议立即逐台关闭 Server 服务，并运行免疫工具，同时提取病毒样本进行分析。

疫情分析

安服人员现场实地勘察后发现：确实是该视频监控系统的服务器中招了，罪魁祸首正是WannaCry，并且由于服务器中招已经使部分办公终端中招。溯源分析显示，“永恒之蓝”先在一台视频网络服务器上发作，然后迅速扩散，导致该市局视频专网终端及部分服务器（大约 20 多台）设备被病毒感染，数据均被加密，导致大量监控摄像头断开连接。断网将对当地的生产生活产生重要影响。

处置方案

安服人员首先在交换机上配置 445 端口阻塞策略；其次，分发勒索病毒免疫工具，在未被感染的终端和服务器上运行，防止病毒进一步扩散；另外，对于在线终端，第一时间推送病毒库更新和漏洞补丁库；由于部分被加密的服务器在被感染之前对重要数据已经做了备份，因此对这些服务器进行系统还原，并及时采取封端口、打补丁等措施，避免再次感染。

至 5 月 16 日，该机构的视频监控系统已经完全恢复正常运行，13 日凌晨被感染的终端及服务器以外，没有出现新的被感染主机。

（三） 某新能源汽车厂商的工业控制系统被 WannaCry 攻击而停产

场景回顾

2017 年 6 月 9 日，某新能源汽车制造商的工业控制系统开始出现异常。当日晚上 19 时，该机构生产流水线的一个核心部分：动力电池生产系统瘫痪。该生产系统日产值超百万，停产直接损失严重，同时也就意味着其电动车的电力电机模组部分出不了货，对该企业的生产产生了极其重大的影响。该机构紧急向 360 安全监测与响应中心进行了求助。

实际上，这是永恒之蓝勒索蠕虫的二次突袭，而该企业的整个生产系统已经幸运的躲过了 5 月份的第一轮攻击，却没有躲过第二次。监测显示，这种第二轮攻击才被感染情况大量存在，并不是偶然的。

疫情分析

安服人员现场实际勘测发现：该机构的工业控制系统已经被 WannaCry 感染，运行异常，重复重启或蓝屏，而其办公终端系统基本无恙，这是因其办公终端系统上安装了比较完善的企业级终端安全软件。但在该企业的工业控制系统上，尚未部署任何安全措施。感染原因主要是由于其系统与企业办公网络连通，间接存在公开暴露在互联网上的接口。后经综合检测分析显示，该企业生产系统中感染 WannaCry 的工业主机数量竟然占到了整个生产系统工业终端数量的 20%。

事实上，该企业此前早已制定了工业控制系统的安全升级计划，但由于其生产线上的设备环境复杂，操作系统五花八门（WinCE 终端、Win2000、WinXP 终端及其他各种各样的终端都会碰到），硬件设备也新老不齐（事后测试发现，其流水线上最老的电脑设备有 10 年以上历史），所以部署安全措施将面临巨大的兼容性考验，所以整个工控系统的安全措施迟迟没有部署。

处置方案

因厂商的生产系统中没有企业级终端安全软件，于是只能逐一对其电脑进行排查。一天之后也仅仅是把动力电池的生产系统救活。此后，从 6 月 9 日开始一直到 7 月底差不多用了两个月时间，该企业生产网里中的带毒终端才被全部清理干净。经过此次事件，该机构对工

业控制系统安全性更加重视，目前已经部署了工控安全防护措施。经过测试和验证，兼容性问题也最终得到了很好的解决。

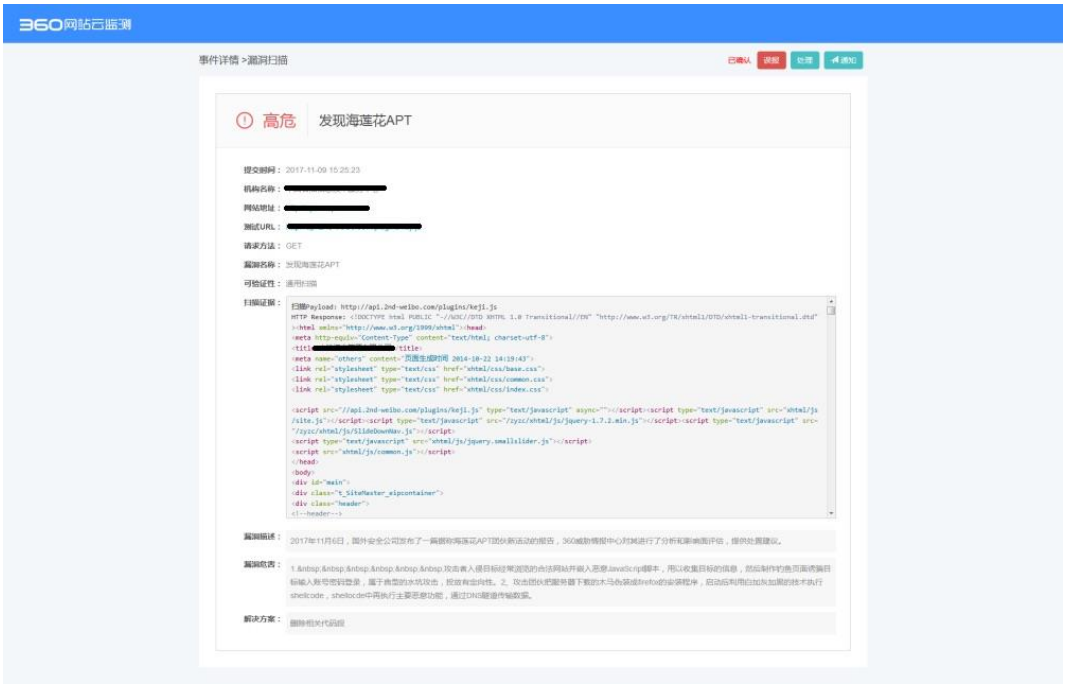
二、 工业系统服务器遭攻击典型案例

（一） 某大型能源公司网站遭遇 APT 入侵

海莲花（OceanLotus）是首个由国内安全机构（360 威胁情报中心，2015 年 5 月）披露的 APT 组织。2012 年 4 月起至今，该境外黑客组织对中国政府、科研院所、海事机构、海域建设、航运企业等相关重要领域展开了有组织、有计划、有针对性的长时间不间断攻击。该组织主要通过鱼叉攻击和水坑攻击等方法，配合多种社会工程学手段进行渗透，向境内特定目标人群传播专用木马程序，秘密控制部分政府人员、外包商和行业专家的电脑系统，窃取系统中相关领域的机密资料。

场景回顾

2017 年 11 月，云监测发现，某大型能源公司网站被海莲花 APT 组织攻陷。我们认为网站是整个组织暴露在外的非常关键的入口，这是 360 云监测第一次发现 APT 与网站入侵直接相关的国内案例。



疫情分析

该大型能源公司被海莲花 APT 组织攻陷，云监测发现其采取的是“水坑攻击”方式，并且目前网站首页上存在海莲花 APT 水坑域名相关的 js。攻击者团伙入侵网站后，不仅破坏网站的安全性，还会收集所访问用户的系统信息。如果确认感兴趣的目标，则会执行进一步的钓鱼攻击获取敏感账号信息或尝试植入恶意程序进行秘密控制。

处置方案

1） 建议该企业及时清理被篡改的相关页面。

2） 该企业与 360 合作，展开全面调查。

（二） 某地全市监控系统可泄露敏感信息

场景回顾

某市监控系统邀请工控安全联合实验室对分布于全市的监控设备及其服务系统进行安全检测。检测结果显示，该市很多区域的监控视频均可通过互联网进行查看，其中包括很多敏感区域的监控视频，如：政府、医院、私人办公区、危险化学品仓储等。这些监控视频一旦被犯罪分子掌握和利用，后果不堪设想。

某矿井内部监控可发现用于爆破的危险物品（上面图像经过处理）

某医院监控能清楚的了解该医院的实时情况（上面图像经过处理）

某办公区域监控系统（上面图像经过处理）

疫情分析

造成该市多个区域监控视频外泄风险的主要原因有两点：一是监控视频的管理服务器直接暴露在了互联网上，可被远程访问。二是监控视频服务器的管理员帐号使用了弱密码，弱密码为该视频监控系统服务商设置的初始密码。

处置方案

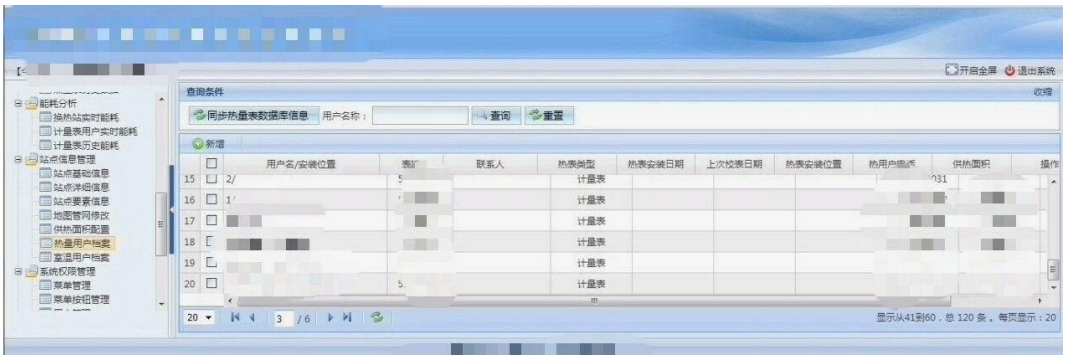
1） 修改服务器的管理员帐号和密码，不要使用弱密码。

2） 做好服务器设备隔离，阻止来自互联网的访问。

（三） 某热力公司内部服务器可无密码登录

场景回顾

某市热力公司邀请工控安全联合实验室对其系统进行安全检测。检测结果显示，该热力公司的内部服务器可以通过互联网直接访问，并无需帐号密码认证即可以管理员身份登陆，可造成大量服务器数据泄露。此外，检测还发现，该热力公司控制系统中的大量 PLC 也暴露在了互联网上，可以直接被攻击者攻击，并造成设备停产。



通过公网无需认证即可登录某热力公司内部数据系统

疫情分析

检测显示，该机构内部服务器的业务代码存在设计缺欠，导致其登录认证过程可以被绕过。同时，该服务器对于互联网没有完全隐藏隔离，因此导致攻击者可以直接从互联网访问，并以管理员权限登录。进一步调查现实，攻击者远程登录后，还可以访问系统数据库。

该热力公司的 PLC 也被暴露在网络，攻击者可以直接查看，并实施攻击。PLC 是连接办公系统和工控系统的控制设备，攻击者通过暴露在互联网上的 PLC 信息，直接对 PLC 设备发起远程攻击，可删除或篡改数据，甚至直接破坏系统造成设备停产。

处置方案

1） 立即排查所有登录权限，删除非法登陆者。

2） 修正服务器系统设计缺欠，修改并添加账号密码，避免认证绕过。

3） 尽快排查，在该企业自己可控的服务范围内，删除意外暴露的敏感数据。

4） 加强安全监控，做好数据备份，以防有攻击者恶意破坏服务器数据。

5） 全面排查内部网络中，暴露在互联网上的设备和网络节点，做好全面的网络隔离。

三、 其他典型案例

（一） 某知名汽车合资厂商工控软件带毒运行

场景回顾

2017 年 11 月，某知名汽车合资厂商邀请工控安全联合实验室对其生产系统进行安全检测。结果发现其生产系统中的监控主机上存在大量木马病毒，包括大量感染型病毒，某些木马病毒样本的历史甚至超过 10 年以上。同时，该系统的工业控制部分也存在大量已知安全漏洞。虽然上述问题暂未对该企业的生产活动产生实质性影响，但安全隐患已经非常明显。

注：所谓感染型病毒，是将自身加入在其它的程序（如 exe 文件）或动态库文件（DLL 的一种）中，从而实现随被感染程序同步运行的功能，进而对感染电脑进行破坏和自身传播的病毒。感染型病毒近年来在一般民用系统中已经非常少见，但在 21 世纪初期还很流行。

疫情分析

检测发现，导致该汽车厂商生产系统感染大量木马病毒，存在大量安全漏洞的主要原因有两个方面：一是生产系统部分设备过于老旧疏与维护，二是缺乏有效的安全运维和管理。

1） 生产系统部分设备过于老旧

该企业使用的自动化生产系统中，有大量设备已经超过原厂提供的质保期或自动化集成商的维保期，如：西门子 S7-300 PLC 等，某些设备的使用时间超过 10 年以上，系统长期处于无人进行升级维护的状态。上位机监控系统中存在大量老旧病毒并且带毒工作多年。

2） 缺乏有效的安全运维和管理

该企业安全运维手段不足和管理不严主要表现为 USB 管理疏失和网络管控不严。首先，尽管该企业明令禁止员工在工控系统的 USB 接口上进行手机充电或插拔其他无关设备，但并没有采取任何技术手段对 USB 端口的使用进行限制；其次，尽管该企业的生产系统并不需要互联网协同工作，但其部分设备的端口却暴露在了互联网上，可以从互联网自由访问。这就使得该生产系统随时处于来自互联网攻击的巨大威胁之下。

处置方案

首先需要说明的是，该汽车厂商生产系统中的木马病毒，特别是感染型病毒，已经很难完全清除干净。这是因为，一般来说，如果操作系统中的驱动程序感染了感染型病毒，修复方法通常只能用原生系统的相同文件来替换掉被感染的文件。但是，工业主机上的操作系统都不是完全原生的操作系统，其中大量的驱动程序都是经过工控设备制造商根据生产需求修改过的。而鉴于相关设备早已超出保修年限，不仅得不到设备供应商的维护保养，而且也已经很难获得所需驱动程序样本。这时如果直接用原生操作系统驱动替换被感染文件，可能立即造成相关设备失灵，进而无法再生产。

因此，工控安全联合实验室给该汽车厂商建议如下处置方案：

1） 排查内部网络，封禁生产系统暴露在互联网上的端口，网络内部做好访问控制。

2） 请专业技术人员协助清除目前工业主机上可以清除的病毒。

3） 使用终端安全管控软件等技术措施，封禁生产系统中所有主机设的备 USB 端口；在不影响生产的情况，也可以直接物理封禁所有 USB 端口。

（二） 某市自来水厂内部信息存在泄露风险

场景回顾

某市自来水供水厂邀请工控安全联合实验室，对其内部生产系统进行安全检测，并提供了某日一段时间内，该厂内部网络中的部分流量数据请我们协助做安全分析。检测分析结果显示：该系统存在大量内网 IP 地址暴露问题，可以直接通过互联网自由访问，这可能导致内网管理的机密数据和部分供水设备运行的敏感信息泄露。

疫情分析

内网 IP 与节点的暴露问题，主要是由于内部网络隔离不彻底。调查显示，该自来水厂内部网络并不存在联网需求，即并没有需要通过互联网来管控的设备节点和业务系统，因此，其内部网络与互联网之间理应进行完全隔离。而造成其内部网络节点暴露在互联网上的主要原因，应属工作人员缺乏安全意识，对系统进行了不当配置。

此外，该自来水厂对内部网络的监控和管理，缺乏有效的技术手段，仅靠自查自纠，很难完全杜绝此类问题再次发生。

处置方案

1） 立即进行网络系统排查，全面测试还有那些节点与互联网相连，并将不必要的连接节点全部与互联网断开，必要的连接节点应进行必要的技术保护。

2） 建立健全内部网络的访问控制、安全监控和数据审计系统。

3） 加强对 IT 运维人员的技术培训和安全意识培训。

第五章　工业信息安全标准与政策动向

一、　国际工控安全标准及重要文件

（一）　2017 美国工控安全标准及重要文件

2017 年 2 月，美国纽约州金融服务部（DFS）颁布了新的网络安全监管规则，这意味着在纽约运营的主要金融机构迎来了相比过去更为严厉的网络安全防控义务。从适用范围来看，这部规章适用于所有在纽约运营的具有银行、保险和金融服务牌照的企业。总体来看，这部规章涵盖的内容较为广泛，包括对网络书写政策的设置、管理、审计、侦查、防御、测试要求以及突发事件报告等多方面的网络安全事项。

首先，企业将需要设置“保持网络安全计划”。其次，规章要求企业有相关的记录和报告义务。再次，企业还须设置强调一系列网络安全事项的政策，内容包括信息安全、数据管理、登陆控制、系统以及网络监控、数据隐匿和突发事件应对等。此外，企业必须任命一名首席信息安全执行官，用以监测这些政策的实施和执行情况。

2017 年 3 月，美国众议院科学、空间与技术委员会通过了《网络安全框架》V1.1 版草案提议修改项。V1.1 草案中的提议修改项，包括：

修改网络安全度量的内容。企业领导者希望明确这里指的是自我评估，而非审计或法律标准。

在身份与访问管理中新增子节，即身份验证。包括基于风险身份验证方法的三层描述：单一、多因素和持续验证。

将网络供应链风险管理实现层级（Cyber Supply Chain Implementation Tier）融入到其它三个实现层级内容中。

删除第 3.7 节，联邦机构应用框架的部分。特朗普行政令 EO13800 已经解决了这个问题，联邦机构具有独立的框架指南。

最根本的是，整个文件的评估和内容更新是为了更好地适应物联网和工控系统网络安全。

2017 年 5 月，特朗普签署了《增强联邦政府网络与关键性基础设施网络安全》行政令，并表示，政府将开始在整个美国政府机构范围内管理网络风险，让联邦机构各自负责保护自身网络，并将实现联邦 IT 现代化作为加强计算机安全的核心。该项名为“增强联邦政府网络与关键性基础设施网络安全”的行政指令，按联邦政府、关键基础设施和国家三个领域来规定将采取的增强网络安全的措施。

1） 联邦政府网络安全

在联邦政府网络安全方面，“行政令”认为，已知但未得到处理的漏洞是行政部门所面临的最严重的网络风险之一，这些漏洞包括使用开发商不再支持的过时操作系统或硬件，未及时安装安全补丁或落实特定安全配置。

2） 关键基础设施网络安全

在关键基础设施网络安全方面，这项“行政令”要求采取一系列措施来增强联邦政府及关键基础设施的网络安全。按联邦政府、关键基础设施和国家三个领域来规定将采取的增强

网络安全的措施。

3） 国家网络安全

在国家网络安全方面，“行政令”称，美国的政策是确保互联网开放、互动、可靠和安全，在促进效率、创新、交流和经济繁荣的同时，尊重隐私并防止欺骗、偷窃和破坏。

2017 年 12 月，美国国家标准与技术研究院（National Institute of Standards and Technology ，NIST）发布《改进关键信息基础设施网络安全框架》第二稿，NIST 方面指出，第二稿草案旨在澄清、改进及加强网络安全框架，夸大其价值与易用性。NIST 网络安全框架最初发布于 2014 年，此项网络安全框架基于美国前任总统奥巴马发布的总统行政令，现任特朗普政府亦将该框架视为一套适用于政府机构以及各关键信息基础设施运营商的最佳实践指导方案。

（二） 2017 澳大利亚工控安全标准及重要文件

2017 年 5 月，澳大利亚总理特恩布尔日前宣布发布政府首次年度修订版《国家网络安全战略》。该战略于 2016 年 4 月推出，涵盖 33 个网络安全计划，投入资金达 2.31 亿澳元（约合 12 亿人民币）。修订版战略称，自《网络安全战略》推出以来，网络安全行业的利益、活力和关注度都在快速增加。澳大利亚在网络安全研发方面的专利申请排名全球第四。《网络安全战略》举措除了带来了直接效果，在业界、学术界和政府机构也提高了网络安全活动的参与率。网络安全行业正在成长为一个蓬勃发展的共同体，这将有助于保护澳大利亚经济发展，并使其自身成为一个有价值的行业。

根据修订版战略，下一步澳大利亚政府将致力于打击网络犯罪、联合业界以提高物联网设备安全性、降低政府 IT 系统的供应链风险等。

2017 年 8 月，澳大利亚维多利亚州政府正式启动新一项五年网络安全战略，旨在增强国家政府网络防御体系并确保国家信息、服务与关键基础设施安全。不过，该战略目前首要保护公民敏感信息免遭丢失、恶意更改或未经授权使用。

与此同时，由于政府希望国家服务、系统与基础设施在遭受严重网络攻击时能够迅速得以恢复，因此该战略发布后政府不仅对国家基础设施的威胁采取了全方位应对措施，还强调了公共管理部门的网络安全战略需要根据行业实践进行改进，使之保持一致并适合每个组织风险状况。另外，维多利亚州政府还希望国家能够将安全与维护功能纳入公民新数字服务项目，旨在提高政府核心基础设施的安全性与可行性。因此，该战略的发布首先要求私营企业与其共享安全信息。

2017 年 10 月，澳大利亚总检察署发布了《关键基础设施安全法草案 2017》。法案将创建关键基础设施相关的国家安全风险管理框架，包括保存关键基础设施资产的资产登记信息，并启动部长级“终极权力”。该法案的重要部分在于确定关键基础设施的所有者和运营者。法案将管理港口、水电高风险行业 100 项资产，为个人或组织机构提出不同的监管要求。澳大利亚政府将个人称为“直接利益所有人”，将组织机构称为“责任实体”。

该草案旨在加强澳大利亚政府对于外商投资关键基础设施业务所产生的间谍、破坏、和胁迫等国家安全风险的管理能力。

（三） 2017 其他国家工控安全标准及重要文件

1） 韩国

2017 年 1 月，韩国政府向国会正式提交了《国家网络安全法案》。《国家网络安全法案》旨在防止威胁国家安全的网络攻击，迅速积极应对网络危机，为保障国家安全及国民利益做出贡献。主要内容包括四大部分，在国家网络安全推进机制方面，设立国家网络安全委员会、确立负责网络安全保护的责任机构、设定网络空间保护技术支援机构、指定网络安全专门企业和研究机构。在网络安全预防机制方面，制定网络安全基本计划、网络安全实态评价、网络安全威胁信息共享、网络危机应对演练、网络攻击的探测。在网络安全应对体系方面，进行网络攻击的探测、网络攻击事故的通报和调查、网络危机警报的发布、网络危机对策本部等。

2） 新加坡

2017 年 7 月，新加坡通信部与网络安全局共同发布了《网络安全法案 2017》（草案）征求公众意见，该草案是新加坡继去年 10 月宣传的旨在加强全球合作伙伴关系的“网络安全战略”之后又一网络安全举措。草案共分为六个部分，第一部分为序言，明确了法案的名称、生效起始时间、适用范围，对草案中的一些术语进行概念界定；第二部分为监管，主要规定了网络安全官员的任命和职责；第三部分为关键信息基础设施，主要规定了关键信息基础设施的认定与撤回、关键信息基础设施所有者的义务；第四部分为网络安全事件的预防及响应；第五部分为网络安全服务提供者；最后一部分为一般规定。此外，还附有基础服务（essential service）及需许可的网络安全服务（licensable cybersecurity service）两个目录。

3） 英国

2017 年 8 月，英国政府出台《智能汽车网络安全新指南》，指南的全称为《面向联网和自动驾驶汽车的网络安全关键原则》，目标是将之拓展到汽车制造和供应链上的每一方。指南细分出了 8 个原则：组织上应确保在董事会层面将安全重视起来；制造商应该评估潜在的风险（尤其是第三方承包商）；汽车安全需要在整个生命周期内持续存在；组织与分包商必须携手认证它们的安全流程和产品；安全系统应该有冗余；制造商应在系统制造周期内对软件进行管理；数据的存储必须是安全的；车辆或系统应能够承受攻击并继续工作。

二、 国内工控安全标准及重要文件

2017 年 1 月，工信部印发《信息通信网络与信息安全规划（2016-2020）》，规划》明确了以网络强国战略为统领，以国家总体安全观和网络安全观为指引，坚持以人民为中心的发展思想，坚持“创新、协调、绿色、开放、共享”的发展理念，坚持“安全是发展的前提，发展是安全的保障，安全和发展要同步推进”的指导思想；提出了创新引领、统筹协调、动态集约、开放合作、共治共享的基本原则；确定了到 2020 年建成“责任明晰、安全可控、能力完备、协同高效、合作共享”的信息通信网络与信息安全保障体系的工作目标。

2017 年 3 月，经中央网络安全和信息化领导小组批准，外交部和国家互联网信息办公室 1 日共同发布《网络空间国际合作战略》（下称“战略”）。战略以和平发展、合作共赢为主题，以构建网络空间命运共同体为目标，就推动网络空间国际交流合作首次全面系统提出中国主张，为破解全球网络空间治理难题贡献中国方案，是指导中国参与网络空间国际交流与合作的战略性文件。这是中国就网络问题首度发布国际战略。

2017 年 4 月，工信部印发《云计算发展三年行动计划（2017-2019 年）》。结合现有基础以及面临的问题和挑战，《行动计划》从提升技术水平、增强产业能力、推动行业应用、保障网络安全、营造产业环境等多个方面，推动云计算健康快速发展。此外，《行动计划》还

提出了未来三年我国云计算发展的指导思想、基本原则、发展目标、重点任务和保障措施。

2017 年 5 月，国家互联网信息办公室发布《网络产品和服务安全审查办法（试行）》，于 6 月 1 日起实施。《办法》指出，关系国家安全的网络和信息系统采购的重要网络产品和服务，应当经过网络安全审查。国家互联网信息办公室会同有关部门成立网络安全审查委员会，负责审议网络安全审查的重要政策，统一组织网络安全审查工作，协调网络安全审查相关重要问题。2017 年 5 月，国务院办公厅印发《政务信息系统整合共享实施方案》，围绕政府治理和公共服务的紧迫需要，以最大程度利企便民，让企业和群众少跑腿、好办事、不添堵为目标，提出了加快推进政务信息系统整合共享、促进国务院部门和地方政府信息系统互联互通的重点任务和实施路径。2017 年 5 月，水利部正式印发《水利网络安全顶层设计》。国家标准《信息安全技术大数据安全管理指南》征求意见稿也于 5 月发布。

2017 年 5 月，为贯彻落实《中华人民共和国网络安全法》《国务院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），指导做好工业控制系统信息安全事件应急管理相关工作，保障工业控制系统信息安全，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》。该指南旨在加强工业控制系统信息安全（以下简称工控安全）应急工作管理，建立健全工控安全应急工作机制，提高应对工控安全事件的组织协调和应急处置能力，预防和减少工控安全事件造成的损失和危害，保障工业生产正常运行，维护国家经济安全和人民生命财产安全。

2017 年 6 月，《中华人民共和国网络安全法》正式实施，这是我国网络领域的基础性法律，其中明确规定要加强对个人信息保护。另外，最高人民法院和最高人民检察院发布的相关法律解释也将于今天实行，进一步明确了侵犯公民个人信息罪的定罪量刑标准。《网络安全法》进一步界定了关键信息基础设施范围；明确加强对个人信息保护；对攻击、破坏我国关键信息基础设施的境外组织和个人规定相应的惩治措施；增加惩治网络诈骗等新型网络违法犯罪活动的规定等。2017 年 6 月，中国人民银行印发了《中国金融业信息技术“十三五”发展规划》。6 月 8 日，国务院办公厅日前印发《政府网站发展指引》，对全国政府网站的建设发展做出明确规范。6 月 9 日，国家互联网信息办公室会同工业和信息化部、公安部、国家认证认可监督管理委员会等部门制定了《网络关键设备和网络安全专用产品目录（第一批）》。6 月 27 日，中央网信办印发《国家网络安全事件应急预案》。同日，第十二届全国人民代表大会常务委员会第二十八次会议通过《中华人民共和国国家情报法》。

2017 年 7 月，为了保障关键信息基础设施安全，根据《中华人民共和国网络安全法》，国家互联网信息办公室发布《关键信息基础设施安全保护条例（征求意见稿）》，该《条例》对关键信息基础设施在网络安全等级保护制度基础上，实行重点保护。关键信息基础设施安全保护坚持顶层设计、整体防护，统筹协调、分工负责的原则，充分发挥运营主体作用，社会各方积极参与，共同保护关键信息基础设施安全。

2017 年 8 月，为规范工业控制系统信息安全（以下简称工控安全）防护能力评估工作，切实提升工控安全防护水平，根据《中华人民共和国网络安全法》《国务院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），工信部印发《工业控制系统信息安全防护能力评估工作管理办法》，本办法适用于规范针对工业企业开展的工控安全防护能力评估活动。本办法所指的防护能力评估，是对工业企业工业控制系统规划、设计、建设、运行、维护等全生命周期各阶段开展安全防护能力综合评价。工业和信息化部负责指导和监督全国工业企业工控安全防护能力评估工作。8 月，工信部印发了《移动互联网综合标准化体系建设指南》。

2017 年 11 月，为进一步健全公共互联网网络安全突发事件应急机制，提升应对能力，根据《中华人民共和国网络安全法》和《国家网络安全事件应急预案》等，制定《公共互联网网络安全突发事件应急预案》，工信部印发《公共互联网网络安全突发事件应急预案》，该预案编制目的是建立健全公共互联网网络安全突发事件应急组织体系和工作机制，提高公共互联网网络安全突发事件综合应对能力，确保及时有效地控制、减轻和消除公共互联网网络安全突发事件造成的社会危害和损失，保证公共互联网持续稳定运行和数据安全，维护国家网络空间安全，保障经济运行和社会秩序。

2017 年 12 月，为贯彻落实《国务院关于深化制造业与互联网融合发展的指导意见》、《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》等文件精神，加快我国工业控制系统信息安全保障体系建设，提升工业企业工业控制系统信息安全防护能力，促进工业信息安全产业发展，工业和信息化部制定了《工业控制系统信息安全行动计划（2018-2020 年）》。工业控制系统信息安全（以下简称工控安全）是实施制造强国和网络强国战略的重要保障。近年来，随着中国制造全面推进，工业数字化、网络化、智能化加快发展，我国工控安全面临安全漏洞不断增多、安全威胁加速渗透、攻击手段复杂多样等新挑战。为全面落实国家安全战略，提升工业企业工控安全防护能力，促进工业信息安全产业发展，加快我国工控安全保障体系建设，制定本行动计划。

三、 国内外工控安全行业动态

对比 2016 年和 2017 年 Gartner 技术成熟度曲线：OT 安全进入低谷期 (Trough of Disillusionment)，估计会在 2018 年进入稳步爬升的光明期 (Slope of Enlightenment)。

Figure 1. Hype Cycle for Managing Operational Technology, 2016

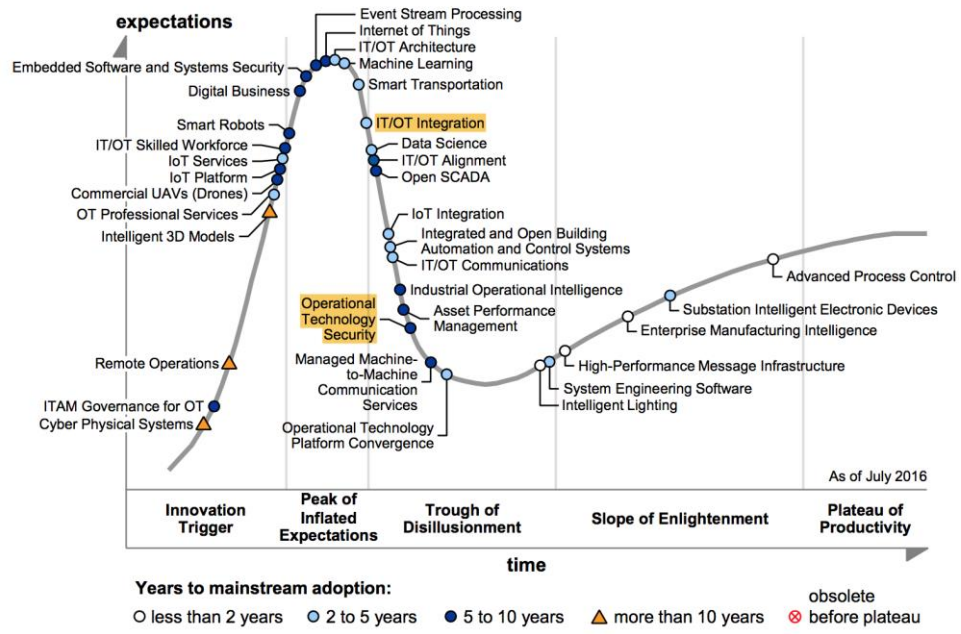
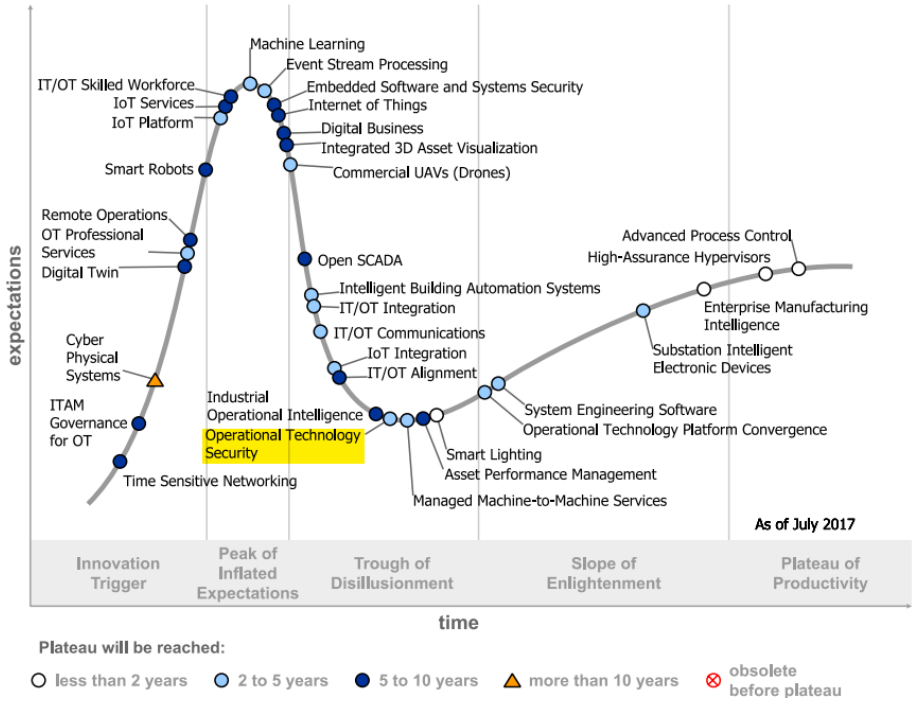


Figure 1. Hype Cycle for Managing Operational Technology, 2017



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。2016 年，已经有 30%的企业设置首席信息安全官 CISO 或首席安全官 CSO；到 2020 年，新部署的 IIOT（Industrial Internet of Things）或 OT 系统将支持时间敏感网络 TSN，目前 0%；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。Gartner 认为，OT 安全对关键基础设施、智能楼宇、工厂管理、医疗和零售行业等资产密集型或资产中心化的组织是非常有用的。

通过以上数据分析，IT/OT 一体化发展趋势可以概括如下：IT 和 OT 分离管理的情况将会打破；基于以太网的尽力交付模型将不再适用；开始考虑时间敏感网络（TSN）自底向上打通；数字孪生。

同时，在工业安全 2018-2020 行动计划中，通过对 MarketsandMarkets、Credence Research、和讯网、工控安全蓝皮书等的统计分析，国内市场 2018 工控安全市场保守预计在 4.4 亿，工信部 451 号文、指南、《网络安全法》落实后，合规市场有望快速增长，竞争者陆续进入。

在国际市场中，2017 年 OT 安全全球市场规模 102.4 亿美元，2022 年将达到 138.8 亿美元，年均复合增长率为 6.3%；利润率高，市场渗透度为 5%-20%；到 2019 年，65%的企业 OT 安全将有 CIO（首席信息官）负责，而在 2016 年仅有 30%的企业设置首席信息安全官 CISO 或首席安全官 CSO；到 2020 年，新部署的 IIOT 或 OT 系统将支持时间敏感网络 TSN，目前 0%；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。由此可见，工业安全越来越重要，越来越火。

第六章　工业信息安全改进建议

一、　工业信息安全问题总结

随着 IT\OT 一体化进程的不断推进，工业控制系统的网络复杂程度在不断提高，各生产单元内部系统与受控系统的信息交换的需求也不断增长，主要包括外部信息流入和内部信息流出。系统的核心系统，一方面，面临数据受灾、泄漏等影响较大的威胁；另一方面，面临病毒攻击导致工业控制系统失效、错误控制导致工业生产突然中断、公共基础设施瘫痪、环境污染、财产损失、人员伤亡等损伤性较高的威胁。工业控制系统安全防护重点在于信息的可用性、完整性和机密性。工业网络主要面临以下安全问题：

（一）　工业网络安全威胁级别越来越高，漏洞类型多种多样

通过 2017 年 ICS-CERT 和 CNVD 安全漏洞平台统计新增漏洞数据发现，工业控制系统信息安全事件大幅提高，高危漏洞比重增多，攻击破坏力不断增强，对关键基础设施的安全防护存在重大威胁。

（二）　网络结构快速变化，目前工控技术存在隐患

1)　工业控制系统规模急速膨胀，工控系统极少升级，易受病毒攻击感染；

2)　系统普遍缺乏监测手段，无法感染未知设备；在执行服务器操作时，缺乏系统审计；

3)　在执行关键操作时，缺乏日志记录；工控设备存在诸多漏洞，RTU/PLC 安全隐患突出；

4)　在工控系统中，开放对外接口会带来安全隐患；网络结构快速变化，原有 IP 数据网信息安全技术远远不能满足工业控制系统的安全要求。

（三）　网络边界不够清晰，局部安全问题易扩散到整个系统

在工业控制系统中，对网络内各个组成部分的安全需求缺乏统一规划，没有对核心业务系统的访问进行很好的控制；各接入系统之间没有进行明确的访问控制，网络之间彼此可以互相访问，边界入手易，系统内入手难。

（四）　工控安全标准有待完善，安全企业重视不足

根据 2017 漏洞统计结果来看，漏洞种类和数量上都有显著增多。此外，工控信息安全企业积极性不高，控制器厂商之间相互观望，对于工控安全建设关注度不够，一旦有攻击者攻击工控系统，难以做到安全防护。

二、　工业信息安全建议与展望

工业控制系统安全是国家关键信息基础设施安全的重要组成部分。在工业互联网、“中国制造 2025”、“工业 4.0”等趋势驱动下，随着云计算、物联网、大数据技术的成熟，信息化与工业化进行了深度融合，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。因此，为促进工控网络安全健康发展，提出如下建议：

（一）　建立网络安全滑动标尺动态安全模型

该标尺模型共包含五大类别，分别为架构安全（Architecture）、被动防御（Passive Defense）、积极防御（Action Defense）、威胁情报（Intelligence）和进攻反制（Offense）。这五大类别之间具有连续性关系，并有效展示了防御逐步提升的理念。

架构安全：在系统规划、建立和维护的过程中充分考虑安全防护；

被动防御：在无人员介入的情况下，附加在系统架构之上可提供持续的威胁防御或威胁洞察力的系统，如：工业安全网关/防火墙、工业主机防护、工业审计等；

积极防御：分析人员对处于所防御网络内的威胁进行监控、响应、学习（经验）和应用知识（理解）的过程；

威胁情报：收集数据、将数据利用转换为信息，并将信息生产加工为评估结果以填补已知知识缺口的过程；

进攻反制：在友好网络之外对攻击者采取的直接行动（按照国内网络安全法要求，对于企业来说主要是通过法律手段对攻击者进行反击）。通过以上几个层面的叠加演进，最终才能够实现进攻反制，维护工业互联网的整体安全。

（二） 从安全运营的角度，建立企业的工业安全运营中心

在 IT 和 OT 一体化推进发展中，IT 技术在 OT 领域大量使用，IT 所面对的风险也跟随进入了 OT 网络，因此工业企业对这两个应用角度都要识别风险的切入点，列举相关的风险，并且要进行一体化的规划。

工业安全运营中心（IISOC）基于威胁情报和本地大数据技术对工控系统通信数据和安全日志进行快速、自动化的关联分析，及时发现工控系统异常和针对工控系统的威胁，通过可视化的技术将这些威胁和异常的总体安全态势展现给用户，通过对告警和响应的自动化发布、跟踪、管理，实现安全风险的闭环管理。威胁情报、威胁检测、深度包解析、工业大数据关联分析、可视化展现、闭环响应实现以工业安全运营为中心的一体化防护体系。安全运营目的是解决越来越多的安全产品部署在网络中形成的“安全防御孤岛”问题。

（三） 组建 IT&OT 融合的安全管理团队

组建 IT&OT 融合的信息安全管理团队，对整个工业控制系统进行安全运营。对安全管理团队进行必要的指导，根据具体场景建立合适的安全策略管理和响应恢复机制，及时应对

安全威胁。企业要想成功部署工业网络安全项目，需重视同时掌握信息技术（IT）和操作技术（OT）的人才，有的放矢。订购安全服务和威胁情报，定期对安全管理团队进行培训，建立IT、OT的安全统一规划，使得安全管理团队成员尽量利用统一标准进行安全事件的处理。

（四） 在技术层面提高防护能力

终端层面：针对 CNC 等老旧设备，部署轻量级白名单（系统进程）的防护措施；针对性能好的生产设备，部署统一的终端杀毒软件，如 360 天擎；移动介质，例如 U 盘，进行统一管控（主机防护）。

网络层面：横向分区、纵向分层，将办公网、工控网、生产网有效划分；网络边界处部署安全网关，最小权限原则：只开放必要端口，进行精细化访问管控。

监控层面：摸清资产家底，集中统一管理，并精心维护；部署工业安全运营中心，对公司网络安全状况进行持续监测与可视化展现。

可恢复性（备份层面）：针对 CNC 等老旧设备，定期请工控厂商进行系统备份；针对性能好的办公和生产电脑，定期自行进行系统和数据备份。

附录 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 11 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、工业审计、工业态势感知与监测预警平台、工业安全运营中心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，工程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，努力成为工业信息安全产业创新的龙头。