中国工业互联网安全应急响应和产业态势分析报告（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

✧ 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。

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；

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。

✧ 建立低位、中位、高位能力“三位一体”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。

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。

✧ 梳理工业资产，重点关注工业主机资产，做好工业主机防护。

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，将取得“最高费效比”实现“事半功倍”。

摘要

- 病毒攻击的目标为主机，而工业主机基本处于裸奔状态；
- 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；
- 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；
- 防护监测层产品处于产品体系功能层级的最低层，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；
- 安全运营层产品处于产品体系功能层级的中层，此类产品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处于产品体系功能层级的最高层，此类产品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。
- 梳理工业资产，重点关注工业主机资产，做好工业主机防护；
- 持续监测生产风险；
- 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

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 一体化工业信息安全态势报告》，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，联合实验室编撰了《中国工业互联网安全应急响应和产业态势分析报告（2018）》。本报告旨在总结 360 工业安全应急响应中心在 2018 年处置的工业安全事件为基础，分析总结应急处置后的经验，工业互联网安全产品体系及工业互联网安全发展建议，供合作伙伴及企业客户决策参考使用。

《中国工业互联网安全应急响应和产业态势分析报告（2018）》内容被综合收录到《IT/OT 一体化工业信息安全态势报告（2018）》年度报告中。《IT/OT 一体化工业信息安全态势报告（2018）》是续 2017 年发布《IT/OT 一体化工业信息安全态势报告（2017）》后，总结分析 2018 年工业互联网 IT/OT 融合带来的新挑战，安全现状、产业发展趋势、重大应用案例等，给出 2019 年工业信息安全建议和展望。

最后，希望本报告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。

第一章　　工业互联网安全应急响应典型案例及总结

随着互联网与工业融合创新的不断推动，电力、交通、市政等大量关系国计民生的关键信息基础设施日益依赖于网络，并逐步与公共互联网连接，一旦受到网络攻击，不仅会造成巨大经济损失，更可能带来环境灾难和人员伤亡，危及公众生活和国家安全，安全保障能力已成为影响工业互联网创新发展的关键因素。

近年来，工业互联网安全事件层出不穷，安全形式日益严峻。本节主要分析 360 在 2018 年处理分析的典型应急响应案例，并对处置的应急响应进行总结。

一、 360 在工业安全应急响应中的典型案例

（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

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。

（二）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。

（三）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。

（四）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。

二、 工业互联网安全应急响应案例总结

(一) 勒索病毒主要攻击目标瞄准工业主机

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：

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。

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；

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。

(二) 构造完善的工业安全产业体系

应急处置只能暂时性解决当下存在的问题，从工厂整体改造要求出发，从确保生产安全、连续、稳定和企业发展的长远利益出发，制定全面解决方案建立完善的工业安全防护体系刻不容缓。企业可从以下方面开展工作：

提高安全意识和培训。人是安全的尺度，网络攻击者知道人仍然是信息安全中最薄弱的环节，大多数安全漏洞都是由人为错误造成的。通过培训提升 OT 人员的安全意识和技能，将是最快最有效的规避，因为人的不了解带来的低级安全风险，缩短隐患、事件的判断和恢复时间。

对 OT 资产进行清点，分级和分类。OT 资产是安全防护的对象，包括：设备，操作，软件，网络和人员，分析这些资产之间的互连和依赖关系。定义各类 OT 资产重要性及安全要求，以达到所要求的风险降低水平，确定所要进行的安全工作，如：网络分割、身份和访问管理应急计划（备份等）、漏洞管理、远程访问（包括特权和非特权访问）安全监控、第三方管理修补程序管理事件响应。

实施工业主机安全防护。网络攻击首要对象是工业主机，如：勒索挖矿病毒等，相比改进重新分隔 OT 网络，对工业主机实施“白名单”类的安全防护更简单易行，可以在生产间隙或检修时完成，效果十分明显。

构建全面的防御和监测体系。在网络边界处部署工业级防火墙，接入交换、核心交换处旁路部署全流量监测产品，对病毒和网络攻击进行全面拦截，即便是入侵发生亦可快速被发现、被告警、被定位，全面建立工厂、公司、集团的多发预警监测。

第二章　　工业互联网安全产业态势

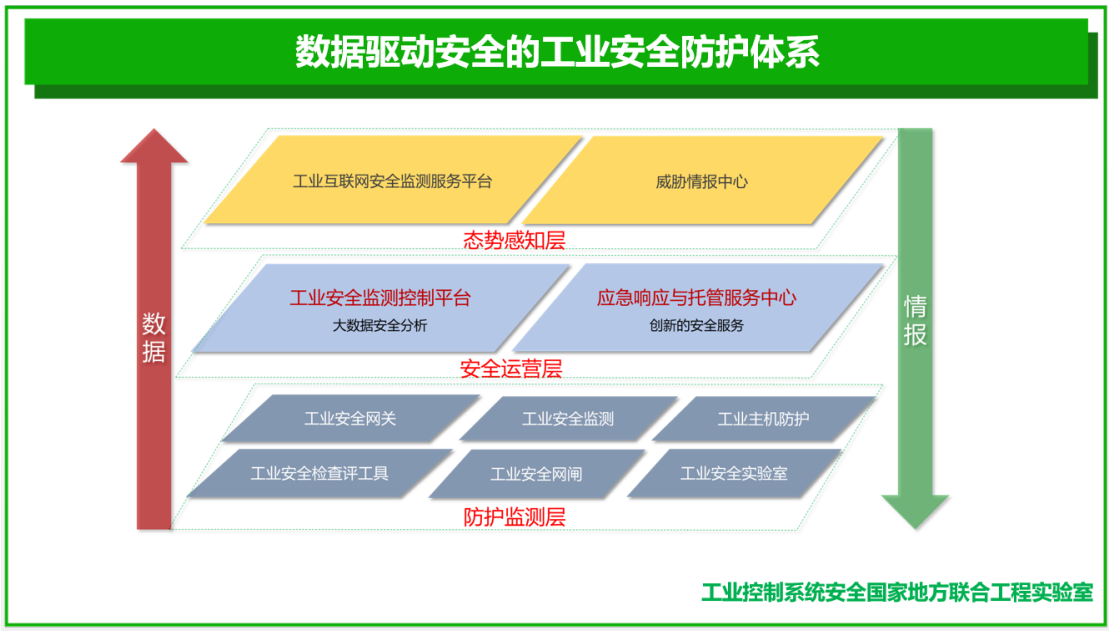
面对频发的工业互联网安全事件，传统的安全防御产品已逐渐乏力、无法有效应对越来越严重的安全威胁，构建层次清晰、定位明确、融合联动的工业互联网信息安全产品体系将成为产业未来发展的重要趋势。

一、 工业互联网安全产业结构

（一）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。

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。



（二）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。

（三）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。

（四）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。

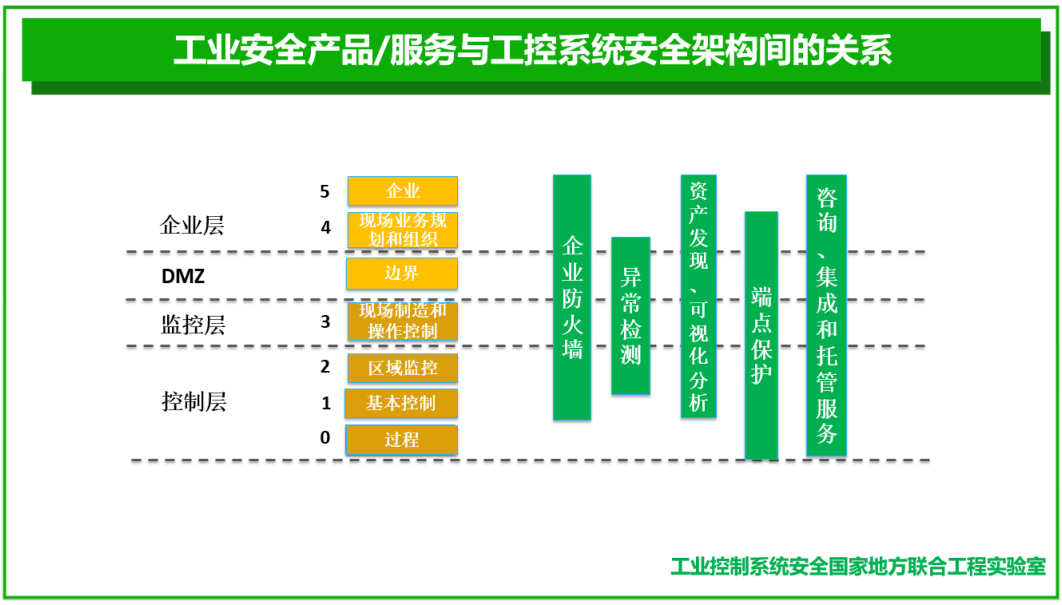
二、 Gartner 关于 OT 市场的分析

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）。

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。

第三章　工业互联网安全发展建议

一、 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。

二、 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。

三、 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。

附录一 工业互联网安全事件

一、 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。

二、 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。

三、 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。

四、 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。

五、 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。

六、 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。

七、 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。

八、 某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，某市北控水务集团远程数据监测平台遭到黑客攻击，致使网页被篡改。某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，某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。