

共筑工业信息安全的“命运共同体”

文/北京交通大学计算机与信息技术学院 李滢东
360企业安全集团 陶耀东



李滢东

北京交通大学计算机与信息技术学院副院长、
博士生导师

作为国家安全的重要组成部分,工业信息安全是指工业运行过程中的信息安全,涉及工业领域各个环节,直接关系到经济发展、社会稳定和国家安全,具体包括工业控制系统安全、工业互联网安全、工业大数据安全、工业云安全、工业电子商务安全和关键信息基础设施安全等领域。随着工业信息化和智能化的不断发展,工业信息安全领域正在发生着巨大的变革。德国率先提出工业4.0计划,为深化改革促进发展,我国也继而提出“中国制造2025”战略,为确保国家可持续发展提供坚实有力的后盾。

工业信息安全发展现状

当前,随着云计算、大数据和人工智能等新一代信息化技术与

工业化技术深层次融合,工业信息安全形势日趋严峻,“三大风险”与日俱增,大量具有危害性的信息安全事件层出不穷,逐步将工业信息安全方面存在的各种隐患暴露了出来,这对处于上升趋势的工业信息安全领域来说是一大障碍,提升工业信息安全保障能力已迫在眉睫。

一是大规模、高强度工业信息安全事件频发,工业领域成为攻击的“重灾区”。2010年伊朗布什尔核电站遭受了“震网病毒”(Stuxnet)入侵,导致核电站的离心机运行失常;2014年黑客组织“蜻蜓组织”对欧、美地区企业发起大规模攻击,利用Havex病毒攻击了近一千家能源企业;2015年乌克兰电力系统遭受黑客攻击,导致地区大面积停电数小时;2018年以来,相继发生“熔

断”和“幽灵”漏洞,威胁工业信息平台安全,美国天然气输气管道遭供应链攻击引发系统故障等。在国内,各种相关事件也是接踵而至(见图1)。

二是工控安全漏洞层出不穷,高危漏洞比重较高,并且漏洞修复速度极为缓慢,这些现象在制造、能源、商业设施、水务和市政等重点领域较为突出,严重威胁国家信息基础设施安全。我国国家信息安全漏洞共享平台(CNVD)所收录的安全漏洞数量近年来持续走高,据CNVD统计,2018年1月—2018年5月信息安全漏洞总数达6730个,工业控制系统漏洞总数为190个。在CNVD工业控制系统子漏洞库中,新增的高危漏洞有95个,占该子漏洞库新增数量的50%。

三是大量工业信息系统及设备

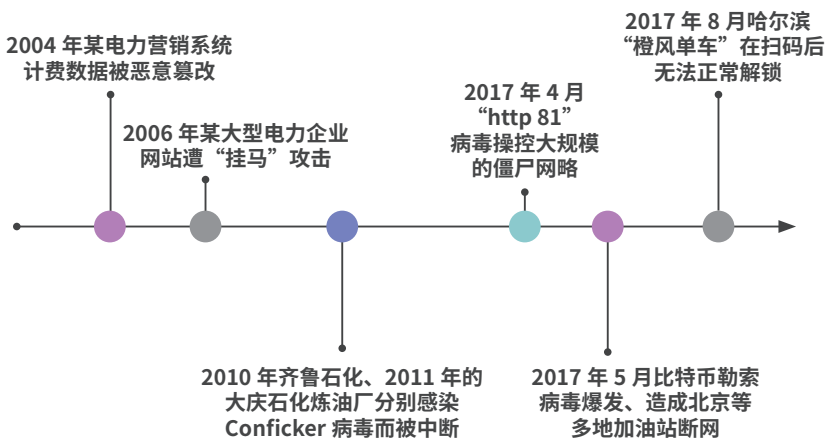


图1 大规模、高强度工业信息安全事件频发,工业领域成为攻击的“重灾区”

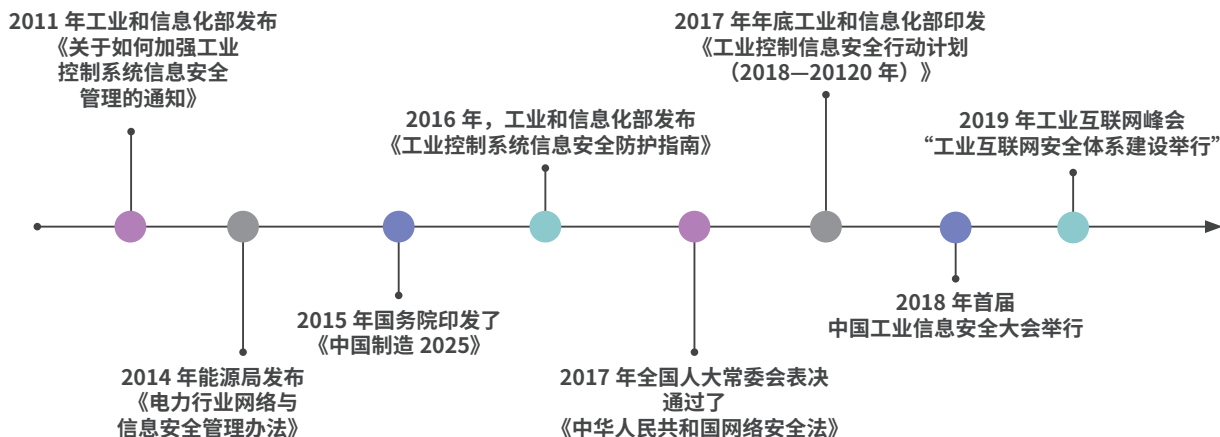


图2 工控安全漏洞层出不穷，高危漏洞比重较高，并且漏洞修复速度极为缓慢

暴露于互联网，成为我国工业信息安全的软肋。截止2018年5月，国内范围内暴露在互联网上的工业控制系统设备数量高达97 625个，呈现逐渐上升的趋势。

同时，我国工业信息安全市场主要集中在工业隔离网关/电力专用隔离装置和工业防火墙/电力防火墙等领域，硬件、服务业务占比较低，特别是在芯片、核心软件等关键领域，我国处于“跟跑”阶段，与欧美市场差距较大。

由此可知，我国在工业信息安全方面的研究还处于比较薄弱的境地，相关防护技术的研究还不成熟，产业发展不充分、不全面，严重滞后于工业信息安全的发展需求。总体来看，起步晚、基础薄和研究不平衡是我国工业信息安全领域的实际状况。

但不可否认的是，我国在工业信息安全方面一直在做着努力，尤其对工业控制系统的信息安全问题进行了一定的对策研究。国内许多知名学者从系统的整体到局部给出了各种安全防护的理论观点，针对整个控制系统建立纵深防御的安全防护体系，研发异常监测技术，给系统局部的组件如人机界面实施信息安全策略等。并且工业信息安全现已成为我国科研院所和企业重视

的领域，并被提高到了国家战略的高度（见图2），我国的工业信息安全领域在稳步提升。

工业信息安全存在的问题与认知误区

目前，我国在工业信息安全领域还存在着明显的短板：

一是安全意识有待提高，需进一步优化和落实工业信息安全方面的政策法规。多地区、部门与工业企业对信息安全重视不够，重发展轻安全，漏洞不重视、修复不及时的现象普遍存在，系统内部人员也容易发生违规操作和越权访问，从根本上是责任意识、风险意识不足的表现。工业信息安全各领域发展参差不齐，层次不清，缺乏统一规划，对安全问题缺乏系统的理论总结，面对干扰时缺乏一套有效且可实施的措施，成熟规范的安全标准需进一步结合市场改进和落实。

二是相关产业核心技术积累不足，大中型研究团队及人才亟待扩充。许多领域的工业信息安全核心技术仍被国外专家和企业所掌握，相关的重点工程项目与重大装备的技术系统来自于国外产品，尤其是欧美日系的部分企业仍主导着我国工业信息安全的高

端市场。并且，国内自主原创的技术及产品极少，缺少竞争力，很难全方位保障我国工业控制系统的安全可控。

作者认为有以下方面的误区和原因致使了上述短板的出现：

1. 认知的误区

1) 我国现有研究主要集中在工业信息安全的规范制定、导则制定和控制系统的软件漏洞发现方面，很少从具体控制系统的自身技术特性入手，来研究工业信息安全的具体问题和处理措施。

2) 工业信息系统在设计之初多数考虑的是系统的可靠性和实时性，盲目被认定系统内的装置与设备是安全可靠的，而不太关注信息安全的问题，而致使缺乏足够的安全机制，如采用的授权、鉴别和加密等信息安全技术不足，因此很容易被攻击者利用。

3) 工业信息安全不同领域的理论与技术混合使用。不同工业领域的产品并不完全兼容，所用到的防护技术与方法存在差异。如果一旦发生问题，轻则影响相关产品的使用与推广，重则导致整个系统瘫痪，其损失和后果不可估量。

2. 受到信息化产业的冲刷

随着物联网、工业云等信息

化产物的高速发展以及其与工业系统的深度融合,信息系统与工业系统的联系越来越密切,信息系统中普遍存在的安全漏洞和入侵泄露等问题出现在了工业系统中,使得工业系统在不断壮大的同时其信息安全的防护也越发复杂。与信息系统安全相比,工业系统信息安全较难管理,原因在于旧有的系统很少进行升级,大量分散的资产需要频繁的远程访问服务,安装杀毒软件和防火墙等传统防护措施并不完全适用于工业信息系统。且工业系统与信息系统存在一定的差异,这就导致信息系统中很多安全防范技术很难适用于工业系统的信息安全防护中。正因如此,信息安全在之前的工业系统中并未得到相应的关注。在此背景下,国内信息安全企业和科研机构主要致力于互联网和传统信息系统的安全问题,对工业领域信息安全的关注度明显存在不足。

信息化与工业安全齐发展

工业信息安全领域在感受公开、融合和互联技术所带来的安全威胁时,其防护技术水准、产业生产率与竞争力也在不断提高和不断增强。可以说,信息化产物的高速发展与工业信息安全是一个相辅相成、相互壮大的过程。随着云计算、工业云和大数据技术的逐步成熟,信息化与工业化进行了深度融合,使工业系统能更高效地进行资源优化配置,实现经营管理的科学化,从而推动产业不断升级,促进产品“智能化”“网络化”和“机电一体化”,降低了不安全的因素与行为,拓展了工业生产系统、智慧交通和智能电网等工业系统发展的空间,极大提高了工业领域的综合效益。同时,工业信息安全

的发展与提高又促进了物联网等信息化产物的飞速前进,给信息化产物提供了很好的落脚点与应用基础,促进了“产学研用”融合技术创新体系的建设。

随着信息化与工业化的不断交叉融合,近年来我国的电力、石油、交通、轨道和航天等各个行业都在争相开展信息安全类的工作,其中,电力领域的信息安全工作已属于国内外的佼佼者。智能电网的发展,使得电力领域的安全已经涉及到电网调度运行、电力企业生产、经营的各个方面,并日益综合化、复杂化。同时,电力产品与外界接口不断增加,特别是与银行等合作单位业务的接口、网上电力服务、三网融合、数据大集中应用以及内部各系统间的互联互通,致使来自外界的攻击越来越多,信息安全隐患的风险与损失越来越严重。

针对电力领域信息安全问题,需要建立完整的信息安全防护体系,根据建设的发展,结合实际情况统一规划,分步建设,逐步投资。

1) 制定完整的信息安全防范体制。对每一个细节都应实行严格的安全防范,力求在最大限度上保障信息安全的合理运行。可以借鉴国外知名电厂的管理运维模式,健全管理制度,规范好操作标准。

2) 推进电力应急资源库和信息通报预警平台的建设。在突发电力信息安全事件时,能有力支撑相关部门进行分析研判并进行有效处理,能及时地发布风险预警信息,形成快速高效各方联动。

3) 落实好安全防护技术措施,加强系统认证准入。采用信息安全新技术,主要从数据库安全策略(包括系统安全策略、数据安全策略和用户安全策略三个方面)、

数据备份和恢复、网络服务和应用系统的安全、网络防病毒、防火墙的相关技术的应用(防火墙的策略、入侵检测系统、虚拟专用网)、数据加密及传输安全等方面着手,以电力企业信息安全为中心,建立一个技术联合、多层次的技术结构安全体系,提高信息系统总体防护能力,体现“智能、整合、管理”趋势,确保业务数据安全可靠,保证电力企业及产品信息安全。

4) 着力完善产业生态。信息系统开发时应要求公开系统源代码,并在此基础上加快电力领域信息系统的自主研究,以安全策略、安全服务和安全机制的有效结合为中心,提高硬件、软件、数据库和网络等方面的研究水平,保证电力信息系统的可控。加大优秀产品和服务的应用推广,充分利用工业信息安全产业发展联盟等行业组织的“产学研用”合作优势,推动工业信息安全产品高质量地生产和发展。

结束语

“以人为本,辅以技术,重在管理,刚柔并济”是安全规划的根本要则,不仅仅适用于电力领域信息安全管理,也可应用于其他工业领域信息安全的建设。工业信息安全领域是真实世界的重要组成部分,同时也是现代人类文明发展的基石,工业信息安全问题将直接影响着人类社会的发展,是一个挑战,也是一个机遇。要充分了解各种不安全因素之后,加强自身实力与能力的培养,真正把我国的工业信息安全做强做大起来,并积极推进工业信息安全产业“走出去”,乘着“一带一路”红利的帆船,加强与沿线国家和地区的合作,共筑工业信息安全命运共同体。EA