匡恩网络

2015工业控制网络安全态势报告

前 言

随着信息技术和网络技术的迅猛发展，国家安全边界已经超越地理空间限制，延伸到了信息网络。“棱镜门”事件后，世界各国深刻认识到网络治理权关乎国家网络空间安全和利益，网络空间已经成为继陆、海、空、天之后的第五大国家主权空间；2015年末发生的乌克兰电网断电事件以及2016年年初刚发生的乌克兰机场受攻击事件都表明：一直以来被认为相对安全的工业控制系统已经成为黑客攻击的目标，而且工业控制系统安全漏洞及攻击方式已经成为“黑市”热销商品，甚至被作为“特殊武器”列入“瓦森纳协定”的控制清单，而中国在被禁运国家之列。

工业控制系统广泛应用于我国电力、水利、污水处理、石油化工、冶金、汽车、航空航天等诸多现代工业，其中超过80%的涉及国计民生的关键基础设施（如铁路、城市轨道交通、供排水、邮电通讯等）都依靠工业控制系统来实现自动化作业，随着国务院“中国制造2025”战略提出，中国工业控制领域正在发生重大的变革，两化深度融合是产业结构调整和升级转型的重要支撑，工业控制系统网络安全已经成为两化融合的重要组成部分，深刻地影响着工业控制系统及相关产业的发展，工业控制系统网络安全风险所带来的，不再仅仅是信息泄露、信息系统无法使用等“小”问题，而是会对现实世界造成直接的、实质性的影响，其安全性不仅关系到生产安全和经济发展，而且影响到社会稳定和国家安全。

为给政府部门、研究机构提供参考和借鉴，匡恩网络连续第二年撰写和发布工业控制网络安全态势报告。

本报告分为六个章节：第一章对国际工业控制网络安全形势进行分析和总结，概述国际工业控制网络安全总体情况、面临的主要威胁和发展趋势；第二章介绍国际工业控制网络安全政策方面的情况，尤其是欧美国家在2015年度在政府管理、行业指导方面的政策动向；第三章对我国工业控制网络安全情况进行总体分析，结合匡恩网络安全实验室的研究成果，对影响我国工业生产安全的漏洞进行深入分析；第四章介绍国际重要工控网络安全事件，以及匡恩网络安全实验室的部分研究成果；第五章是结合匡恩网络智能工业网络安全研究院的研究成果，以及2015年的大量项目实践，针对我国重点工业行业工控网络安全趋势进行分析和展望；第六章总结我国工控网络安全领域面临挑战和发展机遇，结合匡恩网络在工控网络安全方面的实践和思考，对我国工控网络安全的发展提出了具体建议，供政府部门或研究机构决策参考。

目 录

国际工业控制网络安全情况总体分析

工业控制领域正在发生重大的变革，德国和美国相继提出了“工业4.0”“工业互联网”概念，我国也于2015年5月8日提出“中国制造2025”战略，在两化深度融合的基础上继续进行产业结构调整和升级转型。作为工业控制网络重要的组成部分，工业控制网络安全深刻地影响着工业控制网络及相关产业的发展，具有极强的产业关联度和产业渗透能力，因此工业控制网络安全产业得到了各国极大的关注。

近几年，走进公众视线的工业控制网络安全问题越来越多，各界对工业控制网络安全问题关注度大幅上升，针对工业控制网络安全的研究呈现爆发式增长。

1.1 工业控制网络设备漏洞数量仍居高位

美国工业控制系统网络应急响应小组（ICS-CERT）发布的2014年关键基础设施安全报告显示，在2014年共收集了167个工控漏洞报告，涉及的设备分布在能源、制造业等多个领域，图1-1中显示了从2012年到2014年工控漏洞报告数量和所涉及到工控设备的数量。

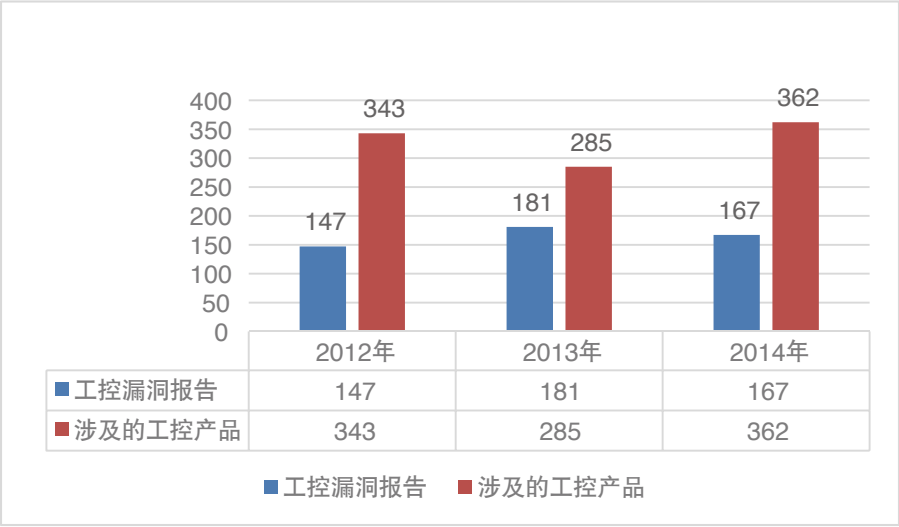


图1-1 工控漏洞及相应的工控产品统计

1.2 工业控制网络安全事件呈逐年增加趋势

工业控制网络安全事件在近几年呈现稳步增长的趋势，2015年被ICS-CERT收录的攻击事件达到了295件。

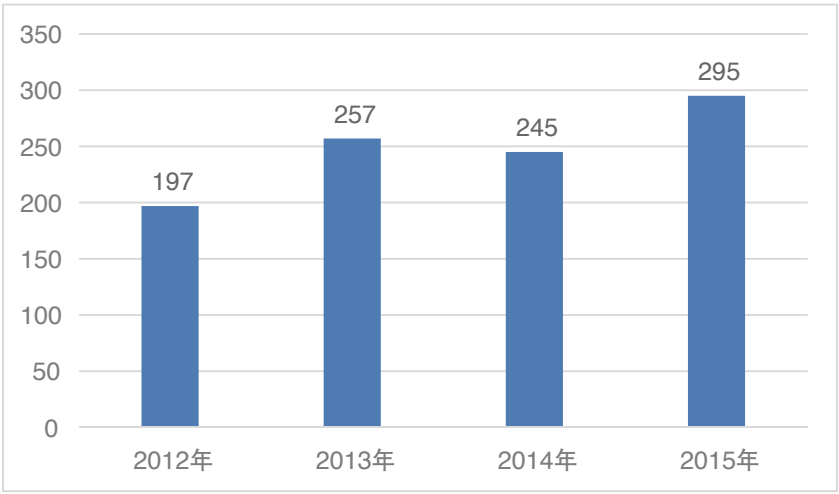


图1-2 工业控制网络安全事件统计

1.3 关键制造业成为本年度受攻击最多的行业

2015年ICS-CERT共收集了295起涉及关键基础设施的安全事件（见图1-2），关键制造业、能源、水处理成为被攻击最多的三个行业。这些事件由个人、团体、第三方/研究机构和美国政府多方提供。不过，这些数据虽然为工业控制网络管理者们提供了一些参考，但也有人指出统计结果与实际情况可能会有较大差距，并不是所有的组织选择与ICS-CERT分享关于关键基础设施安全事件的信息。

由图1-3可知，2015年有97个安全事件是关于关键制造业的，占到全部事件的33%，成为本年度受攻击最多的行业（2014年是能源行业）。

另外，ICS-CERT还对攻击方式进行了统计，见图1-4。

通过对攻击方式的分析我们会发现，2015年鱼叉式攻击数量达到了37%。很多的安全事件是由于系统架构设计不合理、不完善而导致的，如果工控设备直接或间接的与互联网连接，就会使鱼叉式攻击极易成功。

ICS-CERT反复强调网络安全监测和入侵检测技术（帮助管理者探测、响应和分析事件）的重要性，但仍有37%的网

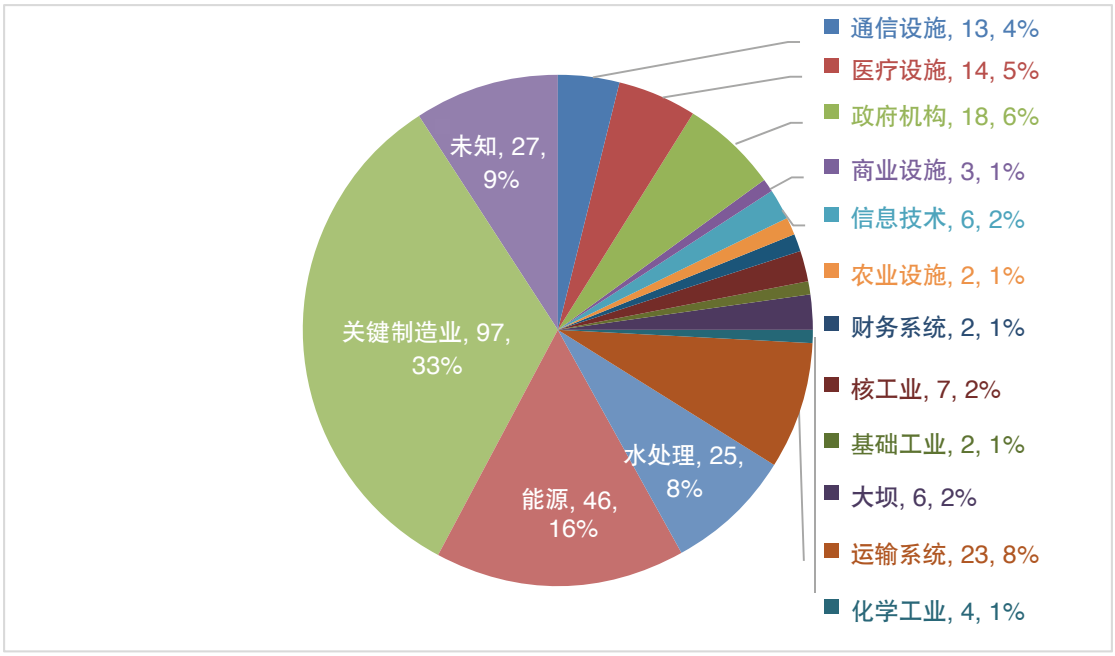


图1-3 2015年各行业攻击事件统计

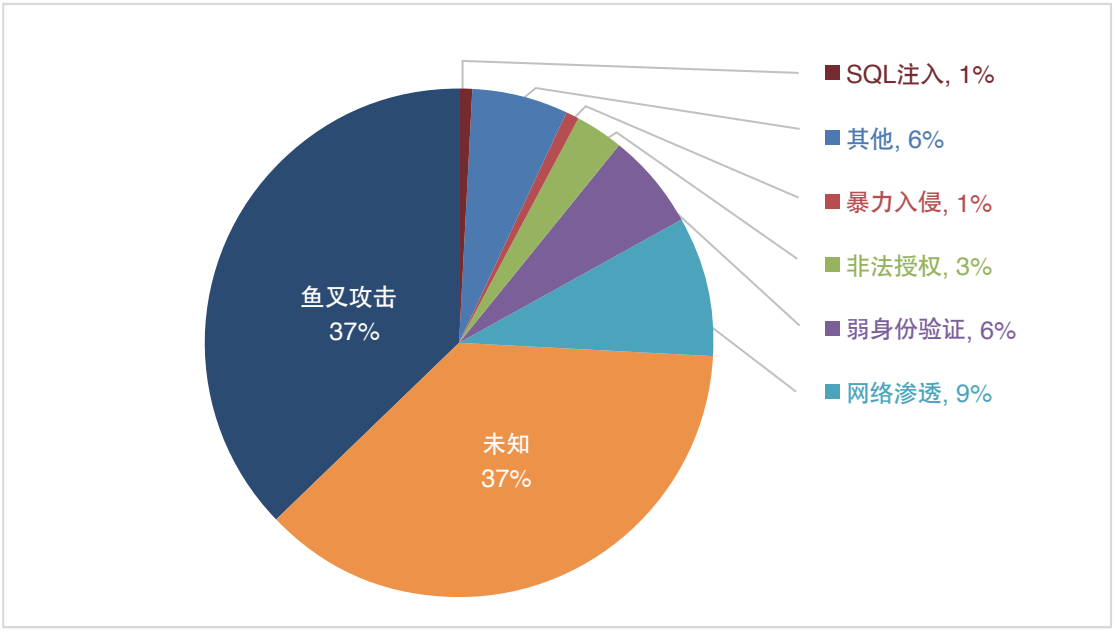


图1-4 工控网络攻击方式

络安全攻击没有甄别出是如何实现的。

在已知的攻击方式统计中，鱼叉式攻击占到了总数的37%，可见对重要基础设施来说，鱼叉式攻击是一种相对容易的攻击手段，其多利用Email附件传播木马程序进行攻击。与2014年相比，统计表中网络渗透攻击的数量虽然急剧下降，但这种下降并不意味着真实攻击数量的减少，而是因为部分关键基础设施的所有者具备了成熟处理这种攻击的能力，从而减少了向ICS-CERT请求支持的报告。

另外，ICS-CERT的统计数据也显示出资产所有者能够保护自己的设备，大量的攻击以失败告终。统计显示，有69%的攻击没有入侵成功，而在2014年这一数据是49%。不过，有12%的攻击入侵到了工业现场级的控制系统，这一数据要高于2014财年的9%。

2 国际工业控制网络安全政策动态

自2005年开始，美国和欧盟就高度重视工业控制网络安全技术的发展，大力推动相关前沿技术研究，相继发布了保护国家关键基础设施的国家战略和政策法规，并牵头建立了多个国家级工业控制网络安全实验室，构建了全维度的工控网络安全国家体系。

美国和欧盟均已发布了关于网络安全和保护关键基础设施的国家战略。美国于2006年专门设立了“国家基础设施保护计划”，并在2010年设立了控制系统安全计划（CSSP），将保护美国国家基础设施的控制系统上升为国家战略。欧盟继美国之后于2013年发布了“欧洲关键基础设施保护项目（EPCIP）”，协调欧盟各个国家保护其关键基础设施，应对日益增加的针对关键基础设施的网络攻击。

美国国防部、国土安全部、能源部、国家标准局、审计署和财政部协调各自职能，为该战略提供相应的资源协助。欧洲则是由欧洲委员会、欧洲高级议会、欧洲对外行动处、欧洲防务局、欧洲网络犯罪中心和欧洲标准机构，协调欧盟各个国家的相关职能，部署各个国家的关键设施保护计划。

同时，美国国土安全部成立了工业控制系统应急响应组（ICS-CERT），作为CSSP的实施部门。欧盟也成立了类似的欧洲网络应急响应组（CERT-EU），同时计划成立针对工业控制网络安全的应急响应组（ICS-CSIRT）。

表2.1：世界各国工控网络安全发展情况对比简表

对比项 / 国别	国家政策	监管部门	法律法规	标准规范
美国	• 2003年《网络空间安全国家战略计划》； • 2006年“国家基础设施保护计划”； • 2010年“控制系统安全计划（CSSP）”；	美国国防部、国土安全部、能源部、国家标准局、审计署和财政部、ICS-CERT等。	• 2013年“国家赛博安全和关键基础设施保护法案”； • 2015年第二版网络战略报告；	• 2014年ISA/IEC62443工业自动化和控制系统（IACS）系列标准； • NIST SP800-82工业控制网络安全指南；
欧盟	• 2005年的《保护信息时代社会安全战略》； • 2013年“欧洲关键基础设施保护项目（EPCIP）”； • 2013年《关键基础设施保护计划》；	欧洲委员会、欧洲高级议会、欧洲对外行动处、欧洲防务局、欧洲网络犯罪中心和欧洲标准机构、欧洲网络应急响应组CERT-EU等。	• 2013年《欧盟网络安全战略》； • 2014年《Certification of Cyber Security skills of ICS/SCADA professionals》；	
日本	• 2013年《网络安全战略》（2015年5月25日更新）；	2015年日本成立内阁网络安全中心		

对比项 / 国别	国家政策	监管部门	法律法规	标准规范
新加坡	• 新加坡2014年《国家网络安全总体规划》；	2015年新加坡成立网络安全局		
印度	• 印度2013年《国家网络安全政策》；			

2.1 世界各国历年来的重点政策动态

美国历年来的重点政策动态

美国早在20年前就已经在政策层面上关注工业控制系统信息安全问题，近年来美国政府发布一系列关于关键基础设施保护和工业控制系统信息安全方面的国家法规战略。

2002年美国国家研究理事会将“控制系统攻击”作为需要“紧急关注”的事项；

2003年美国出台了《网络空间安全国家战略计划》，指出保护网络空间需要政府和社会各界作出协调一致的努力，并将网络空间定义为一个“由信息技术基础设施组成的相互依赖的网络”；

2005年美国出台了《改进SCADA网络安全的21项措施》，给出了针对SCADA网络安全的最佳实践；

2006年6月，国土安全部发布《国家基础设施保护计划》，以及“能源行业防护控制系统路线图”，为现行和未来的保护关键基础设施和重要资源方案和活动提供了一个总体框架；

2009年美国出台“国家基础设施保护计划（NIPP）”；

2011年发布“实现能源供应系统信息安全路线图”；

2013年12月11日，美国两党共同推出了3696号法案，即“2013年国家赛博安全和关键基础设施保护法案”（NCCIP法案）。该法案支持私营企业和联邦政府间真实开展的合作。

美国在国家层面上工业控制系统信息安全工作还包括2个国家级专项计划：美国能源部（DOE）的国家SCADA测试床计划NSTB和美国国土安全部（DHS）的控制系统安全计划（CSSP）。

2014年12月31日，媒体报道称美国国家标准与技术研究所（NIST）正在开发一种用户工业控制系统的网络安全测试平台。在测试平台上执行国家和国际标准和准则规定的做法，然后衡量集成电路的性能。测试结果将为工业行业实施网络安全标准和指导方针提供指导，且不会对集成电路性能产生负面影响。本项目覆盖的标准和指导方针包括ISA/IEC 62443工业自动化和控制系统（IACS）系列标准和NIST SP800-82工业控制网络安全指南等。

2015年1月13日，美国总统奥巴马拜访了美国国土安全部国家网络安全与通信集成中心（NCCIC），提出了一项针对网络安全信息共享的立法提案以加强网络安全的信息共享，对抗网络犯罪。另外，美国能源部将在未来五年内，向网络安全教育团队提供2500万美元的政府补贴。2015年1月20日，奥巴马发表2015年国情咨文，专门提到了保护网络安全。

2015年4月24日，美国国防部发布第二版网络战略报告（第一版于2011年发布），指导美国网络力量的发展，加强网络防御建设与网络威慑力量。

2015年6月8日，美国国家标准与技术研究院发布第二版工业控制网络安全指南。该指南包括如何调整传统IT安全控制系统以适应工业控制网络独特的性能、可靠性和安全性的要求。同时对威胁与漏洞、风险管理、实施方案、安全体系架构等部分进行了更新。自2006年美国国家标准与技术研究院首次发布工业控制网络指南以来，该指南下载量超过了300万次。

欧盟历年来的重点政策动态

从2005年开始，欧盟也相继出台了安全管理政策，如2005年的《保护信息时代社会安全战略》；2007年《使用隐私信息增强技术改进数据保护意见》；2012年《美国国土安全部和欧洲委员会关于欧洲网络安全的联合声明》；2013年《欧盟网络安全战略》及《关键基础设施保护计划》。这些文件相继出台，体现了欧盟国家加强工控网络安全的需求。

2014年12月，欧洲网络与信息安全局（ENISA）针对工业控制系统发布了《Certification of Cyber Security skills of ICS/SCADA professionals》。该报告探讨了现有信息安全技术及举措如何引申应用到工业控制网络，明确了工业控制网络安全面临的挑战并提出了一系列的发展建议。

其他国家历年来发布的重要文件

此外，一些亚洲国家也相继出台了关于保护国家基础设施和网络安全的政策文件，比如日本2013年《网络安全战略》（2015年5月25日更新）；印度2013年《国家网络安全政策》；新加坡2014年《国家网络安全总体规划》等，其中均提到了建议应对国家关键基础设施网络攻击的紧迫性和重要性。

2.2 2015年重点国家安全政策梳理

美国

加大网络安全投资规模、出台网络和信息安全法规、调整组建网络安全机构、修订完善网络和信息安全标准、强化网络空间军事能力、扩充网络空间军事力量、开展网络安全多方合作、举行网络安全演练、严格网络空间治理、研发信息安全关键技术、培养网络安全人才、开展网络安全审计等。

1月2日，美国总统下达行政命令，加强对朝鲜的制裁，以报复其对索尼影业公司的网络攻击。

1月7日，美国国防部提出在2016年底前将网络部队人数增加至现在的三倍，达到约6200人员规模。

1月11日，美国国防信息系统局建立联合部队总部，初期人数约100人。

1月12日，美国总统呼吁出台《个人数据通知与保护法案》和《学生数据隐私法案》。

1月13日，美国防信息系统局发布新的《云计算安全采办指南（SRG）》。

1月14日，美国国防部颁布新的《国防后勤管理标准》。

1月15日，美国司法部长与10个欧盟国家的内政部长、加拿大公共安全部长举行了紧急反恐会议，加强网络反恐合作。

1月21日，美国情报部门发布首个安全信息共享路线图《数据汇总参考框架（DARA）》。

1月22日，美国和英国达成一致，将举行网络空间联合演习。

2月2日，美国政府宣布，2016财年将投资140亿美元加强网络安全，其中，国防部比2015财年增加4亿美元。

2月10日，美国宣布建立“网络威胁情报整合中心（CTIIC）”。

2月12日，美国白宫行政管理和预算办公室（OMB）称，将修改相关信息安全标准，以适应新的网络安全形势。

2月27日，美国联邦通信委员会批准通过《网络中立规则》。

3月6日，美国中央情报局宣布，将成立一个新的数字指挥部以及建立十个任务中心。

3月7日，美国检方对涉嫌盗窃近十亿个电子邮件数据的3名网络黑客提出法律诉讼。

3月12日，美国参议院通过《网络安全信息共享法案（CISA）》。

3月17日，美国国防部成立新的电子战委员会。

3月18日，美国政府要求所有联邦政府网站（含国防部网站）在两年内使用HTTPS协议。

4月1日，美国总统签署了行政命令，授权对美国实施网络攻击的海外组织或个人进行经济制裁。

4月7日，美国陆军国民警卫队表示，将在未来3年内成立10个网络保护小组。

4月9日，美国和欧洲警方共同采取行动，打击计算机犯罪网络团伙。

4月14日，美国在加利福尼亚硅谷等地进行网络人才招聘，以加强国民警卫队和预备役网络力量。

4月21日，美国众议院通过《保护计算机网络法案（PCNA）》。

4月22日，美国众议院通过《国家网络安全保护促进法案》。

4月23日，美国国防部发布新版《网络安全战略》。

5月11日，欧盟和美国就数据共享安全性达成协议。

5月15日，美国众议院通过《美国自由法案》。

5月20日，美国商务部称，将禁止未公开软件漏洞的出口。

5月30日，美国和日本发表联合声明称，美国的网络防御保护伞将扩大至日本。

6月1日，美国发布《移动应用开发通用评估和验证标准》。

6月3日，美国参议院通过《美国自由法案》。

6月4日，美国国家标准与技术研究院公布未来20年发展无缝宽带公共安全通信网络技术的路线图。

6月5日，美国国家标准与技术研究所发布工业控制系统（ICS）安全指南（第二次修订版）。

6月14日，鉴于美国人事管理局网络遭黑客入侵事件，美国政府启动了为期30天的网络安全审计调查行动。

6月8日到26日，美国举行了旨在加强关键基础设施安全的第四届年度“网络卫士”演习。

7月16日，美国国防部称，将成立新的分析中心以应对网络内部人员威胁。

7月22日，日美举行“网络对话”会议。

7月29日，美国发布《国家战略计算计划（NSCI）》。

8月1日，美国总统称应当对中国的网络攻击进行报复性回击。

8月10日，美国土安全部拟新建网络信息防御中心，整合各部门网络安全信息。

8月11日，美国发布《联邦民用网络安全战略》。

8月20日，美国国防部称，已设立跨部门的网络工作委员会。

9月4日，美国国防部称，将于2015年秋季推出绝密级智能手机。

9月7日，美国国防部计划设立数字服务办公室。

9月9日，美国国防部发布云安全指南。

9月18日，美国国家标准技术研究院发布网络物理系统框架文件草案。

9月22日，美国推出首个安全漏洞多方应对方案。

9月23日，美国称正在研发网络安全自动化工具。

9月25日，美国政府要求智能手机公司留下后门，以便于调查人员破解恐怖分子或犯罪嫌疑人手机上加密通信数据。

9月29日，美国网络司令部发布4.6亿美元的网络技术外包合同。

9月30日，美国众议院通过国土安全部网络安全战略法2015（H.R.3510）。

10月6日，美国国家标准与技术研究院研发能解决邮件安全问题的关键技术。

10月17日，美国逮捕ISIS网络攻击幕后黑手。

10月21日，美国举行“国家安全局网络日”活动。

10月26日，美国金融监管机构发布网络安全新规。

10月27日，美国参议院通过《网络安全信息共享法案（CISA）》。

11月10日，美国国土安全部招聘1000名网络员工。

11月11日，美国战略与国际研究中心发布《美日网络安全合作》报告。

11月14日，美国国会向美国网络司令部发出命令，要求组织以俄罗斯、中国、伊朗以及朝鲜为假想敌的模拟网络军事演习。

11月15日，美国国防部制定反钓鱼政策，禁用外部邮件中的链接。

11月16日，美国破获史上最大网络盗窃案，涉及1亿多份个人信息被泄漏。

11月17日，美国启动1亿美元IT人才招聘计划。

11月18日，美国发布《美国国家反间谍战略2016》。

11月19日，美国国会鼓吹对中国进行“网络反击”。

11月24日，美中两国称，将联合打击网络销售假药行动。

11月30日，中美进行首次打击网络犯罪高级别对话。

12月1日，美国发布报告称，美国银行业于9月份举行了“量子黎明”网络攻击演习。

12月2日，美众议院提出《电邮隐私法案》。

12月6日，美国总统呼吁高科技公司协助政府反恐。

俄罗斯

2015年俄罗斯在网络和信息安全方面的新政策、新举措主要包括9个方面：出台新的信息安全学说、完善网络安全法规、严格网络空间监管、打击网络恐怖主义、开展网络安全审查、研发网络关键技术、加强电子政务安全、扶持本国信息技术产业、开展国际网络安全合作等。

1月12日，俄罗斯称，2014年共冻结（限制访问）逾900家宣扬极端主义思想的网站或社交媒体账号。

2月21日，俄罗斯竞争监管机构联邦反垄断局（FAS）表示，已针对谷歌涉嫌违反反垄断法展开调查。

3月4日，俄罗斯总统表示，俄内务部门需要警惕国内的网络极端主义行为，及时采取行动制止网络极端主义犯罪。

4月11日，谷歌公司按照俄罗斯政府规定，将部分服务器迁移至俄罗斯。

4月18日，俄罗斯提议金砖国家在信息技术和网络空间方面加强协调与合作。

4月24日，俄罗斯常驻联合国代表称，俄罗斯支持积极使用媒体和网络来打击极端主义。

5月8日，俄罗斯与中国签署国际信息安全合作协定。

5月19日，俄罗斯与中国称，两国反对信息通信技术领域威胁他国安全行为。

6月29日，俄罗斯与越南加强在信息技术领域的合作。

7月4日，俄罗斯议会通过《网络隐私保护法》。

7月18日，俄罗斯内政部发布安全须知，旨在警示那些用智能手机拍照的自拍爱好者。

7月22日，俄罗斯称，出于保护当地厂商的考量，将不会签署《信息技术协定》（ITA）扩围协议。

8月4日，俄罗斯国家杜马信息政治委员会称，将审议一项法案，禁止国家公务员使用工作电脑和手机登录社交媒体。

8月21日，俄罗斯国家杜马建议政府机构禁止使用Window10操作系统。

8月24日，俄罗斯政府封禁俄语版维基百科网站。

9月1日，俄罗斯《个人数据保护法》正式生效，要求俄罗斯公民的个人信息数据只能存于俄境内的服务器中，以实现数据本地化。

9月10日，俄政府准备制定有关无线电电子市场的重要决定，以扶持本国信息技术产业发展。

10月13日，俄罗斯卡巴斯基公司联合欧洲反欺凌联盟举行活动，共同应对网络欺凌。

10月16日，俄罗斯称，将发布2016年新版《俄联邦信息安全学说》，替换2000年旧版本。

10月26日，俄罗斯正在研发能隔绝本国互联网、不受外国干扰的关键技术。

10月28日，俄罗斯国防部通过了发展机器人系统并将其用于军事目的的规划。

11月17日，俄罗斯总理签署政府令，规定自2016年1月1日起国家机关只能购买国产软件特别清单上所列产品，只有俄罗斯缺乏同类产品时才可购买外国软件。

11月26日，俄罗斯称，正在开发新的反窃听系统。

12月1日，俄罗斯政府新闻处称，俄罗斯总理将参加在中国召开的世界互联网大会。

日本

日本2015年日本在网络和信息安全方面的新政策、新举措主要包括10个方面：修订网络安全战略、完善网络安全管理机构、制定网络和信息安全法规、加强个人信息安全防护、严格网络安全治理、健全网络安全应急处理机制、加强网络安全人才培养、举行网络安全演习、研发关键网络安全技术、开展网络安全国际合作等。

1月3日，日本称，正加速与各国磋商应对网络攻击。

1月7日，日本总务省召开专家会议，就网络接入服务提供商如何保存用户的通信记录进行讨论。

1月8日，日本政府公开招聘计算机知识和经验丰富的技术人员。

1月9日，日本政府在内阁府成立“内阁网络安全中心”，统管各行政机关的相关网络安全业务。

1月13日，日本期望与澳大利亚在2015年年底前展开网络安全方面的定期对话。

1月15日，日本政府通过《反不正当竞争法》修改草案。

1月18日，日本与法国表示，将在打击极端组织“伊斯兰国”等网络恐怖主义方面展开合作。

1月24日，日本警方以涉嫌协助违反《禁止针对儿童的买春和色情法》，对亚马逊日本公司进行了搜查。

1月28日，日本安全公司称，日本有超过4成的企业已组建计算机安全事件响应小组（CSIRT）。

2月1日－3月18日，日本举办“网络安全月”活动。

2月7－8日，日本举办全国第一大黑客比赛“SECCON 2014”。

2月10日，日本政府召开“网络安全战略总部”年度首次会议，计划出台新版“网络安全战略”。

2月11日，日本政府称，将修改民法条款以保护网购消费者利益。

3月1日，日本政府根据《网络安全基本法》，将负责“关键基础设施”的48个企业或组织指定为网络安全合作的对象。

3月8日，日本政府将起用在计算机和通信网络领域拥有高级技能的专家，即所谓的“正义黑客”。

3月10日，日本政府通过《个人信息保护法》及《个人号码法》修正案。

3月18日，日本政府和相关企业举行网络响应演习。

3月24日，日本警方根据《反不正当竞争法》，逮捕网售DVD防复制破解软件涉嫌人。

3月26日，日本欲将打击网络犯罪核心办案人员增加一倍。

4月27日，日美两国发布新的《日美防卫合作指针》。

5月10日，日本国内大学开始致力于培养可以应对网络攻击的人才。

5月16日，日中韩举行反恐合作工作磋商，将打击网络恐怖主义列为合作事宜。

5月25日，日本举行“网络安全战略本部”会议，制定了新的《网络安全战略》（草案）。

6月3日，日本30家公司成立跨行业组织，应对网络攻击。

6月12日，日本逮捕一名涉嫌免费蹭WiFi的人员。

6月24日，日本总务省将成立“目标型”网络攻击对策研究小组。

7月3日，日本参议院通过新的《反不正当竞争法》。

7月16日，日本开始禁止并惩罚持有儿童色情照片和视频的行为。

7月23日，日本政府规定重要信息系统不得接入互联网。

8月5日，日本公布非法网络程序防扩散技术，能对非法程序篡改网站后扩散性行为进行预防。

8月14日，日本警方根据《禁止非法入侵计算机法》，逮捕了制作病毒工具的嫌疑人。

8月19日，日本经产省拟设国家考试培养网络安全人才。

8月20日，日本正式公布新版《网络安全战略》。

9月24日，日政府拟召集“民间高手”应对网络攻击。

10月1日，日本与东盟（ASEAN）举行部长级会议，共同打击网络犯罪。

11月8日，日本在冲绳举办网络安全国际会议。

11月11日，日本将修改《著作权法》，配合TPP生效。

11月28日，日本政府拟新设网络专家培训制度。

12月4日，日本首相与美国高官会谈，确认合作应对网络攻击。

12月7日，日本拟修改法律允许公布低安全级别软件名单。

12月7日，日本警察厅发表2015年版《治安回顾与展望》报告称，将严厉打击网络恐怖主义。

12月8日，日本东京法院勒令雅虎删除部分个人信息搜索结果。

韩国

韩国2015年韩国在网络和信息安全方面的新政策、新举措主要包括8个方面：出台网络安全法规、完善网络安全机构、严格网络安全治理、制定保护关键基础设施措施、打击网络恐怖主义、提升网络军事能力、保护青少年上网安全开展网络安全国际合作。

1月20日，韩国网络审核机构着手打击有关宣传恐怖主义的网络信息。

1月21日，韩国核监管部门讨论加强打击网络攻击的能力，增加网络安全人员，并加大投资力度，确保核设施安全。

1月22日，韩国国防部长与美国国防部部长表示，双方商定加强在网络安全领域的合作。

1月22－23日，韩国参与东盟电信和信息技术部长会议（TELMIN），加强与东盟地区的信息安全合作。

1月27日，韩国公布的资料显示，2013年以来，韩国政府为提取调查大型门户网站的邮件等通信记录而发出的搜查令数量较2012年激增了2-5倍。

2月2日，韩国执法部门宣布，将着手调查Twitter等社交媒体涉嫌传播色情信息一事。

2月10日，韩国对“韩军网络司令部令”修正案进行审议表决，指定联合参谋议长接受国防部长官的命令，指挥并监督韩军网络司令部的网络作战。

2月11日，韩国信息安全局与越南互联网中心签署互联网合作备忘录，将在网络资源管理和网络安全方面分享信息和经验。

3月25日，韩国将重整网上个人识别号码系统（I-PIN），预防黑客袭击。

4月1日，韩国审议《青瓦台国家安保室职制部分修订案》，将在国家安全室旗下设立“网络安全秘书室”，并设网络安全秘书一职。

4月20日，韩国表示，为应对朝鲜网络攻击决定投入1千亿韩元预算，至2018年构建网络模拟演练场，开发网络攻击系统。

6月18日，韩国规定19岁以下购买手机者需安装网络监管软件。

8月10日，韩国技术与标准局发布G/TBT/N/KOR/597号通报，修订电器安全管理法实施细则的技术法规草案。

8月17-20日，韩国举行全国范围内的“乙支演习”，应对网络恐怖袭击。

10月15日，韩中日网络安全事务磋商机制第二次会议在韩国首尔举行。

10月26日，韩国国家情报局和韩国国防部联合举办网络攻防竞赛，选拔招募计算机网络高手。

10月27日，韩国和美国举行国防网络政策工作组会议，共同讨论应对朝鲜网络攻击的方案。

10月30日，韩国未来创造科学部（未来部）与中国工信部举行会议，就双方加强网络安全领域的合作方案进行讨论。

11月16－17日，韩国在首尔举办亚洲太平洋通讯社组织执行委员会第39次会议，共同讨论信息技术发展和网络安全合作。

11月16日，韩国举行恐袭对策会议，建议出台《恐怖主义防止法》。

11月25日，韩国讨论在电子政务领域推广云服务技术及相关安全技术。

澳大利亚

2015年澳大利亚在网络和信息安全方面的新政策、新举措主要包括7个方面：完善网络安全法规、扩充网络军事力

量、打击网络恐怖主义、研制网络攻防武器、严格网络空间治理、开发网络安全技术、加强网络安全国际合作。

1月13日，澳大利亚与日本商定于2015年年底前展开网络安全定期对话。

2月2日，澳大利亚信号局称，正在开发自己的网络武器，并将其部署在海外的反恐行动中。

2月28日，澳大利亚与新西兰双方就犯罪信息共享、网络安全合作等议题达成多项协议和共识。

4月15日，澳大利亚参议院通过《加强儿童网络安全法案2014》。

4月24日，澳大利亚国防军公开招募具有黑客经验的人员，扩充网络军事力量。

6月19日，澳大利亚政府称将投入4.85亿澳元重启个人可控制的电子医疗档案系统（PCEHR）。

6月22日，澳大利亚参议院通过网络著作权侵权修正案。

6月25日，澳大利亚国防部发布9亿美元的通信网络采购项目，提升国防军事通信网络能力。

7月，将成立澳大利亚电子医疗委员会，负责医疗档案系统的运行。

7月22日，澳大利亚与中国举行数字出版传媒领导人圆桌论坛，共同打击网络侵权。

7月29日，澳大利亚推出新的网络监管政策，要求全国400余所学校对校园网进行监督。

8月26日，澳大利亚法律事务所报告称，近年来因在社交媒体发表言论而被卷入诽谤起诉的案件几乎占到了诽谤案件总数的一半。

9月10日，澳大利亚国防军称，正在开发新一代军用通信网络。

9月16日，澳大利亚竞争和消费者委员会宣布，将建立宽带网络服务质量监测管理体系。

10月21日，澳大利亚新数据保留法律生效，要求在澳大利亚经营的电信公司保留两年的通信数据。

11月26日，澳大利亚政府宣布，新的防恐警报系统从即日起正式运行。

11月27日，澳大利亚政府称，正在开发针对国防、政府和银行部门网络攻击的安全系统。

12月7日，澳大利亚启动国家创新与科学计划，政府将投资3000万澳元建立网络安全增长中心。

印度

2015年印度在网络和信息安全方面的新政策、新举措主要包括6个方面：修订完善网络安全法规、发布实施网络安全指令、组建网络空间司令部、严格网络空间监管、开展网络安全审查行动、加强网络安全国际交流。

1月1日，印度高级法院做出判决，禁止中国“一加”手机在印度销售。

1月4日，印度电信部下令封锁30个知名网站，防止宣传“圣战”的网络恐怖主义思潮蔓延。

3月23日，印度国防部针对网络间谍活动威胁，发布确保机密系统信息安全的指令。

3月24日，印度最高法院废除了于2000年颁布实施的信息安全法的第66A条。

4月7日，印度政府授权网络与移动协会负责鉴定和管理有害信息。

5月23日，印度与蒙古国确定加强双方在网络安全和信息共享方面的合作。

7月1日，印度在首都新德里启动“数字印度周”活动。

7月31日，印度政府发布一项禁令，并通知各大网络服务供应商，关闭包括“色情港湾”在内的857家色情网站，打击网络色情。

8月11日，印度与美国进行网络安全对话，就全球信息安全问题进行磋商。

8月19日，印度政府通过频谱共享法规，规定印度移动运营商可以通过签署频谱共享协议的方式共享同一通信服务区的频谱资源。

8月21日，印度计划组建网络空间联合司令部。

8月27日，印度发射新型军事通信卫星，以提高印军网络中心战能力。

8月31日，印度公平竞争委员会指控谷歌滥用其在搜索市场的主导地位，对其开展反垄断调查。

9月8日，印度和俄罗斯同意成立一个专家小组，应对日趋严峻的网络安全和恐怖组织。

9月21日，印度通信和技术部发布国家信息加密政策。

11月21－24日，印度总理访问马来西亚和新加坡，就网络安全合作、海上威胁信息共享与两国进行了交流。

英国

2015年英国在网络和信息安全方面的新政策、新举措主要包括9个方面：完善网络安全法规、严格网络空间监管、扩充网络空间力量、提升网络军事能力、打击网络恐怖主义、保护儿童上网安全、培养网络安全人才、研发网络安全技术、加强网络安全国际合作；

1月5日，英国知识产权局向反知识产权犯罪部门拨款300万英镑，用于打击网络盗版行为。

1月13日，英国称将禁止使用无法被国家安全部门所监控的通信方式。

1月16日，英国与美国签署联合法案，深化两国在网络战争和网络犯罪打击过程中的合作机制，共同举办应对网络攻击的演习。

2月1日，英国国防部决定于2015年4月成立网络部队“77旅”，负责监控恐怖组织在社交网站的活动。

2月13日，通过《刑事司法和法庭》修正案，禁止网络色情报复。

2月16日，英国教育部投资50万英镑，用以培训网络安全教师和增加网络安全课程。

3月13日，英国政府通信总部发布打击网络恐怖主义指南。

3月14日，举行英国网络安全挑战赛。

3月18日，英国发布严厉新规，对拨打骚扰电话和发送垃圾短信的公司处以最高达50万英镑罚款。

4月1日，公布网络安全学徒计划。

4月11日，英国第77旅社交媒体部队计划招募2000名网络专家。

4月13日，政府与私营部门合作向企业推广网络安全保险。

4月16日，英国与日本就加强网络威胁情报共享方面的合作达成协议。

5月19日，修改通过计算机滥用法案。

5月26日，英国国防部国防科学与技术实验室研究网络战术战法。

5月28日，英国新保守党提出《比尔调查权》，打击网络恐怖主义。

6月17日，英国企业研发出全球首个以表情符号为基础的密码系统。

7月13日，英国议会审议《调查权力法案》。

8月14日，英国推出一个总额6.5亿英镑的网络安全战略计划，强化个人信息安全。

8月18日，英国称将在今后五年投入20亿英镑，加强网络作战能力。

8月28日，英国国家反犯罪局拘捕 6 名青少年黑客。

9月21日，英国国家计算机应急响应小组呼吁建立网络安全共享伙伴关系。

9月28日，英国向高校提供50万英镑基金，用于培养网络安全人才。

9月30日，英国启用在线服务网站，以保护儿童网络安全。

9月2日，英国政府发布对外服务网站TLS（安全传输层协议）部署指南，要求公共服务网站启用全站HTTPS加密技术。

10月14日，英国电信公司在全球范围内推出“金融道德黑客”安全服务，用于测试金融服务机构受到网络攻击的危险性。

10月22日，英国与中国签订首个网络安全协定。

11月2日，英国政府公布新版《调查权法草案》。

11月4日，英国宣布一条法律草案，禁止互联网企业对所传输内容过度加密。

11月11日，英国政府提出打击暗网罪犯行动计划。

11月12日，英国斥资650万英镑，建立网络安全投资基金。

11月16日，英国宣布计划，招募1900名情报和安全人员，以应对恐怖袭击。

11月17日，英国称未来五年将打击网络犯罪的预算提高至19亿英镑，该预算是以前计划的两倍。

11月23日，英国发布《国家安全战略及战略防务与安全审查2015：一个安全和繁荣的英国》战略文件，提出应对网络威胁和加强网络安全。

11月26日，英国国家统计局首次将网络犯罪纳入年度犯罪统计项目。

11月27日，英国废止私人复制豁免条例，规定拷贝音乐犯法。

11月30日，为防罪犯上网，英国监狱提升网络屏蔽技术。

法国

2015年法国在网络和信息安全方面的新政策、新举措主要包括6个方面：完善网络安全法规、打击网络恐怖主义、严格网络空间监管、开展网络安全审查、研发网络安全技术、加强网络安全合作；

1月18日，法国与日本表示将在打击极端组织“伊斯兰国”等网络恐怖主义方面展开合作。

1月21日，针对煽动宗教仇恨和恐怖主义的网络攻击，法国将加强互联网监管并与多国展开网络联合反恐行动。

3月6日，法国称将对网络民族主义言论进行打击，取缔和关闭散发网络恐怖主义思想的网站。

3月16日，法国屏蔽了五家纵容恐怖主义的网站。

4月13日，法国国民议会审议通过第一部情报法草案，强化应对网络威胁的能力。

4月21日，法国参议院通过决议，要求搜索引擎公司提交搜索算法，确保其竞争对手得到公平对待。

4月22日，法国警方宣传网络欺凌危害，设立免费专线供学生咨询。

5月25日，法国数据保护机构公布2015年度检查计划，重点关注电子支付和数据中心安全。

6月2日，法国推介其研发的网络假货预防工具技术。

6月12日，法国国家信息与自由委员会表示，谷歌旗下所有版本的搜索网站都要执行“被遗忘权”。如果谷歌不执行该项规定，将启动制裁程序。

9月8日，法国颁布“数字共和国法”（草案）。

11月22日，法国称，巴黎的恐怖袭击之后，应关注移动应用程序和智能手机的加密问题。

12月8日，为了提高打击恐怖主义的效率，法国内政部推出一系列举措：一是终止网络匿名机制，实行实名制。二是在紧急状态期间，“禁止链接自由分享无线网络（Wifi）”，取消“公共无线网络链接”；三是“禁止和封杀法国的Tor”等。

德国

2015年德国在网络和信息安全方面的新政策、新举措主要包括4个方面：完善网络安全法规、严格网络空间监管、研发网络安全技术、强化网络安全协作；

1月13日，德国法院对一名男子在网上散播其前女友裸照判处5个月的监禁处罚。

3月11日，德国联邦政府宣布，将在2015年至2020年投入1.8亿欧元，加强信息安全技术研究。

4月6日，德国经济和能源部、教育和研究部共同启动升级版“工业4.0平台”建设，关注信息安全。

5月13日，德国与越南联合举行“新闻与社交网络相互作用”研讨会，就新闻与社交网络运用及安全进行交流。

5月27日，德国政府提出《安全数字通讯及医疗应用法》草案，强调医疗保健行业的数字安全。

7月8日，德国议会批准了一项旨在支持数字教育和提高媒体能力的政府建议，将所有学校连接到宽带网络，并创建一个学习材料免费的“安全的数字化学习环境”。

10月15日，德国警方告诫家长们不要把孩子的照片发到社交媒体上。

11月4日，一名德国男子因网络贩毒被法院判刑7年。

伊朗

2015年伊朗在网络和信息安全方面的新政策、新举措主要包括5个方面：研发网络安全技术、出台网络安全战略、颁布网络安全法规、严格网络空间监管、研发网络攻击武器。

2014年12月29日，伊朗政府表示，正在扩大“互联网智能过滤”技术功能，以便屏蔽网站上某些特定内容，同时又能让用户访问网站的非敏感部分。

2015年1月10日消息，伊朗已经开始制定一个新的网络安全战略，使网络作战成为军队和国家情报机构的首要任务。新战略提出两大目标：一是开发关键技术，以保护关键基础设施和绝密资料免遭各种形式的入侵；二是压制在网络空间中的反伊活动。

3月2日，伊朗通讯部表示，只要谷歌遵循当地文化习俗，将同意谷歌进入伊朗互联网领域。

4月17日，美国企业研究所及一家网络安全公司联合进行的一项调查显示，伊朗近几年来大大增加了对网络攻击的研究，正大力研发网络战武器。

4月25日，伊朗德黑兰上诉法庭对利用社交媒体散布谣言、煽动非法聚会的6名人员分别判处5-7年不等的监禁。

6月13日，伊朗安全官员表示，由于担心遭到他国秘密监控，接触机密的伊朗官员禁止在工作时使用智能手机或移动装置。

7月4日，伊朗政府通过《信息接触自由法案》。

8月10日，伊朗民防组织表示，政府设计了威胁评估指挥和控制系统，以应对大规模网络袭击。

2.3 美国工控系统网络安全产业的发展措施

在工业控制网络安全研究方面，美国给予了世界范围内领先的政策支持，建设了多个国家级实验室，先于其他国家制定工控系统安全的行业路线图。

美国协调各相关部门和行业协会制定的工业控制网络安全路线图包括：能源行业路线图；核能行业路线图；化工行业网络安全指南；水行业路线图；跨行业路线图；交通运输行业路线图。

根据2011年ICS-CERT发布的跨行业工业控制网络安全路线图，确定了未来十年各行业工控系统安全的的三个主要目标，分别为：调查和评估各行业工控安全防护能力；开发和整合工控安全防护措施，减少工控系统的漏洞；主动发现威胁侵入并执行应对措施。

美国的关键战略性行业如能源、电力和公用设施等均属于私营部门，因此各行业协会积极响应国家政策，制定相关的行业标准，如电气和电子工程师协会（IEEE）、美国石油研究所（API）、美国公共交通联合会（APTA）、北美电力保障组织（NERC）、水环境研究基金会（WERF）、核电研究院（NEI）、国家制造业协会（NAM）等机构均制定了行业应对网络威胁指南，推动了网络安全在各自行业中的发展。

大型的工业企业，如思科、通用电气、爱默生、洛克希德马丁等，也非常活跃地组织工控系统网络安全的培训和推广，以增加公众对该领域的认识。同时，工控系统网络安全的供应商、客户与政府部门紧密合作，不断完善相应的解决方案和行业标准。

另外，美国也开展了如下一系列的工作。

激发业主企业内在驱动力

美国要求重点行业企业内部设立CISO（首席信息安全官）。CISO的资质由联邦政府审核、颁发，由企业任命，对企业的工控网络的安全负责，其职责就是与政府和科研机构配合，推广风险评估、漏洞挖掘和保护设备在企业的最终落实，最大限度地保证企业不会受到黑客的恶意攻击。

大力扶持私营企业

美国对从事工控安全领域的第三方私营企业给予大力度扶持，不仅从税收等方面给予优惠，而且每年还有大量的研究经费可以申请，同时当企业的产品推向市场时，政府往往会成为第一个买家。一些特别有实力的企业，政府甚至会对其进行“收编”，FireEye公司就是一个典型例子。

大力培养渗透检测团队

这类公司的日常工作就是渗透检测目标行业，寻找入侵系统的办法。他们的目标包括浏览器、电邮客户端、即时通讯客户端、Flash、Java、工业控制网络，以及任何可以被攻击者作为突破口的系统。这类公司往往具有一定的政府背景，在发现漏洞后第一时间配合政府和其他安全企业研究出对策。

大力培养专业人才

美国政府历来重视信息安全人才的培养，为培养信息安全人才出台了各类信息安全教育项目。其中比较有代表性的教育项目包括：联邦计算机服务（FSC）项目，它是综合性的项目，很多活动都遵循信息安全培训概念性框架；服务奖学金（SFS）项目：政府资助研究生和本科生的信息安全学习，待其毕业后服务于联邦政府；联邦范围内的信息安全意识培养项目等。

我国工业控制网络安全情况总体分析

2015年，随着互联网+、中国制造2025等国家战略方针的出台，随着“两化融合”政策的深入推进，国内工业控制网络的网络化、智能化水平快速提高，同时工业控制网络的信息安全持续2014年的热度，继续被政府组织、科研机构、安全厂商、自动化厂商密切关注。虽然国内工控系统依然比较脆弱，整体安全形势面临严峻挑战，但我们也能看到从政府、企业、厂商各方都在为积极推进国内工控安全的发展。

3.1 我国工控网络的脆弱性不容忽视

新增漏洞的价值越来越高

截至2015年底，我们根据中国国家信息安全漏洞共享平台所发布的2015年新增漏洞信息[CNVD]，共整理出2015年新增的工业控制网络相关的漏洞108个。重点分析新增漏洞的统计特征和变化趋势，主要涉及公开漏洞的总体变化趋势、漏洞的严重程度、漏洞所影响的工控系统类型、漏洞的危害等几个方面的对比分析。

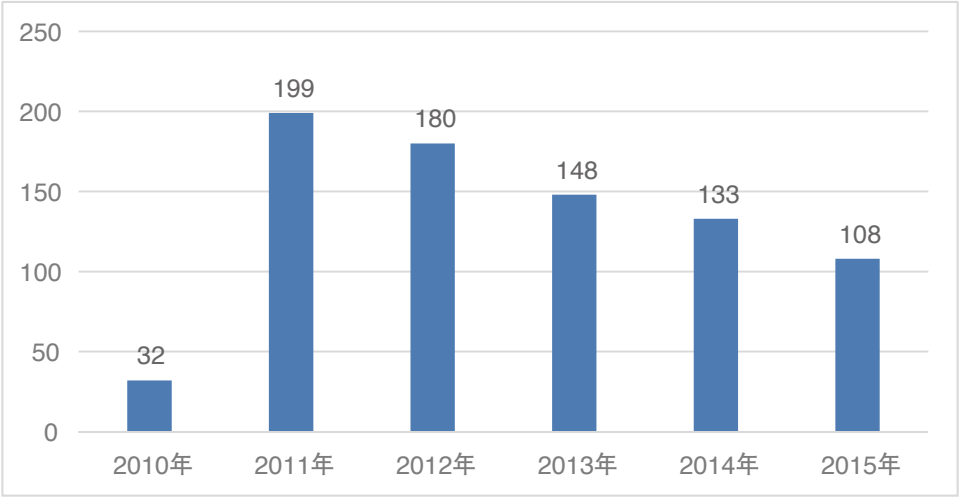
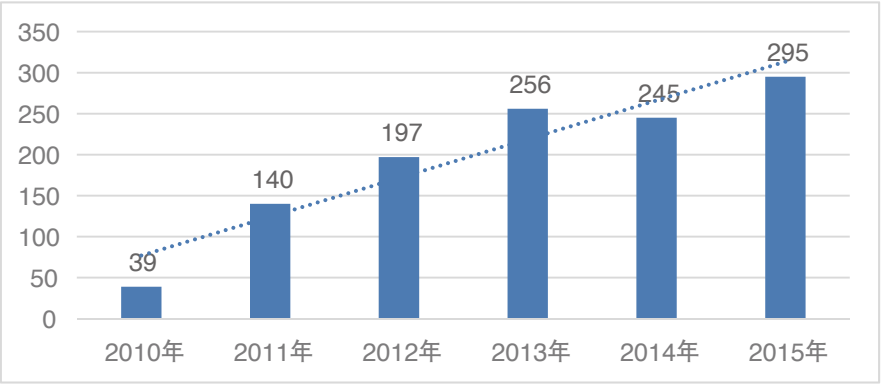


图3-1 工控行业每年新增漏洞统计（数据来源：CNVD、匡恩网络）

工业控制网络已经成为信息安全工作者关注的焦点，一些不怀好意的攻击者不断扫描工控系统的漏洞并使用针对工控系统的专用黑客工具发动网络攻击；从图3-1可以看出，除了2011年爆发式增长外，每年公开发布的新增漏洞数量有下降趋势。

一方面工控系统的主要厂商意识到其产品已经成为出头鸟，从而加强安全方面的开发，所以再挖掘这些产品漏洞的难度越来越大。

另一方面，由于政治、军事等因素的影响，作为国家基础设施建设的工控系统已经成为网络战争的必争之地，所以很可能一些漏洞信息被限制公开或转为地下交易，从美国ICS-CERT每财年发布的安全事件数量可以印证这一点。虽然每年新增漏洞数量有下降趋势，但工控安全事件却有上升趋势，从而也说明工控漏洞的价值和影响力越来越大。



3-2 工控行业每年安全事件数量统计（数据来源：ICS-CERT）

2015年，工控安全厂商和国家安全组织仍在不遗余力收集工控安全漏洞信息，以提醒和帮助工控企业提高自身系统的安全防护能力，提高攻击者的攻击门槛和攻击成本。

中高危漏洞比例居高不下

根据CNVD公布的2015年工控系统漏洞数据分析，其中高危漏洞和中危漏洞所占比例居高不下。

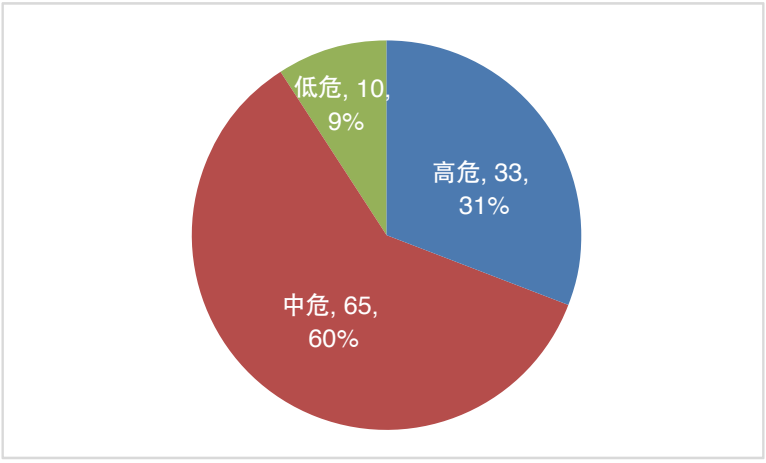


图3-3 工控行业漏洞危险级别统计（数据来源：CNVD）

由此可以看出，工控相关应用系统和软件的安全健壮性不足。无论是应用软件漏洞，还是设备固件漏洞，均是目标系统在开发过程中遗留的安全设计和实现缺陷所导致的，1个高危漏洞就意味着目标系统中存在1个或多个致命安全性bug。

隐患严重的软件Bug通常在软件发布初期出现的较多，随着软件版本不断更新而减少。工控应用系统中的高危漏洞的占比如此之高，说明这些目标系统的安全性设计和验证还处于初期阶段，存在着大量的安全优化空间，亟待自动化厂商在开发测试阶段就加入安全因素，降低中高危漏洞的数量。

漏洞类型复杂多样

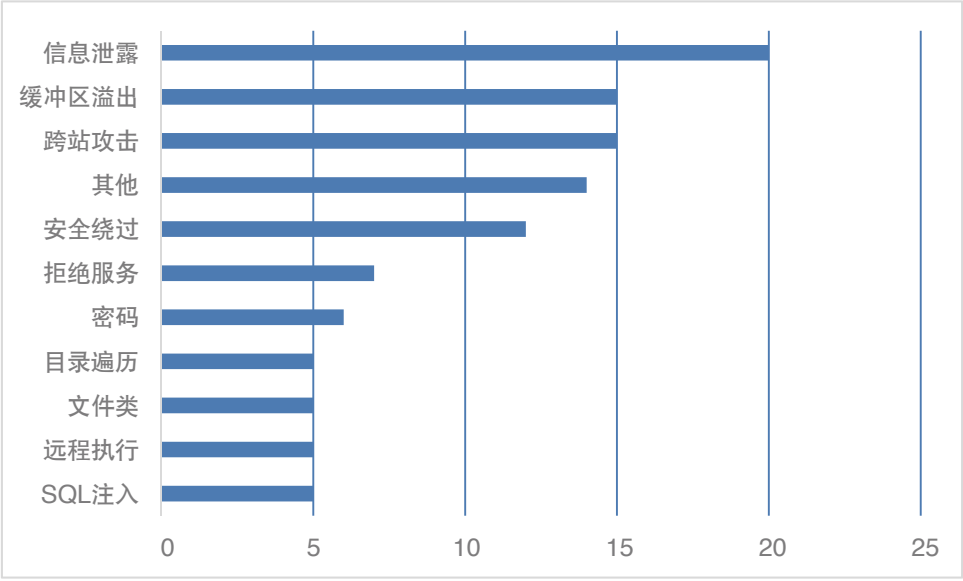


图3-4 漏洞数量统计（数据来源：CNVD、匡恩网络）

从统计的数据可以看出，信息泄露方面的漏洞高居榜首，对工控系统的影响主要体现在两个方面，一方面企业内部的工艺流程、图纸、排产计划等关键信息容易成为攻击者窃取的对象，所以对这些关键数据的保护构成严重威胁。另一方面信息泄露的漏洞经常被攻击者利用间谍工具来收集被攻击目标各种信息，为真正的网络攻击方式、工具的使用提供情报。紧随其后的是缓冲区溢出漏洞和跨站攻击漏洞，缓冲区溢出在各种操作系统、应用软件中广泛存在。利用缓冲区溢出攻击，可以导致程序运行失败、系统宕机、重新启动等后果，甚至可以利用它执行非授权指令，对工业现场的智能设备下发非法指令（例如修改运行参数、关闭阀门开关等），以达到其攻击目的。工控系统中的跨站攻击漏洞主要体现在现场设备的WEB管理界面漏洞，利用该漏洞，攻击者可以盗取现场工程师或操作员的账号信息，并利用盗取的身份信息进行非法操作，或者利用该漏洞使工程内部工作人员成为病毒扩散的载体，协助其快速扩散到攻击目标。

另外值得一提的是密码类漏洞明显增多（该类漏洞在信息网的漏洞中已经并不多见），主要包括密码存储和传输过程中未做加密和编码变换的处理，让攻击者很容易就能获取管理密码。

漏洞的补丁发布严重滞后

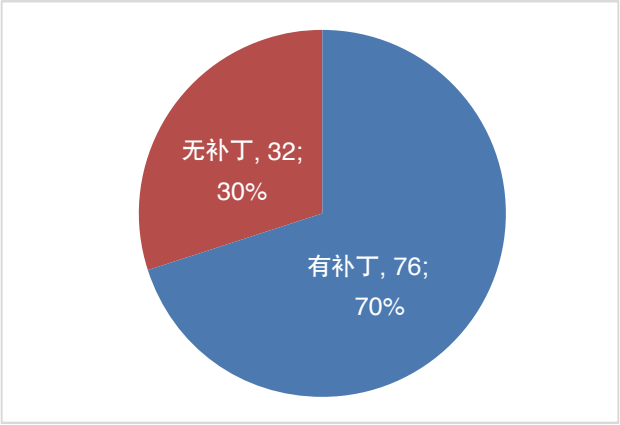


图3-5 有无补丁的漏洞统计（数据来源：CNVD）

从发布的数据看，2015年发布的新增漏洞，有30%的漏洞在发布的时候相关厂家并未提供补丁，也就意味着向所有人通告，这里有一个敞开的大门，可以随意做任何事情，这对于工控系统是非常危险的事情。发现漏洞并打补丁在信息安全领域是安全防护工作的常态，但在工控安全领域却经常面临着发现了漏洞却无补丁的尴尬状态。例如某厂家的RTU的加密算法中存在安全漏洞，而没有该漏洞的补丁，那么攻击者则可以很容易的利用该漏洞获取通信信息，甚至伪造控制命令。

3.2 我国工控网络安全形势更加严峻

conficker病毒仍在石化企业内作乱

在石化行业，conficker病毒感染了多个工控系统并造成严重危害。该病毒在工控网络中正在实时寻找外联途径，一旦满足通信外联条件，将造成感染主机被远程控制、服务器和控制器通讯中断、关键数据被盗取等危害。2015年，匡恩开展了某石化装置工控系统的安全检测与加固项目，检测结果确认其DCS系统中感染了“Conficker”蠕虫病毒。

Vxworks设备接入在互联网数量惊人

VxWorks操作系统是美国WindRiver公司于1983年设计开发的一种嵌入式实时操作系统，是嵌入式开发环境的关键组

成部分。它以其良好的可靠性和卓越的实时性被广泛地应用在通信、军事、航空、航天等高精尖技术及实时性要求极高的领域中，如卫星通讯、军事演习、弹道制导、飞机导航等。鉴于VxWorks应用在军工和工控的关键领域，如果使用该系统的主机IP可通过互联网直接访问，且存在较多高危漏洞，对于工控系统和设备很危险的。

2015年7月初，匡恩网络对国内互联网中暴露的VxWorks系统进行了调研，发现了运行着VxWorks系统的16202个IP。这些主机中有11304个运行FTP服务，占总数的70%，其FTP 220响应报文中暴露了VxWorks的系统版本号、FTP支持的命令列表等信息；另外有4291个运行SNMP服务，占总数的26%。

这些主机运行的VxWorks版本分布在：4.2.x、5.3.x、5.4.x、5.5.x，并未发现VxWorks 6以上的版本。低版本的VxWorks系统中存在着较多漏洞，如：WDB代理调试的漏洞、loginDefaultEncrypt算法加密漏洞、FTP守护程序访问控制漏洞等。以WDB代理调试的远程内存读取漏洞为例，匡恩对16202个IP做了详细探测，发现1763个VxWorks系统存在该漏洞（占总数的11%），可利用WDB服务远程读取内存映像。这些内存映像中存在明文的用户名、密码等关键信息，攻击者可以利用这些信息获取VxWorks系统的控制权。该漏洞影响的行业包括电力、石油、医疗、通信、军事、航空、航天等领域。

国内PLC设备接入互联网情况仍存在

2015年7月，匡恩网络对国内互联网中暴露的工业控制设备进行了调研，发现吉林、北京、江苏、上海等沿海工业发达地区暴露的PLC设备较多，设备厂商主要是漏洞数量最多的知名自动化厂商，如Siemens、Schneider、Rockwell、Omron等。以Siemens的PLC设备为例，发现其主要集中在东部沿海和东北地区。如果这些设备暴露在互联网上，意味着攻击这些控制系统网络的难度非常小，成本非常低。所以这些工控系统的风险极高，值得注意。

3.3 我国2015工控网络安全政策

2015年，我国的网络安全基础工作进一步深化，政策环境明显改善，关键基础设施风险评估和安全保障、新兴信息技术安全预警工作取得了突破性的进展。国家信息通报机制得到进一步完善，积极开展了专题研究和技术检测工作。

国内工控网络安全管理

中央机构编制委员会办公室于2015年4月20日颁布《中央编办关于工业和信息化部有关职责和机构调整的通知》（中央编办发〔2015〕17号），明确了工业控制系统安全管理的机构及工作职责。

《通知》内容表明，我国工业控制系统与信息安全规划、政策及标准的拟定、组织实施，工业控制系统安全审查、网络安全防护及应急管理和处置等均属于工业和信息化部的职责所在，具体则由工业和信息化部信息化和软件服务业司承担

相关工作任务。基于此，信息化和软件服务业司负责“统筹指导工业领域信息安全；研究拟定工业信息安全和信息安全产业发展战略、规划、政策和标准；指导做好重要工业领域工业控制系统安全保障工作；指导协调信息安全技术、产品研发及产业化”，并设系统安全处开展具体工作。

国家网络安全法（草案）

2015年6月，第十二届全国人大常委会第十五次会议初次审议了《中华人民共和国网络安全法（草案）》，并将其在中国人大网公布，向社会公开征求意见。

网络安全法的指导思想是：坚持以总体国家安全观为指导，全面落实党的十八大和十八届三中、四中全会决策部署，坚持积极利用、科学发展、依法管理、确保安全的方针，充分发挥立法的引领和推动作用，针对当前我国网络安全领域的突出问题，以制度建设提高国家网络安全保障能力，掌握网络空间治理和规则制定方面的主动权，切实维护国家网络空间主权、安全和发展利益。

为了保障关键信息基础设施安全，维护国家安全、经济安全和保障民生，草案设专节对关键信息基础设施的运行安全作了规定，实行重点保护。范围包括基础信息网络、重要行业和领域的重要信息系统、军事网络、重要政务网络、用户数量众多的商业网络等。并对关键信息基础设施安全保护办法的制定、负责安全保护工作的部门、运营者的安全保护义务、有关部门的监督和支持等作了规定。（草案第二十五条至第二十九条、第三十二条、第三十三条）

国家网络安全法草案作为建设网络强国的制度保障，为工业控制系统安全既带来了机遇，也带来了挑战。机遇方面，随着国家网络安全法草案公开征求意见及后续将要开展的进一步工作，工业控制系统安全行业将更加有序、更加有章可循，相关工作也会更加规范地开展和实施。所涉及的相关组织机构、人员等的重视程度、意识形态也将得到明显的改善和提升；挑战方面，也正是因为相关工作需要更加有序、规范的进行，要求相关组织机构、人员等必须不断完善工作制度，不断提升工作要求，依章、依规、依法开展工业控制系统安全工作。

行业网络安全发展政策介绍

各行业密切跟踪网络安全发展动态，紧密围绕国家信息化和信息安全发展战略，实施了一系列安全措施和举措，逐步提升了信息安全防护水平。2015年4月国家能源局发布了《电力企业网络与信息安全专项监管报告》。报告显示，电力企业网络与信息安全形势保持了持续稳定态势，保证了电力行业重要信息基础设施安全、稳定、高效运行。

石油石化行业的信息化经过多年的持续建设，已经行成覆盖其上中下游全部企业、一体化的网络系统以及配套的信息化基础设施平台，信息系统已经成为其生产运营和经营管理的“中枢神经系统”。

2015年，工业控制系统信息安全总体形势并不乐观。工业控制系统面临的安全威胁持续增长，工控安全漏洞仍处高发状态，针对工控网络的APT攻击明显增加，已对工业生产运行造成“实质性”影响。工业领域虽已关注工控系统的信息安全问题，但受限于工业环境特殊性、安全防护技术成熟度、基层人员安全意识等多种因素的限制，目前我国工业控制系统的信息安全防护水平较为薄弱，相对前几年状况并未好转。随着“互联网+”、物联网、智能制造、智慧城市、车联网等各种创新应用不断发展和深入，工业控制系统未来面临网络攻击风险将进一步加大。自2010年震网病毒以后，工控信息安全事件数量居高不下，针对工控系统的APT攻击逐渐增多。工控核心硬件漏洞数量增长明显。漏洞已覆盖工控系统主要组件，主流工控厂商无一幸免。继2014年全年发生多起重大工控APT攻击事件之后，2015年更是在工业控制系统核心设备中发现了木马和预置后门，工控APT攻击已成为现实威胁。

继德国西门子提出工业4.0、美国提出工业互联网之后，2015年5月8日，国务院正式发布《中国制造2025》规划，提出了中国制造强国建设三个十年的“三步走”战略。规划要求推进信息化与工业深度融合，加快推动新一代信息技术与制造技术的融合发展，把智能制造作为两化深度融合的主攻方向。尽管工控信息安全问题已得到世界各国普遍重视，但在工业生产环境中如何落实信息安全管理和技术却没有切实可行的方法，工控信息安全防护面临着“无章可循”，工控信息安全标准已迫在眉睫。当前，无论是国外还是国内，工控信息安全标准的需求非常强烈，标准制定工作也如火如荼在开展，但目前成果还极为有限。从总体上看，我国工业控制系统信息安全标准化工作正积极稳步推进，拟逐步形成涵盖安全管理、系统安全防护、产品安全评估等全面的工控信息安全标准体系，但工控系统的特殊性导致目前工控安全技术和管理仍处探索阶段，目前绝大多数标准正处于草案或征求意见阶段。工控安全防护技术开始试点，但离大规模部署和应用有一定差距。当前许多信息安全厂商和工控自动化厂商纷纷研究工业控制系统的信息安全防护技术并开发相应产品，近几年出现了一系列诸如工控防火墙、工控异常监测系统、主机防护软件等产品并在部分企业进行试点应用。

4 国内外工业控制网络安全事件分析

在信息技术与传统工业融合的过程中，工业控制正面临越来越多的网络安全威胁，2014年工控用户在生产中发生网络安全事故的比例有所提升，受网络安全事件影响的企业由13年的25%上升到2014年的28.6%，因病毒事件造成的工控网络停机的企业高达19.1%。

2015年仅美国ICS-CERT就收到了295起针对关键基础设施的攻击事件，更多的工业控制网络安全事件秘而不宣，但每一起走到世人面前的都让人震惊。以下将针对2015年典型的工业控制网络安全事件进行分析。

4.1 国内工业控制网络安全事件

某电力公司感染Welchia蠕虫

2015年3月，某南方电网部分无人值守变电站出现数据采集中断告警的现象，该公司委托匡恩网络对其现网数据进行分析，并调查问题产生的原因。检测结果发现其流量中存在着大量的TCP RST报文和异常的ICMP的PING流量。通过对这些异常的ICMP的流量分析，发现其业务网络中的终端服务器上的Windows系统感染了“Welchia”蠕虫病毒。该病毒利用特殊的ICMP的PING来发现局域网中的其他存活主机，并尝试传播感染。

该病毒影响的系统为Windows XP和Windows 2000等基于NT内核的操作系统，涉及电力行业变电与配电的工控主机。

该病毒溯源为Welchia蠕虫，全名W32.Welchia.Worm。它会利用DCOM RPC的漏洞MS03-026、MS03-039来攻击目标机的TCP 135端口；并利用WebDav的漏洞MS03-007来攻击TCP 80端口。Welchia蠕虫试图清除冲击波蠕虫，它会试图下载并安装来自微软升级网站的补丁程序并重启计算机，这会导致网络速度减慢甚至瘫痪。

某石化企业感染Conficker蠕虫病毒

2015年3月，匡恩网络应邀开展对某石化3#酮苯装置Honeywell（霍尼韦尔）TPS工业控制网络的安全检测与安全加固项目，采用我国工控网络安全领域领先的技术和工具，从实时在线运行的石化行业典型DCS（分布式控制系统）中捕获通信数据进行深入解析，在不影响该系统正常运行的情况下发现Conficker蠕虫病毒。所幸的是由于该病毒尚未与互联网上的病毒服务器交互成功，故没有进行通过网络的传播行为，也尚未产生严重危害。但值得警惕的是，该病毒在工控网络中正在实时寻找外联途径，一旦满足通信外联条件，如管理疏忽插入U盘、使用无线网卡等，甚至是正常的远程调试，即可接受互联网上病毒服务器的指令，进行病毒传播、关键数据盗取等一系列恶意操作。

该病毒影响的系统为Windows XP SP3英文版，涉及某石化3#酮苯装置（酮苯脱蜡脱油装置）于2000年左右上线的老旧系统。

Conficker蠕虫最早于2008年11月20日被发现，以微软的Windows操作系统为攻击目标。它借助互联网或USB设备传播，其C&C服务器（远程命令和控制服务器）多数位于美国。

值得注意的是，该生产过程是石化系统生产过程中不可或缺的关键环节，具有普遍性。在石化行业因感染该病毒对工控系统造成危害的并非个案，国内多家石化企业曾由于感染该病毒，导致部分服务器和控制器通讯中断，对生产造成了巨大影响。

海康威视安全事件

2015年3月1日，国内著名网络摄像头生产制造企业海康威视遭遇“黑天鹅”安全门事件，“监控设备存在严重安全隐患，部分设备已经被境外IP地址控制”。经分析海康威视安防监控设备主要存在以下三个方面安全风险：一是容易被黑客在线扫描发现。黑客至少可以通过3种方式探索发现海康威视安防监控产品：通过百度、Google等网页搜索引擎检索海康威视产品后台URL地址、通过Shodan等主机搜索引擎检索海康威视产品HTTP/Telnet等传统网络服务端口关键指纹信息、通过自主研发的在线监测平台向海康威视产品私有视频通讯端口发送特定指令获取设备详细信息。二是弱口令问题普遍存在，易被远程利用。据监测统计，有超过60%的海康威视产品的root口令和web登陆口令均为默认口令。三是产品自身存在安全漏洞。海康威视产品在处理RTSP协议（实时流传输协议）请求时缓冲区大小设置不当，被攻击后可导致缓冲区溢出甚至被执行任意代码。此次事件，凸显了安防行业乃至整个工控行业面临的严峻的网络安全挑战。相关工作人员的安全意识亟待提升，整个行业的网络安全技术水平亦需要全方位的改善和提高。

某石化SCADA安全事件

2015年5月23日，上海市奉贤区人民法院宣判了一起破坏中石化华东公司SCADA系统的案件。一名犯罪嫌疑人为中石化华东公司SCADA系统设计了一套病毒程序。而另一名犯罪嫌疑人则利用工作便利，将此病毒程序植入到华东公司SCADA系统的服务器中，并最终导致病毒爆发，系统无法正常运行。面对系统的崩溃，软件公司先后安排十余名中外专家前来维修都无功而返。此时，两名嫌疑人再里应外合，由公司内部的嫌疑人推荐开发病毒程序的嫌疑人前来“维修”，从而赚取高额维修费用，实现非法牟利。此次事件，充分暴露出工控现场网络安全管理制度、防护措施的严重缺乏，相关工作人员网络安全技术水平、防范意识不足等一系列问题。

4.2 国外工业控制网络安全事件

德国钢厂网络攻击事件

2014年12月，德国联邦信息安全办公室（BSI）发布了一份2014年信息安全报告，公布了德国一家钢铁厂遭受高级持续性威胁（APT）网络攻击并造成重大物理伤害。攻击者使用鱼叉式钓鱼邮件和社会工程手段，获得钢铁厂办公网络的访问权，然后利用这个网络，设法进入到钢铁厂的生产网络。攻击者的行为导致工控系统的控制组件和整个生产线被迫停止运转，由于不是正常的关闭炼钢炉，从而给钢铁厂带来了重大的破坏。

SCADA系统攻击事件

2014年12月，Joe Weiss公布了位于伊利诺斯州的Curran-Gardner乡镇公共供水区的水SCADA系统遭到网络攻击的消息，因而掀起一阵风波。这已是南休斯顿市第二个被黑客攻击的水厂。据悉攻击者破坏了管理或制造Curran-Gardner使用的SCADA系统的公司的IT系统，同时还窃取了用户名和密码。然后攻击者利用这些信息侵入Curran-Gardner的SCADA系统。

Laziok木马

2015年4月2日，赛门铁克公司发表声明称，发现了一个针对能源行业的木马程序，赛门铁克称之为Laziok。该木马能够收集目标机器的数据然后发送到制作者的服务器端进行分析，来决定要不要进行进一步的入侵。其主要针对石油、天然气等能源行业。

波兰航空公司安全事件

2015年6月21日，波兰航空公司的地面操作系统遭遇黑客攻击，致使出现长达5小时的系统瘫痪，至少10个班次的航班被迫取消，超过1400名旅客滞留在华沙弗雷德里克·肖邦机场。这是全球首次发生航空公司操作系统被黑的情况。好在这次黑客攻击活动只侵入了地面操作系统中的航班出港系统，未造成进一步的严重损害。这次黑客事件也提醒全球航空业以及同行运营商，黑客技术已经具备入侵航空系统核心部分的能力。

乌克兰电网攻击事件

2015年12月23日，乌克兰至少有三个区域的电力系统被具有高度破坏性的恶意软件攻击并导致大规模的停电，伊万诺-弗兰科夫斯克地区，有超过一半的家庭（受影响的人口数量约为140万）遭受了停电的困扰，而且整个停电事件持续了

数小时之久。在发电站遭受黑客攻击的同一时间，乌克兰境内的其它多家能源公司也遭受到了黑客有针对性的网络攻击。

据乌克兰新闻通讯社TSN报道，黑客在乌克兰国家电网中植入了恶意软件，该恶意软件断开了电气变电站的电路链接，其间多座变电站处于离线状态，从而导致大规模停电。如果被证实，那么此次停电事件将是第一个已知的有人故意使用恶意软件从而引起停电的实例。

图4-1乌克兰电厂

在此次攻击中，攻击者在微软Office文件（一个xls文档）中嵌入了恶意宏文件，并以此作为感染载体来对目标系统进行感染。

攻击者通过钓鱼邮件的方式，将恶意文档以附件形式发送到乌克兰国家电网内部人员，目标用户在接收到这封含有恶意文件的钓鱼邮件之后，系统就会被病毒感染。攻击者将该邮件的发送地址进行了伪装，使用户认为这些邮件是来自于Rada（乌克兰议会）的。在恶意文件中，还包含一些文字信息，这样才能欺骗用户来运行文档中的宏。

如果攻击者成功地欺骗了目标用户，那么他们的计算机系统将会感染BlackEnergy恶意程序，再通过BlackEnergy释放出具有破坏性的KillDisk组件和SSH后门。KillDisk插件能够破坏计算机硬盘驱动器中的核心代码，并删除指定的系统文件。利用SSH后门黑客可通过一个预留的密码（passDs5Bu9Te7）来远程访问并控制电力系统的运行。

Killdisk恶意软件的运行过程如下：

- 接收时间参数作为定时攻击触发器。
- 通过ShellExecuteW执行cmd命令创建服务，以实现服务运行。
- 当以服务形式运行时，此组件仅仅以LocalService参数运行。

运行过程中，不断查询注册表中保存的定位配置信息，与当前时间比较，判断是否可进行攻击，如果攻击被触发，Killdisk组件会执行破坏活动。

乌克兰最大机场网络遭到攻击

基辅鲍里斯波尔机场是乌克兰最大的机场。它提供了乌克兰约65%的航空客运量，每年进出港超过800万人次。机场连接亚洲，欧洲和美洲的许多空中航线的交叉点，大约有50家国内和国外航空公司和机场通航，客运和货运有100多条定期航线。乌克兰政府发言人安德烈·李申科（Andriy Lysenko）表示：“国家特种通信服务专家阻止了来自俄罗斯黑客攻击的可能性。”

援引俄罗斯国际文传电讯社消息称“昨天，通讯专家认为机场里面一个工作站是被Black Energy病毒感染，而之后连接机场的计算机网络被断开，目前CERT-UA团队安全专家已经通报了这件事情。”

2015年12月23号发生的持续三个小时的停电事故，最后导致伊万诺-弗兰科夫斯克（Ivano-Frankivsk）、Horodenka、卡卢什（Kalush）、多利纳（Dolyna）、Kosiv、Tysmenytsia、Nadvirna以及Yaremche regions等地区停电。当时乌克兰电力供应商Prykarpattyaoblenergo电话中心接到大量的电话。

而当时乌克兰计算机紧急响应小组（即CERT-UA）向信息安全媒体集团确认称，其目前正在针对此次停电进行调查，并发现黑客在此期间获得了对发电系统的远程接入能力。该小组同时确认称，BlackEnergy间谍木马与KillDisk恶意软件都在被入侵能源供应商的受感染系统当中出现。与之相伴的则是2015年12月23号发生的持续三个小时的停电事故，其间多座变电站处于离线状态，并直接导致约乌克兰国内西伊万诺至弗兰科夫斯克地区的约140万个家庭无电可用。

事件还在调查中。早前Eset公司安全威胁主管Anton Cherepanov曾指出，恶意软件编写者们正利用BlackEnergy木马的新型KillDisk组件对乌克兰境内多个未知机构进行攻击，且总计销毁了约4000种不同类型文件并导致相关设备无法重启。而攻击者们已经设置了一种延时执行命令，能够对35种文件类型加以清除，此外还针对其它Windows日志及设置文件，并会覆盖某些特定工业控制软件的可执行文件。

BlackEnergy最初于2007年被发现，其间经历了功能升级并借此由单纯的分布式拒绝服务攻击恶意软件转化为技术水平较高的模块化木马。ESET公司已经查明有位于乌克兰及波兰的多个目标受到已知及未知安全漏洞及向量的攻击影响。

CERT-UA（乌克兰计算机紧急响应小组）成员也建议系统管理人员查看系统日志，并注意软件异常行为。目前该网络攻击事件仍然在调查，但Andriy Lysenko表示这次的网络攻击事件和之前的事件有很多相同之处。

匡恩网络安全实验室正在紧密跟踪此事件，并就BlackEnergy对我国工业控制网络安全潜在影响进行分析评估。

4.3 工控系统近期活跃的病毒木马

Havex病毒

影响行业：水电、核电、能源

Havex被编写来感染SCADA和工控系统中使用的工业控制软件，是通用的远程访问木马，近来被用于从事工业间谍活动，主要攻击对象是欧洲的许多使用和开发工业应用程序和机械设备的公司。这种木马可能有能力禁用水电大坝、使核电站过载、甚至可以做到按一下键盘就能关闭一个国家的电网。

Havex被命名为W32/Havex.A，存在超过88个变种，其通信用的C&C服务器多达146个，并且有1500多个IP地址向C&C服务器通信。2014年8月之后其变种配备了一个新的组件，其目的是通过利用OPC DA协议来收集网络和联网设备的信息。

OPC DA是一种基于Windows操作系统的DCOM通信扩展的应用标准，它允许基于Windows的SCADA应用与过程控制硬件进行交互。该恶意软件会扫描本地网络中会对OPC DA请求作出响应的设备，以搜集工业控制设备的信息，然后将这些信息反馈到C&C服务器上。除此以外，它也包含从受感染系统收集数据的信息收获工具，比如：

- 操作系统的相关信息。
- 凭证获取工具，用来窃取存储在开发Web浏览器的密码。
- 使用自定义协议进行不同C&C服务器之间通信的组件，并在内存中执行有效载荷。

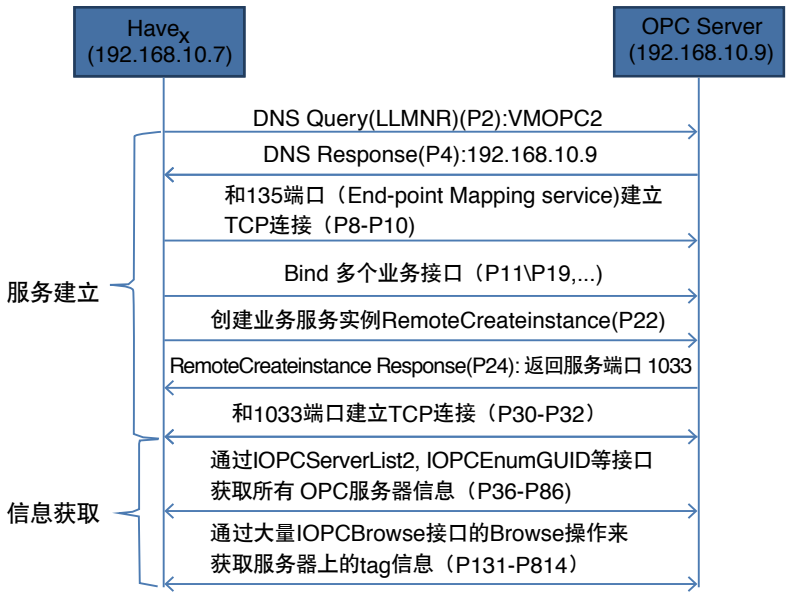
Havex利用合法的OPC DA标准指令来收集网络和联网设备的信息，通讯行为分析如下图所示。

病毒传播途径

- 垃圾邮件
- 漏洞利用工具
- 通过被入侵的厂商主站，将木马植入相关厂商产品的软件升级包

病毒来源分析

网络安全公司CrowdStrike披露了一项被称为"Energetic Bear"的网络间谍活动，该报告称Havex有可能以某种方式被俄罗斯黑客连接，或者由俄罗斯政府资助实施。



Sandworm沙虫病毒

影响行业：电信、能源

Sandworm沙虫病毒利用的漏洞几乎影响所有微软Windows Vista以上装有MS Office软件的系统主机操作系统，通俗地说，这类攻击是通过发送附件文档的方式发起，受害者只要打开文档就会自动中招，也就是只要电脑中安装了MS Office软件，都有可能受到该漏洞的影响。轻则信息遭到窃取，严重的则成为高级可持续威胁的攻击跳板，该漏洞还绕开常见的杀毒软件的特点，漏洞风险性较高。

TrendMicro报告发现Sandworm发起后续攻击的恶意载荷包含了对工控企业的人机界面软件的攻击（主要是GE Cimplicity HMI），目的是进一步控制HMI，并且放置木马。该攻击利用了GE Cimplicity HMI软件的一个漏洞，打开攻击者恶意构造的.cim或者.bcl文件允许在用户机器上执行任意代码，以及安装木马文件。.cim或者.bcl文件是Cimplicity的工程文件。

病毒传播途径

- 直接通过攻击连接在网络上的GE Cimplicity软件来打开含有恶意代码的cim文件。
- 通过发送钓鱼攻击，诱使用户打开含有恶意代码的cim文件。

病毒来源分析

国外厂商iSIGHT Partners 2014年10月14日发布公告称，俄罗斯黑客利用微软Windows系统中的SandWorm（沙虫）漏洞对欧美国家政府、北约，以及乌克兰政府展开间谍活动。

韩国核电站格盘病毒

影响行业：核电

格盘病毒分为两部分，一部分是系统的感染程序，一部分是MBR区的改写程序。

• 感染程序的行为概括如下：

结束指定进程，删除注册表中“安全模式”相关的项，使系统无法进入安全模式；映像劫持，在用户执行被劫持的程序时，会运行指定的程序。

篡改系统文件，关闭Windows系统文件保护，病毒在修改系统文件之前会执行该操作；查找安全软件进程，运行后删除自身，利用输入法机制，注入文件到指定进程。

• MBR区的改写程序行为概括如下：

修改磁盘MBR，该手法常被病毒用于获取更早的控制权。

查找安全软件进程并终止。

提升系统权限。

启动指定服务。

查找指定进程。

图4-2 韩国核电厂

病毒传播途径

通过发送钓鱼邮件，使用了大量的社会工程学诱使受害者打开这些文件。

病毒来源分析

2014年12月21日，一名黑客通过Twitter向韩国水电与核电公司发出严重警告，要求官方立即停止运行核电站。同时黑客还公开了包括两座核电站部分设计图在内的4份压缩档案。这次事件中所用的木马是“格盘病毒”（MBR Wiper）。在闹得沸沸扬扬的针对索尼影视的攻击中，黑客使用的正是“格盘病毒”。

方程式组织

影响行业：工业、军事、能源、通信、金融、政府等基础设施和重要机构

作为史上最强的网络攻击组织，“方程式”拥有一个庞大而强悍的攻击武器库。传统的病毒往往是单兵作战，攻击手段单一，传播途径有限，而“方程式”动用了多种病毒工具协同作战，发动全方位立体进攻，是名副其实的最强网络攻击工具。

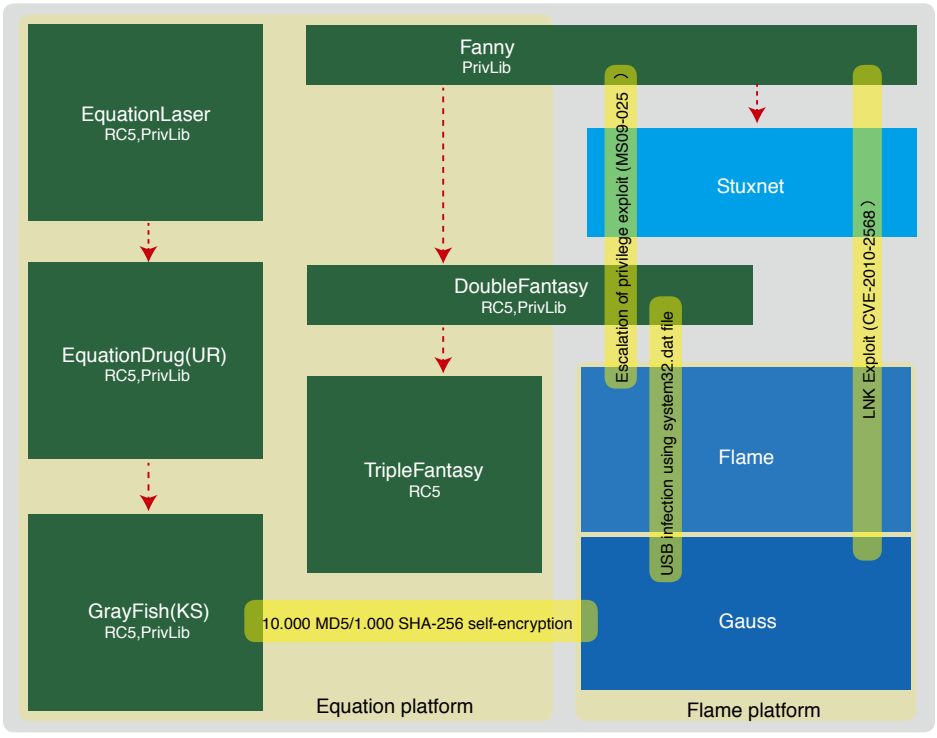


图4-3 “方程式”组织病毒家族

表4-1 “方程式”组织病毒家族分析

组件名称	说明	时间
EquationLaser	方程式组织早期使用的植入程序，大约在2001至2004年间被使用。兼容Windows 95/98系统。	2001-2003
EquationDrug	方程式组织使用的一个非常复杂的攻击组件，用于支持能够被攻击者动态上传和卸载的模块插件系统。怀疑是EquationLaser的升级版。	2003-2013
DoubleFantasy	一个验证式的木马，旨在确定目标为预期目标。如果目标被确认，那么已植入恶意代码会升级到一个更为复杂的平台，如Equationdrug或Grayfish。	2004-2012
TripleFantasy	全功能的后门程序，有时用于配合Grayfish使用。看起来像是Doublefantasy的升级版，可能是更新的验证式插件。	2012-至今
Fanny	创建于2008年的利用USB设备进行传播的蠕虫，可攻击物理隔离网络并回传收集到的信息。Fanny被用于收集位于中东和亚洲的目标的信息。一些受害主机似乎已被升级到DoubleFantasy，然后又升级为Equationdrug。Fanny利用了两个后来被应用到Stuxnet中的0day漏洞。	2008-2011
GrayFish	方程式组织中最复杂的攻击组件，完全驻留在注册表中，依靠bootkit在操作系统启动时执行。	2008-至今

“方程式”的典型攻击路线是：首先，诱使用户点击某个网站链接。当用户上当点击后，病毒就会被下载到用户电脑、或iPhone、iPad等手持设备上。

然后，病毒会将自己隐藏到电脑硬盘之中，并将自己的藏身之处设置为不可读的，避免被杀毒软件探测到。隐藏起来的病毒，就是“方程式”攻击的核心程序：“Grayfish”。这是一个攻击平台，其它攻击武器都通过该程序展开。它会释放另一些程序，去收集用户的密码等信息，发送回Grayfish储存起来。

同时，病毒也会通过网络和USB接口传播。病毒修改了电脑和手持设备的驱动程序，一旦探测到有U盘插入，病毒就会自动传染到U盘上，并且同样把自己隐藏起来。当U盘又被插入到另一个网络，例如一个与外界隔离的工控网络，病毒就被引入到那个网络，并逐步传遍整个网络。

以上攻击方式中，尤其值得一提的，是“方程式”开创了入侵硬盘的病毒技术。当它感染用户电脑后，会修改电脑硬盘的固件程序，在硬盘扇区中开辟一块区域，将自己储存于此，并将这块区域标记为不可读。这样，无论是操作系统重装，还是硬盘格式化，都无法触及这块区域，因此也就无法删除病毒。只要硬盘仍在使用，病毒就可以永远存活下去，并感染其所在的网络、以及任何插入该电脑的U盘。

能够被“方程式”病毒修改固件程序的硬盘，包括希捷、西数、三星、迈拓等十几种主流品牌，覆盖了市面上绝大多数硬盘。因此，绝大多数电脑或手持设备，只要接触到“方程式”病毒，就会被它入侵硬盘，并且永远无法删除。

“方程式”病毒另一个可怕之处，在于其特别擅长攻击隔离网络，并在隔离网络和互联网之间传送信息。所谓隔离网络，是指那些隔离开来、与互联网并不直接连通的网络。隔离网络广泛应用于工业控制之中，用以隔绝在互联网上泛滥成灾的病毒。

方程式组织的武器库中的Fanny蠕虫，创建于2008年，它利用USB设备进行传播蠕虫，可攻击物理隔离网络并回传收集到的信息。

方程式组织的武器库中的DoubleFantasy是攻击前导组件，它用来确认被攻击目标，如果被攻击的目标方程式组织感兴趣，那么就会从远端注入更复杂的其他组件。DoubleFantasy会检测13种安全软件，包括瑞星（Rising）和360。鉴于360安全卫士和瑞星的用户均在中国，这也进一步验证了中国是方程式组织的攻击目标之一。

病毒传播途径

- 诱使用户点击某个网站链接，当用户上当点击后，病毒就会被下载到用户电脑、或iPhone、iPad等手持设备上。
- 修改电脑硬盘的固件程序，在硬盘扇区中开辟一块区域，将自己储存于此，并将这块区域标记为不可读。
- 病毒也会通过网络和USB接口传播。

病毒来源分析

2015年2月16日，卡巴斯基实验室披露，他们发现了一个活动了二十多年的网络犯罪组织：“方程式”。这不是一个普通的黑客集团，根据卡巴斯基的分析，该组织的攻击能力和危害程度，超过了此前我们所知道的所有犯罪团伙。“方程式”是一个非常活跃的犯罪集团。二十年来，倒在他们枪口下的牺牲品不计其数，遍布全球四十多个国家，例如伊朗、俄罗斯、美国、德国、巴基斯坦、印度等。中国也是“方程式”的重点目标，是感染率最高的国家之一，被卡巴斯基实验室列为重灾区。

BlackEnergy黑客工具

影响行业：电力、军事、通信、政府等基础设施和重要机构

BlackEnergy（黑暗力量）是一款自动化的网络攻击工具，被各种犯罪团伙使用多年，在俄罗斯的地下网络广泛流传。其客户端采用了插件的方式进行扩展，第三开发者可以通过增加插件针对攻击目标进行组合，实现更多攻击能力，比如有些人利用它发送垃圾邮件，另一些人用他来盗取银行凭证。BlackEnergy工具带有一个构建器builder应用程序，生成

感染受害者机器的客户端。同时该工具还配备了服务器脚本，用于构建命令及控制（C&C）服务器。这些脚本也提供了一个接口，攻击者可以通过控制僵尸机。该工具有简单易用的特点，意味着任何人只要能接触到这个工具，就可以利用它来构建自己的僵尸网络。

该恶意软件曾经于2008年俄格冲突期间被用来对格鲁吉亚实施网络攻击。2014年夏，乌兰克剧烈动荡之时，攻击者针对乌克兰政府对软件进行了改进，并利用它从乌克兰政府那里窃取情报。

病毒传播途径

攻击者在微软Office文件（一个xls文档）中嵌入了恶意宏文件，并以此作为感染载体来对目标系统进行感染。

攻击者通过钓鱼邮件的方式，将恶意文档以附件形式发送到乌克兰国家电网内部人员，目标用户在接收到这封含有恶意文件的钓鱼邮件之后，系统就会被病毒感染。攻击者将该邮件的发送地址进行了伪装，使用户认为这些邮件是来自于Rada（乌克兰议会）的。在恶意文件中，还包含一些文字信息，这样才能欺骗用户来运行文档中的宏。

如果攻击者成功地欺骗了目标用户，那么他们的计算机系统将会感染BlackEnergy恶意程序，再通过BlackEnergy释放出具有破坏性的KillDisk组件和SSH后门。KillDisk插件能够破坏计算机硬盘驱动器中的核心代码，并删除指定的系统文件。利用SSH后门黑客可通过一个预留的密码（passDs5Bu9Te7）来远程访问并控制电力系统的运行。（黑客攻击的是电力系统中哪类设备没有披露）。

攻击过程分析

Killdisk恶意软件的运行过程如下：

- 接收时间参数作为定时攻击触发器
- 通过ShellExecuteW执行cmd命令创建服务，以实现服务运行。
- 当以服务形式运行时，此组件仅仅以LocalService参数运行

运行过程中，不断查询注册表中保存的定时配置信息，与当前时间比较，判断是否可进行攻击，如果攻击被触发，Killdisk组件会执行如下破坏活动：

- 破坏系统连接所有硬盘数据，遍历所有硬盘设备PhysicalDrive%Num%（Num从0到10）并且直接向硬盘前256个扇区写零。
- 通过wevtutil工具清除日志。
- 查找指定后缀的文件并且使用随机数据来覆盖文件开头部分。

- 遍历进程，结束sec_service.exe并删除sec_sercice服务，向sec_service.exe中写入随机数据。sec_service.exe是被用于工业控制串口服务器转换程序。
- 通过执行shutdown命令关机，此时系统遭到严重破坏，关机之后已经无法重启，导致电力系统无法恢复运行，致使乌克兰出现大面积的断电事件。

病毒来源分析

这是一次有组织、有预谋的工业网络攻击事件。乌克兰的国家安全局（SBU）表示，俄罗斯的特工在乌克兰的国家电网中植入了恶意软件，导致发电站意外关闭。英国《金融时报》报道，乌克兰认为是俄罗斯组织通过网络攻击制造了本次停电事件。iSIGHT Partners认为是俄罗斯境内的黑客组织（沙虫）使用了BlackEnergy黑客工具，实施了本次网络攻击。

本次攻击事件显示出乌克兰国家电网的整体安全管理能力较弱。BlackEnergy是已知黑客工具，在2007年出现，2010年已经添加到病毒样本库。工作人员安全意识不强，通过钓鱼邮件轻易入侵。

本次事件显示出乌克兰国家电网的安全防御能力较弱，网络隔离被轻易绕过：通过钓鱼邮件感染信息网，进而感染在控制网的设备。控制操作被轻易执行，控制设备可能没有经过可信检查，控制指令的合规性也未得到检测。

5 我国工业控制网络安全趋势分析

国内的工控网络安全形势十分严峻，存在大量严重、紧迫、危险的问题，总体上来说：

- 工控系统广泛互联，逐步同生产管理、ERP系统、电子商务系统相连，纳入到统一的信息系统中但由此带来的信息安全问题并未得到充分认识和重视。
- 随着工业控制网络技术的发展，多工控系统集成、通过互联网/内联网/外联网进行Web访问等方式开始逐渐流行，工控系统直接暴露的风险也不断增加。
- 工控系统中采用的工业协议存在缺乏加密和认证等网络安全的考虑。
- 工业控制网络安全尚未纳入生产安全、信息安全检查的工作范围。
- 工控系统运行的环境存在大量漏洞和隐患：操作系统长期未升级、缺乏基本安全设置；与公用网络存在接口，相关安全机制存在安全隐患；野外设备普遍缺乏物理安全防护；远程无线通信系统缺乏接入认证和通信保密防护。
- 控制系统基础和核心设备严重依赖国外产品和技术。
- 生产工艺设计人员和控制系统设计人员几乎没有任何网络安全意识。
- 系统体系架构缺乏基本的安全保障。
- 系统外联缺乏风险评估和安全保障措施。
- 工业控制系统产品供应链方面，缺少针对工业控制设备的信息安全检测手段、标准和方法。

另外，工业控制网络具有很强的行业特性，每个行业都具有自身的特点，本报告将针对我国典型行业的工业控制网络安全进行分析。

5.1 城市轨道交通行业工控网络安全

城市轨道交通系统技术发展趋势分析

综合监控与信息系统一体化

按照发展新型工业和企业信息化的要求，自动化应该是集管理和控制于一体的，它包含底层的控制与高层次的管理自动化。企业信息化对系统的自动化程度提出了更高的要求，它包含了从经营管理层、生产执行层、过程控制层直到现场设备层的全过程，涵盖了从传感器开始到整个系统优化运行的全部底层控制及高层管理。为保证整个控制过程中的所有有用的信息不沉淀和流失，便于实现实时协调，加强对上层决策的辅助支持，应建立全局化的概念，统一信息平台，克服“自动化孤岛”、“信息孤岛”现象，实现管控一体化的无缝集成。

云主机和桌面云将运用于轨道交通综合监控系统

当前的综合监控系统在每个车站都部署两台服务器和数个工作站，这对一条线路的服务器和终端维护带来较大成本，如果综合监控前期在系统环境架构上考虑不足，在后期系统改造时会带来前期投资的损失，为了保障前期投资，现在针对地铁综合监控系统提出了采取云主机和桌面云的方式，这样既能保护现有投资，同时又能很好的满足以后综合监控集成ATS系统升级扩展的需要。据国内地铁综合监控系统技术标准权威人士消息，云主机和桌面的方案将写进2016年地铁综合监控技术规范修订版当中，这势必会推动云主机和桌面云在地铁信息系统中的运用。

LTE等4G通信技术将更多的运用到车地通信系统中

LTE技术具有通信速率高，频谱效率高，系统抗干扰能力显著提高，QoS保证CBTC业务系统部署灵活，能够支持多种系统带宽，高速度适应性，满足更高速度（大于200km/h）下的系统吞吐量性能。LTE技术具有的技术优势使得它相比WiFi技术更适合于进行综合业务承载，LTE技术在城市轨道交通领域的使用将更加广泛，也将迎来发展的黄金时期。

机电设备逐渐智能化实现设备自我诊断

随着城市地铁线网规模越来越大，地铁中的机电设备的数量越来越多，设备的监控和运维面临挑战，为了本质安全和节约成本的目的，将通过设备的在线监测和其他信号监测、状态监测诊断、定向风险评价、设备数据采集和分析、维修任务优化，从事后故障维修发展到预防维修和预知维修、在故障发生之前修理故障设备或替换损坏设备。在北京地铁和深圳地铁的多条线路上，已经开始采用智能仪表，减轻对人工经验的依赖。智能仪器仪表替代传统的人工巡检的方式的示意图如下。

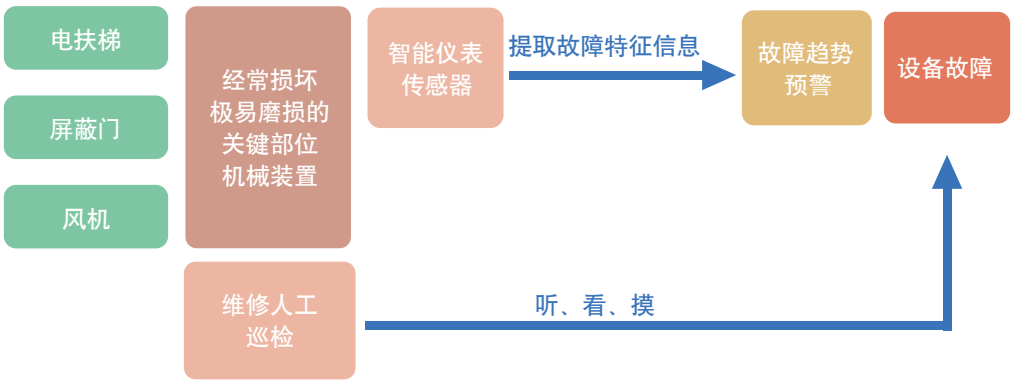


图5-1 智能仪表巡检方式示意图

综合监控系统与ATS将进一步集成

以行车调度指挥为核心的集成方式是城市轨道交通综合监控的发展方向，并且系统的集成度都得到进一步提高，实现

了对轨道交通中环境、供电、设备、乘客和列车的全面监控。提升整个轨道交通机电设备的整体运营性能，提供一些新的功能和手段，实现系统间快速联动和反应，提高轨道交通运营的安全性能。真正做到为运营指挥部门服务，提高轨道交通运营指挥自动化水平。

互联互通信号系统研发及应用进展迅速

随着国产化CBTC系统的成熟，实现各厂商信号系统互联互通成为可能，重庆地铁、北京地铁的业主都在牵头各信号厂商推进相关的标准编制及产品研发工作，重庆地铁业主已经以示范工程的方式开始互联互通信号系统工程实施，中国城市轨道交通协会也在全力推动这一技术的应用。

城市轨道交通工控网络安全趋势分析

综合监控与信息化系统一体，传统网络安全威胁将进入轨交的工控网络

地铁综合监控系统传统上大家都认为是一个相对比较封闭的、自成一体的网络系统，随着地铁企业管理决策层越来越依赖数据决策时，综合监控系统和上层企业ERP系统的对接将不断推进，综合监控也是越来越普遍的使用标准化系统平台和应用开放标准的网络协议，也即地铁综合监控系统通用会感染来自信息网络的恶意代码。地铁行业同样也面临两化深度融合的趋势，这一趋势容易被忽略。

智能仪器仪表或智能执行设备的引入，轨交工控系统的攻击路径发生反转，从下至上的攻击将发生

在工控控制系统环境中，仪器仪表和执行装置处在工控网络最下层，仪器仪表的数据采集将通过PLC等控制设备，然后再往上比如OPC服务器传送。随着智能仪器仪表和物联网的推进，智能仪器仪表在数据上传在走一条不同的路，即智能仪器仪表即接入PLC满足原来的数采要求，同时又直接连接到工业交换机上并连接到新的业务应用服务器上，满足仪器仪表自身维修和维护、业务优化等新业务需求。这个时候，我们看到对整个地铁的机电设备的组网结构发生非常大的变化，也即达到工控控制系统的核心部分即现场执行设备和控制设备有了两条网络路径，及上文所提到的从上之下和从下至上。

综合监控系统集成了ATS的功能，将导致综合监控系统的安全和可靠性面临更高要求

由于信号系统属于故障安全性系统，安全级别较高，ATS虽然不属于故障安全性系统，但和ATP/ATO系统联系紧密，因此，集成ATS后，综合监控系统直接负责行车指挥调度，要求综合监控系统的功能和可靠性更高。

传统上ATS虽然不是故障安全性系统，但仍具有安全相关功能，中途停车、取消临时限速、解除区间封锁或施工区等可能潜在地导致系统危害的操作，故其安全完整性等级是SIL2级。并且，与传统综合监控系统紧密集成后还可能产生新的安全相关功能。因此，当集成后的系统采用统一的硬件、统一的人机界面和统一的基础数据平台时，也要按照安全工程的要求，实施一个从需求到设计到实现贯穿完整生命周期的风险分析过程，包括初步危害分析、子系统危害分析、系统危害

分析和操作与支持危害分析（O&SHA）等。

由于ATS的安全完整性等级是SIL2级，因此业界普遍认为与综合监控系统集成后的目标系统的安全完整性也应是SIL2级。

云计算的安全问题在轨道交通领域将不断受到关注

随着云主机和桌面云在地铁综合监控系统中的部署应用，轨道交通领域将首次面云计算的安全问题。从面前来看，采取私有云的方式是应是轨道交通领域能够接受的云计算部署方式。私有云主要面临以下安全问题需要解决。

- 安全边界难以定义：在传统网络中通过物理上和逻辑上的安全域定义，可以清楚地定义边界和保护设备用户，但云计算由于其用户数量庞大，数据存放分散，很难充分为用户提供安全保障。
- 数据安全：目前在网络中用户基本采用数据加密方式共享数据，但在云计算环境下，如果能够将自己的数据与其他用户的数据隔离开可以更加有效地保证数据安全。因为所有客户数据将被共同保存在唯一一个软件系统实例内，所以需要开发额外的数据隔离机制来保证各个客户之间的数据的保密性并提供相应的灾备方案。

5.2 城市燃气行业工控网络安全

城市燃气工控系统技术发展趋势分析

城市燃气随着业务的飞速发展，同时人力成本的上升，管网的不断变长以及复杂话，原有的燃气工控系统的“监而不控”方式已经无法适应，原有的手工的巡检和抄表方式已经开始制约燃气系统的业务发展，城市燃气的智能管网技术的发展成为未来发展的趋势，智能管网技术指利用传感、嵌入式处理、数字化通信和IT技术，将管网信息集成到管道公司的流程和系统，使管网可观测（能够监测所有主要设备的状态）、可控制（能够控制所有主要设备的状态）和智能化（可自适应并实现智能分析策略），从而打造更加安全、环保、节能、经济、供需平衡的管网系统城市燃气的工控系统技术发展已经呈现以下几种趋势：

城市燃气管网调控智能化

城市燃气管网调控智能化自动化随着城市燃气行业的发展不断提高。输气管网系统已由最初的独立干线向集群管网方向发展，其输送过程将越来越复杂。及时、全面、准确地掌握整个管网的动态情况将是保障安全平稳输送的重要手段和措施，这些都为管线运行的调控提出了更高的要求。一方面，智能化管道建设发展，对自动化程度提出了更高的要求，要求其控制系统在控制、安全等方面有更高的可靠性、开放性；另一方面，调度和控制向着智能化方向发展，这也是的无人化门站和所站的持续增多。

物联网技术广泛应用

智能管网技术离不开物联网技术，其中就包括网络无线射频识别（RFID）系统——把所有物品通过射频识别等信息传感设备与互联网连接起来，实现智能化识别和管理。目前国内外企业就是使用RFID技术已经应用在设备及备件采购、仓库管理、设备维修等方面。而无线定位技术在现有GIS系统的深层利用下，在结合智能手机技术，开发便携式无线手持终端则应用在无线巡检、厂区定位等方面有更好的发展。另外可佩戴的气体传感器的应用，可以进一步提高城市燃气管道现场检修人员的生命安全保护能力以及应急抢救能。

将物联网技术应用于城市燃气管道设计、建设、运营、维护和管理的全过程，有利于促进管道的完整性管理和失效控制，提高管道运行的安全性和经济效益。物联网涉及的技术主要包括：无线、有线网络技术，传感器技术和智能终端技术。油气管道物联网建设的主要内容是通过传感器连接资产和设备，提高数字化程度；建立数据的整合体系，实现数据的综合分析与利用；基于业务需求开发智能化应用系统，实现对管道运营各个环节的优化管理。

智能仪表将广泛应用于智能管网中

作为智能管网的数据采集和业务执行的端点，智能仪表的采用是确定城市燃气是否真正智能的标识之一，智能仪表内置微处理器，具有一定的运算处理能力和精确的测量能力，一般具有以下特点：

- 精度高：智能仪表普遍采用嵌入式系统，具备一定的数据处理能力，数据测定精度高等特点。
- 功能强：能够依赖自身的微处理能力执行一定的业务功能，具有初步的自我诊断能力。
- 通信功能强：为了方便普及和节省人工，城市燃气的智能仪表普遍具有支持无限通信和有线通信技术，方便部署和数据采集以及执行命令。
- 较强的安全性：其仪器和芯片应该具有一定的防物理破坏和网络攻击的能力。

云计算将运用于城市燃气SCADA系统

在智能管网的计算平台中，云系统可以应用在IT基础设施、信息集成、分析应用等多个方面，降低信息化的成本，提高IT的灵活性和支撑能力。随着云计算技术的发展，IT资源的应用和共享方式发生了巨大的变化。企业私有云为智能管网数据集成与业务集成提供基础性服务，它用来解决目前国内企业信息化中普遍存在的数据孤岛和业务隔离现象。包括可以建立共享数据中心或者云服务平台。

城市燃气工控网络安全趋势分析

城市燃气工控网络安全技术从最早利用信息化升级改造的过程中，尝试使用用于传统IT环境的信息安全技术来解决工控网络的安全问题，发现问题并没有得到很好的解决，其中最主要的原因就是传统的信息安全技术不适用于城市燃气的工

业控制环境，这包括以下几点：

- 城市燃气工控网络使用不是传统的TCP/IP技术，而是工业以太网技术，在安全性和可靠性方面都与传统的网络技术存在差异；
- 站控系统环节，尤其PLC和RTU，甚至包括智能仪表，其多使用嵌入式操作系统，业务相对单一，无法采用传统的植入安全软件的方式保护工业控制网络；
- 城市燃气的工控系统多为国外厂商所垄断，所以安全措施由于协议约定的原因很难部署国外厂商非授权的安全产品；
- 多数城市燃气公司在部署工控系统时采用的是“监而不控”的技术，工控系统只采集数据，不直接对管网进行控制，而是通过派发工单，由人工方式进行现场操作，而且网络相对独立，所以轻易不会感染病毒，同时哪怕系统遭受攻击，很快可以使用手工方式来保障运行的安全。
- 城市燃气公司普遍信息安全意识薄弱，对网络安全的重要性认识不足也是原因之一。
- 随着智慧城市的建设以及智能管网技术的兴起，城市燃气公司的发展逐渐开始由封闭走向开放，原有的“监而不控”即将成为历史，但是处在开放的环境以及脆弱的防护体系下的工控系统，其工控网络安全呈现新的态势：
- 城市燃气的工控安全技术必须要适应企业的工业网络环境，包括能够解析工业网络协议，深度解析数据包和自我智能学习的能力；
- 城市燃气的工控系统本身的安全成为未来的主流，既要加强安全自主可控，使用国产工控系统，又要加强自身的安全防护；
- 智能管网最大的特点监控同时在网络上实时快速的实现，而且另外一个特点与企业的信息网络连接，这使得其暴露在威胁的可能性变大，城市燃气公司的业主已经开始意识到必须强化其保护措施。

由于工控安全技术普遍比较复杂，所以对于工控安全产品的要求既要能够保护工控系统的安全，也要简单可操作，这对城市燃气的工控安全产品提出了更高的要求。

5.3 智能汽车与车联网安全

智能汽车与车联网网络安全趋势分析

智能汽车与车联网的黑暗面之一，就是给违法者进入汽车内部网络的可趁之机：入侵GPS模块，黑客能掌握车主的所有行踪，或把车主导航到他想要车主去的地点；入侵安装摄像程序，可以拍下车主在车内的一举一动；入侵蓝牙电话系统，能够窃听车主的一言一语；入侵行车安全模块，就可以控制车的油门刹车……

事实上，与智能汽车、车联网相关的安全事件也呈现逐年增加的趋势：

2011年黑帽大会，研究人员仅仅利用手机对车内的无线设备发送文字信息，就使一辆斯巴鲁傲虎汽车的防盗器被破解、门锁被打开，引擎也正常发动起来。

2013年DefCon、Charlie Miller和Chris Valasek，对2010丰田普锐斯和2010福特翼虎进行了攻击。车辆静止的情况下令时速表爆表，让车辆在满箱油的状态下令油表灯报警。高速行驶的状态下令车辆自动急刹车、猛打方向、令制动踏板失效等等。

2014年7月，360公司专业团队研究了特斯拉（Tesla）ModelS型汽车后发现，特斯拉汽车应用程序流程存在设计缺陷。攻击者利用这个漏洞，可远程控制车辆，实现开锁、鸣笛、闪灯、开启天窗等操作，并且能够在车辆行驶中开启天窗。

2015年2月，美国国防部高级研究计划局（DARPA）的研究人员成功入侵了一辆雪佛兰Impala上的安吉星（Onstar）系统，并对车辆的刹车功能进行控制。这一举动再次提醒了人们那些拥有各种智能系统和传感器的汽车，在黑客面前仍然是不堪一击的。研究员在破解了安吉星应急通信系统之后，用庞杂的数据让原有系统崩溃，并输入控制车辆的代码，随后仅通过一台笔记本就可以远程控制车辆的刹车是否起作用。

2015年7月，两位研究人员演示了无线入侵Jeep切诺基的网络系统，在其行驶过程中，侵入Uconnect车载系统，远程通过软件向该系统发送指令，启动车上的各种功能，包括减速、关闭发动机、制动或让制动失灵，在之后的BlackHat上，两人面向全球黑客奉献了经典的汽车破解秀。首次让克莱斯勒因信息系统问题召回140万辆汽车，引爆全世界对汽车信息系统安全的关注。

从各种安全事件看，智能汽车与车联网的安全问题包括功能安全与网络安全两部分：

- 功能安全：目前汽车电子控制单元越来越多，传统中低档车汽车电子系统成本占整车成本18%左右，高级车占比达28%左右，而新能源汽车占比高达45%左右。汽车电子系统本身的功能安全在汽车安全中扮演越来越重要的角色。
- 网络安全：一旦智能汽车连接到互联网，相关的信息就面临安全风险，轻则泄露个人信息，重则影响行车安全；半自动驾驶、无人驾驶等技术有时会伴随若干不稳定的“非必要系统行为”，在严重的情况下将出现威胁到人身安全的后果。

2015年，Charlie Miller与Chris Valasek分析了21款车，涉及到奥迪、宝马、通用、福特、克莱斯勒、本田、丰田、英菲尼迪、路虎品牌及其旗下品牌车型，以2014年款为主，共13款，对比年款2006年款4个，2010年款3个，2015年款1个。从研究的内容中，他们得到了一些结论：

随着时间推进，所有品牌车型都表现出ECU（Electronic Control Unit，电子控制单元，又称“行车电脑”、“车载电脑”等）数量的增多，不仅是整体ECU数目，桥梁ECU数目更是大幅增加，功臣有两个：车联网与驾驶辅助技术的发展。也就意味着，车辆的被攻击可能性、可选择手段都在增加。

车内网络拓扑结构的复杂性随着ECU增多也在增加，被分割的网络架构越来越多。但是这些网络架构的分割并不都是以“将控制核心功能ECU与其他类ECU分开”为目的。在2014年款中，有6款并没有根据功能重要性不同进行隔离，而更多的，虽然隔离了，但是并不代表安全性就高。因为隔离之后并没有设置网关或者安全边界，没有增加安全策略，而只是单纯的分开。

尽管内部结构大不相同，但是大多数车辆都采用了类似PC的技术，比如浏览器和车内App等，这些都是黑客们十分熟悉的东西，提供了与PC、移动端类似的攻击方式。胎压监测与无钥匙进入系统最容易成为黑客远程攻击ECU的跳板。

同一地区的汽车制造商的内部拓扑图有着类似的结构，日系车（丰田与英菲尼迪）、德系车（奥迪与宝马）、美系车（通用与福特）之间都表现出来这个特性。两位研究员认为可能是因为他们思考问题的方式比较类似，还有就是工程师的跳槽。存在这些问题的车辆，都没有OTA（Over－the－Air Technology，空中下载技术）功能，发现问题只能召回处理。

智能汽车与车联网网络安全发展制约因素

从2015年的情况看，未来智能汽车与车联网网络安全发展的主要制约因素包括：

相关标准的缺失

与工业控制网络安全的相关标准类似，车联网的相关标准仍在制定之中。目前车联网产业仍属起步阶段，包括人车互联、车车互联、车与外部环境的互联仍未有一套业内公认和遵守的标准。应尽快制定中国车联网和智能汽车的发展战略、技术路线、相关标准。如车联网和自动驾驶的安全标准、云服务规划、数据安全和通讯协议等，并在交通执法、保险责任、黑客侵袭等方面制定相关的法律政策，为智能汽车的到来做好准备。

不过，在这一方面，顶层设计正在释放出积极信号。2015年底，工信部发布了《关于印发贯彻落实〈国务院关于积极推进“互联网＋”行动的指导意见〉行动计划（2015－2018年）的通知》，其中首度提及车联网未来发展规划，表示将会出台《车联网发展创新行动计划（2015-2020年）》，加快车联网产业布局，推动车联网技术研发、标准制定，组织开展车联网试点和基于5G技术的车联网示范，推动行业的整体发展。

从目前情况看，工控系统安全的相关标准进程是领先于智能汽车与车联网标准的，而如前所述，智能汽车与车联网具有工控系统的某些特征，因此未来可以借鉴工控系统安全相关标准。

企业对网络安全的重视程度

车联网之于车企其实比较鸡肋，鸡肋并不代表不重要，而是因为车企目前尚没有能力掌控车联网，车联网很大程度上需要引入互联网科技公司，而两者严格的说属于竞合关系，而且谁都想把握车联网的主导权。在此情况之下，车企往往以安全之名以令互联网科技企业，车企往往不开放协议，不开放数据，最终车联网进程缓慢。偶有的一小步，比如福特，其实是以车企为绝对主导的，很早就曾提出了互联网战略。而其他的车企，引入的一些应用，都还得严格按照车企的要求。

传统车企们的小心翼翼并非没有道理。一方面，网络基础条件并不完备，业内专家表示，想要真正支持“万物互联”，仍需移动互联网进一步发展，比如5G的建设和铺开。工业和信息化部无线电管理局局长谢飞波曾表示，5G将重点解决万物互联的问题，5G初期会选择从车联网切入，逐步解决人与设备，设备与设备的自动交互问题。

由于车联网是从端到云的统一整体，缺一不可，由于车联网中汽车智能化的部分是由车厂主导，然而目前汽车集成式的供应链形态决定其封闭性，很难建立起可持续发展的创新业务模式，造成平台与其他行业的信息割裂，信息无法共享，导致业务和应用开发成本较高，业务创新和研发速度缓慢，所以，对于开发者来说其开发应用和服务的积极性也相应降低。因此整车厂商对于车载信息终端的把控是整个车联网市场迅速发展的阻碍因素。

而与信息厂商相比，传统汽车厂商在网络安全领域无疑相对力量较弱，因此需要：

- 促进汽车网络安全审查机构建设，监管汽车行业网络安全发展；
- 促进产业链上下游合作，实现优势互补，完善行业网络安全发展环境；
- 适时成立联盟，加强行业公共服务，形成协同创新交流机制。

5.4 石油化工行业工业控制网络安全

石油化工行业网络安全分析

石油化工企业是典型的资金和技术密集型企业，生产的连续性很强，装置和重要设备的意外停产都会导致巨大的经济损失，因此生产过程控制大多采用DCS等先进的控制系统，DCS控制系统的供应商主要有霍尼韦尔、艾默生、横河电机、中控科技等。

在早期，由于信息化程度水平有限，控制系统基本上处于与信息管理层处于隔离状态。因此，石化企业的信息化建设首先从信息层开始，经过10多年的建设积累，石化&化工行业信息层的信息化建设已经有了较好的基础，涉及到了石油勘探、开发、炼油、化工、储运、销售、数据管理等诸多研究领域，企业在管理层的指挥、协调和监控能力，提高上传下达的实时性、完整性和一致性都有很大提升，相应的网络安全防护也有了较大提高。与其他行业一样，在信息管理层面，石

化石化企业大量引入IT技术，同时也包括各种IT网络安全技术，包括如防火墙、IDS、VPN、防病毒等常规网络安全技术，这些技术主要面向商用网络应用，应用也相对成熟。

与此同时，在信息技术不断发展的推动下，石化&化工企业的生产管理理念和技术也在不断发展，DCS发展到今天，已经进入了第四代，新一代DCS呈现的一个突出特点就是开放性的提高。石化&化工企业普遍开始采用基于ERP/SCM、MES和PCS三层架构的的管控一体化信息模型思想，随着两化融合政策的推进，越来越多的石化企业实施MES系统，使管理实现了管控一体化。

随着石化&化工企业管控一体化的实现，越来越多的控制网络系统通过信息网络连接到互联上，潜在的威胁就越来越大。在这种背景下，客观要求对于工业控制网络进行的网络安全防护显得尤为重要。

石油化工行业工控网络安全发展趋势

石化&化工行业是ICS普及度较高的行业之一，同时也是对ICS的稳定性和控制策略复杂性要求很高的行业。石化的ICS系统一旦出现故障，不仅造成巨大的经济损失和能源安全冲击，还会造成人身安全的影响。因此，石化行业对控制层的网络安全重视程度最高。随着石化&化工信息化建设，管控一体化项目的推进，越来越多的用户将对ICS实施安全防护。

2015年，中石油、中石化等用户正在组织研讨会，加强论证和探讨ICS网络安全在石油化工行业的实际应用推广方案优化工作，届时ICS网络安全在石油化工行业的推行将越来越落地。

5.5 冶金行业工控网络安全

冶金行业工控网络安全状况

目前冶金行业的生产管理领域，主要涉及生产过程控制自动化系统、生产制造执行系统、能源管理系统、信息系统等，这些系统在冶金企业的应用发展的成熟度，将成为决定冶金企业信息化和网络安全发展的基础。

生产过程控制自动化

生产过程控制自动化是冶金企业信息化的重要组成部分，是实施现代先进工艺的重要关键手段和保障条件。目前，冶炼过程控制自动化的系统技术除大型高炉和转炉的系统平台仍存在依赖于国外的情况外，其它基本上是外采配套PLC和DCS系统，自行开发应用软件。轧制过程自动化，特别是带钢冷热轧过程自动化，由于系统庞大，对控制速度、通讯速度要求高，大部分企业引进国外系统，部分企业采用自主设计、自主集成过程计算机控制系统，并自主开发控制模型及各项控制功能。目前，冶金行业的生产过程控制自动化已经相当成熟。

生产制造执行系统

生产制造执行系统是钢铁企业信息化体系结构中重要的组成部分，它是企业经营管理与生产控制的接合部。对于生产宽厚板、热轧板、冷轧板等高附加值的精品板材生产系统的钢铁企业，特别是一切按用户需求安排生产的产线，更重视MES的建设。近年来，许多钢铁企业积极建设MES，取得了重要的成果和经验。现阶段企业在车间级制造执行管理信息系统已普及，统计显示，全部或部分产线建设了车间级制造执行管理系统的企业比例已经超过80%。

能源管理系统

能源管理是钢铁企业实现优化资源配置、合理利用能源、改善环境，实现从单一的装备节能向系统优化节能的战略转变的重要措施，也是创建节约型企业、实施清洁生产的必然要求。目前，半数以上的冶金企业已经建设了能源管理系统。

信息系统

根据调查，95%以上的冶金企业已经建设了协同办公管理信息系统。

由于冶金行业各系统的不断完善，信息化建设也在不断提速，冶金企业每年对信息化的资金投入占销售收入比重呈上升趋势。在信息化快速发展的同时，冶金企业对于网络安全的关注度也逐年更高。但相对于信息建设的投入，冶金企业对于网络安全的投入相对较少，尤其针对ICS网络安全的投入就更加有限。

冶金行业工控网络安全发展趋势

冶金行业的信息化水平较高，大部分钢铁企业都有生产信息化部、能源管理部、网络管理部和生产信息系统的应用，对于网络和信息安全有着较为完善的管理。包括MES、EMS等系统在冶金行业的广泛应用，与此同时，冶金行业的控制策略复杂程度属于中等，大型控制系统如DCS的应用普及程度和深入程度并不是太高，大型PLC应用较多。由此产生，冶金行业信息安全防护时，应用场合更加分散，业主下属单位对于ICS网络安全单独采购的情况较多。这种情况，造成对ICS网络安全供应商跟踪业务难度的增加，从调查反馈来看，绝大多数ICS网络安全供应商对于冶金行业的开发力度有限。因此，对于冶金行业而言，加大对于用户ICS网络安全培训和推广尤为重要。

5.6 烟草行业工控网络安全

烟草行业工控网络安全状况

中国烟草产业是中国经济的支柱型产业，因此一直是中国行业发展的重点，由于信息化建设既能够增加效率减少消耗，又能够增进产业流通速度，增加与市场的交流频率，从而提升行业中企业竞争力。因此，烟草行业的信息化建设一直

以来都被企业列为发展的重点。

随着烟草行业坚持不懈的信息化建设，使卷烟企业已经初步建立起了以企业资源计划（MRP Ⅱ/ERP）系统为核心的企业管理信息系统，提高了企业的管理水平，同时也对信息化工作提出了更高的要求。由于上层生产计划管理受市场影响越来越大，明显感到计划跟不上变化。面对客户对交货期的苛刻要求，面对更多产品的改型，订单的不断调整，企业决策者认识到，计划的制订要依赖于市场和实际的作业执行状态，而不能完全以物料和库存回报来控制生产。

而企业资源计划（MRP Ⅱ/ERP）系统主要是针对资源计划，这些系统通常能处理昨天以前发生的事情（作历史分析），亦可预计并处理明天将要发生的事件，但对今天正在发生的事件却往往留下了不规范的缺口。找出任何影响产品质量和成本的问题，提高计划的实时性和灵活性，同时又能改善生产线的运行效率已成为每个烟草企业所关心的问题。

为解决以上遇到，提升自身的竞争力，国内许多知名烟草企业开始应用MES制造执行系统这项技术。当前，MES制造执行系统已经在烟草行业有了广泛应用。在这种情况下，客观对烟草行业的网络安全防护也提出了更高的要求。

在实施MES导入前，烟草行业在信息管理层实施的信息安全就已经相对成熟，烟草企业普遍采取防火墙、网闸、防病毒、防入侵的安全封堵的防护措施，信息安全的供应商主要由传统IT信息安全厂商组成，包括思科、启明星辰、网御星辰、网御神州等众多企业。

随着MES系统在烟草行业的逐步实施，越来越多烟草企业开始考虑综合防护，但目前采取的防护体系中，仍主要从信息层，延伸到生产管理层，生产控制层的防护仍然比率较低。MES层与信息层之间的边界防护成为烟草行业ICS网络安全的主要需求。

烟草行业工控网络安全发展趋势

从烟草生产流程来看，烟草行业以农产品作为原材料，制丝车间为流程性生产，卷接包属于离散性生产，生产模式属于混和生产模式。实施MES系统之后，企业对于信息安全防护意识有了进一步提高，但相对石化、冶金等流程行业而言，影响更偏向于经济损失，比如由于宕机造成烟丝报废，客观上对于人身伤害较低，因此目前烟草企业管理层对于信息安全防护的关注重点仍主要集中于信息层，ICS网络安全意识提高，还需政府监管部门加强检查力度，ICS厂商提供合适的安全防护解决方案和产品。

5.7 电网行业工控网络安全

能源互联网行业技术发展趋势分析

能源互联网是互联网技术、能源技术与现代电力系统的结合，是信息技术与能源电力技术融合发展的必然趋势。能源

互联网是解决国家能源环保命题的必由之路，其领域主要可以包括：

- 传统煤电燃气的清洁高效利用；
- 高耗能动力设备装置的节能降耗；
- 风电光伏可再生能源的利用；
- 分布式能源的广泛利用；
- 新能源汽车和储能的应用；
- 电力系统的智能化互联网化。

从特定意义上可是说，所谓能源互联网就是把以上六者有机串联融合起来的纽带。能源互联网是个价值经济体：安全稳定可靠高效节能环保。如果以开放、互联、对等、分享的原则对电力系统网络进行重构，可以提高电网安全性和电力生产的效率，使得能源互联网内可以跟互联网一样信息分享无比便捷。

智能电网交互终端技术

智能交互终端为电力企业和电力用户之间的交互提供了友好、可视的交互平台。可成为电力企业联络客户，为客户提供人性化管理的桥梁。智能交互终端基于网络化、人机交互，融合业务与功能的原则，凭借用电信息采集系统的网络平台，直接向用户显示用电信息、用电方式、告警信息以及电价政策等相关内容。智能交互终端可对用户用电设备的监测，及时发现客户受电装置隐患，以“隐患整改通知书”等书面形式通知客户，履行告知义务，避免出现安全事故，减少企业不必要的经济损失。终端设备的可视化功能，可满足电力企业和电力用户之间的可视化交互沟通。

智能变电站技术

在传感器及实时大数据平台等物联网技术依托下，智能变电站可实现全站监控、在线监测及智能辅助控制等多功能联动，这种集成联动系统正成为国内标准化设计方向。在与云计算、实时大数据融合过程中，除了在设备上预留端口以外，服务方案还包括收集数据、实时监测、信号交互、故障处理等基本维护措施。

分布式能源智能微网

分布式新能源大跃进式的发展，使如何应对风能、光伏发电量的不稳定性成为核心问题，智能电网的建设亦由此上升至国家战略高度。分布式能源智能微网是内核，未来千千万万个智能微网互联互通构建成真正意义上的能源互联网。传统电网在发电和输电的过程中，有高达56%的资源被浪费。智能电网的应用可以让发电厂和用户进行实时数据双向互动，通过网络反馈回来的数据可以使电厂掌握用户的消费习惯，从而对发电量进行合理调节，达到提升资源利用率的目的。借助智能微电网实时大数据监控技术，解决各类新能源并入电网的难题，实现集风电、光伏发电、储能、智能电网“四位一体”的新能源监控平台，实时保障电能质量和电力系统安全稳定运行。

智能大电网数据采集分析诊断技术

智能采集终端对大用户专用变压器、公变和低压居民用户用电信息进行自动采集。实现用户侧电能量、负荷数据采集，用电设备数据采集及在线诊断，支持实时数据的远传。其主要特征如下：

- 根据主站下发的控制定值，实时监测用户用电情况，自动执行本地功率闭环控制、本地电量闭环控制，并能够执行主站遥控、保电/剔除、催费告警、控制解除等控制命令，引导用户合理有序用电。
- 采集终端间支持快速通信，可装置级在线分析用电异常情况。
- 基于IPV6技术下的终端设备的管理，实现采集终端与主站、电能表及终端之间数据的无缝传输。
- 能够实现厂矿、企业、家庭电器工作参数、环境参数等多种数据的定时采集和召唤采集。

电力机器人

近年来，坚强智能电网的快速发展，为电力机器人创造了更多市场机会。电力机器人家族功能互补、可以协同作战，能够更好地解决电网运行管理中的实际问题。它的出现有赖于20世纪国内外科学技术的迅猛发展。

电力机器人的产业化推广同时也伴随着功能的不断升级。随着计算机技术的飞速发展，智能机器人的研究开始进入实质性阶段。经过几十年的发展，目前，基于感觉控制的智能机器人（又称第二代机器人）已达到实际应用阶段，基于知识控制的智能机器人（又称自主机器人或下一代机器人）也取得较大进展。

凭借其灵活的控制运行方式、不受天气因素影响等优点，智能巡检机器人将在未来的电网发展中发挥更多、更大的作用。随着国家电网公司“建设坚强智能电网”总体发展目标和规划的提出以及调控一体运行模式的推广，集成自动化、机械、人工智能、计算机等高新尖端科技的机器人必将成为推动电力行业“工业4.0”进程的重要力量。

电网工控网络安全发展现状分析

智能电网安全标准规范缺乏

随着智能电网规模的扩大，互联大电网的形成，电力系统结构的复杂性将显著增加，电网的安全稳定性与脆弱性问题将会越显突出。同时复杂度的增加，将导致接口数量激增、电力子系统之间的耦合度更高，因此很难在系统内部进行安全域的划分，这使得安全防护变得尤为复杂。

电力智能终端引入信息安全风险

随着大量智能、可编程设备的接入，以实现对电网运行状态实时监控、进行故障定位以及故障修复等，从而提高电网系统的效率和可靠性。这些智能设备一般都可以支持远程访问，比如远程断开/连接、软件更新升级等。这将会带来额外的

安全风险，利用某些软件漏洞，黑客可以入侵这些智能终端，操纵和关闭某些功能，暴露用户的使用记录，甚至可以通过入侵单点来控制局部电力系统。因此这些智能终端可能会成为智能电网内新的攻击点。面对更加复杂的接入环境、灵活多样的接入方式，数量庞大的智能接入终端对信息的安全防护提出了新的要求。

电网环境复杂化，攻击手段智能化

智能电网的建设，信息集成度更高，网络环境更加复杂，病毒、黑客的攻击规模与频繁度会越来越高；此外随着很多新的信息通信技术的采用，比如WIFI、LTE、3G等，它们在为智能电网的生产、管理、运行带来支撑的同时，也会将新的信息安全风险引入到智能电网的各个环节；为了提高数据的传输效率，智能电网可能会使用公共互联网来传输重要数据，这也将会对智能电网的安全稳定运行造成潜在的威胁，甚至可能会造成电网运行的重大事故。不安全的智能网络技术将会给黑客提供他们所附属的不安全网络的快速通道。而且未来有组织的攻击越来越多，网络攻击的手段也会更加多样化和智能化，这都将会给电力系统带来严峻考验。

用户侧的安全威胁

未来用户和电网之间将会出现更加广泛的联系，实现信息和电能的双向互动。基于AMI系统，用户侧的智能设备（比如智能电器、插拔式电动车等）都将直接连到电力系统。这不可避免地给用户带来安全隐患，一方面用户与电力公司之间的信息交互涉及到公共互联网，用户的隐私将会受到威胁；另一方面家用的智能设备充分暴露在电力系统中，易受到黑客的攻击。因此智能电网中端到端的安全就显得非常关键。

除此之外智能电网的信息安全问题还涉及其他因素，如心怀不满的员工、工业间谍和恐怖分子发动的攻击，而且还必须涉及因用户错误、设备故障和自然灾害引起的对信息基础设施的无意破坏。脆弱性可能会使攻击者得以渗透网络，访问控制软件，改动负荷条件，进而以无法预计的方式造成电网瘫痪。电网面临的其他工控安全风险还包括：

- 电网不断增加的复杂性，有可能引入脆弱性，使电网越来越多地暴露在潜在攻击者和无意错误之下；
- 相互连接的网络，会造成各网络共有的脆弱性发作；
- 引发通信中断和恶意软件肆虐的脆弱性日渐增多，有可能导致拒绝服务或破坏软件和系统的完整性；
- 供潜在敌对分子恶意利用的入口点和通道越来越多；
- 破坏数据保密性的潜在可能性，其中包括对用户隐私权的侵犯。

5.8 数控机床工控网络安全

数控机床工控网络安全状况

数控机床属于离散制造、智能制造典型应用系统设备，在军工制造、装备制造等行业得到广泛应用。

在我国，高精度加工企业使用的数控机床主要依赖国外进口，如国内大量使用Siemens、FANUC等国外数控系统，核心技术受制于人，大大增加了不可控因素。国内也存在大量的数控机床厂家，诸如沈阳机床厂、重庆机床厂等大量国产机床企业，国产品牌的机床由于技术相对落后，导致在高精密加工制造领域不被认可，这是国产机床未来亟待提升的问题，国产机床主要应用在一些对加工精度要求不高的领域。

随着我国制造企业的规模化发展，在生产过程中数控网络和设计网（或企业网）之间信息传递越来越多，原始低效的数据摆渡严重阻碍制造业的发展速度，促使数控网与设计网（或企业网）间的网络互联互通越来越迫切。单台数控机床独立作业以不能满足制造企业业务发展的需要，数控机床DNC联网运行以成为趋势。目前我国数控机床系统存在以下几种应用模式与信息安全状况：

- 数控机床未联网：涉密军工生产企业在信息化进程中，设计网（高密网）和生产网（低密网）被禁止互联互通。设计部门开发的数控加工代码只能通过刻光盘或用指定U盘拷贝的办法下发到生产车间，使得相关企业的生产效率大打折扣。有的企业设计部门与生产车间相隔数十公里，这种原始的信息传递模式使得企业生产效率极其低下，而且摆渡介质的安全风险不好控制。
- 数控机床与管理主机直连：管理主机与高端数控机床直连的方式进行数控数据传输，加工代码通常使用FTP、网上邻居共享或者私有通信协议的方式传输至数控机床，数控机床通过HMI进行加工操作，修改后的加工代码将以文件的形式返回管理主机，此过程中管理主机存在操作权限滥用、乱插USB外设等操作，致使管理主机被病毒感染，或误操作使加工数据被篡改，或者因管理主机通过USB口连接上网外设而使管理主机直接暴露在互联网上导致数据泄密等诸多安全隐患。同时也存在设计部门与生产部门相距遥远，加工数据摆渡介质安全问题，存在丢失与泄密隐患。
- 数控机床DNC联网：有些研究机构及企业已完成DNC组网保护方案，有些研究机构及企业已向主管部门提交DNC组网方案申请，甚至开始尝试数控机床DNC网络与设计网络互联实验测试，为提高生产制造效率、实现协同制造进行尝试性研究与应用。

数控机床DNC联网运行会存在以下安全隐患：

- 管理主机未对USB口进行有效的管理，存在违规非法USB连接的情况。
- 管理主机缺乏病毒木马的查杀机制，存在管理主机感染木马病毒影响正常生产的安全问题。
- 一部分现场工作人员缺乏基本的安全意识，存在使用管理主机安装盗版电脑游戏、炒股软件等，存在通过USB口连接上网设备进行互联网的访问行为。
- 未对工业控制网络区域间进行隔离、恶意代码监测、异常监测、访问控制等一系列的防护措施，很容易一点发生病毒或攻击，影响整个网络连接的主机系统。
- 数控编程局域网未采取有效的保护，任何接入该局域网的设备都可直接访问DNC服务器从而下载/上传加工代码，存在加工数据泄密与被恶意篡改的安全风险。

- 缺少完备的工业控制系统安全管理制度和流程，使得部分操作人员不按规定执行导致相关安全问题发生，影响生产质量。如NC程序版本混乱时可能导致一批加工部件质量不合格。
- 未统一对设备及日志进行统一管理，使得相关工控系统事件不能统一收集、分析、不易关联分析设备间的事件和日志，难于及时发现复杂的问题。
- 对外来人员（厂商维修人员）的安全管理不够到位，如国外厂商很容易直接进入涉密区域。

同时针对国外品牌的数控机床系统，自身安全隐患问题也逐渐被制造企业所重视，如数控机床携带GPS模块、自带远程运维模块等，以及自身漏洞问题，都会给使用带来不同程度的泄密问题。

数控机床工控网络安全发展趋势

随着德国工业4.0战略的出现，随着我国两化融合、“互联网+”、“中国制造2025”发展战略的相继提出，中国制造企业未来将向着协同制造、智能制造的方向发展，努力提升我国制造大国的地位。2015年工信部为推进“中国制造2025”战略的执行，在全国范围选取了46家装备制造、智能制造试点企业做示范，为全面推进“中国制造2025”发展战略积累宝贵经验。

在数控机床得到广泛应用的制造业领域，国家的两化融合、“互联网+”与“中国制造2025”的发展战略，为企业科技发展指明了方向。制造企业将充分利用互联网、物联网以及信息化等先进技术，全面整合制造业资源，形成协同制造、智能制造的产业格局，新一代信息技术与制造业的深度融合，将促进制造模式、生产组织方式和产业形态的深刻变革，智能化服务化成为制造业发展的新趋势。在此背景下，数控机床应用与网络安全发展存在以下趋势：

- 制造企业继续加快数控机床DNC联网建设与运行。面对制造企业发展的需要，结合国家战略规划，行业主管部门与制造企业将加快数控机床DNC联网业务需求与网络安全需求的研究与标准制定，加快制造企业数控机床DNC网络的建设，规范数控网与设计网的互联互通与边界防护，规范数控网络的安全防护体系建设，加强数控网络信息安全风险管控能力与应急处置能力的建设，为制造企业两化融合发展提供必要的信息安全保障。
- 全面完善制造企业协同制造、智能制造的技术路线，推进制造企业变革与科技创新能力建设。随着行业主管部门与制造企业在协同制造、智能制造领域的理解与认知不断深入，随着物流、材料供给等相关行业信息化水平的逐步提高，制造企业将逐步实现与上游生产订单商、下游物流商、材料供给商等建立网络互联互通、信息服务、数据交换与共享机制，形成更加广泛的协同制造与智能制造的产业格局，制造企业的设计网、生产数控网将更加开放，内容更加多元化，信息安全防护要求更高，信息安全防护的纵深化、体系化能力更加明显，制造企业将加强对全网安全风险的感知、预警、防控与协同处置的安全防护能力建设，实现新形势下的安全防护体系建设，为制造企业信息化业务应用提供信息安全保障。

6 我国工业控制网络安全发展建议

近年来，我国在网络空间的影响力进一步加大，工控网络安全产业迎来爆发式增长机遇。但我国网络安全战略不明确、网络信任体系建设滞后、网络安全基础能力薄弱、网络攻防技术能力不足等问题也非常突出。与此同时，世界各主要大国都在加大对该领域的投入，2016年2月9日，美国总统公布《网络安全国家行动计划》，提议2017财年190亿美元预算用于加强网络安全，着重保护公众安全以及经济和国家安全。

6.1 我国工控网络安全领域面临严峻挑战

我国工控网络安全行业当前面临的主要问题如下：

我国缺乏明确的网络安全战略，工控网络安全标准体系亟待建立

2015年，《国家安全法》、《网络安全法》等法律相继推出，“网络强国战略”纳入“十三五”规划，国家网络空间安全顶层设计明显加强。但是，我国网络安全战略尚未明确，国家网络安全审查制度尚未出台，网络安全顶层设计仍需细化。工控网络安全标准与信息安全技术标准存在较大的差异，数据格式、通信协议、数据采集等标准的差异造成数据互联互通存在障碍。当前相关标准严重缺乏，尚不能适应工控网络安全产业发展趋势。

我国重要工业制造业领域大量使用国外工控设备

目前，国外工业生产设备提供商已经在各领域垄断了工业生产控制系统和设备市场。以我国工业PLC市场为例，2015年西门子、三菱、欧姆龙、罗克韦尔、施耐德等5家国外厂商占据了超过80%的市场份额。这些设备普遍存在未知的漏洞以及可能存在后门，严重漏洞难以及时处理，是我国国家安全的重大隐患。我国提出了“国产化替代”的要求，但替换国外工控设备还需多年的技术研发和产业发展，这期间的工控网络安全问题也必须要进行解决，因此，工控网络安全是涉及国家整体安全战略的重要环节。

我国工业制造业企业对工控网络威胁感知不足

工控网络安全在我国仍处于认识的初级阶段，政府和企业层面，对工控网络安全的认知仍存在不足。对潜在的工控网络安全威胁认识不到，对国家关键工业生产安全重视不足，对国际先进的网络攻击手段缺乏感知。以至于，我国目前的工业生产系统，没有及时部署针对工控系统漏洞和网络攻击的有效防护系统，在网络攻击来临时无法察觉，在遭受攻击后无法追踪。

我国针对工控网络威胁的持续防护能力缺失

工控网络安全是一个全新的领域，它不是传统信息安全行业的延伸，而是基于“两化融合”框架下的跨界领域。针对工控网络的高级持续威胁是一种严密的组织化行为，拥有大量资金支持，优秀的管理能力和大量高端人才。这些特点使得防护能力建设必须大力投入、持续投入、深度开发。我国工业和基础设施智能化发展很快，针对工控网络安全的防护能力建设严重滞后，目前尚不足以保障“两化融合”战略的稳步推进。

6.2 我国工控网络安全行业迎来难得的发展机遇

第四次工业革命的到来，打破了发达国家对核心技术、工艺和标准的垄断，弥补了发达国家与发展中国家生产力的鸿沟。在“中国制造2025”战略推动下，我国大量工业企业迎来了智能化改造的战略机遇期，因此，工控网络安全作为一个新兴产业也迎来难得的发展机遇。

我国工业信息化、智能化建设具有后发优势

我国工业信息化、智能化建设起步较晚，但新建系统多，自动化水平高，有利于工控网络安全体系的部署和实施，实现弯道超车。

我国工业规模巨大为安全产业发展提供广阔空间

我国现代工业规模为世界之最，具备完整的现代工业体系，为工控网络安全产业的发展提供了最为丰富的土壤。工控网络安全产业与现代工业共生、共同成长，具备全球首屈一指的成长空间和发展潜力。

工控网络安全成为国产化自主可控的契机

以此为杠杆可以撬动国外工控产品的垄断地位，为我国要求国外巨头企业开放产品技术壁垒，促进自主工控产品替代进口打通出口。

工控网络安全正在成长为一个战略新兴产业

该产业与我国现代工业产业互相促进、共同发展，提高工业智能化水平的同时，自身做大做强，形成产业优势，并与我国基础设施建设深入结合，为其植入安全基因。

我国强力、高效的国家安全管控能力和强大的基础设施建设能力使其具备引领全球工控安全产业发展的实力。工控网

络安全产业将伴随中国制造向海外输出，配合“一带一路”等国家战略，占领周边国家及全球市场，使我国成为该领域的先进国家，并主导该领域标准和规范的制定，建立全球影响力。

6.3 针对我国工控网络安全发展给出如下建议

建立完备的工控网络安全体系，掌握芯片级核心技术

加快工控网络安全技术与产品研发，解决工控设备本体安全，实现自主可控；加快工控网络安全体系建设，解决工控网络结构安全，实现真实可靠；加快基于行业应用的工业过程研究，解决工控系统行为安全，在持续对抗中保持领先优势；安全与工控深度融合，以自主安全工控芯片为基础，在工控系统从设计到生产到部署到运营的全过程都有安全因素介入，为工控注入安全基因，实现本质安全。

大力扶持新兴工控网络安全企业，鼓励技术创新和产业化

工控网络安全是跨学科的技术融合，新兴企业的颠覆性技术是创新的重要来源。我国应大力扶持具备深度科研能力的、有活力的工控网络安全企业，鼓励民营企业进入工控网络安全领域。引导和扶持来源于海外的归国创业团队迅速实现本土化，将国外核心技术快速转化为自主知识产权的先进技术并实现产业化落地。

在关键基础设施、智能制造等行业推进工控网络安全落地

在电力、石化、冶金、交通、烟草、先进制造等重要行业，积极推动工控网络安全技术与产品在本行业的应用与融合，在重大工业工程建设中，从规划设计到项目建设到运维实施的全过程将工控网络安全作为重点建设内容和考核指标；在“中国制造2025”等国家重大规划及实施方案中积极开展工控网络安全专项试点、示范工作；积极开展工控网络安全调研、检查、整改工作。

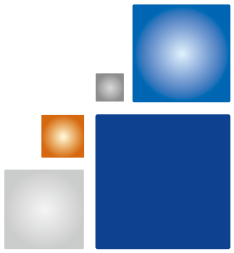
快速推进国外工控产品与国内安全技术结合，把控安全命脉

针对当前工控领域国外进口产品占据主导地位的现状，以国产化替代进口为最终目的，制定相关法规和实施办法，并建立相应的检查、测评机制，将采用国产安全技术作为国外工控产品准入的门槛，鼓励和引导国外主流工控厂商与国内安全企业合作，使用国产安全技术把控进口工控系统的安全命脉。

大力引进与培养工控网络安全专业人才

大力开展海外人才引进，通过人才的引进迅速掌握核心技术，缩小与发达国家差距。推动工控网络安全学科建设和教学、实践环境建设，加强专业人才培养，满足工控网络安全产业长期发展的人才需求。

欧美发达国家已经率先将工控网络安全作为战略新兴产业大力扶持。在这场关乎国家未来发展和前途命运的国际竞赛中，我国政府应给予足够的重视，加大投入，持续投入。如果六十年代以来，中国没有原子弹、氢弹，没有发射人造卫星，中国就不能叫有重要影响的大国，就没有现在的国际地位。未来中国能不能保持并加强国际领先地位，工控网络安全领域的发展是重中之重。



附录 参考文献

1. 德国国家科学与工程学院《“工业4.0”战略计划实施建议》
2. GE 《工业互联网：突破智能和机器的界限》
3. ICS-CERT 《ICS-CERT_Monitor_Sep2014-Feb2015》
4. ICS-CERT 《ICS-CERT Monitor_Nov-Dec2015_S508C》
5. ICS-CERT 《Year_in_Review_FY2014_Final》
6. 美国国土安全部《网络空间安全国家战略计划》
7. NIST SP800-82《Guide to industrial Control Systems Security》
8. ISA/IEC 62443《Industrial network and system security》
9. GB/T 30976.1—2014《工业控制系统安全第1部分：评估规范》
10. GB/T 30976.2—2014《工业控制系统安全第2部分：验收规范》
11. 工信部协〔2011〕451号文《关于加强工业控制系统安全管理的通知》
12. 国务院《2015年政府工作报告》
13. 国务院《中国制造2025》
14. 全国人大常委会《中华人民共和国网络安全法（草案）》
15. 国务院学位委员会《关于增设网络空间安全一级学科的通知》
16. 工信部信〔2013〕317号文《工业和信息化部关于印发信息化和工业化深度融合专项行动计划（2013-2018年）的通知》
17. 工信部电子科学技术情报研究所《2014年工业控制系统安全蓝皮书》
18. 工业控制系统安全产业联盟《工业企业信息系统安全技术指引》
19. CNVD，http://www.cnvd.org.cn/
20. 中国轨道交通网，http://www.rail-transit.com
21. 中国燃气网，http://www.chinagas.org.cn/
22. 国家智能车发展论坛，http://www.caaiv.org/
23. 北极星电力网，http://www.bjx.com.cn/
24. Digital Bond，http://www.digitalbond.com/
25. Scadahacker，http://www.scadahacker.com/
26. Shodan，http://www.shodanhq.com/

专注　创新　合作

北京匡恩网络科技有限责任公司

电话: (010) 5670-5608　传真: (010) 5951-2799

地址：北京市海淀区知春路7号致真大厦D座13层

官网：www.kuangn.com