工业控制系统的安全技术与应用研究综述

锁延锋[1,2] 王少杰[2] 秦 宇[3] 李秋香[4] 丰大军[5] 李京春[2]
(北京科技大学计算机与通信工程学院 北京 100083)[1] (国家信息技术安全研究中心 北京 100084)[2]
(中国科学院软件研究所 北京 100083)[3] (公安部第一研究所 北京 100083)[4]
(中国电子信息产业集团有限公司第六研究所 北京 100083)[5]

摘 要 为应对控制系统与互联网技术深度融合引发的安全新挑战,抵御震网病毒、火焰病毒、BlackEnergy等靶向攻击,针对工业控制系统漏洞挖掘、修复与控制等技术滞后,以及工业控制安全面临的"难发现、难监测、难防护"等问题,通过对工业控制系统的理论模型、关键技术、装备研制及测试评估进行研究,以漏洞挖掘与利用研究为主线,以理论与体系架构研究和安全技术测试验证平台的建设为基础,以动态监测防护和主动防御为目标,以测试样例集的攻防验证与典型示范为应用,提出了包含工业控制系统漏洞挖掘、深度检测、动态防护、主动防御等的整体安全技术解决方案,设计并构建了集漏洞挖掘、验证评估、动态防护、主动防御于一体的工业控制系统安全技术体系。

关键词 工业控制系统,漏洞挖掘,验证评估,动态防护,主动防御
中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.04.004

Summary of Security Technology and Application in Industrial Control System

SUO Yan-feng[1,2] WANG Shao-jie[2] QIN Yu[3] LI Qiu-xiang[4] FENG Da-jun[5] LI Jing-chun[2]
(School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China)[1]
(National Research Center of Information Technology Security, Beijing 100084, China)[2]
(Institute of Software, Chinese Academy of Sciences, Beijing 100083, China)[3]
(The First Research Institute of the Ministry of Public Security, Beijing 100083, China)[4]
(The 6th Research Institute of China Electronics Corporation, Beijing 100083, China)[5]

Abstract In order to face the new challenges caused by the deep integration of control system and Internet technology and resist the target attack, such as shock virus, flame virus and BlackEnergy, aiming at the technical lag of industrial control system vulnerability mining, repair and control, and the problems of "difficult to detect, difficult to monitor, difficult to protect", this paper researched the theoretical model, key technology, equipment development and test evaluation of industrial control system. Besides, through taking the research of vulnerability mining and utilization as the main line, taking theoretical system architecture research and test verification platform construction as the basis, taking dynamically monitoring protection and active defense as the goal, taking test example set attack and defense verification and typical demonstration as the applicationl, this paper proposed security technology solutions including industrial control system vulnerability mining, depth detection, dynamic protection, active defense, and designed the integrated security technology system including vulnerability mining, verification and evaluation, dynamic protection and active defense.

Keywords Industrial control system, Vulnerability mining, Validation evaluation, Dynamic protection, Active defense

1 绪言

近年来,工业控制系统与物联网、互联网呈现出深度融合的态势,这既大幅提升了工业控制系统的智能化和信息化程度,也引发了一系列的安全新挑战[1]。针对工业控制系统的各类新型攻击技术和手段层出不穷,震网病毒[2]、火焰病毒[3]、BlackEnergy[4]等具有明确的靶向攻击特征,这对国家安全、经济发展和社会稳定等产生了严重影响,引起了世界各国政府的高度重视。

安全风险评估结果表明,我国工业控制系统的进口设备存在严重的漏洞后门,硬件漏洞修复的成本高、难度大,作为我国关键基础设施的工业控制系统,其安全隐患无法根除;受

到稿日期:2017-03-23 返修日期:2017-07-11 本文受国家863计划项目:漏洞验证评估与综合服务平台研究(2012AA012901)资助。
锁延锋(1976-),男,博士生,主要研究方向为安全评估、网络审查、安全检测;**王少杰**(1976-),男,博士后,主要研究方向为关键信息基础设施架构安全,E-mail:haoyizz@163.com(通信作者);**秦 宇**(1979-),男,博士,副教授,主要研究方向为计算机网络与信息安全;**李秋香**(1981-),女,硕士,主要研究方向为信息安全;**丰大军**(1974-),男,高级工程师,主要研究方向为工业控制系统安全检测;**李京春**(1959-),男,硕士,博士生导师,主要研究方向为关键信息基础设施安全风险评估、网络安全审查等。

国外工业控制系统“一站到底式”的控制模式的制约，工业控制系统的安全检测、监测、控制与防范等难以深入；我国工业控制系统的自主研制与国产化应用起步较晚，自主可控的高端工业控制系统产品的国产化率较低；工业控制系统的重大共性关键安全技术尚需突破，适应我国工业控制安全需要的安全标准和技术体系等相对滞后[5-6]。

针对上述问题，本文拟系统性地研究工业控制安全领域的有关基础理论和关键技术：重点研究工业控制系统的攻击模型与安全防护体系，针对工业控制器的回路攻击、组态数据篡改等安全威胁，研究涵盖协议安全分析[7]、自适应敌手攻击、纵深防御效果评估的工业控制系统攻击模型；研究工业控制系统的安全漏洞挖掘与利用技术，包括基于行为模式的异常捕获、基于符号执行与污点传播的漏洞判定等技术，挖掘组态软件、监控软件、嵌入式软件等漏洞[8-9]；研究工业控制系统安全技术测试验证和攻防量化评估方法[10-11]，研制针对工业控制系统典型装置的测试验证平台，用于对国内外的主流工业控制系统及协议等开展攻防演练、验证评估等科学实验[12]；研究工业控制系统组件的动态防护技术，包括面向工业控制系统监控层、网络层和现场控制层的防御技术，实现可动态重构、异构冗余、随机多样化的动态防护[13]；对工业控制系统的主动防御技术进行研究与应用，以信息安全漏洞和攻击手段作为设计基线，通过 IO 逻辑控制、状态实时监控、高危攻击应急处理、边界数据隔离等手段实现控制器的主动防护。

通过研究，本文提出工业控制系统安全技术领域的相关理论模型、关键技术、测试评估方法，研制相关的技术装备和系统，设计构建集漏洞挖掘、验证评估、动态防护、主动防御于一体的工业控制系统安全技术体系。本文提出的典型装置测试验证平台，可为工业控制系统的安全性研究提供科研环境，为持续开展工业控制系统的漏洞分析挖掘、检测评估、安全防护和攻防实验等工作提供技术支撑；通过研究工业控制网络的攻击类、检测类、防护类等核心技术的发展趋势，形成工业控制系统信息安全保障技术体系，以引领我国工业控制系统安全的发展；通过研究工业控制系统的安全防护架构、策略和机制等，突破工业控制系统组件动态防护和主动防御等核心技术，可提升我国工业控制系统的安全自主可控水平；借鉴吸收国外工业控制安全体系建设和应用的经验，研究并提出符合国家重要基础行业实际的工业控制安全规范，完善工业控制系统的信息安全标准体系。

2 现状及趋势分析

在全球信息化背景下，网络空间政治化、军事化、经济化进程明显加快，网络空间已成为国际战略竞争的新制高点、经济发展的新支撑、国家主权的新疆域和军事斗争的新战场。自 2010 年震惊全球工业界的震网病毒[2]爆发以来，针对工业控制系统的攻击事件频繁发生。2014 年 10 月韩国核电站病毒、2015 年 12 月乌克兰电网断电[14]、2016 年 3 月德国核电站病毒[15]等安全事件表明，针对工业控制系统的攻击威胁呈有组织、大规模、高隐蔽、强持续的趋势，具有国家背景的网络攻击行为不断增加，攻击手段层出不穷，攻击方法花样翻新，国家安全、经济发展、社会稳定和公众利益面临着巨大威胁。

鉴于工业控制系统对国家安全、社会稳定、经济繁荣的重要性，世界上大多国家都在工业领域开展了安全研究工作。1)在工业控制安全标准研究方面：国际自动化学会(ISA)制定了用于制造业和控制系统的安全标准 SA-99[16]；国际电工委员会 IEC /TC65 /WG10 工作组制定了 IEC62443 系列标准[17]；北美电力安全公司制定了控制系统网络安全标准 CIP[18]；美国国家标准和技术研究所发布了智能电网网络安全标准 NISTIR7628[19]；美国核管理委员会发布了核设施网络安全指南 RG5.71[20]，明确要求核电站应引入纵深防御理念来建立完整的主动防御体系，以使核电站 CDA 免受来自于包括 DBT 在内的信息安全攻击等。2)在漏洞挖掘与利用方面：美国 SANS 网络安全实验室提出了攻击树理论[21]，其可被用来构建信息安全中的一般攻击模型；俄罗斯 EDF 机构的研究人员提出了基于布尔逻辑驱动的马尔科夫过程构建攻击与防御模型的方法[22]，并对比了几种经典的基于图形的攻击模型构建方法；伊朗 Shiraz 大学的学者针对工业控制系统漏洞和网络攻击，设计并实现了一套工业控制专用的实验平台，该平台可以评估工业控制应用程序的安全性，提供了包括静态测试、动态测试和网络测试在内的多种测试评估方法；伊利诺伊理工学院的研究者研发了基于模拟的验证框架，该框架使用跨层次的验证技术，能够对整个工业控制系统进行综合分析，查找漏洞和问题；美国纽约大学(NYU)开发了一套用于智能电网的漏洞挖掘的测试床[23]，并对电网控制单元进行建模测试，美国目前已经至少建成了 35 个用于智能电网漏洞检测的测试床[24]；美国的爱达华州国家实验室开发了一套大型的 SCADA 测试床[25]，专门用于工业控制系统的检测评估、系统改进和安全培训。3)在工业控制安全防护方面：美国国土安全部研究和总结了工业控制系统与网络的主动防御策略，将工业控制系统和资产的外界和内部进行适度区分，在软件系统和网络层次实现识别与隔离[26]；荷兰特温特大学的学者提出了基于内容检测的主动防御方法[27]，该方法主要针对网络传播和被追踪的数据以及应用程序日志进行深入分析，以判断工业控制系统的安全隐患；Security Matters 公司对比总结了几种工业控制系统的主动防御技术，包括白名单、传统的签名保护技术和沙盒检测技术[28]，指出白名单技术具有较强的主动防御能力，能综合各种防御技术达到有效的防御等，并给出了一个工业控制系统的网络监控架构实例。4)工业控制安全产品方面：国际市场上涌现了很多专门用于防护工业控制系统安全的商用产品，如德国的西门子、法国的施耐德、加拿大的多芬诺等企业专注于工业控制系统安全防火墙产品的研制，针对不同型号的 DCS 和 SCADA 提出统一的安全方案；美国的 FireEye 和 Bit9 等专注于工业控制终端环境的漏洞和系统防护，整合了设备标识认证、软件完整性保护、系统策略安全执行的功能，增强了 PLC 等工业控制终端设备的安全性，提升了工业控制网络针对 APT 攻击的防护能力。

工业控制系统被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，已是国民经济关键基础设施的神经中枢，其安全性直接影响社会稳定和国家安全。我国已积极开展工业控制安全研究工作，在工业

控制系统的漏洞挖掘、检测、防护等方面，国家信息技术安全研究中心、中国电子信息产业集团有限公司第六研究所、中国电力科学研究院、中国电子信息产业集团有限公司(CEC)、公安部第一研究所等已经取得了一定成果，启明星辰、匡恩网络、威努特、海天炜业等先后推出了工业控制防火墙、主机防护和远程认证等技术产品，同时我国近期发布了《工业控制系统信息安全标准》(GB/T30976-2014)[29]等。虽然已经取得了一定成果，但整体而言，我国工业控制安全尚处于起步阶段，难以应对控制系统与互联网技术的深度融合引发的工业控制系统网络安全的新挑战，亟需系统性地从理论模型、关键技术、装备研制及测试评估等方面开展工业控制系统的安全技术研究。

3　研究内容

工业控制系统安全是当今信息安全领域的战略高地，随着国家层面的网络对抗日益加剧，工业控制系统因其巨大的政治、经济影响力，已成为各种势力攻击破坏和实施网络战的首选目标；同时，互联网技术与工业控制系统的深度融合，引发了工业控制系统安全的重大挑战。工业控制系统安全防护多数依赖于系统隔离、网络分区分域管理，这些传统的安全防御方法无法抵御震网病毒、火焰病毒、BlackEnergy 等靶向攻击。针对上述问题，本文拟解决以下关键科学和技术问题。

(1)工业控制系统攻击模型与安全防护体系的构建问题。工业控制系统多样性和个性化的安全问题突出，单一的检测防护手段难以抵抗专业化的高级威胁攻击，因此需要针对工业控制系统的特征和攻击的机理，建立工业控制专用协议深度分析模型、自适应敌手攻击模型、纵深防御模型，形成一套完整的工业控制攻防技术体系。

(2)工业控制系统安全漏洞的挖掘与利用问题。针对工业控制系统中的控制器硬件、组态软件等核心部件的漏洞修复难、修复成本高等问题，从分析工业控制系统的运行机制及漏洞触发机理入手，解决基于不同硬件体系的工业控制软件行为特征的提取与判定问题。漏洞挖掘研究主要包括漏洞安全属性建模及推理、工业控制专用协议漏洞分析、漏洞触发模式及运行属性检测、漏洞逼近测试及导向触发理论等科学技术问题。漏洞利用研究主要针对不同功能、不同类型的工业控制部件所存在的漏洞，采用基于各类典型漏洞的行为模式分析、作用机理分析和攻击测试样例设计等方法来解决工业控制系统漏洞利用的问题。

(3)工业控制系统安全技术的测试验证问题。工业控制系统安全防护技术的健壮性离不开高度仿真的攻击测试及验证，需要构建适用于电厂 DCS 系统、PLC 控制系统、电网调度控制系统等典型工业控制系统的安全技术验证试验环境，解决工业控制系统的攻防场景和高仿攻防模拟问题，以及攻防效果评估、攻防场景分析、漏洞危害性验证和安全技术有效性评估问题。

(4)工业控制系统组件的动态防护问题。工业控制系统实施纵深防御和边界防护，需要解决安全域划分的区域防护、上位机防护以及 PLC 控制器和现场总线控制回路防护等多重防护问题。需要研究高速现场总线技术、安全网络技术、安全内存管理技术等，解决多重纵深防御机制影响工业控制系统性能的技术难题。当发生工业控制系统攻击时，应提高系统的冗余性，动态重构系统，以保证控制系统能正常运行；利用控制系统的主-备冗余和关键工业控制应用所特有的异构安全保护系统，在攻击发生前有效探测活动并及时预警定位；利用工业控制系统异构冗余的特点，在工业控制系统发生大规模灾难性攻击前遏制和清除攻击行为。

(5)工业控制的系统主动防御问题。依据国际和国内工业控制系统研发、设计、运行的特征及在安全防护方面的标准和法规要求，采用安全工程思想，分析工业控制系统高危等级威胁的攻击特征，利用 DCS 的动态重构机制切换至系统备份，以恢复安全状态，解决系统面临安全威胁时的主动防御和系统恢复问题。非法设备接入所引发的恶意软件攻击是工业控制系统的主要威胁之一，需要在评估安全审计监控技术的可行性的基础上，解决工业控制系统对非法信息控制流和数据流的监控和预警问题，特别需要解决控制所需的、具备高抗压能力的安全配置数据的制定和动态调整问题。

针对上述研究问题，本文拟开展如下 5 个方面(见图 1)的研究工作。

(1)工业控制系统攻击模型与安全防护体系的研究。1)针对工业控制器回路攻击、组态数据篡改等安全威胁，研究涵盖协议安全分析、自适应敌手攻击、纵深防御效果评估的工业控制系统攻击模型；2)以传统的分区隔离纵深防御技术为基础，将动态防护和主动防御方法相结合，研究以动态的对抗性安全理念为核心的工业控制系统自适应防御体系，并进一步基于威胁情报的攻击路径和系统攻防态势，研究自适应地调整防御资源来实施安全响应和恢复的方法；3)突破控制器安全启动、固件/软件证明、系统内核加固、白名单管控、网络动态监控等核心关键技术，研制基于硬件密码模块的可信工业控制终端防护系统以及基于设备 ID 的海量终端身份鉴别和安全通道加密系统。

(2)工业控制系统安全漏洞挖掘与利用技术的研究。1)研究基于解剖分析和非侵入/半侵入检测分析等技术手段的工业控制系统硬件逆向分析方法，挖掘工业控制系统硬件与芯片的漏洞；研究基于非侵入式测试、半侵入式测试、模拟与数字量混合的测试数据生成等技术，以及基于电路分析、算法分析、逻辑仿真等手段的硬件逆向综合分析方法，挖掘硬件或芯片设计中隐藏的缺陷或漏洞。2)研究基于动态靶向分析的软件漏洞挖掘与分析方法，挖掘工业控制系统的软件漏洞；基于机器学习理论研究工业控制系统的行为模式和异常捕获方法；利用污点传播、符号执行等软件漏洞分析方法，结合符号执行与路径约束求解技术，提高漏洞分析效率；研究工业控制软件的漏洞挖掘平台，使其具备分析、挖掘和检测工业控制核心部件漏洞的能力。3)针对在典型工业装置、主流工业控制系统等核心部件上挖掘出的漏洞，研究相应的利用方法，创建漏洞利用样本，建立漏洞测试样例集；并以此为基础研发工业控制系统漏洞利用工具集，使其涵盖篡改组态数据、伪造控制指令、实时欺骗、获取超级权限等漏洞类型的测试样例。

(3)工业控制系统安全技术测试验证方法的研究。1)研究并构建工业控制系统典型装置的测试验证平台，用于支持电力 DCS 系统、PLC 控制系统、电网调度控制系统等典型工

业控制系统的模拟仿真;构建典型的工业控制系统漏洞挖掘、检测、评估、攻防实验等工业控制系统安全技术测试验证环境,在该环境下可针对国内外主流的工业控制系统及协议等开展漏洞挖掘、攻防演练、验证评估等科学实验。2)研究工业控制系统攻击效果和安全防御量化的评估方法,研究电力工业控制系统的攻防技术并评估其漏洞威胁,测试验证漏洞利用方法的有效性、实用性和隐蔽性;突破多层次的模糊测试、形式化分析和模拟仿真等技术,构建攻击测试用例集,针对防护组件/工具开展工业控制系统的攻防对抗测试,评估其安全风险;在工业控制系统安全防御量化评估方法的基础上,建立电力工业控制产品测评认证、产品供应链备案、漏洞预警通报、应急响应等安全保障机制。

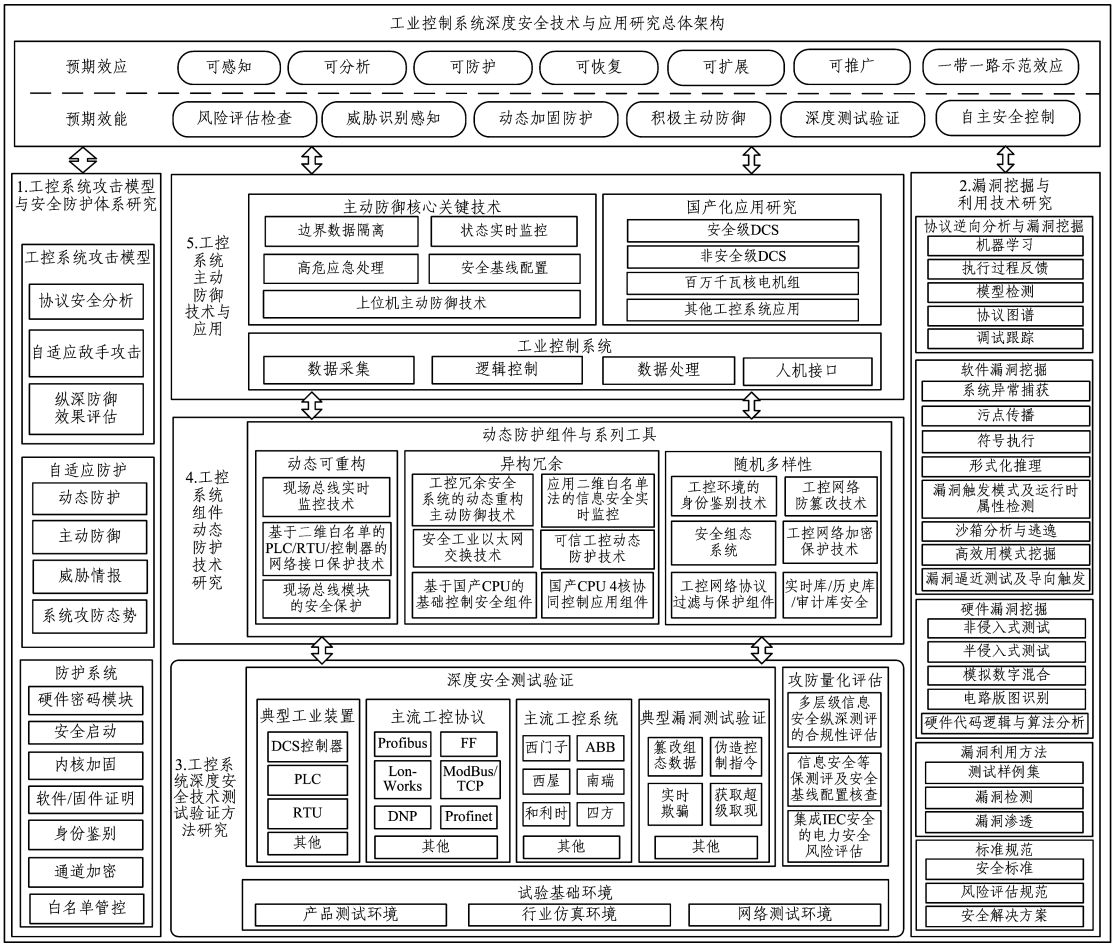

图 1 工业控制系统安全技术与应用研究总体架构

Fig. 1 General framework of security technology and application in industrial control system

(4)工业控制系统组件动态防护技术的研究。1)研究涵盖工业控制系统监控层、网络层和现场控制层的动态防护方法,包括面向国产 CPU 的基础控制和安全保护组件、工业控制系统二维度(基于内容和行为)白名单防护、现场总线实时监控、工业控制环境身份鉴别和防篡改等共性关键技术;2)采用双机/总线/网络冗余等方式,研究动态重构、异构冗余等安全保护技术,对控制回路(由 PLC/控制器-现场总线-传感器和执行器构成)进行故障模式的影响分析,研究异构的安全保护系统,对异构冗余的多路输入信息展开关联分析并捕捉可疑行为,实施主动防御和动态防护;3)研制自主可控的国产 CPU 协同控制组件、工业控制网络协议过滤与保护组件、安全工业以太网交换机等组件,以及工业防火墙、网络行为旁路实时监测与审计等产品,实现工业控制网络的动态深层防护。

(5)工业控制系统主动防御技术的研究与应用。1)研究基于序列保护、多重身份、单一合法数据源、信息验证等的边界数据隔离技术,以漏洞攻防作为设计基准,通过边界数据隔离手段提升控制器防护能力;2)研究针对 IO 逻辑控制、数据交叉校验、状态信息传输等实施监控和高危攻击的应急响应,一旦出现异常就启动应急保护机制,将安全威胁彻底隔离;3)研究工业控制系统安全配置基线的方法和上位机主动防御的方法,结合动态防护组件实现工业控制系统运行环境的可信检查和实时监控。

4 研究方法

本文围绕工业控制系统漏洞的挖掘与利用、深度安全检测与验证等技术难点,重点研究典型的工业控制装备、主流的工业控制协议和系统中的漏洞分析与检测评估等重要科学问题,研究工业控制系统动态防护工具、主动防御工业控制系统、安全测试与验证平台等。主要研究方法和原理如下。

(1)工业控制系统攻击模型与安全防护体系的研究。针对典型工业控制场景进行攻击面和脆弱性的全面分析,研究工业控制系统攻击模型,涵盖协议安全分析、自适应敌手攻击、纵深防御效果评估等多个方面,推演工业控制系统的潜在

攻击行为；并以此为指导，研制基于硬件安全模块的可信工业控制防护系统，构建涵盖工业控制终端和分层化网络的工业控制环境纵深防御体系。研究工业控制领域的密码应用问题，拟基于国家商用标识算法技术研究并实现工业控制的数据加密防护和强身份认证机制，达到数据防篡改、操作防抵赖的目的。

1）工业控制系统攻击模型的研究。工业控制系统的构成复杂，其通讯协议、操作系统、工业控制应用软件、安全策略以及杀毒软件都可能存在安全漏洞和脆弱性。在科学评估敌手攻击范围、攻击能力以及系统脆弱性的基础上，针对工业控制器回路攻击、组态数据篡改等安全威胁，研究涵盖协议安全分析、自适应敌手攻击、纵深防御效果评估的工业控制系统攻击模型。①协议安全性分析。工业控制协议是工业控制系统的重要组成部分，协议设计、实现、接口以及流程上的脆弱性都会给工业控制系统带来安全威胁。本文拟采用仿真与建模的思路对协议进行安全性分析：标准符合性测试，将其与标准规定的内容进行比对，进行一致性测试；协议自动化检测，构建从系统配置或协议输入到分析结果输出的高度自动化工具；协议形式化分析方法，基于模型检验和定理证明理论，借助 Pi 演算和串空间等手段分析协议流程的安全属性。②自适应敌手攻击。在综合分析敌手攻击能力以及工业控制系统脆弱性的基础上，采用攻击防御有向图的方法，基于攻击者挑战游戏框架建立自适应敌手攻击模型，在模型中对攻击防御能力、时间、概率以及成本等因素进行全面的定义和描述。自适应敌手攻击模型的核心拟从传统的以防护能力为主转向以检测能力为主，形成一个涵盖风险识别、安全防御、安全检测、安全响应和安全恢复 5 个阶段的闭环框架。③纵深防御效果评估。工业控制系统的各层次设备和网络构成不一、特点不尽相同，不可能采用统一的防御方法，从而导致每个层次的防御方法是独立分散的，很难评估整体的防御效果。纵深防御效果评估的研究会对各个层次之间的相互关系和交互进行考虑，建立一个涵盖定性和定量两方面的综合防御效果评估模型。因此，研究针对纵深防御效果评估的定性和定量评估方法：定性评估主要用来确立和描述防御效果的有效性；定量评估在定性的基础上给出防御效果的具体量化指标。

2）面向工业控制系统威胁情报的自适应防御体系的研究。①工业控制系统的分区隔离纵深防御。基于信息保障安全理念研究工业控制系统的分区隔离纵深防御，采用一个多层次的、纵深的安全措施全方位地保障工业控制系统的安全。工业控制 DCS 系统采用结构化防护，工业控制网络实施分层分区防护，网络安全传输采用纵深防御机制，通过集中式的安全管理中心制定统一的工业控制系统安全防护策略，用于控制各级安全系统的防御规则。②工业控制系统的动态防护和主动防御。研究工业控制网络的动态防护机制，依托工业防火墙、安全网闸、网络通信加密机、入侵检测系统、身份认证系统、密钥管理系统和全网态势感知系统，建立工业控制系统面对网络攻击的应急响应防护机制，保障网内数据通信的机密性和完整性。研究以工业控制白名单和网络动态监控为核心的主动防御机制，采用网络态势感知、大数据流量分析、入侵检测等方式对工业控制网络通讯和工业控制协议实施实时监控；基于工业控制终端内核安全加固和主机防护，研究工业控制系统的主动防御机制，及时发现网络中的异常事件和被攻击感染的工业控制终端，准确定位潜在危险程序，并根据用户配置采取报警、隔离等多种主动防护手段，提升工业控制系统网络和终端设备的主动防御能力。③基于漏洞深度检测等威胁情报的自适应防御体系。研究基于威胁情报的攻击者的攻击路径以及当前工业控制系统被攻击的态势，自适应地调整防御资源，实施安全响应和恢复。通过收集、评估和应用安全威胁、攻击利用、恶意软件以及漏洞指标等核心关键情报，有针对性地调整和部署重要的防御工具和系统。研究基于漏洞深度检测等威胁情报的工业控制网络可视化分析，实现工业控制系统网络攻击事件的“事前、事中、事后”的全过程覆盖，形成自适应的具备安全威胁的识别、预防、发现、响应等能力的安全防御体系。④基于硬件安全模块的可信工业控制防护系统。基于硬件密码模块的工业控制系统安全增强体系结构，针对工业控制环境的操作站、控制站等系统设备，使用硬件密码模块对工业控制系统体系进行安全增强，实现可信引导、操作系统内核级信任链构建、完整性度量、安全存储、隔离执行以及多因素认证等信任构建技术，达到系统级和硬件级的安全。嵌入式工业控制设备轻量级可信执行环境技术体系，针对工业控制现场的 PLC、控制器、传感器、执行器和底层智能设备等嵌入式系统，实现轻量级的信任根构建技术；设计嵌入式设备的安全度量与启动，完善嵌入式操作系统的加固防护，并实现对嵌入式关键系统组件和模块的芯片级认证功能。

（2）工业控制系统安全漏洞挖掘与利用技术的研究。研究工业控制系统协议、软件、硬件的测试与分析方法，研制工业控制系统的漏洞挖掘平台，挖掘工业控制系统的漏洞。研究针对工业控制系统专用（非公开或私有）协议的逆向分析方法，挖掘工业控制专用协议在设计与实现上的漏洞；针对典型工业控制系统中的组态软件、监控软件、工业实时数据库、控制站嵌入式软件等核心组件，研究静态与动态的漏洞分析挖掘方法，挖掘工业控制系统软件漏洞；针对工业控制系统的硬件与芯片，基于板卡级解剖分析、非侵入/半侵入检测分析等技术手段，挖掘工业控制系统的硬件漏洞；研究针对工业控制系统的漏洞测试样例设计和渗透检测方法，形成漏洞测试样例集并进行测试验证。

1）工业控制协议逆向分析方法与漏洞挖掘的研究。研究针对工业控制系统专用（非公开或私有）协议的逆向分析方法，根据协议的解析结果分析协议的安全性，生成针对性的测试数据，挖掘工业控制协议漏洞。①基于指令语法格式、库函数参数格式等知识，运用数据流分析等动态分析技术，研究提取协议数据包语法格式的方法；②基于工业控制协议数据包的语法格式，运用状态标记、数据规约等技术，研究协议状态机的还原方法；③基于工业控制协议状态机信息，采用模型检测等方法分析协议的安全性，根据协议的语法格式生成测试用例，挖掘工业控制协议漏洞；④研发工业控制协议逆向分析平台，使其具备工业控制私有协议的安全性分析能力，并通过协议逆向分析恢复出 2 种以上的非公开工业控制协议。

2）工业控制系统软件漏洞挖掘方法的研究。针对传统漏洞挖掘方法存在的漏洞针对性不强、准确性不高等问题，研究基于动态靶向分析的软件漏洞挖掘与分析方法，以挖掘工业

控制系统的软件漏洞。研究针对工业控制系统核心部件的、基于动态靶向分析等的逆向分析方法，以挖掘工业控制系统软件漏洞。①研究基于机器学习方式提炼工业控制系统的行为模式，形成以其为引擎来捕获工业控制系统异常行为的方法；②基于工业控制漏洞机理的分析和模型的构造，研究利用污点传播、符号执行等技术判定软件漏洞的方法，同时结合符号执行与路径约束求解技术，根据漏洞对应的异常状态，生成有针对性的测试数据，以提高漏洞分析的效率；③研究工业控制数据采集机制，分析基于定向或非定向的攻击状态捕获方法，形成工业控制调试分析状态监控机；④研究工业控制软件漏洞挖掘平台，使其具备组态软件、监控软件、嵌入式软件等工业控制核心部件的漏洞分析、挖掘和检测能力。

3)工业控制系统硬件漏洞挖掘方法的研究。研究针对工业控制系统硬件的、基于解剖分析和非侵入/半侵入检测分析等技术的逆向分析方法，挖掘工业控制系统硬件与芯片的漏洞。①基于非侵入式测试、半侵入式测试、模拟与数字量混合的测试数据生成等技术，将测试数据注入到硬件或芯片的接口或内部，以挖掘工业控制系统的硬件漏洞；②基于电路分析、算法分析、逻辑仿真等手段的硬件逆向综合分析方法，挖掘硬件或芯片设计中隐藏的缺陷或漏洞；③构建工业控制系统硬件漏洞挖掘平台，使其具备基于板卡解剖分析、芯片解剖分析等技术手段的硬件漏洞挖掘能力。

4)工业控制系统漏洞利用方法的研究。针对在典型工业装置、主流工业控制系统核心部件上挖掘出的漏洞，研究相应的利用方法，创建漏洞利用样本，建立漏洞测试样例集。①基于工业控制系统软、硬件漏洞的威胁对象类型、使用权限、攻击方法等特征要素，研究各类工业控制协议测试样例的构造方法，以构建不同类型工业控制系统的漏洞测试样例集；②基于工业控制系统与传统网络系统的结构性、安全机制差异，结合传统的漏洞扫描技术，研究工业控制系统漏洞扫描方法；③基于漏洞测试样例集，对漏洞进行深度利用分析，研究工业控制系统渗透测试策略、测试框架与测试流程，并在工业控制系统测试验证的基础环境下对漏洞渗透测试方法进行验证；④研发工业控制系统漏洞利用工具集，使其涵盖篡改组态数据、伪造控制指令、实时欺骗、获取超级权限等4类以上漏洞类型的测试样例。

(3)工业控制系统安全技术测试验证方法的研究。以电厂DCS系统、PLC控制系统、电网调度控制系统为典型的工业控制系统测试验证平台，构建覆盖应用软件、嵌入软件、传输网络、通信协议以及设备硬件、板块、芯片器件的工业控制系统漏洞挖掘、检测、评估、攻防实验等工业控制系统安全技术的测试验证环境；开展电力工业控制系统典型攻防仿真与验证技术的研究，形成工业控制系统信息安全的评估方法与标准；建立电力工业控制产品测评认证、产品供应链备案与安全检测验证、漏洞分析与预警通报、应急响应、风险评估、安全管理等的安全保障机制。

1)研究设计工业控制系统典型装置的测试验证平台。研制以电力DCS系统、PLC控制系统、电网调度控制系统为典型的工业控制系统仿真平台，构建覆盖应用软件、嵌入软件、传输网络、通信协议以及设备硬件、板块、芯片器件的工业控制系统漏洞挖掘、检测、评估、攻防实验等工业控制系统安全技术的测试验证环境。主要包括：①搭建可动态扩展和配置的工业控制系统产品测试平台，为工业控制系统产品的漏洞挖掘、安全检测、风险评估、攻防实验、安全防护等活动提供基础测试环境；②构建行业仿真平台，为工业控制系统整体安全性的检测、分析、评估等工作提供基础检测平台，以进行工业控制系统安全检测、风险评估、攻防实验，研究工业控制系统安全防护的相关技术；③建立工业控制系统网络技术研究的测试环境，包括搭建有线/无线通信网络、常用现场控制总线(Profibus，FF，LonWorks，CANBUS等)、常用工业控制通信协议(ModBus/TCP，DNP，ProfiNet等)等测试环境。

2)研究工业控制系统攻击效果和安全防御量化评估方法。①研究工业控制系统的攻防技术，评估工业控制系统漏洞的危害，复现工业控制系统的漏洞，挖掘漏洞之间的关联关系，构建漏洞的验证平台，测试验证漏洞挖掘结果的正确性，漏洞利用方法的有效性、实用性和隐蔽性，以及漏洞规避技术的有效性；②开展典型工业控制系统的仿真攻击和攻防演练，利用攻击测试用例，针对防护组件/工具盒防御系统，开展篡改组态数据、伪造控制指令等工业控制系统攻防对抗测试，评估安全风险。建立工业控制产品测评认证、产品供应链备案与安全检测验证、漏洞分析与预警通报、应急响应、风险评估、安全管理等安全保障机制。

(4)工业控制系统动态防护组件纵深防御功能实现方法。以国产CPU为基础，研究支持多种工业控制协议的可编程嵌入式电子设备以及实时控制与监控软件等工业控制系统组件的动态防护关键技术，从整体上提供主动防御功能。研究具有异构冗余、动态重构、随机多样化特征的动态防护工业控制系统组件，其主要分为4类，包括安全固件、安全功能组件、系统安全组件、控制功能保护组件。安全固件是基于国产SPARC V8 CPU芯片的PLC/RTU/控制器，研发现场总线、安全网络、安全内存管理技术。另外，通过对安全固件技术的研究，能够实现系统的异构冗余，从而提高系统的生存性；通过对安全功能组件及系统安全组件技术的研究，能够使系统具备动态重构的功能，使系统在发生紧急状态时在线切换至备份或安全状态；通过对控制功能保护组件技术的研究，使系统能够防止猜测嗅探、重放攻击等。

研究动态防御组件，突破防护组件的“异构冗余、动态重构、随机多样化”关键技术，研制具备动态防护功能的安全组件。该系列组件覆盖工业控制系统的第0层到第3层，构成纵深防御体系。工业控制网内部用二维白名单法，对设备间的通讯实施访问控制，对表面合法但会干扰或破坏控制过程的行为实行阻隔保护；对于组态数据、关键控制指令、重要模拟量、开关量等，通过加随机数、时间戳、报文摘要及加解密等方法防篡改、伪造、欺骗；用挑战-响应法进行身份鉴别，实现授权/未授权角色识别；对异构冗余、主从备份系统的输入/输出信息关联分析，进行安全预警和应急处理，在攻击发生时实行切换功能重构，以提高抗攻击的生存能力。该组件主要包括：1)基于国产CPU体系结构，面向工业系统的生产控制和安全保护层的基础安全组件。研发的PLC/RTU/控制器选用国产SPARC V8 CPU芯片，研发现场总线、安全网络、安全内存管理技术，根据JEDEC内存接口定义标准，利用SOC插入安全逻辑，构造增强信息安全的体系结构。对CPU驱动、

组件的自主开发，提供以下功能：对 OS、应用程序安全验证后不可改写的保护；敏感数据的保护，实施访问控制；反跟踪技术，即未经授权不能反汇编与调试跟踪；工业控制变量强制，即在运行中不能因信号读入或计算而发生变化，其保证了信息安全，防止恶意逻辑使用强制攻击。2）应用二维白名单法的信息安全实时监控。白名单法的第一维是传统意义上的白名单，如网络的地址、端口号等实体属性，第二维是在第一维实体上的行为模式。在第一维上的合法属性，在第二维上则有合法和非法两种情况，如对 PLC 的正常网络通讯是合法的，但加大通讯量后其就变为攻击。在研究关联分析技术、追溯技术的基础上，开发信息安全实时监控平台，实时收集各设备的运行状态；对非法和偏离正常的行为模式进行监控、处理；应用事件关联分析进行预警防护。3）工业控制冗余安全保护系统的动态重构主动防御技术。对以控制器、现场总线、传感器和执行器构成的控制回路进行故障模式影响分析，鉴于信息安全和功能安全都是保障系统在规定的时间和条件下完成规定的任务，引入有信息安全因素的故障原因分析和故障检测方法，研究双机冗余技术和异构的安全保护系统。对信息安全类的攻击实现动态冗余保护和故障隔离；对冗余和异构的安全保护系统的多路输入信息的差异性进行关联分析，捕捉可疑行为，进行实时监控。4）国产 CPU 4 核协同控制应用组件。基于国产 SPARC V8 CPU 4 核研发的 PLC/RTU/控制器，将控制、现场总线及安全监控、网络及防火墙组件、OPC UA 互联的开放性及安全防护等功能集于一体，解决共享内存 4 核应用的安全协同工作问题。与传统 IT 多核 SMP 方式不同，共享内存的 4 核在该体系中担任不同的角色，屏蔽了网络对控制回路的干扰和攻击，在内存储器和各内核实行分区隔离，网络及防火墙组件内核与其他内核的数据交换通过安全管道实现，形成多重防御，并提供互联互通的开放性。5）工业控制网络协议过滤与保护组件。该组件用于分隔安全域，或集成在网络互联设备上，支持对工业控制协议的过滤保护。6）安全工业以太网交换技术。突破网络全端口实时监控技术，基于白名单的第一维阻止非法访问，对全部网络端口实时监控并及时上传安全信息。7）基于二维白名单的 PLC/RTU/控制器的网络接口保护技术。对设备的网络接口处：对白名单中的第一维网络流实施访问控制；对白名单中的第二维貌似合法但偏离正常行为模式的攻击，根据包速率门限实行关门保护。8）安全组态系统。研发遵循 IEC 61131-3 标准的安全可控的 ST 结构文本、FBD 功能块语言、LD 梯形图语言；基于身份鉴别实现操作管控，采用加密等方式，实现日志防篡改及下装防篡改等；对组态下装操作者实行身份鉴别授权下装。9）现场总线实时监控技术。研发实时监控现场总线运行状态的组件，将掉线、IO 模块脱机、应答丢失、异常迟延、异常信号等事件及时发送到信息安全实时监控平台，并通知人员进行处置。10）现场总线模块的安全保护。现场总线 IO 模块相连接的执行器、传感器都有合理的数据区间，针对超限会引起事故的 IO 模块，研发需由人工通过拨码开关等设置强制限制的保护组件，当设置有效时，攻击者即使篡改了指令，仍无法使执行器做超限动作，例如可防止离心机因超速而被毁坏。11）工业控制环境的身份鉴别技术。使用基于随机阵列的挑战-响应法等随机多样化处理方法提供用户身份鉴别，防止口令嗅探、重放攻击。12）工业控制网络防篡改技术。运用报文摘要算法、密码算法、随机数加时间戳等，对组态下装程序、操作命令、设定的参数、采集的重要数据、SOE（事件顺序记录系统）记录等进行防篡改处理。13）工业控制网络加密保护技术。对有加密需求的网络通讯数据，在应用层加时间戳或随机数，做报文摘要后进行加密处理。14）可信工业控制动态防护技术。针对上位机操作系统面临的安全威胁，研制包含上位机认证和管控、USB 管控等的防护工具，基于安全可信芯片实现工业控制上位机系统安全加固、进程度量和运行状态监控等功能。15）实时库/历史库/审计库安全。研发基于角色的访问机制，三权分立，设有管理员、安全员、审计员，设计实时数据库的细粒度安全访问控制机制。

（5）工业控制系统主动防御技术的研究与应用。对安全级 DCS 和非安全级 DCS 开展主动防御技术的研究。安全级 DCS 针对边界数据隔离（包括多序列保护、单一合法数据源）、状态实时监控（包括 IO 逻辑控制、数据交叉校验等）、高危攻击应急处理等技术进行研究，提升控制器的防护能力；同时开展硬件、网络、数据全冗余和实时诊断措施等研究，确保单一故障不影响工业控制系统的正常运行。非安全级 DCS 对安全配置基线动态扫描技术进行研究，以保障用户数据的保密性和完整性；对策略防护、可信检查、实时进程监控等技术开展研究，以增强上位机的主动防御能力。

1）边界数据隔离。研究序列保护、多重身份、单一合法数据源、信息验证以及通信信息安全相结合的边界数据隔离技术；研究适用于安全级系统与非安全级系统通讯的私有通讯协议；自定义 CRC 算法多项式验证通信信息的完整性；研究通过自定义信息规则判定信息合法性的相关技术；研究纵深防御策略对控制系统与工程师站连接的多重防护技术；研发基于密码验证的维护下装软件和工具；研究多重物理防护的工程师站与控制系统的连接技术，只有在旁通状态下安全级系统才能与工程师站连接。旁通状态下，安全级系统不参与安全功能，在端口连接盘处，保证工程师站同时只能连接一个通道或序列，而且不会同时影响其余通道。

2）状态实时监控。DCS 在正常运行过程中需要处理大量初始和过程变量，每一个变量代表了其背后物理量的实时状态。常规 DCS 无法做到对每一个变量进行实时处理监视，否则会影响 DCS 的正常功能。基于统计理论识别出关键状态数据，确定该关键状态数据在 DCS 内部的生灭过程（产生、传输、运算、执行、终止、清除）所关联的硬件设备和软件程序，在此基础上开展智能机内测试技术、IO 逻辑控制、数据交叉校验、状态信息传输与上报技术的研究，并针对关键状态数据进行实时监视，一旦出现异常就启动高等级处理保护机制，将信息安全威胁彻底隔离，以将后果降至最低。

3）高危攻击应急处理。当高等级信息安全威胁突破 DCS 防护边界并伪装躲过状态实时监控时，表明 DCS 已完全丧失外部保护能力，内部核心数据和算法处在高风险状态，随时可能出现数据窃取或程序篡改等情况。针对这一问题，基于大数据理论，对异常工况数据开展特征分析，抓取正常工况的数据行为作为判断基准。研究基于判断基准的实时启动数据隔离技术和安全输出技术。

4）安全配置基线。研究 DCS 系统的外部影响，剖析 DCS

系统平台进程原型的必要条件，分析 DCS 系统的威胁、弱点和风险，结合安全整改和安全建设确定 DCS 系统服务和应用程序设置、操作系统组件设置、权限和权利分配的原则，识别 DCS 系统运行过程中必需的服务和设置；重点研究操作员站、工程师站、服务器的安全配置，包括密码策略、授权、日志、服务、启动项、注册表、会话设置、协议配置等，形成一套标准的安全配置基线设置方法，在系统检修、停机或新系统上线时进行安全配置基线设置方法的验证。

5)上位机主动防御能力。研究上位机可信检查的方法，实时监控阻断恶意软件的安装和运行，生成审计日志，协助管理员发现异常事件，有效抵御零日攻击及高级持续性威胁，灵活配置增强安全，同时降低维护成本；研究上位机主动检查 U 盘等移动介质的方法，防止病毒传播；研究工程师站身份鉴别技术，仅对获得权限的人员赋予控制权；研究上位机系统对外接口隔离技术，做到控制区和非控制区的隔离。

5 下一步工作

工业控制系统的重大共性关键安全技术尚需突破，适应我国工业控制安全需要的技术体系和安全标准等研究相对滞后。为此，本文针对我国工业控制系统安全尚需解决的关键技术问题展开研究，主要包括以下几方面。

(1)工业控制系统攻击模型与安全防护体系的构建。1)工业控制系统多样性和个性化安全问题突出，单一的检测防护技术手段难以抵抗专业化的高级威胁攻击，需要针对工业控制系统的攻击机理和系统特征，建立系统化、层次化的工业控制深度攻防技术体系和理论模型。2)工业控制系统容易受到病毒或者恶意代码的攻击，工业控制软件容易被篡改，需要研究基于硬件的安全加固机制，从体系结构层面增强工业控制系统底层的安全性；新的高级攻击方式也不断涌现，依赖代码、漏洞等特征的安全技术不足以应对新的威胁，需要建立动态防护和主动防御机制。

(2)工业控制系统漏洞挖掘技术的研究。1)工业控制系统专用协议的深度解析。针对工业控制系统专用(非公开或私有)协议，研究基于动态数据流分析、数据结构分析和数据规约等技术的方法，解决工业控制系统专用协议语法格式信息恢复、交互过程状态机恢复的问题。2)工业控制系统核心部件行为特征的提取。针对典型工业装置主流控制系统的组态软件、监控软件、工业实时数据库、控制站嵌入式软件等核心部件，研究基于源代码审计、二进制代码指纹分析、系统跟踪调试等的静态与动态分析技术方法，解决在不同硬件体系下运行而在不同指令集实现的工业控制软件行为特征提取与判定的问题。3)工业控制系统漏洞机理的分析与深度利用。针对不同功能、不同类型的工业控制部件所存在的漏洞，研究并设计基于各类典型漏洞行为模式分析、作用机理分析和攻击测试的样例，解决工业控制系统漏洞深度利用的问题。

(3)工业控制系统安全技术测试验证方法的研究。1)研究 DCS 系统、PLC 控制系统、电网调度控制系统等典型工业控制系统的安全攻击和防御量化评估技术、漏洞重现技术和验证方法，开展典型工业控制系统仿真攻击和攻防演练，实现工业控制系统安全态势感知和安全指数发布的动态可视化展示技术。2)构建行业级的电力工业控制系统安全防护技术的测试验证环境，该环境覆盖应用软件、嵌入软件、传输网络、IP/Modbus 等通信协议以及设备硬件、板块、芯片器件的工业控制系统漏洞挖掘、检测、评估、攻防仿真和演练，建立电力工业控制产品测评认证、产品供应链备案与安全检测验证、漏洞分析与预警通报、应急响应、风险评估、安全管理等安全保障机制。

(4)工业控制系统组件动态防护技术的研究。针对工业控制系统实时性和连续性强的特点，采用国产化元器件和设备解决现有工业控制系统漏洞防护难的问题。主要关键问题包括：1)工业控制网络内部关键节点的监控和防护问题。研制针对工业控制网络关键节点的安全监控设备，对控制器上工业控制现场网络的第一层控制回路提供防护，实施网络数据流量和异常行为的监控，解决工业控制系统关键 PLC/RTU/控制器和全部端口的动态监控问题。2)国产化工业控制核心组件的关键技术。依据国内外对工业控制信息安全的要求，在工业控制系统的核心安全体系架构的基础上，采用国产化 CPU 实现工业控制现场总线、设备和网络等核心组件的研制，解决国外高端核心技术和产品潜藏的安全漏洞和后门难以防护的问题。3)防护组件的异构冗余、动态重构、随机多样化关键技术。当工业控制系统受到攻击时，提高系统冗余性，动态重构系统，保证控制系统功能的正常运行，利用控制系统的主-备冗余和关键工业控制应用所特有的异构安全保护系统，有效发现攻击探测活动并及时预警定位，应用工业控制系统异构冗余、随机多样化等关键技术解决工业控制的系统安全防护问题。

(5)工业控制系统主动防御技术的研究与应用。1)基于动态重构的高危应急处理技术。研究大数据理论，分析高危等级威胁的攻击特征，当攻击特征量超出正常范围时，触发 DCS 的动态重构机制，迅速对受到破坏的设备进行隔离和报警，并切换至备份系统，重新建立之前已经丧失的保护功能。2)基于智能学习的主动防御技术。本文针对工业控制系统的漏洞和相应的攻击手段，对上位机、工程师站、一层控制站的安全策略进行动态监测，引入具备智能学习能力的防护机制，建立一整套针对工业控制系统的主动防御技术。

结束语 本文紧紧围绕我国工业控制网络安全领域的现实需求，着眼于逐步推动建立起与国际同步并适应我国工业控制安全发展的、自主的工业控制网络安全保护体系和测评分析体系，聚焦工业控制网络的安全重要技术，着力研究并提出工业控制网络的安全基础理论和关键技术，以漏洞挖掘与利用研究为主线，以理论与体系架构研究和安全技术测试验证平台建设为基础，以动态监测防护和主动防御为目标，以测试样例集攻防验证与典型示范为应用，提出工业控制系统漏洞挖掘、深度检测、动态防护、主动防御等整体安全技术解决方案，设计并构建集漏洞挖掘、验证评估、动态防护、主动防御于一体的工业控制系统安全技术体系。本文同时还提出了工业控制系统安全研究的主要内容和研究方法，并归纳总结了我国工业控制系统安全尚需解决的关键技术问题。这些研究工作的有效落实以及关键技术问题的有效解决，对于提高我国工业控制领域的安全技术水平具有十分重要的现实作用和深远的社会意义。

参 考 文 献

[1] SADEGHI A R, WACHSMANN C, WAIDNER M. Security and privacy challenges in industrial internet of things[C]// Proceedings of the 52nd Annual Design Automation Conference. ACM, 2015: 54.

[2] THABET A. Stuxnet_Malware_Analysis_Paper[J]. Freelancer MMware Reseafcher, 2010: 3-28.

[3] 安天实验室. 对 flame 病毒攻击事件的分析报告[R]. 哈尔滨：安全实验室，2012.

[4] RAVAL S. BlackEnergy a threat to Industrial Control Systems network security[J]. International Journal of Advance Research in Engineering, Science & Technology(IJAREST), 2015, 2(12): 31-34.

[5] LAI Y X, LIU Z H, CAI X T, et al. Research on intrusion detection of industrial control system[J]. Journal on Communications, 2017, 38(2): 143-156. (in Chinese)
赖英旭，刘增辉，蔡晓田，等. 工业控制系统入侵检测研究综述[J]. 通信学报，2017，38(2)：143-156.

[6] SUN Y A, JING K, WANG Y Z. A Network Security Protection Research for Industrial Control System[J]. Journal of Information Securyity Research, 2017, 3(2): 171-176. (in Chinese)
孙易安，井柯，汪义舟. 工业控制系统安全网络防护研究[J]. 信息安全研究，2017，3(2)：171-176.

[7] YI S W, ZHANG C B, XIE F, et al. Security analysis of industrial control network protocols based on Peach [J]. Journal of Tsinghua University(Science & Technology), 2017, 57(1): 50-54. (in Chinese)
伊胜伟，张翀斌，谢丰，等. 基于 Peach 的工业控制网络协议安全分析[J]. 清华大学学报(自然科学版)，2017，57(1)：50-54.

[8] ZHANG Y F, HONG Z, WU L F, et al. State based Fuzzing method for industrial control protocols[J]. Computer Science, 2017, 44(5): 132-140. (in Chinese)
张亚丰，洪征，吴礼发，等. 基于状态的工业控制协议 Fuzzing 测试技术[J]. 计算机科学，2017，44(5)：132-140.

[9] YU C Q. The Study of Industry Control System Device Vulnerability Discovery[D]. Beijing: Beijing University of Posts and Telecommunications, 2015. (in Chinese)
于长奇. 工业控制设备漏洞挖掘技术研究[D]. 北京：北京邮电大学，2015.

[10] JIA C Q, FENG D Q. Security assessment for industrial control systems based on fuzzy analytic hierarchy process[J]. Journal of Zhejiang University(Engineering Science), 2016, 50(4): 759-765. (in Chinese)
贾驰千，冯冬芹. 基于模糊层次分析法的工业控制系统安全评估[J]. 浙江大学学报(工学版)，2016，50(4)：759-765.

[11] GONG S D, WANG L. Cyber Security Risk Assessment for Industrial Control System Based on AHP and Information Entropy [J]. Industrial Control Computer, 2017, 30(4): 11-12, 15. (in Chinese)
龚斯谛，王磊. 基于 AHP 与信息熵的工业控制系统信息安全风险评估研究[J]. 工业控制计算机，2017，30(4)：11-12，15.

[12] ZHONG L G. Research of Information Security Solutions of Industrial Control System Based on Trusted Computing [D]. Dalian: Dalian University of Technolngy, 2015. (in Chinese)
钟梁高. 基于可信计算的工业控制系统信息安全解决方案研究[D]. 大连：大连理工大学，2015.

[13] WU H. Research on Industrial Control Environment Computing Node Security Protection Technology[D]. Beijing: Beijing University of Technolngy, 2016. (in Chinese)
吴欢. 工业控制环境计算节点安全防护技术研究[D]. 北京：北京工业大学，2016.

[14] LIU N, YU X H, ZHANG J H. Coordinated Cyber-attack: Inference and Thinking of Incident on Ukrainian Power Grid[J]. Automation of Electric Power Systems, 2016, 40(6): 144-147. (in Chinese)
刘念，余星火，张建华. 网络协同攻击：乌克兰停电事件的推演与启示[J]. 电力系统自动化，2016，40(6)：144-147.

[15] ASGHARI H, CIERE M, VAN EETEN M J G. Post-mortem of a zombie: conficker cleanup after six years[C]// Usenix Conference on Security Symposium. 2015: 1-16.

[16] ISA. Security for Industrial Automation and Control Systems: ANSI/ISA-99. 00. 01-2007[S].

[17] IEC. Industrial communication networks-Network and system security IEC: 62433[S]. Geneva: IEC, 2009.

[18] Department of Energy Federal Energy Regulatory Commission: Mandatory Reliability Standards for Critical Infrastructure Protection [OL]. https://www. gao. gov/products/GAO-08-493R.

[19] The Smart Grid Interoperability Panel Cyber Security Working Group. Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security[OL]. https://www. smartgrid. gov/files/nistir_7628_. pdf.

[20] Regulatory Guide 5. 71. Cyber security programs for nuclear facilities[M]. U. S. Nuclear Regulatory Commission, 2010.

[21] SCHNEIER B. Attack trees[J]. Doctor Dobbs Journal, 1999, 24(12): 21-29.

[22] PIÈTRE-CAMBACÉDÈS L, BOUISSOU M. Beyond attack trees: dynamic security modeling with Boolean logic Driven Markov Processes(BDMP)[C]// Dependable Computing Conference(EDCC). IEEE, 2010: 199-208.

[23] KUIPERS D, FABRO M. Control systems cyber security: Defense in depth strategies[C]// Conference: 2007 ISA Expo.

[24] HADZIOSMANOVIC D, BOLZONI D, ETALLE S, et al. Challenges and opportunities in securing industrial control systems [C]// Complexity in Engineering(COMPENG). IEEE, 2012: 1-6.

[25] ETALLE S, GREGORY C, BOLZONI D, et al. Monitoring Industrial Control Systems to improve operations and security [R]. Security Matters, 2013.

[26] 全国工业过程测量控制和自动化标准化技术委员会. 工业控制系统信息安全：GB/T30976-2014[S].

[27] KONSTANTINOU C, MANIATAKOS M. Impact of firmware modification attacks on power systems field devices[C]// IEEE International Conference on Smart Grid Communications. IEEE, 2015: 283-288.

[28] National Institute of Standards and Technology . Measurement Challenges and Opportunitie s for Developing Smart Grid Testbeds Workshop 2014[OL]. http://www. nist. gov/smartgrid/upload/SG-Testbed-Workshop-Report-FINAL-1-2-8-2014. pdf.

[29] Idaho National Laboratory. National SCADA Test Bed(NSTB) Program[OL]. https://www. inl. gov.