同行专家业内评价意见书编号：20250854346

附件1

浙江工程师学院（浙江大学工程师学院）
同行专家业内评价意见书

姓名：王羽纯

学号：22260276

申报工程师职称专业类别（领域）：电子信息

浙江工程师学院（浙江大学工程师学院）制

2025年03月17日

填表说明

一、本报告中相关的技术或数据如涉及知识产权保护、军工项目保密等内容，请作脱密处理。

二、请用宋体小四字号撰写本报告，可另行附页或增加页数，A4纸双面打印。

三、表中所涉及的签名都必须用蓝、黑色墨水笔，亲笔签名或签字章，不可以打印代替。

四、同行专家业内评价意见书编号由工程师学院填写，编号规则为：年份4位＋申报工程师职称专业类别(领域)4位+流水号3位，共11位。

一、个人申报

（一）基本情况【围绕《浙江工程师学院（浙江大学工程师学院）工程类专业学位研究生工程师职称评审参考指标》，结合该专业类别(领域)工程师职称评审相关标准，举例说明】

1. 对本专业基础理论知识和专业技术知识掌握情况(不少于200字)

在研究生学习期间和专业实践期间，我深入掌握了工业控制系统的基础理论知识与工控安全专业技术知识。我对工控系统的网络结构、通讯原理及其安全性进行了深入研究，为了开展其通信协议的模糊测试研究，我系统性地学习了网络通信原理、数据分析技术、软件开发技术以及模糊测试技术原理，特别是在模糊测试技术方面，我不仅学习了相关的理论知识，还熟练掌握了多种模糊测试工具的使用，如AFL、AFLNet和Peach等，并在常见通信协议上进行了实验测试。此外，对于流量的抓取、分析以及协议的自动化分析也有充分了解。

2. 工程实践的经历(不少于200字)

我参加了中广核研究院有限公司的实践，主要参与网络安全保护系统设计及其在棒控棒位系统上的应用测试部分任务。我参与网络安全保护系统中安全通信网络部分的网络安全防护方案设计，研究通信协议模糊测试技术，以实现通信协议部分的漏洞挖掘，从而提升系统通信网络的安全性；参与网络安全保护系统在棒控棒位系统上的应用测试，以确保系统设备满足网络安全等级保护相关政策规范和技术标准的相关要求，主要参与某核电站棒控棒位系统项目的网络安全保护系统集成测试。实践过程中了解了核电站典型仪控系统网络架构与常用通信协议，完成了系统网络架构的设计与搭建，掌握了模糊测试工具的原理，进行了工业控制系统通信协议的模糊测试技术研究，开发了一种针对工业控制系统通信协议的模糊测试工具，实现了模糊测试工具在核电站典型仪控系统上的应用，基于通信协议模糊测试技术研究核电站棒控棒位系统网络安全保护系统设计，提高了棒控棒位系统的网络安全水平，取得了良好的成果。

3. 在实际工作中综合运用所学知识解决复杂工程问题的案例（不少于1000字）

在实际工作中，我也面临了一些挑战，并综合运用所学的知识来解决这些复杂的工程实际问题。

首先，在核电站仪控系统通信协议模糊测试技术的工作中，我所面临的挑战不仅来源于系统本身的复杂性，还包括在测试过程中必须兼顾的高安全性要求。核电站作为国家基础设施之一，其仪控系统对设备的安全性和稳定性要求极高。任何一个细微的漏洞或测试过程中的误操作，都可能对核电站的正常运行造成严重影响，甚至带来潜在的安全风险。因此，在开展模糊测试的同时，我们必须严格控制风险，确保不会影响系统的正常工作。在实验中，需要采用离线的测试研究方法，以免影响核电站的正常运行。

其次，核电站仪控系统具有较高的复杂性，核电站的仪控系统通常由多个独立的子系统构成，涵盖了实时数据采集、控制指令传输、设备监控等多个环节。每个子系统内部以及各个子系统之间通过复杂的通信协议进行数据交换，且每个协议和设备的通信方式都具有其特定的要求。除此之外，核电站的仪控系统经常采用一些高安全性标准的加密协议和自定义的传输方式，目的是为了防止外部攻击或内部数据泄露。对于我们来说，如何应对这些高安全性设计，并在不干扰正常运行的情况下，进行全面且高效的模糊测试，成为了一个巨大的挑战。为了应对这一挑战，我结合了多种技术方法，包括流量分析、程序分析等，结合通信协议模糊测试技术，来对系统进行全方位的安全性评估。

其中，最具挑战性的部分是核电站仪控系统的通信协议大多存在复杂的状态，如何准确识别这些状态是一个难题。我通过提取程序执行过程中保存程序状态信息的变量信息，并将每一组状态变量数据与协议程序状态一一对应，来识别出程序的状态，具有较高的准确性。具体

而言，通过建立目标协议程序的调用关系图和抽象语法树实现抽象化分析，制定一系列启发式规则识别程序中的状态变量，采用程序插桩实现状态变量的数据信息提取，对独热编码后的数据使用k-means聚类算法建立状态模型，表示协议程序的状态。

此外，在实施过程中，我还面临了如何有效选择合适的测试用例生成策略的问题。为了确定测试用例变异字节的权重，采用基于机器学习模型可解释性方法的字节变异算法，改进测试用例生成过程中变异字节的选择策略，提高测试用例生成效率。核电站仪控系统的协议非常复杂，通过反复调试和优化，结合历史数据，逐步确定了最有效的测试用例生成策略。

通过这一系列的工作，我们在核电站典型仪控系统中发现了几个关键的安全隐患，并提出了有效的防护措施。这一过程让我深刻理解了理论与实践相结合的重要性。通过将所学的专业技术知识，如数据分析、机器学习、网络通信原理以及安全防护等，应用到实际工作中，我不仅解决了复杂的工程问题，还进一步提升了自己在复杂工程挑战中分析和解决问题的能力。最终，通过这一案例，我们不仅增强了核电站仪控系统的安全性，也为其他类似领域的安全测试提供了重要的参考价值。

（二）取得的业绩（代表作）【限填3项，须提交证明原件（包括发表的论文、出版的著作、专利证书、获奖证书、科技项目立项文件或合同、企业证明等）供核实，并提供复印件一份】

1.
公开成果代表作【论文发表、专利成果、软件著作权、标准规范与行业工法制定、著作编写、科技成果获奖、学位论文等】

成果名称	成果类别 [含论文、授权专利（含发明专利申请）、软件著作权、标准、工法、著作、获奖、学位论文等]	发表时间/授权或申请时间等	刊物名称/专利授权或申请号等	本人排名/总人数	备注
一种基于状态的工控协议模糊测试方法	发明专利申请	2024年04月11日	申请号：202410435510.5	1/8	
面向核电站仪控系统的通信协议模糊测试技术研究	学位论文送审专家评阅结果全优	2025年01月07日	三优学位论文	1/1	
CNVD漏洞证书	获奖	2023年06月01日	漏洞证书2项		

2. 其他代表作【主持或参与的课题研究项目、科技成果应用转化推广、企业技术难题解决方案、自主研发设计的产品或样机、技术报告、设计图纸、软课题研究报告、可行性研究报告、规划设计方案、施工或调试报告、工程实验、技术培训教材、推动行业发展中发挥的作用及取得的经济社会效益等】

（三）在校期间课程、专业实践训练及学位论文相关情况	
课程成绩情况	按课程学分核算的平均成绩： 88 分
专业实践训练时间及考核情况(具有三年及以上工作经历的不作要求)	累计时间： 1.1 年（要求1年及以上） 考核成绩： 85 分
本人承诺	
个人声明：本人上述所填资料均为真实有效，如有虚假，愿承担一切责任，特此声明！ **申报人签名：** 王羽纯	

2226076

二、日常表现考核评价及申报材料审核公示结果

日常表现考核评价	非定向生由德育导师考核评价、定向生由所在工作单位考核评价： ☑优秀 ☐良好 ☐合格 ☐不合格 德育导师/定向生所在工作单位分管领导签字（公章）：2025年3月18日
申报材料审核公示	根据评审条件，工程师学院已对申报人员进行材料审核（学位课程成绩、专业实践训练时间及考核、学位论文、代表作等情况），并将符合要求的申报材料在学院网站公示不少于5个工作日，具体公示结果如下： ☐通过 ☐不通过（具体原因： ） 工程师学院教学管理办公室审核签字（公章）： 年 月 日

浙 江 大 学 研 究 生 院

攻读硕士学位研究生成绩表

学号：22260276	姓名：王羽纯	性别：女	学院：工程师学院	专业：电子信息	学制：2.5年
毕业时最低应获：24.0学分	已获得：29.0学分			入学年月：2022-09	毕业年月：
学位证书号：		毕业证书号：			授予学位：

学习时间	课程名称	备注	学分	成绩	课程性质	学习时间	课程名称	备注	学分	成绩	课程性质
2022-2023学年秋季学期	工程技术创新前沿		1.5	90	专业学位课	2022-2023学年冬季学期	产业技术发展前沿		1.5	91	专业学位课
2022-2023学年秋季学期	工业互联网安全系统工程		2.0	94	专业学位课	2022-2023学年秋冬学期	研究生论文写作指导		1.0	90	专业选修课
2022-2023学年秋季学期	工业互联网系统安全前沿技术		2.0	90	专业学位课	2022-2023学年冬季学期	工程中的有限元方法		2.0	99	专业选修课
2022-2023学年冬季学期	新时代中国特色社会主义理论与实践		2.0	90	专业学位课	2022-2023学年春季学期	研究生英语基础技能		1.0	69	公共学位课
2022-2023学年秋冬学期	工程管理		2.0	85	跨专业课	2022-2023学年春季学期	自然辩证法概论		1.0	86	专业学位课
2022-2023学年秋冬学期	信息安全前沿技术与研究方法论		2.0	87	跨专业课	2022-2023学年春夏学期	高阶工程认知实践		3.0	90	专业学位课
2022-2023学年秋冬学期	工程伦理		2.0	86	专业学位课	2022-2023学年春夏学期	研究生英语		2.0	85	专业学位课
2022-2023学年秋冬学期	工业系统动态建模求解及优化		2.0	91	专业学位课		硕士生读书报告		2.0	通过	

说明：1.研究生课程按三种方法计分：百分制，两级制（通过、不通过），五级制（优、良、中、及格、不及格）。

2.备注中“*”表示重修课程。

学院成绩校核章：

成绩校核人：张梦依

打印日期：2025-03-20

(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 118427821 A
(43)申请公布日 2024.08.02

(21)申请号 202410435510.5

(22)申请日 2024.04.11

(71)申请人 浙江大学
地址 310058 浙江省杭州市西湖区余杭塘路866号

(72)发明人 王羽纯 车欣 胡玉娇 朱恒晔 孟捷 邓瑞龙 程鹏 陈积明

(74)专利代理机构 杭州求是专利事务所有限公司 33200
专利代理师 刘静

(51)Int.Cl.
G06F 21/56(2013.01)
G06F 21/57(2013.01)
G06F 11/36(2006.01)

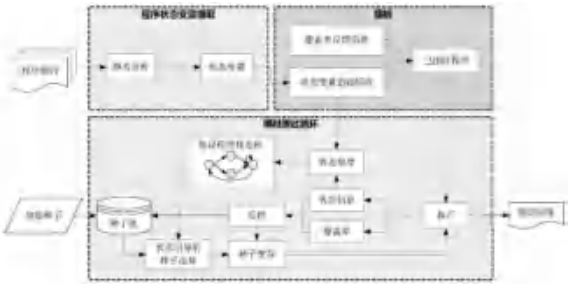
权利要求书2页 说明书4页 附图1页

(54)发明名称

一种基于状态的工控协议模糊测试方法

(57)摘要

本发明公开了一种基于状态的工控协议模糊测试方法。本发明对工控协议程序源码进行静态分析来提取状态变量;通过插桩实现状态变量追踪;执行初始模糊测试循环,收集每个变异生成的测试用例对应的状态变量值数据,完成状态变量矩阵构建,并建立状态变量矩阵对应的状态模型,构建初始协议程序状态机;再次执行模糊测试循环,挑选状态并使程序进入所选状态;生成新测试用例并执行,将产生新状态或新状态转换的新测试用例添加到种子池中,并更新状态模型与协议程序状态机,以进行新一轮循环重新选择测试用例进行变异。本发明能够检测工控协议程序的状态信息,并基于状态信息对协议程序执行状态引导的模糊测试,对于有状态的工控协议具有较好的效果。



CN 118427821 A

分类号：TP273　　单位代码：10335

密　级：无　　学　　号：22260276

浙江大学

硕士学位论文
（专业学位）

中文论文题目：面向核电站仪控系统的通信协议模糊测试技术研究

英文论文题目：Research on Communication Protocol Fuzzing for Instrumentation and Control Systems of Nuclear Power Plant

申请人姓名：王羽纯

校内导师（组）：程鹏

行业导师：钟质飞

专业学位类别、领域：电子信息　控制工程

研究方向：工业控制系统安全

培养类型：全日制非定向

所在学院：工程师学院

论文提交日期　二〇二五年三月

摘要

随着工业互联网的快速发展，原本处于信息隔离中的核电站逐渐走向开放，这在提高管理效率、提升经济性的同时，也给核电站的各个系统带来了更多的网络安全风险。核电站仪控系统在核电站中主要负责运行控制，其通信协议担负着传输生产数据和下达控制命令的重要任务，一旦仪控系统的通信协议存在安全漏洞并被攻击者利用，将会对核电站的正常运行造成严重的影响。

为了高效发现通信协议存在的安全漏洞，协议模糊测试技术成为近年来国内外研究人员的研究热点，但现有的研究成果还存在着一些不足：（1）无法准确推断目标协议的状态机；（2）无法准确地度量测试用例中不同字节的重要性；（3）目前还没有专门用于核电站仪控系统的通信协议模糊测试工具，对核电站仪控系统的通信协议缺乏系统性的安全测试。

针对以上不足，本文的主要工作和贡献如下：

（1）本文提出了一种基于程序变量的状态识别算法。通过对程序进行抽象化分析并建立启发式规则，提取协议程序中的状态变量，使用程序插桩技术收集模糊测试过程中的状态变量信息，进而建立状态模型，实现运行时协议程序的状态识别，为后续的模糊测试提供状态反馈，从而提升模糊测试的深度和覆盖度。

（2）本文提出了一种基于鲸鱼优化算法的字节变异方法。为了度量测试用例不同字节的优先变异权重，在轻量级梯度提升模型的基础上，采用鲸鱼优化算法对 SHAP 和 LIME 这两种模型可解释性算法进行优化融合，计算得到字节变异权重系数，基于此选择更重要的字节进行变异并生成新的测试用例，避免产生大量无效的测试用例，显著提高了模糊测试效率。

（3）本文设计并实现了一种面向核电站仪控系统的通信协议模糊测试工具 SWOFuzz。经实验验证，本文使用 SWOFuzz 对 4 种核电站仪控系统常见通信协议的程序进行模糊测试，共触发了 27 个崩溃，挖掘到 2 个已知漏洞，与 AFLNet、AFLNWE 这两种主流通信协议模糊测试工具相比，SWOFuzz 在分支覆盖数量上分别提升了 3.86%和 26.37%，在独特路径数量上分别提升了 23.12%和 417.28%，实验结果证明了 SWOFuzz 的有效性。

关键词：核电站；仪控系统；通信协议；模糊测试

目录

1 绪论

1.1 研究背景及意义

近年来，我国的经济进入了稳中求进的发展阶段，随着城市化和工业化进程的快速推进，人民生活水平不断提升，能源的需求量也日益增长。能源是现代经济社会的基础性来源，具有不可替代的重要性。在这样的背景下，能源领域的技术进步成为推动经济社会发展的关键因素之一，尤其是在清洁能源的发展和应用方面。

随着全球气候问题日益严重，我们对清洁能源的需求也变得愈加迫切。为了应对全球气候变暖的问题，我国提出了“碳达峰”和“碳中和”目标，致力于在未来几十年内减少碳排放，推动经济社会的绿色低碳发展。我国将逐步从过去依靠经济发展推动绿色转型，转变为通过绿色低碳的能源引领经济发展。

核能作为一种清洁、安全、高效、节能的能源形式，具有资源消耗少、发电能力强、二氧化碳排放量低等显著优势，在能源领域扮演着越来越重要的作用，逐渐成为全球能源格局中的重要一环。

我国核电技术的发展历程较短，开始较晚，但通过一系列政策引导和技术积累，已经逐步走上自主化、规模化发展的道路。伴随着改革开放的浪潮，我国商用核电在引进并消化吸收国外先进技术的同时，始终坚持自主创新，致力于打造核电技术的自主发展之路。我国不仅掌握了核电站的自主设计和建设技术，还在核反应堆、核电站运行管理、核安全保障等方面积累了丰富的经验，为后续的大规模核能应用提供了有力支持。随着技术研究的不断推动，我国的核电产业逐步形成了自主研发、设计、建设和运营的完整技术体系。特别是在新一代核电技术的研发上，我国已经逐渐实现了自主创新。例如，华龙一号核电技术作为我国自主研发的三代核电技术，已经在国内外多个核电项目中得到了应用和验证。这些技术的成熟不仅提高了核电站的安全性和可靠性，也推动了中国核能产业在国际市场的竞争力。经过数十年的努力，我国在核能安全利用的领域取得了举世瞩目的成就，跻身世界核电大国行列。

核能发展蓝皮书《中国核能发展报告（2024）》[1]从核电运行、工程建设、科技创新等方面总结分析了当前我国核能行业发展状况。报告中显示了我国核电行业的稳定发展状况，2023 年新开工了 5 台核电机组，实现了 949 亿元核电工程建设投资完成额，创下近五年的新高。我国商运核电机组安全稳定运行，“双碳”工作积极推进，能源结构持续优化，全国电力系统安全稳定运行，电力供需总体平衡，用电增速呈恢复性增长态势。

未来，核电将在中国能源转型、绿色低碳发展和应对气候变化的过程中发挥越来越重要的作用。随着全球能源结构的深刻变革，核能将成为推动全球能源可持续发展的重要力量。立足核能领域的技术积累和产业优势，我国将在全球能源格局中占据重要地位，核电必将在“碳达峰、碳中和”目标的实现过程中，发挥不可或缺的战略作用。

核电站作为能源生产的重要设施，能够提供大量清洁稳定的电能，为能源的稳定供应做出重要贡献，有助于维持经济的正常运行。核电站在提供清洁能源、促进社会发展的同时，它的安全性和稳定性一直是公众关注的焦点。核电站是一个非常复杂的系统，它的运行涉及到大量的机械设备、自动化仪器控制系统等多个领域，这些系统的安全性直接关系到核电站的整体安全。传统的核电站系统由于不需要和外界进行频繁的数据传输交互，通常通过物理隔离的方法阻断来自外部网络的攻击。然而，随着科技的快速发展，核电站使用了更多的新兴技术，在提高生产力的同时，也在无形中增加了更多的安全风险，信息安全问题日益突出。

近年来，全球范围内发生的一些核电站安全事故，暴露出核电站存在潜在的漏洞和风险[2]。2003 年 1 月，美国 Davis-Besse 核电站遭受了 SQL Slammer 蠕虫攻击，导致该核电站计算机处理速度下降，安全参数显示系统和过程控制计算机持续 5 小时无法正常运行。2006 年 8 月，美国 Browns Ferry 核电站 3 号机组受到网络攻击，导致反应堆再循环泵和冷凝除矿控制器出现故障，该机组被迫关闭。2010 年，“震网”病毒利用零日漏洞攻击伊朗核设施，致使伊朗的核计划推迟[3]。2016 年 4 月，德国 Gundremmingen 核电站的计算机系统因在进行安全检测的过程中发现了恶意程序而被迫关闭。2018 年 6 月，法国公司 Ingerop 遭到网络攻击，导致费森海姆核电站敏感数据被泄露。2019 年 9 月，印度 Kudankulam 核电站的内网感染了恶意软件。这些问题使得各国对核电站的安全性提出了更加严格要求。

在信息技术日新月异的今天，如何保障核电站的网络信息安全成为了核电安全管理的重要议题。

2023 年 7 月 14 日至 15 日，全国网络安全和信息化工作会议召开，习近平总书记对网络安全和信息化工作作出重要指示，提出了新时代新征程网信工作的使命任务，把“防风险保安全”摆在突出位置，为我国网络安全事业进一步锚定了前进航向。核电站的安全关系着国家安全，这对保障核电站的网络安全提出了更高的要求[4]。

核电站的仪控系统作为核电厂的核心部分，直接关系着反应堆、冷却系统、辐射监测、应急响应等重要的功能的控制。因此，核电站仪控系统的安全性不仅影响着核电站的运行效率，还关系着核电站的安全稳定，更关系着社会的正常发展。随着工业化和信息化的不断融合与发展，越来越多的信息化技术被应用于核电站仪控系统上。这种转变虽然提高了核电站仪控系统的自动化与智能化水平，但随之而来的是越来越大的安全挑战。由于传统的核电站仪控系统设计采用物理隔离来抵御网络攻击，因此其所采用的通信协议在设计时缺乏加密、认证、测试等安全步骤。信息化的不断发展打破了核电站仪控系统的信息隔离屏障，导致核电站仪控系统面临着巨大的安全风险。

在核电站的仪控系统中，众多控制指令和反馈信息需要通过通信协议进行传输，以实现设备之间的协调与监控。这些通信协议在核电站仪控系统的正常运行中起着至关重要的作用，涉及从设备状态监测、指令下达到报警处理等多个环节。然而，随着信息技术的不断发展与复杂性增加，通信协议的安全性问题逐渐成为威胁核电站安全运行的重要因素之一。通信协议的漏洞和潜在的攻击风险不容忽视，攻击者通过漏洞或缺陷对通信协议进行恶意操作，可以轻易地篡改控制信息，伪造或重放数据，可能导致控制指令在传输过程中出现错误或在执行阶段发生偏差。这种异常的指令传输和执行过程可能引发仪控系统功能失常，造成设备无法正常运行，甚至引发更为严重的核安全事故。

因此，加强核电站仪控系统通信协议的安全防护对于保障核电站的整体安全性具有至关重要的作用，已成为提升核电站安全性和防范潜在核风险的重要任务。针对核电站仪控系统通信协议的安全问题需要采取多层次、全方位的安全策略，从而确保核电站能够在安全、稳定的环境下运行，最大限度地降低潜在风险，保障核能安全和人民生命财产安全。

通过模糊测试技术，可以有效发现通信协议存在的漏洞，防止潜在的攻击者通过这些漏洞攻击核电站仪控系统，产生不可逆转的影响。为了发现协议实现中潜在的安全风险，通信协议模糊测试技术通过向目标程序发送大量随机或半随机的测试用例来测试其响应，从而探索程序可能存在的漏洞[5-10]。对于核电站这类高安全要求的设施而言，通信协议模糊测试技术具有重要的意义。传统的测试方法通常依赖于已知的测试用例和边界条件，这可能无法覆盖所有可能的异常情况。相比之下，模糊测试通过自动化生成大量的输入数据，模拟各种可能的恶意攻击或数据传输错误，能够揭示传统测试方法难以发现的安全漏洞，且降低了人力成本。

此外，通信协议的模糊测试技术还可以帮助提高协议实现的鲁棒性。核电站的仪控系统通常需要实现长时间的持续稳定运行，如果通信协议在面对异常输入时不能进行正确处理，可能导致系统故障或崩溃。通过通信协议模糊测试技术，开发人员能够发现并修复这些潜在的问题，增强系统在面对未知情况时的稳定性和容错性。

1.2 国内外研究现状

1.2.1 核电站仪控系统安全研究现状

目前，针对核电站仪控系统的安全研究主要为面向功能安全的测试分析。朱国亮等[11]采用潜在失效模式和影响分析工具，对棒控棒位系统的关键设备在正常的功能实现中可能出现的关键零部件失效问题进行分析，以识别设备的薄弱环节，并提出相应的改进措施，从而提高控制棒的安全性和可靠性。刘燕芳等[12]针对某核电厂棒控棒位系统现场联调时发现的问题，通过对机柜在生产、运输及工作过程中受到的环境应力进行分析，得到其所经受的环境应力及失效机理并进行研究，提出改进措施，保障系统的质量安全。何攀等[13]针对控制棒驱动机构，基于机构结构噪声检测原理，研发了一套故障检测仪，并在模拟控制棒驱动机构上进行了测试，结果表明该检测仪能够实现故障监测，具有科学性和有效性。罗慧等[14]提出了一种基于风险自动分析模型的仪控系统故障风险分析方法，将传统的分析技术互相融合，构建了风险自动分析模型，并开发了故障风险自动化分析融合平台，能够有效提高故障的定位效率和准确性。这些安全研究虽然在一定程度上为

6 总结与展望

6.1 本文工作总结

随着工业互联网的发展，核电站仪控系统的安全问题更容易被攻击者利用。核电站仪控系统的通信协议是仪控系统通信的纽带，具有很高的的安全性要求，但目前尚缺乏专门针对其设计的模糊测试工具。本文针对核电站仪控系统采用的通信协议，进行了模糊测试方法的研究以及工具的开发。具体研究内容如下：

第一、分析了通信协议模糊测试研究现状，总结了当前研究中存在的不足，包括对通信协议状态机的推断结果准确度有限、对测试用例变异字节关注不足以及缺乏专门用于核电站仪控系统的通信协议模糊测试工具的问题，并有针对性地提出了基于通信协议模糊测试工具 AFLNet 的改进思路。

第二、针对模糊测试方法在协议状态定义方面的不准确性，提出了基于程序变量的状态识别算法，通过分析并提取协议程序的状态变量，建立状态模型来识别协议程序内部的状态，为后续基于状态选择与引导的模糊测试过程提供支持，提高模糊测试探索的深度。

第三、针对模糊测试方法对变异字节关注不足的问题，提出了基于鲸鱼优化算法的字节变异算法，重点针对字节变异过程进行了优化设计，采用鲸鱼优化算法对各个模型可解释性方法进行优化融合，得到各个字节的变异权重，引导生成更有测试价值的测试用例，提高模糊测试工具的性能。

第四、基于上述两种算法，设计了一项模糊测试工具 SWOFuzz，对初始测试用例构造模块、程序状态识别模块、测试用例生成模块和测试监控模块进行了扩展。对所设计的模糊测试工具进行实验评估，在 4 个通信协议（Modbus/TCP、S7Comm、EtherNet/IP、DNP3）的程序上，与主流的通信协议模糊测试工具 AFLNet 和 AFLNWE 进行对比，在分支覆盖数量上分别实现了 3.86%和 26.37%的平均提升，在独特路径数量上分别实现了 23.12%和 417.28%的平均提升，反映了更好的测试效果，并触发了 27 个崩溃，复现了 2 个已知漏洞，展现了良好的测试性能。

6.2 未来工作展望

本文首次提出了面向核电站仪控系统的通信协议模糊测试技术，设计了一项模糊测试工具并进行了实验评估，具有良好的效果。但此工具还不够完善，存在可以改进的地方，具体如下。

第一、本研究虽然设计了一种状态识别算法，但没有针对基于状态重要性的状态选择算法进行改进，缺乏对状态的理解与分析。本文后续研究方向可以针对识别到的协议状态机进行进一步的分析，实现状态选择算法的改进。

第二、本研究只针对了两种模型可解释性方法进行了优化，没有涉及到其他方法，且没有对不同方法的准确性进行对比。后续可以加入更多的模型可解释性方法，对比得到更优的方法。

第三、本研究的应用场景只能局限于可获得源码的通信协议上，对于私有协议无法实现。后续可根据需要扩大应用场景。

评阅结果

学号：22260276　　姓名：王羽纯

论文题目：面向核电站仪控系统的通信协议模糊测试技术研究

英文题目：Research on Communication Protocol Fuzzing for Instrumentation and Control Systems of Nuclear Power Plant

**** **** ****

评阅意见

* 评阅意见：该论文针对核电站仪控系统通信协议面临的安全问题，首先考虑通信协议中程序状态与模糊测试深度与覆盖度的关联性，研究了基于程序变量的状态识别算法，实现了运行时协议程序的状态识别；进一步考虑测试效率问题，提出了基于鲸鱼优化算法的字节变异方法，实现测试用例中不同字节权重系数的计算。此外，该论文设计并实现了一种面向核电站仪控系统的通信协议模糊测试工具，验证了所提方法的有

* 不足之处及修改意见：修改建议如下：
1、该论文第三章的标题为"模糊测试系统算法优化与改进"。但此前并没有相关的算法设计，此处直接进行优化与改进，有待进一步斟酌，建议体现该章节的核心贡献或创新。

* 总体评价：A（优秀）

* 评阅结果：同意修改后直接答辩

评阅结果

学号：22260276　　姓名：王羽纯

论文题目：面向核电站仪控系统的通信协议模糊测试技术研究

英文题目：Research on Communication Protocol Fuzzing for Instrumentation and Control Systems of Nuclear Power Plant

**** **** ****

评阅意见

* 评阅意见：该论文选题具有较强的现实意义，对于推动核电仪控系统的信息安全技术进步具有重要价值。
论文提出了基于程序变量的状态识别算法和基于鲸鱼优化算法的字节变异方法，实现了面向核电站仪控系统的通信协议模糊测试工具SWOFuzz，设计了科学合理的实验方案并进行了验证。改进思路清晰，算

* 不足之处及修改意见：1.文中个别内容存在小错误，建议修改：如，35页的图3.8最右侧图框中有两个SHAP；参考文献3、10、42在文中未标识引用位置。
2.建议增加研究应用结果进一步分析，补充测试结果对核电仪控系统的信息安全和网络安全的改进或优化建议。

* 总体评价：A（优秀）

* 评阅结果：同意修改后直接答辩

评阅结果

学号：22260276　　姓名：王羽纯

论文题目：面向核电站仪控系统的通信协议模糊测试技术研究

英文题目：Research on Communication Protocol Fuzzing for Instrumentation and Control Systems of Nuclear Power Plant

**** **** ****

评阅意见

* 评阅意见：评阅意见.docx

* 不足之处及修改意见：无

* 总体评价：A（优秀）

* 评阅结果：同意答辩

CNVD 国家信息安全漏洞共享平台
CHINA NATIONAL VULNERABILITY DATABASE

原创漏洞证明

漏洞编号：CNVD-2023-60798

漏洞名称：台达电子企业管理(上海)有限公司 DVP50MC11T存在工控设备漏洞

漏洞类型：通用—网络设备-中危

贡 献 者：王羽纯、车欣、邓瑞龙、孙铭阳、赵成成、程鹏、陈积明

贡献者单位：浙江大学307LAB

证书编号：CNVD-YCGN-202306029203

收录时间：2023年06月01日

中国互联网协会网络与信息安全工作委员会

国家互联网应急中心（CNCERT）

CNVD 国家信息安全漏洞共享平台
CHINA NATIONAL VULNERABILITY DATABASE

原创漏洞证明

漏洞编号：CNVD-2023-61195

漏洞名称：台达电子企业管理(上海)有限公司DVP50MC11T存在工控设备漏洞

漏洞类型：通用—网络设备-中危

贡 献 者：王羽纯、车欣、张镇勇、程鹏、陈积明

贡献者单位：浙江大学、贵州大学

证书编号：CNVD-YCGN-202306088501

收录时间：2023年06月01日

中国互联网协会网络与信息安全工作委员会

国家互联网应急中心（CNCERT）