同行专家业内评价意见书编号：20240854156

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： 张严

学号： 22160018

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

2024年03月18日

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】

一、对本专业基础理论知识和专业技术知识掌握情况

本人专业为电子信息（控制工程），研究方向为网络空间安全、工业控制系统安全。在基础理论方面，我深入学习了计算机网络、软件开发、工业互联网系统安全前沿技术、工业互联网安全系统工程等课程，掌握了信息安全、工业控制系统安全等基础知识。在专业技术方面，我专注于网络空间安全和工业控制系统安全等领域的研究工作，熟悉常见的网络攻防技术，包括但不限于入侵检测与防御、恶意代码分析、安全协议等，具备在网络环境下进行安全防护和应急响应的能力。同时，我还对工业控制系统的安全性进行了深入研究，了解工控系统的特点和安全威胁，掌握了针对工控系统的安全评估与防护技术。

二、工程实践的经历

在工程实践方面，本人参与了浙江大学与山东临工联合研究中心的《高端工程装备智能与安全技术研究》项目中，实践内容主要是针对临工的内网AG V设备开展网络安全态势感知技术研究，设计并实现一套AGV物流系统下的网络安全态势感知系统。

三、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

在临工的项目工程实践期间，本人作为项目主要参与人，负责了《高端工程装备智能与安全技术研究》项目中的控制器入侵检测与网络安全态势感知技术子课题。该课题的研究主要针对内网生产线的不同物联网设备进行态势感知系统开发，目标是:

能准确识别内网的所有设备资产；从流量层面感知网络攻击行为并进行相关的攻击溯源、应急响应；同时能对公网各大漏洞、威胁情报平台进行信息收集，对内网系统进行网络安全态势评估。

该项目工程实践的过程中，遇到的主要技术难点有：针对内网不同控制系统、操作系统的AGV设备漏洞挖掘工作；资产识别、入侵检测等模块的研究工作；网络安全态势感知系统的开发与应用工作。面对该项目中的复杂工程问题，本人在实际工作用运用所学知识进行了研究与解决，具体而言如下所示：

在AGV资产识别部分：网络资产扫描是AGV物流调度安全态势研究的基础，项目采用基于搜索的AGV设备识别技术，设计并实现AGV设备识别框架。实现物联网设备的准确识别，需要精确提取协议标识中的设备信息并构建完备的AGV设备信息库。

AGV漏洞挖掘和入侵检测部分：鉴于AGV物流调度系统部署在一个特定网络下，因此采用基于网络的入侵检测方法。首先开展基于规则的入侵算法研究，由于AGV小车的无线通讯协议为私有协议，因此对部分AGV小车控制器进行人工协议逆向，开展漏洞挖掘工作，以提取攻击流量特征构建基于特征的入侵检测规则库。考虑到基于规则的入侵检测算法只能检测已知网络攻击，无法有效检测Oday攻击，通过采集海量AGV物流调度系统通讯流量，构建正常生产流程特征轮廓，通过机器学习、深度学习等相关算法开展基于异常的入侵检测算法研究。

公网威胁情报及漏洞聚合部分：研究基于爬虫的漏洞信息及威胁情报信息聚合技术，通过爬虫技术实现对CVE、CNVD、ICS-CERT各大公网漏洞库中漏洞信息以及威胁情报信息的爬取，以构建丰富的漏洞态势资源库。同时基于AGV设备识别技术实现资产关联设备漏洞信息以及威胁情报信息的及时聚合，以帮助工程师、安全研究人员获取公网漏洞态势、评估AGV物流调度系统安全态势，开展漏洞修复、主动防御工作。

具体的研究路线：第一步针对AGV物流调度场景，设计和实现一种AGV资产扫描系统，实现对物流调度网络下AGV资产信息的准确识别。接着设计出一种针对AGV物流调度场景的入侵检测

系统，实现基于规则和基于异常的AGV物流调度入侵检测。然后针对AGV物流调度场景，设计和实现一种公网威胁感知策略，实现对公网资产关联设备威胁情报以及漏洞信息的聚合。最后整合上述研究成果，设计并实现一套AGV物流调度场景下的安全态势感知系统，实现AGV物流调度系统的网络安全态势感知。

综上所述，在项目研发中本人综合运用所学知识，开展了内网相关AGV设备的漏洞挖掘工作，同时还有AGV物流网络安全态势感知系统软件中资产识别、入侵检测、攻击溯源以及威胁聚合等模块的后端开发工作。通过学习和实践，本人具备了将理论知识应用于实际问题解决的能力，并且在相关领域取得了一定的研究成果，为进一步深入研究和实践打下了坚实的基础。

（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AGV物流场景下的网络安全态势感知系统	发明专利申请	2023年10月19日	申请号：202311367854 9	1/9	

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】

CNVD（国家信息安全漏洞共享平台）原创漏洞证明：
2022年5月：《信捷　　PLC编程工具软件密码泄露漏洞　　(中危)　　》——
CNVD（国家信息安全漏洞共享平台）原创漏洞证明
2022年5月：《信捷电气　　XD5E-24T-E　　密码泄露漏洞　　(中危)　　》——
CNVD（国家信息安全漏洞共享平台）原创漏洞证明

（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： 87 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： 1.3 年（要求1年及以上） 考核成绩： 89 分（要求80分及以上）
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：**	

22160018

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）：　　年5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：22160018	姓名：张严	性别：男	学院：工程师学院	专业：控制工程	学制：2.5年
毕业时最低应获：24.0学分	已获得：24.5学分			入学年月：2021-09	毕业年月：2024-03
学位证书号：1033532024602124			毕业证书号：103351202402600350		授予学位：电子信息硕士

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
2021-2022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	2021-2022学年秋冬季学期	工程师实践能力训练		4.0	良	专业选修课
2021-2022学年秋季学期	工业互联网系统安全前沿技术		2.0	96	专业学位课	2021-2022学年春季学期	研究生英语基础技能		1.0	免修	公共学位课
2021-2022学年冬季学期	模式识别与人工智能		2.0	92	专业选修课	2021-2022学年春季学期	研究生英语		2.0	免修	公共学位课
2021-2022学年秋冬季学期	中国特色社会主义理论与实践研究		2.0	93	公共学位课	2021-2022学年夏季学期	自然辩证法概论		1.0	93	公共学位课
2021-2022学年冬季学期	工程伦理		2.0	94	公共学位课	2021-2022学年夏季学期	无线网络的控制和优化		1.5	86	专业选修课
2021-2022学年冬季学期	工程中的有限元方法		2.0	95	专业选修课	2021-2022学年夏季学期	工业物联网与大数据实践		2.0	92	专业学位课
2021-2022学年秋冬季学期	研究生论文写作指导		1.0	86	专业学位课						

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：2024-04-02

国 家 知 识 产 权 局

310013

浙江省杭州市西湖区古墩路 701 号紫金广场 C 座 1506 室 杭州求是专利事务所有限公司

刘静(0571-87911726-809)

发文日：

2023 年 10 月 23 日

申请号：202311367854.9　　**发文序号：**2023102301168470

专 利 申 请 受 理 通 知 书

根据专利法第 28 条及其实施细则第 38 条、第 39 条的规定，申请人提出的专利申请已由国家知识产权局受理。现将确定的申请号、申请日等信息通知如下：

申请号：2023113678549

申请日：2023 年 10 月 19 日

申请人：浙江大学,山东临工工程机械有限公司

发明人：张严,赵成成,车欣,阮煜程,杨秦敏,程鹏,陈积明,陈博,魏一丁

发明创造名称：一种 AGV 物流场景下的网络安全态势感知系统

经核实，国家知识产权局确认收到文件如下：

权利要求书 1 份 3 页,权利要求项数 ： 10 项

说明书 1 份 7 页

说明书附图 1 份 2 页

说明书摘要 1 份 1 页

专利代理委托书 1 份 3 页

发明专利请求书 1 份 5 页

实质审查请求书 文件份数：1 份

申请方案卷号：刘-231-200-政

提示：

1.申请人收到专利申请受理通知书之后，认为其记载的内容与申请人所提交的相应内容不一致时，可以向国家知识产权局请求更正。

2.申请人收到专利申请受理通知书之后，再向国家知识产权局办理各种手续时，均应当准确、清晰地写明申请号。

国家知识产权局 专利申查业务章 1101081359734

审 查 员：杨艳

联系电话：010-62356655

审查部门：初审及流程管理部

纸件申请，回函请寄：100088 北京市海淀区蓟门桥西土城路 6 号 国家知识产权局专利局受理处收

电子申请，应当通过专利业务办理系统以电子文件形式提交相关文件。除另有规定外，以纸件等其他形式提交的文件视为未提交。

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-2022-45445

漏洞名称：信捷电气XD5E-24T-E PLC存在密码泄露漏洞

漏洞类型：通用—网络设备-中危

贡 献 者：张严，车欣，赵成成，孙铭阳，邓瑞龙，程鹏，陈积明

贡献者单位：浙江大学307LAB

证书编号：CNVD-YCGN-202205054559

收录时间：2022年05月19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-2022-45447

漏洞名称：信捷PLC编程工具软件存在密码泄露漏洞

漏洞类型：通用—网络设备-中危

贡 献 者：张严、车欣、赵成成、孙铭阳、邓瑞龙、程鹏、陈积明

贡献者单位：浙江大学307LAB

证书编号：CNVD-YCGN-202205054357

收录时间：2022年05月19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）