**兰州理工大学**

**2025届毕业设计（论文）**

**开题报告-终稿**

|  |  |
| --- | --- |
| 题 目： | 电力行业工控网络威胁评估系统 |
| 专业班级： | 网络空间安全一班 |
| 姓 名： | 张欣 |
| 学 号： | 210162601055 |
| 指导教师： | 谢鹏寿 |

**计算机与通信学院**

说 明

**一、开题报告主要内容**

1.设计的背景和意义

2.国内外在该方向的发展趋势及分析

3.设计的主要内容及技术指标

4.设计方案的制定

5.设计进度安排，预期达到的目标

6.设计过程中可能遇到的困难和问题，解决的措施

7.主要参考文献

**二、开题报告要求**

1.报告内容用宋体小4号字，行距1.25倍，段前0行,段后0行编辑，采用A4号纸双面打印。要求内容明确，语句通顺。

2.开题报告字数要求在3000字左右。

3.阅读的主要参考文献应在10篇以上,其中,外文资料不少于2篇。教材、产品说明书、国家标准、未公开发表的研究报告不宜作为参考文献。

4.开题报告由指导教师填写评语用黑色笔手写或小四号宋体字编辑，签名必须手写。

5.开题报告应在毕业设计工作开始四周内完成。

**兰州理工大学本科毕业设计开题报告**

|  |
| --- |
| **一、设计的背景和意义（简述题目的技术背景和设计依据，说明选题目的、意义）**  随着电力行业数字化、智能化转型加速，工控网络成为电力系统运行的核心支撑。然而，其安全状况不容乐观，开发威胁评估系统迫在眉睫。基于此，电力企业迫切需要一套高效的威胁评估系统。它能实时监测工控网络状态，及时发现异常流量、安全漏洞等威胁，准确评估风险等级，并提供应对建议。通过该系统，可主动防御，提升工控网络安全防护能力，保障电力生产与供应的安全有序。  电力行业工控网络威胁评估系统成果显著。它极大增强了电力系统安全防护能力，实时监测异常流量与恶意入侵，精准评估风险，及时阻断攻击、修复漏洞，保障电力稳定供应。其开发积累的经验与数据，为完善行业安全标准提供支撑，推动安全管理、设备运维等规范化。此外，该系统实现安全管理智能化，自动生成报告，大幅提升企业安全管理效率，降低成本。​  此外，学生通过该题目的设计过程，掌握网络空间安全领域的基本原理、基本知识和基本方法，了解网络空间安全标准和法律法规，能够考虑系统中涉及的技术经济、工程伦理及行业规范，具备开展网络空间安全相关领域科学研究和应用开发的基本能力，提高团队合作、沟通表达及项目管理能力。 |
| **二、国内外在该方向的发展趋势及分析**  在电力行业工控网络威胁评估系统的开发设计领域，国内外已取得诸多成果，涵盖技术、应用与理论方法层面。  技术上，国外在检测技术方面起步较早，如美国研发出基于人工智能的电力工控网络入侵检测技术，能精准识别复杂多变的攻击模式，通过对海量正常与异常流量数据的深度学习，构建行为模型，快速甄别入侵行为，检测准确率较高。国内在电力协议解析技术上成果斐然，像国网山东电科院提出全新的全流量电力协议解析算法，可对各类电力协议进行高效解析，全面洞察网络行为，助力发现网络中的潜在威胁，为网络安全监测筑牢根基 。  应用层面，国外部分电力企业已将威胁评估系统大规模应用于实际电网，如欧洲一些国家的电力公司借助威胁评估系统，实时监测电网运行状态，及时发现并处置网络攻击，有效保障了电网的安全稳定运行，大幅减少停电事故的发生频率。国内在智能变电站领域应用成果显著，例如国网山东电科院的 “守望者” 网络安全监测融合装置，已在多座变电站试点部署，通过对变电站网络通信数据的采集与分析，成功定位并解决多起异常通信问题，避免重大网络安全事故。  理论方法上，国外提出风险量化评估理论，将电力工控网络中的各类风险因素进行量化分析，综合考虑资产价值、威胁发生概率、脆弱性严重程度等，为制定针对性防护策略提供依据。国内则建立了基于漏洞价值、资产价值和利用影响业务范围的工控漏洞定级方法，构建工控安全状态脆弱性评价模型，能够准确评估电力系统安全状态，为威胁评估提供科学有效的方法。  然而，当前研究仍存在不足。技术上，面对新型攻击手段，如量子计算攻击、针对电力物联网设备的攻击，现有检测技术和协议解析技术难以快速应对，缺乏前瞻性和通用性。应用方面，不同地区、不同规模电力企业在威胁评估系统应用程度上差异较大，部分企业因资金、技术等原因，系统应用范围有限，且系统间数据共享与协同联动不足。理论方法层面，各类评估模型和方法在实际复杂多变的电力工控网络环境中，准确性和适应性有待进一步提高，尚未形成统一、完善的理论体系 。 |
| **三、设计的主要内容及技术指标**   1. 制定“电力行业工控网络威胁评估系统”设计方案，开发“电力行业工控网络威胁评估系统”的原型系统，并撰写毕业设计说明书及相关简介文档。。 2. 该系统由安全风险评估、安全状态评估、危害损失评估、威胁综合评估等模块组成； 3. 该系统具有深入扫描工控系统和网络中可能存在的脆弱性，做到提前预警，为工控安全防护提供数据支撑等要求； 4. 采用机器学习、决策树算法等算法来解决电力行业工控网络威胁评估系统中的数据处理、威胁识别与风险评估问题； 5. 采用Python、MySQL、Wireshark等开发该系统的软件； 6. 设计中体现项目中所涉及的非技术因素； 7. 该系统采用模拟数据进行测试。 |
| **四、设计方案的制定**  本系统采用分层架构设计，涵盖数据采集层、数据处理层、威胁评估层和用户交互层。电力行业工控网络威胁评估系统的实现基于 Python、MySQL 和 Wireshark 构建。其中，Python 作为主要的编程语言，用于数据处理、算法实现和系统集成；MySQL 用于存储网络数据和评估结果；Wireshark 用于捕获网络数据包。  实现思路  数据采集：借助 Wireshark 捕获网络数据包，接着利用 Python 的pyshark库对这些数据包进行解析。  数据存储：把解析后的数据包信息存入 MySQL 数据库。  威胁评估：基于预定义的规则或者机器学习算法，对存储在数据库中的数据开展威胁评估。  结果展示：输出威胁评估的结果。   1. 安全风险评估模块   资产 - 威胁 - 脆弱性三维建模  工业协议指纹识别（Modbus/TCP、IEC 61850）与图数据库构建资产关系图谱，动态识别设备漏洞。  基于 ATT&CK for ICS 框架建立电力专属威胁库，结合马尔可夫链推演攻击路径对电网稳定性的影响。  采用 FAIR 模型量化风险（漏洞利用成本 × 停电损失），输出年度预期经济损失。   1. 安全状态评估模块   多源实时监测与智能预警  边缘计算节点集成协议探针，采集工控流量、设备日志及电网运行数据，通过 InfluxDB 存储高频时序数据。  LSTM+Transformer 模型构建设备行为基线，联邦学习提升新型攻击识别率，数字孪生与 AR 实现三维态势可视化。   1. 危害损失评估模块   业务影响与经济量化  Petri 网建模电力业务流程，结合 ETAP 仿真分析攻击对电网潮流的物理影响，量化停电范围与用户数。  实时损失模型集成电力市场数据（电价），区块链存证攻击事件，支持经济损失精准计算与责任追溯。   1. 威胁综合评估模块   多维度决策融合  证据推理（D-S 理论）融合风险、状态、损失评估结果，知识图谱推理推荐防护策略（如漏洞关联业务隔离）。  强化学习优化评估模型权重，博弈论模拟攻防策略生成最优处置方案（如 5 分钟内切断感染设备连接）。  共性技术支撑  电力协议深度解析：专用引擎检测协议异常（如非法遥控命令），模糊测试发现未知漏洞。  轻量化边缘计算：容器化部署模型压缩技术（MobileNetV3），满足实时性要求。  安全合规：遵循 NERC CIP-007、IEC 62443 标准，集成漏洞扫描工具生成合规审计报告。 |
| **五、设计进度安排，预期达到的目标**   |  |  |  | | --- | --- | --- | | **设计内容** | **起止周** | **预期达到的目标** | | 搜集参考资料，分析题目要求，撰写开题报告文档初稿，将外文翻译初稿排版在毕业设计说明书中 | 第1周 | 完成外文文献翻译和毕业设计说明书。 | | 教师指导学生进行系统需求分析，并将其撰写在毕业设计说明书文档之中，完成开题报告文档终稿 | 第2周 | 完成开题报告文档终稿。 | | 学生在毕业设计说明书文档中撰写系统总体设计和详细设计方案 | 第3 周~第4周 | 完成系统总体设计与详细设计方案文档。 | | 系统设计方案的实现，包含软件编程，并将研究成果、部分代码撰写在毕业设计说明书文档之中 | 第5周~第8 周 | 实现系统的主要功能，代码与文档的同步更新。 | | 软件测试、调试，并将调试的经验和测试报告撰写在毕业设计说明书文档的总结部分 | 第9周 | 完成测试报告。 | | 修改完善毕业设计说明书，撰写毕业设计说明书简介 | 第10周~第12 周 | 提交毕业设计说明书终稿。 | | 准备答辩资料（制作答辩PPT、打印毕业设计说明书及其简介文档等） | 第13周 | 答辩材料准备齐全，准备答辩。 | |
| **六、设计过程中可能遇到的困难和问题，解决的措施**  1.研究条件层面​  数据获取受限​  电力工控网络数据涉及电网安全，访问权限严格，难以获取足够数据用于分析建模。  解决措施：与电力企业建立合作机制，签订保密协议，确保数据安全。​  2.技术层面​  检测技术滞后​  新型网络攻击手段不断涌现，现有检测技术难以快速准确识别，如针对电力系统特定协议的未知攻击。​  解决措施：引入人工智能、大数据分析等技术，构建智能检测模型，通过对海量数据的学习，识别异常行为；持续关注安全技术发展动态，及时更新检测算法和规则库。  3.政策层面​  法规标准不健全​  电力行业工控网络安全法规和威胁评估标准尚不完善，系统设计缺乏明确规范指引。​  解决措施：积极参与行业法规和标准的制定修订工作；参考国际通行标准和最佳实践，结合国内电力行业特点开展系统设计。​  4.经济层面​  运维成本高​  系统部署后，设备更新、软件升级、人员培训等运维成本持续产生，给企业带来经济压力。​  解决措施：采用模块化设计，降低系统维护难度；建立远程运维机制，减少现场运维工作量；通过自动化工具实现设备和软件的批量更新，降低运维成本。 |
| **七、主要参考文献**   1. Jadidi, Z (Jadidi, Zahra); Lu, Y (Lu, Yi).A Threat Hunting Framework for Industrial Control Systems[J].IEEE ACCESS,2021,9. 2. Shan, Y (Shan, Yao); Yao, Y (Yao, Yu); Zhao, T (Zhao, Tong); et all.NeuPot: A Neural Network-Based Honeypot for Detecting Cyber Threats in Industrial Control Systems[J].IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS,2023,19(10). 3. 张秋余，张聚礼，柯铭，等. 软件工程 [M]. 西安：西安电子科技大学出版社，2014. 4. 张聚礼，谢鹏寿，马威，等. 软件项目管理 [M]. 西安：西安电子科技大学出版社，2014. 5. 王泽鹏,马超,张壮壮,等.动态决策驱动的工控网络数据要素威胁检测方法[J].计算机研究与发展,2024,61(10):2404-2416. 6. 陈瑞滢,陈泽茂,王浩.基于攻击图的工控网络威胁建模研究[J].信息网络安全,2018,(10):70-77. 7. 安树勇.基于大数据分析的电力工控网络威胁检测与预警系统设计[J].网络安全和信息化,2023,(10):125-127. 8. 白强,胡博元,宣中忠,等.工控网络安全风险分析与应对策略[J].现代工业经济和信息化,2024,14(2):80-82. 9. 王璐瑶,贾令涛,陈潇,等.基于工控网络的管理系统安全设计方法[J].信息与电脑,2025,37(1):188-190. 10. 张晋宾.工控网络安全新兴理念及发展态势分析[J].自动化博览,2024,41(1):16-21. 11. 胡朝辉,陈善锋,杨逸岳.电力工控网络0day漏洞风险自动识别技术[J].自动化技术与应用,2025,44(1):97-100. 12. 邓志森.电网工控网络流量分析[J].信息网络安全,2020,(S1):127-130. 13. 赵起超,杨晓龙,赵文宇,等.基于语义级协议解析的工控网络安全监测方法[J].信息安全与通信保密,2024,(9):19-30. |

**兰州理工大学本科毕业设计开题报告**

|  |
| --- |
| **指导教师评语：** |
| 指导教师签字： |
| 年 月 日 |