面向工业安全的跨领域网络安全课程建设探索实践*

孙彦斌　　李默涵**　　田志宏

广州大学网络空间安全学院，广州 510000
广东省工业控制系统攻防对抗重点实验室，广州 510000

摘　要　工业领域网络攻击从网络空间渗透至物理空间，导致环境污染、人员伤亡等严重问题，传统网络空间安全专业课程仍局限在信息领域，难以适应具有跨域特点安全需求，因此亟待探索可满足工业安全需求的网络安全课程建设方法，本文分析工业安全人才及教学需求，结合方班网安人才培养模式，以需求为导向提出“安全理论”、“安全技能”、“安全意识”、“安全视野”四位一体的课程建设方案，为跨领域相关课程建设提供参考。

关键字　工业安全，跨领域，课程建设

Exploration and Practice of Cross-Domain Cybersecurity Curriculum Development for Industrial Security

Yanbin Sun　Mohan Li　Zhihong Tian

Cyberspace Institute of Advanced Technology of Guangzhou University
Guangzhou 510000, China
limohan@gzhu.edu.cn

Abstract—Cyberattacks in the industrial domain increasingly extend from cyberspace to physical space, resulting in severe consequences such as environmental pollution and loss of life. Traditional cybersecurity courses are predominantly confined to the information domain, making them inadequate to address the cross-domain security demands of industrial systems. Thus, it is imperative to explore methods for developing cybersecurity curricula tailored to the needs of industrial security. This study analyzes the requirements for industrial security professionals and educational needs, proposing a demand-driven, four-dimensional curriculum framework integrating "security theory," "security skills," "security awareness," and "security perspective." The proposed framework aims to provide a reference for the development of cross-domain courses in related fields.

Keywords—Industrial Security, Cross-Domain, Curriculum Development

1　引　言

网络空间已发展成为全球性的信息环境域，直接关系到人类生产、生活、社会活动乃至意识形态等各个方面，与现实世界交织、映射和关联，被作为继陆海空天后的第五大主权领域空间。俄乌战争表明，网络攻防对抗已经成为国家间斗争的一部分，也是西方国家遏制我国发展和转移其内部矛盾的重要手段。习近平总书记指出“没有网络安全就没有国家安全”，网络空间安全始终是国家重点关注的重要领域。网络空间安全是国家发展规划和战略实施重要一环。

2021 年十三届全国人大四次会议通过的《中华人民共和国国民经济和社会发展第十四个五年规划和2035 年远景目标纲要》[1]（简称十四五规划和远景目标），“安全”已成为最重要的关键词之一，网络空间安全作为“安全领域”不可或缺的重要组成部分备受关注。“维护水利、电力、供水、油气、交通、通信、网络、金融等重要基础设施安全”是我国《十四五规划和远景目标》提出的重要任务。其中，水利、电力、供水、油气、交通等工业领域由于与实际生产、生活相关，跨信息域和物理域，一旦遭受网络攻击将直接导致环境污染、人员伤亡等重大安全事件，影响社会稳定和国家安全，因此，工业领域安全问题成为国家重点关注对象。

随着 “中国制造 2025”战略的持续推进，工业互联网得到快速发展。工业化和信息化两化深度融合，工业企业为提高生产效率和灵活性，将工业控制系统（简称工控系统）由传统的封闭、隔离转为开放、互联。在生产效率提高和竞争力增强的同时，也增加了工控系统的攻击面。工控系统作为与工业生产

*基金资助：广州市高等教育教学质量与教学改革工程项目(2023QTJG058, 2024KCSZ010)，广州市教学成果培育项目(2023128728),广东省重点实验室项目(2024B1212020010

**通讯作者：李默涵 limohan@gzhu.edu.cn。

直接相关的关键信息基础设施成为 APT(Advanced Persistent Threat)攻击的主要目标，其面临攻击威胁呈现攻击持续性、针对性、潜伏性、隐蔽性与未知性等特点，直接对实际生产过程产生不利影响，影响范围覆盖国家、军工、民用等多种工业场景。

在此背景下工业网络安全持续受到国家重视。国家出台了一系列工业网络安全相关的法律法规和制度标准，2019 年发布的国家《网络安全等级保护 2.0》[2]中，专门增加了对工业控制系统安全的扩展要求。2021 年实施的《关键信息基础设施安全保护条例》[3]也重点强调了对能源、交通、水利、国防科技工业等重要工业场景的保护。可见，保障工业网络安全已成为国家重大安全需求。

现有的网络安全人才培养和教学难以满足我国工业网络安全需求。在网安人才培养和教学方面，我国本身存在诸多不足，尤其在应对工业领域网络安全人才培养和教学特殊需求时面临更多问题，主要体现在：

（1）网络安全人才需求旺盛而供给严重不足，特定领域网安人才更是奇缺。据教育部 2022 年《网络安全人才实战能力白皮书》[4]数据显示，国内仅有 34 个高校设立网络空间安全一级学科。到 2027 年，我国网络安全人员缺口将达 327 万，而高校人才培养规模为 3 万/年。从人才需求方角度，当前网络安全业务份额越来越重，然而招到匹配和适合的网络安全技术人才却很难，各行业均面临着网络安全人才缺失的困境。工业领域由于涉及更宽泛、更专业的知识，其对人员素质和技能的要求更高，因此也面临更多人才缺口。

（2）现有网络安全教学方法面向通用网安人才，不符合工业网络安全特定需求。我国网络空间安全研究生专业相关课程设置、教学方法多面向信息系统安全问题，培养通用型网安人才，未能考虑当前工业互联网、5G 等新技术、新应用发展带来的新需求。工业网络安全面临跨信息域和物理域特点，行业相关的安全防护需要跨专业的知识基础。以专业划分为基础的本科人才培养体系和教学方法难以培养出具有跨学科基础的网络安全人才。由于本科教育具有以基本原理、基础理论为主的鲜明特点，很难在原有专业体系中加入其他专业的基础课程。研究生教育又以研究型、工程型人才为目标，缺乏相关专业基础技能的培养，本科教育与研究生教育之间脱节使得我国在面向特定领域高层次网安人才培养受到极大限制。因此，亟需在网络空间安全相关课程建设中应融入国家工业安全需求，以满足不同领域高层次网安人才需求。

综上，网络安全相关课程教学应以国家需求为导向，在保证基础理论、技能满足研究需要同时兼顾与特定领域结合，树立学生服务国家需求意识，形成前沿领域安全视野，培养国家、地区真正需要的高层次网安人才。针对以上问题和需求，本课题以工业网络安全为应用场景，依托漏洞挖掘相关课程，以需求为导向，探索符合国家重大安全需求的高质量网络安全课程建设，形成“安全理论”、“安全技能”、“安全意识”、“安全视野”四位一体的课程建设方案，培养安全理论和实践结合、安全意识和视野并存的符合国家安全需求的网安人才。

2 工业网络安全发展现状及需求分析

2.1 工业网络安全发展趋势

BlackEnergy 病毒、Triton 病毒、Havex 病毒等相关攻击事件表明，针对工业网络的攻击可直接影响物理世界，从网络空间引发物理空间危害，如：BlackEnergy 使得乌克兰至少三个电力区域被攻击，导致数小时的停电事故;Triton 恶意软件具有国家背景，攻击者可接管工厂安全仪表系统(SIS)，可能导致爆炸或释放有毒气体，造成工作人员生命损失。近年来，针对工控系统的网络攻击逐年增加，据卡巴斯基的最新数据，2021 上半年大约三分之一的工业控制系统遭遇针对性的恶意活动。美国、欧盟分别自 1996、2004 年开始出一系列关键信息基础设施保护相关的政策文件和法律法规。

我国从 2015 年开始，对工业互联网的重视程度和资源投入逐渐增加。2015 年 5 月，国务院发布《中国制造 2025》[5]，提出建设制造强国的“三步走”计划，被认为是未来制造业转型发展的纲领性文件，也正式拉开了我国工业互联网发展的序幕。2017 年 11 月，国务院印发《深化“互联网+先进制造业”发展工业互联网的指导意见》[6]，明确了我国工业与互联网融合的长期发展思路，已经成为中国工业互联网建设的行动纲领。工业互联网目前是国家目前重点关注的发展方向，是国家新型基础设施建设的重要方向之一。相关工业网络安全政策、法规随着工业互联网发展逐步开始实施执行。

2.2 网络安全人才培养和教学现状

网络安全人才缺乏是全球性问题，在工业网络安全领域因增加新的需求，面临问题更加严峻。

美国政府采用自上而下的“专业精英”网络空间治理模式，采取以“专业性”“任职经验”为标准组建了由网络安全领域“专业精英”构成的网络空间治理团队。同时，还组建了世界上最早网络军队，2020 年已具备作战能力，培养大批实战型网络安全人才。此外，还通过社会公开、政府军队内部等发起多种网络安全比赛，以培养、锻炼和挖掘网安人才，组建覆盖攻、防两端的实践性人才队伍。针对人才缺乏问题，建立了人才流动制度，要求网络安全从业人员在公共

领域和私营领域之间的顺畅流动,充分发挥人员技能、经验和才华,实现人才资源利用最大化。美国高度重视工业控制系统信息安全培训认证工作，但教学尚未涉及重点领域。美国对网络安全高等教育的重视程度、学科研究和教学水平世界领先。美国政府通过专门机构把握关键环节，以设立专项、经费资助等方式，把网络安全教育研究放在与网络安全教育同等重要地位，开发了一系列高水平网络安全知识体系和课程认证标准，如NSA/DHS CAE认定机制、CSEC 2017知识体系、ABET课程认证标准。这些知识体系和课程认证标准具备一下特点：（1）制定了相对固定的知识体系；（2）注重时效性，定期对知识体系进行更新；（3）需求导向,全部或直接参考美国NIST发布的人才分类标准“网络安全人力框架”，确保培养出可满足社会实际需求的网络安全人才[7]。

欧洲注重强化网络安全教育和技能，认为网络安全需建立在强大的教育基础之，有效网络安全高度依赖相关人员技能。2019年，建立欧洲网络安全能力网络和中心（European Cybersecurity Competence Network and Centre），启动了四个试点项目，以建立和开展欧洲网络安全能力网络试点，制定共同的欧洲网络安全研究与创新路线图。

我国网络安全人才缺乏且培养机制与需求不符。网络安全的对抗实质是高层次和实践创新型人才的竞争。当前我国网络安全的人才数量远不能满足行业的需求。据BOSS直聘发布《2021网络安全人才趋势报告》[8]显示，2021年一季度，全国网安领域人才需求同比增幅超过50%，其中，核心技术研发人才的招聘需求占比达到65%。网络安全人才培养不仅用于保证政企事业单位的安全防护需求培养实践性人才，还要从国家层面和国家网安发展角度培养网络安全战略型、精英型人才。2022年通过的《国家“十四五”期间人才发展规划》强调要大力培养使用战略科学家，打造大批一流科技领军人才和创新团队，造就规模宏大的青中年队伍，培养大批卓越工程师。同时，教育部发建设布“101”计划,高等教育教学人才培养改革要从传统“知识为主”转向“能力为先”[9]。可见，我国顶层规划中已经开始将战略型、实战型人才作为下一步培养和挖掘的重点，需要相应地培养体制和方法上的调整以满足国家和行业需求，尤其工业关键信息基础设施安全的重要性及特殊性，更需要面向需求细化人才培养机制。

2．3　工业网络安全教育人才培养需求

工业关键信息基础设施面临跨信息域和物理域特点，行业相关的关键信息基础设施安全防护需要跨专业的知识基础。以专业划分为基础本科人才培养体系难以培养出具有跨学科基础的安全人才，研究生教育又以研究型、工程型人才为目标,缺乏相关专业基础。因此，在当前高等教育人才培养体系基础上，如何通过课程改革以培养出具备跨领域知识的网络安全人才是值得探索的问题，重点关注以下两方面挑战：

（1） 跨领域网络安全教学依赖跨专业的知识体系

目前尚无工业网络安全相关专业和教学体系，高校往往面向计算机、网络安全、自动化等单一专业和学科，而工业网络安全涉及信息技术、安全技术、自动化技术等多个领域的理论和技术。要做好工业网络安全人才教育和研究，要求学生必须具备跨领域、跨专业的知识，这种对跨专业知识体系的依赖是亟需解决的问题

（2） 网安人才需求和教育目标导向不匹配

高校教育往往具备较强的理论功底，缺乏实践经验，而发现和解决工业生产中的实际安全威胁是工控安全研究最主要的目的。以应用目标为导向，工业网络安全人才培养一方面要求学生应具备工控安全相关的基础理论知识，另一方面应了解工业生产实际业务流程，具备动手操作实践能力，能够真正运行所具备的技能解决工业生产中的网络安全问题。

3　工业网络安全课程改革目标

3．1　课程改革目标

随着小班课、微专业等多种灵活课程形式出现，结合现有本科课程体系、教学安排及教学目标的逐年调整，以及本硕一体人才培养模式，在本科及研究生阶段成体系地完成跨领域、跨学科的知识积累和提升。因此，本文重点对网络安全课程改革展开研究，将方班“研讨厅”、“演武堂”等特色人才培养思路和做法融入课堂，希望通过课程改革，将特定领域安全问题、安全技能、安全理念引入研究生课堂和实践，拓展学生对网络安全的认知，加深学生对网络安全的理解，使学生建立起网络安全与行业特性结合的研究理念，以支撑学术在未来工作中应对不同行业网络安全问题具备良好的研究和实践能力。

3．2　课程改革内容

为确保课程改革落地可行，本文以网安专业典型课程《漏洞挖掘》为例，探索符合跨领域网络安全人才培养的课程改革思路、方法，为其他课程形成行之有效的参考。主要从以下四方面展开课程改革研究。

（1） 安全理论：探索以漏洞为中心的跨专业课程基础理论

工业领域安全问题涉及自动化、计算机、网络空间安全等多个专业相关知识，来自不同专业的研究生

可能具备不同的基础知识，知识结构各不相同，知识面也参差不齐。由于课程内容、时间有限，很难通过一门课程或几门课程将所有基础理论知识补充完善。因此，需要围绕本课程核心漏洞，以漏洞为中心梳理并补充不同专业领域与漏洞相关的理论知识。

（2） 安全技能：探索以需求为导向的创新实践能力培养

工业控制系统涵盖了信息系统和控制系统，传统面向信息系统的安全技能仅能部分满足工业安全需求，解决信息系统的安全问题。然而，在国家间攻防对抗中，针对工控系统的网络攻击往往以控制或损毁工业生产为主要目标，呈现跨信息域和功能域的特点，现有漏洞分析技术缺乏对工业控制系统的漏洞挖掘和分析能力。同时，现有的课程教学也缺乏针对性，对学生能力培养缺乏有效参考和依据。课程建设应以国家、企事业实际安全需求为导向、以实战为目标，培养学生创新实践能力，做到真正服务的高质量人才。

（3） 安全意识：探索基于工业安全事件案例分析的安全意识构建

漏洞是导致各类安全问题的根源之一，单纯围绕漏洞展开安全意识培养过程枯燥，不易为学生接受，也缺乏信服力。在工业场景下同时存在类似问题，同时，工业场景下漏洞挖掘和利用方式跟传统信息系统存在差异，通过与具体工业安全事件结合，学生真切意识到漏洞导致的一系问题，并发现工业场景下漏洞利用特有方式，并通过事件复现加强学生安全意识。

（4） 安全视野：探索前沿领域网络安全技术形成动态安全发展视野

安全是一种伴生技术，随着新技术的出现安全问题也会不断出现，继而引发一系列的问题。本课题课程改革应使学生了解安全发展的客观规律，了解前沿领域和技术手段，对新的安全问题具有一定预判能力或者对不同领域的安全问题具备迁移学习的处理能力。

4 工业网络安全课程改革方案及实践

4．1 课程改革方案

（1）以漏洞为中心的跨专业课程基础理论构建

基于已有的网络安全理论和实践基础，结合水利、化工、智能制造等自动化专业的基础理论和实践，将网络安全拓展到工业控制领域，探索工业机器人、智能制造等专业在工控安全涉及的理论、技术以及面临的实际问题。完善在工业安全方面的能力培养，解决教师在教学中与实际应用脱离的问题。具体地采用以轮换学习模型主先，结合案例研究模型展开设计：

首先，明确工业控制系统典型模型和框架，界定工业安全相关资产以及资产可能面临的脆弱性风险。围绕漏洞挖掘和分析这一核心目标，梳理与漏洞相关资产、功能和运行机理等，将漏洞相关内容作为课程基础理论。面向流程工业和离散工业等典型工业过程，梳理和学习工业控制所涉及的基础理论和技术方法，如工控协议、工业控制设备编程、PID 控制过程等，打造坚实的专业基础。通过漏洞挖掘领域知识和工控领域知识的轮流学习，使学生逐步形成综合性视野。

然后，以典型工控安全事件为案例，重点讲授工控安全事件流程，明确其中由漏洞引发的安全问题，分析工控漏洞成因。通过安全事件案例，融合跨领域知识。同时结合实践教学，使学生进一步融汇贯通跨领域知识。

（2）以领域需求为导向的实践创新能力培养

从教师和学生两方面展开能力培养。针对教师教学能力，通过参加行业、企业专家及高级工程师授课，企业实地考察调研等，学习启发式、讨论式、参与式的教学方法，熟悉工业生产中的实际需求和技术应用，避免理论灌输式的教学，帮助年青教师在工控安全领域形成理论、技术、实践结合的教学理念。同时，带着问题深入企业，参与企业专业技能培训、熟悉企业真实工业场景和流程、学习企业实践教学的方法，结合高校教学的实际需求、条件现状，摸索工控安全理论和实践相结合的知识体系、教学方法等。依托国家及企事业需求，明确实战化的攻防对抗技能，继而落地到漏洞检测与分析相关能力的培养。

针对学生创新能力培养，引入方班网络安全人才培养创新模式[10]，将精简版“研讨厅”、“演武堂”引入课堂，结合工业领域特定需求培养学生创新实践能力。一方面培养学生创新思辨能力，使得学生能力打牢理论基础，紧跟学术前沿；另一方面，培养学生动手实践能力，通过构建工业网络靶场，复现多种典型工业控制场景，为工业领域网络攻防实践和技术研究提供基础的安全演练和技术验证平台。

（3）基于工业安全事件案例分析的安全意识构建

工业安全案例分析结合案例教学和实践教学方法。案例教学前期可收集典型工控安全事件，以事件作为案例分析结合 ATT&CK 攻击矩阵，梳理攻击链路，形成模块化攻击步骤。针对单个攻击步骤模块，分析攻击步骤由漏洞触发和利用的原理。基于对多个漏洞梳理，复盘整个攻击过程。从而实现从整体到细节，由细节再回到整体的漏洞分析。

为进一步提升学生安全意识，增加学生动手实践能力，引入方班“演武堂”模式，基于案例分析利用网络靶场对工业安全事件场景进行复现，继而进行漏

洞复现和攻击过程还原，通过分享复现过程和漏洞利用原理。从而深入理解工业场景下漏洞产生机理，利用漏洞实施攻击的原理。

（4）前沿领域技术探索的动态安全发展视野

教学内容中加入网络安全发展的客观规律，明确网络安全伴生特性以及安全问题的客观存在性。同时，教学过程中加入前沿工业安全问题及技术方法，通过讨论式教学、引导式教学方式，引导学生主动思考，能够对前沿问题具有自己认识或通过对已知问题的学习，进行知识迁移，解决其他问题。同时，也可邀请国内外知名专家报告讲座，将前沿漏洞检测和分析技术引入课堂。

4．2　课程改革实践

（1）立足调研，形成整体需求认识

通过查询专业书籍、经典论文、技术报告等形式进行书面调研，对工控安全的基础知识体系形成整体的认识；同时，通过专家咨询、讲座等形式请教行业和学术领域专家，对行业和学术最新动态具有一定认识。

（2）成立课程组，制定学生课程培养规划

按照网络安全不同方向成立课程组，由各课程组长牵头，成立跨组的工控安全师资培养小组，结合网络空间安全、工业机器人、智能制造等专业基础，规划工控安全本科和研究生教学中所需的专业基础理论、技能方法以及可能适合的教学方法，为后续调研制定好目标，做好准备，做到“有的放矢”。

（3）深入工业企事业单位，加强实践能力培养

带着问题深入工业企业，参与企业专业技能培训、熟悉企业真实工业场景和流程、学习企业实践教学的方法，结合高校教学的实际需求、条件现状，依托工控网络靶场摸索工控安全理论和实践相结合的知识体系、教学方法等。

（4）小班试验，展开教学改革成果验证

基于“方班”教学平台，成立小规模的工控安全教学小组，通过迭代的方法，将“调研-教学-反馈-思考/咨询”的过程不断循环往复，验证调研和培训成果，总结和积累经验。

（5）深度思考，树立新型教学理念

基于培训和试验结果，深度思考工控安全教师需要具备的条件，形成包括知识和技能体系、教学目标、教学方法等在内的一整套新型教学理念，为打造工控安全领域的“双师”型教师队伍提供支撑。

5　课程改革效果

围绕漏洞，课程从漏洞概念、漏洞实例（包括程序内存结构、栈溢出、堆溢出等）、漏洞挖掘等漏洞机理相关内容纳入课程。同时，围绕工业控制系统及工业控制系统安全内容，加入工控系统基础、工控系统安全分析（包括工控安全现状、工控安全威胁、工控安全事件分析、工控漏洞挖掘等）、工控安全验证等内容。

同时，以方班人才培养模式为参考，探索本硕一体工控安全人才培养，自 2021-2022 学年起连续 3 年

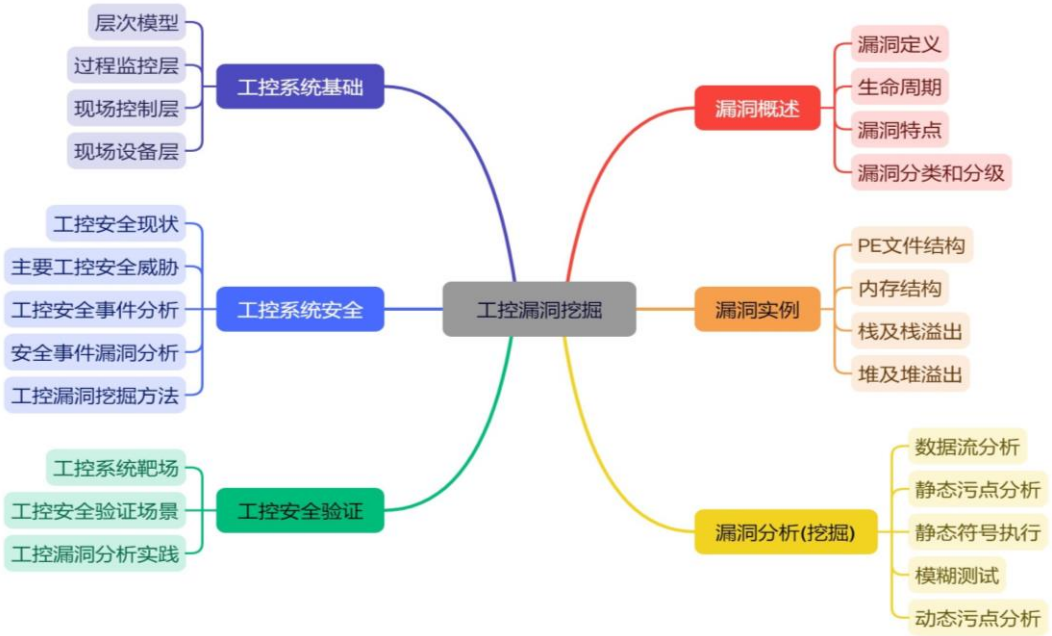

图 1　课程建设框

开设小班课，展开验证式教学。课程中引入对上位机攻击、工控协议攻击、恶意控制逻辑注入攻击、虚假数据注入攻击等热点攻击手段的介绍，并加入“伊朗核电站事件-震网病毒”、“乌克兰电网事件-黑色能量病毒”等典型工控安全事件，提升学生对工控安全问题的认识和理解。培养一批了具备工控安全基础理论、技能、意识和视野的学生。

培养学生动手实践能力，通过构建工业网络靶场，复现多种典型工业控制场景，在网络靶场中构建了流程工业控制场景、柔性生产线场景、三轴机器人、液体混合控制、饮料生产线、装配场景、温度控制、水处理等10余个虚实场景，为工业领域网络攻防实践和技术研究提供基础的安全演练和技术验证平台。

小班课学生展开工控安全相关研究，近3年发表学术论文4篇，申请国家发明专利20余项，挖掘漏洞7个，并获批国家级大创项目立项1项，获全国研究生网络安全比赛二等奖、中国机器人大赛二等奖、中国大学生计算机设计大赛三等奖、中国高校计算机大赛网络技术挑战赛总决赛三等奖、互联网+大赛省级银奖等，达到较好育人成效。

图 2 工控靶场场景

6 结束语

本文从工业安全人才培养需求角度展开跨领域课程建设方案探讨，以《漏洞挖掘》相关课程为例，以符合国家工业安全需求为导向，以高质量网络安全课程建设为目标，建立了“安全理论”、“安全技能”、“安全意识”、“安全视野”四位一体的课程建设方案，培养安全理论和实践结合、安全意识和视野并存的跨领域网络安全人才。

参 考 文 献

[1] 中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要. 2023

[2] 马力, 陈广勇, 张振峰等. 信息安全技术—网络安全等级保护基本要求(GB/T 22239-2019)

[3] 关键信息基础设施安全保护条例（国令第 745 号）

[4] 网络安全人才实战能力白皮书. 2022

[5] 中国制造 2025(国发〔2015〕28 号)

[6] 深化“互联网+先进制造业”发展工业互联网的指导意见(2017 年第 34 号)

[7] 王星. 美国高等教育网络安全知识体系规范综述[J]. 中国信息安全,2018(4):100-103.

[8] 智联招聘,奇安信. 2021 网络安全人才趋势报告.2021

[9] 张婷，孙磊，藏韦菲.“101 计划”背景下数据库系统与安全课程的思政教学探索[J]. 计算机技术与教育学报, 2024,07(12):7-11.

[10] 田志宏, 王乐, 鲁辉. 创新网络安全人才培养体系支撑网络强国建设[J]. 中国网信, 2023(9):27-31.