 DOI: https://doi.org/10.12345/xdjyjz.v4i7.38265

Research on the Training Model for Industrial Control Security Talent Under the Cooperation Between Universities and Enterprises

Changsong Yang Hai Liang

Guilin University of Electronic TechnologSchool of Computer and Information Security, Guilin, Guangxi, 541004, China

Abstract

With the increasing networking, automation and intelligence of industrial control systems, their security issues have become increasingly prominent. To address the increasingly severe industrial control security problems, the cultivation of industrial control security talents has received widespread attention. Currently, there are still problems such as insufficient practical ability, disconnection between education and industry, and single assessment in the cultivation of industrial control security talents. Therefore, the establishment of an industrial control security talent cultivation model through school-enterprise collaboration becomes the key to solving the problem. This paper studies the industrial control security talent cultivation model under school-enterprise collaboration and establishes a close school-enterprise collaborative education mechanism. By constructing a training system, designing interdisciplinary courses, reforming practical teaching, and establishing a collaborative education model, the training goals are precisely positioned; integrating cutting-edge knowledge to optimize the curriculum system, innovating teaching and practical models, introducing multiple teaching methods, and combining successful cases, the quality of talent cultivation is improved, providing support for the cultivation of industrial control security talents.

Keywords

industrial Control Security; school-Enterprise Cooperation; talent Cultivation; practical teaching reform

校企共建下工控安全人才培养模式研究

杨昌松 梁海

桂林电子科技大学计算机与信息安全学院，中国 · 广西 桂林 541004

摘 要

随着工业控制系统日益网络化、自动化、智能化，其安全问题日益凸显。为应对日益严峻的工控安全问题，工控安全人才培养得到广泛关注。当前工控安全人才培养仍然存在实践能力不足、产教脱节、考核单一等问题，为此校企共建下工控安全人才培养模式成为破局的关键。本文研究校企共建下工控安全人才培养模式，建立紧密校企协同育人机制。通过构建培养体系、跨学科课程设计、实践教学改革和协同育人模式，精准定位培养目标；整合前沿知识优化课程体系，创新教学与实践模式，引入多元教学法，结合成功案例，提升人才培养质量，为工控安全人才培养提供支撑。

关键词

工控安全；校企共建；人才培养；实践教学改革

1 引言

工业控制系统（简称工控系统）作为国家关键基础设施的核心组件，其安全直接关乎国家安全战略全局 [1]。随着工业互联网的深度融合，传统封闭的工控系统加速向开放互联演进，攻击者可基于系统或协议漏洞，借助暴力攻击、恶意代码植入等手段突破安全隔离防线，严重危害工控系统安全。为此，工控安全人才培养已超越单纯的教育命题，演变为关乎国家工业命脉的战略性议题。

当前我国工控安全人才供给面临多重结构性矛盾。一方面攻击技术呈现低门槛、高扩散等特征，而防御能力培养却需跨越工控协议解析、安全架构设计等复合型知识体系 [2]；另一方面传统教育模式的课程体系与真实工业场景存在代际差，导致人才培养滞后于产业需求 [3]。上述工控安全人才培养供需错位在工控系统数字化转型进程中愈发凸显，亟待通过培养模式创新实现破局。

校企共建模式在此背景下展现出独特价值与优势 [4]，

【基金项目】校企共建下工控安全人才培养模式研究项目，广西研究生教育创新计划项（项目编号：JGY2024136）。

【作者简介】杨昌松（1989—），男，中国广西平南人，博士，副教授，从事网络空间安全、安全教育研究。

通过双师型教学团队构建、虚实融合的工控靶场建设等方式，将实战技能深度嵌入培养过程。国家层面已形成政策协同效应，《工业控制系统网络安全防护指南》确立了能力培养基准，而教育部推行的产业导师驻校机制促进了工控系统企业技术向教学资源转化 [5]。这种行业需求驱动 - 教育资源重构 - 安全能力输出的闭环体系，为破解工控安全人才短缺困境提供新范式。本文聚焦校企共建模式的核心创新机制，通过实证研究揭示其对提升工控安全人才实战能力的作用路径，为新型工业化进程中的网络安全人才培养提供理论支撑与实践参照。

2 当前模式研究现状与不足

工控系统的攻防博弈正面临深刻的非对称困境，攻击者依托互联网的无边界性实施跨域渗透，单点攻击即可触发全局性防御响应 [6]，而防御体系的构建却受制于人才能力与系统规模。攻防失衡在人才培养层面表现为显著的路径分化：攻击者通过靶场演练即可快速迭代，但防御能力的塑造须跨越理论认知、漏洞机理分析、安全架构设计等多重知识壁垒 [7]。尤其工控系统与新兴技术的深度融合，防御者既要洞悉工控组件的运行逻辑，又需掌握宿主技术的安全边界，使传统培养模式面临严峻挑战。

当前工控安全人才培养模式存在结构性断裂问题：高校教育受限于知识更新速度，难以同步工业互联网的演进节奏，导致毕业生需企业二次培训方能适配真实工控环境 [8]；社会培训机构聚焦短期技能速成，忽视安全理论体系构建，难以应对复杂威胁；自学成才者虽具备攻击突破能力，却在防御体系设计、安全标准解读等方面存在明显短板。此外，人才评价体系缺乏动态映射行业需求的能力，既无法精准识别防御人员的漏洞挖掘深度，也难以量化评估安全架构师的风险预见能力，致使企业陷入高需求、低匹配的用人困局。

这种能力断层在国际对比中尤为凸显：美国 NICE 网络安全人才框架通过构建包含 7 大角色、33 项职能的立体化能力矩阵，实现了人才培养与工控系统安全需求的精准对接 [9]。反观我国，《工业控制系统网络安全防护指南》虽确立了行业能力基准，但在校企协同育人、跨学科课程开发等环节仍存在实践脱节问题，传统培养模式已难以支撑国家关键基础设施的安全防护需求，迫切提出能贯通技术演进、教育创新与产业应用的新型人才培养模式。

3 “校 – 企 – 赛”人才培养模式构建

本文针对工控安全人才培养的痛点，构建校 - 企 - 赛深度协同的创新人才培养模式，以政府引导为牵引、行业需求为导向、能力产出为核心，将竞赛平台作为检验能力、激发潜能、连接供需的关键纽带。该模式共划分为宏观治理、课程与大纲设计、实践教学与基地建设、标准化认证与评估、持续改进与能力保鲜五大层次，形成闭环培养体系，突出校 - 企 - 赛三环联动。

3.1 宏观治理层

宏观治理层通过构建权责明晰的多方协同机制，为校 - 企 - 赛三环联动提供制度层面保障，其核心架构包含两个关键组织。

一是三方联席指导委员会，成员涵盖教育主管部门代表、高校信息安全领域负责人、工控头部企业安全负责人、行业协会及标准化专家，履行统筹战略规划、资源统筹、进度监控、政策对接四项职能。战略规划主要人员为教育主管部门代表，负责制定区域化工控安全人才培养中长期规划；资源统筹主要人员为高校信息安全领域负责人，负责协调政府经费、企业设备捐赠，重点负责密码学实验室、工控靶场及竞赛平台的经费保障；进度监控主要人员为工控头部企业安全负责人，负责定期审议培养方案执行与竞赛成效；政策对接主要人员为行业协会及标准化专家，负责推动工控安全（含密码应用）纳入专业认证体系，探索校企学分互认机制。

二是密码与工控安全标准工作组，由国家或地方密码管理局专家、工控安全标准委员、高校学科带头人、企业密码工程师及攻防专家组成。聚焦标准制定、技术转化、竞赛赋能三大职能：标准制定主要工作为动态更新《工控安全（密码方向）人才培养能力标准》《工控系统密码应用规范实训大纲》等相关文件；技术转化主要负责将前沿技术转化为教学资源；竞赛赋能负责为校 - 企 - 赛提供权威工控安全赛题，确保竞赛的前瞻性与实战性。

3.2 课程与大纲设计层

该层主要构建基于密码学应用、贯穿理论 - 工具 - 实践的模块化工控安全人才课程体系，强化校 - 企 - 赛三环联动的底层知识基础。课程设计采用核心领域 + 进阶能力双轨框架，核心领域在课程设置上设置工控基础、网络安全、密码学核心及工控安全攻防等课程。

在资源建设上，由校 - 企 - 赛共建知识载体：校方主导工控系统基础与密码理论教材编写，企方主导工控安全案例集与工业安全产品手册，联合开发《工控协议安全实现与分析实验指南》《工控数据安全实训手册》等实战资源，确保课程内容与企业需求同步更新。竞赛平台定期融入工控安全主题赛题，强化学生理论与实践的转化能力。

采用逐级进阶的方式进行能力培养，能力进阶分三级：初级（大一 / 大二）掌握基础原理与密码算法应用，中级（大二 / 大三）熟练漏洞分析、密码配置与审计，高级（大三 / 大四 / 本科毕业后）系统架构设计、密码方案实施与管理。自低向上形成工控安全人才的知识框架，构建工控安全方向的理论学习路线。

3.3 实践教学与基地建设层

实践教学层通过联合实训基地建设与项目驱动，实现校 - 企 - 赛三环联动的技能锻造。

联合实训基地包括校内端与企业端，校内靶场构建虚拟化工控设备仿真平台和攻防演练沙盘，支持密码漏洞挖掘

与红蓝对抗；企业沙箱环境镜像真实生产网络，集成工业防火墙、加密网关等设备，提供企业演练剧本。

双导师制为该层的核心，通过校内导师与企业导师的深度协同，为工控安全人才培养提供全方位过程指导。校内导师依托高校实验室，主导密码学理论与基础实验教学，系统讲授工控协议加密原理、后量子密码迁移策略等核心知识，培养学生的创新思维。企业导师则基于行业实战经验，定期开展工控安全专题讲座，将企业实际项目案例转化为教学素材，让学生获取工业级密码分析资源，供学生实操演练，弥补教学设备与产业一线的代际差。

在项目式学习上，双导师通过理论 - 实践 - 评估的循环评审模式。校内导师审核方案的技术严谨性，企业导师聚焦方案的实施可行性，通过定期的小组联席评审会，对学生的密码漏洞修复方案、应急响应流程等成果提出改进意见，通过不断反馈迭代，确保人才培养与行业需求的动态契合。

项目式学习与竞赛相衔接，校、企共同搭建的竞赛平台作为实践载体，将年度工控安全攻防大赛预赛嵌入校内靶场，决赛在企业环境进行。学生在平台上，可结合仿真系统进行攻防练习，并获取学习结果反馈；导师可统一查看学生学习效果，实现校、企、赛三者无缝衔接。

3.4 标准化认证与评估层

该层通过科学评估体系保障校 - 企 - 赛三环联动的质量闭环。

分级认证体系中，初级认证方式为笔试和实验考核，内容覆盖密码学基础与工控协议安全，实验考核内容为在校内靶场完成标准化任务；中级认证为案例分析与项目设计，聚焦真实工控安全事件，由校企联合打分；高级认证需现场演练，在竞赛平台进行。初级进阶至中级水平依靠量化后的理论知识和实践操作学习成果，累积理论学分与实践学分；中级进阶至高级则借助企业项目经历与行业赛事成绩换算机制。

多维度考核指标采用雷达图模型 [10]，主要考核学生知识掌握度（考试成绩）、技术应用力（项目成果质量）、职业素养（团队协作评分）、企业适配度（企业导师评价与录用意向）。

数字化管理平台中，学生培养档案、成绩 / 项目进度、导师评价、证书颁发均可在线追踪，平台包括学生端、管理端、企业端，三端协同操作：学生端实现学习轨迹可视化与能力短板诊断，管理端配备教学质量预警与资源调度看板，企业端则对接人才能力图谱与招聘通道。

该层经过一系列量化指标与动态反馈，确保工控安全技能达成的可测量性与持续改进。

3.5 持续改进与能力保鲜层

该层通过常态优化机制促进校 - 企 - 赛三环联动的生态进化。

常规反馈与优化通过建立月度问题清单→专项攻关→大纲更新这一逐级、分类的问题解决机制，借助校企联席会议，集中审议课程和项目效果。行业宣传与文化则通过赛事、刊物、文化日等途径。赛事运营过程分别为预赛校级、决赛企业命题、公开赛行业直播；线上建立安全漏洞分析实例、最佳实践案例库；线下设立工控安全主题开放日，并邀请企业工程师进课堂。此外，定期开展研讨会邀请密码专家分享前沿技术，强化安全文化认同。

人才跟踪评价实施毕业 1/3/5 年追踪问卷与企业年度回访，收集岗位匹配度与继续教育需求，并推出能力保鲜计划。竞赛平台作为文化载体，将大赛优秀案例纳入教学资源库，实现校、企、赛资源共享与迭代升级。确保人才培养体系动态适应技术演进，为工控安全提供可持续人才支撑。

4 结语

在工控系统日益网络化、智能化背景下，校企共建的工控安全人才培养模式研究意义重大。本文深入剖析传统工控安全人才培养模式的不足，研究校企共建下工控安全人才培养模式，通过构建培养体系、跨学科课程设计、实践教学改革和协同育人模式，结合成功案例，提升人才培养质量，为工控安全人才培养提供支撑。

参考文献

[1] 乔标. 2 023-2024年中国装备工业发展蓝皮书[M]. 电子工业出版社: 202412: 242.

[2] 孙彦斌, 汪弘毅, 田志宏, 等. 工业控制系统安全防护技术发展研究[J]. 中国工程科学, 2024, 25(6): 126-136.

[3] 朱德全, 曹渡帆. 数字经济时代职业教育人才培养的新使命——基于对就业市场变革的反思[J]. 华南师范大学学报(社会科学版), 2023 (3): 94-105.

[4] 李天松, 周海燕, 黄建华. 校企共建实验室培养创新人才的探索与实践[J]. 桂林电子科技大学学报, 2009, 29(2): 176-179.

[5] 张兵, 邹一琴, 蒋惠凤. 共生视角下的地方本科院校产业学院建设[J]. 高等工程教育研究, 2021, 4: 125-132.

[6] 吕金虎, 任磊, 谭少林, 等. 工业互联网层级架构与安全:复杂网络新视角[J]. 中国科学: 技术科学, 2024, 54(10): 2042-2052.

[7] 徐洁, 袁雪敬. 攻防技术和对抗实训相融合的网络安全创新实践人才培养模式探索[J]. 教育学, 2025, 1(6).

[8] 李晖, 杨超, 张美茹. 知识能力使命三位一体的一流网络安全人才培养体系构建[J]. 工业信息安全, 2024, (03): 58-63.

[9] 秦艳锋, 奚琪, 彭建山. 创新型网络安全人才培养探讨[J]. 网信军民融合, 2019, (04): 62-65.

[10] 迟晓妮, 李洁, 李郴良. 大数据时代统计学专业创新人才培养质量的综合评价模型[J]. 桂林电子科技大学学报, 2024, 44(1): 7-12.