

项目公示信息

一、项目名称：信息物理融合系统安全与控制方法研究及应用

二、提名者及提名意见

提名单位：陕西省教育厅

提名意见：

该项目面向煤矿典型场景信息物理融合系统（Cyber-Physical System, CPS）安全的重大应用需求，对CPS安全与控制方法进行了系统深入的研究，并在煤矿领域开展了示范应用。取得了以下成果：

1. 提出了CPS模糊测试方法，显著提升了煤矿工控系统CPS漏洞挖掘效率。

2. 建立了CPS恶意软件传播动力学模型并揭示其传播机理，提出了一种混合分岔控制方法，有效提升了CPS的安全韧性。

3. 形成了CPS多模态对抗攻击技术体系，大幅提升了煤矿自动驾驶CPS在真实工业环境中的高鲁棒性与高可靠性。

4. 突破了CPS临界可观性验证与强化控制关键技术，实现了系统在恶意攻击下的临界状态精准感知，有效增强了CPS在攻击下的韧性保障能力。

项目成果在陕西彬长小庄矿业有限公司、内蒙古神东天隆武家塔露天煤矿和青岛慧拓智能机器有限公司等多家企业得到了成功应用，显著提升了煤矿领域CPS主动防御能力，有效降低了信息安全事件导致的非计划停产。近年来，累计创造经济效益超过1.3亿元，经济和社会效益显著。

成果材料齐全、规范，经完成单位公示，无知识产权纠纷，人员排序无争议，符合陕西省科学技术奖提名条件。

提名该项目为陕西省科学技术进步奖二等奖。

三、项目简介

信息物理融合系统(Cyber-Physical System, CPS)集成了计算、通信与控制功能，是计算进程和物理进程深度协作和有机融合的下一代智能系统。CPS在煤矿生产、自动驾驶、智能电网、航空航天等安全

关键领域具有广泛应用，已成为学术界与工业界关注的焦点。作为国家关键信息基础设施，CPS 常因设计缺陷与安全漏洞面临外部干扰、恶意攻击或恶意代码注入等威胁，致使系统行为异常甚至失控，进入接近失效的临界状态，严重威胁生产安全，造成重大经济损失与社会影响。因此，保障 CPS 安全可控运行已成为当前亟待突破的关键技术挑战。

本项目面向煤矿典型场景中 CPS 安全的国家重大应用需求，聚焦于“漏洞挖掘—威胁传播—智能攻击—韧性控制”的安全协同保障问题，系统开展了 CPS 漏洞挖掘方法、恶意软件传播建模与分析、对抗样本生成、临界可观性验证与强化控制等多个关键方向的创新研究，构建了覆盖“风险感知、威胁预警、主动防护与弹性恢复”的 CPS 安全协同防御技术体系，为提升 CPS 的主动安全防御与弹性恢复能力提供了系统性解决方案。

主要创新成果有：

创新点 1：针对 CPS 漏洞深度隐匿与高效检测难题，提出了 CPS 工控协议和深度学习模型模糊测试方法，实现了多维度安全威胁的主动侦测与精准溯源。

创新点 2：针对 CPS 中恶意软件传播引发的级联破坏效应难以预测与控制的难题，建立其传播动力学模型，提出了混合分岔控制方法，实现了对系统动态行为的稳定调控。

创新点 3：针对 CPS 中多模态对抗样本生成效率低、隐蔽性差与迁移性不足的难题，提出了面向自动语音识别、图像分类与目标检测模型的对抗样本生成方法，攻克了高迁移性对抗样本的生成效率与隐蔽性提升的技术瓶颈。

创新点 4：针对 CPS 遭受攻击时系统临界状态不可见、验证效率与控制实时性难以协同的难题，提出了高效的临界可观性验证与强化控制方法，攻克了系统隐匿状态精准感知与安全韧性协同增强的技术瓶颈。

紧密围绕“信息物理融合系统安全与控制方法研究及应用”项目，各单位协同攻关，取得了一系列相关核心成果，截止 2024 年 12 月项

目授权国家发明专利 11 项，发表高水平学术论文 20 余篇，培养毕业硕士研究生 15 人。

四、客观评价

本项目相关成果发表于《IEEE Transactions on Automatic Control》《IEEE Internet of Things Journal》等计算机与控制科学领域权威期刊，受到专家学者充分肯定：（1）东北大学付俊教授在著名期刊《IEEE Transactions on Systems, Man, and Cybernetics: Systems》论文中评价临界可观性验证的工作是开创性的；（2）同济大学蒋昌俊教授团队在著名期刊《IEEE Transactions on Computational Social Systems》论文中高度评价本项目所提出的“Petri 网框架下系统临界可观性验证和强化控制方法”。他们指出该方法很好地避免了系统全部状态空间的遍历并找到了有效的控制策略。

五、代表性知识产权和标准规范等目录（限 10 条）

序号	知识产权类别	知识产权名称	国家(地区)	授权号	授权日期	证书编号	权利人	发明人
1	论文	CGFuzzer: A fuzzing approach based on coverage-guided generative adversarial networks for industrial IoT protocols	中国	2022, 9(21): 21607-21619	2022.06.16	IEEE Internet of Things Journal	西安科技大学	Zhenhua Yu, Haolu Wang, Dan Wang, Zhiwu Li, Houbing Song
2	论文	SEI ² RS malware propagation model considering two infection rates in cyber-physical systems	中国	2022, 597: 127207	2022.03.15	Physica A: Statistical Mechanics and its Applications	西安科技大学	Zhenhua Yu, Hongxia Gao, Dan Wang, Abeer Ali Alnuaim, Muhammad Firdausi, Almetwally M. Mostafa
3	论文	Critical observability verification and enforcement of labeled Petri nets by using basis markings	中国	2023,68(12):8158-8164	2023.07.05	IEEE Transactions on Automatic Control	西安科技大学	Xuya Cong, Maria Pia Fanti, Agostino Marcello Mangini, Zhiwu Li

4	论文	Critical observability of labeled time Petri net systems	中国	2023, vol. 20, no. 3, pp. 2063-2074	2022.08.03	IEEE Transactions on Automation Science and Engineering	西安科技大学	Xuya Cong, Maria Pia Fanti, Agostino Marcello Mangini, Zhiwu Li
5	论文	Critical observability of discrete-event systems in a Petri net framework	中国	2022, vol. 52, no. 5, pp. 2789-2799	2021.03.10	IEEE Transactions on Systems, Man, and Cybernetics: Systems	西安科技大学	Xuya Cong, Maria Pia Fanti, Agostino Marcello Mangini, Zhiwu Li
6	论文	Autonomous driving in underground mines via parallel driving operation systems: challenges, frameworks and cases study	中国	10.1109/TIV.2024.3450609	2024.08.28	IEEE Transactions on Intelligent Vehicles	中国科学院大学	Bin Tian, Jing Yang, Caiji Zhang, Xuedi Hao, Shi Meng, Shibin Wang, Zheng Yang, Long Chen, Yanlong Zhao, Shirong Ge
7	发明专利	基于决策边界引导的深度神经网络模型模糊测试方法	中国	ZL202411312996.X	2024.11.15	7529714	西安科技大学	于振华, 李西滕, 李江涛, 杨文建, 丛旭亚, 王丹

8	发明专利	基于增强型神经预测器的黑盒语音对样本生成方法	中国	ZL202411204364.1	2024.12.03	7571262	西安科技大学	于振华，张蕴，胡旭飞，丛旭亚，金浩
9	发明专利	面向图像显著区域的黑盒有目标对抗样本生成方法	中国	ZL202411226146.8	2024.11.22	7543036	西安科技大学	于振华，遆亚舟，叶鸥，丛旭亚，张文超，张蕴
10	发明专利	面向行人目标的多视角自适应权重平衡对抗攻击方法	中国	ZL202410845651.4	2024.09.10	7357751	西安科技大学	张蕴，于振华，殷正，叶鸥，金浩

六、主要完成人情况

姓名	排名	行政职务	技术职称	工作单位	完成单位	对本项目贡献
于振华	1	院长	教授	西安科技大学	西安科技大学	1. 项目负责人，负责项目总体方案设计与组织实施； 2. 负责恶意软件传播、对抗攻击和漏洞挖掘技术研发。
赵彦龙	2	总经理	博士生	中国电信股份有限公司陕西分公司政企群工业行业事业部	中国矿业大学（北京）	1. 项目总体方案设计，项目组织与协调； 2. 理论研究与验证以及项目推广与应用。
丛旭亚	3	无	副教授	西安科技大学	西安科技大学	1. 项目理论研究、总体方案研讨与实施； 2. 负责Petri网临界可观性验证与强化控制研究。
张蕴	4	无	讲师	西安科技大学	西安科技大学	1. 项目理论研究、实施与应用； 2. 负责对抗攻击和漏洞挖掘技术研发及验证工作。
王丹	5	无	副教授	西安科技大学	西安科技大学	1. 项目理论研究、总体方案研讨与实施； 2. 负责恶意软件传播技术和漏洞测试研发及验证工作。
叶鸥	6	无	副教授	西安科技大学	西安科技大学	1. 项目理论研究、实施与应用； 2. 负责对抗攻击技术设计及验证工作。
张文超	7	无	讲师	西安科技大学	西安科技大学	1. 项目理论研究、实施与应用； 2. 负责对抗攻击技术设计及验证工作。
金浩	8	副院长	教授	西安科技大学	西安科技大学	1. 项目理论研究、实施与应用； 2. 负责对抗攻击技术设计及验证工作。

七、主要完成单位情况

1. 西安科技大学

西安科技大学是国家中西部高校基础能力建设工程实施高校、应急管理部和陕西省人民政府共建高校、陕西省国家“双一流”培育高校，是我国西部重要的能源、安全领域人才培养和科技创新基地。在全国第四轮学科评估中，安全科学与工程学科获批 A-，在第五轮学科评估中实现新突破。工程学、材料科学、地球科学、环境科学与生态

学、化学、农业科学等 6 个学科进入 ESI 全球排名前 1%。

学校有雁塔校区和临潼校区，设有研究生院和 21 个学院（部）。拥有安全技术及工程国家重点学科，8 个省级优势特色（重点）学科，涵盖 49 个二级学科。拥有国家煤炭工业采矿工程重点实验室、煤矿智能安全技术与装备重点实验室（省部级）、西部煤矿安全教育部工程研究中心等 36 个省部级以上科研平台，1 个教育部创新团队、13 个陕西省重点科技创新团队。现有 20 个国家级一流本科专业建设点、12 个省级一流本科专业建设点，8 个国家级特色专业、11 个省级特色专业，22 个专业通过中国工程教育专业认证（评估）；17 门国家级一流本科课程、59 门省级一流本科课程，1 门国家精品课程、1 门国家精品资源共享课、62 门省级精品资源共享课程（精品课程），24 门省级课程思政示范课程，1 个国家级教学团队、28 个省级教学团队，1 个省级课程思政教学研究示范中心，1 个国家级人才培养模式创新实验区、15 个省级人才培养模式创新实验区、2 个国家级实验教学示范中心（虚拟仿真实验教学中心），18 个省级实验教学示范中心（虚拟仿真实验教学中心）。近年来，获国家级教学成果奖 3 项。

学校现有 8 个一级学科博士点、1 个专业学位博士点，7 个博士后科研流动站，27 个一级学科硕士点、13 个专业学位硕士点，60 个本科专业，形成了以地矿、安全及其相关学科为特色，以工科为主体，工、理、文、管、法、经、艺、教、交叉协调发展的办学格局，全日制在校生 2.6 万人。

学校有教职工 2300 余人，专任教师 1500 余人，教授、副教授 800 余人，教师中具有博硕士学位者 1400 余人。学校“十四五”以来，承担科研项目 6400 余项，其中国家重大科技专项课题、国家重点研发计划、国家自然科学基金以及国家社科基金等国家级项目 370 余项，科研经费合同总额已逾 18 亿元，获得省部级以上科技奖 605 项，授权专利 960 余项。签订千万元以上重大横向项目 7 项，500 万元以上横向项目 30 项，100 万元以上横向项目 230 余项。科研项目总数、项目合同额和到款总经费稳步增长。

3. 中国矿业大学(北京)

中国矿业大学（北京）是教育部直属的全国重点高校、国家“211工程”、“985优势学科创新平台项目”、“双一流”建设高校，是全国首批产业技术创新战略联盟高校，同时也是教育部与原国家安全生产监督管理局共建高校。1960年和1978年，学校先后两次被确定为全国重点高校，为全国首批具有博士和硕士授予权的高校之一，设有研究生院和13个学院。学校有两个校区：学院路校区坐落于北京市高校云集的海淀区学院路，沙河校区坐落于北京市昌平沙河高教园区。目前在校学生1.9万余人，其中本科生9200余人，硕士生7800余人，博士生1900余人。

1997年，学校被确定为国家“211工程”重点建设高校，2006年成为“985优势学科创新平台项目”建设高校，2017年成为世界一流学科建设高校，2022年入选新一轮“双一流”建设高校。目前，学校矿业工程、安全科学与工程2个学科列入国家“双一流”建设学科，城市工程地球物理、城市地下空间工程2个学科列入北京高校高精尖学科建设名单。在教育部多次学科评估中，学校均取得了优秀成绩。10个学科进入ESI排名前1%，其中工程学学科、地球科学学科及环境科学与生态学学科进入ESI排名前1%。党的十八大以来，学校完成与煤炭科技相关重要课题1600余项，主持国家重点研发计划等国家级重大项目81项，获批国家自然科学基金创新研究群体项目2项。共获国家级科技奖励20项，省部级科技奖励926项。学校建有2个全国重点实验室，1个国家工程研究中心，1个国家技术创新中心，2个教育部工程研究中心，3个应急管理部重点实验室，1个北京市重点实验室，共建应急管理部国家安全科学与工程院。

八、完成人合作关系说明

“信息物理融合系统安全与控制方法研究及应用”项目研制过程中主要完成人共8人，于振华、丛旭亚，张蕴，王丹，叶鸥，张文超，金浩7人为西安科技大学成员，赵彦龙1人为中国矿业大学（北京）成员，合作期间2个单位在项目研制过程中取得了一系列共同的研究成果。完成人和完成单位按照实际贡献大小依次排名，各完成人和完成单位一致同意其排名。现对完成人合作关系及参与并做出重要贡献说

明如下：

序号	合作方式	合作者/项目排名	合作起始时间	合作完成时间	合作成果	证明材料
1	论文合著	于振华/1 王丹/5	2020 年 8 月 15 日	2022 年 6 月 30 日	CGFuzzer: A fuzzing approach based on coverage-guided generative adversarial networks for industrial IoT protocols	doi: 10.1109/JIOT.2022.3183952
2	论文合著	于振华/1 王丹/5	2020 年 7 月 14 日	2022 年 3 月 31 日	SEI ² RS malware propagation model considering two infection rates in cyber-physical systems	doi: 10.1016/j.physa.2022.127207
3	论文合著	丛旭亚/3	2021 年 7 月 1 日	2023 年 7 月 31 日	Critical observability verification and enforcement of labeled Petri nets by using basis markings	doi: 10.1109/TAC.2023.3292747
4	论文合著	丛旭亚/3	2020 年 11 月 1 日	2022 年 8 月 10 日	Critical observability of labeled time Petri net systems	doi: 10.1109/TASE.2022.3193493
5	论文合著	丛旭亚/3	2020 年 8 月 1 日	2021 年 3 月 31 日	Critical observability of discrete-event systems in a Petri net framework	doi: 10.1109/TSMC.2021.3056693
6	论文合著	赵彦龙/2	2022 年 6 月 1 日	2024 年 8 月 28 日	Autonomous driving in underground mines via parallel driving operation systems: challenges frameworks and cases study	doi: 10.1109/TIV.2024.3450609
7	共同知识产权合作	于振华/1 丛旭亚/3 王丹/5	2020 年 11 月 1 日	2024 年 11 月 25 日	基于决策边界引导的深度神经网络模型模糊测试方法	发明专利授权号: ZL202411312996.X

8	共同知识 产权合作	于振华/1 丛旭亚/3 张蕴/4 金浩/8	2020 年 11 月 15 日	2024 年 12 月 31 日	基于增强型神经预测器 的黑盒语音对样本生成 方法	发明专利授权 号： ZL2024112043 64.1
9	共同知识 产权合作	于振华/1 丛旭亚/3 张蕴/4 叶鸥/6 张文超/7	2020 年 11 月 1 日	2024 年 11 月 31 日	面向图像显著区域的黑 盒有目标对抗样本生成 方法	发明专利授权 号： ZL2024112261 46.8
10	共同知识 产权合作	于振华/1 张蕴/4 叶鸥/6 金浩/8	2022 年 10 月 1 日	2024 年 9 月 30 日	面向行人目标的多视角 自适应权重平衡对抗攻 击方法	发明专利授权 号： ZL2024108456 51.4
11	项目共同 立项合作	于振华/1 赵彦龙/2 丛旭亚/3 叶鸥/6	2022 年 5 月 1 日	2022 年 12 月 31 日	陕西小保当矿业有限公 司面向数据-云服务体系 结构的智慧矿区建设模 式及应用研究项目	项目编号： 6000229230