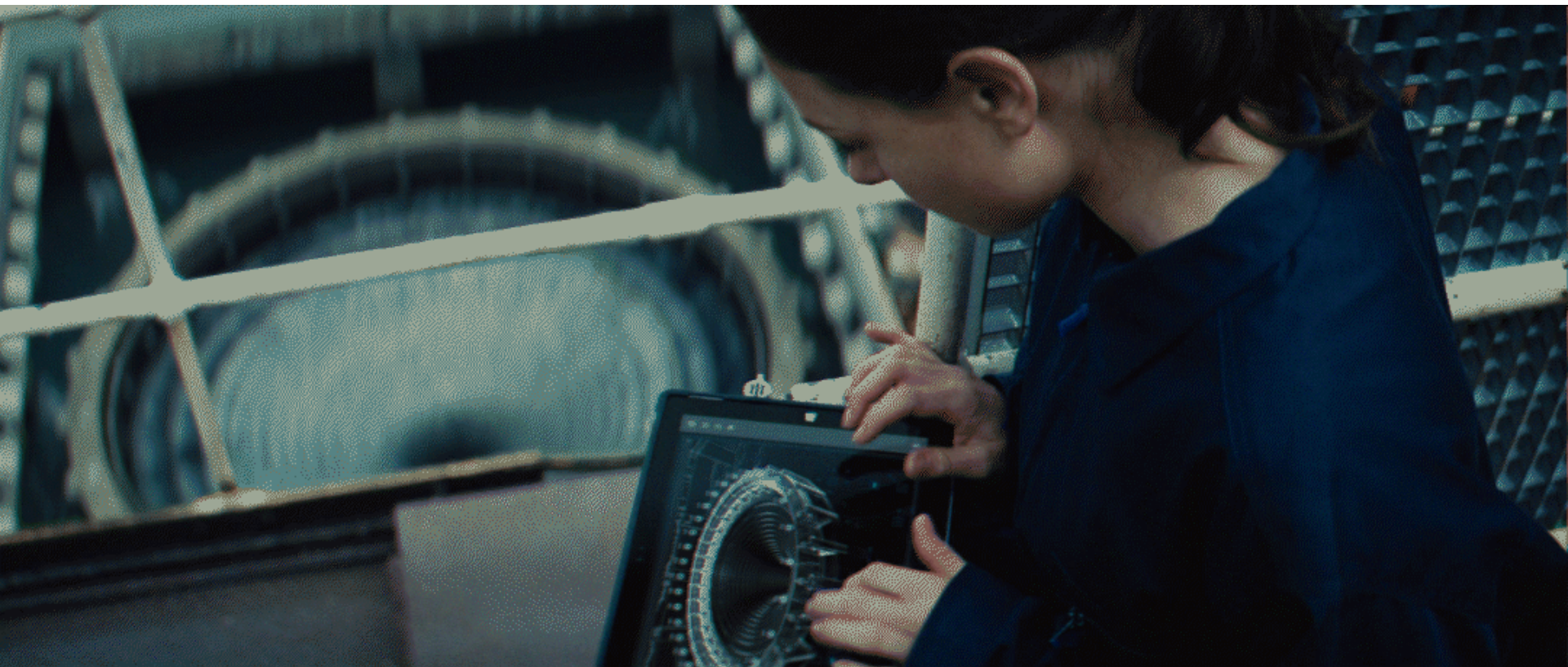


The background of the entire image is a black and white photograph of an industrial setting. It shows a large machine, possibly a lathe or a mill, with a workpiece being processed. Bright sparks are flying from the point of contact between the tool and the workpiece, creating a dynamic and somewhat chaotic scene. The sparks are concentrated in the lower-left and lower-right areas, while the upper part of the image is dominated by the dark, metallic structure of the machine. The overall tone is industrial and technical.

工业控制网络安全，人才先行

秦征

 匡恩网络 | 北京匡恩网络科技责任有限公司



工业控制网络安全涉及的领域

基础设施



智能制造



智慧城市



军工生产



全球工控网络安全态势

工业控制网络安全事件呈逐年增加趋势

2016

年04月

德国核电站遭恶意攻击停产



2016

年01月

以色列电力供应系统受到重大网络攻击



2016

年01月

乌克兰最大机场被控制



2015

年12月

BlackEnergy”病毒攻击乌克兰电网



2015

韩国核电站被朝鲜攻击



工控网络安全成为各国网络空间主战场和反恐新战场

- 工控网络安全领域的对抗提升为国家核心竞争力
- 美国、欧盟等增加预算应对日益升级的网络威胁
- “代码”即武器
- 恐怖主义威胁渗透到工业控制系统，关键基础设施成为主要攻击目标

中国工控网络安全态势

- 工业控制系统规模巨大且超过80%依赖进口
- 智能化改造，生产网络从开放走向互联，在线系统网络安全威胁加剧
- 大规模新建系统依然缺乏网络安全规划和设计

工控网络
现状体现
高覆盖率
与高危

工控网络安全
产业任重
而道远

- 工控系统责任单位安全意识有待加强
- 工控网络安全风险感知能力欠缺
- 现有防护手段无法防御不断升级的网络攻击和数据窃取
- 安全标准有待完善
- 产业生态有待构建

防御之道——“4+1”安全防护体系



4+1 安全防护体系

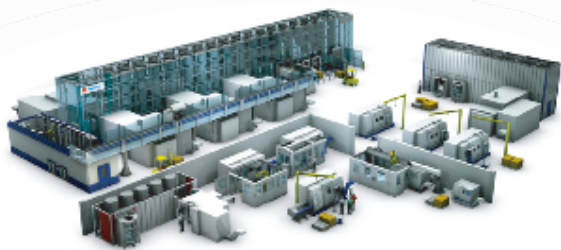
完美诠释智能工业网络安全防护精髓，实现从网络安全到功能安全到基础设施安全的一体化大安全，实现综合防护能力，奠定行业领先优势

以检测和保护两大类产品、

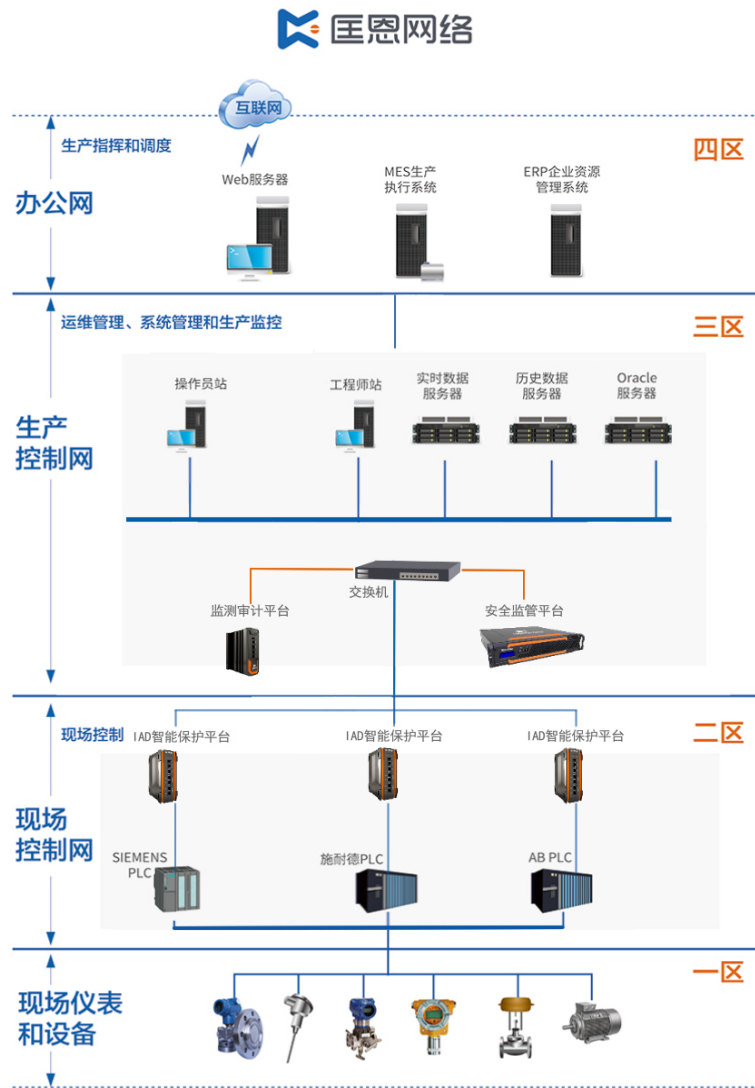
11个产品系列为支撑的全生命周期解决方案，保障国家关键基础设施安全

工控网络与互联网和办公网有本质的区别

- 网络通讯协议不同
- 对系统稳定性要求高
- 系统运行环境不同
- 更新代价高
- 网络结构和行为稳定性高



工业控制网络



跨界的尖端实验室



打造复合型应用创新型工控网络安全人才



短期与长期阶段性人才发展目标

- 面向工业生产、物联网、智慧城市相关的企业、部门
- 基于岗位职责定义安全人才知识结构和技能需求
- 基于知识和技能需求，定义课程体系和认证体系
- 有针对性的推出不同行业不同岗位不同级别的培训和认证

**基于岗位的应用
型人才培养**

短期培养目标

**基于知识领域的
学科教育**

长期人才发展

- 面向高校计算机、信息安全、自动化相关专业
- 基于市场和行业定义工控安全理论和实践型人才的需求
- 基于知识层次和人才发展目标，从理论和实践定义教材和实验环境。
- 有针对性的推出不同专业的教材、教案、实验环境

工控网络安全人才认证评测体系

资质类认证：

专家级认证

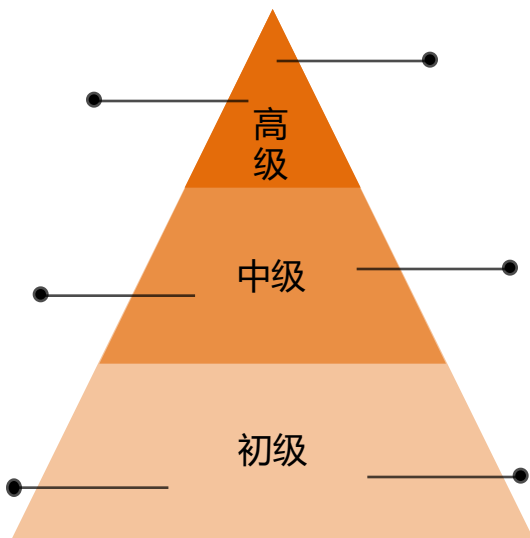
- 认证工控网络安全专家
- CISSP **CISAW**

专业级认证

- 认证工控网络安全工程师
- CISP **CISAW**

基础级认证

- 认证工控网络安全基础级
- **ASC-ICSF**



培养目标：面向管理岗，培养具备工控安全管理规划、策略设计等能力的工控安全专业人士

培训内容：工控安全技术基础、工控安全管理体系建设、工控安全政策态势

培养目标：面向工控技术，岗培养具备工控安全技术检查、防护、运维能力的专业工程师

培训内容：工控安全防护技术、工控风险分析技术、工控安全运维技术和应急案例

培养目标：面向工控行业需求的基础岗位，培养具有安全基础能力和安全意识的人员

培训内容：工控安全意识、工控网络安全管理基础、工控网络安全技术基础

基于工控安全理论知识框架与行业安全特点，总结工控安全人才技能特点，强调认证人员对工控安全知识技能的掌握与应用，解决各行业对各层次工控安全人员的技能评价标准，推进工控安全人才的专业晋升通道，提升各行业安全保障能力水平。

匡恩网络教育项目

助力培养工业网络安全人才



联合人才培养

面向人才亟缺的工业网络安全设计、开发、管理、维护人才开设课程，设计人才培养方案；设立奖学金，接收学生实习等



共建实验室

与学校共建针对工业网络、攻防对抗、高仿真的实验室，供学校教学、科研的需要。



联合科研

面向工业网络安全的一些关键技术和课题，与学校开展科学研究，并针对相应行业的安全标准研究展开合作。



创新创业

依托溢斯德瑞创新产业创新集团的平台，支持和孵化学校师生的创新创业项目

联合人才培养

专业建设



- ✓ 联合课程开发
- ✓ 联合教材建设
- ✓ 师资培训和交流
- ✓ 工控安全教育联盟

校企合作育人



- ✓ 设立奖学金
- ✓ 学生实习实训
- ✓ 学生竞赛

对外培训



- ✓ 联合培训中心
- ✓ 联合技能认证
- ✓ 各级各类企业培训

共建实验室



工控安全教学实验室

- 针对控制流程的实验
- 针对工控安全的实验

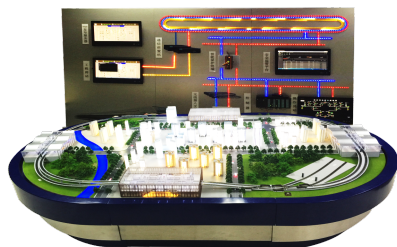


面向行业的高仿真平台

- 电力、化工、制造、交通等
- 智慧城市



面向国家重大基础设施、 智能制造等方向的攻防对抗平台

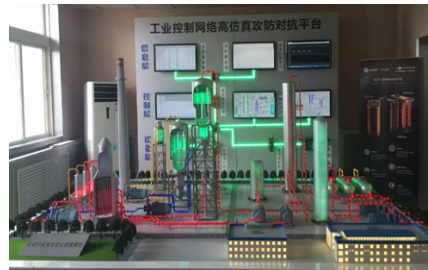


 中国电子技术标准化研究院
China Electronics Standardization Institute

 匡恩网络



 SIPAI[®] 上海工业自动化仪表研究院
西派埃 Shanghai Institute of Process Automation Instrumentation

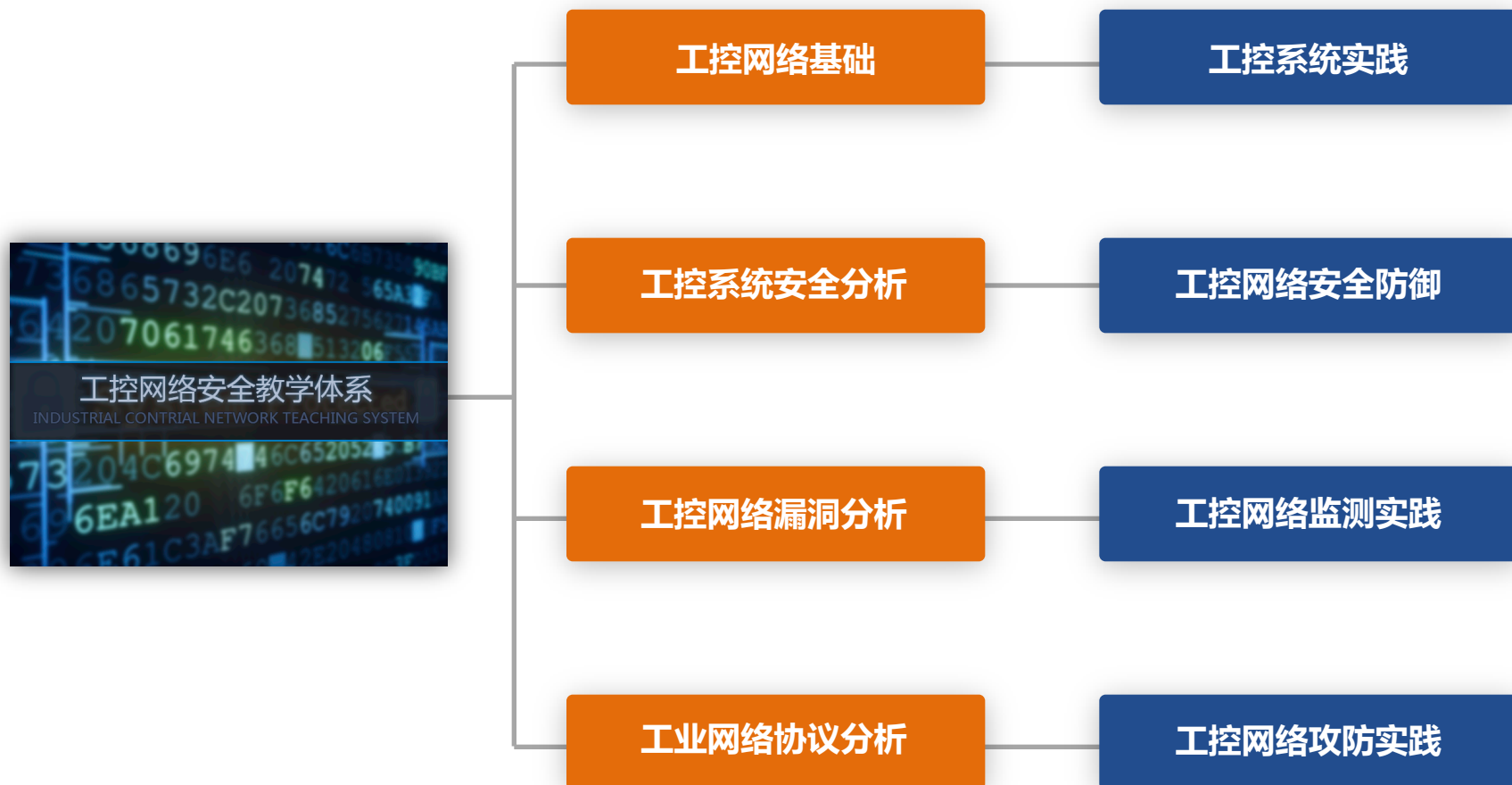


山东省电子信息产品检验院
中国赛宝（山东）实验室
山东省网络与信息安全测评中心



四川大学
SICHUAN UNIVERSITY

丰富的工控网络安全教学体系



典型的工业控制系统环境



集成主流PLC、
HMI
构建的小型工业控
制系统

具有典型自动化行业
控制元素

展示工业控制系统
拓扑架构和特点

支持自动化控制系
统实验

真实的工控网络安全攻防实验环境

工控网络
攻击
实验



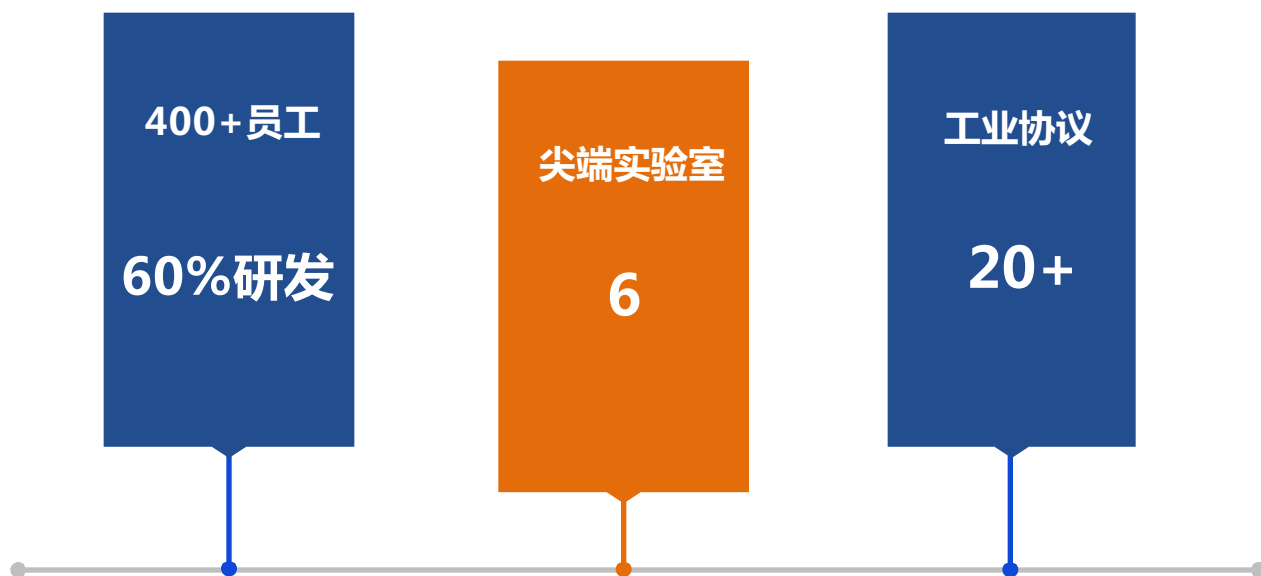
工控网络
监测和异
常行为分
析实验

工控网络
攻击防护
实验

以实际工控系统
为攻防目标

理论结合实践系统学
习、实践和研究工控
网络安全

专业工控安全研究团队支持



双创基地建设

创新

新学科建设

创新项目 引导支持

创业

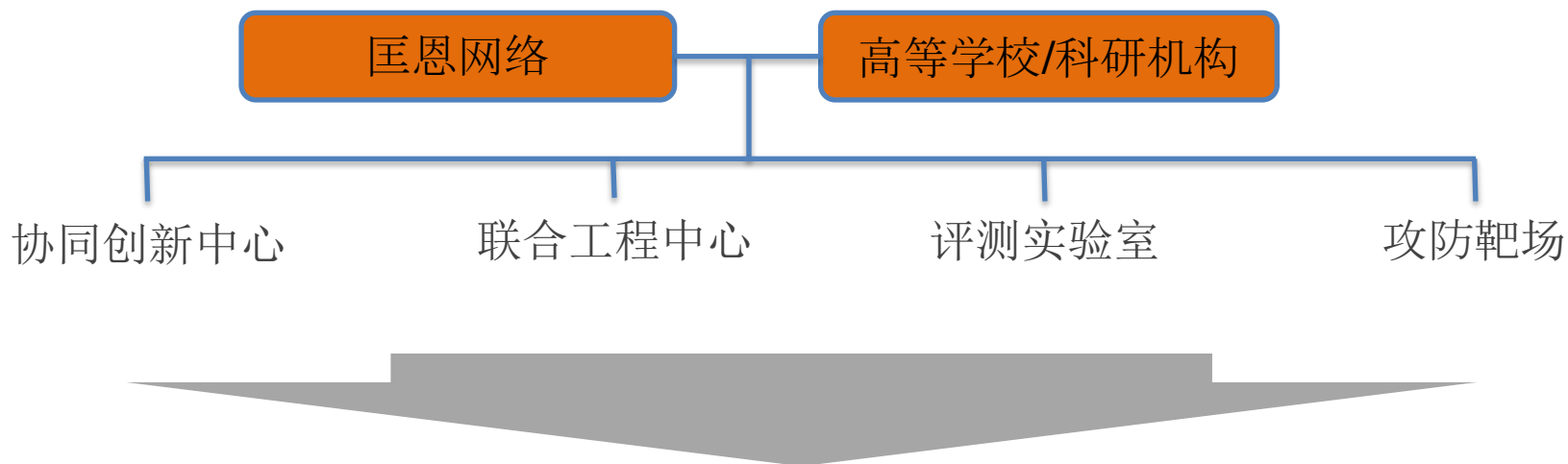
安全类产品孵化

创业指导

多方共建共享：由学校、学生、企业、社会团体共同参与。学校作为基地主要建设者和管理者，企业作为一定社会资源的持有者，学生在基地中实习实践，社会团体提供公共服务。学生在提高实践能力的同时为企业提供技术资源，为学校争取荣誉，为社会创造价值。

产学深度结合：提供良好的学生实习实践平台，从而激励学生创造出优质的资源，为各类高新技术企业合作生产、研发提供支持，以具有可营利性的项目为纽带，促进校企深度合作，将学习研发产生的成果产业化，真正实现产学结合。

联合科研



- 行业工控安全研究
- 标准研究
- 研究成果工程化、产品化
- 工业控制网络安全测评
- 联合申请科研项目



· 匡恩网络，守护未来 ·

电话: (010) 5670-5608 传真: (010) 59512799

官网: www.kuangn.com

地址: 北京市海淀区知春路7号致真大厦D座13层