一、工业信息安全及汽车安全方向

拟招收人数：2人

科研项目相关信息：

**题目：工业信息安全关键技术研究**

**来源：**工业信息安全综合保障体系建设

**背景及重要性：**工业控制系统信息安全（以下简称“工控安全”）是国家网络和信息安全的重要组成部分，是推动智能制造、互联网+制造业发展的基础保障。当前，随着工控系统从单机走向互联、从封闭走向开放、从自动化走向智能化，工控安全形势日益复杂、严峻和紧迫。面对工控安全的严峻形势，急需面向工业信息安全保障相关领域，开展技术研究、标准研制等工作，在为相关行业主管部门提供技术支撑的同时，切实提升我国工业企业工业信息安全防护能力。

**研究内容：**围绕当前我国工业领域可靠性高、实时性强等特点，结合工业互联网等新兴业态特征，提炼工业领域信息安全实际需求，运用人工智能、云计算、大数据等新兴技术，开展风险评估、入侵检测、协议安全性分析、主动防护技术等方面的研究以及标准化相关研究，形成论文专利、标准规范等成果。

**知识掌握情况：**通过开展工业信息安全关键技术研究工作，学生可熟练掌握工业控制系统信息安全、工业互联网安全等当前热点交叉领域相关技术知识，且具备现场实地开展工业信息安全相关工作经验，同时具备相关标准化能力。

**题目：**汽车网络安全技术研究项目

**研究内容：**围绕汽车内部网络（车内以太网、CAN等）与汽车外部网络（C-V2X、蓝牙等）的不同安全需求，开展相关安全研究，提出相应的网络安全防护技术要求，以及对其技术实现有效性进行测试评价的方法，包括网络控制、网络审计、网络异常检测等方面，最终形成相关科研成果及标准规范。

**背景及重要性：**智能汽车的发展催生出日益多样化的电控单元（Electronic Control Unit，ECU）的出现，为了实现ECU之间进行数据的共享和快速交换，同时保障信息安全性能，行业内逐步实现了由LIN、CAN/CANFD、MOST、FlexRay、以太网多种总线技术和以太网实现的复杂汽车电子网络系统。同时，随着5G及自动驾驶技术的发展，V2X通信将越来越普遍，是构筑未来智慧交通的基础。而汽车内部和外部网络的安全问题是将这些技术应用到现实场景中的关键，也是目前的研究热点方向，具有十分重大价值和意义。

 **知识掌握情况：**通过汽车网络安全技术研究，可帮助学生熟悉、掌握当前汽车内部网络、外部网络相关安全技术、测评方法等，同时掌握相关科研能力、标准化工作能力。

二、生物特征信息安全与隐私研究

**今年拟招收学生人数：**2

**科研题目：**国家重点研发计划《人体生物特征识别安全技术标准研究》

**科研背景及重要性：**通过研究人体生物特征识别呈现攻击检测、安全评估和安全防范等相关技术，研制人体生物特征识别系统中呈现攻击检测的框架、数据格式与测试，信息保护要求，安全评估框架、准则与方法，公共安全领域数据生命周期管理安全要求和评测数据库要求等方面标准，为人体生物特征识别系统的安全防范提供标准化指导。

**科研具体内容：**针对恶意者伪造和窃取他人的生物特征攻击或欺骗生物特征识别系统事件频发而相关标准缺失的问题，开展生物特征识别系统呈现攻击检测共性技术系列标准研制。通过研制呈现攻击检测框架、测试和报告等国家标准，提升生物特征识别呈现攻击检测能力；通过研制呈现攻击检测数据格式标准，规范检测结果的通用数据格式，为实现其他应用系统与生物特征识别系统间互联互通操作提供支撑，保证数据格式的统一性和互操作性。

**学生掌握程度：**掌握生物特征信息全生命周期管理过程中的安全与隐私保护方法以及基础理论。

三、移动互联网数据安全与隐私研究

**今年拟招收学生人数：**1人。

**科研题目：**移动应用隐私数据保护及隐私数据泄露检测关键技术研究。

**课题来源：**App违法违规收集使用个人信息专项治理；

重点研发计划：移动互联网隐私课题。

**科研背景及重要性：**随着移动互联网的发展，各种移动应用已经成为了我们日常生活中必不可少的工具。有报告显示，我国移动互联网用户中，手机每日亮屏累计超过两小时的用户占比超过42%。移动互联网用户平均使用应用16.6个。移动应用在方便人们的日常生活的同时也带来了严重的用户隐私泄露问题。调查显示，移动应用导致的隐私泄露已经超过了手机丢失导致的隐私泄露，成为Android手机用户最担心的隐私泄露渠道。与此同时，近来频发的用户隐私泄露事件以及欧盟GDPR和我国《个人信息安全规范》的发布，使得用户隐私问题成为了全社会关注的热点问题。移动应用隐私数据保护及隐私数据泄露检测技术是在移动互联网环境下保护用户隐私的关键技术，也是目前的研究热点方向，具有十分重大价值和意义。

**科研具体内容：**围绕移动应用的隐私数据保护技术和移动应用的隐私数据泄露检测技术，从数据生命周期的角度开展相关研究，提出相应的移动应用隐私数据保护技术要求，以及对其技术实现有效性进行测试评价的方法，包括差分隐私保护、数据流分析、App动静态检测等方面，最终形成相关科研成果及标准规范。

**学生掌握程度：**通过对移动应用隐私数据保护技术及隐私数据泄露检测技术的研究，可帮助学生熟悉、掌握当前移动应用中采用的主流安全技术、App动静态分析技术、App逆向分析技术、数据流分析技术等，同时掌握相关科研能力、标准化工作能力。

**前期培养情况总结：**

前期，我院联合西安电子科技大学，面向信息安全方向，开展硕士研究生培养工作。截至目前，已培养硕士研究生11名。所培养硕士研究生，在我院实习、研读期间，在信息安全标准化、工业控制系统信息安全、物联网安全、军工标准等领域，获得了大量实践机会和科研经历，有助于学生个人能力的全面提升。

四、数据安全及人工智能安全方向

拟招收人数：1人

科研项目相关信息：

**题目：数据安全与人工智能安全技术研究**

**来源：工业互联网数据安全防护与技术评估**

**背景及重要性：**工业互联网是全球工业系统与高级计算、分析、感应技术以及互联网连接融合的结果。工业互联网通过智能机器间的连接并最终将人机连接，结合软件和大数据分析，重构全球工业、激发生产力。工业互联网涉及软硬件平台、数据、人工智能等诸多关键技术领域，具有应用场景多、融合度高、智能化需求强等特点，其安全问题也日益复杂、严峻和紧迫。基于工业互联网领域安全需求，急需推进数据安全、人工智能安全等相关领域保障能力建设，深入开展技术研究、标准研制等重点工作，在为相关行业主管部门提供技术支撑的同时，切实提升我国工业互联网安全防护能力。

**研究内容：**围绕工业互联网数据安全保护需求，研制覆盖收集、存储、处理、转移、删除等各环节的数据安全防护解决方案，实现数据分级分类管理、统一认证、隐私保护等能力。围绕工业互联网环境下人工智能技术广泛应用和安全风险，研究人工智能安全评估技术，开展人工智能安全技术能力建设。

**知识掌握情况：**基于工业互联网复杂场景，开展数据安全和人工智能安全技术研究工作，学生可熟练掌握数据安全、工业互联网、人工智能安全等热点交叉领域技术知识，具备工业互联网环境下开展数据安全和人工智能安全相关工作和研究能力，同时具备相关标准化能力。