

基于RISC-V的工业机器人安全增强装置

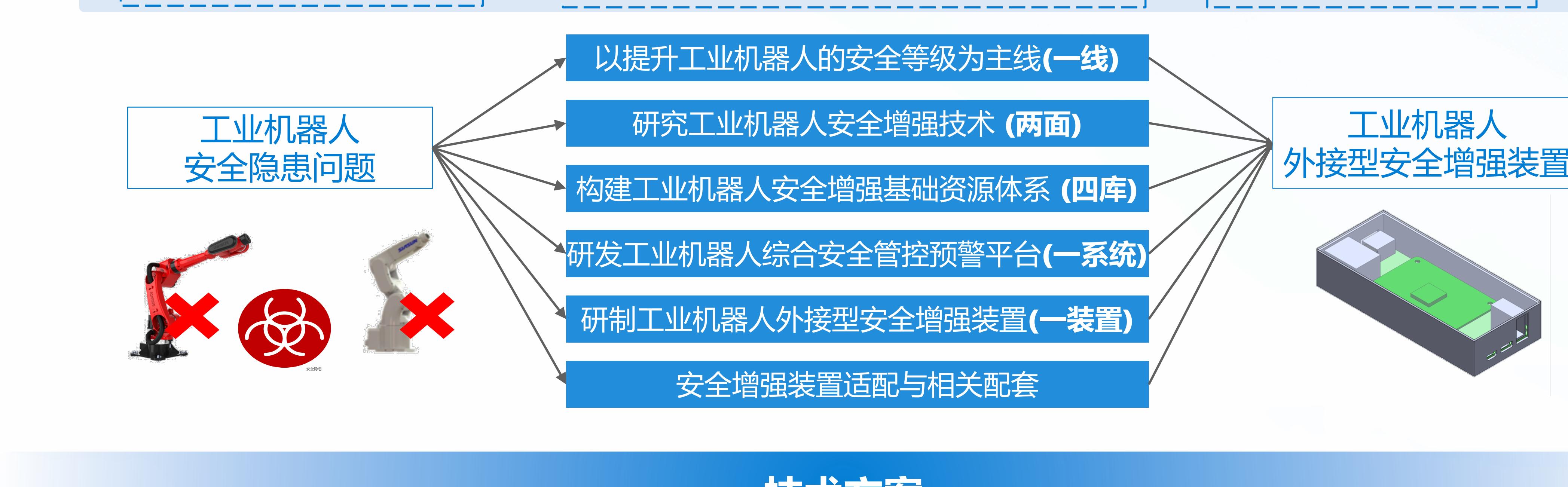
芮志清 常逐阳 武延军 罗天悦 朱琳 吴敬征

芮志清 电话: 18811520398 邮箱: zhiqing@iscas.ac.cn

研究目标

总体目标

基于工业机器人安全隐患问题, 研究首个国产自主可控的工业机器人安全增强装置



技术方案



研发过程由技术基础研究、预警平台搭建、外接装置设计组装、工业机器人适配四部分组成，其中外接装置采用RISC-V芯片研发，从根本上解决技术制约问题，实现国产自主可控。

研发成果及特点

外接型安全增强装置本体

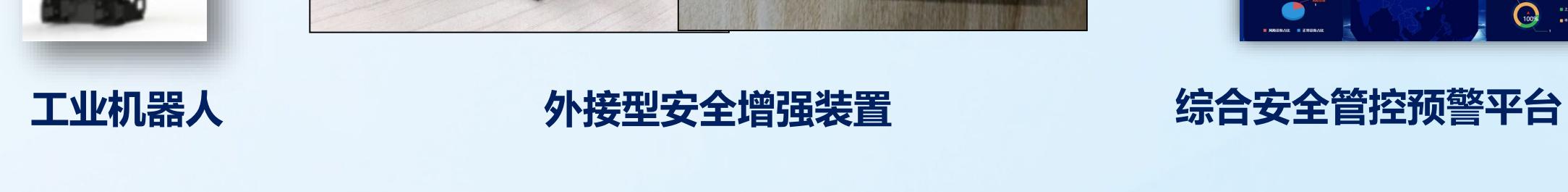
- 硬件基础：自主研发小型外接装置硬件

采用RISC-V处理器研发，实现国产自主可控

- 接口适配：支持4种常见通信接口
- 系统接入：支持接入全部主流操作系统
- 基础技术：病毒扫描、流量分析等安全技术
- 通信安全：通过安全信道接入外接装置
- 电磁屏蔽：满足GB17625.1, GB9254, GB4943.1标准
- 安全支持：提供系统安全信息采集、安全加固功能，内置**身份认证、口令加密、日志记录、协议分析**，具备**入侵检测、系统漏洞和木马扫描、可信启动保护及可信执行**等功能。



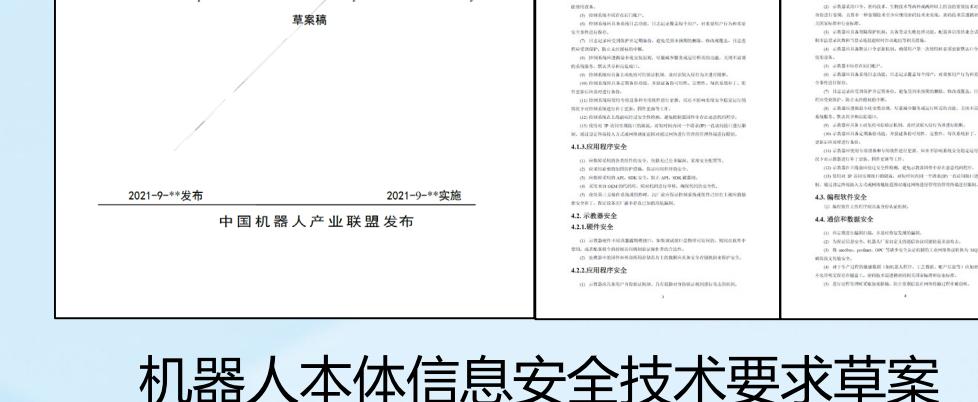
综合安全管控预警平台



- 与外接安全装置建立可信连接
- 采集工业机器人信息
- 检测包括异常攻击、漏洞扫描等工业机器人安全威胁
- 检测结果**数据可视化**分析展示，具备**态势感知**功能
- 依托数据支撑做出**安全决策**
- 下发安全加固策略，及时拦截工业机器人安全威胁

整体作用及影响

- 首个工业机器人外接型安全增强装置
- 基于RISC-V研发，实现**软硬件全面自主可控**
- 支持Linux、QNX、VxWorks、SylinxOS等全部**主流操作系统的工业机器人**使用，覆盖市面主流机型
- 动态感知工业机器人信息，可防范**50多种**常见工业机器人攻击方式，阻断**50种**工业机器人异常行为
- 支持**1.6万种**常用开源基础软件漏洞扫描
- 已生产1050台外接装置，并在**20多家规模以上企业**开展应用
- 已发现工业机器人**安全漏洞31个**
- 已形成工业机器人本体安全、安全防护装置产品设计标准草案，**建立行业安全检测标准**



机器人本体信息安全技术要求草案