前　言

随着人工智能技术的快速发展，人机物融合智能系统（AI-enabled HCPS）深度融合人、信息与物理环境，智能化水平不断提升，对系统安全可信运行提出了更高要求。然而，人工智能在安全性、可靠性和可信性等方面仍存在不足，算法、模型及系统层面的潜在风险制约了其在高安全需求场景中的应用。因此，加强人机物融合智能系统的安全可信保障，已成为推动人工智能技术落地应用、支撑系统可靠运行的重要前提。面向这一需求，本专题以“面向人机物融合智能系统的安全可信”为主题，聚焦可信人机物融合智能系统的前沿进展与实践探索，邀请领域专家围绕系统安全可信理论、技术与方法开展深入讨论，重点关注智能系统规约、建模与验证、漏洞检测以及攻击与防御等关键问题。

嵌入式系统需求规约是系统开发的基础，承担着将用户意图转化为明确、可执行软件需求的重要作用。当前，该过程高度依赖领域专家的人工推导与撰写，存在效率低、可解释性不足等局限。尽管自动化需求生成被视为潜在解决途径，但仍面临领域知识嵌入不足，以及难以同时满足意图可满足性与需求可追溯性等挑战。为此，王春晖等人提出了一种基于大语言模型的可解释需求规约方法，通过构建融合领域知识与需求工程的提示链，在人机协同下逐步补全和细化用户意图，生成具备可解释性的软件需求。

搜索树类算法广泛应用于数据库索引、编译器设计和文件系统等领域，其正确性验证是保障软件可靠性的关键。针对传统方法中数学建模不足、验证过程依赖手工证明且成本较高等问题，左正康等人提出了一种 Isabelle 驱动的搜索树类算法建模与自动化验证方法。该方法基于形式化验证的函数式建模库，构建了面向搜索树结构的模块化建模与自动验证框架，并结合可复用引理库和分块验证策略，有效降低了验证复杂度，同时支持函数式可执行程序生成，框架为特定领域复杂数据结构算法的形式化验证提供了系统性且高度自动化的解决方案，同时为生成正确的函数式可执行程序提供了可行路径与方法保障。

人机物融合智能系统面临多源异构数据的动态访问需求，高优先级数据的高效检索对系统实时感知与智能决策至关重要。优先搜索树融合了搜索树与优先队列特性，但其静态优先级机制在访问分布偏斜场景下易导致检索效率下降。为此，左正康等人提出了一种函数式自适应优先搜索树，在函数式建模与机械化验证保障正确性的基础上，依据访问分布动态调整数据优先级，并引入热点转移机制缓解旧热点固化问题，从而提升访问敏感数据的检索性能。

在人机物融合智能系统中，软件漏洞检测是保障系统安全可信运行的重要环节。图神经网络和代码预训练模型虽已广泛应用于漏洞检测，并在常规数据集上取得优异性能，但这类数据集中的漏洞样本与非漏洞样本通常来源不同，易导致模型学习到与漏洞本质无关的虚假特征。针对现有方法难以准确区分漏洞代码及其修复版本的问题，朱嘉豪等人构建了包含漏洞代码及对应修复版本的配对数据集，并在此基础上系统评估了主流漏洞检测模型的成对预测能力，揭示了现有模型在漏洞语义建模和局部关键信息聚合方面的不足，进一步提出了新的改进方法，为提升漏洞检测模型的鲁棒性与可靠性提供了新思路。

在人机物融合智能系统中，大语言模型通过调用外部工具与环境交互，为系统智能化提供了新的能力，也带来了新的安全风险。随着模型上下文协议（MCP）的应用扩展，MCP服务器所集成工具的权限配置与调用控制，正成为影响系统安全可信的重要因素。针对现有MCP服务器及工具权限边界不清、易被滥用的问题，张泉等人提出了一种面向MCP服务器的自动化分析框架，通过静态分析识别工具调用的权限接口及其调用方式，并依据权限敏感性与行为特征开展分类分析，揭示了当前MCP生态中的权限使用风险，为构建更安全的权限控制机制提供了依据。

面向人机物融合系统的安全可信是一个具有重要理论价值和应用前景的研究方向。本专题的出版，对于推动该领域相关理论、方法与技术研究具有积极意义。受篇幅所限，本专题难以全面呈现这一方向的全部最新进展，但我们希望所收录的工作能够为相关研究和实践提供参考与启发，进一步促进学术交流与创新发展。

在此，我们衷心感谢《计算机研究与发展》为本专题提供宝贵平台，感谢作者、审稿专家和编辑部老师为本专题顺利出版所付出的辛勤努力。谨向所有关心和支持本专题工作的专家学者致以诚挚谢意！

董震（复旦大学）
杜德慧（华东师范大学）
张民（华东师范大学）
岳涛（北京航空航天大学）
梁鹏（武汉大学）

2026年4月