DOI: 10.7544/issn1000-1239.ps20230702
60(7): 1432−1432, 2023

黑盒验证：无人驾驶系统安全挑战的解决途径

蒲戈光

（华东师范大学软件工程学院　上海　200062）

无人驾驶是未来交通的必然. 当今，无人驾驶汽车在限制场景中已经展示出广泛的应用前景，如园区的物流配送、矿区的自动运载、固定路线的垃圾清除等. 在无人驾驶的大规模应用之前，急需解决的挑战是无人驾驶的安全性. 全球各国已经充分意识到了无人驾驶安全的重要性，不仅发布了多角度的无人驾驶安全技术标准，也出台了相关政策用以规范无人驾驶车辆的安全管理. 黑盒验证是提高无人驾驶系统安全性的关键解决途径. 黑盒验证是指无人驾驶的软硬件研发完成之后，对其系统进行测试确认，最大程度保证其系统安全性. 黑盒验证可以使用硬件在环测试，也可以使用软件模拟硬件进行仿真测试. 仿真测试不但能高效地发现系统的安全性问题，也能极大地节约研发成本. 复旦大学的杨珉教授团队在无人驾驶的安全性方面做了深入探索，并对仿真模糊测试技术进行了回顾与展望.

显然，仿真测试的有效性直接由虚拟场景配置的质量决定，即测试人员能否设计出易导致无人驾驶安全事故的虚拟场景. 设计事故场景绝非易事，究其原因是因为虚拟场景中包含着种类丰富的待配置要素，如天气环境、道路地图和交通车流等，这些要素的排列组合将构成难以估量的场景搜索空间. 为有效应对该难题，前沿的学术工作正尝试将传统的模糊测试技术与仿真测试相结合，构成面向无人驾驶系统的仿真模糊测试. 该技术的基本原理如下：给定数量有限的初始场景配置，通过类模糊测试的变异操作来自动调整种子场景中的可配置要素（如将天气参数由晴天变更为雨天），以此源源不断地生成新的更易导致事故的场景配置. 基于上述原理，仿真模糊测试技术即可自动化地探索庞大的场景搜索空间，并从中挖掘出易导致无人车事故的驾驶场景.

仿真模糊测试工作已在无人驾驶系统的安全测评中初见成效，但面向该技术的研究仍在起步阶段，相关的研究成果还无法系统性地缓解无人驾驶系统的功能安全问题. 在此背景下，杨珉教授团队撰写的论文“面向无人驾驶系统的仿真模糊测试：现状、挑战与展望”一文首先梳理了仿真模糊测试的基本架构以及研究现状，随后总结了已有工作的不足与面临的挑战，并最终提出了针对性的优化方案. 为验证这些优化方案的有效性和先进性，该文进一步将其用于主流开源无人驾驶系统 Apollo 和 Autoware 的安全评测中. 结果显示，这些方案可以极大地提升现有仿真模糊测试技术的事故挖掘与分析能力. 在此基础上，该文进一步展望了该领域中可能的研究方向，为后续工作提供指导性建议.

面向无人驾驶系统的仿真模糊测试是一种极具前途的安全保障技术. 通过对该技术的回顾与展望，将会给从事无人驾驶安全的研究人员提供新视角. 我相信，仿真模糊测试不会是无人驾驶安全性保障的唯一技术，希望本文能够启发广大科研人员，进一步对无人驾驶的安全性进行深入与持久的研究与探索，以发现更加有效的无人系统的安全性保障技术. 通过安全性技术的创新与无人驾驶产业的迭代，无人驾驶汽车大规模落地也许就在不久的将来.

评述专家：

蒲戈光，教授，上海工业控制安全创新科技有限公司总经理. 主要研究方向为可信软件与人工智能安全.

亮点论文：

戴嘉润，李忠睿，张婉琪，张源，杨珉. 面向无人驾驶系统的仿真模糊测试：现状、挑战与展望 [J]. 计算机研究与发展，2023，60(7)：1433−1447. DOI: 10.7544/issn1000-1239.202330156