QAI4ASE: 汽车软件工程中的量子人工智能

米尔科·德·文森西斯
意大利巴里大学计算机科学系
mirko.devincentiis@uniba.it

亚历山德罗 Pagano
意大利巴里大学经济与金融系
alessandro.pagano@uniba.it

法比奥·卡萨诺
意大利巴里大学计算机科学系
fabio.cassano1@uniba.it

安东尼奥 Piccinno
意大利巴里大学计算机科学系
antonio.piccinno@uniba.it

摘要

如今，汽车开发生命周期的规模和复杂性增加了网络攻击的可能性。在这种情况下，团队开发人员在管理网络安全、风险评估和软件应用程序开发的所有阶段(概念阶段、产品开发、网络安全验证、生产、操作和维护)中发挥主要作用。目前，由于缺乏所需的技能和知识，只有通用标准，难以实施。因此，本文提出了一种基于量子人工智能的视觉模型，支持开发人员在汽车开发生命周期中集成具体设计方法的决策。组织需要开发符合新汽车标准的汽车部件的开发流程。我们建议在 Quan- tum 人工智能算法上使用现有的数据源(例如，现有的分类法)来建议最佳的方法，或者正确的步骤，按照时间来实现用户解决方案。

CCS 的概念

• **软件及其工程→软件原型;**•计**算方法→人工智能;●硬件→**量**子计**算。

关键字

软件工程，人工智能，量子计算

ACM 参考格式:

米尔科·德文森蒂斯，法比奥·卡萨诺，亚历山德罗·帕加诺和安东尼奥·皮钦诺。2022. QAI4ASE: 汽车软件工程中的量子人工智能。第 *一届软件工程量子编程国际研讨会论文集(QP4SE ' 22)， 2022 年 12 月 18 日， 新 加 坡， 新 加 坡* 。 ACM， 纽 约， 美 国， 3 页 。 https://doi.org/10.1145/3549036.3562059

允许免费制作本作品的全部或部分数字或硬拷贝供个人或课堂使用，前提是副本不是为了盈利或商业利益而制作或分发的，并且副本在第一页上带有本通知和完整的引用。本作品组件的版权归 ACM 以外的其他人所有，必须得到尊重。允许有信用的摘要。以其他方式复制或重新发布，在服务器上发布或重新分发到列表，需要事先获得特定许可和/或付费。从 permissions@acm.org 请求权限。

QP4SE 22, 2022 年 11 月 18 日，新加坡，新加坡

& # 169;2022 年计算机协会。Acm isbn 978-1-4503-9458-1/22/11

https://doi.org/10.1145/3549036.3562059

1 介绍

由于现代计算机的日益强大，研究人员可以将人工智能(AI)方法应用于各种各样的应用。人工智能是一个广泛的术语，涵盖了许多先进的统计技术，可以应用于数据源来解决特定问题。通常，汽车领域的人工智能算法用于检测利用软件或标准协议漏洞的攻击(例如，不提供身份验证和加密机制的控制器局域网)[12,17]。然而，尽管这些系统是足够的，但在开发过程开始时往往需要用户的操作[20]。解决方案可能是采用风险评估，以确定关键组件并引入安全措施。同时，汽车标准强制组织在其开发过程中引入网络安全，这可能需要时间和经验[9]。在目前应用人工智能最成功的领域中，我们可以列举:计算机视觉，其中图像用于训练模型以识别特定模式，生物学用于发现特定的癌症模式或支持临床医生的决策，以及许多其他领域，如经济，教育[19]等。人工智能的新视野使量子计算成为近十年的突破性技术之一[10]。 量子计算(QC)最近出现强劲，加速了机器学习(ML)计算，并为现有方法提供了替代表示[16]。对于经典计算机在人的一生中无法解决的问题，基于 qc 的解决方案可以在合理的时间内获得[15]。另一方面，我们相信人的方面和人与这种复杂系统的相互作用不应该是次要的。例如，在汽车领域[5]，风险检测应该是实时的，量子人工智能不仅可以帮助识别攻击，还可以向驾驶员建议正确的决策，以避免灾难。考虑到这些需求，本研究旨在通过称为 QAI4ASE(汽车软件工程量子人工智能)的视觉模型，为汽车开发生命周期中的所有团队开发人员 (最终用户) 提供支持。

在本文中，我们提供了一个示例场景来解释汽车软件工程和量子人工智能如何协同工作，以支持组织开发符合标准的流程(QAI4ASE):量子机器学习(QML)和传统数据挖掘算法可以成功地帮助组织实现这一目标。本文的结构如下: 第二节

介绍了量子的相关工作，以及人工智能如何与人机交互;第 3 节介绍了关于汽车标准和我们的视觉模型——汽车软件工程量子人工智能模型(QAI4ASE)的描述。最后，第四部分得出结论。

2 相关工作

现代车辆通常采用最新的技术部件。对于这些车辆，需要超国家机构制定精确的规则，并对技术人员和维修技术人员进行广泛的培训[13,14]。特别是，现代车辆在安全开发过程中受到不同标准的约束。2021 年 8 月，国际标准化组织(ISO)发布了 ISO/SAE 21434《道路车辆——网络安全工程》。[18]。该文件解决了道路车辆电气和电子(E/E)系统工程中的网络安全观点。Dobaj 等人[9]提出了一个考虑 ISO/SAE 21434[18]的生命周期模型。为了提高开发过程的质量，汽车 SPICE (AS-PICE)[22]成为汽车组织的强制性标准。对于未来的自动驾驶汽车来说，考虑到交换信息的私密性也很重要。例如，Baldassarre 等人。[2]提出了一种基于隐私知识的方法来支持软件开发中的决策。然而，开发一个必须考虑到这两个标准的解决方案需要组织和程序员为优化付出很大的努力[3,6]。此外，它可能需要大量的计算能力和时间来测试该过程是否符合标准。

QAI 可能是克服传统 AI 模型的计算限制的一个很好的解决方案，并为开发过程中固有的决策提供支持。在[11]中，作者将人工智能与软件工程过程相结合。算法的主要类型是经典机器学习算法的量子实现，如支持向量机[4]或 k 近邻模型，以及经典深度学习算法，如量子神经网络[8,10]。相反，Martín-Guerrero 和 Lamata[16]讨论了量子强化学习(RL)。

3 QAI4ASE: 视觉模型

我们在这里提出的方法需要尽可能地一般化。在下一节中，我们将提出一个案例研究场景，其中最终用户设备和量子人工智能可以合并，以支持用户开发汽车解决方案[7]。即将发布的 ISO/SAE 21434 标准为开发现代车辆的安全解决方案提供了指导方针。考虑到这个标准，组织可以检查软件解决方案是否符合 ISO/SAE 21434。本标准提供了不同的条款。特别是，应该考虑到发展进程。产品开发阶段定义网络安全规范，实施并验证特定于项目或组件的网络安全需求[18]。

现在让我们考虑一个组织为汽车领域开发安全开发流程的需求。ISO/SAE 21434 的普遍问题是它没有提供具体的设计

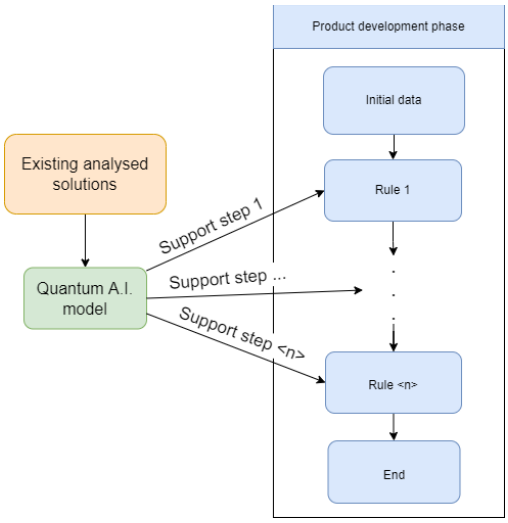

图 1: 支持用户开发的 QAI4ASE 模型

方法和在每个阶段可能难以理解[9]。出于这个原因，让我们假设一个组织有规则来检查开发过程是否符合 ISO/SAE 21434。这些规则包含了有关车辆软件安全开发的安全概念。Sommer 等人。[21]提出了一种可用于车辆开发过程的分类法。要做到这一点，开发人员应该控制生产过程是否遵循这些规则。然而，这项任务需要时间，也是网络安全任务中的一项优势技能。此外，Sommer 等人提出的分类方法。[21]由于分类数量多(如作者所述)，需要付出很大的努力。

考虑到刚才描述的例子，量子人工智能可能会支持组织改进汽车领域的安全解决方案。

通过在数据集上训练量子人工智能模型，例如在给定时间为组织创建的所有规则生成的数据集，可以指导用户一步一步地检查解决方案是否符合 ISO/SAE 21434。图 1 显示了视觉模型 QAI4ASE。理想情况下，我们可以将 ISO/SAE 21434 划分为必须检查的多个规则。量子人工智能模型从包含之前构建的解决方案的所有步骤的数据集中进行训练，建议在特定时刻哪一步最适合开发人员。

提出的想法可以对其他标准(如 Automotive SPICE)进行多个扩展。

这里要解决的另一个方面是，在构建之后，量子人工智能如何与开发人员进行交互，以支持他/她开发解决方案。因此，我们可以考虑多种方法来建议用户下一步采取的最佳行动，但在这里我们只想描述一些适合这种情况的想法:

- 图形通知:这是现在在设备和软件上非常常见的东西。该工具可以在屏幕的固定部分显示带有简短描述的通知。例如，在[1]中，作者提供了一个可视化工具

- 这支持开发人员在所有软件开发阶段集成隐私和安全需求的决策。建议叠加:如果这个过程符合汽车标准，量子人工智能模型可能会向开发人员建议正确的规则或分类，就像现代电话键盘在用户输入文本时提示新单词一样。

最后要考虑的事项与 QAI 模型的训练以及如何从开发人员的操作中获得反馈有关。即使我们没有讨论任何特定的量子人工智能模型，也可以采用一些方法来达到建议的目标。例如，我们可以考虑一个多分类方法，其中每个 1，…， *1* 步是模型的一个输出类，可以对之前用户所做的所有类似步骤–生行训练。其他方法可能与无监督模型相关，其中分析解决方案构建过程中每个步骤的特征，以查看用户(在给定步骤上)与其他建议的解决方案的接近程度。

4 结论

汽车开发生命周期的规模和复杂性增加了网络攻击的可能性。目前只有通用标准，由于缺乏所需的技能和知识，难以实施。然而，我们相信这个困难是可以克服的，采用一种我们称之为QAI4ASE 的新方法。在这里，我们讨论了如何将汽车软件工程和量子人工智能结合使用，以支持开发人员创建符合 ISO/SAE 21434 标准的汽车开发流程。特别地，我们提出了一个远景模型(QAI4ASE)作为起点，它可用于处理来自现有分类法的数据，并支持开发人员开发安全的开发过程。通过这种方式，量子人工智能不会取代开发人员的角色，而是作为一个积极的助手来实现开发目标。

尽管本文描述了理论方法，但我们相信我们的工作可以在工程领域和网络安全方面有多种应用。

一个可能的限制是量子解决方案限制了软件开发。未来的工作包括从汽车标准中检索技术，并确定量子人工智能技术，以便能够开发所提出的视觉模型。目标将是量子人工智能技术识别，适用于处理汽车系统中有用的开发解决方案。一旦系统被开发出来，它就可以与汽车公司合作进行测试，目的是在真实的环境中实现它。在未来的情况下，一个可能的限制是，汽车公司不希望披露他们的开发过程，即使他们将网络安全技术纳入软件编码。

致谢

本研究部分由以下项目资助: SIMPLe(室内种植综合自动化系统)由普利亚地区资助;PSR 2014-2020 普利亚- Articolo 35 del regamento (VE) n. 1305/2013 Misura 16 Cooperazione - Sottomisura 16.2 - Sostegno a progetti pilota e allo siluppo di nuovi prodotti，实践，工艺技术;CUP:B89J20000100009。

参考文献

[1] Maria Teresa Baldassarre, Vita Santa Barletta, Danilo Caivano 和 Antonio Piccinno。2020.在面向隐私的软件开发中支持决策的可视化工具。*高级视觉界面国际会议论文集*。1 - 5。

[2] Maria Teresa Baldassarre, Vita Santa Barletta, Danilo Caivano, Antonio Piccinno 和 Michele Scalera。2021.支持软件开发决策的隐私知识库。在 *IFIP 人机交互会议上*。施普林格,147 - 157。

[3] Maria Teresa Baldassarre, Vita Santa Barletta, Danilo Caivano 和 Michele Scalera。2019.面向隐私的软件开发。信 *息和通信技术质量国际会议*。施普林格,18 32。

[4] Vita Santa Barletta, Danilo Caivano, Mirko De vincitis, Alessio Magrì 和 Antonio Piccinno。2022.物联网安全检测的量子优化。环 *境智能-软件与应用-第十三届环境智能国际研讨会*。接受。

[5] Vita Santa Barletta, Danilo Caivano, Antonella Nannavecchia 和 Michele Scalera。2020.车载通信网络入侵检测的 Kohonen SOM 体系结构。*应用科学 10,15(2020)*。

[6] 贝维拉夸、卡萨诺、米尼诺和亚卡。2015. 基于多目标进化算法的前馈神经网络拓扑优化:基于生物医学数据集的比较研究。意 *大利人工生命和进化计算研讨会*。Springer, Cham, 53-64 页。

[7] 达尼洛·卡瓦诺、法比奥·卡萨诺、罗莎·兰齐罗蒂和安东尼奥·皮奇诺。2018.面向智能设备评估的物联网模型。2018 *高级视觉界面国际会议论文集*。1 - 3。

[8] 法比奥·卡萨诺、安东尼奥·卡萨莱、保拉·里贾纳、卢阿纳·斯帕达菲娜和佩塔尔·塞库利克。2019.改进空气质量指数预测的递归神经网络方法。环 *境智能国际研讨会*。施普林格，查姆，36-44。

[9] rgen Dobaj, Georg Macher, Damjan Ekert, Andreas Riel 和 Richard Messnarz。2021.迈向安全驱动的汽车开发生命周期。*软件杂志: 演化与过程(2021)，e2407*。

[10] 大卫·佩尔·加西亚、胡安·克鲁兹-贝尼托和弗朗西斯科·何塞;Garc& # 237; a-Pe& # 241;阿尔瓦诺。2022.系统文献综述: 量子机器学习及其应用。*中国农业大学学报(自然科学版):2201.04093(2022)*。

[11] Rajesh H Kulkarni 和 Palacholla Padmanabham。2017.软件开发过程中人工智能活动的集成和集成有效性的度量。*软件学报，2017(1)，18-26*。

[12] Siti-Farhana Lokman, Abu Talib Othman 和 Muhammad-Husaini Abu-bakar。2019.汽车控制器局域网(CAN)总线系统的入侵检测系统综述。*无线通信与网络学报，2019,1(2019)，1 - 17*。

[13] 阿戈斯蒂诺·马伦戈，亚历山德罗·帕加诺和露西娅·拉迪萨。2017.面向企业培训的移动增强现实原型。*欧洲电子学习会议论文集，ECEL 2010- 10 月，362 - 366*。

[14] 阿戈斯蒂诺·马伦戈，亚历山德罗·帕加诺和露西娅·拉迪萨。2018. 面向企业培训的移动增强现实原型: 一个新的视角。*2018 年第 14 届移动学习国际会议论文集，ML 2018, 129 - 135*。

[15] 乔斯# 233; 马特·n·格雷罗和卢卡斯·拉马塔。2020.量子机器学习。2020(10)。

[16] 乔斯# 233;D. Martín-Guerrero 和 Lucas Lamata。2022.量子机器学习: 一个教程。*神经计算机学报，2012,33(4):457-461* 。*科学 pii* / 文章 / / S0925231221011000 https://www.sciencedirect.com/

[17] 查理·米勒和克里斯·瓦拉塞克。2015.远程利用未改装的乘用车。*美国黑帽 2015,s91(2015)*。

[18] ISO 国际标准化组织。2021.ISO/SAE DIS 21434 道路车辆-网络安全工程。

[19] 亚历山德罗·帕加诺和阿戈斯蒂诺·马伦戈。2021.基于自适应学习策略的训练时间优化。*信息、计算与技术创新与智能国际会议，3ICT 2021, 563 - 567。https://doi.org/10.1109/3ICT53449.2021.9582096*

[20] Christian Plappert, Daniel Zelle, Henry Gadacz, Roland Rieke, Dirk Scheuermann 和 Christoph Krauß2021.面向汽车领域网络安全工程的攻击面评估。2021 *年第 29 届并行，分布式和基于网络的处理(PDP)国际会议*。IEEE 266 - 275。

[21] 弗洛里安·索默，Jürgen Dü rwang 和赖纳·克里斯滕。2019.汽车安全攻击的调查与分类。*情报 10,4(2019)，148*。

[22] VDA QMC 第 13 工作组/汽车 SIG。2015.汽车 SPICE 过程评估/参考模型。https://www.automotivespice.com/fileadmin/ 软 件 下 载 / Automotive_SPICE_PAM_30.pdf。