QAI4ASE: Quantum Artificial Intelligence for Automotive Software Engineering

Mirko De Vincentiis
Department of Computer Science, University of Bari
Bari, Italy
mirko.devincentiis@uniba.it

Fabio Cassano
Department of Computer Science, University of Bari
Bari, Italy
fabio.cassano1@uniba.it

Alessandro Pagano
Department of Economics and Finance, University of Bari
Bari, Italy
alessandro.pagano@uniba.it

Antonio Piccinno
Department of Computer Science, University of Bari
Bari, Italy
antonio.piccinno@uniba.it

ABSTRACT

Nowadays, the size and complexity of the automotive development life-cycle increase the possibility of cyber-attacks. In this context, team developers play a primary role in managing cyber security, risk assessment, and all phases of software application development (concept phases, product development, cyber security validation, production, operations, and maintenance). Currently, only generic standards exist and they are difficult to put into operation due to the lack of the required skills and knowledge. Therefore, this paper presents a vision model based on Quantum Artificial Intelligence that supports developers' decisions to integrate concrete design methods in the automotive development life-cycle. Organizations need to develop their process for developing vehicle components that comply with the new automotive standards. We suggest the usage of existing data sources (e.g., existing taxonomies) on Quantum Artificial Intelligence algorithms to suggest the best way, or the correct steps, to follow time by time to achieve user solutions.

CCS CONCEPTS

• **Software and its engineering** → **Software prototyping**; • **Computing methodologies** → **Artificial intelligence**; • **Hardware** → *Quantum computation.*

KEYWORDS

Software Engineering, Artificial Intelligence, Quantum Computing

ACM Reference Format:
Mirko De Vincentiis, Fabio Cassano, Alessandro Pagano, and Antonio Piccinno. 2022. QAI4ASE: Quantum Artificial Intelligence for Automotive Software Engineering. In *Proceedings of the 1st International Workshop on Quantum Programming for Software Engineering (QP4SE '22), November 18, 2022, Singapore, Singapore*. ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3549036.3562059

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
QP4SE '22, November 18, 2022, Singapore, Singapore
© 2022 Association for Computing Machinery.
ACM ISBN 978-1-4503-9458-1/22/11…$15.00
https://doi.org/10.1145/3549036.3562059

1 INTRODUCTION

Thanks to the increasing power of modern computers, researchers can apply Artificial Intelligence (AI) methods to a wide variety of applications. AI is a broad term that covers many advanced statistical techniques, that can be applied to data sources to solve specific problems. Usually, AI algorithms in the automotive field are used to detect attacks that exploit vulnerabilities in software or standard protocols (e.g. a Controller Area Network that does not provide authentication and encryption mechanisms) [12, 17]. However, although these systems are adequate, users actions are often needed as early as the development process starts [20]. A solution could be the adoption of a risk assessment, to identify critical components and introduce security measures. At the same time, the automotive standards enforce the organization to introduce cyber security in their development process which could require time and experience [9]. Among the most successful fields where AI is currently applied, we can cite: computer vision, where images are used to train models to recognise specific patterns, Biology to find specific cancer's pattern or to support clinicians in their decisions and many others such as economy, education [19] etc.. New horizons in Artificial Intelligence enable quantum computing as one of the breakthrough technology of the latest decade [10]. Quantum Computing (QC) emerged strongly lately, speeding up Machine Learning (ML) calculations and providing alternative representations to existing approaches [16]. QC-based solutions can be obtained within a reasonable amount of time for problems that would be impossible to solve by a classical computer in a human lifetime [15]. On the other hand, we believe that human aspects and human interaction with such complex systems must not be secondary. For example, in the automotive field [5], the risk detection should be in real-time and Quantum AI will help not only to identify attacks but also to suggest to the driver the correct decisions to avoid a disaster. Considering these needs, this research aims to support all team developers (end users) in the automotive development life-cycle thanks to the vision model called QAI4ASE (Quantum Artificial Intelligence for Automotive Software engineering).

In this paper we present an example scenario to explain how Automotive Software Engineering and Quantum AI can work together to support organizations in developing processes compliant with standards (QAI4ASE): quantum machine learning (QML) and traditional data mining algorithms can successfully help organizations to reach this goal. The paper is structured as follows: Section 2 introduces related works about quantum and how AI meets Human-Computer Interaction; Section 3 presents a description regarding the automotive standards and our vision model Quantum AI model for Automotive Software Engineering (QAI4ASE). Lastly, Section 4 draws the conclusions.

2 RELATED WORK

Modern vehicles often implement the latest components of technology. For these vehicles, precise rules issued by supranational bodies are necessary as well as extensive training for technicians and maintenance technicians [13, 14]. In particular, modern vehicles are subject to different standards regarding the secure development process. In August 2021, International Organization for Standardization (ISO) published the ISO/SAE 21434 "Road vehicles - Cyber security engineering" [18]. The document addresses the cyber security perspective in engineering of electrical and electronic (E/E) systems within road vehicles. Dobaj et al [9] proposed a life-cycle model taking into account the ISO/SAE 21434 [18]. To improve the quality of the development process, Automotive SPICE (ASPICE) [22] became mandatory for the automotive organizations. For future autonomous vehicles, it is also important to take into consideration the privacy of the exchanged pieces of information. For example, Baldassarre et al. [2] proposed a Privacy Knowledge Based to support the decision in software development. However, developing a solution that must take into account these two standards requires high effort for the organization and the programmer for the optimization [3, 6]. Moreover, it could take a lot of computational power and time to test if the process is compliant with the standard.

QAI could be an excellent solution to overcome the computational limitations of traditional AI models and provide support for decisions inherent in the development process. In [11], the authors integrated Artificial Intelligence with the software engineering process. The main types of algorithms are quantum implementations of classical machine learning algorithms, such as support-vector machines [4] or the k-nearest neighbour model, and classical deep learning algorithms, like quantum neural networks [8, 10]. Instead, Martín-Guerrero and Lamata [16] discussed quantum Reinforcement Learning (RL).

3 QAI4ASE: VISION MODEL

The approach we present here needs to be considered as general as possible. In the following section, we are going to propose a case study scenario, where End user devices and Quantum AI can merge to support the user in the development of automotive solutions [7]. The upcoming ISO/SAE 21434 standard provides the guidelines to develop security solutions for modern vehicles. Considering this standard, an organization could check if the software solutions comply with ISO/SAE 21434. This standard provides different clauses. In particular, the development process should be taken into consideration. The Product development phases defines the cyber security specification, and implement and verifies cyber security requirements specific to an item or component [18].

Let's now consider an organization's need to develop a secure development process for the automotive domain. The general problem of the ISO/SAE 21434 is that it does not provide concrete design

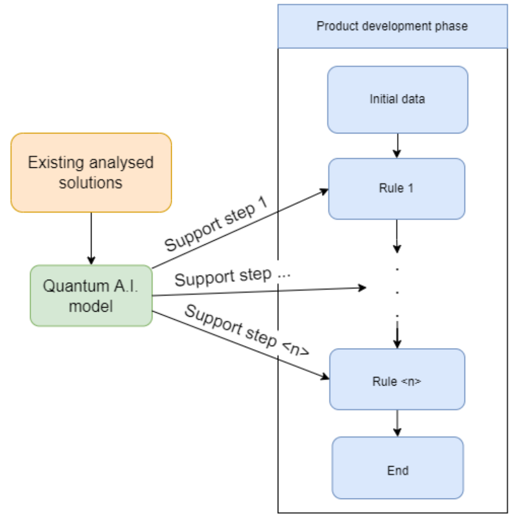

Figure 1: QAI4ASE model to support user development

methods and could be difficult to understand at each stage [9]. For this reason, let's suppose that an organization has rules to check if the development process is compliant with the ISO/SAE 21434. These rules enclose safety concepts regarding the secure development of software in vehicles. Sommer et al. [21] proposed a taxonomy that could be used in the vehicle development process. To do this, a developer should control if the production process follows these rules. However, this task requires time and is also an advantageous skill in cyber security tasks. Moreover, the taxonomy proposed by Sommer et al. [21] required high effort caused by the high number of categories (as reported by the authors).

Considering the example just described, Quantum AI might come to support the organization to improve security solutions in the automotive field.

By training the Quantum AI model over a dataset such as the one generated from all the rules that have been created at a given time for the organization, it is possible to guide the user step by step to check if the solution is compliant with the ISO/SAE 21434. Figure 1 shows the vision model QAI4ASE. Ideally, we can divide the ISO/SAE 21434 into multiple rules that must be checked. A Quantum AI model, trained from a dataset containing all the steps of the previously built solutions, suggests which step would fit the most for the developer in that specific moment.

The idea proposed could have multiple extensions to the other standard like Automotive SPICE.

Another aspect to address here is how, after being built, Quantum AI could interact with the developer to support him/her with the development of the solution. Thus we can think about multiple ways how to suggest to users the best next step to take, but here we want just to describe a couple of ideas that would fit the case:

- Graphical notification: this is something very common to find nowadays on devices and software. The tool could show up notification with a brief description on a fixed part of the screen. For example, in [1] authors provide a visual tool that supports developers' decisions to integrate privacy and security requirements in all software development phases.

- Suggestion overlay: the Quantum AI model might suggest to the developer the right rules or taxonomy if the process violates the automotive standards as a modern phone keyboard does suggest new words when the user is typing the text.

The last considerations are related to the training of the QAI model and how to get feedback from the developer's actions. Even if we did not discuss any specific Quantum AI model, some approaches might be pursued to reach the suggested goal. For example, we can consider a multi-classification approach where each of the $1, \ldots, n-1$ steps are an output class of the model, and the training could be performed on all the similar steps made by previous users. Other approaches could be related to unsupervised models, where features from each step of the solution-building process, are analysed to see how close the user is (on a given step) to other proposed solutions.

4 CONCLUSIONS

The size and complexity of the automotive development life-cycle increase the possibility of cyber-attacks. Currently only generic standards exist and they are difficult to put into operation due to the lack of the required skills and knowledge. However we believe that this difficulty could be overcome, adopting a new approach that we called QAI4ASE. Here we discussed how Automotive Software Engineering and Quantum AI could be used together to support the developer to create a vehicle development process compliant with the ISO/SAE 21434. In particular, we present a vision model (QAI4ASE) as a starting point and could be used to handle data from existing taxonomy and support developers to develop a secure development process. In this way, Quantum AI does not replace the developer's role but acts as an active helper to reach the development goal.

Despite the theoretical approach described in the presented here, we believe that our work could have multiple application in the engineering field and cyber security.

One possible limitation is that quantum solutions are limiting in software development. Future works involves retrieving techniques from the automotive standards and identifying Quantum AI techniques to be able to develop the vision model presented. The aim will be the Quantum AI techniques identification suitable for processing useful development solutions in automotive systems. Once the system has been developed, it can be tested in collaboration with automotive companies with the aim of implementing it in a real context. In this future scenario, one possible limitation is that automotive companies do not want to disclose their development processes and even if they put cyber security techniques into software coding.

ACKNOWLEDGEMENTS

This study has been partially funded by the following project: SIMPLe (Integrated AutoMatized Systems For Indoor coLtivation) funded by Regione Puglia "PSR 2014-2020 Puglia — Articolo 35 del Regolamento (VE) n. 1305/2013 Misura 16 Cooperazione — Sottomisura 16.2 - "Sostegno a progetti pilota e allo sviluppo di nuovi prodotti, pratiche, processi e tecnologie", CUP:B89J20000100009.

REFERENCES

[1] Maria Teresa Baldassarre, Vita Santa Barletta, Danilo Caivano, and Antonio Piccinno. 2020. A visual tool for supporting decision-making in privacy oriented software development. In *Proceedings of the International Conference on Advanced Visual Interfaces*. 1–5.

[2] Maria Teresa Baldassarre, Vita Santa Barletta, Danilo Caivano, Antonio Piccinno, and Michele Scalera. 2021. Privacy Knowledge Base for Supporting Decision-Making in Software Development. In *IFIP Conference on Human-Computer Interaction*. Springer, 147–157.

[3] Maria Teresa Baldassarre, Vita Santa Barletta, Danilo Caivano, and Michele Scalera. 2019. Privacy oriented software development. In *International Conference on the Quality of Information and Communications Technology*. Springer, 18–32.

[4] Vita Santa Barletta, Danilo Caivano, Mirko De Vincentiis, Alessio Magrì, and Antonio Piccinno. 2022. Quantum Optimization for IoT Security Detection. In *Ambient Intelligence – Software and Applications - 13th International Symposium on Ambient Intelligence*. Accepted.

[5] Vita Santa Barletta, Danilo Caivano, Antonella Nannavecchia, and Michele Scalera. 2020. A Kohonen SOM Architecture for Intrusion Detection on In-Vehicle Communication Networks. *Applied Sciences* 10, 15 (2020).

[6] Vitoantonio Bevilacqua, Fabio Cassano, Ernesto Mininno, and Giovanni Iacca. 2015. Optimizing feed-forward neural network topology by multi-objective evolutionary algorithms: a comparative study on biomedical datasets. In *Italian Workshop on Artificial Life and Evolutionary Computation*. Springer, Cham, 53–64.

[7] Danilo Caivano, Fabio Cassano, Rosa Lanzilotti, and Antonio Piccinno. 2018. Towards an IoT model for the assessment of smart devices. In *Proceedings of the 2018 international conference on advanced visual interfaces*. 1–3.

[8] Fabio Cassano, Antonio Casale, Paola Regina, Luana Spadafina, and Petar Sekulic. 2019. A Recurrent Neural Network Approach to Improve the Air Quality Index Prediction. In *International Symposium on Ambient Intelligence*. Springer, Cham, 36–44.

[9] Jürgen Dobaj, Georg Macher, Damjan Ekert, Andreas Riel, and Richard Messnarz. 2021. Towards a security-driven automotive development lifecycle. *Journal of Software: Evolution and Process* (2021), e2407.

[10] David Peral García, Juan Cruz-Benito, and Francisco José García-Peñalvo. 2022. Systematic Literature Review: Quantum Machine Learning and its applications. *arXiv preprint arXiv:2201.04093* (2022).

[11] Rajesh H Kulkarni and Palacholla Padmanabham. 2017. Integration of artificial intelligence activities in software development processes and measuring effectiveness of integration. *Iet Software* 11, 1 (2017), 18–26.

[12] Siti-Farhana Lokman, Abu Talib Othman, and Muhammad-Husaini Abu-Bakar. 2019. Intrusion detection system for automotive Controller Area Network (CAN) bus system: a review. *EURASIP Journal on Wireless Communications and Networking* 2019, 1 (2019), 1–17.

[13] Agostino Marengo, Alessandro Pagano, and Lucia Ladisa. 2017. Towards a mobile augmented reality prototype for corporate training. *Proceedings of the European Conference on e-Learning, ECEL* 2010-October, 362 – 366.

[14] Agostino Marengo, Alessandro Pagano, and Lucia Ladisa. 2018. Towards a mobile augmented reality prototype for corporate training: A new perspective. *Proceedings of the 14th International Conference on Mobile Learning 2018, ML 2018*, 129 – 135.

[15] José Martín-Guerrero and Lucas Lamata. 2020. Quantum Machine Learning. (10 2020).

[16] José D. Martín-Guerrero and Lucas Lamata. 2022. Quantum Machine Learning: A tutorial. *Neurocomputing* 470 (2022), 457–461. https://www.sciencedirect.com/science/article/pii/S0925231221011000

[17] Charlie Miller and Chris Valasek. 2015. Remote exploitation of an unaltered passenger vehicle. *Black Hat USA* 2015, S 91 (2015).

[18] ISO International Standardization Organisation. 2021. ISO/SAE DIS 21434 Road vehicles—cybersecurity engineering.

[19] Alessandro Pagano and Agostino Marengo. 2021. Training Time Optimization through Adaptive Learning Strategy. *2021 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies, 3ICT 2021*, 563 – 567. https://doi.org/10.1109/3ICT53449.2021.9582096

[20] Christian Plappert, Daniel Zelle, Henry Gadacz, Roland Rieke, Dirk Scheuermann, and Christoph Krauß. 2021. Attack surface assessment for cybersecurity engineering in the automotive domain. In *2021 29th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP)*. IEEE, 266–275.

[21] Florian Sommer, Jürgen Dürrwang, and Reiner Kriesten. 2019. Survey and classification of automotive security attacks. *Information* 10, 4 (2019), 148.

[22] VDA QMC Working Group 13 / Automotive SIG. 2015. Automotive SPICE Process Assessment / Reference Model. https://www.automotivespice.com/fileadmin/software-download/Automotive_SPICE_PAM_30.pdf.