Predictive Simulation within the Process of Building Trust

Emilia Cioroaica
Safety Engineering
Fraunhofer IESE
Kaiserslautern, Germany
emilia.cioroaica@iese.fraunhofer.de

Barbora Buhnova
Faculty of Informatics
Masaryk University
Brno, Czech Republic
buhnova@mail.muni.cz

Thomas Kuhn
Embedded Systems
Fraunhofer IESE
Kaiserslautern, Germany
thomas.kuhn@iese.fraunhofer.de

***Abstract*—The emerging dynamic architectures of autonomous digital ecosystems raise new challenges in the process of assuring trust and safety. In particular, the admission of software smart agents into autonomous dynamic ecosystems will become a significant future topic. In this work we propose the concept of predictive simulation, which elevates from the concept of virtual Hardware-in-the-Loop (vHiL) testbed, to support rapid runtime evaluation of software smart agents in autonomous digital ecosystems. Based on this testbed, we introduce a novel strategy for building trust in software components that enter an ecosystem as black boxes without executing their behavior which can be potentially malicious, but by executing corresponding digital twins which are abstract models fed with real-time data.**

***Index Terms*—Smart Ecosystems, Automotive, Virtual Evaluation, Building Trust, Malicious Behavior, Simulation, Predictive Simulation, Digital Twins**

I. Introduction

Emerging development within automotive dynamic ecosystems [1] is pushing forward the runtime delivery of software smart agents in safety critical domains [2]. Aiming at forming coalitions that support the achievement of high-level business goals that cannot be achieved otherwise, when becoming part of complex ecosystems, safety critical systems are endangered by possible malicious behavior introduced by actors that join the ecosystem with declared collaborative goals but act in competition. Such malicious behavior can be hidden in software smart agents delivered at runtime. As a consequence, safety-critical autonomous dynamic ecosystems need new means to assess the trustworthiness of new software components. In our opinion, the trust evaluation of software components delivered during runtime can be possible through deployment of new platforms that enable their testing at runtime as well.

By integrating emergent research results from Industry 4.0 and requirements from safety critical standards, in this paper, we present our approach for building trust based on runtime predictive evaluation of software smart agents' behavior. To this end, we propose the concept of Digital Twins (DT) of software smart agents, which are used during operation of the software smart agents to assess their runtime behavior. The evaluation results are then used to override detected malicious behavior before it takes effect and assure a trusted and safe operation of the vehicle.

II. Background

A. Motivating Scenario in the context of Autonomous Driving

Emerging POSIX-based automotive platforms [3] will support runtime dynamic deployment of automotive smart agents, enabling in this way creation of autonomous dynamic ecosystems. Such ecosystems will comprise a changing number of participants pursuing different goals and interacting with each other to achieve these goals in the best possible manner [4]. For example, a smart ecosystem could force vehicles entering a city to download software a smart agent that activates a speed limit of 30 km/h around school areas.

For vehicles, which are safety-critical systems, the process of integrating automation requires compliance with safety standards. Aiming at benefiting from deployment of innovative technology, in order to make the autonomous driving a reality, a wide range of legal considerations need to be addressed. In this regard, the recent Code of Practice [5] provides guidelines developing innovative technologies aimed to be deployed on automotive systems.

B. Our Approach

We base our approach for building trust on an uplift of the notion of Digital Twin (DT), introduced by NASA [6] as a realistic digital representation of a system used in lab-testing activities. The notion has transitioned in the Industry 4.0 [7] where it is representing the status of production devices for forecasting change impacts.

While the concept of DT is currently used only for simulation and testing of systems detached from object operation, we see great potential in the incorporation of the concept into an object's runtime operation. As a consequence, in our approach we are proposing the use of digital twins for evaluating behavior of software smart agents delivered as black boxes. Through the execution of the digital twins in a simulated environment, we can create safe conditions for detecting malicious behavior without endangering the real world system execution. By focusing the scope of the evaluation to either scheduling, function interaction or communication protocol between the intelligent software and other interacting entities within a vehicle, specialized and faster evidence of trust is achieved.

III. Summary of the Work

For enabling the process of trust evaluation in a software smart agent, we propose deployment of a *predictive simulation* platform within a vehicle. As introduces in [8] and depicted in Fig. 1, our method requires the delivery of DTs, which are specialized abstractions of a software smart agent. Used for evaluating specific aspects of a software behavior such as: synchronization, function interaction with other system components as well as the communication protocol, the DTs are specialized abstract models fed with real-time data. In a predictive simulation environment, the digital twins are executed (c.f. Fig. 1 Phase 1) in interaction with digital twins of inter-related components and a *trusted behavior signature* is delivered to a conformity monitoring component (c.f. Fig. 1, Phase 2). While receiving the trusted behavior signature from the predictive simulation, the conformity monitoring checks for the order, type and the number of events triggered by the execution of the software smart agent on a real-world processor, such as an Embedded Control Unit (ECU) within the vehicle. In case of major deviations, a redundant, simpler fail-over behavior can be triggered with the scope of bringing the system in a safe state [9].

A trusted execution of the digital twins in the simulated environment can be assured by a dedicated DSL (Domain Specific Language) which guides the specification of smart agent behavior in a way that complies with the requirements of the simulation platform and makes sure that the digital twin cannot detect it is under evaluation.

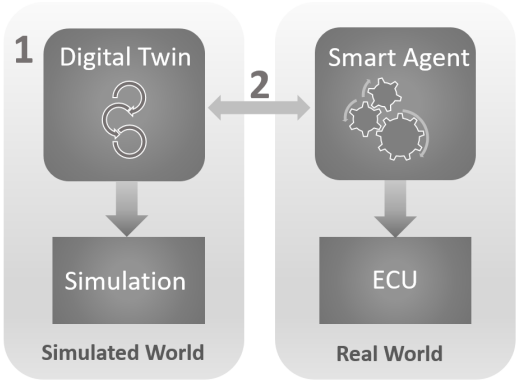

Fig. 1. The two phases of the runtime process of building trust

IV. Current and potential Industry Impact

Our approach emerged from analyzing new development trends in the automotive domain and emerging technological needs in assuring a trusted operation of autonomous vehicles endangered by malicious attacks. Our solution entails an uplift of existing practices for addressing emerging requirements of trusted autonomous driving and imposes the creation of dedicated abstraction of software smart agents which, when fed with real-time data become digital twins of the software smart agent. The predictive execution of the DTs in a simulated environment provides the evidence of trust used for checking the real-world execution. For providing a holistic view of the situation in which trust needs to be judged, dedicated software abstractions are executed in inter-relation with dedicated abstractions of the hardware resources and/or other interacting platforms that for automotive domain need to be ASIL (Automotive Safety Integrity Level) compliant.

Technological advancements towards fast transfer of data deployed within vehicles will be capable to support the deployment of the platform that enables the implementation of the runtime phase of our process of building trust. Concurrently, the emerging developments of 6G technology might enable deployment of the platform on the cloud, requiring regular information transfer to the system when the software smart agents run.

V. Discussion and Conclusion

The concept of runtime simulation platform presented in this paper is directed towards performing an evaluation of the trustworthiness of the software smart agents joining dynamic architectural ecosystems, without endangering the system by the potentially malicious behavior of the agents.

For enabling the fast execution of dedicated simulation models created towards specific scopes of the evaluation (functional interaction, synchronization and communication protocol) for safety critical domains, the creation of abstract models need to be performed in accordance with safety practices.

Acknowledgment

This work is co-funded from the European Union's Horizon 2020 research and innovation programme under grant agreement No 952702 (BIECO), and ERDF/ESF "CyberSecurity, CyberCrime and Critical Information Infrastructures Center of Excellence" (No. CZ.02.1.01/0.0/0.0/16_019/0000822).

References

[1] R. Capilla, E. Cioroaica, B. Buhnova, and J. Bosch, "On autonomous dynamic software ecosystems," *IEEE Transactions on Engineering Management*, pp. 1–15, 2021.

[2] techcrunch.com, "Tesla has activated its camera," Mar. 2021. [Online]. Available: https://techcrunch.com/2021/05/27/tesla-has-activated-its-in-car-camera-to-monitor-drivers-using-autopilot/

[3] "AUTOSAR," https://www.autosar.org/, [Online; accessed 03-September-2018].

[4] E. Cioroaica, A. Purohit, B. Buhnova, and D. Schneider, "Goals within trust-based digital ecosystems," in *2021 IEEE/ACM Joint 9th International Workshop on Software Engineering for Systems-of-Systems and 15th Workshop on Distributed Software Development, Software Ecosystems and Systems-of-Systems (SESoS/WDES)*. IEEE, 2021, pp. 1–7.

[5] "L3Pilot," https://l3pilot.eu, 2021, [Online; accessed 22-November-2021].

[6] M. Shafto, M. Conroy, R. Doyle, E. Glaessgen, C. Kemp, J. LeMoigne, and L. Wang, "Modeling, simulation, information technology & processing roadmap," *National Aeronautics and Space Administration*, 2012.

[7] R. Rosen, G. Von Wichert, G. Lo, and K. D. Bettenhausen, "About the importance of autonomy and digital twins for the future of manufacturing," *IFAC-PapersOnLine*, vol. 48, no. 3, pp. 567–572, 2015.

[8] E. Cioroaica, T. Kuhn, and B. Buhnova, "(do not) trust in ecosystems," in *2019 IEEE/ACM 41st International Conference on Software Engineering: New Ideas and Emerging Results (ICSE-NIER)*. IEEE, 2019, pp. 9–12.

[9] D. Seto, B. Krogh, L. Sha, and A. Chutinan, "The simplex architecture for safe online control system upgrades," in *Proceedings of the 1998 American Control Conference. ACC (IEEE Cat. No. 98CH36207)*, vol. 6. IEEE, 1998, pp. 3504–3508.