Virtual Evaluation of Dependability Attributes for Mission-Critical Cyber-Physical Systems

Adam Bachorek*, Benedikt Lüken-Winkels†, Iron Prando da Silva‡, Stefan Schwenk§, Markus Damm¶
and Pablo Oliveira Antonino‖
Fraunhofer IESE, Kaiserslautern, Germany
Email: {*adam.bachorek, †benedikt.lueken-winkels, ‡iron.prandodasilva, §stefan.schwenk, ¶markus.damm, ‖pablo.antonino}
@iese.fraunhofer.de

***Abstract*—Assuring dependability of complex mission-critical cyber-physical systems in various domains including automotive and agriculture is becoming an increasingly demanding challenge. This is due to the ongoing evolution of land vehicles and machinery such as tractors and implements from mainly electro-mechanical devices towards software-driven and interconnected processing units enabling highly automated applications like smart farming. In particular, the underlying communication infrastructure of the involved distributed subsystems is subject to high demands in view of functional but also quality aspects like security and safety. And, testing the countless component interactions against associated criteria is not feasible without sophisticated techniques and tooling support, which continuous engineering solutions tackle with experimental evidence based on virtual evaluation environments. While these facilitate advanced practices for handling system complexity, formal verification of specific system properties remains a complementary and effective part of modern product development.**

In this paper, we present a generic methodical concept which combines virtual experimentation with formal analysis to substantiate decisions regarding the design and implementation of dependable CPS. We validate our approach by means of a case study on a common evaluation problem with regard to weighing up competing dependability attributes in the context of resource-constraint communication. To this end, we instantiate a virtual testbed based on the established VCIP reference architecture and FERAL simulation framework and we conduct empirical trials using systematic fault-injection combined with analytical proofing in terms of a trade-off evaluation. Specifically, we generate different CAN data frame variants during back-to-back tests for assessing the impact of cyclic redundancy checks and message authentication codes on the level of functional safety and security, respectively. The results show the general viability of our approach in conjunction with the capabilities of the evaluation platform for the continuous verification and validation of quality-related characteristics of a CPS under development.

***Index Terms*—Virtual Verification and Validation, Continuous Engineering, Simulation-based Testing, Trade-off Analysis, Evaluation Platform, VCIP/FERAL, Cyber-Physical Systems, Dependability Attributes, Functional Safety, Security**

I. Introduction and Related Work

In recent years, the evolution and cross-field integration of cyber-physical systems (CPS) has revolutionized various industries, ranging from automotive and healthcare to manufacturing and agriculture [1]. Bonding digital technologies for computation and communication to physical devices and processes more and more ushers in an era of unprecedented efficiency, productivity, and automation, especially regarding agricultural practices to optimize resource utilization, enhance decision-making, and increase yields [2]. However, this transformation has also led to severe challenges, particularly the balanced preservation of intertwined quality attributes like functional safety and security of these increasingly accessible and, thus, more vulnerable mission-critical systems [3]. Mission-criticality of software/hardware-based constructs like CPS refers to their vital role in supporting the objectives or essential functions of an organization or entity in that their failure or disruption generally implies significant negative consequences for the operation of critical infrastructures, products, and services [4]. This applies to the wide array of networked devices, sensors, actuators, and control subsystems that monitor, manage and execute agricultural processes, from crop cultivation to livestock management and beyond.

Besides leveraging advanced technologies such as wireless sensors, data analytics, and machine learning techniques, the underlying and increasingly service-oriented distributed system architectures crucially rely on differently scaled communication networks. These complementary structures, which cross-link local, wide, and global areas, enable the required interaction between the involved machine and cloud components in the first place [5]. Considering tractor-implement communication in particular, Controller Area Network (CAN) is still a widely used network technology for local inter-machine data exchange due to its high resource efficiency, transmission reliability, and the locality constraint of electronic control units (ECUs) being connected [6].

Now, as CPS become increasingly autonomous through further interconnection, they also become more susceptible to various security threats and safety hazards, the prevention and circumvention of which is meant to be achieved by corresponding design tactics in terms of technical measures and counteractions. In the context of legacy CAN-based integration, a well-proven tactic to foster functional safety is the utilization of cyclic redundancy checks (CRC), a method used to detect random errors in transmitted data based on an error-detection code, which is appended to the end of a message frame before transmission and then verified by the receiver to ensure data integrity [7]. In terms of security-related goals, protecting messages against intended data manipulation by means of message authentication

2325-6664/24/$31.00 ©2024 IEEE
DOI 10.1109/DSN-W60302.2024.00028

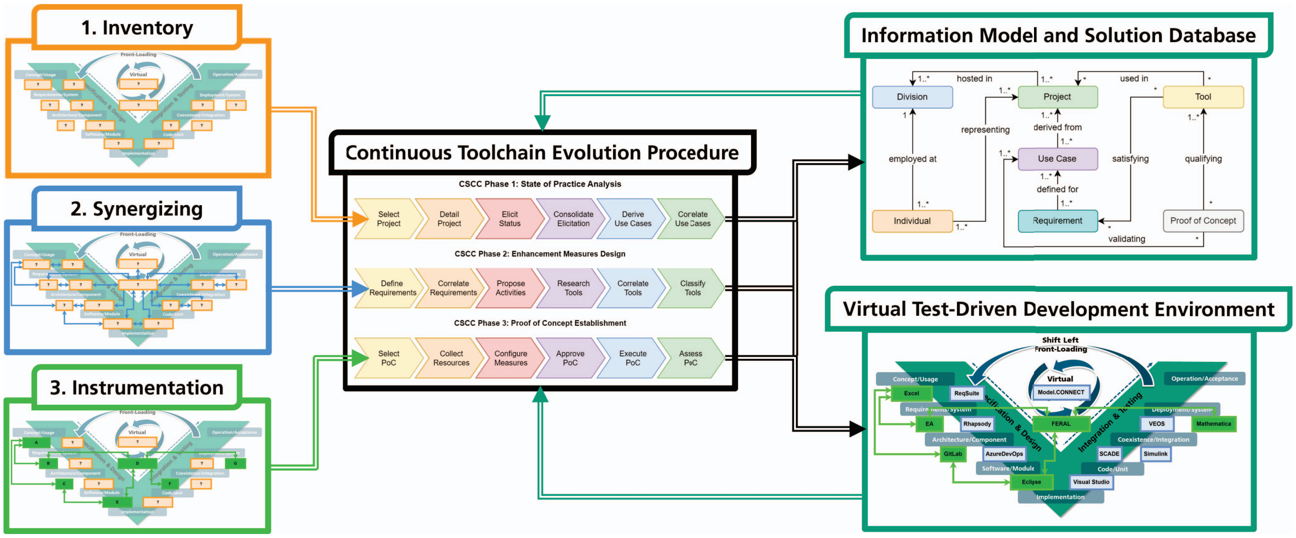

Fig. 1. Overview of continuous shift-left convergence concept and associated building blocks. The multi-phase continuous toolchain evolution procedure is used to incrementally synergize toolchains from the tool inventory for the qualified instrumentation of a virtual test-driven development environment (VTDE), the details of which are stored in an information model and solution database. A baseline VTDE supports generic cross-project development use cases.

codes (MAC) constitutes an established cryptography-based tactic, which ensures data integrity and authenticity in that transmitted messages are not altered or tampered with and originate from a trusted source. While CRC-based protection is a specified part of the complete CAN family of standards, MAC-based security is not considered and not even viable for legacy CAN variants up to version 2.0B. This is due to the lack of support for frames sizes allowing to incorporate sufficiently large authentication codes within the payload portion of a data frame [8]. A comprehensive overview of related works on applying co-analysis of safety and security during system engineering in various domains is provided in [9]. The presented results emphasize the interdependence between security and safety aspects in terms of mutual influence, which implies the imperative need for simultaneous consideration of their trade-off and emerging side effects when designing and deploying individual quality enhancement measures.

II. Continuous Evaluation of CPS Design

Given the evident challenges around balanced preservation of intertwined functional and particularly qualitative characteristics like functional safety and security, eligible solutions for future-proof CPS development must facilitate technically sound processes along with corresponding tooling support for virtual evaluation technologies. Also, any associated resources need to be adaptable for seamless integration into superordinate continuous engineering pipelines to maintain organizational development infrastructures long-term competitive and sustainable [10], [11].

In this context, the continuous shift-left convergence concept (CSCC) introduced in [12] defines a systematic approach for the establishment and adaptive evolution of virtual test-driven development environments (VTDE) based on the VCIP reference architecture as per virtual continuous engineering (VCE) framework [13]. Figure 1 outlines its integral parts summarized by general activities as follows.

1) **Inventory** of tools supporting single use cases in the context of product development within an organization.
2) **Synergizing** of inventory items with potential substitutes and complements into chains of tools required to optimize support of combined development use cases.
3) **Instrumentation** of baseline VTDE instances with qualified toolchains based on synergized tool inventory items with support for generic development use cases.

Once a baseline VTDE is initially established within an organization, it shall be instantiated and configured for concrete development projects. Therefore, we propose the continuous design evaluation cycle (CDEC), a recurrent multi-step process extending CTEP as a complementary building block of the VCE framework. CDEC augments the framework by a systematic approach for dynamically adapting the configuration of a baseline VTDE to effectively develop a CPS in a concrete project context. To this end, CDEC utilizes the iterative outcome of the design and evaluation activities to incrementally enhance the tools, models, scripts, and parameters of the instantiated VTDE in terms of its suitability for developing that specific CPS or variants thereof. The CPS design candidates and associated architecture drivers as well as driver solutions in common hereby allow the VTDE instance to evolve with the variants of CPS in the course of development projects even across subsequent product generations. Amongst other benefits, this allows for flexibly applying different testing approaches like virtual experimentation and formal analysis to substantiate decisions regarding the design of CPS subject to manifold functional and quality-related demands.

While CTEP defines the initial creation and continuous

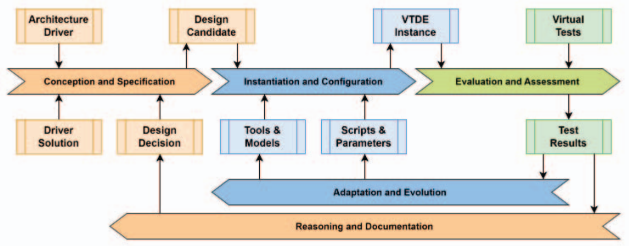

Fig. 2. Overview of the continuous design evaluation cycle (CDEC) during CPS development including input/output artifacts and process steps.

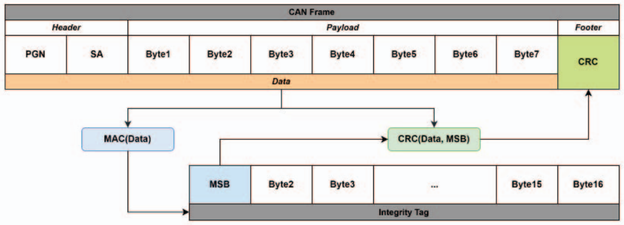

Fig. 3. CAN data frame structure for protecting inter-ECU communication as per security conception based on combination of most-significant byte (MSB) of MAC function integrity tag and CRC function checksum calculation.

adaptation of a baseline VTDE making up a cross-project development environment on the long run, CDEC constitutes the short-term counterpart during actual product development when using that environment. In this regard, CDEC enables the utilization of exchangeable and complementary testing activities with the aim of improving test result quality through, e.g., mutual safeguarding and increasing efficiency by parallel and synchronized virtual test execution. To this end, both procedures share access to the information model and solution database storing details on associated projects and resources.

In the course of CPS development, the configured VTDE instance might be required to be dynamically instrumented by further synergized tool inventory items in case new or changing architecture drivers for the developed CPS imply to do so. This may involve the repeatable execution of necessary parts of the CTEP, which can be triggered by the same rules as conventional development pipelines. In fact, the CSCC processes are meant to become an integral part of such pipelines preserving continuity, albeit heavily driven by project-specifics at least in terms of their cadence. That is, the evolution of a baseline VTDE is anticipated to occur much less frequently than, e.g., product release increments during a CPS development lifecycle. In contrast, the adaptation of a project-specific VTDE instance configuration can occur as often as several times during the specification and evaluation of a single design candidate. In turn, this depends on different factors like available resource capacities, product complexity, and the level of automation possible for the individual steps of both CSCC processes. Figure 2 illustrates the step sequence of the cyclic multi-phase CDEC as detailed in the following.

1) **Conception and Specification** of design candidates derived from architecture drivers and potential driver solutions for the CPS under development.
2) **Instantiation and Configuration** of VTDE based on tools and models by means of integrative coupling and parameterization in the context of virtual tests.
3) **Evaluation and Assessment** of design candidate based on virtual tests enabled by configured VTDE instance.
4) **Adaptation and Evolution** of VTDE instance and baseline properties depending on required changes as interpreted from obtained test results.
5) **Reasoning and Documentation** of design decisions based on yield test results.

III. CDEC-based Trade-Off Evaluation of CPS Dependability Attributes: A Case Study

In order to validate the practicability of CDEC including its adaptability to organizational circumstances, we showcase our approach in the context of an industrial reference project from the agricultural sector. The generalized outcome of that anonymized project acts as a case study describing the application of CDEC as part of the VCE framework for real-world CPS development on the basis of a project-specific VDTE instance. For the sake of focused comprehension, only selected project results are presented, which substantiate the benefits and drawbacks of the proposed and applied concepts.

A. *Conception and Specification*

The reference project deals with the development of a tractor-implement coupling subsystem meant to be secured from intentional threats, while its level of functional safety shall be preserved as far as possible. This system under test relies on a legacy CAN-based communication protocol, SAE J1939, for the exchange of diagnostics and control information as the major constraint. Also, no physical prototypes of the involved ECUs are available, rendering the VTDE to virtual technologies only. In this context, two individually well-understood network frame-related mechanisms, CRC and MAC, are taken into consideration. The actual goal of the aspired evaluation is to comprehend in how far those measures influence each other in terms of their mutual impact on the levels of the considered quality properties. Figure 3 visualizes the structure of a CAN data frame and the conceived architecture driver solution candidates in terms of using dedicated portions of the MAC integrity tag as input for the CRC checksum calculation in different variations.

B. *Instantiation and Configuration*

To meet the elicited architecture drivers, we apply CSCC to establish a productive VTDE consisting of baseline toolchain components configured to support, a.o., requirements management, system architecture and detailed design, data visualization and analysis, as well as software code development. Further, the simulation and simulator coupling toolbox FERAL is selected for modelling, execution, and assessment of virtual tests. With that VCIP-based setup, we are able to model and virtually integrate the relevant

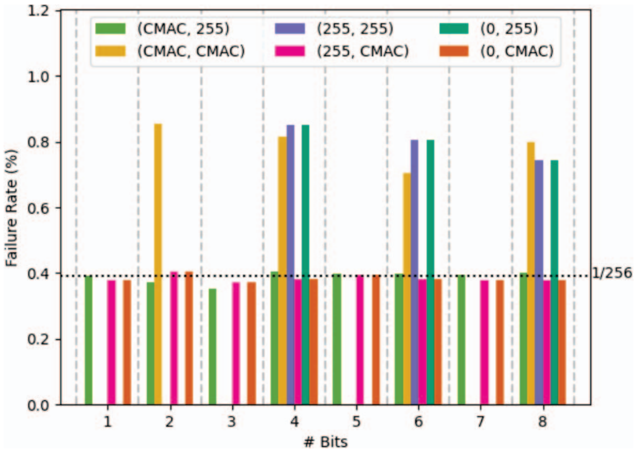

Fig. 4. Excerpt of representative evaluation results in terms of detection failure rate against number of bit flips for different design candidates including legacy AUTOSAR-CRC (255,255) and MAC-MAC-CRC (CMAC,CMAC), which is accepted per design decision due to its trade-off performance outperforming any tested alternatives with regard to security and functional safety properties.

SUT components required to reflect the quality properties under evaluation. These include a CAN medium abstraction, network and application interfaces of communicating ECUs with CRC and MAC algorithm implementations along with fault-injection and statistics calculation components.

C. Evaluation and Assessment

As part of the test results depicted in Figure 4, several design candidates intended to achieve combined security and functional safety properties for the tractor-implement communication are compared to the legacy AUTOSAR-CRC standard lacking security support whatsoever. Amongst other results obtained from empirical observations of statistical simulation models and solving formal counterparts based on theoretical hypotheses, we found that the alternative design candidate MAC-MAC-CRC features error detection capabilities fully comparable to AUTOSAR-CRC in the higher range of bit fault bursts above 10 bits. However, the conducted investigations have also shown that AUTOSAR-CRC is still superior in the lower range from 1 up to 10 bit burst lengths.

D. Adaptation and Evolution

Since early results yield in the course of conducting virtual experiments revealed exceptional phenomena worthwhile deeper insights, we opted for adapting the VTDE by adding a tool with support for formal analysis. To this end, we applied CTEC to scan our tool inventory for viable options, which offered the required set of features, and selected Mathematica.

E. Reasoning and Documentation

In terms of documenting the decisions regarding design candidates, the yield test results substantiated the acceptance of the MAC-MAC-CRC variant while discarding the other tested alternatives. The rational lies in the balanced trade-off performance regarding the introduction of security with only little impact on the quality of the functional safety attribute.

IV. Conclusions and Future Work

In this work, we introduced a virtual testbed adaptation and evolution process to facilitate trade-off evaluation of CPS dependability attributes by means of conducting virtual experimentation and formal analysis in a continuous cycle. Our approach enables the focused and systematic evaluation of design candidates meant to increase the level of quality properties individually and in combination. For the sake of validation, we applied our approach in an industrial context for the reasoning of design decisions with respect to a tractor-implement coupling subsystem subject to functional safety and security requirements in the agricultural domain. The yield results testify the practicability of our solution, its integrability into continuous engineering pipelines, and the capabilities of the established virtual test-driven development environment.

As future work, we intend to increase the automation level of CSCC-based development pipelines to foster, a.o., their functional suitability and performance efficiency. Therefore, further VCIP integration connectors shall be implemented to automatize the interplay in terms of mutual safeguarding and parallelization between tooling used for virtual experiments and formal analytics. Furthermore, we plan to develop AI-based automation assistance for different parts of the VCE framework like the dynamic configuration of multipurpose virtual testbeds, traceable execution of holistic system evaluations, as well as result-based decision-making.

References

[1] D. Serpanos, "The cyber-physical systems revolution," *Computer*, vol. 51, no. 3, 2018.

[2] M. S. Farooq *et al.*, "Role of iot technology in agriculture: A systematic literature review," *Electronics*, vol. 9, no. 2, 2020.

[3] E.-Y. Kang, "Assa-cps: Automated formal safety and security assessments in cyber-physical systems," in *2023 7th International Conference on System Reliability and Safety (ICSRS)*, 2023.

[4] A. Banerjee, K. K. Venkatasubramanian, T. Mukherjee, and S. K. S. Gupta, "Ensuring safety, security, and sustainability of mission-critical cyber–physical systems," *Proceedings of the IEEE*, vol. 100, no. 1, 2012.

[5] N. ElBeheiry and R. S. Balog, "Technologies driving the shift to smart farming: A review," *IEEE Sensors Journal*, vol. 23, no. 3, 2023.

[6] A. Al-Mallahi *et al.*, "Development of robust communication algorithm between machine vision and boom sprayer for spot application via iso 11783," *Smart Agricultural Technology*, vol. 4, 2023.

[7] "Specification of CRC Routines," AUTOSAR Classic Platform, Standard R22-11, DID 16, 2022. [Online]. Available: www.autosar.org

[8] N. Nowdehi, A. Lautenbach, and T. Olovsson, "In-vehicle can message authentication: An evaluation based on industrial criteria," in *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*, 2017.

[9] E. Lisova *et al.*, "Safety and security co-analyses: A systematic literature review," *IEEE Systems Journal*, vol. 13, no. 3, 2019.

[10] B. Fitzgerald and K.-J. Stol, "Continuous software engineering: A roadmap and agenda," *Journal of Systems and Software*, vol. 123, 2017.

[11] P. O. Antonino, M. Jung, A. Morgenstern, F. Faßnacht, T. Bauer, A. Bachorek, T. Kuhn, and E. Y. Nakagawa, "Enabling continuous software engineering for embedded systems architectures with virtual prototypes," in *Software Architecture*, C. E. Cuesta, D. Garlan, and J. Pérez, Eds. Cham: Springer International Publishing, 2018.

[12] A. Bachorek and J. Jung, "Establishing virtual test-driven development environments in the automotive domain: A continuous engineering approach," in *IEEE/ACM International Workshop on Software Engineering for Systems-of-Systems and Software Ecosystems (SESoS)*, 2023.

[13] A. Bachorek, F. Schulte-Langforth, A. Witton, T. Kuhn, and P. O. Antonino, "Towards a virtual continuous integration platform for advanced driving assistance systems," in *IEEE International Conference on Software Architecture Companion (ICSA-C)*, 2019.