26th INTERNATIONAL DEPENDENCY AND STRUCTURE MODELING CONFERENCE, DSM 2024
STUTTGART, GERMANY, 24 – 26 September, 2024

Ensuring Consistency and Credibility in Cyber-Physical Systems Validation

Francesco Pio Urbano, Patrick Grycz, Jonas Freyer, Katharina Bause, Arne Bischofberger, Tobias Düser and Albert Albers

Karlsruhe Institute of Technology, IPEK

Keywords: Cyber-Physical Systems, Systems Engineering, XiL, Validation Environment

1 Introduction

Modern cyber-physical systems (CPS) are complex systems of multiple domains, such as mechanics, electrical, and software. Each of these domains uses different models, tools, and processes during their product development. These artifacts can range e.g., from CAD Data to electrical models and software code. Often, multiple developers or teams are working with different model-based tools. These tools are not synchronized, and errors during integration are common. Different variants and generations of implementation artifacts increase the complexity even further. The collaborative research “center consistency in the view-based development of cyber-physical systems” (CONVIDE) investigates how these artifacts and models can be linked using semantic relations expressed in a formalized way. (Reussner et al., 2023) The goal is to minimize integration efforts and detect inconsistencies between models of different disciplines early on in the product development process. These semantic relations can also be used for validation, especially to analyze which impact a change has on a system and which test cases need to be reevaluated or how validation environments must be changed to be still functional. During product development, it is necessary to carry out validation activities in order to gain knowledge of the System in Development (SiD). An adequate validation environment is essential, as it serves as a model of the system and inherently involves a degree of abstraction. Therefore, it is crucial to continually assess the credibility of the test outcomes produced in these environments. (Düser, 2022) If the credibility is not sufficient, a new validation configuration must be created. Assessing the credibility of models and creating new validation configurations is an experience-based process, which is particularly challenging with complex systems of systems. This is why a formalized process is necessary. A promising approach is to leverage a comprehensive system model, which includes the SiD, scenarios, and test cases. The model illustrates the properties, limitations, and features of both the validation environment and the SiD and assists in assessing the credibility. In this contribution, we want to outline a vision for a novel process for verifying and validating cyber-physical systems, including variants and generations and the related validation environments, using semantic relations provided by the CRC 1608 CONVIDE. (Reussner et al., 2023)

2 Motivation & Current Research

In systems engineering, validation plays a critical role in ensuring that the developed solution or product aligns with stakeholder requirements. Therefore, during validation the complete behavior of systems and residual subsystems is examined. These residual systems are tested using different environments, which are selected based on maturity, effort, cost or credibility, for example. One approach to this validation process is the IPEK-X-in-the-Loop (IPEK-XiL) as shown in Figure 1.

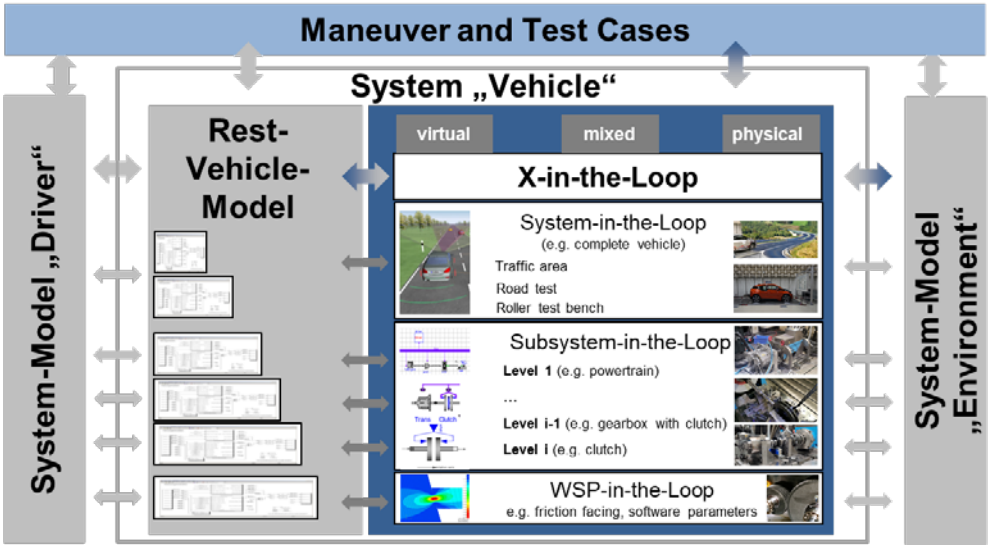

Figure 1 IPEK-X-in-the-Loop (IPEK-XiL) approach adapted from (Albers et al., 2008)

This approach builds upon established methods such as Model-in-the-Loop (MiL), Software-in-the-Loop (SiL), and Hardware-in-the-Loop (HiL). It integrates the respective advantages of these methods and expands them to address the specific needs of the domain of mechanics and mechatronics, as well as involving developers from various disciplines. Consequently, the IPEK-XiL approach provides a comprehensive framework for validating subsystems by integrating them into the overall system, the relevant environment, and potentially other interacting systems, such as the driver. (Albers et al., 2008; Albers et al., 2016)

Modern validation environments must be flexible enough to be able to react to different test requirements or system changes. Although self-adaptation strategies already exist for CPS such approaches are lacking in XiL environments. However, there is currently a lack of suitable, formalized methods and processes for finding the most suitable validation environment and validation configuration for a specific validation objective out of all the possible validation configurations. The choice of validation configuration is often based on experience and implicit knowledge (Freyer and Düser, 2023). In contrast to validation, verification checks the correctness of a system, component, or artifact. This check relies on testing. They reach from simple unit test (Olan, 2003) cases that check code to complex scenario-based tests, which are the industry standard (ISO, 2022) to verify automated driving functions. These scenario-based tests are often generated based on boundary conditions, like speed, initial velocity, or position. The execution of the complete suite of scenarios is highly resource intensive and therefore not feasible. For one scenario, there can be millions of permutations of boundary conditions. The entirety of all tests is called the test suite of a CPS. Given the complexity of modern CPS and the increasing number of iterations due to agile approaches, it is not possible to test the entire test suite every time a change is made to the system. Therefore, methodologies are needed to select and prioritize test cases in these test suites. There are already methodologies based on ontologies (Hasnain et al., 2021), genetic algorithms, or reinforcement learning (Bagherzadeh et al., 2021). We aim to improve existing data-driven metrics by taking dependencies, provided by the CONVIDE meta model (Klare et al., 2021), between artifacts of different domains into consideration.

3 Process for Validation and Verification of Cyber-Physical Systems

3.1 Overview

Figure 2 shows our proposed process for verifying and validating cyber-physical systems. Based on a set of changes, an interdisciplinary change analysis is performed. During this analysis, all from the change affected artifacts and variants are identified and passed to the analysis step. Firstly, the possibilities for validation offered by the existing environments are analyzed. The validation environment analysis used for identifying a set of required validation configuration adaptions needs to be executed before the test case execution step. In addition to that, a set of configurations is provided that is used during the runtime of the test case execution. The further analysis is used to select all relevant test cases from the test suite. It prioritizes them according to their potential likeliness to fail. The results of this step are then sent to the test case execution step. The test cases are executed according to the selection and prioritization, and test results are stored.

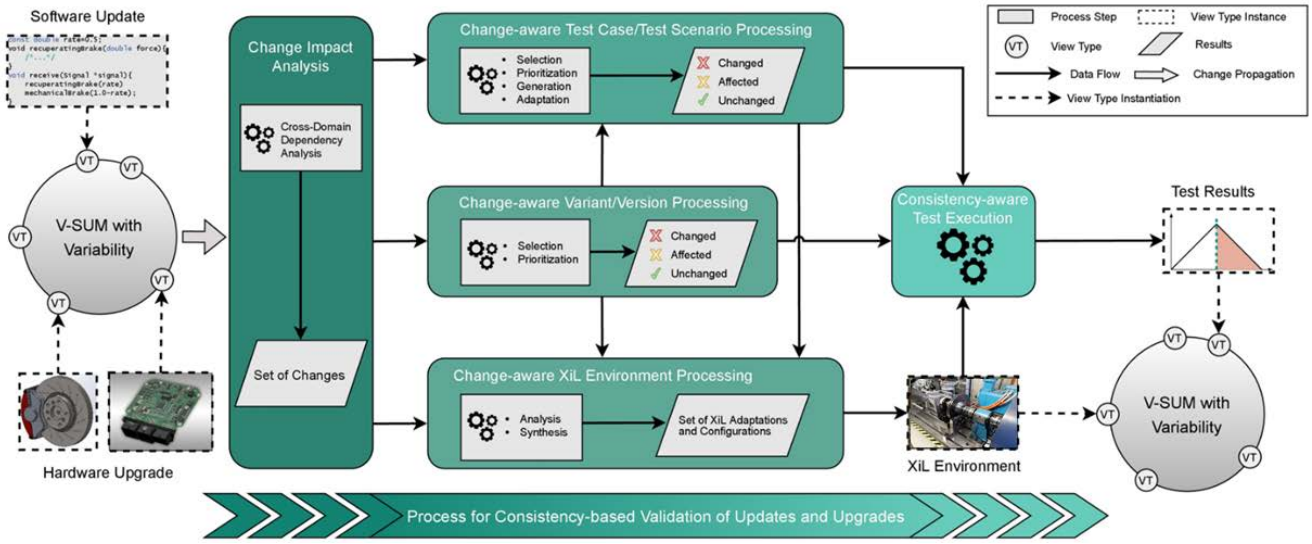

Figure 2. Proposed Process for Validation and Verification of Cyber-Physical Systems

3.2 Interdisciplinary Change Impact Analysis

The change impact analysis is the first step in the process. Based on the system models and the set of introduced changes, the analysis returns the following three key results. The first result is the boundary definition and the selection of the SuI.

The first result is the definition of the limits and the selection of the system to be analyzed. In this paper, the SuI is a vehicle braking system. Braking systems are modern CPS that are highly relevant to safety. Depending on the changes, the SuI can range from a pure software, hardware, or mechanical subsystem to combined subsystems or even complete systems like a car. In addition to that all affected artifacts were estimated. This is done by using the semantic relations provided by the CONVIDE meta model and other data sources. In general, there are two types of relations. A strong relation, which is extracted from the meta model, can estimate qualitative and quantitative implications on artifacts. A weak relation indicates there is a connection between certain artifacts but does not specify any concrete semantics. Using these relations, the changes are now propagated, and by applying semantic slicing, affected artifacts and models are identified. Based on these selected artifacts affected variants and the SuI can now be identified. It is possible, that multiple variants or SuI are identified. If there are multiple relevant SuI, the downstream analyses are performed for each SuI individually. Our main research question regarding this analysis is how a semantic slicing algorithm should look to capture all relevant artifacts.

3.3 System Model of the XiL Environments

The characteristics of XiL environments can vary significantly. Figure 3a illustrates a brake system integrated with a mechanical setup, while Figure 3b depicts a synthetic environment used for virtual test driving. Depending on the validation objectives, these environments can be interconnected. Adapting the mechanical setup, such as replacing brake pads or the change of the recuperation rate that impacts the dimensioning of the brake assembly and E/E architecture, requires manual intervention. Conversely, modifications to the virtual environment are more straightforward, as standardized configuration descriptions like OpenDrive and OpenScenario have become widely adopted. The goal is to describe which changes to the SiD require corresponding adjustments in the XiL environment. Ideally, the analysis will result in an automatic configuration for the virtual environment and a step-by-step guide for modifying the mechanical environment. Creating a system model of the XiL environment is crucial for maintaining consistency and credibility when changes occur in the SiD. This model enables effective comparison and ensures the integrity of the overall system.

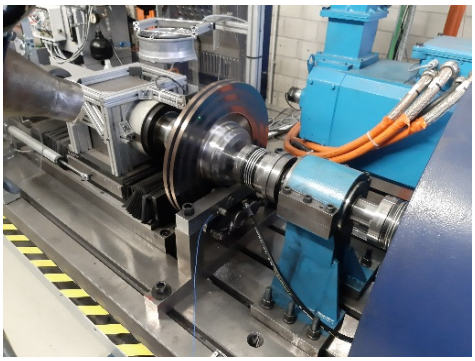

Figure 3a. Brake System in-the-Loop Test Environment

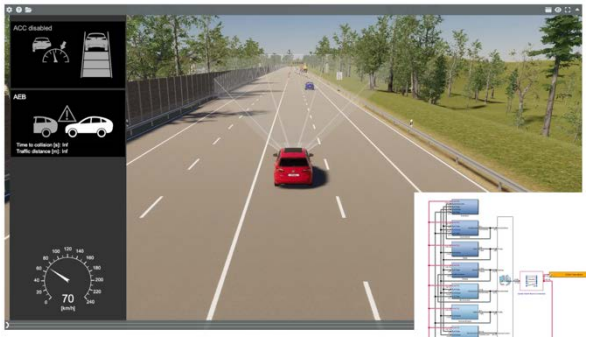

Figure 3b. Virtual Scenario Test Environment

3.4 Test Case Analysis

Based on the results of the change impact analysis, it is determined which specific test environments are appropriate to execute the tests. If conditions outside the validated operational design domain of a model or test environment are required, such as wet brake conditions, it may be necessary to use models with a lower level of abstraction, such as a mechanical Brake System in-the-Loop Test Environment (Figure 3a). Our goal for the test case analysis is to determine the correct environment using custom attributes added in the system models. The second step is the selection of test cases from the test suite. This is especially challenging for scenario-based tests, where multiple continuous input parameters need to be sampled. By using semantic relations, we can sample these parameters and test cases systematically by only sampling cases where they are affected. In our brake system example, when the surface is changed, we only need to sample properties related to the vehicle's longitudinal velocity. Based on the relations also, the test cases are prioritized based on their likeliness to fail. This is especially useful to find errors introduced by the change. If an error is found, further testing can be stopped.

4. Application of Methods and Processes

A case study will be carried out to evaluate the results of the proposed process. This case study is planned to be carried out with a Formula Student Team, where the developed methods are applied and tested on different test cases. This serves as a proof of concept as well as a source of new requirements for adapting the methods to the automotive sector. The case study deals with both the validation of software updates and the validation of hardware upgrades in CPS. The software updates to be investigated will be based on realistic use cases for optimizing the efficiency, performance and safety of the Formula Student vehicles. The consistency-based test strategies developed in CONVIDE will be implemented and

evaluated based on the available vehicle variants from current and past racing seasons. In addition, the XiL environment developed in 3.3 is also analyzed and evaluated. This evaluation is done for two main use cases with increasing complexity: First, the development and integration of updates for functions with a low degree of automation. Secondly, the investigation of updates for systems with a higher degree of automation (SAE level 3), whereby the scenario-based test methods developed are evaluated. For the validation of hardware upgrades in CPS, the change in the braking system is first investigated at the subsystem level, considering interactions with the rest of the system, before the entire vehicle behavior is analyzed. For example, the influence of a change in the braking system on its braking distance is analyzed. The added value of this case study is the practical application of the results of this project to evaluate their applicability in practice, but also to gain insights that cannot be obtained in a laboratory-like or theoretical environment.

5. Summary and Outlook

This paper presents a vision for a novel verification and validation (V&V) process for CPS that utilizes the semantic relationships provided by the CONVIDE project. Our motivation stems from the need to reduce the complexity and effort involved in the integration and testing of CPS. This includes the adaptation and configuration of XiL environments as well as the prioritization and selection of relevant test cases. The proposed process begins with an interdisciplinary change analysis that identifies all affected artefacts and variants. Necessary adjustments are then made in XiL environments, both automatically and manually. The process ends with the selection and prioritization of test cases in order to use test resources efficiently and identify errors quickly. A case study with a Formula Student Team demonstrates the practical applicability of our methods. This case study includes both software updates and hardware upgrades and evaluates the efficiency and safety of the developed strategies in real scenarios. The results of this research make an important contribution to the field of CPS by providing a framework for more efficient and accurate verification and validation processes. Future work will focus on improving the adaptability and credibility of XiL environments. In addition, further case studies in different domains will help to generalize the methods and validate their robustness in different CPS applications. This research will contribute to the development of automated and intelligent V&V tools that can be seamlessly integrated into existing system models and ultimately lead to more reliable and secure CPS.

Acknowledgements

This paper is funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – SFB 1608 – 501798263.

References

Albers A., Behrendt M., Klingler S., Matros K., 2016, Verifikation und Validierung im Produktentstehungsprozess In: Lindemann (Ed), Handbuch Produktentwicklung, München: Carl Hanser Verlag, München, 541–569.

Albers A., Düser T., Ott S. (Eds), 2008, X-in-the-loop als integrierte Entwicklungsumgebung von komplexen Antriebsystemen, Kassel, Haus der Technik.

Bagherzadeh M., Kahani N., Briand L., 2021, Reinforcement Learning for Test Case Prioritization.

Düser T. (Ed), 2022, Credibility Argumentation - Correlation of virtual and physical testing.

Freyer J., Düser T. (Eds), 2023, A study on the transformation of virtual validation methods in the development of new mobility solutions.

Hasnain M., Ghani I., Pasha M.F., Jeong S.-R., 2021, Ontology-Based Regression Testing: A Systematic Literature Review, Applied Sciences, 11, 9709.

ISO, 2022, ISO 21448-1: 2022 Road vehicles — Safety of the intended functionality.

Klare H., Kramer M.E., Langhammer M., Werle D., Burger E., Reussner R., 2021, Enabling consistency in view-based system development — The Vitruvius approach, Journal of Systems and Software, 171, 110815.

Olan M., 2003, UNIT TESTING: TEST EARLY, TEST OFTEN, Journal of Computing Sciences in Colleges 19, 319–328.

Reussner R., Schaefer I., Beckert B., Koziolek A., Burger E., 2023, Consistency in the View-Based Development of Cyber-Physical Systems (Convide) In: 2023 ACM/IEEE International Conference on Model Driven Engineering Languages and Systems Companion (MODELS-C), 83–84.

Contact: Francesco Pio Urbano, Karlsruhe Institute of Technology, Institut für Produktentwicklung (IPEK), Kaiserstraße 10, Karlsruhe, Germany, 4972160847211, francesco.urbano@kit.edu