A Process for Sound Conformance Testing of Cyber-Physical Systems

(Position Paper)

Hugo Araujo, Gustavo Carvalho, and Augusto Sampaio
Universidade Federal de Pernambuco, Brazil
Email: {hlsa,ghpc,acas}@cin.ufpe.br

Mohammad Reza Mousavi and Masoumeh Taromirad
Halmstad University, Sweden
Email: {m.r.mousavi,m.taromirad}@hh.se

***Abstract*—We present a process for sound conformance testing of cyber-physical systems, which involves functional but also non-functional aspects. The process starts with a hybrid model of cyber-physical systems in which the correct behavior of the system (at its interface level) is specified. Such a model captures both discrete behavior and evolution of continuous dynamics of the system in time. Since conformance testing inherently involves comparing continuous dynamics, the key parameters of the process are (1) the conformance bounds defining when two signals are sufficiently close to each other, and (2) the permitted error margin in the conformance analysis introduced by sampling of continuous signals. The final parameter of this process is (3) finding (and adjusting) the sampling rate of the dynamic behavior. In the specified process, we provide different alternatives for fixing the error margin of the conformance testing if the sampling rate is fixed, establishing the sampling rate if the error margin is fixed and finding conformance bounds once the sampling rate and the error margin are fixed.**

I. Introduction

Cyber-Physical Systems (CPSs) integrate the computer-controlled world with the physical world in a feedback loop. They feature a tight integration of software, hardware, and physics in various safety critical domains (such as automotive and healthcare). Hence, their thorough and rigorous validation and verification are of utmost importance.

To put verification on rigorous grounds, conformance testing has been studied and used extensively [1]. As a formal notion of model-based testing, conformance testing assumes the availability of a specification model that describes the system expected behavior. Besides this model, it is assumed that the implementation behavior can also be described using the same notation of the specification model. (Such a description of the implementation is only theoretically assumed to exist; practically, it is often too large to be generated, stored, or analyzed explicitly.) This requirement is known as the testability hypothesis. Furthermore, for the conformance testing to be rigorous, these models are typically assumed to have well-defined syntax and formal semantics; such models include various kinds of labelled transition systems [2], and hybrid automata [3], among others. Conformance is then defined as a mathematical relation between the specification and the implementation models.

In the context of CPSs, conformance testing can be used to verify the correctness of an implementation with respect to a model, or to verify the correctness of a model with respect to a high level specification. The latter is particularly useful, since in many domains the implementation code is automatically generated from models (e.g., in Matlab Simulink / Stateflow). Hereafter, we refer to the higher level specification or model collectively as the *model*, and to the implementation or the lower level model as the *system under test (SUT)*.

Conformance testing of CPSs not only involves checking discrete input-output conformance (e.g., in the sense of [2], [4]), but also measuring the closeness of the continuous behavior. CPSs naturally take into account aspects of the system that are traditionally considered non-functional (e.g., timing and energy consumption properties), since they are significant and commonly inseparable part of the system description. Therefore, conformance relations for CPSs often accommodate both functional and non-functional aspects as well. For this purpose, several notions of approximate conformance for CPSs have been defined in the literature [5], [6], [7], [8], [9]. Such notions of conformance will inevitably involve setting various parameters, such as the measures of closeness of the system under test with its model, the permitted error margin in the conformance analysis for discretized (continuous) signals, and the sampling rate involved in generating and executing test cases.

In [10], we present an overview and a general roadmap for conformance testing of cyber-physical systems. Among the most developed notions hitherto is the notion of (τ, ϵ)-conformance [5], on which we mostly focus in this paper. In our previous work [11], we studied how checking the conformance relation (τ, ϵ)-conformance [5] can be performed soundly using a simple test case generation algorithm. In this paper, we present the initial ideas for defining a practical process for sound conformance testing based on the algorithm proposed in our previous work [11]. In particular, we show how to set the various parameters of this notion of conformance in an iterative refinement. It is worth noting that this process is potentially scalable to real-world large-scale CPSs, since it is based on testing (and simulation). Typically, formal verification is not scalable, but testing, on the contrary, tends to scale for large systems.

The rest of this paper is structured as follows. In Section II, we introduce the key parameters of the process. In Section III, we present the proposed process for sound conformance testing, structured in five well-defined steps. Afterwards, in

Section IV, we outline a research agenda for conformance testing of CPSs. Finally, we summarize our results in Section V.

II. Parameters of Conformance Testing

The key parameters of the proposed process for sound conformance testing of CPSs are described in the following subsections.

A. Closeness

When comparing physical systems, it is often necessary to measure how "close" they are from each other. In conformance testing of CPSs, that can mean measuring the distance between two output signals or computing the intersection of a signal with a region. The most common approach is using Euclidean distance, which is a widely known method for computing the distance between points in a geometrical space.

In addition to the Euclidean distance, other approaches have also been used. In [8] and [12] Skorokhod distance is used to measure the closeness between continuous signals with promising results. In [8], the author argues that Skorokhod is well suited for conformance checking and also provides benchmarks using a prototype tool that mechanises his strategy. In [12], however, the author questions the use of Skhorokod in a multiple input system and also in unstable systems.

In the process presented in Section III, although we consider Euclidean distance by default, it is straightforward to adopt other closeness notions, as well. In particular, we consider the conformance relation (τ, ϵ)-conformance [5], which takes the Euclidean measure for closeness of signals by considering two parameters representing the allowed conformance bounds in time (τ) and space (ϵ), respectively. Informally speaking, this conformance relation compares the output reaction of the specification model and the system under test (implementation) to the same input stimuli. The system under test is said to conform to the model, if the output behavior is "similar", i.e., it differs, from that of the model, temporally or in signal values not more than the pre-defined τ and ϵ thresholds, respectively.

B. Precision

Conformance relations are typically defined in a theoretical framework involving the formal semantics of the model and the formal semantics of the SUT. However, the latter is practically impossible to obtain for sufficiently large systems. Hence, one has to check the conformance relation using test cases that are generated from the model and are executed on the system under test. The result of this test execution must then be compared with the expected results of the model up to the specified conformance bounds. We refer to this process as conformance testing. Conformance testing involves observing the system behavior on a finite number of points and hence, involves reducing the comparison of the continuous behaviors to comparison of discretized samples of the two behavior; this process inherently deviates from the precise comparison of the continuous signals. Moreover, conformance testing needs to take into account measurement errors introduced by sensors and signal noises in general, such that the smallest disturbance in the signal will not necessarily yield unsound conformance results.

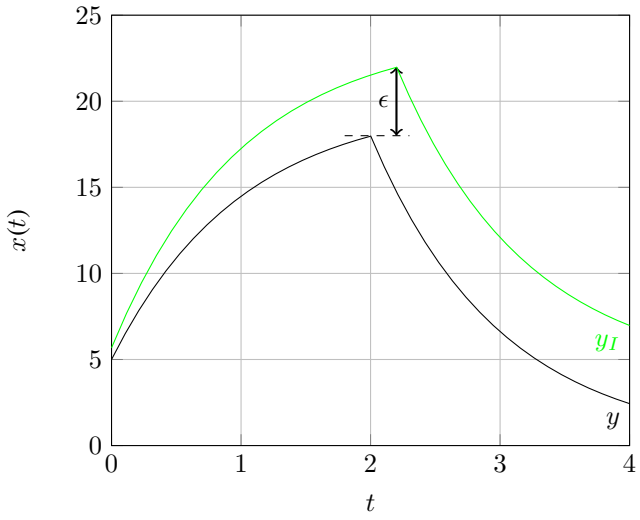

Fig. 1. The output trajectory of the spec. (y) and that of an imp. (y_I) [11]

In [11], it has been shown that in order to generate sound test-cases for the notion of (τ, ϵ)-conformance [5], one has to incorporate an error margin (Δ_p) that is inversely proportional to the rate of changes of the dynamics in the specification within the sampling intervals, i.e., the higher the sampling rate, the lower the error margin.

To give a concrete example, consider a thermostat system from [11]. Figure 1 shows an output trajectory obtained from its model (labelled as y), and an output trajectory of a conforming system under test (labelled as y_I). The trajectory y_I has been obtained by shifting y to the right by 0.2 and to above by 4. Considering $\tau = 1 > 0.2$ and $\epsilon = 4$, one can see that y_I satisfies the (τ, ϵ)-conformance notion. Assume that for conformance testing of the system under test, we consider a sampling function with sampling period of 0.03. If the set of sampling points P is selected such that $t = 2.2 \in P$, then $2 \notin P$. Therefore, under the described sampling function, this latter point is not included in the test case. As a result, the system under test fails even being in conformance with the model, since the corresponding expected value (considering the margin ϵ) is not observed in the model (specification).

To overcome this issue, in [11], we state that, given a specification and a periodic test-case with period $p > 0$, it is possible to compute the maximum changes within the specification, namely Δ_p. Furthermore, we make use of the straightforward algorithm for (τ, ϵ)-conformance testing, which considers τ and ϵ as parameters, and we prove that, by extending the parameter value representing the error margin (ϵ) of a $\Delta > \Delta_p$, one can always obtain sound results.

C. Sampling rate

As stated before, discrete sampling of continuous signals is often a necessary step when dealing with CPSs and is

closely related to the error margin involved in the discretization step [11]. The issue arises because information is always lost whenever a continuous signal is sampled. For instance, it is possible for the value of the signal to abruptly increase and decrease between two sample points, causing the sampled function not to capture this behavior.

The efficacy of conformance testing relies on choosing appropriate sampling rates that are proportional to the pace of changes in system dynamics; otherwise, conformance testing may yield unsound results due to the sampling function missing sharp signal variations. The process to define an adequate sampling rate requires analysis of the system dynamics. For instance, it can be computed by inspecting and defining a frequency limit from which the system ceases to provide significant responses and finally applying the Nyquist rate to find a suitable period.

III. Process for Checking Conformance

In this section, we present our process for sound conformance testing of cyber-physical systems (Figure 2). It starts with the definition of a sampling rate (Figure 2—step 1), which is used to sample the specification behavior. Higher sampling rates typically lead to fine-grained observations. However, in practice, it is not always possible to choose a high rate due to constraints the hardware and the environment impose to the system. Therefore, it is important to define a sampling rate that is both feasible, but also minimises the relevant data loss from the observations and hence, also the error margin allowing for sound test cases. In order to choose this rate, besides the knowledge about the system (specification) and its environment, one can benefit from traditional signal processing techniques such as wavelets and Fourier transform [13].

Also based on the specification and the knowledge about the techniques and tools employed to develop the implementation, it is necessary to define the conformance bounds (Figure 2—step 2): τ (time related) and ϵ (data related). As already explained in the previous section, these bounds cope with the closeness of signals in time and space, respectively. In other words, the τ-margin creates a time range that is considered acceptable for a given observation. For instance, suppose that, according to the specification, a value v should be observed at time $t1$. With respect to this aspect, it is considered acceptable if one observes the implementation producing a corresponding value within $[t1 - \tau/2, t1 + \tau/2]$. Similarly, the ϵ-margin creates a value range that is considered acceptable for a given observation (i.e., $[v - \epsilon/2, v + \epsilon/2]$).

As the next step, it is necessary to define (or calculate) the error margin (Δ_p) to guarantee that our conformance analysis is sound (Figure 2—step 3). Parameter Δ_p represents the model maximum change within the sampled points. In other words, this margin copes with the unseen values due to the chosen sampling rate. The conformance testing algorithm presented in [11] is proved to be sound if T and E, the algorithms time and value thresholds, are set such that $T = \tau$ and $E = \epsilon + \Delta$, where $\Delta \geq \Delta_p$. The computation of Δ_p can

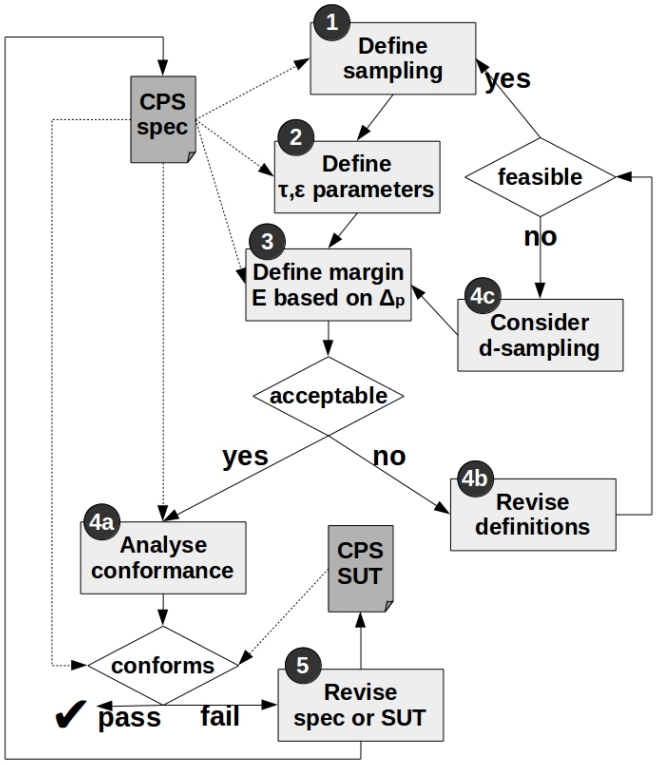

Fig. 2. Process for sound conformance testing

be practically performed via reachability analysis, such as the one provided by the CORA toolbox.[1]

Despite the aforementioned theoretical conclusion, the minimum possible value for E may prove to be an unacceptable (i.e., too high) error margin in practice. In such a scenario, the alternatives are to revise the conformance bounds or the sampling rate (Figure 2—step 4b). In other words, if a higher sampling rate can be used or if tighter τ and ϵ thresholds can be considered, lower E values may result for the conformance testing algorithm. With a more intricate conformance testing algorithm, dynamic sampling may be used (Figure 2—step 4c); this can lead to tighter error bounds with respect to different dynamics of the partial specification trajectories. Therefore, each local rate (r_i) will have a corresponding specification maximum change (Δ_i).

Finally, after defining the relevant parameters properly, one can apply the conformance testing algorithm presented in [11] to analyze whether the implementation under test conforms to the corresponding model (Figure 2—step 4a). If the fail verdict is reached, the implementation or the specification needs to be revised to reinstate conformance (Figure 2—step 5).

IV. Research Roadmap

Applying conformance testing to analyze the behavior of cyber-physical systems unfolds relevant, challenging, and unsolved problems. Although traditional conformance relations,

[1] http://www6.in.tum.de/Main/SoftwareCORA

such as ioco [2], can be lifted to the context of CPSs (e.g., hioco [6]), additional issues need to be addressed (e.g., the notion of closeness and the error margin in conformance testing). Furthermore, proper tools need to be provided to support practical applications of conformance testing of CPSs.

After comparing and contrasting the conformance relations for CPSs [10], we have chosen the (τ, ϵ)-conformance [5] as a suitable relation. We then considered an additional error margin (Δ_p) to guarantee the soundness of the testing process [11], and developed tool support [14]. In this paper, we propose process sketch for testing CPSs combining these results.

Despite the structured characterization of the proposed process, further work needs to be done in order to make it effectively applicable in practice. Therefore, we plan to address the following topics as future work.

- As it can be seen in Figure 2, defining the sampling rate plays an important role in our process. As previously mentioned, in practice, this definition is also constrained by the hardware and environmental aspects, including the test execution platform, particularly, when performing on-line testing. If the chosen sampling rate is too high, while the communication protocol of the test adapter (i.e., the one that sends/collects data to/from the SUT) is slow, information might be lost during the test execution. Mitigating this problem is an interesting and relevant research topic for practical conformance testing of CPSs.
- Another topic mentioned beforehand that also needs further investigation is dynamic (variable) sampling of continuous dynamics. For instance, when using Matlab / Simulink, the sampling rate can be suggested by a numeric solver, and it may actually vary over the simulation period. Considering CPSs modeled as hybrid automata, we plan to analyze whether there is some relation between different sampling rates and the automata states and classes of input trajectories, and then revisit our proposed process in the light of this analysis.
- Typically, CPSs have very large input spaces. When performing conformance testing, it is expected that a relevant, but also tractable, part of this space is considered. For instance, in [15] a coverage-guided test generation strategy is proposed for hybrid systems. Therefore, we plan to incorporate coverage criteria as part of our testing framework.
- Applying our process to real-world examples is also among our future plans. As a first step, we are currently considering a controller for an automotive air-fuel ratio control system [16].
- Related to the previous topic, we also desire to conduct real-world large-scale empirical studies to gather and analyze metrics related to the proposed strategy for testing CPSs. Based on these empirical studies, we expect to provide practical evidence for the scalability of our proposal.

V. Conclusion

In previous work [11], we presented a conformance testing algorithm for CPSs, based on the (τ,ϵ)-conformance notion defined in [5]. We have shown that conformance verification for this notion is sensitive to the dynamics of system model and to the sampling rate. In order to ensure soundness of the verification, we specified and proved error bounds for a given model and sampling rate, as discussed in the previous section.

In this paper, these previous results were embodied into a potentially scalable, more general, and sound process sketch for checking conformance of CPSs. Particularly, we have explicitly defined the parameters of a modularized process sketch, split into five steps, with the aim of providing support for an engineer to adopt a systematic strategy.

Acknowledgments: The work of M. R. Mousavi has been partially supported by the Swedish Research Council (Vetenskapsradet) award number: 621-2014-5057 (Effective Model-Based Testing of Concurrent Systems) and the Swedish Knowledge Foundation (Stiftelsen for Kunskaps- och Kompetensutveckling) in the context of the AUTO-CAAS HoG project (number: 20140312) and the Strategic Research Environment ELLIIT.

The work of M. Taromirad has been partially supported by the Swedish Research Council (Vetenskapsradet) award number: 621-2014-5057 (Effective Model-Based Testing of Concurrent Systems) and the Strategic Research Environment ELLIIT.

The work of Hugo Araujo, Gustavo Carvalho and Augusto Sampaio was partially supported by the CIn-UFPE/Motorola cooperation project, as well as CNPq grants 303022/2012-4 and 132332/2015-9.

References

[1] R. M. Hierons, K. Bogdanov, J. P. Bowen, R. Cleaveland, J. Derrick, J. Dick, M. Gheorghe, M. Harman, K. Kapoor, P. J. Krause, G. Lüttgen, A. J. H. Simons, S. A. Vilkomir, M. R. Woodward, and H. Zedan, "Using formal specifications to support testing," *ACM Comput. Surv.*, vol. 41, no. 2, 2009. [Online]. Available: http://doi.acm.org/10.1145/1459352.1459354

[2] J. Tretmans, "Model based testing with labelled transition systems," in *Formal Methods and Testing, An Outcome of the FORTEST Network, Revised Selected Papers*, ser. Lecture Notes in Computer Science, vol. 4949. Springer, 2008, pp. 1–38.

[3] T. A. Henzinger, *The Theory of Hybrid Automata*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2000, pp. 265–292. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-59615-5_13

[4] M. Yannakakis and D. Lee, "Testing of finite state systems," in *Computer Science Logic*, ser. Lecture Notes in Computer Science, vol. 1584. Springer Berlin Heidelberg, 1999, pp. 29–44.

[5] H. Abbas, "Test-based falsification and conformance testing for cyber-physical systems," Ph.D. dissertation, Electrical Engineering – Arizona State University, 2015.

[6] M. van Osch, "Automated model-based testing of hybrid systems," Ph.D. dissertation, Eindhoven University of Technology, The Netherlands, 2009.

[7] T. Dang, "Model-based testing of hybrid systems," *Monograph in Model-Based Testing for Embedded Systems, CRC Press*, 2010.

[8] J. V. Deshmukh, R. Majumdar, and V. S. Prabhu, *Quantifying Conformance Using the Skorokhod Metric*. Cham: Springer International Publishing, 2015, pp. 234–250. [Online]. Available: http://dx.doi.org/10.1007/978-3-319-21668-3_14

[9] H. Roehm, J. Oehlerking, M. Woehrle, and M. Althoff, "Reachset conformance testing of hybrid automata," in *Proceedings of the 19th International Conference on Hybrid Systems: Computation and Control, HSCC 2016, Vienna, Austria, April 12-14, 2016*, A. Abate and G. E. Fainekos, Eds. ACM, 2016, pp. 277–286.

[10] N. Khakpour and M. R. Mousavi, "Notions of Conformance Testing for Cyber-Physical Systems: Overview and Roadmap (Invited Paper)," in *26th International Conference on Concurrency Theory (CONCUR 2015)*, ser. Leibniz International Proceedings in Informatics (LIPIcs), L. Aceto and D. de Frutos Escrig, Eds., vol. 42. Dagstuhl, Germany: Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2015, pp. 18–40. [Online]. Available: http://drops.dagstuhl.de/opus/volltexte/2015/5397

[11] M. Mohaqeqi and M. R. Mousavi, "Sound test-suites for cyber-physical systems," in *10th International Symposium on Theoretical Aspects of Software Engineering (TASE 2016)*, ser. IEEE Computer Society, 2016.

[12] P. Caspi and A. Benveniste, *Toward an Approximation Theory for Computerised Control*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002, pp. 294–304. [Online]. Available: http://dx.doi.org/10.1007/3-540-45828-X_22

[13] J. Proakis and D. Manolakis, *Digital Signal Processing*, 4th ed. Pearson, 2006.

[14] A. Aerts, M. R. Mousavi, and M. Reniers, *A Tool Prototype for Model-Based Testing of Cyber-Physical Systems*. Cham: Springer International Publishing, 2015, pp. 563–572. [Online]. Available: http://dx.doi.org/10.1007/978-3-319-25150-9_32

[15] T. Dang and T. Nahhal, "Coverage-guided test generation for continuous andhybrid systems," *Formal Methods in System Design*, vol. 34, no. 2, pp. 183–213, 2009. [Online]. Available: http://dx.doi.org/10.1007/s10703-009-0066-0

[16] J. A. Cook, J. Sun, J. H. Buckland, I. V. Kolmanovsky, H. Peng, and J. W. Grizzle, "Automotive powertrain controla survey," *Asian Journal of Control*, vol. 8, no. 3, pp. 237–260, 2006.