Verification and Validation of Cyber-Electro-Mechanical Vehicles

Position Statement

Xenofon Koutsoukos
Institute for Software Integrated Systems (ISIS)
Vanderbilt University

Verification and validation (V&V) of cyber-electro-mechanical systems is a key enabler to the development of advanced aero-, hydro-, and ground vehicles by dramatically improving system assurance with compressed qualification times. System assurance is extremely challenging because of the high degree of uncertainty and variability during the system operation and interaction with the physical environment. V&V aims at analyzing functional and behavioral correctness in the presence of multiple sources of non-determinism and has a crucial role in model-based design that is based on an iterative progression from requirement models to implementation models using the repeated steps of model construction, verification, and transformation.

In spite of significant progress, V&V of complex cyber-electro-mechanical systems remains a very hard problem. The primary unsolved challenges can be categorized along the following four dimensions: (1) complexity due to highly nonlinear and nondeterministic dynamics, (2) heterogeneity of components and behaviors, (3) scalability due to large number of components, and (4) epistemic uncertainty due to neglecting certain effects in the models because of knowledge gaps. Further, these challenges are coupled and this coupling magnifies the V&V problem. The fundamental gap in V&V is the lack of understanding the interrelations among different abstractions and the lack of methods for the automated composition of multi-abstraction models that are adapted to the property to be verified.

Component-Based Models of Complex Systems

Model-based design of cyber-electro-mechanical systems typically employs component models interconnected through ports. Ports can define (1) physical interactions through exchange of energy, (2) cyber interaction through exchange of information, and (3) cyber-physical interactions through sensing and actuation. For example, tools based on the Modelica language are extensively used in the design of such systems. Typical component models in this framework are developed for simulation purposes and they are not amenable to V&V methods. The major obstacle is that the behavioral semantics is defined in an operational manner reflected only in the execution traces. V&V requires the generation of an extremely large number of traces and does not scale to large systems operating in the presence of uncertainty and non-determinism. An alternative approach is to transform component-based simulation models to formal models with denotational semantics that allow the application of V&V methods. The challenge is to use a representation that can capture complex nonlinear and nondeterministic phenomena while at the same time supporting formal verification methods.

Our work uses a port-Hamiltonian approach for modeling complex systems which (1) is based on the concept of the port for defining interactions, (2) is multi-physics supporting electro-mechanical systems, (3) captures nonlinearities present in real systems, and (4) has equivalent representations with well-defined denotational semantics [1]. Central to the approach is the notion of a Dirac structure, which is a representation of the power conserving interconnection

structure of the system. The dynamics of a port-Hamiltonian system is specified by the constraints on the various port variables imposed by the Dirac structure which in a coordinate representation generally will consist of a mixed set of differential and algebraic equations.

The objective is to develop abstractions that preserve notions related to energy storage in the components and energy exchange between components. Such abstractions are developed based on passivity that can be used for design and analysis of cyber-physical systems [2]. In addition, a well-known method for stability analysis in Hamiltonian systems is to consider candidate Lyapunov functions within the class of combinations of the Hamiltonian function and dynamic invariants representing conserved quantities [1]. Such Lyapunov functions can be used to obtain discrete abstractions that approximate the dynamical behavior and are amenable to V&V methods.

Model Validation and Robust Verification

Model validation is necessary to account for uncertainty in the design and manufacturing processes. V&V methods rely on the credibility of predictive modeling. Computational models are used to predict system behavior which is not tested experimentally. Assessment of the model's predictive accuracy must be based on the following aspects: (1) improved fidelity-to-data which ensures reproducibility of past experiments using simulations, (2) robustness-to-uncertainty which is ensured that a system property is robustly satisfied in the presence of uncertainty and lack of knowledge, and (3) confidence in prediction which limits the range of predicted values from the model [3].

Selection of the model parameters to optimize fidelity-to-data does not take into account uncertainty and epistemic gaps. On the other hand, maximizing robustness-to-uncertainty may lead to large range of predicted values or even inconsistent predictions. Model validation methods must select ranges of model parameters that trade-off these criteria. The proposed V&V framework will consider uncertainty in the model parameters and employ measures that estimate how robustly a property is satisfied by a system model.

Tool Development and Integration

V&V can impact design of vehicles if technology advances are implemented in comprehensive tools that enable V&V automation. Our objective is to develop tools that demonstrate the proposed V&V methods and integrate them into existing modeling tools like Modelica.

References

[1] V. Duindam, A. Macchelli, S. Stramigioli, and H. Bruyninckx, (Eds.). *Modeling and Control of Complex Physical Systems: The Port-Hamiltonian Approach*. Springer, 2009.

[2] X. Koutsoukos, N. Kottenstette, J. Hall, E. Eyisi, H. LeBlanc, J. Porter, and J. Sztipanovits. "A Passivity Approach for Model-Based Compositional Design of Networked Control Systems", *ACM Transactions on Embedded Computing Systems, Special Issue on the Synthesis of Cyber-Physical Systems,* 11(4), December 2012.

[3] Y. Ben-Haim, and F. M. Hemez, "Robustness-to-uncertainty, fidelity-to-data, and prediction-looseness of models," *Proceedings of the 22nd IMAC*, Dearborn, MI, 2004.