Artificial Intelligence for Simulation-based Design of Cyber-Physical Systems

Toni Mancini, Igor Melatti, Enrico Tronci
Model Checking Lab
Department of Computer Science
Sapienza University of Rome, Italy
{ tmancini | melatti | tronci }@di.uniroma1.it

Abstract

Design of Cyber-Physical Systems (CPSs) heavily rests on simulation in order to test the software without damaging the physical devices and in order to effectively explore the design space.

Both activities can actually be cast as optimization problems where a *worst case* is sought (as for software *verification*) or a *best case* is sought (as for design optimization). In both cases then AI techniques can be effectively used to save on the verification and design optimization times.

In this short paper we review some of the research activities carried out on these topics at the Model Checking Lab of the Department of Computer Science, Sapienza University of Rome, Italy.

1 Research Themes

We have developed a set of AI based methods and tools to save time and cost in the design and Verification & Validation (VV) of safety or mission critical systems. Our main focus is on simulation based design, since, through *Digital Twins*, this is most effective approach in our setting. Here is a short outline of the main topics we addressed recently.

1. Design of distributed control strategies for complex systems. An example is in the activity described in Section 1.1.
2. Uniform sampling of solutions from a set of temporal constraints. An example is in the activity described in Section 1.2.
3. Enable the use of search heuristics in a simulation setting by developing tools to *save and restore* the simulation state. An example is in the activity described in Section 1.3.

1.1 A Two-Layer Near-Optimal Strategy for Substation Constraint Management via Home Batteries

Within electrical distribution networks, substation constraints management requires that aggregated power demand from residential users is kept within suitable bounds. Efficiency of substation constraints management can be measured as the reduction of constraints violations with respect to unmanaged demand.

Home batteries hold the promise of enabling efficient and user-oblivious substation constraints management. Centralized control of home batteries would achieve optimal efficiency. However, it is hardly acceptable by users, since service providers (e.g., utilities or aggregators) would directly control batteries at user premises.

Unfortunately, devising efficient hierarchical control strategies, thus overcoming the above problem, is far from easy. We have devised a novel two-layer control strategy for home batteries that avoids direct control of home devices by the service provider and at the same time yields near-optimal substation constraints management efficiency.

Our simulation results on field data from 62 households in Denmark show that the substation constraints management efficiency achieved with our approach is at least 82% of the one obtained with a theoretical optimal centralized strategy.

Further details on this research activity are available in [2]

1.2 Any-horizon uniform random sampling and enumeration of constrained scenarios for simulation-based formal verification

Approaches to the verification of non-terminating CPSs usually rely on numerical simulation of the System Under Verification (SUV) model under input scenarios of possibly varying duration, chosen among those satisfying given constraints.

Such constraints typically stem from requirements (or assumptions) on the SUV inputs and its operational environment as well as from the enforcement of additional conditions aiming at, *e.g.*, *prioritizing* the (often extremely long) verification activity, by, *e.g.*, focusing on scenarios explicitly exercising selected requirements, or avoiding vacuity in their satisfaction.

In this setting, the possibility to efficiently sample at random (with a known distribution, *e.g.*, uniformly) within, or to efficiently enumerate (possibly in a uniformly random order) scenarios among those satisfying all the given constraints is a key enabler for the practical viability of the verification process, *e.g.*, via simulation-based statistical model checking.

Unfortunately, in case of non-trivial combinations of constraints, iterative approaches like Markovian random walks in the space of sequences of inputs in general fail in extracting scenarios according to a given distribution (*e.g.*, uniformly),

and can be very inefficient to produce at all scenarios that are both legal (with respect to SUV assumptions) and of interest (with respect to the additional constraints).

For example, there are cases where up to 91% of the scenarios generated using such iterative approaches would need to be neglected because illegal or of no interest for testing.

In this activity we have shown that, given a set of constraints on the input scenarios succinctly defined by multiple finite memory monitors, a data structure (scenario generator) can be synthesised, from which any-horizon scenarios satisfying the input constraints can be efficiently extracted by (possibly uniform) random sampling or (randomised) enumeration.

Our approach enables seamless support to virtually all simulation-based approaches to CPS verification, ranging from simple random testing to statistical model checking and formal (i.e., exhaustive) verification, when a suitable bound on the horizon or an iterative horizon enlargement strategy is defined, as in the spirit of bounded model checking.

Further details on this research activity are available in [1].

1.3 Reconciling interoperability with efficient Verification and Validation within open source simulation environments

A CPS comprises physical as well as software subsystems. Simulation-based approaches are typically used to support design and VV of CPSs in several domains such as: aerospace, defence, automotive, smart grid and healthcare. Accordingly, many simulation-based tools are available to support CPS design. This, on one side, enables designers to choose the toolchain that best suits their needs, on the other side poses huge interoperability challenges when one needs to simulate CPSs whose subsystems have been designed and modelled using different toolchains.

To overcome such an interoperability problem, in 2010 the Functional Mock-up Interface (FMI) has been proposed as an open standard to support both *Model Exchange* (ME) and *Co-Simulation* (CS) of simulation models created with different toolchains.

FMI has been adopted by several modelling and simulation environments. Models adhering to such a standard are called Functional Mock-up Units (FMUs). Indeed FMUs play an essential role in defining complex CPS through, *e.g.*, the *System Structure and Parametrisation* (SSP) standard.

Simulation-based VV of CPSs typically requires exploring different simulation scenarios (*i.e.*, exogenous input sequences to the CPS under design). Many such scenarios have a shared prefix. Accordingly, to avoid simulating many times such shared prefixes, the simulator state at the end of a shared prefix is saved and then restored and used as a start state for the simulation of the next scenario. In this context, an important FMI feature is the capability to save and restore the internal FMU state on demand. This is crucial to increase efficiency of simulation-based VV.

Unfortunately, the implementation of this feature is not mandatory and it is available only within some commercial software. As a result, the interoperability enabled by the FMI standard cannot be fully exploited for VV when using open-source simulation environments.

This motivates developing such a feature for open-source CPS simulation environments. Accordingly, in this activity, we focused on JModelica, an open-source modelling and simulation environment for CPSs based on an open standard modelling language, namely Modelica.

We have endowed JModelica with our open-source implementation of the FMI 2.0 functions needed to save and restore internal states of FMUs for Model Exchange. Through 934 publicly available benchmark models, we evaluated correctness and efficiency of our extended JModelica. Our experimental results show that simulation-based VV is, on average, 22 times faster with our get/set functionality than without it.

Further details on this research activity are available in [3].

2 Projects

Energy Demand Aware Open Services for Smart Grid Intelligent Automation (SMARTHG)

- Funding agency: European Commission (FP7-ICT-2011-8)
- Project funding: Eur 3,299,998.00.
- Project web-site: http://smarthg.di.uniroma1.it/

A System for Detection of Hostile UAV (SCAPR)

- POR FESR 2014-2020, Aerospace and Security
- Project funding: Eur 340,234.31.
- Project web-site: http://mclab.di.uniroma1.it/site/index.php/projects/57-scapr-por-fesr-2014-2020-aerospazio-e-sicurezza

Satellite Driven Fire Simulator (SDFS)

- POR FESR 2014-2020, Aerospace and Security
- Project funding: Eur 250,000.00.
- Project web-site: http://mclab.di.uniroma1.it/site/index.php/projects/60-sdfs-por-fesr-2014-2020-aerospazio-e-sicurezza

3 Software Tools

FMU 2.0 for JModelica This is the tool outlined in Section 1.3. It is available in https://bitbucket.org/mclab/jmodelica.org .

SyLVer SyLVer is a software allowing System Level Formal Verification (SLFV) of Cyber Physical Systems (CPSs). SyLVer implements an assume-guarantee approach to the problem of SLFV. It is available in http://mclab.di.uniroma1.it/site/index.php/software/49-sylver .

4 Challenges and future work

We are extending our methods and technologies to enable automatic learning of the constraints for the admissible operational scenarios. This would significantly ease the definition of the set of admissible operational scenarios for the system under verification.

References

[1] Toni Mancini, Igor Melatti, and Enrico Tronci. Any-horizon uniform random sampling and enumeration of constrained scenarios for simulation-based formal verification. *IEEE Transactions on Software Engineering*, 2021.

[2] Igor Melatti, Federico Mari, Toni Mancini, Milan Prodanovic, and Enrico Tronci. A two-layer near-optimal strategy for substation constraint management via home batteries. *IEEE Transactions on Industrial Electronics*, 2021.

[3] Stefano Sinisi, Vadim Alimguzhin, Toni Mancini, and Enrico Tronci. Reconciling interoperability with efficient verification and validation within open source simulation environments. *Simulation Modelling Practice and Theory*, 109, 2021.