ADVANCES IN CYBER-PHYSICAL SYSTEMS

Vol. 3, No. 1, 2018

ON THE APPROACHES TO CYBER-PHYSICAL SYSTEMS SIMULATION

Vadym Shkarupylo, Ravil Kudermetov, Olga Polska

Department of Computer Systems and Networks,
Zaporizhzhia National Technical University, Zaporizhzhia
Author's e-mail: *shkarupylo.vadym@gmail.com*

Submitted on 07.12.2018

Abstract: **A comparative analysis of existing approaches to Cyber-Physical Systems simulation has been conducted. The intrinsic peculiarities of Cyber-Physical Systems have been reasoned and generalized. The limitations of available simulation tools have been pointed out. The approach to Cyber-Physical Systems design solutions checking on the basis of timed automata, UPPAAL integrated tool environment and Temporal Logic of Actions usage has been proposed. The proposed approach is supposed to be applied at designing stage – to prevent the potential time and computational expenses on overcomplicated or faulty formal models checking. A case study on electric power delivery system usage scenario has been conducted.**

***Index Terms*: Cyber-Physical System, Model, Model Checking, Simulation, TLA, UPPAAL, Verification.**

I. INTRODUCTION

Nowadays, on the verge of manufacturing industry transformation into Industry 4.0, the concept of Cyber-Physical System (CPS) is thoroughly exploited in different domains [1]. It is known that CPSs are the integration of computation and physical processes. Moreover, it is stated that the key principle to follow during the designing of CPSs is that the components at any level of abstraction should, if possible, be made predictable and reliable [2].

The CPS can also be characterized as a system with a tight relation between the digital computing component and a continuous-time dynamical system – the physical layer; there are plenty of examples of such systems, e.g., an auto pilot, anti-lock breaking system (ABS) etc. [3].

Taking into consideration the intrinsic features of CPSs, e.g., concurrency, heterogeneity and timings sensitivity [4], bringing the simulation of such systems into practice is a non-trivial task to be resolved.

There are plenty of diverse approaches to CPSs modeling and simulation to be conducted during the designing in particular. It is stated that typical CPS is supposed to be a large-scale distributed system composed from the communicating devices, and to successfully model the cyber and physical layers in conjunction, the Modelica framework is proposed to be used [5]. The accent is put here on timings simulation, but scale and scalability aspects – especially in terms of numerous communicating devices of the composition – are left behind.

With an accent on production scenarios, the concept of Cyber-Physical Production System (CPPS), to be implemented in future “Smart Factories”, arises. Corresponding simulation tools are supposed to accelerate and optimize the phases of production lifecycle – to support the processes of engineering and decision making [6].

Apart from the accent on timings simulation, e.g., the aforementioned Modelica framework [5], there are the approaches encompassing the aspects of devices heterogeneity and reusability of the models of subsystems – a system-of-systems (SoS) approach to formal modeling of CPS [7]. Moreover, it is stated that, despite the existence of various simulation tools, only few of them, e.g., Ptolemy II, LabVIEW, are capable to capture the interactions between the heterogeneous subsystems [8].

Taking the scale and heterogeneity aspects of CPSs in mind, the need for a generalized framework for CPSs design, modeling and simulation has been stated [9]. And the requirements to such a framework have also been formulated: the support of heterogeneity (in terms of variation of sensors and actuators types), scalability, mobility, usability, integration of existing simulation tools, integration of proprietary solutions with open ones, software reuse, and also the support of various physical modeling environments. It should be noted though that an attempt to bring into life such an all-around comprehensive solution can be characterized skeptically as an idealized goal requiring potentially an enormous efforts and resources – just taking into consideration the perspectives to provide the interoperability between proprietary and open solutions.

Analyzing the given list of requirements, it can be concluded that to make certain approach to CPSs designing, modeling and/or simulation more feasible, the

The work has been conducted as a part of Erasmus+ Internet of Things: Emerging Curriculum for Industry and Human Applications ALIOT Project (reference number 573818-EPP-1-2016-1-UK-EPPKA2-CBHE-JP), participated by the Department of Computer Systems and Networks (CSN) of Zaporizhzhia National Technical University (Ukraine).

V. V. Shkarupylo is with the Department of Computer Systems and Networks, Zaporizhzhia National Technical University, Zaporizhzhia, 69063, Ukraine (e-mail: shkarupylo.vadym@gmail.com).

R. K. Kudermetov is with the Department of Computer Systems and Networks, Zaporizhzhia National Technical University, Zaporizhzhia, 69063, Ukraine (e-mail: kudermetov@gmail.com).

O. V. Polska is with the Department of Computer Systems and Networks, Zaporizhzhia National Technical University, Zaporizhzhia, 69063, Ukraine (e-mail: ol.polsk@gmail.com)

list of requirements should be shortened, bringing to the first-order position the accounting of solely native features of CPSs, e.g., heterogeneity and scale.

Generalizing the aforesaid it should be noted that the approaches considered are devoted to the designing stage of engineering process. During the designing of CPS, plenty of artifacts, e.g., formal models, are obtained to check and/or refine the design solutions. This process is tightly bound with diverse formal verification techniques, e.g., the model checking methods [10], usage.

The model checking technique is considered to be the most preferable tool for design solutions correctness checking because of its automation – a critical point in terms of the scale and the complexity of CPSs.

II. RELATED WORK

A brief look at CPS modeling and simulation applicability, e.g., automatic CPSs models abstraction, numerical simulation, has been given previously [11].

Taking into consideration the scale and the complexity, and the analog nature of physical layer of CPSs, it seems to be natural to speculate on the non-deterministic properties of these systems. Moreover, non-deterministic models are significantly less complex and can encompass many of system's behaviors. On contrary, deterministic models are significantly more complex and can represent only a single behavior at most [12]. Reasoning in terms of non-deterministic models, it should be noted that model checking technique on the basis of FSM (Finite-state Machine) has already proved itself to be a plausible solution: checking the design solutions for Amazon Web Services [13], implementing the Temporal Logic of Actions (TLA), corresponding TLA+ formalism and TLC (TLA Checker) model checker [14]; specifying and verifying the rules of Firewall (on the basis of TLA) [15]; modeling and developing the fault-tolerant safety-critical modules for a platform for railway control applications up to safety integrity level 4 (on the basis of TLA) [16].

It has been shown previously that, because of the exponential growth of state space, the limitation of computational and time resources can be faced [17]. More or less, these expenses can be diminished – by choosing the right way of model checking method implementation, e.g., the Depth-first Search-based approach over the Breadth-first Search-based one [18]. Nevertheless, the verification-related computations are directly dependent on the complexity of formal models, and, because of the exponential growth of state space, can be overabundant and/or inexpedient. To diminish the effect of such scenarios, the preventive simulation on the basis of simplified model is proposed to be conducted.

III. PROBLEM STATEMENT

Grounding on the analysis conducted, it can be stated that, despite the plethora of applicability scenarios the model checking methods can potentially be or have successfully been utilized in, there is still a significant drawback taking place – an exponential growth of state space from the number of state variables. To this end, the preventive sanity checking of CPS formal model (specification) by way of simulation is proposed to be conducted – to potentially prevent or lower the verification-related time costs and computational expenses. This lowering can be achieved on the basis of simulation results – by formal model refinement prior to the time consuming verification by way of model checking.

IV. APPROACH AND CASE STUDY

To do the preventive simulation, the CPS is proposed to be represented as a timed automaton (TA) [19]:

$$\langle L, l_0, C, A, E, I \rangle, \tag{1}$$

where L – set of locations; $l_0 \in L$ – initial location; C – set of clocks; A – set of actions; $E \subseteq L \times A \times B(C) \times 2^C \times L$ – set of edges between locations with an action, a guard and a set of clocks to be reset; $B(C)$ – set of conjunctions over simple conditions of the form $x \lozenge c$ or $(x-y)\lozenge c$, $x, y \in C$, $c \in N$, $\lozenge \in \{<, \le, =, \ge, >\}$; $I : L \to B(C)$ – function assigning the invariants to locations.

It can be seen that model (1) is focused on timings, leaving behind such aspects as heterogeneity, scalability etc. [9]. To widen the range of requirements the proposed approach satisfies, it has been proposed to use the formal specification of CPS on the basis of TLA+ formalism as a starting point [14]. Due to mathematical strictness, modularity and a wide range of applicability scenarios of TLA [13, 15, 16], corresponding TLA+ formalism and TLC model checking method have been chosen to be the building blocks of the approach.

The activity diagram representing the proposed approach is given in Fig. 1.

In Fig. 1 the TA-model is the timed automaton (1). The UPPAAL integrated tool environment provides both the simulator and the model checker [20]. During the case study conducted, it has been acknowledged that built-in simulator provides a good level of usability and demonstrativeness, but corresponding model checker seems to be not enough in terms of modularity and scalability – taking into consideration the intrinsic peculiarities of CPSs, e.g., scale.

With respect to the proposed approach, the physical and cyber layers of CPS are proposed to be modeled in conjunction. To this end, the control system (controller) and physical equipment layers of CPS architecture have been contemplated [21]. The electric power delivery system (EPDS) functioning scenarios have been considered as a case study (Fig. 2).

In Fig. 2, with respect to the scenarios of EPDS functioning, the three locations of TA-model of controller are represented (1): $l_0 \in L$ – power generation exceeds the consumption, with no accumulation; $l_1 \in L$ – power generation exceeds the consumption, plus the accumulation; $l_2 \in L$ – power consumption exceeds the generation, plus the accumulation. The $s!$ label means that corresponding edge has been synchronized with an edge labeled with $s?$ (Fig. 3). Each scenario is supposed to be obtained from corresponding behavior, specified in TLA+ specification [22].

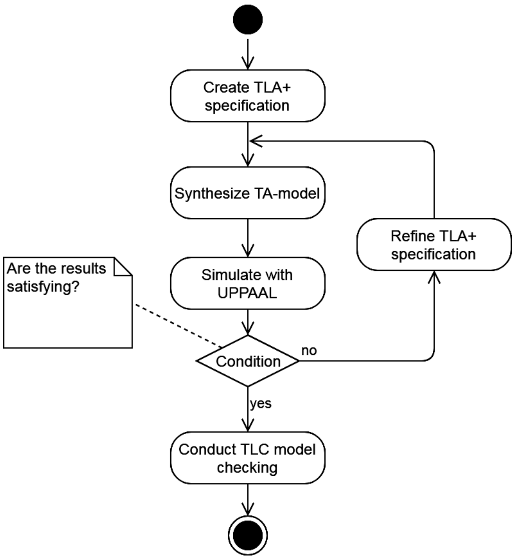

Create TLA+ specification
Synthesize TA-model
Refine TLA+ specification
Are the results satisfying?
Simulate with UPPAAL
Condition
no
yes
Conduct TLC model checking

Fig. 1. Activity diagram for the proposed approach

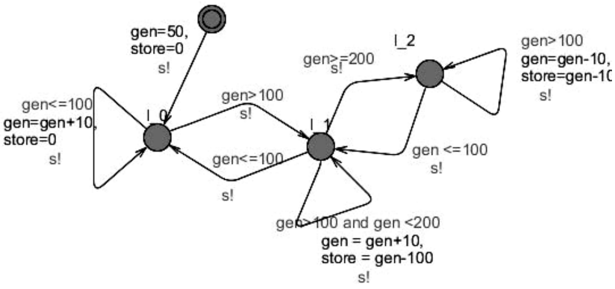


Fig. 2. TA-model of the controller

In Fig. 3 – $L = \{l_0, l_1\}$ – the edges, labeled with $s?$ mark, mean that corresponding transitions are dependent on the transitions taking place in the controller model.

The simulation conducted has proved the behavioral sanity of CPS design at chosen abstraction level. This means that corresponding TLA-based formal model can be checked with TLC in an automated manner. The template of TLA+ specification is given in [22]. The corresponding verification-related time costs and computational expenses are covered in [17] and [18].

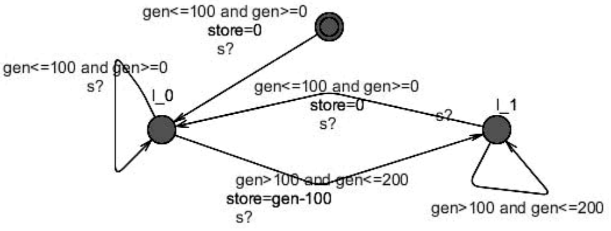


Fig. 3. TA-model of physical equipment layer

Thus, the proposed approach demonstrates the flexibility towards facing the state space explosion problem by preventing the overabundant time and computational expenses by way of preventive simulation in UPPAAL environment.

V. CONCLUSIONS

Thus, the comparative analysis of the approaches to CPSs modeling and simulation has been conducted and the approach to CPS design solutions checking has been proposed.

The following results have been obtained:

The expediency of simulation prior the model checking of CPS design solutions has been substantiated. It has been stated that conducting the sanity checking prior to the exhaustive state space search during the model checking can potentially prevent the unreasonable expenses of time and computational resources on verification of overcomplicated formal models.

The approach to CPS design solutions checking, accented on the aspects of timings and scalability and grounded on the representation of CPS design as timed automaton, intended to be obtained from TLA+ specification, has been proposed. The proposed approach is supposed to be applied during the designing of CPSs to prevent the unreasonable expenses of time and computational resources on verification.

To demonstrate the applicability of proposed approach, a case study on the electric power delivery system simulation has been conducted. To conduct the simulation, the UPPAAL integrated tool environment has been used.

Future work is aimed at development of the technique providing the automated translation of TLA+ specification of CPS to a timed automaton.

VI. ACKNOWLEDGMENT

The work has been conducted as a part of Erasmus+ Internet of Things: Emerging Curriculum for Industry and Human Applications ALIOT Project (reference number 573818-EPP-1-2016-1-UK-EPPKA2-CBHE-JP), participated by the Department of Computer Systems and Networks (CSN) of Zaporizhzhia National Technical University (Ukraine).

REFERENCES

[1] J. Lee, B. Bagheri, and H.-A. Kao, “A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems”, *Manufacturing Letters*, vol. 3, pp. 18–23, Jan. 2015.

[2] E. A. Lee, “Cyber Physical Systems: Design Challenges”, in Proc. 2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC), Orlando, FL, USA, 2008, pp. 363–369.

[3] E.M. Clarke and P. Zuliani, “Statistical Model Checking for Cyber-Physical Systems”, *ATVA 2011, Lecture Notes in Computer Science*, vol. 6996, pp. 1–12, 2011.

[4] P. Derler, E. A. Lee, and A. S. Vincentelli, “Modeling cyber-physical systems”, *Proceedings of the IEEE*, vol. 100, no. 1, pp. 13–28, Jan. 2012.

[5] D. Henriksson and H. Elmqvist, “Cyber-Physical Systems Modeling and Simulation with Modelica”, in *Proc. 8th Modelica Conference*, Dresden, Germany, 2011, pp. 502–509.

[6] S. Weyer, T. Meyer, M. Ohmer, D. Gorecky, and D. Zühlke, "Future Modeling and Simulation of CPS-based Factories: an Example from the Automotive Industry", *IFAC-PapersOnLine*, vol. 49, no. 31, pp. 97–102, 2016.

[7] K. H. Lee, J. H. Hong, and T. G. Kim, "System of Systems Approach to Formal Modeling of CPS for Simulation-Based Analysis", *ETRI Journal*, vol. 37, no. 1, pp. 175–185, Feb. 2015.

[8] J. C. Jensen, D. H. Chang, and E. A. Lee, "A model-based design methodology for cyber-physical systems", in *Proc. 2011 7th International Wireless Communications and Mobile Computing Conference*, Istanbul, Turkey, Jul. 2011, pp. 1666–1671.

[9] J. E. Kim and D. Mosse, "Generic framework for design, modeling and simulation of cyber physical systems", *ACM SIGBED Review*, vol. 5, no. 1, pp. 1–2, Jan. 2008.

[10] E.M. Clarke, O. Grumberg, and D.A. Peled, *Model Checking*. Massachusetts: MIT Press, 2001, 309 p.

[11] J. Shi, J. Wan, H. Yan, and H. Suo, "A survey of cyber-physical systems", in *Proc. 2011 International Conference on Wireless Communications and Signal Processing (WCSP)*, Nanjing, China, Nov. 2011, pp. 1–6.

[12] E.A. Lee, "The Past, Present and Future of Cyber-Physical Systems: A Focus on Models", *Sensors*, vol. 15, no. 3, pp. 4837–4869, 2015.

[13] C. Newcombe, T. Rath, F. Zhang, B. Munteanu, M. Brooker, and M. Deardeuff, "How Amazon web services uses formal methods", *Communications of the ACM*, vol. 58, no. 4, pp. 66–73, 2015.

[14] L. Lamport, *Specifying Systems: The TLA+ Language and Tools for Hardware and Software Engineers*. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 2002, 348 p.

[15] Y-M. Kim, M. Kang, and J-Y. Choi, "Formal Specification and Verification of Firewall using TLA+", in *Proc. 2017 International Conference on Security and Management, SAM'17*, Las Vegas, Nevada, USA, Jul. 2017, pp. 247–251.

[16] S. Resch and M. Paulitsch, "Using TLA+ in the Development of a Safety-Critical Fault-Tolerant Middleware", in *Proc. 2017 IEEE International Symposium on Software Reliability Engineering Workshops, ISSREW 2017*, Toulouse, France, Oct. 2017, pp. 146–152.

[17] V. V. Shkarupylo, I. Tomicic, K. M. Kasian, and J. A. J. Alsayaydeh, "An Approach to increase the Effectiveness of TLC Verification with Respect to the Concurrent Structure of TLA+ Specification", *International Journal of Software Engineering and Computer Systems*, vol. 4, no. 1, pp. 48–60, 2018.

[18] V. V. Shkarupylo, I. Tomicic, and K. M. Kasian, "The investigation of TLC model checker properties", *Journal of Information and Organizational Sciences*, vol. 40, no. 1, pp. 145–152, 2016.

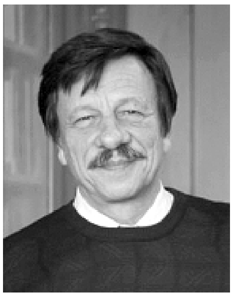
[19] G. Behrmann, A. David, and K.G. Larsen, "A Tutorial on Uppaal", Formal Methods for the Design of Real-Time Systems. SFM-RT 2004. Lecture Notes in Computer Science, vol. 3185, pp. 200–236, 2004.

[20] J.H. Kim, K.G. Larsen, B. Nielsen, M. Mikucionis, and P. Olsen, "Formal Analysis and Testing of Real-Time Automotive Systems Using UPPAAL Tools", *Formal Methods for Industrial Critical Systems. FMICS 2015. Lecture Notes in Computer Science*, vol. 9128, pp. 47–61, 2015.

[21] Y. Liu, Y. Peng, B. Wang, S. Yao, and Z. Liu, "Review on cyber-physical systems", *IEEE/CAA Journal of Automatica Sinica*, vol. 4, no. 1, pp. 27–40, 2017.

[22] V. Shkarupylo and O. Polska, "The Approach to SDN Network Topology Verification on a Basis of Temporal Logic of Actions", in *Proc. 14th Int. Conf. on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, TCSET'2018*, Lviv-Slavske, Ukraine, Feb. 2018, pp. 183–186.

Vadym Shkarupylo was born in 1988 in Zaporizhzhia, Ukraine. He obtained his PhD degree in Pukhov Institute for Modelling in Energy Engineering of National Academy of Sciences of Ukraine, Kyiv, Ukraine, in 2014. He has been working at the Department of Computer Systems and Networks, Zaporizhzhia National Technical University, Zaporizhzhia, Ukraine, since September 2011. He has been working as the Associate Professor of the Department of Computer Systems and Networks, Zaporizhzhia National Technical University, Zaporizhzhia, Ukraine, since October 2015.



Ravil Kudermetov was born in 1952 in Kerki, Turkmenistan. He obtained his PhD degree in Pukhov Institute for Modelling in Energy Engineering of National Academy of Sciences of Ukraine, Kyiv, Ukraine, in 1996. He has been working as the Associate Professor at the Zaporizhzhia National Technical University, Zaporizhzhia, Ukraine, since September 1998. He has been working as a Head of the Computer Systems and Networks Department, Zaporizhzhia National Technical University, since February 2002.

Olga Polska was born in 1968 in Zaporizhzhia, Ukraine. She has been working at the Zaporizhzhia National Technical University, Zaporizhzhia, Ukraine, since 2000. She has been working as the Senior Lecturer of the Department of Computer Systems and Networks, Zaporizhzhia National Technical University, since 2013.