



HAL
open science

Hippo-CPS: Verification of Boundedness, Safeness and Liveness of Petri Net-Based Cyber-Physical Systems

Marcin Wojnakowski, Mateusz Poplawski, Remigiusz Wiśniewski, Grzegorz Bazydło

► **To cite this version:**

Marcin Wojnakowski, Mateusz Poplawski, Remigiusz Wiśniewski, Grzegorz Bazydło. Hippo-CPS: Verification of Boundedness, Safeness and Liveness of Petri Net-Based Cyber-Physical Systems. 13th Doctoral Conference on Computing, Electrical and Industrial Systems (DoCEIS), Jun 2022, Caparica, Portugal. pp.74-82, 10.1007/978-3-031-07520-9_7 . hal-04308398

HAL Id: hal-04308398

<https://inria.hal.science/hal-04308398>

Submitted on 27 Nov 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution 4.0 International License



This document is the original author manuscript of a paper submitted to an IFIP conference proceedings or other IFIP publication by Springer Nature. As such, there may be some differences in the official published version of the paper. Such differences, if any, are usually due to reformatting during preparation for publication or minor corrections made by the author(s) during final proofreading of the publication manuscript.

Hippo-CPS: Verification of Boundedness, Safeness and Liveness of Petri Net-based Cyber-Physical Systems

Marcin Wojnakowski, Mateusz Popławski, Remigiusz Wiśniewski,
Grzegorz Bazydło

Institute of Control and Computation Engineering, University of Zielona Góra,
65-516 Zielona Góra, Poland

{m.wojnakowski, m.poplawski, r.wisniewski, g.bazydlo}@issi.uz.zgora.pl

Abstract. The paper describes the Hippo-CPS tool in the verification of Petri net-based cyber-physical systems. In particular, verification of the key properties such as boundedness, safeness and liveness is presented and discussed. Hippo-CPS allows for analysis of the control part of the CPS with the set of various algorithms (such as reachability tree exploration or place invariants computation) giving the designer an opportunity to select the most suitable technique. Each method is based on the theoretical background (with adequate algorithms, theorems, and proofs, described in other Authors' works). Moreover, the efficiency and effectiveness of the presented methods were verified experimentally.

Keywords: Petri nets, boundedness, safeness, liveness, verification, analysis, cyber-physical systems.

1 Introduction

Petri net is a fruitful modelling technique used for the graphical specification of broadly defined control systems [1], [2]. It is supported by methods toward verification, validation, and analysis that enable checking the correctness and reliability of the prototyped system [3]–[6]. The broad possibilities of formal verification of Petri net-based systems [7] have formed them popular in numerous areas of life, including embedded systems [8], manufacturing systems [9], [10], management systems [11], logic controllers [12], smart homes [13], transport management [14] and cyber-physical system (CPS) [15]. The latter consolidates computational and physical components [16]. Industry 4.0 could benefit from CPS concept [17]. CPS emphasizes the interactions between control (cyber) and physical parts of the system. The Petri net-based approach focuses on the modelling of the control part of the CPS [18]. Moreover, this approach applies the system analysis methods at the earlier specification stage, which permits to reduce the time and cost of prototyping the entire control system [19]. The main properties of CPS described by Petri nets are boundedness, safeness, and liveness [2], [4]–[6], [18], [19]. A bounded Petri net ensures that the model has a finite number of reachable states in the system [20]. A safe model establishes the behaviour of the control part [21], [22]. The

liveness is responsible for the absence of deadlocks in the system [23]. In addition, several design techniques are dependent on algorithms that require bounded, safe, or live Petri nets as their input, e.g., [24], [25], [18].

There are two wide-known analysis approaches that allow examining the boundedness, safeness, and liveness of Petri nets. The first one is based on the reachability tree exploration [26], while the second one applies the methodology of linear algebra for instance by calculating place invariants [27]. However, both techniques have serious limitations, since the number of reachable states in the reachability tree or invariants can be exponential [7], which in practice means that results may not be found within the assumed time [5], [6]. It is claimed that the method is not efficient in that case.

This paper describes the modules of the Hippo-CPS tool for efficient and effective analysis of boundedness, safeness, and liveness properties. The main contributions can be summarized as follows:

- proposition and description the module of the Hippo-CPS tool aimed at the liveness verification of the Petri net-based CPS;
- proposition and description two (alternate) modules of the Hippo-CPS tool aimed at the safeness verification the Petri net-based CPS;
- proposition and description two (alternate) modules of the Hippo-CPS tool aimed at the boundedness verification of the Petri net-based CPS;
- the presented modules are based on the authors' algorithms;
- the efficiency and effectiveness of the presented modules were verified experimentally with the set of 242 test-modules (benchmarks).

2 Technological Innovation for Digitalization and Virtualization

The ongoing industrial revolution 4.0 is dominated by smart and intelligent devices. This is the effect of the processes currently taking places like an intense digitalization and digital transformation of all sectors of society. This transformation and digitalization are supported by the development of efficient, flexible, agile, and sustainable solutions. The cyber-physical systems also will play a big role in these processes of the 4th industrial revolution [17], because they are designed in terms of efficiency, flexibility, and low energy consumption. On the other hand, the modern CPSs are very often complex, concurrent, and hierarchical (modular), and designing their control parts without efficient and effective methods and tools is nowadays rather impossible.

The Hippo-CPS tool presented in the paper attempts to fulfil these requirements. It offers the modules for the analysis of boundedness, safeness, and liveness of Petri net (used for describing the control part of the CPS). The implemented innovative analysis methods are efficient (in some cases even sixty times faster than the classic method) and effective (i.e., could obtain results for the benchmarks, where the popular methods were not able to complete the task within one hour).

3 Related Tools

There are many tools that permit for analysis of the boundedness, safeness, and liveness properties of the Petri net-based system. Let us present selected ones from 25 tools examined by us, that can be applied to the verification of the Petri net properties.

IOPT-Tools [28], [29] is one of the most functional and well-developed software for creating, editing, and analysing Petri nets. The simulator component allows for performing advanced manual analysis of the model. IOPT-Tools can also automatically analyse typical Petri net properties such as boundness, safeness, and occurrence of deadlocks, but the verification of the net properties is based only on the state-space exploration. The limitation of the tool is that the broader analytical research of the model is impossible like place invariants coverage. Hence, the checking properties of some Petri net models cannot be accomplished efficiently.

PIPE2 is an open-source Petri net editor and analysis software. An advantage of the tool is open access to the source code and the possibility to develop own analysis modules or edit existing ones. The tool enables, among others, verification of boundedness, safeness, deadlocks occurrence, determination of the Petri net class, computation of place and transitions invariants, and determination of siphons. Furthermore, PIPE generates a graphical representation of the reachability graph. On the other hand, the limitations of the functionalities are the lack of the strict liveness analysis, and problems with the state-space analysis module. Using the latter feature causes the exponential computation, which for relatively small models (about twenty places and transitions) can end with application error or suspension of the program.

CPN Tools is a common system for creating, editing, and analysing Petri net models. It is not only limited to coloured Petri nets but also applicable to other classes of Petri nets. The latest version (4.0.1) of the tool was released 7 years ago. Using the program could be quite complicated for a new user, and probably without studying extensive documentation, performing the simulation or analysis of the modelled Petri net is impossible. However, the documentation and user guide are available on the official website of the tool.

Yasper is a simple graphical tool with a Petri net simulation module. The graphical user interface (GUI) appears to be friendly and accessible. However, the tool has not been developed since 2005. Moreover, a major limitation of the program is the lack of Petri net analysis methods apart from the manual simulator feature.

JSARP is an interesting tool for the analysis and simulation of Petri net models. The program has a very intuitive and friendly GUI. The simulator allows for a graphical indication of the fired transitions. The analysis module based on the reachability graph provides information about the boundness and liveness of a designed Petri net. Unfortunately, the tool has a very limited ability to analyse the Petri net properties, limited only to the boundness and liveness.

There are more Petri net tools, but unfortunately, many of them have not been developed for years, e.g., PAPETRI, PROD, PETRUCHIO. Some tools were only an academic application of novel methods and were abandoned after the projects ended. However, it is pleasing that new tools are constantly being developed and that modelling using Petri nets and their analysis is a popular topic in the literature.

4 Hippo-CPS

Hippo-CPS consists of several separate modules supporting designers in the designing process of concurrent systems specified by Petri nets. The tool was launched in 2005 and since that it has been constantly developed. Now, it is mainly aimed at cyber-physical systems (especially at design and verification of their control part), but not only limited to them. This paper is focused on the proprietary algorithms that are included within Hippo-CPS. In particular, verification of boundedness, safeness, and liveness are the main objectives of the work. The main bottlenecks of the existing techniques refer to the computational complexity of algorithms. Exact methods guarantee optimal results, but they require examining all the possible cases. Therefore, in the worst case, the solution may be not found in the assumed time. On the other hand, approximate algorithms are able to find results, but the solution may not be optimal. It means that analysis methods balance between efficiency (run-time of algorithms) and effectiveness (remaining results). Hippo-CPS permits for verification of the main properties with the application of alternative methods (exact, approximate). Let us describe them in more detail.

4.1 Boundedness Analysis

The boundedness of a Petri net can be verified within Hippo-CPS by two algorithms. The first one is based on the construction of a tree of reachable states in the system. The method searches for an unbounded place to oppose that the tested model is bounded. The idea is strictly based on the definition of boundedness, that is, if there exists one unbounded place (in any marking), the whole Petri net is unbounded by the definition [6]. Therefore, the state space generation process is interrupted once the unbounded place is found. This is done by acquiring places marked by ω according to Murata's tree generation algorithm. Furthermore, the size of the tree is reduced and hence the whole computational time is reduced. Nevertheless, the method is exponential in the general case. However, applied reductions may heavily influence the run-time of the algorithm. Results of experiments showed that the technique is effective for 223 benchmarks (out of 242). This means that for 92% of all tested cases the method was able to find a solution. For the remaining benchmarks, the run-time of the algorithm exceeded the assumed time (which was set to 1 hour).

The second method for the boundedness analysis utilizes the linear algebra technique. The applied technique computes the reduced set of place invariants (p-invariants) in the analysed Petri net-based system, according to the algorithm shown in [20]. In opposite to the technique based on the reachability tree, computation of the reduced set of p-invariants is an approximate method. Therefore, the algorithm is oriented mainly on the efficiency (run-time), but it has a strict limitation. According to the theorem shown in [26], a Petri net-based system is bounded if it is covered by place invariants. However, the lack of coverage of a Petri net by place invariants does not imply unboundedness. It should be noted that obtaining all p-invariants is exponential in the general case. Therefore, the utilized method allows computation of a reduced set (just required for the coverage) of place invariants [20]. Performed experiments confirmed the efficiency of the method. The results were achieved for all

examined benchmarks. However, in the case of 28 benchmarks (which states 11.6% of all examined tests), the algorithm indicated that the system is not covered by p-invariants, and thus we do not know if the system is bounded or not. In such cases, additional verification is required (for example with the application of reachability tree). Nevertheless, let us clearly underline that this particular method is oriented on the preliminary analysis of the system, and the results are obtained much faster than in the other, similar techniques.

4.2 Safeness Analysis

Examination of the safeness property can be performed with the Hippo-CPS in two ways. The first technique is based on the reachability tree. The algorithm consecutively searches for the unsafe places in the Petri net. Once such a place is found, the method terminates with the information that the system is not safe. The applied technique is based on the theoretical algorithm, shown in [21]. The experimental verification indicated that the method was able to find the solution for 218 tested cases. This means that it is effective for 90% of all examined benchmarks.

The second approach applies place invariants and further computation of the state machine components (SMCs) cover in the analysed system. In particular, the method firstly searches for the subsequent place invariants and examines whether they form proper SMCs (according to the algorithm shown in [22]). Since the technique is approximate, it is aimed at efficiency. Indeed, the experimental results confirmed that the method was able to compute results for all tested cases. However, similarly to the technique presented in the previous subsection, the method is not effective in the case of systems that are not covered by SMCs [22]. There were 31 (18.8%) such benchmarks in the performed experiments.

4.3 Liveness Analysis

Liveness is the third main property (along with boundedness and safeness) that is very often verified in the Petri net-based system. Hippo-CPS offers a technique that is based on the reachability tree analysis. However, let us underline that in opposite to the boundedness and safeness verification of the system, examination of liveness is much more complicated. First of all, a full state space of the system ought to be generated. Next, according to the guidelines shown in [30], verification of liveness is determined by the boundedness of the Petri net. In the other words, the method is effective for bounded systems. In particular, the analysis procedure consists of the exploration of the generated reachability tree, starting from the final state and finishing at the initial state with simultaneous checking, whether all the transitions are present on that path [23]. The number of states increases exponentially, and this is the main bottleneck of the method. Experimental results showed that the method is effective for 223 benchmarks (out of 242). This means that the algorithm was able to find the result (indicate whether the system is live or not) for 92% of all tested cases.

4.4 Case-Study Example

Let us show the functionality of the presented Hippo-CPS tool by an example. Figure 1 shows a cyber-physical system describing a coffee machine for independent making a caffeinated and decaffeinated drink with four shared resources. Two kinds of coffee can be made in one big machine (started by pressing button $b1$ or $b2$, respectively). There are four shared resources: (1) a grinder that grinds the coffee beans, (2) a nozzle that prepares hot water and pushes it with high pressure into one of the directions, (3) a milk nozzle to troth the milk (make a milk foam), and (4) a chocolate dispenser that sprinkles the chocolate on top of the drink. The prepared drink is taken by the customer before starting a new one.

That real-life example was analysed by all the algorithms shown in Section 4. The reachability tree analysis showed that the system is bounded and safe. The results were achieved within 35.780ms and 36.216ms (for boundedness and safeness verification, respectively). Moreover, the same CPS was examined with the use of linear algebra. Hippo-CPS confirmed previous results, by finding six p-invariants that cover the Petri net. Moreover, six SMCs cover the system. This means that the system is bounded and safe. However, in opposition to the reachability tree analysis, the runtime of algorithms was much quicker. In particular, the solutions were found after 0.313ms (boundedness), and 0.338ms (safeness). Let us underline that such results confirm theoretical assumptions since approximate algorithms were faster than exact ones. Nevertheless, both types of methods reached the same results: the system is bounded and safe. Finally, the liveness of the modelled coffee machine was checked. The applied Hippo-CPS technique finished in 38.906ms with the information that the system is live. Concluding, the verification of the system was completed successfully. The modelled cyber-physical system is live, bounded, and safe.

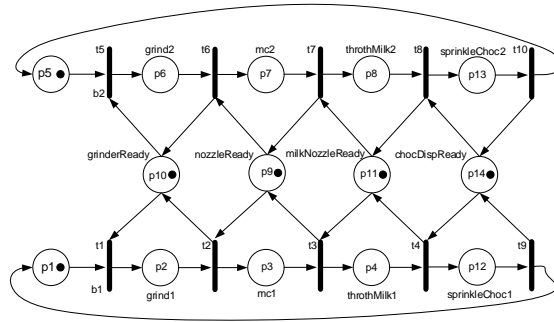


Fig. 1. A cyber-physical system Petri net-based specification real-life example.

5 Conclusions

Verification of the main properties of the Petri net-based systems (especially control parts of the CPSs) with the application of the Hippo-CPS tool was presented in the paper. In particular, verification of boundedness, safeness, and liveness was described and discussed in detail. It should be exposed that Hippo-CPS offers an alternative

analysis of particular properties (boundedness, safeness), giving the designer an opportunity to choose the most suitable algorithm. Results of experiments confirmed the efficiency and effectiveness of the presented methods. The exact algorithms were effective, but due to the exponential complexity were not able to compute results for all tested cases. On the other hand, approximate techniques were efficient and always founded solutions. However, in the case of systems not covered by p-invariants (or SMCs), the result is insufficient, and additional analysis is required.

The main limitation refers to the verification of liveness. Although there are alternative techniques for boundedness and safeness examination, Hippo-CPS currently offers only one method for liveness analysis. Therefore, the future work includes enhancement of the tool by other mechanisms oriented on the liveness verification of the Petri net-based CPS. Moreover, it is planned to perform researchers oriented on the particular classes of the Petri net.

Acknowledgements. This work is supported by the National Science Centre, Poland, under Grant number 2019/35/B/ST6/01683.

References

- [1] Q. Zhu, M. Zhou, Y. Qiao, and N. Wu, "Petri Net Modeling and Scheduling of a Close-Down Process for Time-Constrained Single-Arm Cluster Tools," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, no. 3, pp. 389–400, Mar. 2018, doi: 10.1109/TSMC.2016.2598303.
- [2] C. Girault and R. Valk, *Petri Nets for Systems Engineering: A Guide to Modeling, Verification, and Applications*. Berlin Heidelberg: Springer-Verlag, 2003. doi: 10.1007/978-3-662-05324-9.
- [3] I. Grobelna and A. Karatkevich, "Challenges in Application of Petri Nets in Manufacturing Systems," *Electronics*, vol. 10, no. 18, Art. no. 18, Jan. 2021, doi: 10.3390/electronics10182305.
- [4] Z. Li, "System modeling and control with resource-oriented petri nets by NaiQi Wu and MengChu Zhou," *International Journal of Production Research*, vol. 49, no. 21, pp. 6585–6586, Nov. 2011, doi: 10.1080/00207543.2010.515415.
- [5] R. Wiśniewski, *Prototyping of Concurrent Control Systems Implemented in FPGA Devices*. Springer International Publishing, 2017. doi: 10.1007/978-3-319-45811-3.
- [6] A. Karatkevich, *Dynamic Analysis of Petri Net-Based Discrete Systems*. Berlin Heidelberg: Springer-Verlag, 2007. doi: 10.1007/978-3-540-71560-3.
- [7] T. Murata, "Petri nets: Properties, analysis and applications," *Proceedings of the IEEE*, vol. 77, no. 4, pp. 541–580, Apr. 1989, doi: 10.1109/5.24143.
- [8] A. Yakovlev, L. Gomes, and L. Lavagno, Eds., *Hardware Design and Petri Nets*. Springer US, 2000. doi: 10.1007/978-1-4757-3143-9.
- [9] I. Koh and F. DiCesare, "Transformation methods for generalized Petri nets and their applications to flexible manufacturing systems," in *[1990] Proceedings. Rensselaer's Second International Conference on Computer Integrated Manufacturing*, May 1990, pp. 364–371. doi: 10.1109/CIM.1990.128126.
- [10] H. Kaid, A. Al-Ahmari, Z. Li, and R. Davidrajuh, "Automatic Supervisory Controller for Deadlock Control in Reconfigurable Manufacturing Systems with Dynamic Changes," *Applied Sciences*, vol. 10, no. 15, Art. no. 15, Jan. 2020, doi: 10.3390/app10155270.
- [11] W. M. P. van der Aalst, "Workflow Verification: Finding Control-Flow Errors Using Petri-Net-Based Techniques," in *Business Process Management: Models, Techniques, and Empirical Studies*, W. van der Aalst, J. Desel, and A. Oberweis, Eds. Berlin, Heidelberg: Springer, 2000, pp. 161–183. doi: 10.1007/3-540-45594-9_11.
- [12] A. Barkalov, L. Titarenko, and K. Mielcarek, "Improving characteristics of LUT-based Mealy FSMs," *AMCS*, vol. 30, no. 4, pp. 745–759, Dec. 2020, doi: 10.34768/amcs-2020-0055.

- [13] C.-S. Shih, J.-J. Chou, N. Reijers, and T.-W. Kuo, "Designing CPS/IoT applications for smart buildings and cities," *IET Cyber-Physical Systems: Theory Applications*, vol. 1, no. 1, pp. 3–12, 2016, doi: 10.1049/iet-cps.2016.0025.
- [14] Y. Guo, X. Hu, B. Hu, J. Cheng, M. Zhou, and R. Y. K. Kwok, "Mobile Cyber Physical Systems: Current Challenges and Future Networking Applications," *IEEE Access*, vol. 6, pp. 12360–12368, 2018, doi: 10.1109/ACCESS.2017.2782881.
- [15] R. Wiśniewski, G. Bazydło, P. Szcześniak, and M. Wojnakowski, "Petri Net-Based Specification of Cyber-Physical Systems Oriented to Control Direct Matrix Converters With Space Vector Modulation," *IEEE Access*, vol. 7, pp. 23407–23420, 2019, doi: 10.1109/ACCESS.2019.2899316.
- [16] E. A. Lee and S. A. Seshia, *Introduction to Embedded Systems: A Cyber-Physical Systems Approach*, Second edition. Cambridge, Massachusetts: The MIT Press, 2016.
- [17] 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, doi: 10.1016/j.mfglet.2014.12.001.
- [18] I. Grobelna, R. Wiśniewski, and M. Wojnakowski, "Specification of Cyber-Physical Systems with the Application of Interpreted Nets," in *Proceedings of the IECON'19 - 45th Annual Conference of the IEEE Industrial Electronics Society*, Lisbon, Portugal, pp. 5887–5891.
- [19] B. Li, M. Khelif-Bouassida, and A. Toguyéni, "On-The-Fly Diagnosability Analysis of Bounded and Unbounded Labeled Petri Nets Using Verifier Nets," *International Journal of Applied Mathematics and Computer Science*, 28(2), pp. 269–281, 2018, doi: 10.2478/amcs-2018-0019.
- [20] M. Wojnakowski and R. Wiśniewski, "Verification of the Boundedness Property in a Petri Net-Based Specification of the Control Part of Cyber-Physical Systems," in *Technological Innovation for Applied AI Systems*, Cham, 2021, pp. 83–91. doi: 10.1007/978-3-030-78288-7_8.
- [21] M. Wojnakowski, M. Popławski, R. Wiśniewski, and G. Bazydło, "Safeness Analysis of Petri net-based Cyber-Physical Systems Based on the Linear Algebra and Parallel Reductions," presented at the 17th International Conference of Computational Methods in Sciences and Engineering, Heraklion, Greece, Sep. 2021.
- [22] M. Wojnakowski, R. Wiśniewski, G. Bazydło, and M. Popławski, "Analysis of safeness in a Petri net-based specification of the control part of cyber-physical systems," *AMCS*, vol. 31, no. 4, pp. 647–657, Dec. 2021, doi: 10.34768/amcs-2021-0045.
- [23] M. Popławski, M. Wojnakowski, G. Bazydło, and R. Wiśniewski, "Reachability Tree in Liveness Analysis of Petri Net-based Cyber-Physical Systems," presented at the 17th International Conference of Computational Methods in Sciences and Engineering, Heraklion, Greece, Sep. 2021.
- [24] E. Badouel, L. Bernardinello, and P. Darondeau, "Polynomial algorithms for the synthesis of bounded nets," in *TAPSOFT '95: Theory and Practice of Software Development*, Berlin, Heidelberg, 1995, pp. 364–378. doi: 10.1007/3-540-59293-8_207.
- [25] J. Esparza and M. Silva, "A polynomial-time algorithm to decide liveness of bounded free choice nets," *Theoretical Computer Science*, 102(1): 185–205, 1992, doi: 10.1016/0304-3975(92)90299-U.
- [26] W. Reisig, "Nets Consisting of Places and Transitions," in *Petri Nets: An Introduction*, W. Reisig, Ed. Berlin, Heidelberg: Springer, 1985, pp. 62–76. doi: 10.1007/978-3-642-69968-9_6.
- [27] J. Martinez and M. Silva, "A simple and Fast Algorithm to Obtain all Invariants of a Generalised Petri Net," in *Application and Theory of Petri Nets*, Berlin, Heidelberg, 1982, pp. 301–310. doi: 10.1007/978-3-642-68353-4_47.
- [28] R. Wisniewski, G. Bazydło, L. Gomes, A. Costa, and M. Wojnakowski, "Analysis and Design Automation of Cyber-Physical System with Hippo and IOPT-Tools," in *IECON 2019 - 45th Annual Conference of the IEEE Industrial Electronics Society*, Oct. 2019, vol. 1, pp. 5843–5848. doi: 10.1109/IECON.2019.8926692.
- [29] L. Gomes, F. Moutinho, and F. Pereira, "IOPT-tools — A Web based tool framework for embedded systems controller development using Petri nets," in *2013 23rd International Conference on Field programmable Logic and Applications*, Sep. 2013, pp. 1–1. doi: 10.1109/FPL.2013.6645633.
- [30] S. Wang, M. Zhou, Z. Li, and C. Wang, "A New Modified Reachability Tree Approach and Its Applications to Unbounded Petri Nets," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 43, no. 4, pp. 932–940, Jul. 2013, doi: 10.1109/TSMCA.2012.2226878.