УДК 004.052.42
DOI https://doi.org/10.32782/2663-5941/2024.4/33

Шкарупило В.В.
Національний університет біоресурсів і природокористування України,
Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України

Душеба В.В.
Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України

Зайко Т.А.
Національний університет «Запорізька політехніка»

Шкарупило В.В.
Національний університет «Запорізька політехніка»

Скрупський С.Ю.
Національний університет «Запорізька політехніка»

ІНДУКТИВНИЙ ПІДХІД ДО ПОБУДОВИ ФОРМАЛІЗОВАНИХ ПОДАНЬ ПРОГРАМНО-АЛГОРИТМІЧНОГО ЗАБЕЗПЕЧЕННЯ ПРИ ПРОЄКТУВАННІ

У наш час рівень складності актуальних комп'ютерних систем, на основі яких реалізуються виробничі і невиробничі предметно-орієнтовані сценарії, є зростаючим. Це твердження справедливе і по відношенню до систем критичного призначення – систем, збої і відмови у роботі яких можуть призвести до небажаних наслідків значного масштабу. Передбачуваність роботи таких систем досягається, у тому числі, за рахунок комплексного застосування методів і засобів контролю подань розроблюваного програмно-алгоритмічного забезпечення при проєктуванні. Зазначені подання, у загальному випадку, є неформалізованими, що, серед іншого, ускладнює процес їх контролю за показником несуперечливості програмно-алгоритмічного забезпечення.

У якості методу контролю охоплено поширений формальний метод перевірки на моделі TLC (TLA Checker), а у якості супутніх засобів – темпоральну логіку дій TLA (Temporal Logic of Actions) Леслі Лемпорта, включно із відповідним виразним засобом TLA+. У свою чергу, формалізовані подання (формальні специфікації) на основі TLA+, за рахунок математичної строгості і модульності формалізму, розглянуто як засоби уможливлення автоматизації процесу контролю шляхом формальної верифікації на основі методу TLC, а також на основі відповідного розвитку методу, призначеного до застосування за ітеративного підходу до організації процесу формальної верифікації при проєктуванні.

І первинні неформалізовані, і похідні від них формалізовані подання узагальнено у межах праці як артефакти, призначені до опрацювання на етапі проєктування у складі етапів процесу розроблення програмно-алгоритмічного забезпечення.

Викладений індуктивний підхід представлено у якості засобу, призначеного для вирішення допоміжної задачі, що постає при побудові похідних формалізованих подань – задачі варіювання рівня деталізації формалізованих подань. Доцільність такого кроку обумовлена, у тому числі, проявами ефекту експоненційного зростання простору станів для систем переходів, що будуються у процесі формальної верифікації, а також обмеженістю доступних розробникам часових і обчислювальних ресурсів.

Ключові слова: *TLA, артефакт, верифікація, програмно-алгоритмічне забезпечення, проєктування, формальна специфікація.*

Постановка проблеми. У контексті розроблення комп'ютерних систем критичного призначення складова людського фактору постає серед визначальних, оскільки вносить / розширює аспект недетермінізму стосовно запланованих сценаріїв функціонування розроблюваної системи у визначених режимах експлуатації. Така ситуація обумовлює важливість застосування численних методів і засобів контролю, серед яких все більшого поширення набувають формальні методи і засоби, що обумовлено, у тому числі, високим ступенем придатності до автоматизованого застосування відповідних представників сімейства формальних методів перевірки на моделі (Model

Checking) [1, 2]. У якості відмінної риси зазначених методів варто вказати при цьому на те, що судження стосовно досліджуваної властивості розроблюваної системи виноситься не на підставі проведення перевірки системи / компонента системи безпосередньо, а на підставі контролю відповідних формалізованих подань – формальних специфікацій (ФС). Така особливість, у свою чергу, обумовлює необхідність проведення додаткового контролю, направленого на отримання достовірних свідчень стосовно правомірності поширення суджень за результатами верифікації ФС також і на відповідні первинні, у загальному випадку неформалізовані, подання. При цьому зазначений крок не є тривіальним. Причиною тому є, серед іншого, є і прояв ефекту експоненційного зростання простору станів систем переходів, які будуються у процесі формальної верифікації методами перевірки на моделі: у площинах і обчислювальних [3], і просторових витрат [4].

У охоплених нижче працях було показано, що прояв вказаного ефекту істотним чином залежить, у тому числі, від архітектурної складової одержуваних і досліджуваних ФС.

Об'єктом дослідження є процес проєктування програмно-алгоритмічного забезпечення (ПАЗ) систем критичного призначення.

Зауваження: тут і надалі за текстом контекстне навантаження використовуваного поняття «архітектура» у межах словосполучення «архітектурна складова» є таким, що розширює зміст поняття «структура» – за рахунок залучення також і зв'язків між елементами структури.

У попередніх дослідженнях було виокремлено граничні випадки для архітектурної складової проєктованого ПАЗ: для випадку відсутності умовних переходів прояв ефекту експоненційного зростання простору станів виявився істотно помірнішим [3], у порівнянні з іншим граничним випадком, де паралелізм було подано згідно моделі чергування [5]. Для останнього випадку, для 2^4 змінних станів, мали місце близько $2{\cdot}10^6$ альтернативних шляхів від початкового до заключного стану системи переходів. Варто стосовно цього зауважити, що така специфіка узгоджується із відповідними тезами фундаментальних праць за напрямом – наприклад, праць лауреата премії Тюрінга – Леслі Лемпорта [6, с. 3].

Серед інших чинників, що обумовлюють стрімкість прояву озвученого ефекту – також і обраний розробником / колективом розробників рівень деталізації ФС. Зазначений вибір визначає, зокрема, кількість змінних станів, що фігурують у ФС. І це, у свою чергу, спонукає потребу пошуку компромісного рішення – у частині досягнення балансу між обраним рівнем деталізації ФС, з урахуванням відповідної архітектурної складової, і супутніми обчислювальними і просторовими витратами на проведення верифікації методом перевірки на моделі [7, с. 5], з урахуванням доступних обчислювальних можливостей наявних програмно-апаратних систем.

Вказаний пошук типово проводиться розробниками, ґрунтуючись, у значній мірі, на їх досвіді. Такий канонічний підхід, однак, відкритими полишає питання, зокрема, у частині передбачуваності одержуваного корисного ефекту від застосування формальних методів і засобів у якості засобів контролю при проєктуванні ПАЗ.

У контексті означеного вище об'єкту дослідження в роботі представлено розроблений підхід до вирішення важливої науково-технічної проблеми варіювання рівня деталізації ФС, у залежності від наявних обчислювальних ресурсів, а також враховуючи архітектурну складову ФС. При цьому результат вирішення даної проблеми розглянуто у якості складової комплексу засобів уможливлення реалізації уніфікованої методології встановлення достатності обраного рівня деталізації ФС.

Проблему опрацьовано у межах представленого індуктивного підходу з урахуванням наступних припущень:

– математичну строгість використовуваного формалізму подання ФС розглянуто як чинник сприяння однозначності і уніфікованості інтерпретації контекстного навантаження ФС;

– при опрацюванні рівнів деталізації ФС застосовано дуальний підхід: охоплено і випадок підтвердження несуперечливості ФС, і протилежну варіацію.

Аналіз останніх досліджень і публікацій. Серед показових прикладів результативності застосування формальних методів і засобів у процесі розроблення комп'ютерних систем критичного призначення постають, у тому числі, сценарії атомної енергетики Фінляндії, стосовно яких було засвідчено, що, у період з 2008 по 2020 рр., за рахунок застосування формальних методів і засобів, було виявлено 66 підтверджених помилок у ФС досліджуваних властивостей розроблюваних систем [8]. Автором при цьому відзначено важливість автоматизації процесу синтезу ФС.

Серед інших демонстративних сценаріїв критичних предметних областей, де у процесі розроблення ПАЗ комп'ютерних систем було успішно

залучено формальні методи і засоби у якості засобів контролю – у тому числі залізнична галузь [9, 10]. Серед відомих представників корпоративного сектору економіки – компанії Intel (сповіщено про виявлення 45 суттєвих суперечливостей) [11], Microsoft, Amazon [12] та ін.

Враховуючи контекст актуальних подій у державі, до прикладів, де залучення формальних методів і засобів супроводжувалося значимим корисним ефектом, варто долучити також і сценарії керування безпілотними літальними апаратами [13, 14].

Поєднує охоплені і подібні сценарії загальний підхід, що полягає в покладанні на досвід розробників при виборі рівня деталізації ФС, до яких застосовуються формальні методи і засоби, у тому числі поширений формальний метод перевірки на моделі TLC (TLA Checker), а також супутні засоби – темпоральна логіка дій TLA (Temporal Logic of Actions) і відповідний формалізм TLA+ Леслі Лемпорта [15].

Постановка завдання. Завдання представленого дослідження полягає у розробленні підходу до варіювання рівня деталізації ФС для результативного проведення формальної верифікації ФС при проєктуванні ПАЗ систем критичного призначення. У відповідності до вказаного вище припущення стосовно залучення дуального підходу, результативним вважається і випадок підтвердження несуперечливості ФС, і випадок виявлення суперечливості / суперечливостей.

Викладення основного матеріалу. Для викладення розробленого індуктивного підходу до побудови формалізованих подань ПАЗ комп'ютерних систем, змістове навантаження згаданого вище поняття «архітектура» було розширено до такого, що є означенням поняття «артефакт» – сутності, що характеризується архітектурою і змістом [16]. Таку інтерпретацію було сформульовано як розширення відносно базової, запропонованої професором Мюнхенського технічного університету Манфредом Броєм, за рахунок заміщення поняттям «архітектура» поняття «структура» [17].

Крок у частині інтерпретації у якості артефактів і первинних, у загальному випадку неформалізованих, подань, і похідних від них формалізованих представлень ПАЗ здійснено для уніфікації процесу їх аналізу і опрацювання розробником / колективом розробників при проєктуванні.

Охоплений вище понятійний апарат залучено у відповідності до підходу стосовно комплексного опрацювання показників функціональних і нефункціональних характеристик при проєктуванні ПАЗ; графічна форма представлення зведена на рисунку 1 [18].

На рисунку 1 у якості засобів сполучення складових діаграми застосовано відношення агрегування і розширення. Використання саме відношення агрегування, а не композиції, призначене ставити наголос, що відповідні агреговані складові допустимі до інтерпретації і як елементи комплексної конструкції, і як автономні частини.

Представлений індуктивний підхід до побудови формалізованих подань, одержуваних при проєктуванні ПАЗ, охоплює дві концептуальні площини опрацювання досліджуваних артефактів, у складі яких – і, у загальному випадку неформалізовані, первинні подання, і похідні від них формалізовані подання – ФС. При цьому ФС розглядаються як артефакти, залучення яких дозволяє проводити формальну верифікацію методом перевірки на моделі в автоматизованому режимі. У якості означених площин охоплено аналітичний рівень опрацювання артефактів і рівень реалізації. Рівень реалізації при цьому виокремлено як такий, на якому фігурують виразні засоби уможливлення автоматизації процесу опрацювання ФС у частині проведення їх контролю за показником несуперечливості шляхом застосування поширеного формального методу перевірки на моделі

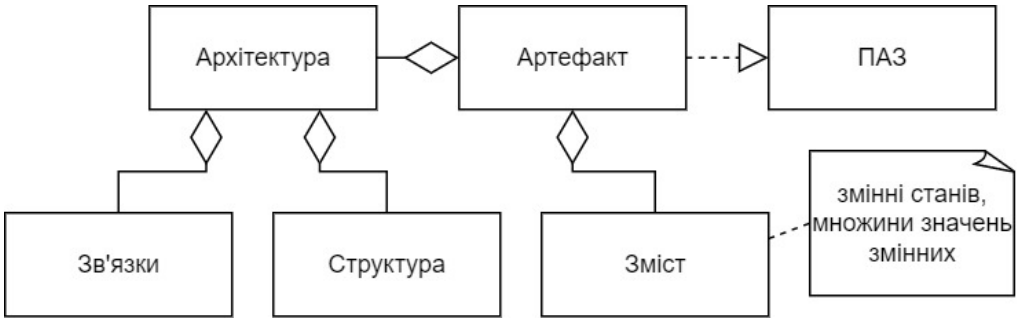

Рис. 1. Графічне представлення залученого понятійного апарату у формі UML-діаграми

TLC або розробленого розвитку цього методу, призначеного до використання за ітеративного підходу до організації процесу формальної верифікації [19].

Представлений індуктивний підхід полягає у виокремленні ієрархічних рівнів – у площинах і аналітичній, і реалізації: для цього було опрацьовано концепції «подій» і «дій» [20].

Трійки Гоара залучено для сполучення елементів спільного ієрархічного рівня. При цьому правило композиції Гоара застосовано для формування елементів наступного ієрархічного рівня [21, 22].

Запропонований індуктивний підхід полягає у поступальному висхідному зміщенні між суміжними ієрархічними рівнями ФС, починаючи від найнижчого, – допоки таким чином не буде сформована результуюча темпоральна формула на основі виразних засобів TLA+, що характеризується властивостями математичної строгості та модульності. Така формула призначена до опрацювання на виокремленому концептуальному рівні реалізації представленого підходу – шляхом застосування по відношенню до неї методу TLC або розробленого розвитку цього методу [19].

Дієвість представленого індуктивного підходу було підтверджено, у тому числі, для критичних сценаріїв аерокосмічної галузі і галузі енергетики [16, 23].

Подяки. Дослідження проведено у відповідності до вирішуваних задач науково-дослідної роботи № 0120U102683 «Розроблення спеціалізованих комп'ютерних технологій моделювання та опрацювання оперативної інформації в задачах енергетики», виконуваної відділом математичного та комп'ютерного моделювання Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України.

Висновки. Таким чином, у роботі представлено розроблений індуктивний підхід до побудови формалізованих подань як артефактів, одержуваних і досліджуваних у процесі проєктування програмно-алгоритмічного забезпечення комп'ютерних систем, і призначених слугувати засобами контролю первинних, у загальному випадку неформалізованих, подань за показником їх несуперечливості.

Запропонований підхід реалізовано з урахуванням специфіки виразних засобів формалізму TLA+ темпоральної логіки дій TLA Леслі Лемпорта, і призначено до застосування у комплексі із формальним методом перевірки на моделі TLC або розвитком зазначеного методу у частині ітераційного підходу до організації процесу формальної верифікації. Такий крок уможливив отримання формалізованих подань, що характеризуються наступними властивостями: математична строгість, модульність. Модульності, у свою чергу, було досягнуто шляхом виокремлення ієрархічних рівнів і оперування при цьому конструкціями «подій» і «дій».

Подальші дослідження спрямовано на розвинення представленого підходу у частині формулювання і узагальнення рекомендацій стосовно встановлення достатності обраного рівня деталізації формалізованих подань, по відношенню до яких в автоматизованому режимі застосовується поширений формальний метод перевірки на моделі TLC, або згаданий вище розвиток зазначеного методу, що дозволяють проводити контроль артефактів проєктування, у тому числі, за показником їх несуперечливості.

Список літератури:

1. Clarke E. M., Grumberg O., Kroening D., Peled D., Veith H. *Model checking*: 2nd ed. Massachusetts: The MIT Press, 2018.

2. Шкарупило В.В., Зайко Т.А., Шкарупило В.В., Тіменко А.В. Обґрунтування доцільності формалізації артефактів процесу розроблення програмних систем // *Світ наукових досліджень. Випуск 29: матеріали Міжнародної мультидисциплінарної наукової інтернет-конференції* (м. Тернопіль, Україна, м. Ополе, Польща, 23–24 квітня 2024 р.) / за ред. : О. Патряк та ін. ГО "Наукова спільнота", WSZIA w Opolu. Тернопіль: ФОП Шпак В.Б. 2024. С. 88–90. URL: https://www.economy-confer.com.ua/full-article/5512/

3. Shkarupylo V.V., Tomičić I., Kasian K.M. The investigation of TLC model checker properties. *Journal of Information and Organizational Sciences*, 2016, Vol. 40, No. 1. P. 145–152. DOI: https://doi.org/10.31341/jios.40.1.7

4. Шкарупило В.В., Чемерис О.А., Душеба В.В. Оцінювання просторової складності задачі формальної верифікації, вирішуваної методом перевірки на моделі. *Вчені записки Таврійського національного університету імені В.І.Вернадського, серія «Технічні науки»*, 2020, Том 31 (70), № 5. С. 147–151. DOI: https://doi.org/10.32838/2663-5941/2020.5/24

5. Shkarupylo V. V., Tomičić I., Kasian K. M., Alsayaydeh J. A. J. 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, 2018. Vol. 4, No. 1. P. 48–60. DOI: https://doi.org/10.15282/ijsecs.4.1.2018.4.0037

6. Lamport L. *A science of concurrent programs* (preprint, version of 16 March 2024). URL: https://lamport.azurewebsites.net/tla/science.pdf (Accessed: 10.07.2024)

7. Clarke E. M. , Henzinger T. A., Veith H., Bloem R. *Handbook of model checking*. Springer Publishing Company, Inc., 2018. 1210 p. DOI: https://doi.org/10.1007/978-3-319-10575-8

8. Pakonen A. Model-checking I&C logics – insights from over a decade of projects in Finland. In *12th Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies, NPIC&HMIT 2021*. American Nuclear Society (ANS), 2021. P. 792–801 DOI: https://doi.org/10.13182/T124-34322

9. Resch S., Paulitsch M. Using TLA+ in the development of a safety-critical fault-tolerant middleware. Software Reliability Engineering Workshops : *Proc. 2017 IEEE International Symposium* (Toulouse, France, 23–26 October 2017). P. 146–152. DOI: https://doi.org/10.1109/ISSREW.2017.43

10. Butler M., Körner P., Krings S., Lecomte T., Leuschel M., Mejia L.-F., Voisin L. The first twenty-five years of industrial use of the B-method. *Formal Methods for Industrial Critical Systems, FMICS 2020 : 25th Int. Conf.* / eds. M. ter Beek, D. Ničković (Vienna, Austria, September 2–3, 2020). 2020. Lecture Notes in Computer Science, Vol. 12327. Springer, Cham. P. 189–209. DOI: https://doi.org/10.1007/978-3-030-58298-2_8

11. Beers R. Pre-RTL formal verification: an Intel experience. *Design Automation Conference, DAC '08: Proceedings of the 45th annual Conference* (Anaheim, California, June 2008). New York, NY, United States : Association for Computing Machinery, 2008. P. 806–811. DOI: https://doi.org/10.1145/1391469.1391675

12. Kuppe M. A., Lamport L., Ricketts D. The TLA+ Toolbox. *Formal integrated development environment, F-IDE 2019 : 5th Workshop* (Porto, Portugal, October 7, 2019). EPTCS 310, 2019. P. 50–62. DOI: http://doi.org/10.4204/EPTCS.310.6

13. Surya A. et al. Formal specification and verification of time-sensitive drone systems using TLA+: a case study. *Proc. 2024 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI)*, Gwalior, India, 14-16 March 2024. DOI: https://doi.org/10.1109/IATMSI60426.2024.10503145

14. Das M., Mohan B. R., Guddeti R. M. R. Formal specification and verification of drone system using TLA+: a case study. *2022 IEEE/ACIS 23rd International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*, Taichung, Taiwan, 07–09 December 2022. DOI: https://doi.org/10.1109/SNPD54884.2022.10051801

15. Lamport L. *Specifying systems: The TLA+ language and tools for hardware and software engineers*. Boston, MA, United States : Addison-Wesley Longman Publishing Co., Inc., 2002. 364 p. DOI: https://dl.acm.org/doi/10.5555/579617

16. Shkarupylo V., Blinov I., Dusheba V., Alsayaydeh J. A. J. Case driven TLC model checker analysis in energy scenario. *CEUR Workshop Proceedings*, 2023. Vol. 3392. P. 65–75. ISSN 1613-0073. DOI: https://doi.org/10.32782/cmis/3392-6

17. Broy M. A logical approach to systems engineering artifacts and traceability: from requirements to functional and architectural views. *Engineering dependable software systems : NATO Science for Peace and Security Series – D: Information and Communication Security* / eds. M. Broy, D. Peled, G. Kalus. Amsterdam : IOS Press, 2013. Vol. 34. P. 1–48. DOI: https://doi.org/10.3233/978-1-61499-207-3-1

18. Шкарупило В.В., Душеба В.В., Скрупський С.Ю., Блінов І.В. Стратифікована модель подання нефункціональних характеристик системи критичного призначення при проєктуванні. *Електронне моделювання*, 2022. Т. 44, № 2 (2022). С. 90–106. ISSN 0204–3572. DOI: https://doi.org/10.15407/emodel.44.02.090

19. Шкарупило В., Блінов І., Кучанський В., Давидюк А., Дімітрієва Д. Методи і засоби контролю артефактів процесу проєктування програмно-алгоритмічної складової систем критичного призначення: монографія / за заг. ред. В. В. Шкарупила. Publishing House «European Scientific Platform», 2023. 120 с. ISBN: 978-617-8126-22-3 DOI: https://doi.org/10.36074/mzkapppasskp-monograph.2023

20. Шкарупило В. В., Блінов І. В. Сценарії, методи та засоби формальної верифікації артефактів процесу проєктування систем критичного призначення : монографія. Вінниця : ГО «Європейська наукова платформа», 2021. – 104 с. ISBN 978-617-8037-55-0 DOI https://doi.org/10.36074/smtzfvappskp-monograph.2021

21. Shkarupylo V., Chemerys O., Dusheba V., Kudermetov R., Oliinyk A. On Hoare triples applicability to dependable system specification synthesis. *Dependable Systems, Services and Technologies, DESSERT'2020 : The 11th International Conference* (Kyiv, Ukraine, May 14–18, 2020). P. 371–375. DOI: https://doi.org/10.1109/DESSERT50317.2020.9125074

22. Hoare C. A. R. Communicating sequential processes. *Communications of the ACM*, 1978. Vol. 21, No. 8. P. 666–677.

23. Shkarupylo V.V., Blinov I.V., Chemeris A.A., Dusheba V.V., Alsayaydeh J.A.J. On Applicability of Model Checking Technique in Power Systems and Electric Power Industry. In: Zaporozhets A. (eds) *Systems, Decision and Control in Energy III. Studies in Systems, Decision and Control*, 2022, Vol. 399. Springer, Cham. pp. 3-22. DOI: https://doi.org/10.1007/978-3-030-87675-3_1

Shkarupylo V.V., Dusheba V.V., Zaiko T.A., Shkarupylo V.V., Skrupsky S.Yu. INDUCTIVE APPROACH TO SOFTWARE AND ALGORITHMIC COMPONENT FORMALIZED REPRESENTATIONS CONSTRUCTION AT DESIGN

Nowadays, the level of complexity of modern computer systems, on the basis of which both production and non-production subject-oriented scenarios are implemented, is growing. This statement is also true with respect to the safety-critical systems – systems whose faults and failures may lead to the unwanted consequences of a significant scale. Predictability of such systems functioning is achieved, in particular, due to the complex application of control methods and tools with respect to the software and algorithmic component representations at the design stage of development process. These representations are informal in general. Specified obstacle, among other limitations, complicates the process of representations control based on the index of software and algorithmic component consistency.

As a control method, the widespread TLC (TLA Checker) model checker has been considered. As the corresponding formal tools, the Temporal Logic of Actions (TLA, by Leslie Lamport) and the related TLA+ formalism have also been encompassed. In its turn, formalized representations (formal specifications) based on the TLA+, due to the mathematical rigor and modularity of the formalism, have been considered as the means of enabling the automation of the control process through formal verification based on the TLC method, as well as on the basis of the appropriate development of the method intended for use during the iterative approach to the organization of the process of formal verification at design.

Both the initial non-formalized and derived from them formalized representations have been generalized within the paper as artifacts intended for processing at the design stage of software and algorithmic component development process.

The introduced inductive approach is presented as a tool intended for solving the auxiliary problem that arises during the construction of the derived formalized representations – the problem of varying the atomicity level of formalized representations. The expediency of such a step is, among other factors, due to the occurrence of the effect of exponential growth of the state space of the transition systems constructed during the process of formal verification, as well as to the limitation of time and computing resources available to developers.

Key words: *TLA, artifact, verification, software and algorithmic component, design, formal specification.*