УДК 004.052.42
DOI https://doi.org/10.32838/2663-5941/2019.6-1/34

Шкарупило В.В.
Інститут проблем моделювання в енергетиці імені Г.Є. Пухова
Національної академії наук України

Євдокимов В.Ф.
Інститут проблем моделювання в енергетиці імені Г.Є. Пухова
Національної академії наук України

Душеба В.В.
Інститут проблем моделювання в енергетиці імені Г.Є. Пухова
Національної академії наук України

ЗАСТОСУВАННЯ ФОРМАЛЬНИХ МЕТОДІВ ДЛЯ ПЕРЕВІРКИ СИСТЕМ КРИТИЧНОГО ПРИЗНАЧЕННЯ

У наш час застосування формальних методів стає все більш поширеним явищем у різноманітних предметних областях. Шляхи їх використання охоплюють сценарії як комерційного, так і некомерційного характерів. Особливої уваги при цьому заслуговують системи критичного призначення – системи, відмови або збої в роботі яких можуть призвести до критичних наслідків. Прикладами відповідних предметних областей можуть слугувати космічна галузь, енергетика тощо. В роботі увага приділяється методам перевірки на моделі – представникам формальних методів. Характерною ознакою останніх є можливість автоматизації процедури їх застосування. Це слугує позитивним фактором з позиції практичного їх використання в задачах прикладного характеру. Суттєвим недоліком формальних методів є експоненційний характер росту часових витрат на процедуру формальної верифікації від числа змінних станів системи переходів в основі формальної специфікації, що підлягає автоматизованій перевірці. Така специфіка зумовлює потребу пошуку компромісних рішень з позицій корисного ефекту від верифікації, супутніми цьому процесу часовими витратами і доступними обчислювальними ресурсами. В роботі увага приділяється програмному складнику систем критичного призначення. З урахуванням складності таких систем і зазначеного недоліку методів перевірки на моделі, формулюється завдання роботи. Воно полягає в аналізі аспектів застосування формальних методів для перевірки систем критичного призначення. За результатами проведеного аналізу формулюється перелік рекомендацій для застосування методів перевірки на моделі під час проектування систем критичного призначення. Як демонстративний приклад в роботі було узято космічну галузь – розглянуто систему керування орієнтацією космічного апарату. Посилаючись на результати попередніх досліджень, сформульовано рекомендації до застосування формальних методів під час проектування систем критичного призначення.

Ключові слова: *перевірка на моделі, формальна специфікація, верифікація, система критичного призначення, системний підхід.*

Постановка проблеми. Сучасне суспільство у різних сферах своєї діяльності істотним чином покладається на функціонування критичних систем (систем критичного призначення, Safety-critical Systems). Це такі системи, до надійності функціонування яких висуваються підвищені вимоги, тобто такі системи, відмова яких у процесі експлуатації може призвести до критичних наслідків [1]. Відповідними прикладами можуть слугувати система керування орієнтацією космічного апарату, різноманітні системи управління у сфері атомної енергетики тощо [2]. Іншими прикладами предметних областей є оборонна, хімічна промисловості, авіація, медицина [3].

Названі системи характеризуються високим рівнем складності. Це зумовлює потребу використання ефективних підходів до проектування та розроблення таких систем – підходів, використання яких сприяло би зменшенню кількості та критичності помилок проектних рішень – помилок, що потенційно можуть призвести до критичних наслідків. Відповіддю на це питання слугує використання модельно-орієнтованого підходу (MBSA, Model-based Safety Analysis) до аналізу надійності систем критичного призначення (СКП) [4]. Шляхом реалізації такого підходу є використання формальних методів під час проектування. При цьому доречно зазначити три альтернативних

напрями розвитку відповідних методів: дедуктивна верифікація, перевірка еквівалентності і перевірка на моделі (Model Checking). Окремої уваги тут заслуговує сімейство методів перевірки на моделі, коли судження стосовно коректності роботи тієї чи іншої системи (підсистеми) робиться на основі відповідної формальної моделі – специфікації [5]. Відмінною рисою методів перевірки на моделі є можливість автоматизації процедури їх використання. Це є вагомим аргументом на користь розгляду названих методів як засобу реалізації MBSA-підходу з позиції озвученої складності СКП. Саме використанню цих методів при проектуванні СКП і присвячена дана робота.

Перш ніж продовжити викладення основного матеріалу, спрощено представимо процес розроблення системи послідовністю наступних етапів: аналіз вимог до системи, проектування, реалізація, тестування. Зростання складності СКП проявляється, зокрема, і у зростанні складності процесу їх розроблення з позиції як матеріально-технічних, так і часових витрат. Усунення помилок проектних рішень на пізніх етапах процесу розробки супроводжується істотно більшими матеріальними і часовими витратами [6]. Навіть більше, ґрунтуючись на накопиченій статистиці, стверджується, що кожна п'ята аварія у космічній галузі пов'язана з відмовою комп'ютерних систем управління та їх компонентів [7]. У цьому контексті помилки проектних рішень доречно виявляти і усувати вже на етапі проектування процесу розробки. Навіть тестування не гарантує відсутності помилок, а лише виявляє деякі з них за умови використання вдалим чином підібраних тестових послідовностей. У контексті СКП така специфіка не є задовільною, оскільки не виявлені на етапі тестування помилки можуть потенційно призвести до критичних наслідків під час експлуатації системи.

Під час розгляду і аналізу методів перевірки на моделі оперуватимемо поняттям «верифікація», що регламентується стандартом IEEE 1012-2016 [8]. Процедура верифікації у стандарті розглядається як складова частина більш комплексного процесу V&V (Verification and Validation), що охоплює вищенаведені етапи процесу розробки. Верифікація при цьому визначається як засіб встановлення відповідності одержуваних артефактів процесу розробки, зокрема моделей-результатів етапу проектування, специфікаціям вимог до системи. Процедура валідації передбачає встановлення придатності розроблюваної системи до цільового використання. Тут доречно провести паралелі між супутніми поняттями верифікації, перевірки на моделі, валідації, імітаційного моделювання і тестування (рис. 1).

На рис. 1 ромбовидною стрілкою зображується відношення композиції, а пунктирною – відношення реалізації. Це означає, що перевірка на моделі є шляхом здійснення верифікації, а імітаційне моделювання і тестування – шляхами здійснення валідації. Окремо варто відзначити техніку RV (Runtime Verification), що не відображена на рис. 1, розглядається як доповнення до перевірки на моделі і тестування, і дозволяє перевіряти властивості системи в режимі виконання [9]. Перевагою такого підходу є порівняно менші обчислювальні витрати ніж під час перевірки на моделі, недоліком (з позиці скорішого виявлення помилок) є те, що система вже має бути реалізованою.

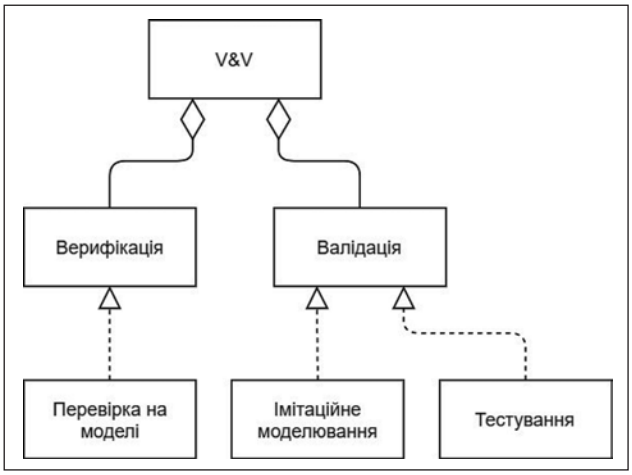

Рис. 1. Спрощена концептуалізація процесу V&V

Спрощення рис. 1 полягає в тому, що тут наводиться лише поверхнева класифікація концепцій, аби надлишковою інформацією не «розмити» акцент роботи. Наприклад, як альтернативи перевірки на моделі можуть виступати дедуктивна верифікація, перевірка еквівалентності. Істотним, на нашу думку, недоліком останніх двох варіацій є неможливість їх автоматизації, що критично з позиції складності досліджуваних систем.

Аналіз останніх досліджень і публікацій. Стверджується, що більше 80% функцій сучасних інформаційно-керуючих систем реалізуються програмно [10]. Також зазначається, що складність таких систем потребує застосування спеціальних методів забезпечення надійності.

Прикладом успішного застосування методів перевірки на моделі під час проектування СКП є платформа TAS Control Platform, призначена

слугувати основою програмної системи керування рухом залізничного транспорту [11]. В роботі, проте, не було висвітлено питань автоматизації залучення формальних методів до процесу проектування. Це стосується і питання автоматизації синтезу формальних специфікацій. Навіть більше, атомна енергетика Фінляндії з 2008 р. використовує методи перевірки на моделі для перевірки програмного складника контрольно-вимірювальних пристроїв [12]. З причині закритості зазначеної тематики багато питань стосовно аспектів застосування формальних методів лишаються неоприлюдненими. Одне з ключових, на нашу думку, з таких питань – досягнення балансу між корисним ефектом від верифікації, супутніми цьому процесу часовими витратами і доступними обчислювальними ресурсами. У цьому контексті попередні експерименти показали негативний вплив надмірної деталізації специфікації, де паралелізм було представлено в специфікації на основі моделі чергування [13]. Результатом стало вичерпання доступних ресурсів оперативної пам'яті та дострокове припинення процесу автоматизованої перевірки.

Постановка завдання. Проаналізувати аспекти застосування формальних методів для перевірки СКП. За результатами проведеного аналізу сформулювати перелік рекомендацій для застосування методів перевірки на моделі під час проектування СКП.

Виклад основного матеріалу дослідження. Як сферу застосування СКП розглянемо космічну галузь. Для демонстрації спрямованості роботи скористаємось системним підходом, викладеним у стандарті ECSS-E-00A (рис. 2) [14], що був замінений стандартом ECSS-S-ST-00C [15].

На рис. 2 показано, що етапом процесу системного інжинірингу (розробки) обрано етап проектування – етап, на якому планується використовувати методи перевірки на моделі. При цьому СКП розглядається як складний програмно-апаратний комплекс, де в роботі охоплюється програмний складник. При цьому, з урахуванням експоненційного характеру росту обчислювальних витрат від кількості змінних стану формальної моделі, розглядається лише підсистема СКП. Прикладом може слугувати підсистема керування орієнтацією космічного апарату.

Вісь Oy, зображена на рис. 2, деталізується на рис. 3, де відображаються етапи процесу системного інжинірингу.

На рис. 3 пунктиром виділено акцент роботи. Під входом розуміються вимоги до системи, які ще не сформульовано, під виходом – артефакти процесу проектування (моделі, проектні рішення). Загалом рис. 3 демонструє спрощену інтерпретацію процесу системного інжинірингу [14]. Під верифікацією розуміється процедура формальної верифікації, призначена бути здійсненою в автоматизованому режимі методом перевірки на моделі.

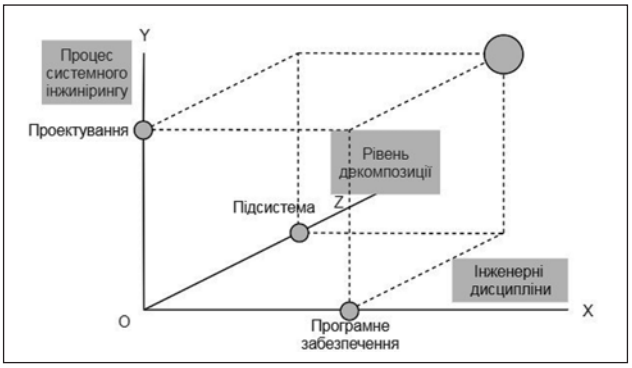

Рис. 2. Демонстрація системного підходу до аналізу СКП

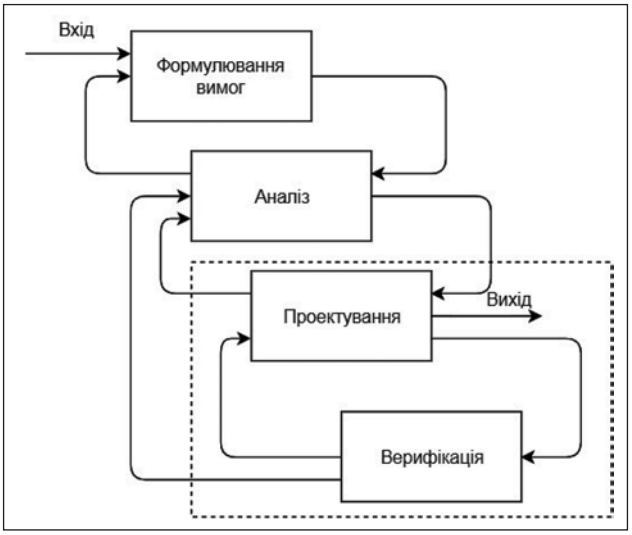

Рис. 3. Демонстрація спрямованості роботи

Застосування методів перевірки на моделі під час проектування СКП висуває підвищені вимоги до адекватності формальних моделей, на основі яких формулюються твердження стосовно відсутності / наявності помилок в проектних рішеннях. Така ситуація потребує ґрунтовного аналізу специфіки досліджуваної системи. В даній роботі розглядається програмний складник системи управління, призначеної до використання в космічній галузі. Для цього узято типовий розподіл операцій, характерний для вирішення задач управління в названій галузі – Суміш Шатл (табл. 1) [2, с. 70].

З табл. 1 видно, що найбільш істотний кількісний вклад (77,7%) вносять операції завантаження операнду, складання, занесення до пам'яті, пере-

ходу. Це дає підстави розглядати питання варіації ступеню деталізації формальних специфікацій, з урахуванням відповідного розподілу операцій. Для порівняння, для загального випадку вирішення науково-технічних задач використовується суміш Гібсона, де 40,3% відводяться під операції складання (з фіксованою і плаваючою крапкою), 19% – під операції індексної модифікації (робота з масивами), 17,5% – під операції пересилання даних, що формує 76,8% усього складу операцій [2, с. 69; 16]. Видно, що порівняно із сумішшю Шатл, для Суміші Гібсона відсоткова частка операцій складання у 2,6 рази більша. Таке порівняння дає підстави сформулювати нижченаведені рекомендації до синтезу формальних моделей (специфікацій), призначених до автоматизованої формальної верифікації методами перевірки на моделі.

Таблиця 1

Розподіл операцій для вирішення задач управління у космічній галузі

№ з/п	Операція	Відсотковий склад
1	Завантаження операнду	26,1
2	Складання	15,5
3	Занесення до пам'яті	13,8
4	Множення	6,0
5	Ділення	1,9
6	Логічні операції	5,4
7	Зсув на 4 розряди	7,2
8	Перехід	22,3
9	Завантаження адреси	1,8
	Разом:	100,0

З табл. 1 видно, що найбільш істотний кількісний вклад (77,7%) вносять операції завантаження операнду, складання, занесення до пам'яті, переходу. Це дає підстави розглядати питання варіації ступеню деталізації формальних специфікацій, з урахуванням відповідного розподілу операцій. Для порівняння, для загального випадку вирішення науково-технічних задач використовується суміш Гібсона, де 40,3% відводяться під операції складання (з фіксованою і плаваючою крапкою), 19% – під операції індексної модифікації (робота з масивами), 17,5% – під операції пересилання даних, що формує 76,8% усього складу операцій [2, с. 69; 16]. Видно, що порівняно із сумішшю Шатл, для Суміші Гібсона відсоткова частка операцій складання у 2,6 рази більша. Таке порівняння дає підстави сформулювати нижченаведені рекомендації до синтезу формальних моделей (специфікацій), призначених до автоматизованої формальної верифікації методами перевірки на моделі.

Як перша рекомендація пропонується варіювати рівень деталізації формальної специфікації (фрагментів специфікації). Це означає, що доцільно враховувати характер розподілу операцій для заданої предметної області застосування програмної СКП (табл. 1). Відповідно до цього розподілу встановлювати ступінь деталізації фрагментів специфікації для операцій (конструкцій), що є більш поширеними, для менш поширених операцій – нижчий. При цьому, зважаючи на складність СКП та експоненційний характер зростання обчислювальних витрат на верифікацію від кількості змінних стану системи переходів [17], заданої формальною специфікацією, на прикладі системи управління орієнтацією космічного апарату (тисячі рядків програмного коду), доречно перейти від представлення операцій змінними станів системи переходів до представлення конструкцій на основі цих операцій (фрагментів програмного коду) змінними станів. При цьому виникає ряд супутніх завдань, що потребують вирішення. Відповідним прикладом є знаходження компромісу між рівнем деталізації формальної специфікації (фрагментів специфікації), а також доступними обчислювальними ресурсами і часовими обмеженнями. Цей компроміс своєю чергою має бути орієнтованим на одержання корисного ефекту від здійснення формальної верифікації, що може проявлятися у виявленні помилок проектних рішень чи підтвердженні їх відсутності. При цьому постає інше питання – наскільки правомірно судити відносно коректності тих чи інших проектних рішень на основі відповідних моделей (специфікацій). Мається на увазі підвищення вимог до адекватності названих моделей.

Поштовхом у напрямі сприяння підвищенню рівня довіри до адекватності формальних моделей передбачається наступна рекомендація: будувати також аналітичні моделі на основі структури Кріпке і порівнювати результати аналізу таких моделей із статистичними даними, одержуваними під час автоматизованої перевірки відповідних формальних специфікацій [17].

Розглядаючи проектування як ітераційний процес [18], доцільним вбачається також забезпечення автоматизації процедури синтезу формальних специфікацій – заключна рекомендація. Кроком у цьому напрямі може бути використання допоміжних формалізмів більш високих рівнів абстракції, ніж формалізм цільової специфікації, і засобів генерації цільових специфікацій на основі таких моделей з вищим рівнем абстракції. Демонстративним прикладом може слугувати алгоритмічна мова PlusCal [19], що використовується як

проміжна ланка для синтезу цільової специфікації на мові TLA+ [20], призначеної до автоматизованої формальної верифікації методом перевірки на моделі TLC (TLA Checker) [21].

Висновки. Таким чином, в роботі було проаналізовано аспекти застосування формальних методів для перевірки систем критичного призначення, а саме програмного складника названих систем. За результатами проведеного аналізу сформульовано наступні рекомендації:

1. Враховувати характер розподілу операцій для заданої предметної області. У якості останньої розглянуто космічну галузь і відповідну систему керування орієнтацією космічного апарату.

2. Для підвищення ступеню довіри до результатів верифікації формальної специфікації методом перевірки на моделі перевіряти адекватність формальних моделей також шляхом співставлення результатів аналізу аналітичних моделей на основі структури Кріпке з результатами автоматизованої перевірки формальних моделей.

3. З позиції ітераційного погляду на процес проектування використовувати засоби автоматизації процесу синтезу формальних специфікацій. Для синтезу специфікацій з більш високим рівнем абстракції як допоміжний засіб запропоновано використовувати алгоритмічну мову PlusCal.

Список літератури:

1. Харченко В.С. Аналіз проблем IT-інженерії безпеки: проект TEMPUS-SAFEGUARD. *Радіоелектронні і комп'ютерні системи*. 2010. № 7 (48). С. 297–300.

2. Конорев Б.М., Манжос Ю.С., Харченко В.С., Алексеев Ю.Г., Сергиенко В.В., Чертков Г.Н. *Инвариантно-ориентированная оценка качества программного обеспечения космических систем* / под ред. Б.М. Конорева, В.С. Харченко. Харьков : Государственный центр регулирования качества поставок и услуг, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», 2009. 224 с.

3. Омельчук Л.Л. *Формальні методи специфікації програм* : навч. посібник. Київ : УкрІНТЕІ, 2010. 78 с.

4. Sharvia S., Papadopoulos Y. Integrating model checking with HiP-HOPS in model-based safety analysis. *Reliability engineering & system safety*. 2015. Vol. 135. P. 64–80.

5. Кларк Э.М., Грамберг О., Пелед Д. *Верификация моделей программ*: *Model checking* : пер. с англ. / под ред. Р. Смелянского. Москва : МЦНМО, 2002. 416 с.

6. Reinertsen D.G. *The principles of product development flow: second generation lean product development* : 1st ed. Redondo Beach, CA : Celeritas Publishing, 2009. 304 p.

7. Харченко В.С., Скляр В.В., Конорев Б.М., Алексеев Ю.Г., Чертков Г.Н., Засуха С.А., Семенов Л.П. *Оценка и обеспечение качества программных средств* / под ред. Б.М. Конорева, В.С. Харченко. Харьков : Государственный центр регулирования качества поставок и услуг, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», 2007. 244 с.

8. IEEE 1012-2016. IEEE Standard for system, software, and hardware verification and validation. [Approved 28 September 2017].

9. Leucker M., Schallhart C. A brief account of runtime verification. *The journal of logic and algebraic programming*. 2009. Vol. 78, No. 5. P. 293–303.

10. Петрик В.Л. Экспертиза программного обеспечения информационно-управляющих систем с использованием дескрипторного семантического пространства. *Радіоелектронні і комп'ютерні системи*. 2007. № 2 (21). С. 29–35.

11. 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 on Software Reliability Engineering Workshops (Toulouse, France, 23-26 October 2017). P. 146–152.

12. Pakonen A., Tahvonen T., Hartikainen M., Pihlanko M. Practical applications of model checking in the Finnish nuclear industry. *Nuclear Plant Instrumentation, Control and Human Machine Interface Technologies* : Proc. 10th International Topical Meeting (San Francisco, CA, USA, 11–15 June 2017). P. 1342–1352.

13. 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.

14. ECSS-E-00A. Space engineering. Policy and principles. [Cancelled]. The Netherlands : ESA Publications Division, 1996. 46 p.

15. ECSS-S-ST-00C – ECSS system. Description, implementation and general requirements. [Чинний від 2008-07-31]. AG Noordwijk, The Netherlands : ESA Requirements and Standards Division, 2008. 34 p. URL: https://ecss.nl/standard/ecss-s-st-00c-description-implementation-and-general-requirements-31-july-2008/ (дата звернення: 09.11.2019).

16. Феррари Д. *Оценка производительности вычислительных систем* : пер. с англ. Горлина А.И. / под ред. В.В. Мартынюка. Москва : Мир, 1981. 576 с.

17. 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.

18. Ларман К. *Применение UML и шаблонов проектирования* : 2-е изд. / пер с. англ. Москва : Издательский дом «Вильямс», 2004. 624 с.

19. Lamport L. The PlusCal algorithm language. *Theoretical Aspects of Computing* : 6th Int. Colloquium, part of LNCS, (Kuala Lumpur, Malaysia, Aug. 2009), vol. 5684. P. 36–60.

20. Shkarupylo V., Kudermetov R., Timenko A., Polska O. On the Aspects of IoT Protocols Specification and Verification. *Problems of Infocommunications. Science and Technology* : 2019 International Scientific-Practical Conference (Kyiv, Ukraine, October 8-11, 2019). P. 93–96.

21. Lamport L. *Specifying systems: The TLA+ language and tools for hardware and software engineers*. Boston: Addison-Wesley, 2002. 382 p.

Shkarupylo V.V., Evdokimov V.F., Dusheba V.V. FORMAL METHODS USAGE WITH RESPECT TO CRITICAL SYSTEMS CHECKING

Nowadays, the usage of formal methods becomes more and more widespread in different spheres. The ways of these methods usage encompass diverse scenarios of both commercial and non-commercial nature. Special attention here is paid to safety-critical systems the systems, where the faults and failures can lead to critical consequences. The examples of corresponding domains are the space industry, energetics, etc. In given work the accent is put on model checking methods the representatives of formal methods. The definitive feature of the latter is the ability to automate the procedure of such methods usage. It is considered as a positive factor from the viewpoint of its practical applicability. The significant drawback though is the exponential growth of verification procedure time costs from the number of transition system's state variables. This peculiarity fosters the need for searching the tradeoffs with respect to the outcome of verification process, corresponding time costs and available computational resources. In paper, the accent is put on software constituent of safety-critical systems. Taking into consideration the complexity of such systems and the aforementioned drawback of model checking methods, the goal of work conducted is formulated as follows: analyze the aspects of formal methods usage with respect to safety-critical systems checking. As a result of the analysis conducted, the recommendations to model checking methods usage while designing safety-critical systems have been formulated. As a representative example, the space industry domain has been covered spacecraft orientation control system has been considered. Basing on the results of previously conducted experiments, the recommendations to formal methods usage while designing the safety-critical systems have been formulated.

Key words*: model checking, formal specification, verification, safety-critical system, systems approach.*