УДК 004.94
DOI https://doi.org/10.32782/2663-5682/2024/41/22

В. І. Салагор
здобувач вищої освіти ступеня доктора філософії
за спеціальністю 123 – Комп'ютерна інженерія
факультету кібербезпеки, програмної інженерії та комп'ютерних наук
Міжнародний гуманітарний університет
м. Одеса, Україна

МЕТОДИ ВЕРИФІКАЦІЇ КОМП'ЮТЕРНИХ СИСТЕМ КРИТИЧНОГО ПРИЗНАЧЕННЯ

Анотація. *Верифікація комп'ютерних систем критичного призначення є ключовим етапом забезпечення їх надійності та безпеки. Ці системи, що використовуються в умовах підвищених ризиків, потребують спеціальних підходів для тестування та аналізу. У статті розглядається методика верифікації на основі діагностичних експериментів, проведених в інтерактивних комп'ютерних мережах. Описуються основні етапи моделювання системи, визначення критичних сценаріїв, розробка та проведення діагностичних експериментів. Наводяться переваги та недоліки використання інтерактивних мереж для верифікації систем критичного призначення.*

Ключові слова: *вирифікація, комп'ютерні системи критичного призначення, діагностичні експерименти, інтерактивні комп'ютерні мережі, надійність.*

В умовах стрімкого розвитку інформаційних технологій і їх проникнення в усі сфери людської діяльності, забезпечення надійності та безпеки комп'ютерних систем критичного призначення стає однією з найважливіших задач сучасної інженерії. Такі системи використовуються в галузях, де навіть найменші збої можуть призвести до серйозних наслідків, включаючи втрату даних, фінансові збитки, порушення функціонування життєво важливих інфраструктур, а також загрозу для життя та здоров'я людей. Тому верифікація таких систем, що полягає у всебічному тестуванні та підтвердженні їхньої відповідності визначеним вимогам, є критично важливою.

Діагностичні експерименти в інтерактивних комп'ютерних мережах надають можливість проводити комплексне тестування систем в умовах, наближених до реальних, з урахуванням різноманітних факторів та сценаріїв, що можуть виникнути під час їх експлуатації [1]. Інтерактивні мережі дозволяють моделювати складні ситуації та перевіряти реакцію системи на них, що сприяє виявленню потенційних вразливостей і підвищенню надійності кінцевого продукту [2].

Актуальність дослідження в даній області обумовлена також зростанням вимог до забезпечення кібербезпеки. У світі, де загрози кіберзлочинів і атак на критичні інфраструктури стають усе більш поширеними, розробка та впровадження ефективних моделей верифікації комп'ютерних систем є надзвичайно важливим завданням [3]. Це дослідження спрямоване на розробку таких моделей, що враховують сучасні вимоги до безпеки та надійності, а також забезпечують високий рівень достовірності результатів діагностичних експериментів.

Таким чином, розробка та впровадження моделей верифікації комп'ютерних систем критичного призначення на основі діагностичних експериментів в інтерактивних комп'ютерних мережах є важливим науково-технічним завданням, що відповідає сучасним викликам та потребам у галузі інформаційної безпеки та надійності систем.

Комп'ютерні системи критичного призначення виконують життєво важливі функції в багатьох сферах, таких як авіація, медицина, енергетика та військова справа. Будь-який збій в таких системах може мати катастрофічні наслідки, тому їх надійність і безпека є першочерговим завданням. Верифікація таких систем повинна бути всебічною, охоплювати різноманітні сценарії використання та забезпечувати виявлення потенційних проблем до того, як система буде впроваджена у реальну експлуатацію [1].

Моделювання системи є першим і надзвичайно важливим етапом процесу верифікації. Воно полягає у створенні математичної або формальної моделі, яка точно відображає функціональні можливості системи та її обмеження. Для цього можуть використовуватися різні методи [2, 4], зокрема скінченні автомати, мережі Петрі та інші підходи.

Наступним етапом є визначення критичних сценаріїв, які представляють найбільший ризик для надійної роботи системи. Такі сценарії можуть включати збій апаратного забезпечення, помилки програмного забезпечення, порушення безпеки або відмови комунікаційних засобів.

Розробка діагностичних експериментів полягає у створенні тестів, що дозволяють перевірити коректність роботи системи в умовах, наближених до реальних. Інтерактивні комп'ютерні мережі є ефективним інструментом для проведення таких експериментів, оскільки вони дозволяють моделювати взаємодію між різними компонентами системи в реальному часі. Це забезпечує виявлення потенційних проблем у комунікації між ними.

Після проведення діагностичних експериментів здійснюється детальний аналіз результатів. Це дозволяє виявити можливі недоліки у роботі системи та вжити необхідних заходів для їх усунення. У разі виявлення помилок, система доопрацьовується і проходить повторну перевірку.

Формальна верифікація включає перевірку правильності роботи системи за допомогою методів, таких як модельні перевірки (model checking), математичні доведення та символьне виконання. Верифікація забезпечує підтвердження того, що система відповідає заданим вимогам і буде функціонувати коректно навіть у найкритичніших умовах.

Інтерактивні комп'ютерні мережі мають ряд переваг для верифікації систем критичного призначення:

– Тестування в умовах, максимально наближених до реальних, що забезпечує точність діагностики.

– Можливість охоплення широкого спектру сценаріїв і виявлення більшої кількості потенційних проблем.

– Здатність тестувати систему у великих мережах з багатьма користувачами, що імітує реальне навантаження на систему.

Одним із прикладів використання описаної методики є верифікація авіаційної системи управління повітряним рухом. Ця система повинна забезпечувати безперебійну і надійну роботу, гарантуючи безпеку польотів. Верифікація включає моделювання взаємодії між авіадиспетчерами та літаками в реальному часі, тестування можливостей системи в умовах збою зв'язку та стрес-тестування для перевірки стійкості системи під час надмірного навантаження.

Недоліки використання діагностичних експериментів в інтерактивних комп'ютерних мережах:

1. Проведення діагностичних експериментів в інтерактивних комп'ютерних мережах вимагає значних обчислювальних ресурсів, а також розробки та підтримки складних тестових середовищ. Це може стати суттєвою перешкодою для організацій з обмеженим бюджетом.

2. Інтерактивні комп'ютерні мережі повинні бути точно налаштовані для імітації реальних умов, що може бути складним завданням. Неточності в налаштуванні можуть призвести до некоректних результатів верифікації, що знижує її ефективність.

3. Процес підготовки, проведення та аналізу діагностичних експериментів може займати багато часу, особливо у випадку складних систем. Це може затримати впровадження системи в експлуатацію та збільшити загальний час розробки.

4. Хоча інтерактивні мережі дозволяють тестувати систему у різних сценаріях, деякі унікальні або малоймовірні ситуації можуть залишитися непоміченими. Це особливо актуально для систем, що працюють в умовах високої невизначеності або нестабільності.

5. Надійність результатів діагностичних експериментів залежить від якості використовуваного програмного забезпечення для моделювання та тестування. Помилки або вразливості в програмному забезпеченні можуть спотворювати результати експериментів.

6. Незважаючи на реалістичність моделювання, існує ризик, що умови, створені в інтерактивних мережах, не повністю відображатимуть реальні умови експлуатації системи. Це може призвести до невиявлення деяких проблем, які можуть проявитися під час реальної роботи системи.

7. Діагностичні експерименти в інтерактивних мережах часто генерують величезні обсяги даних, аналіз яких може бути складним і вимагати спеціалізованих інструментів і методів. Це може збільшити час і витрати на аналіз та прийняття рішень.

8. Інтерактивні комп'ютерні мережі можуть бути вразливими до зовнішніх факторів, таких як мережеві збої або кіберзагрози, які можуть вплинути на результати діагностичних експериментів і створити додаткові ризики.

9. Робота з інтерактивними комп'ютерними мережами та проведення діагностичних експериментів вимагає висококваліфікованих спеціалістів, які мають досвід у галузі комп'ютерних мереж, програ-

мування та системного аналізу. Це може ускладнити процес залучення персоналу та збільшити витрати на навчання.

Діагностичні експерименти в інтерактивних комп'ютерних мережах використовуються для виявлення, локалізації та усунення помилок, вразливостей або інших відхилень у роботі систем критичного призначення. Розглянемо кілька прикладів таких експериментів.

Тестування навантаження (Load Testing). Цей тип експерименту спрямований на перевірку того, як система працює під високим навантаженням. У ході тестування навантаження на систему поступово збільшується, щоб оцінити її продуктивність, визначити максимальне навантаження, яке система може витримати, та ідентифікувати точки, в яких відбуваються збої. Наприклад, естування веб-сервера, що обслуговує критичні медичні дані, з імітацією одночасного доступу тисяч користувачів. Метою є виявлення моменту, коли система починає сповільнюватися або давати збої.

Тестування відмовостійкості (Failover Testing). Це експеримент для перевірки здатності системи перемикатися на резервний вузол або режим у разі відмови основного компонента. Це дозволяє оцінити, наскільки швидко система може відновитися після збою та наскільки добре зберігається цілісність даних. Наприклад, Перевірка працездатності банківської системи при раптовому відключенні одного з серверів бази даних. Експеримент оцінює, чи відбудеться автоматичне переключення на резервний сервер без втрати даних та значної затримки в роботі системи.

Тестування безпеки (Security Testing). Діагностичні експерименти з безпеки включають перевірку вразливостей, які можуть бути використані зловмисниками для отримання несанкціонованого доступу до системи або порушення її роботи. Це можуть бути як автоматизовані сканування на вразливості, так і імітація атак. Наприклад, Імітація DDoS-атаки на мережевий шлюз підприємства з метою перевірки його здатності виявляти та нейтралізувати загрозу, не допустивши збоїв у роботі внутрішніх систем.

Тестування часу відгуку (Response Time Testing). Цей вид тестування оцінює, як швидко система реагує на запити користувачів або зовнішніх систем. Час відгуку є критичним для систем, де затримки можуть призвести до значних фінансових або навіть людських втрат. Наприклад, Перевірка системи управління авіаційним трафіком, яка повинна в режимі реального часу обробляти запити від десятків літаків і надавати відповіді протягом декількох мілісекунд.

Тестування збоїв у мережі (Network Fault Testing). Цей тип експерименту спрямований на перевірку стійкості системи до проблем з мережею, таких як затримки, втрата пакетів, або розриви з'єднання. Це дозволяє оцінити, як система справляється з мережевими проблемами, зберігаючи при цьому функціональність. Наприклад, Імітація втрати пакетів даних у системі моніторингу критичних промислових процесів, щоб перевірити, чи система здатна коректно обробляти неповні або затримані дані і відновлюватися після відновлення з'єднання.

Наведені приклади діагностичних експериментів допомагають оцінити надійність і стійкість комп'ютерних систем критичного призначення в умовах реальних експлуатаційних викликів.

Метою даного дослідження є розробка та вдосконалення моделей верифікації комп'ютерних систем критичного призначення з використанням діагностичних експериментів в інтерактивних комп'ютерних мережах. Дослідження спрямоване на:

1. Аналіз існуючих підходів та методів верифікації комп'ютерних систем критичного призначення, визначення їхніх переваг та недоліків.
2. Розробку нових моделей та методик діагностичних експериментів, що забезпечують ефективне тестування та перевірку надійності комп'ютерних систем у реальних умовах експлуатації.
3. Інтеграцію моделей діагностичних експериментів в процес верифікації комп'ютерних систем критичного призначення, з урахуванням специфіки їхнього функціонування та вимог до безпеки.
4. Підвищення точності та ефективності виявлення можливих збоїв та вразливостей у роботі систем шляхом застосування інтерактивних комп'ютерних мереж для моделювання реальних умов та сценаріїв.
5. Оцінку результатів та розробку рекомендацій щодо впровадження запропонованих моделей верифікації в практичну діяльність для підвищення надійності та безпеки комп'ютерних систем критичного призначення.

Дослідження також має на меті продемонструвати можливості вдосконалення існуючих підходів до верифікації та надати науково обґрунтовані рекомендації щодо їхнього застосування в умовах сучасних кіберзагроз.

Отже, верифікація комп'ютерних систем критичного призначення на основі діагностичних експериментів в інтерактивних комп'ютерних мережах є важливим інструментом для забезпечення їх надійності та безпеки. Ця методика дозволяє проводити комплексні перевірки системи у різних сценаріях, забезпечуючи тим самим високу точність та повноту виявлення потенційних проблем. Подальші дослідження та розробки в цій галузі повинні бути спрямовані на вдосконалення методів діагностики та тестування, а також на підвищення ефективності процесу верифікації критично важливих систем.

ЛІТЕРАТУРА

1. Шкарупило В.В. Сценарії, методи та засоби формальної верифікації артефактів процесу проєктування систем критичного призначення: монографія В.В. Шкарупило, І.В. Блінов. – Вінниця: ГО «Європейська наукова платформа», 2021, 104 с.
2. Давидов В.В. Моделі та методи підвищення безпеки програмного забезпечення (монографія). Харків, 2021, 146 с.
3. Мірошник М.А. Обробка подій у цифрових пристроях реального часу. / Мірошник М.А., Шкіль О.С., Рахліс Д.Ю., Пшеничний К.Ю., Мірошник А.Н. / Збірник наукових праць «Вісник ЧДТУ», № 2, 2023, С. 50–57.
4. Негуриця Д.С. Адаптивність та адаптованість програмного забезпечення систем критичного призначення / Д.С. Негуриця // Радіоелектронні і комп'ютерні системи, № 6, 2014, С. 48–52.

V. Salagor. Methods for verification of Safety-Critical Computer Systems. – Article.

Summary. *Verification of critical computer systems is a key step in ensuring their reliability and security. These systems, used in high-risk environments, require special approaches for testing and analysis. The article examines the verification technique based on diagnostic experiments conducted in interactive computer networks. The main stages of system modeling, determination of critical scenarios, development and conducting of diagnostic experiments are described. Advantages and disadvantages of using interactive networks for verification of critical purpose systems are given.*

Key words: *verification, critical purpose computer systems, diagnostic experiments, interactive computer networks, reliability.*