DOI https://doi.org/10.36059/978-966-397-479-8-133

АНАЛІЗ МЕТОДІВ ТА МОДЕЛЕЙ ВЕРИФІКАЦІЇ КОМП'ЮТЕРНИХ СИСТЕМ КРИТИЧНОГО ПРИЗНАЧЕННЯ З ВИКОРИСТАННЯМ ДІАГНОСТИЧНИХ ЕКСПЕРИМЕНТІВ

Салагор В. І.
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

Комп'ютерні системи критичного призначення є важливими компонентами багатьох галузей, таких як транспорт, енергетика та медицина, де від них залежить безпека користувачів і надійність інфраструктур. Ключовою вимогою до таких систем є безпомилкова робота у визначених умовах, що досягається за допомогою різних методів верифікації, таких як модельна перевірка, формальна верифікація та діагностичні експерименти. Діагностичні експерименти дозволяють виявляти й аналізувати відмови, забезпечуючи тим самим підвищену надійність систем у реальних умовах експлуатації.

Тестування на основі діагностичних експериментів дозволяє імітувати аварійні ситуації або сценарії відмов з метою оцінки готовності системи до коректної реакції на потенційні помилки [1]. Це особливо важливо для інтерактивних мереж, де діагностичні експерименти дозволяють перевірити ефективність відновлення системи після збоїв та надійність її складових. Основною перевагою є реалістичність перевірки, адже метод дозволяє виявити недоліки, які не завжди можливо визначити під час інших типів тестування.

Верифікація в реальному часі (runtime verification) застосовується для перевірки поведінки системи під час її фактичного функціонування [2]. Цей підхід передбачає моніторинг поточного стану системи й виявлення можливих відхилень у її роботі. Особливість цього методу полягає в його здатності забезпечувати високу швидкість реагування на можливі загрози або помилки, що є важливим для критичних систем, які функціонують у реальному часі.

Одним із сучасних підходів є співпраця між забезпеченням безпеки та надійності при верифікації критичних систем [3]. Це дозволяє оптимізувати процеси тестування та забезпечити комплексну надійність

комп'ютерних систем критичного призначення. Дослідження вказують на важливість розробки інтегрованих підходів, що дозволяють забезпечити як фізичну безпеку системи, так і її інформаційну захищеність.

Незважаючи на значні досягнення в галузі верифікації комп'ютерних систем критичного призначення, існує низка нерозв'язаних проблем. По-перше, обмеженість обчислювальних ресурсів для виконання верифікації великих інтерактивних мереж залишається актуальною. Крім того, висока вартість діагностичних експериментів у критичних системах потребує значних витрат на спеціальне устаткування і тестові середовища. Існує також потреба у розробці методів інтеграції верифікаційних і безпекових процесів для забезпечення комплексного захисту систем.

Виходячи з цього, основними актуальними завданнями залишаються такі: розробка ефективних методів масштабованої модельної перевірки, які можуть бути застосовані до великих інтерактивних мереж; вдосконалення методів діагностичних експериментів для оптимізації часу і ресурсів, необхідних для тестування складних критичних систем; інтеграція методів реального часу в системи безпеки та моніторингу для підвищення швидкості реакції системи на можливі загрози; розробка комплексних верифікаційних платформ, що дозволять об'єднати кілька методів верифікації в одну систему для зручності користування і підвищення ефективності.

Діагностичні експерименти, модельна перевірка та runtime verification є ключовими елементами забезпечення надійності систем, однак вони потребують вдосконалення для оптимального застосування у складних і динамічних середовищах.

Література:

1. Kassab M. Testing Practices of Software in Safety Critical Systems: Industrial Survey. In *Proceedings of the 20th International Conference on Enterprise Information Systems*. Volume 2: ICEIS; SciTePress, 2018, pp. 359–367. DOI: 10.5220/0006797003590367

2. Ceresa M., Gorostiaga F., Sánchez C. Declarative stream runtime verification (hLola). In: Oliveira, B.C.S. (ed.) APLAS 2020. LNCS, vol. 12470, 2020, pp. 25–43. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-64437-6_2

3. Gleirscher M., Kugele S., & Calinescu R. Safety and Security Co-engineering: A Comprehensive Survey. *ACM Computing Surveys*, 53(5), 2020, 102 p.