УДК 519.718

К.т.н., доцент Романкевич В.О., аспірант Мораведж Сейєд Мілад, магістрант Полєщук С.О.

Національний технічний університет України «Київський політехнічний інститут»

ОЦІНКА ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ ВІДМОВОСТІЙКИХ БАГАТОПРОЦЕСОРНИХ СИСТЕМ, ЩО РЕКОНФІГУРУЮТЬСЯ

Abstract

Vitaliy O. Romankevych, assoc. prof., PhD; Moravej Seyed Milad, postgraduate; Sergiy Poleschuk, student

Functional safety evaluation for the reconfigurable fault-tolerant multiprocessor control systems

This paper concerns the task of the functional safety evaluation for the reconfigurable fault-tolerant multiprocessor control systems. The concepts of reconfigurable fault-tolerant multiprocessor systems and functional safety are given. The modified method of the functional safety evaluation for the fault-tolerant multiprocessor control systems is proposed.

Вступ

Відмовостійкі багатопроцесорні системи (ВБС) сьогодні застосовуються все частіше завдяки двом своїм суттєвим якостям. Перша – висока продуктивність, що дозволяє розв'язувати з їх допомогою складні задачі з великими обсягами оброблюваних даних. Друга – висока надійність, завдяки чому такі системи все частіше знаходять застосування в якості систем управління критичними об'єктами. Критичними називатимемо такі об'єкти, що становлять потенційну загрозу для життя і здоров'я людини, можуть негативно впливати на довкілля, завдавати збитків у матеріальній чи будь-якій іншій формі.

Завдяки закладеній на етапі проектування структурній і часовій надлишковості, реконфігуровні ВБС здатні самі себе тестувати, виявляти модулі, що відмовили, вилучати їх з роботи, реконфігуруватися та продовжувати виконання всіх функцій у повному обсязі.

На відміну від однорідних обчислювальних систем, ВБС управління складними об'єктами складаються з декількох підсистем, кожна з яких має свою ступінь відмовостійкості, різну кількість процесорів, відмінних між собою як за продуктивністю, так і за надійністю, різні шини та ін.

Незважаючи на численні дослідження в області методів оцінки та підвищення надійності ВБС, у тому числі реконфігуровних ВБС управління складними об’єктами [1], проблема функціональної безпеки таких систем досі є малодослідженою. У даній роботі розглядається метод оцінки функціональної безпеки реконфігуровних ВБС управління об’єктами критичного застосування, що базується на аналізі ризиків.

Функціональна безпека як складова гарантоздатності

Останнім часом поняття «гарантоздатність» використовується все частіше, розширюючи поняття «надійність». Надійність – це властивість об’єкта зберігати у часі в межах встановлених границь значення всіх параметрів, які характеризують здатність виконувати задані функції у заданих режимах та умовах застосування, технічного обслуговування, зберігання та транспортування. Надійність є комплексною властивістю, яка включає в себе безвідмовність, довговічність, ремонтопридатність і збережуваність [2].

Гарантоздатність – це комплексна властивість системи надавати необхідні послуги, яким можна виправдано довіряти. Гарантоздатність включає в себе безвідмовність, готовність, живучість, функціональну безпеку, цілісність, конфіденційність, достовірність та складність обслуговування [3, 4].

Розглянемо поняття функціональної безпеки, яке нас цікавить. Згідно з [5], це властивість системи виконувати задані функції без недопустимого ризику створення ним аварійних станів, які можуть призвести до загибелі, травмування, погіршення здоров’я людей, негативного впливу на довкілля, завдання визначеного матеріального чи іншого збитку. Інакше кажучи, функціональна безпека – це властивість усувати або мінімізувати шкідливі (катастрофічні) наслідки при відмовах для користувачів, інших систем та навколишнього середовища [3].

Гарантоздатна система у загальному випадку має множину роботоздатних, частково роботоздатних і нероботоздатних станів. Непрацездатні, в свою чергу, можна поділити на дві підмножини: безпечних (захисних) та небезпечних (аварійних) станів. Небезпечними називають відмови, які переводять систему до нероботоздатного небезпечного (аварійного) стану. Всі інші стани системи вважаються функціонально безпечними. Таким чином, у загальному випадку, підвищення функціональної безпеки системи полягає у мінімізації ймовірності переходу стану системи з множини безпечних (працездатних, частково роботоздатних і нероботоздатних) до множини небезпечних.

Ризик-орієнтована оцінка безпеки

Ризик – одна з основних категорій безпеки. Під ризиком розуміють потенціальну можливість порушення роботоздатного стану технічного комплексу та пов'язаний з цим збиток. Зокрема розглядаючи ризики системи управління, визначають вплив її відмови на загальну безпеку, а збиток полягає у зниженні рівня безпеки технічного комплексу в цілому [6].

Згідно з [3, 5, 6], ризик *R(t)* за час *t*, пов’язаний з деякою подією, визначається як добуток імовірності цієї події *P(t)* на негативні наслідки *D*, спричинені цією подією:

$$R(t) = P(t) \cdot D \qquad (1)$$

Важливо зауважити, що ризик – безрозмірна величина, оскільки *D* відображає сукупність всіх можливих негативних наслідків одним значенням. Крім того, значення ризику часто використовують в якості показника безпеки [3].

Оцінка безпеки відмовостійких багатопроцесорних систем

Зазначимо, що у формулі (1) величина *D* визначається об’єктом управління, тому не будемо заглиблюватися в особливості її отримання. Розглядаючи ВБС управління, зупинимося саме на величині *P(t)*, яку можна, спираючись на описане вище, назвати ймовірністю переходу системи до небезпечного стану на часовому інтервалі *t*.

Щоб визначити, чим можна охарактеризувати цей небезпечний стан, повернемося до поняття надійності. При її оцінці перш за все звертають увагу на ймовірність безвідмовної роботи $P_{б.р}$. У випадку реконфігуровних ВБС ця величина визначається як імовірність того, що продуктивність *S* ВБС на часовому інтервалі *t* буде зберігатися на рівні не нижче S^*, який є необхідним для забезпечення роботоздатності (розв’язання всіх функціональних задач, які стоять перед системою) [1]:

$$P_{á.ð}(t) = P(S(t) \geq S^*)$$

Тоді, взявши продуктивність ВБС за основу оцінки її стану, можна ввести додаткове граничне значення продуктивності, крім S^*. При зниженні продуктивності ВБС в результаті відмов процесорів нижче S^*, система деградує та переходить до частково працездатного стану. При подальших відмовах процесорів продуктивність системи може стати нижчою, ніж деякий рівень $S^*_{зах}$, необхідний для виконання функцій безпеки, що в результаті призведе до аварії.

Функціями безпеки (чи захисними функціями) будемо називати мінімальну підмножину функцій системи, виконання яких необхідно, щоб

система не перейшла до небезпечного стану. Позначимо функції безпеки як $f^*_{\text{зах } i}$. Очевидно, що ці функції мають найвищий пріоритет, і у випадку переходу системи до частково роботоздатного стану, вони повинні виконуватись у повному об'ємі.

Нехай загальна кількість функцій безпеки дорівнює m, а функція безпеки $f^*_{\text{зах } i}$ для свого виконання потребує продуктивності $S^*_{\text{зах } i}$. Тоді:

$$S^*_{\text{çàõ}} = \sum_{i=1}^{m} S^*_{\text{çàõ}\,i}$$

Тепер, повертаючись до оцінки безпеки реконфігуровних ВБС, можна сказати, що ймовірність $P_{\text{н.с}}$ переходу системи на часовому інтервалі t до небезпечного стану дорівнює ймовірності того, що продуктивність S ВБС на часовому інтервалі t стане нижчою, ніж продуктивність $S^*_{\text{зах}}$, яка є необхідною для виконання функцій безпеки:

$$P_{\text{í.ñ}}(t) = P(S(t) < S^*_{\text{çàõ}})$$

Наведемо один з можливих алгоритмів отримання величини $P_{\text{н.с}}$.

Серед усіх векторів стану ВБС w виділимо множину $W_{\text{н}}$, яка відповідає небезпечним станам системи:

$$S_w = \sum_{i=1}^{n} \alpha_i s_i \le S^*_{\text{çàõ}} \Rightarrow w \in W_{\text{í}},$$

де S_w – продуктивність ВБС у стані, що відповідає вектору w;

n – кількість процесорів у системі; α_i – компонента вектора w, яка відповідає стану i-го процесора (0 – відмова, 1 – працездатність); s_i – продуктивність i-го процесора.

Знаючи або розраховуючи ймовірності безвідмовної роботи $p(x_i)$ кожного процесора на часовому інтервалі t, можна визначити ймовірність виникнення кожного з можливих небезпечних станів:

$$\forall w \in W_{\text{í}},\ P_w(t) = \prod_{i=1}^{n} \tilde{p}(x_i), \quad (2)$$

де

$$\tilde{p}(x_i) = \begin{cases} p(x_i), \text{ ÿêùî } \alpha_i = 1, \\ 1 - p(x_i), \text{ ÿêùî } \alpha_i = 0. \end{cases}$$

Тепер можна обчислити ймовірність переходу ВБС на часовому інтервалі t до небезпечного стану:

$$P_{\text{í.ñ}}(t) = \sum_{w \in W\text{í}} P_w(t). \quad (3)$$

(2) та (3) можна об'єднати в одну формулу, яка максимально повно віддзеркалює сенс величини, котру обчислюємо:

$$P_{\text{í.ñ}}(t) = \sum_{w \in W_{\text{í}}} \prod_{i=1}^{n} (p(x_i))^{\alpha i} (1 - p(x_i))^{1-\alpha i}.$$

Висновки

Задача оцінки функціональної безпеки реконфігуровних ВБС управління критичними об’єктами виникає у зв’язку зі специфікою таких об’єктів. Застосовуючи ризик-орієнтований підхід при оцінці безпеки, задачу можна звести до двох підзадач: кількісної оцінки негативних наслідків, які можуть наступити в результаті аварії, та розрахунку ймовірності виникнення аварійного стану. В роботі отримано формулу, яка дозволяє обчислити зазначену ймовірність, спираючись на продуктивність процесорів у якості одного з параметрів.

Література

1. *Романкевич А.М.* О повышении надежности реконфигурируемых відмовостійкых багатопроцесорных систем управления сложными объектами / Романкевич А.М., Романкевич В.А., Мораведж Сейед Милад // Электронное моделирование. – 2010. – Т.32. № 4. – С. 85-92.
2. ДСТУ 2860-94. Надійність техніки. Терміни та визначення.
3. *Бахмач Е.С.* Отказобезопасные информационно-управляющие системы на программируемой логике / Е.С. Бахмач, А.Д. Герасименко, В.А. Головир и др.; под ред. В.С. Харченко, В.В. Скляра. – Х.: Национальный аэрокосмический университет «ХАИ»; Кировоград: НПО «Радий», 2008. – 380 с.
4. *Харченко В.С.* Гарантоздатність комп’ютерних систем: межа універсальності в контексті інформаційно-технічоного стану // Радіоелектронні і комп’ютерні системи. – 2007. № 8. – С. 7-14.
5. ДСТУ 4178-2003. Комплекси технічних засобів систем керування та регулювання руху поїздів. Функційна безпечність і надійність.
6. *Ястребенецкий М.А.* Безопасность атомных станций: Информацион-ные и управляющие системы / Ястребенецкий М.А., Васильченко В.Н., Виноградская С.В. и др.; Под ред. Ястребенецкого М.А. – К.: Техніка, 2004. – 472 с.