УДК 681.3.06

О.А. Зеленков, канд. техн. наук
О.О. Бунчук
О.Г. Мірошниченко, канд. техн. наук

МЕТОДИ ОЦІНКИ НАДІЙНОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ВІДМОВОСТІЙКИХ СИСТЕМ АВІОНІКИ

Національний авіаційний університет, fsu@nau.edu.ua

Розглянуто задачу оцінки надійності програмного забезпечення бортових відмовостійких обчислювальних систем на різних етапах життєвого циклу. Запропоновано різні методи оцінки надійності, які враховують "внутрішні" характеристики програмного модуля, результати тестового контролю, а також різні ймовірнісні характеристики процесу виконання програми.

Вступ

Архітектура інтегрально-модульної авіоніки (IMA) впроваджується на борт літаків цивільної авіації з використанням усіх переваг принципу відмовостійкості. Концепції відмовостійкості розробляються для задоволення вимог високої надійності з метою досягнення можливості програмованої експлуатації, тобто технічного обслуговування за плановою основою. Якщо у відмовостійкій системі модуль або функція в модулі відмовляють, то для нейтралізації несправності система повинна автоматично здійснити реконфігурацію, а потім продовжувати задовільно працювати до запланованого технічного обслуговування.

Аналіз проблеми

Важливим елементом IMA є її програмне забезпечення (ПЗ). Апаратура забезпечує ефектричний інтерфейс, у той час як функції управління літаком переважно реалізуються модулями ПЗ. Як правило, досить складні системи мають тенденцію проектувати свою складність і на ПЗ, що, у свою чергу, підвищує потенційну небезпеку залишкових помилок проектування, тому методи забезпечення відмовостійкості повинно застосовувати і до реалізації ПЗ.

Основним методом забезпечення відмовостійкості є *N*-варіантне програмування, при якому та сама задача розв'язується декількома програмами, розробленими незалежно. Ці програми можуть виконуватися послідовно тим самим процесором або паралельно на декількох процесорах.

Результат голосування, тобто найбільш ймовірне значення розв'язку видається системі. При цьому вважається, що версії не можуть містити ту саму помилку і відмови виникають у них незалежно. Це основне припущення стратегії відмовостійкого ПЗ, яке гарантує коректне функціонування системи в умовах виникнення помилок середовища функціонування (помилок вхідного потоку, помилок апаратури, помилок датчиків тощо) або власних помилок (помилок специфікації).

Для забезпечення ефективності функціонування системи кожен відмінний варіант ПЗ має бути верифікований. Через вартість *N*-варіантне програмування розглядається тільки для функцій із найвищими вимогами до цілісності.

Випадковий характер помилок ПЗ і випадковий характер комбінацій вхідних даних, що викликають появу цих помилок, дає можливість вважати відмови, спровоковані помилками ПЗ, випадковими подіями і, отже, застосовувати апарат математичної статистики для оцінки ймовірності появи таких відмов.

Комплекс програмних модулів (ПМ), що входять до складу ПЗ бортової системи, має задовольняти визначені вимоги до надійності. Для контролю виконання цих вимог існує комплекс випробувань на різних стадіях життєвого циклу програми.

Випробування розроблених програм шляхом тестування не дозволяють перевірити виконання всіх функцій системи при всіх можливих комбінаціях як вхідних, так і управляючих впливів, тобто після проведення випробувань частина помилок залишається невиявленою.

Підтвердження реалізації високих вимог до надійності ПЗ бортових систем управління, як на етапі розробки, так і на всіх наступних стадіях випробувань, а також у період експлуатації є однією з найважливіших задач, для здійснення якої необхідно використовувати аналітичні й експертно-аналітичні методи оцінки надійності ПЗ.

Сучасні підходи не визначають стандартизованих методів розрахунку надійності ПЗ, тому вкажемо на три можливих напрями розв'язання цієї задачі протягом життєвого циклу (див. рисунок): оцінку надійності ПЗ із використанням топологічної моделі програми, оцінку надійності ПЗ із використанням математичної моделі зростання надійності і оцінка вірогідності ПЗ залежно від способу тестування.

Оцінка надійності ПЗ на етапах життєвого циклу

Оцінка надійності програмного забезпечення з використанням топологічної моделі програми

У результаті аналізу тексту вихідної програми будується топологічна модель у вигляді орієнтованого навантаженого графа, що відображає структурні й інформаційні характеристики програми (топологію програми), а також вагові характеристики вершин і зв'язків між ними [1].

Реалізація певного маршруту на графі (при функціонуванні алгоритму) залежить від напрямку передачі управління у предикатних вершинах графа (перехід за умовою).

Випадкові реалізації вхідних даних і випадковий вибір маршруту, обумовлений імовірністю переходу p_{ij} між i-ю і j-ю вершинами графа, визначають статистичний характер дослідження моделі ПМ і комплексу ПМ, що складають ПЗ.

Оцінка середнього значення ймовірності Q відмови ПМ визначається як

$$Q_{\text{ПМ}} = \sum_{L} P(L) \sum_{i \in L} d_i ;$$

$$P(L) = \prod_{(i,j) \in L} p_{ij} ,$$

де $P(L)$ – імовірність проходження L-го маршруту при реалізації алгоритму в ПМ.

При цьому значення вагових характеристик d_i додаються вздовж відповідного маршруту, а вага вершини визначається як

$$d_i = kQm_i ,$$

де k – коефіцієнт, обумовлений частотою проходження малоймовірних маршрутів; Q – оцінка можливої кількості помилок у програмі, нормованих на одну команду; m – кількість операторів, асоційованих із вершиною графа.

Оцінка Q може бути проведена розроблювачем ПЗ на підставі наявних моделей регресії, отриманих раніше шляхом статистичної обробки даних по відмовах подібного типу ПЗ.

У багатьох випадках оцінка ПЗ є експертною оцінкою, що істотно впливає на величину Q.

Розглянутий підхід доцільно використовувати при оцінці надійності декількох версій ПЗ (для порівняння) на етапі їх розробки з метою визначення потенційних можливостей різних реалізацій.

Для високонадійного ПЗ високоцілісних систем, що характеризуються складною розгалуженою структурою моделі, кількість можливих маршрутів уздовж орієнтованого графа може досягати значень $10^5 - 10^8$, а кількісна оцінка надійності може бути проведена методом статистичного моделювання.

Оцінка надійності програмного забезпечення з використанням математичної моделі зростання надійності

Основою кількісної оцінки надійності ПЗ є статистичне тестування, а саме прогнозування надійності ПЗ здійснюється за статистичними даними про відмови або помилки виявлених до кінця періоду тестування ПМ або комплексу ПМ.

Найбільш розповсюдженими моделями є пуассонівські моделі зростання надійності [2], в яких процес виявлення відмов у тестованому ПЗ описується неоднорідним пуассонівським потоком. При цьому вхідні дані вибираються випадковим чином із вхідної області відповідно до прийнятого закону розподілу.

Якщо ПЗ піддається тестуванню протягом часу T, то найбільш важливими кількісними показниками надійності ПЗ можуть бути:

– функція надійності

$$P(\tau/T) = P\{T_k > \tau + T / T_{k-1} = T\} =$$

$$= P\{N(T+\tau) - N(T) = 0\} =$$

$$= \exp\{-[m(T+\tau)] - m(T)\};$$

– очікувана кількість помилок, що залишилися:

$$N_T = N_0 - m(T),$$

де N_0 – кількість помилок на початку тестування; $m(T)$ – середня кількість помилок, виявлених у процесі тестування.

Однією з основних моделей є модель експоненційного зростання надійності ПЗ [3], для якої

$$m(T) = N_0[1 - \exp(-kT)],$$

де k – інтенсивність виявлення окремої помилки.

Тоді

$$P(t/T) = \exp\{-[N_0 - N_0\exp(-k(t+T)) -$$

$$-N_0 + N_0\exp(-kT)]\} = \exp\{-[N_0\exp(-kT) -$$

$$-N_0\exp(-kT)\exp(-kT)]\} = \exp\{-N_0\exp(-kT)\times$$

$$\times[1-\exp(-kT)]\} = \exp\{-m(t)\exp(-kT)\};$$

$$N_T = N_0\exp(-kT).$$

Якщо експериментальні дані являють собою моменти появи n послідовних відмов ПЗ $(t_1, t_2, \ldots t_n)$, то оцінки максимальної правдоподібності параметрів моделі N_0 і k визначаються числовим розв'язанням системи рівнянь:

$$\begin{cases} \dfrac{n}{N_0} - 1 + \exp(-kt_n) = 0; \\ \dfrac{n}{k} - \sum\limits_{i=1}^{n} t_i - N_0 t_n \exp(-kt_n) = 0. \end{cases}$$

Моделі зростання надійності ПЗ можуть використовуватися при кількісній оцінці надійності на етапі комплексного налагодження ПЗ, у т. ч. в процесі стендових і льотних випробувань.

Основним недоліком таких моделей є те, що при їх застосуванні не враховується спосіб проведення тестування для виявлення помилок у ПЗ, хоча очевидно, що вірогідність кількісних показників надійності ПЗ істотно залежить від здатності програм тестування виявляти помилки в ПЗ, а також від того, наскільки програми тестування враховують операційний профіль тестувального ПЗ.

Оцінка вірогідності програмного забезпечення залежно від способу тестування

Основним методом підвищення надійності бортових систем управління є створення відмовостійкого ПЗ за допомогою використання технології N-варіантного програмування. При цьому вирішальну роль відіграють способи статистичного тестування, що вимагають випадкового вибору тестових впливів з області вхідних даних, обумовленої відповідною специфікацією.

Випадкове тестування, проведене на всіх етапах розробки високоцілісного ПЗ різними тестовими наборами, підвищує рівень довіри до нього, тобто надійність ПЗ істотно залежить від того, яким способом проводилося тестування.

Для того, щоб тестування було ефективним, необхідно знати можливості тестових стратегій по виявленню помилок у ПЗ (у більш загальному випадку – різних типів помилок ПЗ).

Як міру такої можливості пропонується використовувати оцінку детектабільності [4], а як кількісну міру довіри до програми – оцінку трастабільності T як імовірність того, що ПЗ, піддане різним методам тестування, не буде містити дефектів.

Мірою детектабільності P може служити ймовірність виявлення хоча б одного дефекту програми. Так, при статистичному роздільному тестуванні за допомогою n тестових наборів j-го типу

$$P_j = 1 - \left[1 - \sum_{i=1}^{k} \frac{1}{k}\theta_i\right],$$

де k – кількість підобластей, на які розбита специфікована область вхідних даних; θ_i – інтенсивність відмов для підобласті D_i: $\theta_i = r_i / d_i$; r_i – кількість підобластей серед D_i, що призвели до відмови ПЗ; d_i – розмір підобласті.

Така міра P_j, статистично визначена на множині випробувань різних програм, може бути характеристикою ефективності j-ї стратегії тестування і використовуватися при порівнянні різних методів тестування.

Для оцінки трастабільності необхідно знати оцінки ймовірностей P_i того, що досліджуване ПЗ містить дефекти i-го типу. Зокрема, якщо з імовірністю P досліджуване ПЗ містить дефекти одного типу, то при використанні s методів тестування, кожен з яких має детектабільність P_i, оцінка трастабільності може бути визначена за умови невиявлення відмови як

$$T \geq 1 - P\left[\min_{1<i<s}(1-P_i)\right].$$

Очевидно, що чим вище детектабільність методів тестування, тим вище трастабільність.

Висновки

Порівнюючи розглянуті три підходи до оцінки надійності ПЗ бортових систем управління, потрібно вказати на необхідність використання всіх методів на відповідних стадіях розробки.

На початкових етапах доцільне застосування методів, що використовують знання структури програми і її функціональних властивостей, а на завершальних етапах – методів, які базуються на випадковому тестуванні програми такими тестовими наборами, що мають найбільшу детектабільність по виявленню помилок відповідних типів.

Список літератури

1. *Отладка* системы управляющих алгоритмов в ЦВМ реального времени /В.В. Липаев, Л.А. Фидловский, В.В. Филипович, Б.Н. Шнайдер. – М.: Сов.радио, 1974. – 328 с.

2. *Мороз Г.Б.* /Пуассоновские методы роста надежности ПО и их применение: Аналитический обзор// УсиМ. – 1996. – № 1/2. – С. 69–84.

3. *Goel A.L., Okumoto K.* A time–depended error–detection rate model for large scale software system // Proc. Third USA – Japan Computer Conf. – 1978. – P. 35–40.

4. *Мороз Г.Б.* Надежность и трастабильность программных средств высокоцелостных систем // УсиМ. – 1999.– № 2. – С. 59–68.

Стаття надійшла до редакції 27.06.03.

А.А. Зеленков, А.А. Бунчук

Методы оценки надежности программного обеспечения отказоустойчивых систем авионики

Рассмотрена задача оценки надежности программного обеспечения бортовых отказоустойчивых вычислительных систем на различных этапах жизненного цикла. Предложены различные методы оценки надежности, учитывающие "внутренние" характеристики программного модуля, результаты тестового контроля, а также различные вероятностные характеристики процесса выполнения программы.

A.A. Zelenkov, A.A. Bunchuk

Methods of the estimation of reliability of the software of failure-safe systems avioniks

The paper deals with providing software reliability control for up to date on-board fault-tolerable computer-assisted management systems, created on the base of integral modular aircraft electronics technology, during operational period. The authors describe the method of software failures probability evaluation and serial calculating algorithm, based determining the margins of software failures number, according to operational control data.