УДК 681.3.06

А.А. Зеленков

КОНТРОЛЬ НАДЕЖНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ БОРТОВЫХ ОТКАЗОУСТОЙЧИВЫХ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ

Поставлена задача контроля надежности программного обеспечения современных бортовых отказоустойчивых вычислительных систем автоматизированного управления, создаваемых по технологии интегральной модульной авиационной электроники, на этапе эксплуатации. Рассмотрены способ получения оценки вероятности отказа программного обеспечения и последовательное решающее правило на основе определения границ для числа отказов программного обеспечения по данным эксплуатационного контроля.

Прогресс в области микроэлектроники позволил промышленности разработать новые концепции проектирования, которые привели к цифровой авиационной электронике высокой степени интеграции. Функциональные возможности бортовых систем интегрально-модульной авиационной электроники (IMA) реализуются прикладным программным обеспечением (ПО), а сами прикладные программы являются функциональными элементами в блочной архитектуре IMA. Технология IMA позволяет создать бортовую отказоустойчивую вычислительную систему (ОВС), способную решать разнообразные задачи управления самолетом в условиях возникновения потока отказов за счет операций контроля, диагностирования и локализации отказов с автоматическим восстановлением работоспособности. В соответствии с этим в ПО должны быть элементы, обеспечивающие контроль состояния операционной системы, где фиксируются различные ошибки и отказы, и стратегию восстановления.

Отказы, обнаруженные в операционной системе, включают в себя ошибки прикладных программ, нарушения связи с периферийной аппаратурой и отказы, обнаруженные прикладными программами и сообщенными операционной системе (например, ошибки датчиков). Таблица восстановления определяет действия, которые необходимо предпринять на конкретный отказ. Сами действия инициирует монитор состояния путем остановки прикладной программы и запуском альтернативной.

Как известно, ОВС допускает возникновение отказов, но при этом используются эффективные методы устранения их последствий как на аппаратном (автоматическое восстановление работоспособного состояния путем дополнительной динамической реконфигурации с помощью резервных элементов и программ), так и на программном (восстановление информации о состоянии ОВС, необходимой для продолжения работы, путем повторения операции или повторного выполнения программы) уровнях. Наибольшей степени отказоустойчивости можно добиться сочетанием различных средств обнаружения и локализации ошибок на различных иерархических уровнях ОВС [1].

Внедряемая в IMA концепция техники удержания отказа позволяет исправным компонентам ОВС продолжать функционирование в присутствии отказа. При этом необходимо установить зоны удержания неисправности по всей архитектуре. В общем случае ОВС, создаваемые по технологии IMA, должны удерживать отказ k-й кратности (аппаратурный, программный или их сочетание), что позволит внедрить концепцию программированной эксплуатации (планируемые интервалы технического обслуживания только на основной базе). Такой подход требует быстрого обнаружения отказа для критической выполняемой функции и изоляции его до данной зоны удержания отказов. Вся информация об отказах выводится

ражений, можно назначить две величины λ_1 и λ_2 ($\lambda_1 \le \lambda_{тр}, \lambda_2 > \lambda_{тр}$), при которых ошибка первого рода не превысит заданной величины α при $\lambda < \lambda_1$, а вероятность ошибки второго рода при $\lambda > \lambda_2$ не превысит заданной величины β. Такая процедура сводит первоначальную задачу проверки сложной гипотезы к проверке простой гипотезы. Оптимальным является последовательное решающее правило отношения вероятностей, которое минимизирует средний объем контроля при заданных вероятностях ошибочных решений α и β. Если последовательный критерий приводит к принятию гипотезы $H_0^*: \lambda = \lambda_1$, то принимается и исходная гипотеза H_0: $\lambda \le \lambda_{тр}$ $(P \ge P_{тр})$.

Пусть данные эксплуатационного контроля надежности ПО образуют достаточную статистику в виде числа отказов $k_1, k_2, \ldots, k_m$. Такая статистика может быть получена фиксацией отказов по нескольким самолетам за время T (так называемый план (N, Б, Т)) таким образом, что

$$T = \sum_{i=1}^{m} T_i ; \qquad T_i = \sum_{j=1}^{n_i} t_{ji} ,$$

где T – общее время наблюдения; m – количество серий; T_i – суммарное время наблюдения в i-й серии; t_{ji} – время j-го непрерывного полета в i-й серии. Тогда функция правдоподобия по полученной выборке определяется выражением

$$f(k_1, k_2, \ldots, k_m) = \prod_{i=1}^{m} f(k_i) = \prod_{i=1}^{m} \frac{(\lambda T_i)^{k_i}}{k_i!} e^{-\lambda T_i} =$$

$$= \lambda^k \frac{T_1^{k_1} T_2^{k_2} \cdots T_m^{k_m}}{k_1! k_2! \cdots k_m!} e^{-\lambda T} , \qquad k = \sum_{i=1}^{m} k_i ,$$

а логарифм отношения функций правдоподобия для альтернативных значений интенсивностей отказов λ_1 и λ_2

$$\ln \frac{f(k_1, \ldots, k_m | \lambda_2)}{f(k_1, \ldots, k_m | \lambda_1)} = k \ln \frac{\lambda_2}{\lambda_1} - (\lambda_2 - \lambda_1) T .$$

Последовательное правило предписывает сравнение логарифма отношения правдоподобия с порогами, определяемыми вероятностями ошибок α и β соответственно [3],

$$\ln \frac{\beta}{1-\alpha} < \ln(\bullet) < \ln \frac{1-\beta}{\alpha} ;$$

откуда

$$\frac{\ln \frac{\beta}{1-\alpha}}{\ln \lambda_2 / \lambda_1} + \frac{\lambda_2 - \lambda_1}{\ln \lambda_2 / \lambda_1} T < k < \frac{\ln \frac{1-\beta}{\alpha}}{\ln \lambda_2 / \lambda_1} + \frac{\lambda_2 - \lambda_1}{\ln \lambda_2 / \lambda_1} T .$$

Обозначив

$$\frac{\ln\frac{\beta}{1-\alpha}}{\ln\lambda_2/\lambda_1}=k_1,\qquad \frac{\ln\frac{1-\beta}{\alpha}}{\ln\lambda_2/\lambda_1}=k_2,\qquad \frac{\lambda_2-\lambda_1}{\ln\lambda_2/\lambda_1}=k_0,$$

определяем выражения для границ числа отказов k:

$$A=k_1+k_0T;$$

$$B=k_2+k_0T,$$

и последовательное решающее правило

$$a(k)=\begin{cases}a_1, & k<A;\\ a_2, & k>B;\\ a_3, & A\le k\le B.\end{cases}$$

Очевидно, что в случае $A\le k\le B$ решение a_3 означает продолжение эксплуатационного контроля, так как при заданных рисках α и β никакого вывода об изменении показателя надежности сделать нельзя вследствие малого объема информации. Среднее значение числа отказов $M[k]$, необходимое для принятия решения a_1 или a_2, зависит от значений α и β:

$$M[k\setminus\lambda_1]=\frac{(1-\alpha)\ln\frac{1-\alpha}{\beta}+\alpha\ln\frac{\alpha}{1-\beta}}{\frac{\lambda_2}{\lambda_1}-1-\ln\frac{\lambda_2}{\lambda_1}};$$

$$M[k\setminus\lambda_2]=\frac{\beta\ln\frac{\beta}{1-\alpha}+(1-\beta)\ln\frac{1-\beta}{\alpha}}{\frac{\lambda_2}{\lambda_1}-1+\ln\frac{\lambda_2}{\lambda_1}}.$$

Определим среднее время $M[t_k]$ до появления k-го отказа. Поскольку закон распределения момента времени t_k имеет вид:

$$P\{t_k<t\}=\sum_{s=k}^{\infty}\frac{[\Lambda(t)]^s}{s!}e^{-\Lambda(t)},$$

то

$$M[t_k]=\int_0^{\infty}P\{t_k>t\}dt=\sum_{s=0}^{k-1}\int_0^{\infty}\frac{[\Lambda(t)]^s}{s!}e^{-\Lambda(t)}dt,$$

где $\Lambda(t)$ – среднее число отказов к моменту времени t. В частном случае постоянства интенсивности отказов $\Lambda(t)=\lambda t$

$$M[t_k]=\sum_{s=0}^{k-1}\int_0^{\infty}\frac{[\Lambda(t)]^s}{s!}e^{-\Lambda(t)}dt=\sum_{s=0}^{k-1}\frac{\lambda^s}{s!}\Gamma(s+1)\lambda^{-(s+1)}=k\lambda^{-1},$$

а дисперсия момента времени t_k определяется соотношением

$$D[t_k] = \int_0^\infty t P_k(t)dt - [M[t_k]]^2 = \sum_{s=0}^{k-1} \frac{2\lambda^s}{s!} \frac{\Gamma(s+2)}{\lambda^{s+2}} - \left(\frac{k}{\lambda}\right)^2 =$$

$$= \sum_{s=0}^{k-1} \frac{2(s+1)}{\lambda^2} - \left(\frac{k}{\lambda}\right)^2 = \frac{k(k+1)}{\lambda^2} - \frac{k^2}{\lambda^2} = \frac{k}{\lambda^2}.$$

Если интенсивность отказов не является постоянной, а изменяется, например, по экспоненциальному закону, то значение $M[t_k]$ можно найти последовательным вычислением $M[t_i]$, представляя зависимость $\Lambda(t)$ кусочно-постоянной на рассматриваемых интервалах времени.

Отметим, что на этапе летных испытаний ПО ОВС, когда выборка измерений сравнительно мала, можно использовать последовательный критерий для проверки гипотезы о вероятности безотказной работы, используя алгоритм [4]:

$$\frac{\ln\frac{\beta}{1-\alpha}}{\ln\frac{1-P_1}{1-P_0} - \ln\frac{P_1}{P_0}} + m\frac{\ln\frac{P_0}{P_1}}{\ln\frac{1-P_1}{1-P_0} - \ln\frac{P_1}{P_0}} < r < \frac{\ln\frac{1-\beta}{\alpha}}{\ln\frac{1-P_1}{1-P_0} - \ln\frac{P_1}{P_0}} + m\frac{\ln\frac{P_0}{P_1}}{\ln\frac{1-P_1}{1-P_0} - \ln\frac{P_1}{P_0}},$$

где $P_1 < P_{тр} < P_0$; m – количество испытаний; r – число отказов в испытаниях.

Количественная оценка показателей надежности ПО обоих типов на всех стадиях жизненного цикла позволяет внести в разработанные и разрабатываемые программные продукты необходимые изменения с целью управления уровнем надежности, а значит и уровнем безопасности полетов.

Список литературы

1. *Каган Б.М.* Электронные вычислительные машины и системы. – М. : Энергия, 1979. – 528 с.

2. *Штрик А.А., Осовецкий Л.Г., Мессих И.Г.* Структурное проектирование надежных программ встроенных ЭВМ. – Л. : Машиностроение, 1989. – 296 с.

3. *Вальд А.* Последовательный анализ. - М.: Физматгиз, 1960.- 328 с.

4. *Синицын Б.С., Белогородский С.Л., Зеленков А.А., Мирошниченко О.Г.* Применение методов математической статистики при анализе точности бортовых систем автоматизированного управления // Измерения, контроль, автоматизация (ИКА). – 1981. № 3(37). С. 43–52.

Стаття надійшла до редакції 20 грудня 1999 року.