

ПРОБЛЕМА ОЦЕНКИ НАДЕЖНОСТИ ПРОГРАММНЫХ КОМПЛЕКСОВ

Н.В. Аболмазова, А.Н. Коварцев

Самарский государственный аэрокосмический университет им. С.П. Королёва

Развернута проблематика оценивания надежности программных комплексов, а также выделены отличия от решения аналогичной задачи для технических устройств. Задано направление для дальнейшего решения поставленной задачи. Определено влияние вероятностных мер на изменение в оценке надежности модулей для одномерного случая.

Введение

Надежность является важным и естественным требованием, предъявляемым к качеству современных аппаратно-программных комплексов (АПК). В области обеспечения надежности технических устройств (ТУ) достигнут высокий уровень. Например, в работе [1] показано, что вероятность отказов вычислителей пилотажно-навигационного комплекса самолетов типа Ту-324 составляет 10^{-10} , что соответствует современным требованиям к аппаратуре космических аппаратов и авиации. В области оценки надежности программного обеспечения (ПО) для АПК положение дел обстоит не столь хорошо.

Известно, что качество программного продукта (ПП) характеризуется набором свойств, определяющих, насколько продукт «хорош» с точки зрения заинтересованных сторон. Каждый из участников его создания может иметь свое представление о свойствах, а также о том, как оценить продукт. Модель качества в рамках стандарта ISO 9126 состоит из 6 факторов, где одним из важнейших является надежность программного продукта.

1. Определение надежности ПП

Наиболее весомой причиной отсутствия методов оценки надежности ПП является неразработанность соответствующей теоретической базы, приемлемой для исследования именно надежности ПП. Попытаемся разобраться в этом вопросе.

Первоначально определим, что такое *надежность* ПП. В работе [2] *надежность* определяется как *вероятность работы ПО без отказов в течение определенного периода времени, рассчитанная с учетом стоимости (степени воздействия) для пользователя каждого отказа*.

Из определения следует, что в понятии надежности применительно к ПП мы должны упоминать, какие типы ошибок имеются в виду. Понятие «надежность элементов ТУ» обычно не связывают с типами отказов. В данном определении надежности ПП есть заимствование из терминологии надежности ТУ – фактор времени.

В ПП ошибки возникают при определенных сочетаниях исходных данных. Бесчисленные запуски программы при ограниченном количестве наборов исходных данных, где она работоспособна, в течение любого интервала времени не породят ни одного отказа. Надежность программных модулей (ПМ) со временем может даже увеличиваться за счет устранения выявляемых ошибок. Поэтому теоретически может возникнуть ситуация, когда при тестировании ошибки уже не будут обнаруживаться.

Такое положение вещей делает совершенно бессмысленным для программирования понятия наработки на отказ или вероятности отказа за определенное время, на которых построена вся теория надежности в технике.

Аксиоматически классическая теория надежности строится на предположении о том, что существует пусть маленькая, но не нулевая вероятность отказа p_0 любого ТУ. Программы не изнашиваются и не ломаются, следовательно, ненадежность ПП – следствие исключительно ошибок проектирования, внесенных в процессе разработки. В то же время можно разработать любое количество простых программ, для которых вероятность отказа равна нулю. Но в этом случае весь аппарат классической теории надежности становится непригодным для практического использования.

Наиболее общее определение *надежности* ПП предлагает Б. Мейер [3], он определяет надежность как *способность программы давать разумные результаты во всех возможных окружениях, и в частности в аномальных условиях*.

В этом случае ненадежность ПП можно трактовать как соотношение мощности множества ошибочных ситуаций $|\Omega_E|$ и мощности множества исходных данных $|\Omega_{In}|$ ($\Omega_E \subset \Omega_{In}$). Применительно к ЭВМ это отношение между количеством сочетаний исходных данных программы, когда возникает ошибочная ситуация, к общему числу сочетаний. В этом случае ненадежность можно вычислить по формуле $q = |\Omega_E| / |\Omega_{In}|$.

Однако количество сочетаний исходных данных ПМ (в общем случае) настолько велико, что перебрать все для современной ЭВМ практически невозможно. Т.о., проблему оценки надежности ПП можно сформулировать как комбинаторную проблему поиска алгоритмов частичного перебора пространства исходных данных модуля. Для сравнительно простых ПМ, имеющих несколько входных параметров, получены положительные результаты. Для некоторых модулей удастся доказать корректность [3], т.е. $q = 0$. В других случаях q можно определить экспериментально [4, 5].

Вместо дискретной меры – мощности – введем непрерывную меру, оценивающую объем многомерного тела, тогда ненадежность модуля можно оценить по формуле

$$q = V(\Omega_E) / V(\Omega_{In}) . \quad (1)$$

Для современных сложных ПП число исходных данных измеряется тысячами переменных, поэтому прямые методы тестирования становятся практически нереализуемыми. Кажется естественным оценивать надежность сложных ПП, используя известные характеристики составляющих его компонент так же, как это делается для ТУ. Однако и здесь обнаруживаются неожиданности:

- 1) как бы ни была сложна структура ПП, она всегда имеет (в смысле надежности) последовательную схему соединения элементов (программных модулей ПП);
- 2) надежность ПП зависит не только от надежности составляющих его программных модулей, но и корректности организации функционирования ПП [6];
- 3) надежность ПП не может быть вычислена непосредственно, исходя из надежностей составляющих его элементов (программных модулей).

2. Постановка задачи

Предположим, что нам известны характеристики надежности всех ПМ, из которых составлен ПП. Пусть q_i – ненадежность i -го модуля $A_i : X_i^{In} \rightarrow Y_i^{Out}$, вычисленная с учетом всевозможных применений модуля, т.е. на достаточно широкой области значений исходных данных $\Omega_{In}^i : X_i^{In} = (x_{1i}^{In}, x_{2i}^{In}, \dots, x_{n_i}^{In}) \in \Omega_{In}^i$. Как же с помощью известной надежности модуля получить значение надежности всей программы?

Допустим, что логические ошибки в организации логики функционирования ПП отсутствуют (данная проблема требует отдельного рассмотрения, см. [4]).

Пусть некоторый ПП имеет L маршрутов исполнения [6]. Каждый из маршрутов обозначим $M_j = i_{j_0} i_{j_1} \dots i_{j_k}$, где i_{j_k} – номер ПМ для ПП. Пусть каждый i -й объект на j -м маршруте вызывается в среднем $\tilde{m}_{ij}$ раз. Ненадежность i -го модуля на j -м маршруте за $\tilde{m}_{ij}$ вызовов можно оценить величиной $Q(\tilde{m}_{ij}) = 1 - (1 - q_i)^{\tilde{m}_{ij}} = Q_{ij}$.

Очевидно, что если в любом из модулей маршрута возникнет ошибка, то маршрут считаем ошибочным. Тогда ненадежность маршрута: $Q_{M_j} = 1 - \prod_{i=1}^{j_k} (1 - Q_{ij})$.

Пусть каждый из маршрутов реализуется с вероятностью r_j , причем справедливо $\sum r_j = 1$. Тогда ненадежность ПП можно оценить величиной

$$Q_n = \sum_{j=1}^L r_j Q_{M_j} \quad (2)$$

Формула (2) справедлива, если оценки ненадежности ПМ неизменны при различных использованиях модулей, но это не так.

3. Пример программы

Рассмотрим программу термогазодинамического расчета двухвального ТРД.

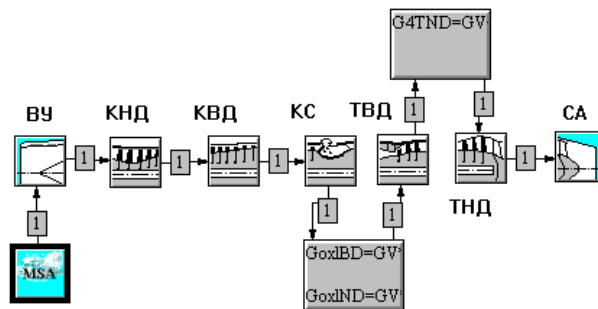


Рис. 1. Программа термогазодинамического расчета двухвального ТРД

Представленная программа достаточно проста и имеет единственный маршрут. Однако при ее выполнении изменяются области изменения исходных данных комплекствующих ее модулей. На рис. 2-7 показаны области изменения исходных данных ПП расчета ТРД и его узлов (турбины высокого и низкого давления и др.).

Как видно из рисунков, изменилась топология областей исходных данных модулей, особенно для турбины НД и соплового аппарата, а для компрессора ВД область исходных данных выродилась в кривую. Первоначально при тестировании области исходных данных имели прямоугольный вид. Кроме того, уменьшились размеры областей исходных данных. Все это способно увеличить характеристику ненадежности ПМ за счет уменьшения знаменателя формулы $q_i = V(\Omega_E^i) / V(\Omega_{in}^i)$.

Но еще большую проблему представляет изменение законов распределения (ЗР) исходных данных модулей за счет соответствующих функциональных преобразований первоначально равномерного распределения исходных данных ПП. На рис. 8 показаны гистограммы распределения входных параметров РЗНД, ТЗНД (входные для соплового аппарата) и РЗВД (входного для модуля расчета турбины НД).

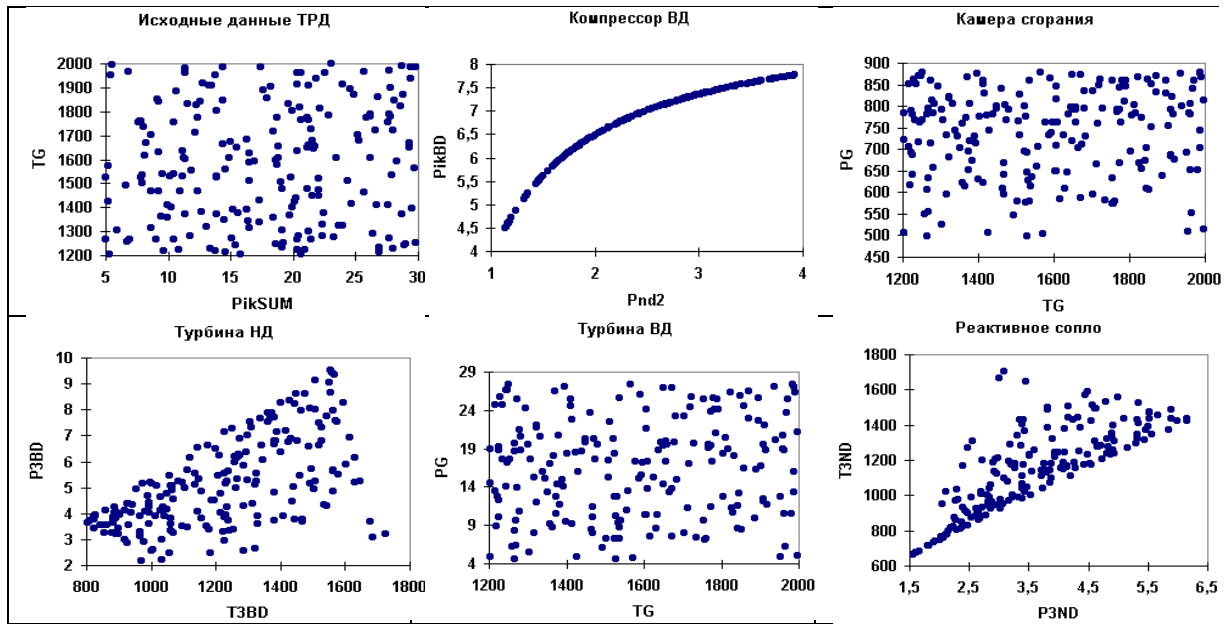


Рис. 2-7. Области изменения исходных данных ПП расчета ТРД и его узлов

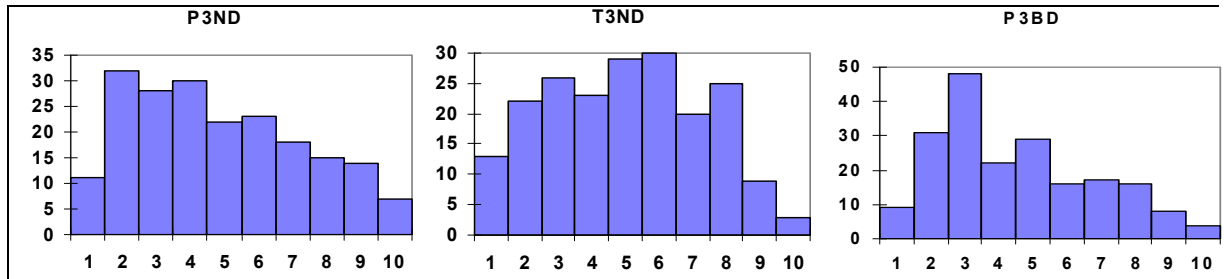


Рис. 8. Гистограммы распределения входных параметров P3ND, T3ND и P3BD

4. Влияние вероятностных мер на изменение в оценке надежности ПМ

Пусть некоторый модуль, имеющий единственных входной параметр x , «прошел» серию испытаний (из N испытаний), в которых не было обнаружено ни одной ошибки, причем $x \in [a, b]$. из чего можно сделать вывод, что $q \leq 1/(N+1)$ и $V(\Omega_E) \approx (b-a)/(N+1)$. Пусть теперь при использовании модуля в ПП изменился диапазон значений входного параметра модуля $x \in [c, d] \subset [a, b]$ без изменения его ЗР. Итоговую ненадежность модуля, с учетом вероятности $P\{\Omega_E \in [c, d]\}$ можно оценить следующим образом: $\tilde{q} = \frac{V(\Omega_E)}{d-c} P\{\Omega_E \in [c, d]\} = \frac{V(\Omega_E)}{d-c} \cdot \frac{d-c}{b-a} = \frac{V(\Omega_E)}{b-a} = q$, т.е. для равномерного ЗР параметра x характеристика ненадежности модуля не изменяет своего значения.

Для простоты положим $a=c=0$. Пусть теперь на отрезке $[0, d]$ параметр x имеет квазиэкспоненциальное распределение с функцией плотности распределения $f(x) = K\lambda e^{-\lambda x}$, где $K = \frac{1}{1-e^{-\lambda d}}$. Положим $V(\Omega_E) = \Delta$. Ненадежность модуля можно опре-

$$\text{делить из выражения } \tilde{q}(x) = P\{\Delta \in [0, d]\} \int_x^{x+\Delta} K\lambda e^{-\lambda x} dx = \frac{d}{b} \frac{e^{-\lambda x}}{1-e^{-\lambda d}} (1-e^{-\lambda \Delta}).$$

Ненадежность модуля теперь зависит от того, куда попадет область ошибочных ситуаций, и не равна полученной в результате автономного тестирования величине q .

В предположении равновероятности попадания области ошибочных ситуаций в любое место отрезка $[0, d]$ вычислим среднюю величину $\tilde{q}(x)$

$$q_{cp} = \int_0^d \tilde{q}(x) \frac{1}{d} dx = \frac{P\{\Delta \in [0, d]\} K(1 - e^{-\lambda \Delta})}{\lambda d} \int_0^d \lambda e^{-\lambda x} dx = \frac{d}{b} \frac{(1 - e^{-\lambda \Delta}) K}{\lambda d} (1 - e^{-\lambda d}) = \frac{(1 - e^{-\lambda \Delta})}{\lambda b}.$$

Введенная характеристика не зависит от параметра x и определяется только размерами области ошибок (Δ) и параметром экспоненциального ЗР (λ). Как показывают расчеты (см. таблицу 1) существенные изменения значений λ (степени неравномерности распределения) практически не сказываются на величине q_{cp} . Более того, $q_{cp} \approx q$.

Таблица 1. Зависимость q_{cp} от λ

λ	q_{cp}	$\max q(x)$	Δx
0,1	9,99999E-06	1,01E-05	0,1
1	9,99995E-06	1,1E-05	0,0975
10	9,9995E-06	2,31E-05	0,0825
100	9,995E-06	0,0002	0,0275
1000	9,95017E-06	0,00199	0,005

В данном примере, $q = 0.00001$, $d = 0.2$, $b = 1$. Для больших неравномерностей $\lambda > 10$ условие $q(x) > q_{cp}$ наблюдается на сравнительно небольших участках области определения входного параметра $x - \Delta x$, а в остальных случаях отмечается $q(x) \leq q_{cp}$.

При небольших значениях λ справедливо $\max q(x) \approx q_{cp}$. Если $q_{cp} \approx q$ справедливо для любых ЗР, то оценки q_i можно использовать для вычисления надежности ПП, интерпретируя Q_n как среднюю ожидаемую величину ненадежности ПП. Однако данный результат необходимо еще обобщить на многомерный случай.

Выводы

Структура ПП всегда имеет последовательную схему соединения программных модулей ПП в смысле надежности. Надежность ПП зависит от корректности организации функционирования системы и не может быть вычислена непосредственно, исходя из надежностей программных модулей.

Т.о., оценивание надежности ПП существенно отличается от решения аналогичной задачи для ТУ и требует разработки соответствующей теоретической базы.

Литература

1. Авакян А.А., Искандаров Р.Д., Новиков Н.Н. и др. Концепция построения высоконадежных вычислителей для авиационной и ракетной техники // Надежность и качество – 2001: Сб. докладов межд. симпоз. Пенза, 2001. С. 33-37.
2. Майерс Г. Надежность программного обеспечения. – М.: Мир, 1980. – 360 с.
3. Мейер Б., Бодуэн К. Методы программирования: В 2-х томах. Т.2. – М.: Мир, 1982.
4. Коварцев А.Н. Автоматизация разработки и тестирования программных средств. – Самар. гос. аэрокосм. ун-т. Самара, 1999. – 150 с.
5. Коварцев А.Н. Автоматизация тестирования вычислительных модулей // Надежность и качество – 2001: Сб. докладов межд. симпоз. Пенза, 2001. С. 285-288.
6. Липаев В.В. Надежность программных средств. – М.: СИНТЕГ, 1998. – 232 с.