

ОЦЕНКА НАДЕЖНОСТИ ВОССТАНАВЛИВАЕМЫХ ЦИФРОВЫХ СИСТЕМ НА ОСНОВЕ МНОГОФРАГМЕНТНЫХ МАРКОВСКИХ МОДЕЛЕЙ

Е.Б. Одарущенко
(представил д.т.н., проф. В.С. Харченко)

Излагается подход, позволяющий проводить оценку надежности восстанавливаемых цифровых управляющих и вычислительных систем технических комплексов с учетом «веса» программных дефектов.

Среди сложных технических комплексов, отказ которых может привести к катастрофическим последствиям, в первую очередь можно назвать комплексы военного назначения, во вторую очередь к ним можно отнести АЭС, транспортные коммуникации, правительственные и банковские информационные системы. Подчеркивая важность решаемых ими задач и возможность катастрофических последствий их отказов, такие объекты называют техническими комплексами критического использования (ТККИ) [1].

Следует отметить, что надежность ТККИ в значительной степени зависит от надежности их системы управления (СУ), ядром которой являются специализированные цифровые управляющие вычислительные системы (ЦУВС). По оценкам специалистов стоимость ЦУВС составляет до 40 % общей стоимости комплексов. Выполнение растущих требований к надежности ЦУВС возможно только на основе тщательного анализа их функций, архитектуры, используемой элементной базы, условий применения по назначению и связанных с ними источников отказов.

Известно, что нарушение работоспособности ЦУВС может быть вызвано двумя основными причинами: кратковременными сбоями или устойчивыми отказами элементов аппаратных средств, обусловленных их физическими дефектами (ДФ АС), а также дефектами проектирования и производства программных средств (ДП ПС), которые оказались не обнаруженными в процессе отладки и испытаний и проявились при использовании систем по назначению. Анализ опыта разработки, испытаний и эксплуатации ЦУВС последних поколений показывает, что ДП ПС становятся весомым фактором ненадежности, который имеет тенденцию устойчивого нарастания. По оценкам специалистов ДП ПС обуславливают 20 - 70% случаев нарушения функционирования сложных ЦУВС [2].

Известно, что при обработке исходных данных создается огромное

число различных маршрутов исполнения для программ. Большое число вариантов исполнения программ не может быть проверено полностью из-за ограничений на длительность отладки. Опыт отладки и эксплуатации ТККИ показывает, что даже после нескольких лет эксплуатации встречаются непроверенные сочетания исходных данных, при которых работающая программа дает неверные результаты [3]. Ранее было предложено для систем с различными режимами функционирования процесс тестирования на этапе применения осуществлять с изменяемыми исходными данными. Это позволяет в идеальном случае перекрыть всю область возможных исходных данных и, таким образом, выявить дефекты, оставшиеся в ПС. С целью решения поставленной задачи разработаны марковские модели, которые позволяют учесть характеристики обоих компонент, изменение надежности программной компоненты во времени и то, что граф состояний системы будет содержать большое число однотипных фрагментов, отличающихся только значением интенсивности проявления ДП ПС.

В основу разработки этих моделей положен принцип многофрагментности, который заключается в представлении марковских моделей оценки надежности в виде композиции регулярных (повторяющихся) марковских фрагментов, отличающихся одним из параметров и описываемых системой дифференциальных уравнений Колмогорова. Однако, введенное допущение о том, что интенсивность восстановления после проявлений ДП ПС есть величина постоянная, не всегда является оправданным. Это обуславливается вероятностным характером внесения ДП ПС при разработке ПС и соответственно их различным «весом». Соответственно, о «весе» того или иного ДП можно судить по времени, которое требуется на его устранение. В силу сказанного предлагается оценку надежности ЦУВС осуществлять с учетом изменяющегося «веса» ДП ПС. В качестве параметра, учитывающего эту особенность, предлагается использовать интенсивность восстановления после проявления ДП ПС ($\mu_{ВП}$). На рис. 1 представлена структурная схема дублированной одноверсионной системы. Регулярная многофрагментная марковская модель, которая представляет собой размеченный граф с пятью параметрами и ($n-1$) состояниями представлена на рис. 1. В качестве параметров модели используются следующие величины: $\lambda_{ДФ}$ – интенсивность проявления дефектов АС; $\mu_{ДФ}$ – интенсивность восстановления после проявления ДФ АС; $\lambda_{ДП}$ – интенсивность проявления ДП ПС; $\mu_{ВП}$ – интенсивность восстановления после проявления ДП ПС; $\Delta\lambda_{ДП}$ – величина изменения $\lambda_{ДП}$ после устранения ДП ПС.

Логика функционирования системы заключается в следующем. В начальный момент система реализует все предписанные функции и находится в состоянии S_1 . В случайный момент возникает отказ ДП ПС или ДФ АС. При возникновении отказа по ДФ система переходит в состояние S_2 с интенсивностью $2\lambda_{ДФ}$. При проявлении ДП ПС система пе-

переходит в состояние S_3 . Из него система с интенсивностью $\mu_{ВП}$ переходит в состояние S_4 , принадлежащее второму фрагменту. Аналогично система функционирует в следующих фрагментах. Особенность заключается в том, что в последующих фрагментах параметр $\mu_{ВП}$ имеет различные значения в силу различного «веса» проявляющихся ДП ПС.

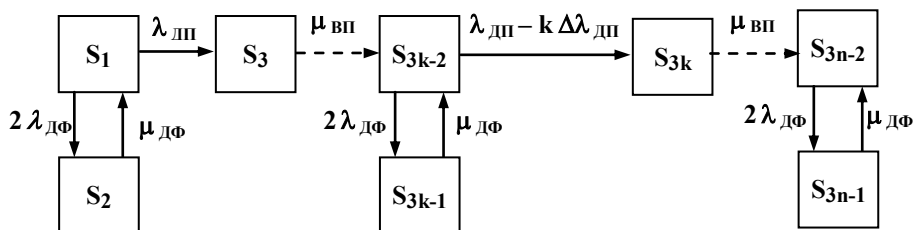


Рис. 1. Пример регулярной многофрагментной марковской модели

В качестве показателя надежности была выбрана функция готовности $P_T(t)$, вычисляемая как сумма вероятностей нахождения системы в работоспособных состояниях в каждый рассматриваемый момент времени.

Анализ результатов исследований показывает, что динамика роста функции готовности при изменяющейся интенсивности восстановления после проявления ДП ПС ниже, чем при фиксированном параметре. Это может служить подтверждением предложения о том, что учет изменяющегося параметра $\mu_{ВП}$ позволяет более адекватно оценивать надежность ЦУВС на этапе ее разработки. Кроме того, анализ значений функции готовности позволяет уточнить время проведения отладки и испытания систем.

Очевидно, что в этих условиях актуальным становится решение задачи оценки параметра $\mu_{ВП}$ и его распределения по фрагментам модели. Решение этой задачи целесообразно проводить на основе сбора статистики по проявляющимся ДП ПС сходных проектов разработки систем рассматриваемого класса.

ЛИТЕРАТУРА

1. Харченко В.С. Использование функций готовности для оценки устойчивости многоальтернативных систем к сбоям и относительным дефектам проектирования // Вопросы технической диагностики. – Ростов: РИСИ. – 1991. – С. 51 - 56.
2. Харченко В.С. Теоретические основы дефектоустойчивых цифровых систем с версионной избыточностью. – МОУ, 1996. – 506 с.
3. Пальчун Б.П., Юсупов Р.М. Оценка надежности программного обеспечения. – С-Пб.: Наука, 1994. – 84 с.

Поступила в редколлегию 19.9.2000
