УДК 004.415.533

Т.В. ГОДУНОВА, И.Б. ТУРКИН

Национальный аэрокосмический университет им. Н.Е. Жуковского "ХАИ", Украина

ОЦЕНКА ЭФФЕКТИВНОСТИ ДИВЕРСИФИКАЦИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В АППАРАТНО-ПРОГРАММНЫХ КОМПЛЕКСАХ КРИТИЧЕСКОГО НАЗНАЧЕНИЯ

В статье рассмотрены проблемы обеспечения безопасности функционирования организационно-технических систем путем повышения их отказоустойчивости. Проведен анализ некоторых моделей надежности программно-аппаратных комплексов, а также выполнена расчетная оценка надежности избыточных аппаратно-программных систем. Рассмотрена возможность повышения надежности аппаратно-программных комплексов на основе построения самодиагностирующегося ПО.

функциональная безопасность, критические системы, надежность аппаратно-программных комплексов

Введение

Надежность сложных технических систем и комплексов, безопасность целых регионов в настоящее время все в большей степени зависит от программного обеспечения. Чтобы подчеркнуть важность проблемы, достаточно упомянуть наиболее громкие катастрофы, произошедшие из-за сбоя программного обеспечения, например, гибель ракеты Ariane 5 [1], катастрофы, произошедшие с американскими самолётами "Osprey MV-22" [2] и российским космическим кораблём "Союз ТМА" [3].

Сейчас гонка за гигагерцами тактовой частоты процессора сменилась соревнованием за количеством ядер, повторяя уже традиционную формулу знаменитого закона Гордона Мура, открытого в 1965 г. Согласно закону новые модели микросхем разрабатываются примерно через 18–24 месяцев после появления своих предшественников, а их емкость (число транзисторов) при этом каждый раз возрастает примерно вдвое.

Существование многоядерных процессоров позволяет повысить не только производительность, но и уровень надежности до значений, недоступных или труднореализуемых в одноядерном процессоре. При этом, если для роста производительности необходимы специальные алгоритмы и методы, обеспечивающие физическую параллельность исполнения программ, то повышения надежности достичь проще. Причина этого заключается в том, что повышение надежности программной системы, состоящей из недостаточно надежных компонентов, достигается за счет избыточности, то есть применения резервных каналов обработки информации, разнообразных программных конструкций контроля, диагностики и самодиагностики. Параллельная работа основных и избыточных элементов программной системы на отдельных ядрах процессора позволяет гарантировать контролируемость процессов информационного взаимодействия между ними.

Отказоустойчивость – это способность вычислительной системы продолжать действия, заданные программой, после возникновения неисправностей [4]. Сегодня, как известно, введение отказоустойчивости требует избыточного аппаратного и программного обеспечения. Направления исследований, связанные с созданием методов предотвращения и парирования неисправностей, – основные для обеспечения надежности. Концепции

параллельности и отказоустойчивости любых вычислительных систем естественным образом связаны между собой, поскольку в обоих случаях требуются дополнительные функциональные компоненты. Многоядерные архитектуры процессоров, располагающие свойством естественной параллельности, обладают избыточными ресурсами, которые могут гибко использоваться как для повышения производительности, так и для повышения надежности.

1. Постановка задачи

Как известно, для обеспечения защиты вычислительного процесса программными методами используется программная, информационная и временная избыточности [4].

Под временной избыточностью понимается использование части производительности для получения диагностической информации о состоянии системы. Программная избыточность используется для контроля и обеспечения достоверности важных решений по управлению и обработке информации Она заключается в применении нескольких вариантов программ в каждом узле системы (так называемое диверсифицированное программирование).

Сопоставление результатов независимых решений одного и того же фрагмента задачи называют элементарной проверкой, а совокупность всех проверок образует систему голосования, которое является основным источником диагностической информации о состоянии аппаратной части системы и вычислительного процесса в каждом активном узле системы. При обеспечении отказоустойчивости широко используются два механизма – протоколы голосования и протоколы принятия коллективного решения.

Таким образом, зависимость критических систем от программных средств порождает необходимость придания применяемым в них программным средствам заданных свойств безопасности и способности противостоять разрушению, нарушениям функционирования системы, сбоям, преднамеренным воздействиям злоумышленников и ошибкам различных видов при выполнении критической системой основной целевой функции. Один из наиболее важных способов достижения требуемых свойств – это построение самодиагностируемых многоверсионных программных систем. Оценка эффективности диверсификации ПО в аппаратно-программных комплексах критического назначения является основной идеей исследования.

2. Модели надежности аппаратно-программных комплексов

Сбои и отказы по месту возникновения в элементах системы классифицируем на аппаратные и программные.

1. Сбои и отказы аппаратного обеспечения носят случайный характер из-за действия механизмов деградации [5].

2. Ошибки программного обеспечения возможны двух типов:

- случайные – это ошибки, которые проявляются в виде сбоев при выполнении операций на конкретных наборах данных; эти наборы в системах реального времени в силу специфики систем данного класса могут быть уникальными и неповторяющимися в параллельно работающих каналах;

- систематические – это ошибки ПО, регулярно повторяющиеся по одной и той же причине, при этом их возникновение не зависит от последовательности и очередности поступления входной информации [5], то есть их выявление возможно только в многоверсионных программных системах.

Как известно, надежность систем можно характеризовать показателем вероятности безотказ-

ной работы (ВБР) — вероятности того, что в заданных условиях работы в течение определенного промежутка времени не произойдет ни одного отказа [4].

Будем полагать, что требуемая надежность всего аппаратно-программного комплекса достигается за счет троирования каналов, обрабатывающих информацию [6]. В таких системах обнаружение дефектного канала обеспечивается выбором по принципу «два совпавших результата из трех» (рис. 1).

Считая компаратор, как достаточно простое устройство абсолютно надежным, рассмотрим три варианта реализации программного обеспечения в канале, их структурные схемы надежности (ССН) и итоговые расчетные формулы для определения вероятности безотказной работы всей системы.

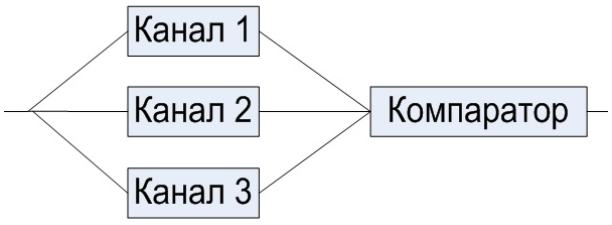


Рис. 1. Структурная схема исследуемой системы

В формулах, приводимых далее, используются обозначения:

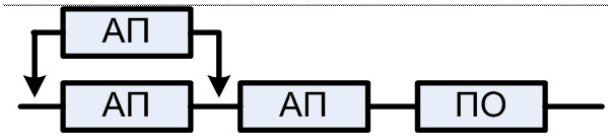
$P_{сл}$ – ВБР системы в предположении случайного типа ошибок ПО;

$P_{сист}$ – ВБР системы в предположении систематического типа ошибок ПО;

P_{hw} – ВБР аппаратной части одного канала;

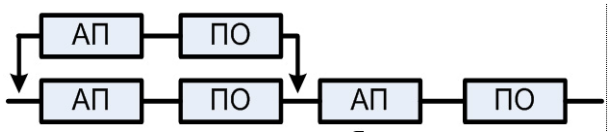
P_{sw} – ВБР версии ПО.

1. При идентичных версиях программного обеспечения в каналах ССН и ВБР системы будут зависеть от типа ошибки ПО: случайной или систематической (рис. 2).



$$P_{сист}=P_{sw}\left(P_{hw}^3+3\left(1-P_{hw}\right)P_{hw}^2\right)$$

а



$$P_{сл}=P_{hw}^3P_{sw}^3+3\left(1-P_{hw}P_{sw}\right)P_{hw}^2P_{sw}^2$$

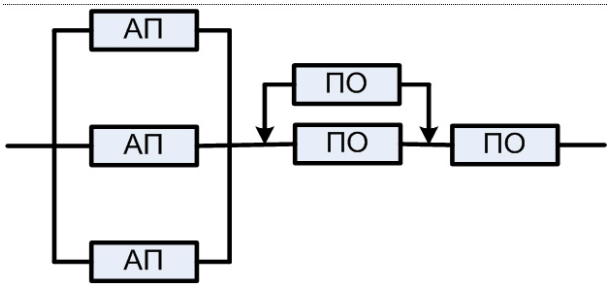
б

Рис. 2. ССН и ВБР аппаратно-программного комплекса, использующего одну версию ПО, при различных типах ошибки ПО: а – случайный отказ; б – систематический отказ

2. Если в каждом канале используется своя, уникальная версия ПО, то ССН такой системы совпадает с приведенной выше (см. рис. 2б), а ВБР системы не зависит от рассматриваемого типа ошибки ПО:

$$P=P_{сист}=P_{сл}=P_{hw}^3P_{sw}^3+3\left(1-P_{hw}P_{sw}\right)P_{hw}^2P_{sw}^2$$

3. Рассмотрим вариант, когда используются те же три версии ПО, но исполняемые параллельно в каждом канале на многоядерной процессорной платформе. Тогда, применяя тот же принцип «два совпавших результата из трех», можно обеспечить автономное самодиагностирование каждого канала. Если каждый из каналов имеет возможность проводить собственную диагностику, то система сохраняет работоспособность при исправности аппаратной части любого канала и совпадении результатов двух версий ПО из трех доступных (рис. 3). Такая модель работоспособна при возникновении как случайных, так и систематических ошибок программного обеспечения.



$$P = P_{сист} = P_{сл} = \left(1-\left(1-P_{hw}\right)^3\right)\left(P_{sw}^3 + 3\left(1-P_{sw}\right)P_{sw}^2\right)$$

Рис. 3. ССН и ВБР аппаратно-программного комплекса, использующего мновесионное ПО и самодиагностируемые каналы

3. Расчетная оценка надежности избыточных аппаратно-программных систем

По данным различных источников вероятность безотказной работы критической системы за срок эксплуатации оценивается величиной 0,995…0,999 [7], с наработкой на отказ 1…0.1 год$^{-1}$ [7].

Надежность програмного обеспечения, как известно, зависит не от старения, или деградации характеристик, а от количества неустраненных, остаточных ошибок. Поэтому для оценки надежности програмного обеспечения используем критерии, которые служат основой для принятия решения о прекращении тестирования критического ПО, а именно – одна выявленная ошибка на группу тестировщиков из 3÷4-х человек в квартал.

Таким образом, надежность програмного обеспечения и надежность аппаратной части являются соизмеримыми.

Результат вычислений, представленный в терминах вероятности отказа, с одной стороны, будет нагляднее для последующего анализа, а с другой – менее подвержен воздействию вычислительных ошибок, резко возрастающих при вычитании близких по величине чисел (табл. 1).

Количественные оценки показателей надежности рассмотренных выше вариантов архитектур системы получены для следующих диапазонов показателей ВБР аппаратной платформы канала и версии программного обеспечения:

– абсолютно надежная аппаратная часть, то есть ВБР аппаратных средств равна единице (рис.4);

– фиксированная ВБР аппаратной платформы канала P_{hw}=0,99 (рис. 5);

– ВБР аппаратной платформы канала равна ВБР версии ПО: $P_{hw} = P_{sw}$ (рис. 6).

Таблица 1

Расчетные формулы для определения показателей надежности систем

Номер рисунка	Вероятность безотказной работы, **P** Вероятность отказа, **Q**
2а	$P_{сист} = P_{sw}\left(P_{hw}^3 + 3\left(1-P_{hw}\right)P_{hw}^2\right)$ $Q_{сист} = Q_{sw} + Q_к - Q_{sw}Q_к,$ где $Q_к = Q_{hw}^3 + 3\left(1-Q_{hw}\right)Q_{hw}^2.$
2б	$P_{сл} = P_{hw}^3 P_{sw}^3 + 3\left(1-P_{hw}P_{sw}\right)P_{hw}^2 P_{sw}^2$ $Q_{сл} = Q_к^3 + 3\left(1-Q_к\right)Q_к^2,$ где $Q_к = Q_{sw} + Q_{hw} - Q_{sw}Q_{hw}.$
3	$P = P_{сист} = P_{сл} =$ $= \left(1-\left(1-P_{hw}\right)^3\right)\left(P_{sw}^3 + 3\left(1-P_{sw}\right)P_{sw}^2\right)$ $Q = Q_{hw}^3 + Q_s - Q_{hw}^3 Q_s,$ где $Q_s = Q_{sw}^3 + 3\left(1-Q_{sw}\right)Q_{sw}^2.$

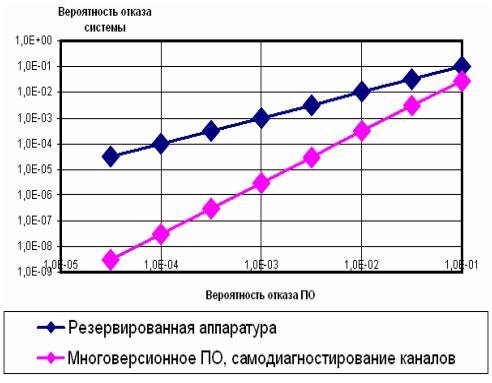


Рис. 4. Зависимость вероятности отказа системы от вероятности отказа версии ПО в предположении абсолютно надежной аппаратной части

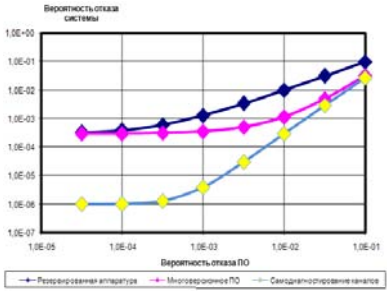


Рис. 5. Зависимость вероятности отказа системы от вероятности отказа версии ПО при вероятности отказа аппаратной платформы канала равной 0,01.

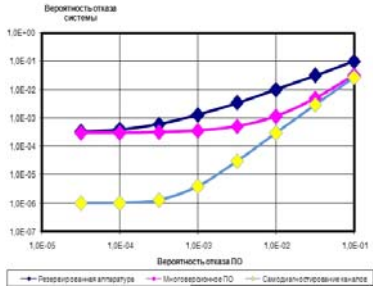


Рис. 6. Зависимость вероятности отказа системы от вероятности отказа версии ПО при равенстве вероятностей отказов аппаратной платформы канала и версии ПО.

4. Заключение

Анализ представленных в статье моделей и построенных на их основе зависимостей позволяет сделать следующие выводы:

– система с резервированием только аппаратной части менее надежна, чем система, дополнительно использующая многоверсионное программное обеспечение, а последняя в свою очередь менее надежна, чем система, в которой реализовано самодиагностирование каналов;

– выигрыш от перехода к системным архитектурам, реализующим принцип самодиагностируемости, максимален при создании высоконадежных систем критического назначения, когда надежности аппаратной платформы канала и версии ПО примерно равны;

– при небольших накладных расходах на реализацию принципа программной самодиагностируемости канала достигается заметное повышение надежности всей системы, а вероятность отказа системы снижается в десятки, и даже сотни раз.

Таким образом, численные оценки подтверждают целесообразность построения надежных аппаратно-программных комплексов критического назначения с использованием многоверсионного программного обеспечения, дополнительно реализующего принцип программной автономной самодиагностируемости каналов, а тенденции развития микропроцессорной техники в направлении многоядерных систем предоставляют для этого все возможности.

Литература

1. Wikipedia, the free encyclopedia. Ariane 5 Flight 501, 17 January 2007 [Электронный ресурс]. – Режим доступа: http://en.wikipedia.org/.

2. Подделанные результаты испытаний [Электронный ресурс]. – Режим доступа: http://korrespondent.net/magnolia/22767.

3. Программная ошибка забросила «Союз» не туда [Электронный ресурс]. – Режим доступа: http://www.businesspress.ru/newspaper/article_mId_37_aId_263133.html.

4. Черкесов Г.Н. Надежность аппаратно-программных комплексов: учеб.пособ. – СПб.: Питер, 2005. – 478 с.

5. Тэллес М. Наука отладки – М.: Кудиц-образ, 2003. – 560 с.

6. Douglass B.P., Real-Time Design Patterns Robust Scalable Architecture for Real-Time Systems. Addison Wesley, 27 September 2002.

7. Соммервилл И. Инженерия программного обеспечения: пер. с англ./И. Саммервилл, 6-е изд. – М.: Изд. дом «Вильямс», 2002. – 624 с.

Поступила в редакцию 28.02.2008

Рецензент: д-р техн. наук, проф. И.В.Чумаченко, Национальный аэрокосмический университет им. Н.Е. Жуковского “ХАИ”, Харьков.