УДК 681.518

ОБОСНОВАНИЕ ПРОГРАММНЫХ ПРОЦЕДУР КОНТРОЛЯ И ДИАГНОСТИРОВАНИЯ ДЛЯ ОБЕСПЕЧЕНИЯ ТРЕБУЕМОЙ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ ЦИФРОВЫХ СИСТЕМ

д.т.н., проф. Е.А. Артёменко, к.т.н. И.Я. Гайворонский, И.Н. Клюшников

Исследуется эффективность различных методов контроля и структурного резервирования в обеспечении отказоустойчивости цифровых систем.

Постановка проблемы. Все более широко используются на практике и совершенствуются микропроцессорные цифровые системы. Для таких систем характерно наличие как устойчивых, так и неустойчивых отказов (сбоев). Отказы и сбои в процессе функционирования цифровых управляющих систем приводят к возникновению ошибок, что влечет нарушение целостности данных, снижение готовности, а также к непредсказуемому поведению системы, которое может повлечь тяжелые последствия. Особенно это относится к системам критического применения, в составе которых, в последнее время, находят применение встраиваемые цифровые вычислительные системы [1, 2]. Необходимая их высокая эффективность может быть достигнута только при реализации требуемых методов контроля и восстановления наряду с использованием разнообразных методов обеспечения высокой безотказности. При этом использование программных средств обеспечения отказоустойчивости позволяет снизить стоимость таких систем, так как не требует каких-либо аппаратных доработок и легко адаптируется к различным аппаратным платформам. Важно установить какие методы резервирования и контроля при этом целесообразно использовать в конкретных практических ситуациях.

Анализ литературы. До недавнего времени при разработке отказоустойчивых решений для цифровых управляющих вычислительных систем чаще всего прибегали к использованию аппаратной избыточности [3, 4]. Достоинством таких решений является их высокое быстродействие. Однако такие решения достаточно дороги, поэтому ведутся разработки, направленные на снижение стоимости разрабатываемых систем [5 – 8]. Предпосылкой для таких разработок явилось то, что за 10 лет быстродействие цифровой техники увеличилось в 1000 раз и ограничение на оперативность вычислений не является таким критичным как ранее. В работах [7, 8] основное внимание уделяется фиксации ошибок в массивах данных и кодов при выпол-

нении алгоритмов. При этом причины их возникновения не рассматриваются. Результаты проведенного моделирования [9] указывают на то, что возникновение отказов и сбоев по-разному влияет на готовность системы вследствие применения различных восстановительных процедур. Ложная идентификация сбоев как устойчивых отказов может привести к снижению готовности на 0,1, в сравнении со случаем правильной идентификации. Поэтому важно не только фиксировать возникновение ошибок, но и правильно определять характер причины их возникновения посредством реализации соответствующего алгоритма контроля и диагностирования.

Цель статьи. Разработка и исследование влияния программных процедур контроля, диагностирования и локализации ошибок, и идентификации их причин и сравнение эффективности таких процедур с аппаратными решениями.

Постановка задачи. Рассмотрим, каким образом организация контроля с применением различных видов избыточности оказывает влияние на эффективность разрабатываемых систем. Под эффективностью будем понимать степень достижения системой ожидаемого результата [10]. При рассмотрении функционирования вычислительных систем различных структур в качестве показателя будем использовать вероятность получения достоверного результата в ходе проведения вычислений (обработки данных) [11, 12]. Рассматриваемые системы функционируют по жестким, заранее известным алгоритмам и осуществляют периодическую обработку поступающей (накапливаемой) информации с выдачей требуемой информации.

В качестве базовых архитектур при анализе будем использовать наиболее интересные структуры: одноканальную, дублированную ($n = 2$ – количество каналов), мажоритарно-резервированную ($n = 3$, $m = 2$ – порог срабатывания мажоритарного элемента) структуры и структуру со схемой голосования «один из двух по два». Примем допущения, что все каналы равно надежны, моменты возникновения отказов (сбоев) подчиняются экспоненциальному закону распределения, интенсивность возникновения отказов (сбоев) $\lambda = 10^{-3}$ 1/ч ($\lambda = 10^{-2}$ 1/ч), схемы голосования (сравнения) абсолютно надежны и их стоимость намного меньше стоимости канала. Сбои, в случае их возникновения, проявляются только в течение времени одного цикла вычислений $\tau = 0{,}001$ ч, если сбои проявляются в течение большего количества циклов, то канал считается отказавшим.

Разработка и исследование различных процедур локализации и идентификации в системах контроля с различной структурой. При использовании одноканальной структуры для повышения достоверности результата применяют программно-логический контроль, суть которого состоит во введении временной избыточности, необходимой для повторного

выполнения вычислений и сравнения результатов вычислений с результатами, полученными ранее. Так как в принятых допущениях сбои проявляются только в одном цикле вычислений, то данный подход можно использовать для обнаружения искажения результатов вычислений из-за возникновения сбоев. При этом в случае совпадения результатов принимается решение об отсутствии сбоев, а при несовпадении возникает необходимость в выполнении еще одного цикла вычислений для того, чтобы при голосовании по большинству выбрать верный результат.

Однако в случае совпадения результата двух вычислений принимается решение об отсутствии сбоев, но данная ситуация может возникнуть и в случае возникновения устойчивого отказа. Тогда целесообразно добавление еще одного цикла для проведения диагностических операций. В качестве последних можно использовать функциональное тестирование – проведение вычислений по основной программе, но над тестовыми значениями, со сравнением полученного результата с эталонным. Примем допущение, что длительность тестового цикла будет на 10 % больше в связи с необходимостью проведения операций загрузки тестовых исходных данных и эталонного результата.

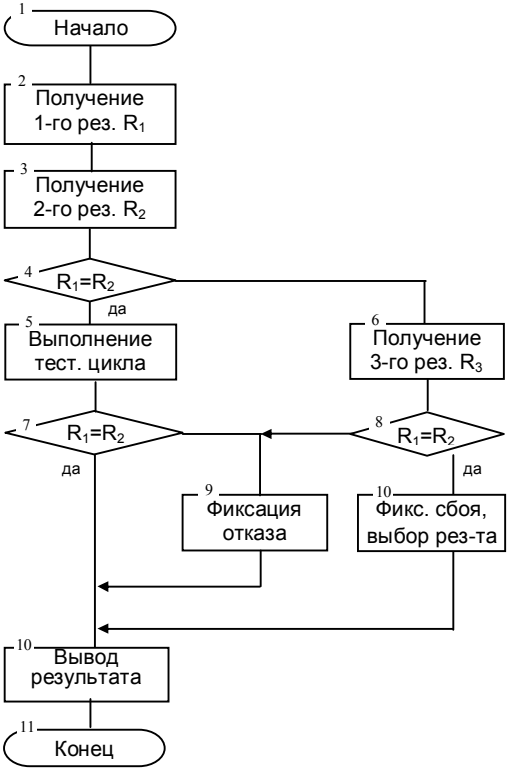

Рис. 1. Алгоритм принятия решения при возникновении отказов и сбоев

Алгоритм принятия решения при возникновении отказов и сбоев для одноканальной системы представлен на рис. 1. Применение данного подхода позволяет не только фиксировать возникновение ошибки при функционировании, но определять их причины.

Для одноканальной системы с учетом контроля и идентификации причин ошибок коэффициент временной избыточности $k_t = 3{,}1$, так как длительность вычислений составля-

ет три цикла (3τ) плюс 10 % от времени выполнения цикла (0,1 τ), необходимые для загрузки эталонных исходных данных и сравнения результатов, полученных при их обработке, с эталоном.

При проведении оценки эффективности будем рассматривать следующий режим функционирования. Пусть система включена (функционирует в режиме ожидания) в течение некоторого времени t, по достижении которого поступают данные, длительность цикла обработки которых равна τ, по окончании выполнения проводятся операции контроля. Тогда вероятность получения достоверного результата равна

$$P_{др} = P_o(t + 3{,}1\tau) \cdot (P_c(3{,}1\tau) + 2P_c(2{,}1\tau) \cdot (1 - P_c(\tau)), \qquad (1)$$

где $P_o(t + 3,\ 1\tau)$ – вероятность отсутствия отказов в течение режима ожидания и времени выполнения задания с учетом контроля; $P_c(3,\ 1\tau)$ – вероятность отсутствия сбоев в течение двух циклов выполнения задания и в течение диагностического цикла; $2P_c(2\tau)\cdot(1- P_c(\tau))$ – вероятность возникновения сбоев в течение первого, либо второго цикла, и отсутствия сбоев в течение времени выполнения третьего цикла.

Реализация принципа отказоустойчивости предполагает не только обнаружение нарушения нормального функционирования, но и продолжение функционирования в случае возникновения отказа. Для одноканальной структуры в случае возникновения устойчивого отказа дальнейшее продолжение работы невозможно. Поэтому наряду с временной необходима реализация структурной избыточности.

Применение дублированной структуры обеспечивает выполнение условий, указанных выше, и позволяет путем сравнения результатов, полученных при выполнении задачи в разных каналах, фиксировать как возникновение сбоев, так и наличие устойчивых отказов. Однако трудность представляет определение канала, в котором возник отказ (сбой). В данном случае необходимо проведение повторного цикла вычислений и анализа полученных результатов. Однако при таком подходе может возникнуть ситуация, требующая дополнительных мероприятий для определения отказавшего канала.

С учетом вышесказанного для дублированной системы $k_t = 3{,}1$.

При функционировании дублированной структуры, рассмотренной выше, вероятность получения достоверного результата равна

$$P_{др} = P_o^2(t + 2\tau) \cdot \left(P_c^2(2\tau) + 4P_c^3(2\tau)(1 - P_c(2\tau)) + 4P_c^2(2\tau)(1 - P_c(2\tau))^2\right) + \\ + 2P_o(t + 3{,}1\tau) \cdot (1 - P_o(t + 3{,}1\tau))\left(P_c(3{,}1\tau) + 3P_c^2(2{,}1\tau)(1 - P_c(\tau))\right). \qquad (2)$$

Аналогичным образом получим выражения, описывающие вероятность получения достоверного результата для мажоритарной структуры (3) и структуры, используемой при производстве отказоустойчивых сер-

веров компанией Stratus (применение дублирования парных каналов– система “один из двух по два”) (4):

$$P_{др} = P_o^4(t+\tau)P_c^4(\tau) + P_o^4(t)\,4P_o^3(\tau)(1-P_o(\tau))P_c^4(\tau) + \\ + 4P_o^3(t)(1-P_o(t))P_c^4(\tau) + P_o^4(t+\tau)\,4P_c^3(\tau)(1-P_o(\tau)); \quad (3)$$

$$P_{др} = P_o^4(t+\tau)P_c^4(\tau) + P_o^4(t)\,4P_o^3(\tau)(1-P_o(\tau))P_c^4(\tau) + \\ + 4P_o^3(t)(1-P_o(t))P_c^4(\tau) + P_o^4(t+\tau)4P_c^3(\tau)(1-P_o(\tau)). \quad (4)$$

Значение k_t для рассматриваемых структур равно 1, так как дополнительных временных затрат для идентификации причин нарушения функционирования не требуется.

График изменения значений вероятности получения достоверного результата рассмотренных структур, вычисленных по формулам (1 – 4) от длительности режима ожидания представлен на рис. 2.

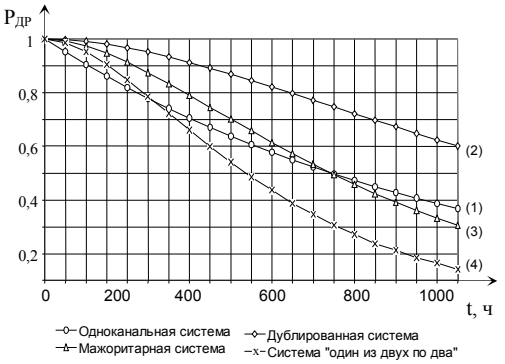

Рис. 2. График зависимости вероятности получения достоверного результата от длительности режима ожидания

Анализ графика указывает на то, что наибольшей вероятностью получения достоверного результата обладает дублированная система. Мажоритарно-резервированная система обладает меньшим значением вероятности, чем дублированная, но большей, чем остальные системы. А при t = 690 ч значение вероятности получения достоверного результата для этой системы становится меньше, чем у одноканальной.

Введем в рассмотрение понятие скорости поступления информации

$$\vartheta = \frac{V}{k_t n}, \quad (5)$$

где n – количество операций, необходимых для выполнения рабочего алгоритма (оп); V – число операций в секунду (оп/с).

Если стоимость системы С определять количеством каналов, то для рассматриваемых структур она будет равна 1, 2, 3 и 4, соответственно для одно-, двухканальной, мажоритарной структуры и структуры с дублированием парных каналов. С учетом стоимости систем коэффициент затрат, учитывающий временные и материальные затраты на организа-

цию контроля, будет иметь вид

$$\delta = \frac{\vartheta}{C} = \frac{V}{k_t n C}. \qquad (6)$$

Для идентичных каналов значения n и V можно считать одинаковыми, поэтому эффективность системы контроля, с учетом допущений, можно определить по формуле

Рис. 3. График зависимости эффективности систем контроля от длительности режима ожидания

$$W = P_{др}\delta = \frac{P_{др}}{k_t C}. \qquad (7)$$

График зависимости эффективности систем контроля от длительности периода ожидания представлен на рис. 3.

Выводы. Анализ результатов, представленных на рис. 3, указывает на то, что системы с использованием программно-логического контроля могут являться альтернативой для систем с аппаратной реализацией контроля даже с учетом временных затрат при больших значениях длительности периода ожидания. Если же учитывать только стоимость систем (рис. 4), то применение систем с программным контролем

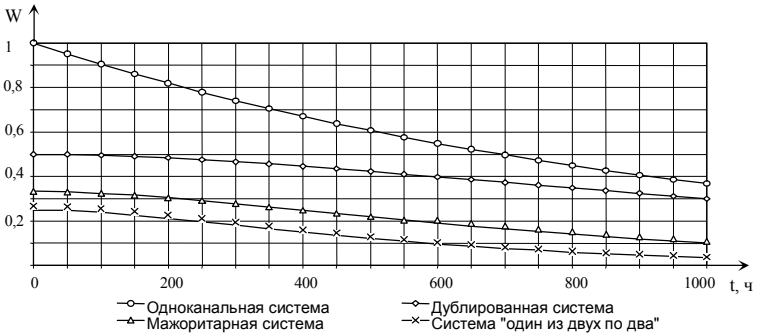

Рис. 4. График зависимости эффективности систем контроля от длительности режима ожидания

(одно- и двухканальные) эффективнее систем, в которых используется только аппаратный контроль при любых значениях длительности периода ожидания.

Полученные результаты дают возможность обосновать целесооб-

разный вариант структуры и организации контроля, обеспечивающий необходимую эффективность цифровых систем.

ЛИТЕРАТУРА

1. *Hiller M. Executable Assertions for Detecting Data Errors in Embedded Control System // Proc. Int'l Conf. Dependable System and Network (DSN 2000). – June 2000. – P. 24 – 33.*
2. *Bauer G., Kopetz H. Transparent Redundancy in the Time-Trigged Architecture // Proc. Int'l Conf. Dependable System and Network (DSN 2000). – June 2000. – P. 5 – 8.*
3. *Шнитман В. Отказоустойчивые компьютеры компании Stratus // Открытые системы, 1998. – № 1.*
4. *Игнатущенко В. Отказоустойчивость компьютеров и банки // Банковские технологии. – 1997. – № 11. – http://www.cpm.ru/publications /bt_oct97.html.*
5. *Holm J.G., Banerjee P. Low Cost Concurrent Error Detection in a VLIP Architecture Using Replicated Instructions // Proc. Int'l Conf. Parallel Processing. – 1992. – P. 102 – 195.*
6. *IAEA Working Materials. Scientific Basis and Engineering Solutions for Cost-Effective Assessments of Software-Based I&C Systems // Proceeding of Coordinated Research Meeting. – Vienna, Austria. – 8 – 12 November, 1999. – P. 67 – 75.*
7. *Oh, N., S. Mitra, E.J. McCluskey. ED^{4}I: error detecting by diverse data and duplicated instructions // IEEE Trahsaction on Computer. – Vol. 51. – Febriary, 02. – P. 180 – 199.*
8. *Oh, N., P.P. Shirvani, E.J. McCluskey. Error detecting by duplicated instructions in super-scalar processors // IEEE Trahsaction on Reliability. – Vol. 51. – March, 2002. – P. 63 – 75.*
9. *Клюшников И.Н. Выбор методов контроля и диагностирования для повышения эффективности функционирования информационно-управляющих систем // Системи обробки інформації. – Х.: НАНУ, ХВУ. – 2002. – Вип. 6 (22) – С. 127 –133.*
10. *Надежность и эффективность в технике. Т.1. Методика, организация, терминология / Под ред. А.И. Рембезы – М.: Машиностроение, 1986. – 224 с.*
11. *Дрозд А.В. Достоверность рабочего диагностирования вычислительных устройств для обработки приближенных вычислений // Системи обробки інформації. – Х.: НАНУ, ХВУ. – 2002. – Вип. 4 (20) – С. 8 – 13.*
12. *Шербаков Н.С. Достоверность работы цифровых устройств. – М.: Машиностроение, 1989. – 288 с.*

Поступила 29.01.2003

***АРТЁМЕНКО Евгений Андреевич**, доктор техн. наук, профессор кафедры ХВУ. В 1948 году окончил Краснознаменную ордена Ленина Военно-воздушную инженерную академию им. Н.Е. Жуковского. Область научных интересов – теория и практическое использование автоматизированных систем контроля сложных технических систем.*

***ГАЙВОРОНСКИЙ Игорь Ярославович**, канд. техн. наук, зам. нач. кафедры ХВУ. В 1992 году окончил ХВВКИУ РВ. Область научных интересов – практическая оптимизация.*

***КЛЮШНИКОВ Игорь Николаевич**, адъюнкт ХВУ. В 1995 году окончил ХВУ. Область научных интересов – системы контроля и диагностирования цифровых управляющих систем.*