УДК 004.315

М. А. ДРОЗД, Ю. В. ДРОЗД

Одесский национальный политехнический университет

ПРОБЛЕМА СКРЫТЫХ НЕИСПРАВНОСТЕЙ ДЛЯ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ КРИТИЧЕСКОГО ПРИМЕНЕНИЯ

Статья посвящена вопросам функциональной безопасности информационно-управляющих систем критического применения, обслуживающих объекты повышенного риска. Рассматривается проблема скрытых неисправностей, связанная с низкой контролепригодностью цифровых компонентов. Определяются пути решения проблемы. Анализируются причины, препятствующие реализации этих путей. Рассматриваются ресурсы для обеспечения функциональной безопасности систем критического применения. Предлагается метод распараллеливания вычислений в последовательном коде, решающий проблему при обеспечении высокой производительности и достоверности результатов.

Ключевые слова: *Система критического применения, цифровой компонент, проблема скрытых неисправностей, контролепригодность, развитие ресурсов, распараллеливание вычислений.*

Введение

Объекты повышенного риска, представленные в энергетике, на транспорте, в космической и оборонной отраслях, уже стали неотъемлемой частью окружения человека. К ним относятся энергетические сети и электростанции, летательные аппараты и наземные системы обеспечения полетов, различные виды вооружений. Их разработка и эксплуатация без широкого использования информационных технологий невозможна [1].

Для обслуживания объектов повышенного риска разрабатываются информационно-управляющие системы критического применения (ИУС), которые являются развитием компьютерных систем с диверсификацией рабочего режима его разделением на нормальный и аварийный [2].

К ИУС предъявляются высокие требования по комплексу показателей, регламентированных международными стандартами. Среди наиболее важных выделяются требования по обеспечению функциональной безопасности [3, 4].

Основой для построения безопасных цифровых компонентов ИУС традиционно служат технологии проектирования отказоустойчивых устройств, включающие использование корректирующих кодов, мажоритарных структур, различных видов резервирования элементов и реконфигурации систем, а также многоверсионных решений для предотвращения отказов по общей причине [5, 6].

Однако одна только отказоустойчивость недостаточна для обеспечения функциональной безопасности цифровых компонентов, что связано с проблемой накопления в них на протяжении продолжительного нормального режима скрытых неисправностей, снижающих отказоустойчивость ИУС в наиболее ответственном аварийном режиме [7].

С ростом сложности и мощности объектов повышенного риска, а также численности и расширения круга областей их применения эта проблема становится ключевой в обеспечении безопасности ИУС и требует проведения исследований по ее решению.

В разделе 1 предлагаются пути решения проблемы скрытых неисправностей, анализируя диверсификацию контролепригодности цифровых компонентов в ИУС, а в разделе 2 обсуждаются объективные и субъективные причины низкой контролепригодности цифровых компонентов ИУС, накладывающие ограничения на реализацию путей. Раздел 3 рассматривает уровни развития ресурсов для решения проблемы скрытых неисправностей по третьему пути. В разделе 4 предлагается метод распараллеливания вычислений в последовательном коде, позволяющий решать проблему скрытых неисправностей с учетом высоких требований к производительности, достоверности и другим показателям.

1. Проблема скрытых неисправностей и пути ее решения

Проблема скрытых неисправностей следует из диверсификации рабочего режима ИУС, вслед за которой аналогичное развитие получает контролепригодность цифровых устройств.

Понятие контролепригодности сформировалось в тестовом диагностировании для оценки сложности синтеза тестов, направленных на выявление неис-

правностей в паузах рабочего режима. Оценка выполняется для точек цифровой схемы путем вычисления управляемости, наблюдаемости и контролепригодности как их произведения [8].

В РД, выполняемом при функционировании цифровых компонентов в рабочем режиме, наблюдаемость совпадает с контролепригодностью, а управляемость является их верхней границей [9].

Для ИУС контролепригодность важна, прежде всего, с позиции сохранения отказоустойчивости их компонентов в аварийном режиме.

Диверсификация контролепригодности заключается в том, что она становится различной для нормального и аварийного режима работы цифровых устройств, приобретает характер функциональной, проявляя зависимость не только от структуры схемы, но и особенностей подаваемых входных последовательностей рабочих слов [10, 11].

Кроме того, контролепригодность проявляет себя ограниченной в нормальном режиме.

В совокупности диверсность контролепригодности и ее ограниченность в нормальном режиме приводят к появлению в схемах потенциально опасных точек, в которых в нормальном режиме могут накапливаться скрытые неисправности, проявляющиеся в аварийном режиме, снижая уровень отказоустойчивости и соответственно безопасности ИУС.

Это определяет три пути решения проблемы скрытых неисправностей:

1) обеспечить полную контролепригодность в нормальном режиме ИУС;

2) выявлять потенциально-опасные точки и устранять те из них, которые представляют реальную угрозу безопасности ИУС;

3) сделать контролепригодность одинаковой для обоих режимов ИУС, чтобы скрытые неисправности нормального режима оставались скрытыми и в аварийном режиме.

2. Объективные и субъективные причины низкой контролепригодности цифровых компонентов ИУС

Для анализа возможностей реализации указанных путей целесообразно различить объективные и субъективные причины диверсности и ограниченности контролепригодности цифровых компонентов ИУС.

Объективные причины определяются особенностями ИУС как систем критического применения. К первой относится структурная избыточность отказоустойчивых цифровых компонентов, снижающая их контролепригодность [12].

Вторая причина следует из проектирования ИУС для функционирования в двух режимах, в которых цифровые компоненты обрабатывают различные, а, следовательно, ограниченные по составу входные данные. Ограничение по входным данным повышает структурную избыточность цифровых схем, дополнительно снижая их контролепригодность и способствуя накоплению скрытых неисправностей в течение продолжительного времени работы ИУС в нормальном режиме. На входных словах аварийного режима накопленные неисправности могут проявиться в количестве, которое превышает возможности цифровых компонентов предотвращать отказы, нарушая функциональную безопасность ИУС и объектов повышенного риска.

Появление скрытых неисправностей на ограниченном множестве входных слов демонстрирует пример, представленный в табл. 1.

Таблица 1

Появление скрытых неисправностей на ограниченном множестве входных слов

№	1	2	3	4	5	6	7	8	9
	c	b	a	C	S	C	S	C	S
0	0	0	0	0	0	0	0	0	0
1	0	0	1	0	1	0	1	0	1
2	0	1	0	0	1	0	1	0	1
3	0	1	1	1	0	–	–	0	1
4	1	0	0	0	1	–	–	0	0
5	1	0	1	1	0	–	–	0	1
6	1	1	0	1	0	–	–	0	1
7	1	1	1	1	1	–	–	0	1

В ее столбцах 1 – 5 приведена таблица истинности функций переноса C и суммы S полного сумматора для слагаемых a, b и c. Столбцы 6 и 7 содержат частичное определение этих функций при работе на ограниченном множестве первых трех наборов, составляющих 37,5% входных слов. В столбцах 8 и 9 показано совпадение частично определенных функций с функциями неисправностей «константа нуля» и «монтажное ИЛИ» замыкания входов слагаемых a и b.

Субъективные причины, поддающиеся устранению, складываются из особенностей построения ИУС, ориентированных на достижение высоких, но не всегда обоснованных показателей, например, высокой стабильности амплитуды сигналов на выходах датчиков измеряемых параметров. Сигналы оцифровываются с преобразованием в двоичные коды, которые при низком уровне шума изменяются только в младших разрядах, что происходит в течение продолжительного времени нормального режима. Кроме того, устанавливается необоснованно высокий коэффициент отношения “сигнал / шум”, используя цифровые компоненты с многими тысячами

состояний для различения только двух режимов – нормального и аварийного. Все эти избыточные решения дополнительно снижают контролепригодность цифровых схем. Но более всего она ограничивается обработкой данных в параллельных кодах на однотактных устройствах с матричным параллелизмом, что стало традиционным для ИУС в стремлении обеспечить высокий уровень производительности цифровых компонентов.

Отмеченные объективные причины не позволяют реализовать первый путь в полной мере. Можно только приблизиться к уровню полной контролепригодности цифровых устройств в нормальном режиме. Разработаны методы повышающие контролепригодность в нормальном режиме до верхней границы, а также методы повышения самой верхней границы [13].

Первый путь предполагает диверсификацию методов и средств РД, выделяя среди них те, которые непосредственно нацелены на выявление скрытых неисправностей в нормальном режиме. С развитием схемотехнических решений до уровня заготовки результатов появляются новые возможности диверсификации методов и средств РД. Их суть состоит в организации выбора не только текущих результатов нормального режима, но также одновременно результатов, характерных для аварийного режима работы ИУС, с целью контроля их достоверности.

Второй путь повышает функциональную контролепригодность, основываясь на методах выявления потенциально опасных точек, анализе рисков проявления в аварийном режиме накопленных в них неисправностей, а также выборе и разработке методов устранения реально опасных точек. В основе этих методов лежит нарушение хотя бы одного из условий, относящих эти точки к потенциально опасным [14].

Третий путь требует совершенствования компьютерных средств, повышая уровень развития используемых целевых ресурсов.

3. Развитие ресурсов для решения задач безопасности ИУС

В развитии ресурсов, используемых для решения задач проектирования ИУС, – моделей, методов и средств – можно выделить ряд уровней: репликацию, диверсификацию и автономизацию (движение к самодостаточности), занимающих в иерархии уровней соответственно нижнее L, среднее и верхнее H положение. Все предшествующие уровни являются обеспечивающими для следующих за ними: переход к автономизации возможен только в результате диверсификации целевых ресурсов, и оба эти уровня основываются на репликации.

На всех уровнях от L до H целью является выживание, которое обеспечивается различными методами: повышением производительности, безопасности (достоверности результатов) и независимости, соответственно.

Виды параллелизма отражают уровни развития ресурсов по степени преодоления зависимостей, ограничивающих возможности распараллеливания вычислений. К таким ограничениям относятся зависимости по данным, когда еще не доступны операнды для выполнения операции, и по управлению в случае еще невычисленного условия, по которому выполняется ветвление алгоритма вычислений [15].

Сравнивая матричный и конвейерный параллелизм, можно отметить, что матричный параллелизм ограничен по обеим зависимостям (при их наличии). Его целесообразно применять в случаях, для которых отсутствуют ограничивающие зависимости. Вместе с тем, он широко используют при множественных зависимостях по данным, включая ИУС. Матричный параллелизм получил развитие в однотактных устройствах при обработке числовых данных в параллельных кодах, т.е. кодах, все разряды которых одновременно доступны для выполнения операции. Однако это не обеспечивает их одновременной обработки, поскольку старшие разряды чисел, как правило, вычисляются, используя младшие.

Арифметический n-разрядный сумматор параллельных кодов, образованный последовательным (по цепи переноса) соединением n одноразрядных, т.е. полных сумматоров, складывает данные последовательно разряд за разрядом. При этом каждый полный сумматор используется только на $1 / n$-ю часть времени выполнения операции.

Матричный умножитель в варианте самой быстрой схемы выполняет операцию за $2n - 2$ задержки полных сумматоров, т.е. такое их количество соединено последовательно [16], и каждый из полных сумматоров схемы используется только на малую, $1 / (2n - 2)$-ю часть времени умножения. Для $n = 32$ полные сумматоры задействованы в схемах сложения и умножения только соответственно на 3,1% и 1,6%, т.е. простаивают 96,9% и 98,4% времени выполнения операции. С переходом на 64-разрядную платформу показатели использования элементов ухудшаются вдвое. Высокие проценты простоя элементов являются существенным ограничителем контролепригодности точек их схем.

Конвейерный параллелизм, характеризуемый диверсификацией вычислений на участках конвейера, снимает зависимость по данным: результаты предыдущей операции используются в качестве операндов в следующих операциях.

Обработка данных, выполняемая с заготовкой результатов, свободна от обеих зависимостей.

Решение проблемы скрытых неисправностей по третьему пути требует минимизации потерь от использования матричного параллелизма.

Для этого достаточно перейти на следующий, средний уровень развития ресурсов – использование конвейера с минимальным присутствием матричного параллелизма на его участках, что достигается при поразрядной обработке данных, когда на участке за обработчиком двоичного разряда следует только регистр или триггер конвейера.

В таких поразрядных конвейерных устройствах входными словами являются отдельные значения двоичных разрядов, что делает их общими для нормального и аварийного режимов ИУС, реализуя в полной мере третий путь. Кроме того, повышается управляемость точек схем, способствующая росту контролепригодности в нормальном режиме, отражая направленность второго пути.

4. Метод распараллеливания вычислений в последовательном коде

Для обеспечения также высоких показателей в производительности и достоверности результатов предлагается метод распараллеливания вычислений в последовательном коде, используя форму многопоточной обработки данных. При этом наряду с конвейерным параллелизмом используется и матричный, но в его лучшем виде – как множество независимых, одновременно работающих конвейеров, т.е. в отсутствии зависимости по данным.

Эффективность предложенного решения может быть оценена следующим образом.

Время повторного выполнения вычислительной операции в однотактном устройстве с матричным параллелизмом и поразрядном конвейерном устройстве определяется по формулам:

$$T_M = t_{CM} + t_R;$$
$$T_P = (t_{CP} + t_R)\, n_P,$$

где t_{CM} и t_R – задержки комбинационной части однотактного устройства и регистра, соответственно;

t_{CP} и n_P – задержка комбинационной части поразрядного конвейерного устройства и количество тактов выдачи разрядов его результата.

Пусть $T_P = k_T T_M$, где k_T – коэффициент сравнения однотактного и поразрядного конвейерного устройства по времени выполнения операции. С учетом значений T_P и T_M коэффициент определяется по следующей формуле:

$$k_T = (t_{CP} + t_R)\, n_P / (t_{CM} + t_R).$$

Например, для устройств, выполняющих умножение двоичных кодов, временные параметры определяются следующим образом:

$$t_{CP} = t_{ADD} + t_{AND};$$
$$t_{CM} = (2n - 2)\, t_{ADD} + t_{AND};$$
$$n_P = 2n,$$

где t_{ADD} и t_{AND} – задержки полного сумматора и элемента И;

n – разрядность двоичных кодов сомножителей;

$$k_T = (t_{ADD} + t_{AND} + t_R)$$
$$2n / ((2n - 2)\, t_{ADD} + t_{AND} + t_R).$$

Пусть $t_{AND} + t_R = z\, t_{ADD}$, где коэффициент z характеризует соотношение задержек регистровой и комбинационной части поразрядного конвейерного устройства. Тогда

$$k_T = 2n\,(1 + z) / (2n - 2 + z). \qquad (1)$$

В табл. 2 приведены значения коэффициента k_T для различных значений разрядности n и коэффициента z.

Таблица 2

Сравнительная оценка времени выполнения умножения в однотактном и поразрядном конвейерном устройстве

n \ z	1	2	3	4	5
8	2,13	3	3,76	4,44	5,05
16	2,06	3	3,88	4,71	5,49
32	2,03	3	3,94	4,85	5,73
64	2,02	3	3,97	4,92	5,86

Табл. 2 показывает, какое количество поразрядных конвейеров обеспечивает замену однотактного устройства при сохранении производительности. Для z = 2, как это следует и из формулы (1), $k_T = 3$, т.е. три поразрядных конвейерных умножителя равносильны по производительности одному однотактному.

По сложности однотактный и поразрядный конвейерный умножители характеризуются соответственно квадратичной и линейной зависимостями затрат оборудования от разрядности n: $H_M = 2(n^2 - n)$ и $H_P = 5n$.

В табл. 3 приведены значения затрат оборудования H_M и H_P, коэффициента $k_H = H_M / H_P$, определяющего соотношение затрат оборудования по формуле

$$k_H = 0{,}4\,(n - 1),$$

а также коэффициента $k_{H/T} = k_H / k_T$, соотносящего производительность и сложность сравниваемых устройств.

Таким образом, метод распараллеливания вычислений в последовательном коде, обеспечивающий развитие однотактной обработки данных к многопоточной поразрядной конвейерной, позволя-

ет не только решить проблему скрытых неисправностей, но также одновременно повышает соотношение производительность / сложность. Это относит его к методам кратного эффекта с возможностью фокусирования эффекта на один или несколько показателей:

– упрощение решения;

– повышение производительности;

– снижение энергопотребления (при понижении уровня напряжения и тактовой частоты);

– повышение достоверности результатов (при объединении части или всех конвейеров в отказоустойчивые структуры).

Таблица 3

Сравнительная оценка однотактного и поразрядного конвейерного устройства по отношению производительности к сложности

n	8	16	32	48	64
H_M	112	480	992	4512	8064
H_P	40	80	160	240	320
k_H	2,8	6	12,4	18,8	25,2
$k_{H/T}$	0,93	2	4,13	6,37	8,4

Выводы

Передовым краем развития КМ является область критического применения, в которой компьютерные системы получили развитие как ИУС для обслуживания объектов повышенного риска, демонстрируя диверсификацию рабочего режима его разделением на нормальный и аварийный. В этих условиях высокие требования к функциональной безопасности ИУС перестали обеспечиваться только ее отказоустойчивостью, поскольку вслед за рабочим режимом диверсификации подверглась контролепригодность цифровых устройств, создав проблему скрытых неисправностей, снижающих отказоустойчивость компонентов ИУС в аварийном режиме.

Обозначились три пути решения проблемы скрытых неисправностей: обеспечение полной контролепригодности в нормальном режиме ИУС; выявление и устранение потенциально-опасных точек, неисправности в которых представляют реальную угрозу безопасности ИУС; обеспечение одинаковой контролепригодности для обоих режимов ИУС.

Первый путь не может быть реализован в полной мере по ряду объективных причин. Контролепригодность в нормальном режиме может быть повышена до ее верхней границы, и возможно частичное повышение самой верхней границы. Второй путь, направленный на выявление и устранение потенциально опасных точек, является затратным в соответствии с индивидуальным обслуживанием таких точек. Третий путь основан на развитии ресурсов до уровня использования поразрядного конвейера, входными словами которого являются значения двоичных разрядов, общие для нормального и аварийного режимов ИУС.

Предложенный метод распараллеливания вычислений в последовательном коде дополнительно обеспечивает кратный эффект высоких показателей производительности, достоверности результатов и низкой сложности, организуя на поразрядных конвейерах многопоточную обработку данных. Эффект может быть сфокусирован на упрощение решения, повышение производительности или достоверности результатов, а также снижение энергопотребления.

Литература

1. Безопасность критических инфраструктур: математические инженерные методы анализа и обеспечения [Текст] / под ред. В.С. Харченко / Министерство образования и науки Украины, Национальный аэрокосмический университет им. Н.Е.Жуковского «ХАИ». – Х., 2011. – 641 с.

2. Yastrebenetsky, M. A. (edit.). NPP I&Cs: Problems of Safety [Text] / M. A. Yastrebenetsky. – Ukraine, Kyiv : Technika, 2004.

3. Харченко, В. С. Компьютерные сети информационных и управляющих систем АЭС, построенные на основе открытых стандартов [Текст] / В. С. Харченко, А. В. Горбенко, В. В. Скляр // Ядерная и радиационная безопасность. – 2004. – Т. 7, №4. – С. 80 – 87.

4. Kharchenko, V. S. (edits). FPGA-based NPP I&C Systems: Development and Safety As-sessment [Text] / V. S. Kharchenko, V. V. Sklyar // RPC Radiy, National Aerospace University "KhAI", SSTC on Nuclear and Radiation Safety. – 2008. – 188 p.

5. Харченко, В. С. Надежность и отказоустойчивость компьютерных средств и систем [Текст] : учеб. пособие / В. С. Харченко, И. В. Лысенко, О. М. Тарасюк. – Х. : ХАИ, 2007. – 44 с.

6. Многоверсионные системы, технологии [Текст] / В. С. Харченко, В. Я. Жихарев, В. М. Илюшко, Н. В. Нечипорук. – Х. : Нац. аэрокосмический ун-т «Харьковский авиационный ин-т», 2003. – 486 с.

7. Checkability of the digital components in safety-critical systems: problems and solutions [Text] / A. Drozd, V. Kharchenko, S. Antoshchuk, J. Sulima, M. Drozd // Proc. IEEE East-West Design & Test Symposium, 9 – 12 Sept. 2011. – Sevastopol, Ukraine, 2011. – P. 411 – 416.

8. Беннетс, Р. Дж. Проектирование тестопригодных логических схем [Текст] / Р. Дж. Беннетс. – М. : Радио и связь, 1990. – 176 с.

9. Суліма, Ю. Ю. Оцінка та метод підвищення контролепридатності цифрових компонентів в системах критичного застосування [Текст] / Ю. Ю. Суліма, О. В. Дрозд // Холодильна техніка і технологія. – 2013. – № 1(141). – С. 90–92.

10. Online testing of safety-critical I&C systems in normal and emergency modes: Problems and solutions [Text] / A. Drozd, V. Kharchenko, S. Antoshchuk, M. Drozd // First International Workshop "Critical Infrastructure Safety and Security" (CrISS-DESSERT'11), 11 – 13 May 2011. – Kirovograd, Ukraine, 2011. – P. 139 – 147.

11. Рабочее диагностирование безопасных информационноуправляющих систем [Текст] / Под ред. А. В. Дрозда, В. С. Харченко. – Х. : Нац. аэрокосмический ун-т им. Н. Е.Жуковского «ХАИ», 2012. – 614 с.

12. Щербаков, Н. С. Достоверность работы цифровых устройств [Текст] / Н. С. Щербаков. – М. : Машиностроение, 1989. – 224 с.

13. Drozd, J. V. Features of Development of the Models and Methods in Co-Design and Testing of Computer Systems and their Components [Text] / J. V. Drozd, O. V. Drozd, J. J. Sulima // 6-th International Conference "Advanced Computer Systems and Networks: Design and Application", 16 – 18 Sept. 2013. – Lviv, Ukraine, 2013. – P. 29 – 31.

14. Checkability of safety-critical I&C system components in normal and emergency modes [Text] / A. Drozd, V. Kharchenko, S. Antoshchuk, M. Drozd // Journal of Information, Control and Management Systems. – 2012. – Vol. 10, No.1. – P. 33 – 40.

15. СуперЭВМ. Аппаратная и программная организация [Текст] / Под ред. С. Фернбаха. – М. : Радио и связь, 1991. – 320 с.

16. Мельник, А. О. Архітектура комп'ютера. Наукове видання [Текст] / А. О. Мельник. – Луцьк : Волинська обласна друкарня, 2008. – 470 с.

Поступила в редакцию 20.02.2014, рассмотрена на редколлегии 24.03.2014

Рецензент: д-р техн. наук, проф. Ю. А. Скобцов, Донецкий национальный технический университет, Донецк, Украина.

ПРОБЛЕМА СКРИТИХ НЕСПРАВНОСТЕЙ ДЛЯ ІНФОРМАЦІЙНО-УПРАВЛЯЮЧИХ СИСТЕМ КРИТИЧНОГО ЗАСТОСУВАННЯ

М. О. Дрозд, Ю. В. Дрозд

Стаття присвячена питанням функціональної безпеки інформаційно-управляючих систем критичного застосування, що обслуговують об'єкти підвищеного ризику. Розглядається проблема скритих несправностей, що пов'язана з низькою контролепридатністю цифрових компонентів. Визначаються шляхи вирішення проблеми. Аналізуються причини, що перешкоджають реалізації цих шляхів. Розглядаються ресурси для забезпечення функціональної безпеки систем критичного застосування. Пропонується метод розпаралелювання обчислень у послідовному коді, що розв'язує проблему при забезпеченні високої продуктивності та достовірності результатів.

Ключові слова: Система критичного застосування, цифровий компонент, проблема скритих несправностей, контролепридатність, розвиток ресурсів, розпаралелювання обчислень.

A PROBLEM OF HIDDEN FAULTS FOR INSTRUMENTATION AND CONTROL SAFETY-CRITICAL SYSTEMS

M. O. Drozd, J. V. Drozd

The paper is devoted to the questions of safety of the instrumentation and control safety-critical systems maintaining the objects of the raised risks. A problem of the hidden faults which is connected with the low checkability of the digital components is considered. The ways of solving the problem is defined. The reasons blocking realization of these ways are analyzed. The resources for ensuring safety of the safety-critical systems are considered A method of calculations paralleling in a serial code which solves the problem at assuring the high throughput and trustworthiness of results is offered.

Key words: system of critical application, digital component, problem of the hidden faults, checkability, development of resources, calculations paralleling.

Дрозд Мирослав Александрович – магистр, аспирант кафедры информационных систем Одесского национального политехнического университета, Одесса, Украина, e-mail: miroslav_dr@mail.ru.

Дрозд Юлия Владимировна – канд. техн. наук, доцент, доцент кафедры информационных систем Одесского национального политехнического университета, Одесса, Украина, e-mail: drozd@ukr.net.