ISSN 2076-2429 (print)
ISSN 2223-3814 (on line)

УДК 004.052
М.А. Дрозд, магистр, Одес. нац. политехн. ун-т

ПОВЫШЕНИЕ КОНТРОЛЕПРИГОДНОСТИ ЦИФРОВЫХ КОМПОНЕНТОВ СИСТЕМ КРИТИЧЕСКОГО ПРИМЕНЕНИЯ

М.О. Дрозд. **Підвищення контролепридатності цифрових компонентів систем критичного застосування.** Розглядається проблема накопичення скритих несправностей та функціональної контролепридатності цифрових компонентів, що обмежує функціональну безпеку систем критичного застосування в управлінні об'єктами підвищеного ризику. Аналізуються причини низької контролепридатності, яка може призвести до втрати відмовостійкості системи в аварійному режимі. Пропонуються методи паралельної обробки даних в послідовному коді, що підвищують функціональну контролепридатність для цифрових компонентів високопродуктивних систем.
Ключові слова: система критичного застосування, цифровий компонент, скриті несправності, функціональна контролепридатність, продуктивність, метод обробки даних.

М.А. Дрозд. **Повышение контролепригодности цифровых компонентов систем критического применения.** Рассматривается проблема накопления скрытых неисправностей и функциональной контролепригодности цифровых компонентов, ограничивающая функциональную безопасность систем критического применения в управлении объектами повышенного риска. Анализируются причины низкой контролепригодности, которая может привести к потере отказоустойчивости системы в аварийном режиме. Предлагаются методы параллельной обработки данных в последовательном коде, повышающие функциональную контролепригодность цифровых компонентов для высокопроизводительных систем.
Ключевые слова: система критического применения, цифровой компонент, скрытые неисправности, функциональная контролепригодность, производительность, метод обработки данных.

M.O. Drozd. **Increase of the digital components' checkability of safety-critical systems.** A problem of latent faults accumulation and on-line checkability of the digital components limiting the functional safety of safety-critical systems in controlling the high risk objects is considered. The reasons of the low checkability, which can lead to the loss of fault tolerance of the system in an emergency mode are analyzed. The methods of parallel data processing in a serial code which increase on-line checkability of the digital components for high throughput systems are offered.
Keywords: safety-critical system, digital component, latent faults, on-line checkability, throughput, method of data processing.

С развитием компьютерных технологий расширяется область их применения для обслуживания объектов повышенного риска в энергетике, на транспорте, в космической и оборонной отраслях. К таким объектам относятся энергетические сети и электростанции, летательные аппараты и наземные системы обеспечения полетов, различные виды вооружений. Компьютерное обслуживание обеспечивается информационно-управляющими системами критического применения (ИУС), которые проектируются для работы в рабочем и аварийном режимах [1]. Для таких систем европейскими и мировыми стандартами регламентируются повышенные требования к функциональной безопасности, распространяемые также на их компоненты [2]. Основой для построения безопасных цифровых компонентов ИУС 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 [3]. Однако одна только отказоустойчивость недостаточна для обеспечения функциональной безопасности цифровых компонентов, что связано с проблемой накопления в их схемах скрытых неисправностей,

снижающих отказоустойчивость ИУС в наиболее ответственном аварийном режиме. 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 для ее решения.

Для ИУС накопление скрытых неисправностей обусловлено различной контролепригодностью цифровых компонентов в рабочем и аварийном режимах. Понятие контролепригодности сформировалось в тестовом диагностировании для оценки сложности синтеза тестов выявления константных неисправностей, с использованием управляемости и наблюдаемости точек цифровых схем [4]. В рабочем диагностировании, выполняемом в процессе функционирования цифровых компонентов при обработке реальных входных данных, наблюдаемость совпадает с контролепригодностью, а управляемость является их верхней границей. Контролепригодность для ИУС важна, прежде всего, с позиции сохранения отказоустойчивости их компонентов в аварийном режиме. Изменение контролепригодности с переходом ИУС из одного режима в другой требует ее рассмотрения в комплексе как функциональной, учитывающей поведение неисправностей схем в обоих режимах. Функциональная контролепригодность оценивается как $1 - N / N_T$, где N — количество потенциально опасных точек схемы, в которых скрытые неисправности могут накапливаться и проявляться соответственно в рабочем и аварийном режимах, N_T — общее количество точек схемы. Оценки функциональной контролепригодности указывают на необходимость ее повышения [5].

Ограниченность функциональной контролепригодности цифровых компонентов обусловлена объективными и субъективными причинами ее низкого уровня в рабочем режиме.

Объективные причины определяются особенностями ИУС как систем критического применения. К первой относится структурная избыточность отказоустойчивых цифровых компонентов, снижающая их контролепригодность [4]. Вторая следует из проектирования ИУС для функционирования в двух режимах, в которых цифровые компоненты обрабатывают различные, а следовательно ограниченные по составу входные данные. Причем создаются ИУС для обеспечения безопасного функционирования объектов управления в аварийном режиме, а основную часть времени находятся в рабочем. 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 рабочем режиме. На входных данных аварийного режима накопленные неисправности могут проявиться в количестве, которое превышает возможности цифровых компонентов предотвращать отказы, нарушая функциональную безопасность ИУС и объектов повышенного риска.

Субъективные причины складываются из особенностей построения ИУС, в которых часто выполняются требования достижения 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 рабочего режима. Кроме того, устанавливается необоснованно высокий коэффициент отношения “сигнал / шум”: для различения только двух режимов — рабочего и аварийного — используются цифровые компоненты с многими тысячами состояний. Все эти избыточные решения дополнительно снижают контролепригодность цифровых схем. Но более всего контролепригодность ограничивается обработкой данных в параллельных кодах, что стало традиционным в ИУС и направлено на обеспечение высокой производительности цифровых компонентов.

Объекты управления могут обладать определенной инерционностью, что значительно снижает требования к временным параметрам и соответственно производительности цифровых компонентов. Например, для ИУС тепловых, атомных и гидроэлектростанций время выполнения ряда операций находится на уровне долей секунды [1]. Вместе с тем, специализированные процессоры, решающие задачи распознавания образов, могут быть нацелены на достижение максимальной производительности цифровых компонентов.

ISSN 2076-2429 (print)
ISSN 2223-3814 (on line)

Однако обработка параллельных кодов в однотактных устройствах существенно ограничена матричным параллелизмом их структур, который проявляет зависимость по данным. Поэтому параллельные коды обрабатываются последовательно-параллельно, и длина критического пути последовательного соединения операционных элементов в сумматорах и умножителях пропорциональна разрядности операндов. Однотактные устройства отличаются также большими затратами оборудования. Для матричных умножителей эти затраты находятся в квадратичной зависимости от разрядности операндов. Для параллельных сумматоров зависимость изменяется от линейной до кубической (при отсутствии и использовании различных способов ускорения распространения переносов). В традиционной обработке данных однотактные устройства, как правило, являются участками конвейера, т.е. матричный параллелизм занимает нижний уровень обработки, а конвейерный — верхний. При этом описанные недостатки матричного параллелизма передаются всей структуре обработки, которая демонстрирует не только низкую контролепригодность цифровых компонентов ИУС, но и их ограниченную производительность.

Для повышения функциональной контролепригодности производительных цифровых компонентов предлагаются методы параллельной обработки данных в последовательных кодах, в основу которых положено три вида параллелизма: конвейерный, матричный и заготовка результатов. Причем, на нижнем уровне обработки выполняется поразрядная конвейеризация вычислений, сокращающая матричную структуру участков конвейера до одного операционного элемента с максимальным снижением зависимости по данным.

Использование поразрядной конвейеризации повышает контролепригодность цифровых компонентов ИУС:

— обработка последовательного кода, содержащего хотя бы один ноль и одну единицу, приводит к изменению значений сигнала во всех точках схемы, т.е. повышает до 100% управляемость цифрового компонента и верхнюю границу его контролепригодности, что важно для рабочего режима работы ИУС;

— вслед за верхней границей повышается наблюдаемость и контролепригодность точек схем, чему способствуют логические элементы “ИСКЛЮЧАЮЩЕЕ ИЛИ”, присутствующие в полных сумматорах операционных элементов [4];

— повышается функциональная контролепригодность цифровых компонентов, поскольку сближаются ее значения в рабочем и аварийном режимах вследствие работы с одними и теми же входными данными, которыми для последовательных кодов являются их отдельные разряды.

На верхнем уровне выполняется многопоточная обработка данных с использованием свободного от зависимости по данным матричного параллелизма, объединяющего множество несвязанных друг с другом одновременно работающих поразрядных конвейеров.

Оценивая описанный метод обработки данных, следует отметить реализованные в нем линейные зависимости времени и сложности от разрядности операндов, которые в традиционной обработке данных имеют соответственно линейный и квадратичный характер, что свидетельствует о повышении соотношения “производительность / сложность”. Кроме того, предлагаемый метод позволяет гибко перераспределять показатели сложности и производительности, наращивая или уменьшая количество конвейеров. К достоинствам метода можно также отнести многократное снижение количества входов и выходов цифрового компонента, что повышает его технологичность и снижает энергопотребление в системе “ввод-вывод” современных интегральных схем.

К недостаткам метода можно отнести увеличенное время выдачи всего результата, растущее пропорционально разрядности обрабатываемых данных. Для приложений, где этот недостаток является существенным, предлагается метод параллельной обработки данных в последовательных кодах, использующие заготовку результатов [6]. В этом методе последовательный код разбивается на равные сегменты. Для старших разрядов сегменты повторяются с заготовкой под различные значения данных, которые могут быть вычислены сегментами младших разрядов. Сегменты обрабатываются одновременно, определяя по окончанию обработки возможные части результата и условие выбора составляющих его частей. Для суммирующих схем

цифровых компонентов, обрабатывающих данные в параллельном коде, таким образом выполняется ускоренное распространение переноса, известное как “условный перенос”, в котором обработка секций старших разрядов дублируется для исходного нулевого или единичного значений переноса [6].

Таким образом, предложенные методы обработки данных позволяют повысить функциональную контролепригодность цифровых компонентов ИУС, обеспечивая одновременно высокие уровни функциональной безопасности и производительности.

Литература

1. FPGA-based NPP I&C Systems: Development and Safety Assessment / E.C. Bakhmach, A.D. Herasimenko, V.A. Golovyr and others / ed. V.S. Kharchenko, V.V. Sklyar. — Kirovograd: RPC Radiy, Kharkiv: National Aerospace University “KhAI”, SSTC on Nuclear and Radiation Safety, 2008. — 188 p.
2. Safety of nuclear power plants: the information and control systems / M.A. Yastrebenetsky, V.N. Vasilchenko, S.V. Vinogradskaya and others; ed. M.A. Yastrebenetsky. — K.: Technika, 2007. — 460 p.
3. Kharchenko, V. Multi-Version FPGA-Based Nuclear Power Plant I&C Systems: Evolution of Safety Ensuring / V. Kharchenko, O. Siora, V. Sklyar // Nuclear Power — Control, Reliability and Human Factors. — Croatia: INTECH, 2011. — P. 27 — 48.
4. Щербаков, Н.С. Достоверность работы цифровых устройств / Н.С. Щербаков. — М.: Машиностроение, 1989. — 224 с.
5. Drozd, A. Checkability of safety-critical I&C system components in normal and emergency modes / A. Drozd, V. Kharchenko, S. Antoshchuk, M. Drozd // Journal of Information, Control and Management Systems. — 2011. — Vol. 1, № 1. — P. 56 — 63.
6. Рабочее диагностирование безопасных информационно-управляющих систем / А.В. Дрозд, В.С. Харченко, С.Г. Антощук и др.; под ред. А.В. Дрозда, В.С. Харченко. — Харьков: Нац. аэрокосм. ун-т им. Н.Е. Жуковского “ХАИ“, 2012. — 614 с.

References

1. FPGA-based NPP I&C Systems: Development and Safety Assessment / E.C. Bakhmach, A.D. Herasimenko, V.A. Golovyr and others / ed. V.S. Kharchenko, V.V. Sklyar. — Kirovograd: RPC Radiy, Kharkiv: National Aerospace University “KhAI”, SSTC on Nuclear and Radiation Safety, 2008. — 188 p.
2. Safety of nuclear power plants: the information and control systems / M.A. Yastrebenetsky, V.N. Vasilchenko, S.V. Vinogradskaya and others; ed. M.A. Yastrebenetsky. — Kyiv, 2007. — 460 p.
3. Kharchenko, V. Multi-Version FPGA-Based Nuclear Power Plant I&C Systems: Evolution of Safety Ensuring / V. Kharchenko, O. Siora, V. Sklyar // Nuclear Power — Control, Reliability and Human Factors. — Croatia: INTECH, 2011. — pp. 27 — 48.
4. Shcherbakov, N.S. Dostovernost’ raboty tsifrovkh ustroystv [Operation reliability of digital devices] / N.S. Shcherbakov. — Moscow, 1989. — 224 p.
5. Drozd, A. Checkability of safety-critical I&C system components in normal and emergency modes / A. Drozd, V. Kharchenko, S. Antoshchuk, M. Drozd // J. of Inform., Control and Management Systems. — 2011. — Vol. 1, # 1. — pp. 56 — 63.
6. Rabochee diagnostirovanie bezopasnykh informatsionno-upravlyayushchikh sistem [On-line testing of the safe instrumentation and control systems] / A.V. Drozd, V.S. Kharchenko, S.G. Antoshchuk and others; ed. by A.V. Drozd, V.S. Kharchenko. — Kharkiv: National Aerospace University named after N.E. Zhukovsky “KhAI”, 2012. — 614 p.

Рецензент д-р техн. наук, проф. Одес. нац. политехн. ун-та Положаенко В.А.

Поступила в редакцию 15 декабря 2013 г.