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

УДК 004.052

Ю.Ю. Сулима, магистр,
А.В. Дрозд, д-р техн. наук, проф.,
Одес. нац. политехн. ун-т

КОНТРОЛЕПРИГОДНОСТЬ ЦИФРОВЫХ КОМПОНЕНТОВ СИСТЕМ КРИТИЧЕСКОГО ПРИМЕНЕНИЯ

Ю.Ю. Суліма, О.В. Дрозд. **Контролепридатність цифрових компонентів систем критичного застосування.** Розглянуто питання контролепридатності цифрових компонентів систем критичного застосування, яка обмежує можливості робочого діагностування та забезпечення функціональної безпеки. Запропоновано оцінювати контролепридатність точок схем цифрових компонентів в штатному режимі за їх спостережуваністю з урахуванням частково контролепридатних точок. На прикладі матричного помножувача кількісно підтверджено низьку контролепридатність цифрових компонентів систем критичного застосування.

Ключові слова: система критичного застосування, цифровий компонент, штатний та критичний режими, робоче діагностування, контролепридатність, матричний помножувач.

Ю.Ю. Сулима, А.В. Дрозд. **Контролепригодность цифровых компонентов систем критического применения.** Рассмотрены вопросы контролепригодности цифровых компонентов систем критического применения, ограничивающей возможности рабочего диагностирования и обеспечения функциональной безопасности. Предложено оценивать контролепригодность точек схем цифровых компонентов в штатном режиме по их наблюдаемости с учетом частично контролепригодных точек. На примере матричного умножителя количественно подтверждена низкая контролепригодность цифровых компонентов систем критического применения.

Ключевые слова: система критического применения, цифровой компонент, штатный и критический режимы, рабочее диагностирование, контролепригодность, матричный умножитель.

Yu.Yu. Sulima, A.V. Drozd. **Checkability of digital components in safety-critical systems.** The problems of checkability of digital components in safety-critical systems, which limits the possibility of on-line testing and of ensuring the functional safety, have been considered. Assess controllability of points of digital components in the normal mode by their observability based on partly traceable points has been proposed. On the example of the iterative array multiplier low checkability of digital components in safety-critical systems is quantitatively confirmed.

Keywords: safety-critical system, digital component, normal and emergency modes, on-line testing, checkability, iterative array multiplier.

Компьютерные информационно-управляющие системы (ИУС) критического применения получают распространение в соответствии с возрастающими возможностями компьютерных технологий и расширением круга задач в областях повышенного риска, таких как энергетика, транспорт, оборонная и космическая отрасли и др. [1].

Одним из наиболее важных является вопрос обеспечения функциональной безопасности цифровых компонентов ИУС, который решается построением отказоустойчивых структур. В основе их получения лежит множество подходов — использование корректирующих кодов, мажоритарных структур, различных видов резервирования и реконфигурации, а также многоверсионных технологий [2].

Поскольку в системах критического применения противостояние отказам носит оперативный характер, то важную роль в обеспечении отказоустойчивости играют методы и средства рабочего диагностирования [3].

Возможности рабочего диагностирования ИУС существенно зависят не только от анализируемого цифрового компонента, но также и от рабочей последовательности входных слов, которая влияет на контролепригодность точек цифровой схемы.

Контролепригодность устройства — свойство, обусловливающее приспособленность к проведению контроля его технического состояния в процессе изготовления и эксплуатации. Контролепригодность цифровых устройств, как правило, рассматривают в тестовом диагностировании, где она оценивается по управляемости и наблюдаемости [4].

Особенности ИУС критического применения накладывают ограничения на формирование рабочих последовательностей входных слов для цифровых компонентов, снижая контролепригодность точек цифровой схемы. К особенностям, характеризующим такие системы, следует отнести, прежде всего, два основных режима работы: штатный и критический. Причем, в основном, ИУС критического применения работают в штатном режиме, а переход в критический режим, ради которого они проектируются, является редким событием и, в лучшем случае, никогда не наступает.

В штатном и критическом режимах ИУС и ее компоненты работают на различных множествах входных слов. Изменение входных слов в ограниченных диапазонах создает проблему низкой контролепригодности цифровых компонентов, которая ведет к накоплению скрытых константных неисправностей в штатном режиме. Эти неисправности могут нарушить функциональность цифровых компонентов ИУС в критическом режиме [5].

Контролепригодность цифровых компонентов в тестовом и рабочем диагностировании служит разным целям, и потому должна оцениваться с разных позиций. В тестовом диагностировании оценка контролепригодности направлена на определение возможности синтеза теста путем вычисления в каждой точке схемы произведения ее управляемости на наблюдаемость. В рабочем диагностировании контролепригодность важна для учета потенциальной угрозы со стороны скрытых неисправностей, при этом контролепригодность полностью определяется наблюдаемостью точек схемы на рабочих последовательностях входных слов.

Вместе с тем, понятие наблюдаемости целесообразно трактовать шире, учитывая в ней возможности частичной оценки точки схемы на наличие или отсутствие скрытых неисправностей.

Определение 1. Точка схемы называется частично наблюдаемой: 0-наблюдаемой или 1-наблюдаемой, если на множестве входных слов активируется путь от этой точки только при значении в ней сигнала “0” или “1”, соответственно. Если путь активируется при всех значениях сигнала, то точка называется наблюдаемой, а в остальных случаях — ненаблюдаемой. Путь активируется при передаче изменения значения сигнала из точки в контрольную точку схемы, подключаемую к схемам контроля цифрового компонента.

Определение 2. Точка схемы называется контролепригодной или частично контролепригодной, если является соответственно наблюдаемой или частично наблюдаемой, и неконтролепригодной в остальных случаях.

Контролепригодность цифрового компонента

$$C = (N_C + 0{,}5N_P) / N_T,$$

где $N_C, N_P, N_T,$ — количество контролепригодных, частично контролепригодных и всех точек схемы, соответственно.

Контролепригодность цифровых компонентов может быть оценена на примере матричного умножителя, выполненного на матрице $n \times (n-1)$ операционных элементов, где n — разрядность сомножителей. Операционный элемент первой строки матрицы состоит из полного сумматора и двух элементов И, а операционный элемент следующих строк — из полного сумматора и одного элемента И. Элементы И вычисляют конъюнкции матрицы произведения, а полные сумматоры складывают их с учетом веса, определяя полное произведение [6].

Сомножителями являются двоичные коды нормализованных мантисс в диапазоне $2^{n-1}...2^n - 1$. Исследуемые точки матричного умножителя — входы элементов И, а также входы и выходы полных сумматоров.

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

Для оценки контролепригодности матричного умножителя построена его программная модель, в которой рассчитывается контролепригодность отдельных точек цифровой схемы и устройства в целом для задаваемых множеств входных слов в штатном режиме. Входные слова составляются из значений сомножителей, каждый из которых изменяется с шагом 1 от задаваемого базового значения B до достижения заданного объема V диапазона. Количество входных слов штатного режима равно V^2, что составляет V_d=400 V^2/n^2 % от объема диапазона входных слов матричного умножителя. Кроме того, задается пороговое значение сомножителей S, с которого начинается критический режим.

В таблице приведены оценки количеств N и N^* неконтролепригодных точек, а также значений C и C^* контролепригодности матричного умножителя, посчитанные соответственно с учетом и без учета частично контролепригодных точек в экспериментах 1...8.

Оценка контролепригодности матричного умножителя в штатном режиме работы ИУС для разрядности n = 8

№ эксперимента	1	2	3	4	5	6	7	8
V	10	20	30	40	50	60	70	80
V^2	100	400	900	1600	2500	3600	4900	6400
V_d, %	0,2	2,4	5,5	9,8	15,3	22,0	29,9	39,1
N	177	128	119	85	81	78	44	42
C, %	36,6	54,2	57,4	69,6	71,0	72,1	84,3	85,0
N^*	195	146	137	103	99	96	62	60
C^*, %	30,2	47,7	50,9	63,1	64,6	65,6	77,8	78,5

Эксперименты проведены для $n = 8$, $B = 128$ и $S = 245$, а также изменения объема V диапазона сомножителей от значения 10 с шагом 10 до верхней границы 80. Две частично контролепригодные точки учитываются как одна контролепригодная и одна неконтролепригодная точка.

Результаты моделирования показывают, что с увеличением объема V диапазона сомножителей от 10 до 80 и соответственно количества V_d входных слов штатного режима от 0,2 до 39,1 % количество N неконтролепригодных точек снижается со 177 до 42, а контролепригодность C повышается от 36,6 до 85 %.

При игнорировании частично контролепригодных точек оценка C^* значения контролепригодности матричного умножителя снижается. Величина $C - C^*$ снижения контролепригодности находится на уровне 6,4 % в абсолютном выражении и уменьшается с ростом количества входных слов от 17,5 до 7,6 % в относительном выражении.

С дальнейшим увеличением количества входных слов значения контролепригодности практически не изменяются, что позволяет рассматривать результаты восьмого эксперимента как предельные.

Таким образом, проведенные эксперименты подтверждают низкую оценку контролепригодности цифровых компонентов СКП в количественном выражении, что ставит задачи на ее повышение.

Литература

1. FPGA-based NPP I&C Systems: Development and Safety Assessment / E.S. Bakhmach, A.D. Herasimenko, V.A.Golovir and others / ed. V.S. Kharchenko, V.V. Sklyar. — RPC Radiy, National Aerospace University “KhAI”, SSTC on Nuclear and Radiation Safety, 2008. — 188 p.
2. Kharchenko, V. Multi-version Systems: Models, Reliability, Design Technologies / V. Kharchenko // 10th Europ. Conf. on Safety and Reliability, — Munich, Germany. — Munich, 1999. — Vol. 1. — P. 73 — 77.
3. Рабочее диагностирование безопасных информационно-управляющих систем / А.В. Дрозд, В.С. Харченко, С.Г. Антощук и др.; под ред. Дрозда А.В., Харченко В.С. — Харьков: Нац. аэрокосмический ун-т им. Н. Е. Жуковского “ХАИ“, 2012. — 614 с.

4. Беннетс, Р.Дж. Проектирование тестопригодных логических схем / Р.Дж. Беннетс. — М.: Радио и связь, 1995. — 180 с.
5. On-line testing of safety-critical I&C systems in normal and emergency modes: Problems and solutions / A. Drozd, V. Kharchenko, S. Antoshchuk, M. Drozd // First Intern. Workshop “Critical Infrastructure Safety and Security“ (CrISS-DESSERT’11), Kirovograd, Ukraine, — Kirovograd, 2011. — P. 139 — 147.
6. Мельник, А.О. Архітектура комп’ютера. Наук. вид. / А.О. Мельник. — Луцьк: Волин. обл. друкарня, 2008. — 470 с.

References

1. FPGA-based NPP I&C Systems: Development and Safety Assessment / E.S. Bakhmach, A.D. Herasimenko, V.A.Golovir and others / ed. V.S. Kharchenko, V.V. Sklyar. — RPC Radiy, National Aerospace University “KhAI”, SSTC on Nuclear and Radiation Safety, 2008. — 188 pp.
2. Kharchenko, V. Multi-version Systems: Models, Reliability, Design Technologies / V. Kharchenko // 10th Europ. Conf. on Safety and Reliability. — Munich, Germany. — Munich, 1999. — Vol. 1. — pp. 73 — 77.
3. Rabochee diagnostirovanie bezopasnykh informatsionno-upravlyayushchikh sistem [On-line testing of safe instrumentation and control systems] / A.V. Drozd, V.S. Kharchenko, S.G. Antoshchuk and others / ed. by A. B. Drozd, V. S. Kharchenko. — Kharkiv, 2012. — 614 pp.
4. Bennets, R.Dzh. Proektirovanie testoprigodnykh logicheskikh skhem [Design of testable logic circuits] / R.Dzh. Bennets. — Moscow, 1995. — 180 pp.
5. On-line testing of safety-critical I&C systems in normal and emergency modes: Problems and solutions / A. Drozd, V. Kharchenko, S. Antoshchuk, M. Drozd // First Intern. Workshop “Critical Infrastructure Safety and Security” (CrISS-DESSERT’11), Kirovograd, Ukraine, — Kirovograd, 2011. — pp. 139 — 147.
6. Mel’nik, A.A. Arkhitektura komp’yutera. Nauk. vyd. [Architecture of computer. Academic publication] / A.A. Mel’nik. — Lutsk, 2008. — 470 pp.

Рецензент д-р техн. наук, проф. Одес. нац. политехн. ун-та Ситников В.С.

Поступила в редакцию 16 ноября 2012 г.