УДК 004.315

А.В. ДРОЗД[1], В.С. ХАРЧЕНКО[2], С.Г. АНТОЩУК[1], М.А. ДРОЗД[1]

[1]Одесский национальный политехнический университет, Украина
[2]Национальный аэрокосмический университет им. М.Е. Жуковского "ХАИ", Украина

КОНТРОЛЕПРИГОДНОСТЬ ЦИФРОВЫХ КОМПОНЕНТОВ СИСТЕМ КРИТИЧЕСКОГО ПРИМЕНЕНИЯ ПО ОТНОШЕНИЮ К НЕИСПРАВНОСТЯМ ТИПА «ЗАМЫКАНИЕ»

Статья посвящена проблеме низкой контролепригодности цифровых компонентов информационных управляющих систем критического применения, предназначенных для обеспечения безопасности объектов повышенного риска. Анализируются потенциально опасные точки цифровых компонентов, в которых в нормальном режиме могут накапливаться скрытые неисправности, снижающие уровень отказоустойчивости схем в аварийном режиме. Определены условия идентификации точек, потенциально опасных по отношению к неисправностям типа «замыкание». На примере однотактного матричного умножителя показано значительное снижение контролепригодности при расширении класса неисправностей от константных к неисправностям типа «замыкание».

Ключевые слова: *система критического применения, цифровой компонент, управляемость, наблюдаемость, контролепригодность, потенциально опасные точки, неисправность типа «замыкание».*

Введение

С развитием высоких технологий расширяется круг объектов повышенного риска, к которым относятся тепловые, атомные и гидроэлектростанции в энергетике, скоростной наземный и воздушный транспорт, оборонные и космические системы. Безопасность таких объектов представляет особую проблему, решение которой невозможно без использования современных информационных компьютерных технологий.

Для обеспечения функциональной безопасности объектов повышенного риска используются информационные управляющие системы (ИУС) критического применения, которые строятся в соответствии с компонентным подходом [1].

Высокие требования, предъявляемые к функциональной безопасности ИУС критического применения, наследуются их цифровыми компонентами. Для выполнения этих требований цифровые компоненты разрабатываются с использованием отказоустойчивых решений, среди которых можно выделить различные виды резервирования, а также многоверсионные технологии [2].

Вместе с тем, одни только отказоустойчивые решения не гарантируют функциональную безопасность ИУС критического применения и их цифровых компонентов. Причиной является двухрежимность ИУС критического применения, которые проектируются для работы в нормальном и аварийном режимах. Двухрежимные ИУС создаются для решения проблем в аварийном режиме, а основную часть времени они функционируют в нормальном режиме. Цифровые компоненты ИУС, часто являющиеся однотактными устройствами, работают в нормальном и аварийном режимах на разных множествах входных слов. Это создает условия для накопления скрытых неисправностей в нормальном режиме. Причем за длительный период нормального режима может накопиться значительно большее количество неисправностей, чем то, которое парируется введенными в цифровые компоненты средствами обеспечения отказоустойчивости. Поэтому наряду с поддержкой отказоустойчивости цифровых компонентов необходимо также заботиться об их контролепригодности, что снизит риски скрытых отказов.

Контролепригодность традиционно рассматривается в теории тестового диагностирования, которая утверждает, что избыточные цифровые схемы являются неконтролепригодными [3]. Отказоустойчивые решения обладают высоким уровнем избыточности, а работа цифровых компонентов в отдельных режимах на ограниченных множествах входных слов делает избыточность цифровых схем еще выше.

Оценка цифровых компонентов с использованием их программных моделей подтверждает низкую контролепригодность, которая для однотактных цифровых компараторов не превышает 46% [4]. Однотактный матричный умножитель повышает контролепригодность до 100% при использовании не менее 39% от множества входных слов [5].

Следует отметить, что контролепригодность до сих пор анализировалась для множества константных неисправностей. Вместе с тем, в ряде работ обосновывается в качестве наиболее вероятной неисправность типа «замыкание», возникающая между двумя точками при пробое слоев микросхемы [6].

Поэтому в данной работе исследуется контролепригодность цифровых компонентов систем критического применения по отношению к неисправностям типа «замыкание».

В разделе 1 анализируются особенности потенциально опасных точек с позиции снижения отказоустойчивости цифровых компонентов. В разделе 2 определяется условие, идентифицирующее точки, потенциально опасные по отношению к неисправности типа «замыкание». В разделе 3 оценивается контролепригодность цифровых компонентов на примере однотактного матричного умножителя.

1. Особенности потенциально опасных точек цифровых компонентов

В тестовом диагностировании контролепригодность цифровых устройств оценивается с использованием понятий управляемости и наблюдаемости, имеющих вероятностный характер. Контролепригодность определенной точки цифровой схемы вычисляется как произведение управляемости на наблюдаемость [7]. В рабочем диагностировании контролепригодность цифровых устройств полностью определяется наблюдаемостью [8].

Противостояние снижению отказоустойчивости цифровых компонентов требует особого рассмотрения контролепригодности, которая должна учитывать не только условия рабочего диагностирования, но и двухрежимность систем критического применения. Точки схемы, в которых неисправности могут снизить отказоустойчивость цифрового компонента в аварийном режиме, в общем случае, не являются неконтролепригодными. Поэтому их целесообразно отличить от неконтролепригодных, называя потенциально опасными.

В идентификации потенциально опасных точек по отношению к неисправности типа «замыкание» могут быть использованы определения, введенные для анализа константных неисправностей цифрового компонента [9].

Точка схемы называется частично-управляемой: 0-управляемой или 1-управляемой, если на множестве входных слов принимает только значение «0» или «1», соответственно. Если принимаются оба значения, то точка называется управляемой.

Точка схемы называется частично-наблюдаемой: 0-наблюдаемой или 1-наблюдаемой, если на множестве входных слов активируется путь от этой точки только при ее значении «0» или «1», соответственно. Если принимаются оба значения, то точка называется наблюдаемой, а в противном случае ненаблюдаемой. Путь активируется при передаче изменения значения точки в контрольную точку схемы.

Управляемость точки схемы принимает три значения: 1, 2 и 3 соответственно для 1-управляемой, 0-управляемой и управляемой точки, а наблюдаемость – четыре значения: 0, 1, 2 и 3 соответственно для ненаблюдаемой, 1-наблюдаемой, 0-наблюдаемой и наблюдаемой точки.

В нормальном и аварийном режимах управляемость С и наблюдаемость О принимают значения C_N, O_N и C_E, O_E, соответственно.

Потенциально опасная точка возникает при совпадении двух условий:

– в этой точке схемы может накопиться скрытая неисправность в нормальном режиме;

– накопившаяся неисправность может проявиться в аварийном режиме.

2. Идентификация потенциально опасных точек

При анализе неисправности типа «замыкание» следует принять во внимание следующее:

– такая неисправность наиболее вероятна между точками, расположенными в локальной области;

– ошибка имеет место при различных значениях точек, одно их которых можно характеризовать как сильный ноль, а другое – как слабую единицу;

– ошибка возникает в точке со слабой единицей, которая переходит в сильный ноль.

Проанализируем выполнение первого условия.

Неисправность типа «замыкание» двух точек схемы остается скрытой на множестве входных слов нормального режима, если эти точки при правильном функционировании принимают одинаковые значения на каждом входном слове из указанного множества.

Кроме того, неисправность остается скрытой, если на входных словах, где точки различаются, точка, принимающая при правильном функционировании слабую единицу, не оказывает влияния на контрольные точки схемы, т.е. является ненаблюдаемой.

Таким образом, алгоритм по выявлению точек, удовлетворяющих первому условию, включает в себя следующие действия:

– определение пар точек локальной области;

– нахождение входных слов нормального режима, на которых значения точек пары различаются;

– исключение пары точек, если точка со слабой единицей наблюдаема на рассматриваемом входном слове.

Проанализируем выполнение второго условия.

В аварийном режиме неисправность типа «замыкание» проявляет себя в случае наблюдаемого единичного значения точки, которое может измениться на значение сильного нуля второй точки пары. Для этого необходимо, чтобы эти точки принимали различные значения, и точка со слабой единицей была наблюдаемой.

Алгоритм по выявлению точек, удовлетворяющих второму условию, включает в себя следующие действия:

– определение пар точек локальной области;

– нахождение входных слов аварийного режима, на которых значения точек пар локальной области различаются;

– выбор пар точек, если точка со слабой единицей наблюдаема на рассматриваемом входном слове.

Пересечение множеств точек, удовлетворяющих первому и второму условию, определяет множество потенциально опасных точек.

С некоторыми упрощениями неисправность типа «замыкание» двух точек может идентифицироваться с использованием приведенных определений, принимая во внимание проявление этой неисправности только в одной точке.

Неисправность типа «замыкание» является скрытой в нормальном режиме при нулевом значении точки, т.е. $C_N = 2$, поскольку значение сильного нуля сохраняется при любом значении второй точки пары. Кроме того, неисправность в точке будет скрытой, если эта точка наблюдается только в нуле или является ненаблюдаемой, т.е. в случаях $O_N = 2$ и $O_N = 0$. Следует отметить, что случай $C_N = 2$ приводится к случаям $O_N = 2$ и $O_N = 0$, поскольку 0-управляемая точка может быть или 0-наблюдаемой, или ненаблюдаемой.

Таким образом, выполнение первого условия может быть описано, анализируя отдельные точки, следующим образом:

$$(O_N = 0) \text{ or } (O_N = 2).$$

В этой записи не учитывается случай наблюдаемых пар точек локальной области, принимающих на всех словах нормального режима одинаковые значения. Такие пары не могут быть описаны в рамках анализа схемы по ее отдельным точкам.

Второе условие может быть описано с учетом возможности проявления неисправности при искажении точки в аварийном режиме: от значения слабой единицы к значению сильного нуля второй точки пары. Этот случай имеет место для точек, наблюдаемых в аварийном режиме в единичном значении, т.е. для 1-наблюдаемых и наблюдаемых точек, что описывается выражением

$$(O_E = 1) \text{ or } (O_E = 3).$$

Таким образом, потенциально опасные точки могут идентифицироваться по отношению к неисправности типа «замыкание» двух точек путем проверки следующей формулы:

$$((O_N = 0) \text{ or } (O_N = 2)) \text{ and } ((O_E = 1) \text{ or } (O_E = 3)).$$

Используя эту формулу, может быть оценена контролепригодность цифрового компонента по отношению к потенциально опасным точкам:

$$K = 1 – ND / NT,$$

где N_D – количество потенциально опасных точек;

N_T – общее количество точек схемы.

Принимая во внимание принятые упрощения, исключающие из рассмотрения некоторые потенциально опасные точки в нормальном режиме, контролепригодность оценивается с избытком, т.е. как верхняя граница.

3. Оценка контролепригодности умножителя по отношению к потенциально опасным точкам

Контролепригодность цифровых компонентов по отношению к потенциально опасным точкам может быть оценена на примере анализа однотактного матричного умножителя с использованием его программной модели.

Умножитель выполнен 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 [10].

Сомножители являются двоичными кодами нормализованных мантисс в диапазоне $2^{n-1} \div 2^n – 1$. Исследуемыми точками ОУ являются входы элементов И, а также входы и выходы полных сумматоров.

Локальными областями для возникновения неисправностей типа «замыкание» являются отдельные операционные элементы.

Оценка контролепригодности цифровых компонентов по отношению к потенциально опасным точкам выполняется для неисправностей типа «замыкание» в сравнении с константными неисправностями, которые анализируются по формуле [5]

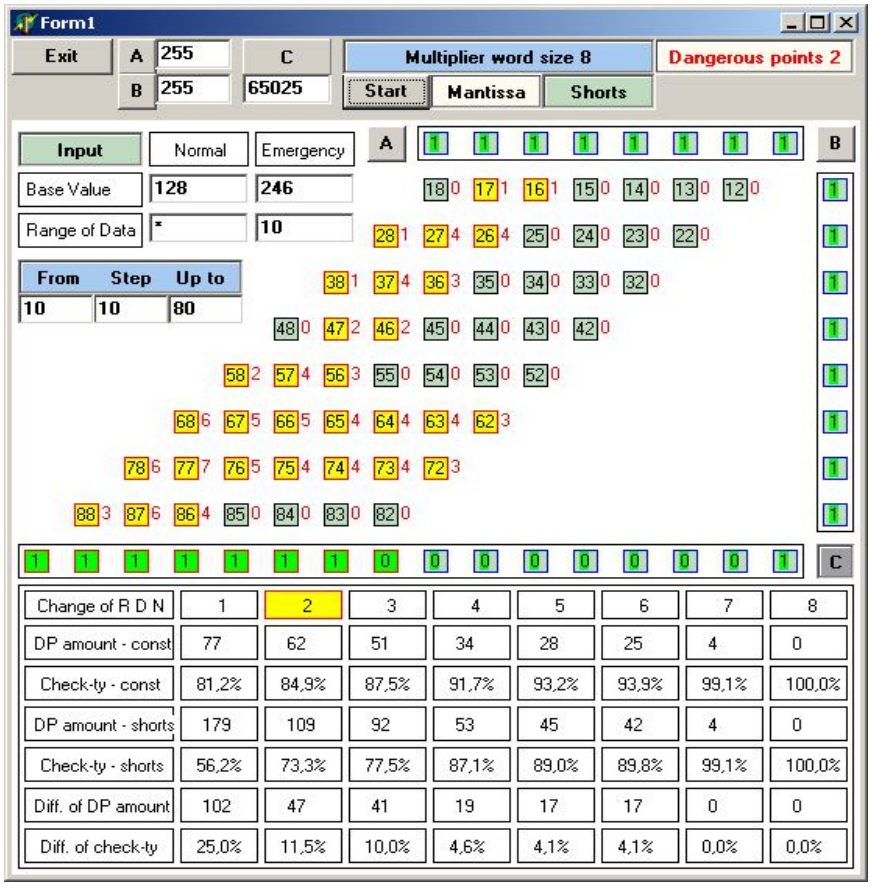
$$((C_N+C_E=3) \text{ or } (O_N+C_E=3) \text{ or } (O_N=0)) \text{ and } (O_E>0).$$

В программной модели задаются 4 параметра: базовое значение (Base Value) и диапазон изменения сомножителей (Range of Data) в нормальном (Normal) и аварийном (Emergency) режимах. Сомножители изменяются в одинаковом диапазоне с шагом 1, начиная с базового значения. В аварийном режиме со-

множители принимают значение порога, с которого начинается критическое состояние, и все следующие за ним значения. Параметр Range of Data в нормальном режиме задается переменным с указанием его начального значения (From), шага изменения (Step) и верхней границы (Up to), определяющей 8 различных значений параметра для проведения 8 экспериментов. В каждом из них вычисляется контролепригодность ОУ с указанием потенциально опасных точек схемы и их количества для неисправностей тип «замыкание» и константных неисправностей.

На рис. 1 показан вид основной панели программной модели после проведения экспериментов для разрядности мантисс n = 8.

В данной серии экспериментов заданы базовые значения 128 и 246 для нормального и аварийного режима, соответственно. Объем диапазона в нормальном режиме изменяется от значения 10 с шагом 10 до верхней границы 80. Таким образом, двоичный код мантисс сомножителей изменяется в нормальном режиме от 128 до 137 в первом эксперименте, до 147 во втором эксперименте и до 207 в последнем, восьмом. Таким образом, в первом эксперименте в нормальном режиме используется по десять значений сомножителей, образующих 100 входных слов, во втором эксперименте участвуют по 20 значений сомножителей и 400 входных слов, а в последнем эксперименте – по 80 значений сомножителей и 6400 входных слов, что составляет 39% от их общего количества. Объем 10 диапазона в аварийном режиме отсчитывается от порога на уровне базового значения 246.



Change of R D N	1	2	3	4	5	6	7	8
DP amount - const	77	62	51	34	28	25	4	0
Check-ty - const	81,2%	84,9%	87,5%	91,7%	93,2%	93,9%	99,1%	100,0%
DP amount - shorts	179	109	92	53	45	42	4	0
Check-ty - shorts	56,2%	73,3%	77,5%	87,1%	89,0%	89,8%	99,1%	100,0%
Diff. of DP amount	102	47	41	19	17	17	0	0
Diff. of check-ty	25,0%	11,5%	10,0%	4,6%	4,1%	4,1%	0,0%	0,0%

Рис. 1. Основная панель программной модели

Внизу панели приведена таблица, в которой показано количество потенциально опасных точек и значения контролепригодности, полученные по окончанию экспериментов для константных неисправностей (строки 1 и 2) и неисправностей типа «замыкание» (строки 3 и 4). В строках 5 и 6 показано количество потенциально опасных точек (в абсолютном и процентном выражении), по которым различаются их множества для двух рассмотренных типов неисправностей.

В строках 1 и 2 таблицы с увеличением количества входных слов количество точек, потенциально опасных по отношению к константным неисправностям, уменьшается от 77 до 0, а контролепригодность повышается от 81,2% до 100%.

В строках 3 и 5 таблицы количество точек, потенциально опасных по отношению к неисправностям типа «замыкание», уменьшается от 179 до 0, а контролепригодность повышается от 56,2% до 100%.

Строки 5 и 6 показывают, что точки, потенциально опасные по отношению к константным неисправностям, входят во множество точек, потенциально опасных по отношению к неисправностям типа «замыкание», составляя для первых экспериментов меньшую часть. При использовании в нормальном режиме 100 входных слов (эксперимент 1) множества точек, потенциально опасных по отношению к неисправностям типа «замыкание» и константным неисправностям содержат соответственно 179 и 77 элементов, т.е. различаются в 2,8 раз или на 102 точки. Это составляет 25% снижения контролепригодности, происходящего за счет расширения класса неисправностей от константных к неисправностям типа «замыкание».

С увеличением количества входных слов множества точек, потенциально опасных по отношению к неисправностям типа «замыкание» и константным неисправностям, уменьшаются и сближаются, совпадая в последних двух экспериментах (оперирующих с 30% и 39% от общего количества входных слов нормального режима).

Выше таблицы представлена матрица операционных элементов умножителя с просмотром количества содержащихся в них опасных точек для каждого эксперимента. Цветом выделяются операционные элементы, содержащие опасные точки (с указанием их количества). В данном случае по результатам проведения второго эксперимента выделено 30 операционных элементов из 56 (для неисправности типа «»замыкание» – «Shorts»). При необходимости структура операционного элемента может быть раскрыта с просмотром для каждой точки значений управляемости и наблюдаемости в штатном и критическом режимах. Опасные точки выделяются цветом.

Выводы

Построение функционально безопасных ИУС связано с необходимостью противостояния в аварийном режиме отказам, накопленным в нормальном режиме. Эта проблема возникает в силу особенностей ИУС критического применения, обуславливающих низкую контролепригодность цифровых компонентов вследствие двух основных факторов: значительной структурной избыточности отказоустойчивых решений, применяемых в компонентах, и ограниченных множеств входных слов, используемых в режимах работы ИУС.

Низкая контролепригодность цифровых компонентов имеет место не только в традиционной трактовке, но также и по отношению к потенциально опасным точкам схем, в которых могут накапливаться неисправности в нормальном режиме и проявляться в аварийном режиме, снижая уровень отказоустойчивости используемых решений.

Расширение класса неисправностей от константных неисправностей к неисправностям типа «замыкание» ухудшает контролепригодность цифровых компонентов ИУС критического применения. Снижение контролепригодности прогрессирует по мере сокращения множества входных слов, используемых в нормальном режиме.

Количество потенциально опасных точек увеличивается многократно.

В этих условиях количество накапливаемых в нормальном режиме скрытых неисправностей может многократно превосходить уровень отказоустойчивости цифровых компонентов, необходимый для обеспечения функциональной безопасности ИУС критического применения.

Следующие шаги в исследовании цифровых компонентов ИУС критического применения предполагается направить на повышение их контролепригодности.

Литература

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

2. Kharchenko, V. Multy-version Systems: Models, Reliability, Design Technologies / V.Kharchenko // 10th European Conference on Safety and Reliability. – Munich, Germany. – Vol. 1, 1999. – P. 73-77.

3. Щербаков, Н.С. Достоверность работы цифровых устройств / Н.С. Щербаков. – М.: Машиностроение, 1989. – 224 с.

4. Рабочее диагностирование безопасных информационно-управляющих систем / А.В. Дрозд, В.С. Харченко, С.Г. Антощук, Ю.В. Дрозд, М.А. Дрозд, Ю.Ю. Сулима / Под ред. А.В. Дрозда, В.С. Харченко. – Х.: Нац. аэрокосмический ун-т им. Н.Е.Жуковского «ХАИ», 2012. – 614 с.

5. Дрозд, А.В. Оценка контролепригодности цифровых компонентов встроенных систем критического применения / А.В. Дрозд, В.С. Харченко, С.Г. Антощук, М.А. Дрозд, Ю.Ю. Сулима // Радіоелектронні і комп'ютерні системи. – 2012. – № 6 (58). – С. 184 – 190.

6. Blyzniuk, M. Probabilistic analysis of CMOS physical defects in VLSI circuits for test coverage improvement / M. Blyzniuk, I. Kazymyra, W. Kuzmicz a.o. // Microelectronics Reliability. – 2001. – Vol. 41/12. – P. 2023 – 2040.

7. Беннетс, Р.Дж. Проектирование тестопригодных логических схем / Р.Дж. Беннетс. – М.: Радио и связь, 1995. – 180 с.

8. Суліма, Ю.Ю. Оцінка та метод підвищення контролепридатності цифрових компонентів в системах критичного застосування / Ю.Ю. Суліма, О.В. Дрозд // Холодильна техніка і технологія. – 2013. – № 1. – С. 77 – 79.

9. Drozd, A. Checkability of the digital components in safety-critical systems: problems and solutions / A. Drozd, V. Kharchenko, S. Antoshchuk,

J. Sulima, M. Drozd // Proc. IEEE East-West Design & Test Symposium. – Sevastopol, Ukraine. – 2011. – P. 411 – 416.

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

Поступила в редакцию 15.02.2013, рассмотрена на редколлегии 6.03.2013

Рецензент: д-р техн. наук, проф., декан факультета радиотехнических систем ЛА В.М. Илюшко, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков, Украина.

ОЦІНКА КОНТРОЛЕПРИДАТНОСТІ ЦИФРОВИХ КОМПОНЕНТІВ ВБУДОВАНИХ СИСТЕМ КРИТИЧЕСКОГО ЗАСТОСУВАННЯ ЩОДО НЕСПРАВНОСТЕЙ ТИПУ "ЗАМИКАННЯ"

О.В. Дрозд, В.С. Харченко, С.Г. Антощук, М.О. Дрозд

Стаття присвячена проблемі низької контролепридатності цифрових компонентів інформаційних управляючих систем критичного застосування, призначених для забезпечення безпеки об'єктів підвищеного ризику. Аналізуються потенційно небезпечні точки цифрових компонентів, у яких у нормальному режимі можуть накопичуватися скриті несправності, що знижують рівень відмовостійкості схем у аварійному режимі. Визначені умови ідентифікації точок, що є потенційно небезпечними відносно до несправностей типу «замикання». На прикладі однотактного матричного помножувача доведено значне зниження контролепридатності при розширенні класу несправностей від константних до несправностей типу «замикання».

Ключові слова: система критичного застосування, цифровий компонент, керованість, спостережуваність, контролепридатність, потенційно небезпечні точки, несправність типу «замикання».

CHECKABILITY OF SAFETY-CRITICAL SYSTEMS COMPONENTS IN RELATION TO FAULTS OF SHORTS TYPE

O.V. Drozd, V.S. Kharchenko, S.G. Antoshchuk, M.O. Drozd

The paper is devoted to the problems of low checkability of the digital components in Instrumentation & Control safety-critical systems ensuring the safety of objects with raised risk. Potentially dangerous points of the digital components in which in a normal mode can be accumulated latent faults reducing a level of circuit fault tolerance in an emergency mode of safety critical systems are considered. Conditions of identification of the points which are potentially dangerous concerning to faults of shorts type are determined. On example of simultaneous iterative array multiplier the significant decrease of checkability at the expanding of the fault set from constant faults up to faults of shorts type is shown.

Key words: Safety-critical system, digital component, controllability, observability, checkability, potentially dangerous points, faults of shorts type.

Дрозд Александр Валентинович – д-р техн. наук, проф., проф. кафедры компьютерных интеллектуальных систем и сетей Одесского национального политехнического университета, Одесса, Украина, e-mail: drozd@ukr.net.

Харченко Вячеслав Сергеевич – д-р техн. наук, проф., зав. кафедрой компьютерных систем и сетей Национального аэрокосмического университета им. Н.Е. Жуковского «ХАИ», Харьков, Украина, e-mail: V.Kharchenko@khai.edu.

Антощук Светлана Григорьевна – д-р техн. наук, проф., зав. кафедрой информационных систем, директор Института компьютерных систем Одесского национального политехнического университета, Одесса, Украина, e-mail: svetlana_onpu@mail.ru.

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