УДК 004.315

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

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

ОЦЕНКА КОНТРОЛЕПРИГОДНОСТИ ЦИФРОВЫХ КОМПОНЕНТОВ ВСТРОЕННЫХ СИСТЕМ КРИТИЧЕСКОГО ПРИМЕНЕНИЯ

Статья посвящена вопросам обеспечения достоверности результатов, вычисляемых цифровыми компонентами систем критического применения. Такие системы проектируются для работы в двух режимах: штатном и критическом. Высокие технологии, применяемые при их построении, снижают контролепригодность цифровых компонентов. Проведенные исследования показывают, как растет риск накопления в штатном режиме скрытых неисправностей, которые могут проявиться в критическом режиме и снизить достоверность результатов. Такой риск не устраняется применением отказоустойчивых решений.

Ключевые слова: *Система критического применения, цифровой компонент, штатный и критический режимы, управляемость, наблюдаемость, контролепригодность, достоверность результатов.*

Введение

Компьютерные технологии занимают важное место в обеспечении безопасности объектов критического применения – электростанций, скоростного транспорта, оборонных и космических систем. Для решения проблемы безопасности этих объектов используются информационные управляющие системы, включая встроенные системы (ВС) критического применения [1]. ВС проектируются, используя компонентный подход, на библиотечных компонентах коммерческого и критического применения, включая компоненты собственной разработки [2].

В ответственных случаях функциональность цифровых компонентов обеспечивается путем использования отказоустойчивых технологий, основанных на применении корректирующих кодов, различных видов резервирования, мажоритарных и многоверсионных структур [3].

В коммерческих приложениях отказоустойчивые цифровые компоненты демонстрируют высокий уровень безопасности, вычисляя, как правило, достоверные результаты. Однако ВС критического применения имеют особенности, которые делают отказоустойчивость недостаточной для обеспечения функциональности их компонентов. К таким особенностям следует отнести их проектирование для работы в двух режимах: штатном и критическом. Причем основное время работы ВС критического применения проходит в штатном режиме, а создаются они ради работы в критическом режиме [4].

Отказоустойчивость ВС критического применения обеспечивается за счет различных видов избыточности с использованием методов и средств рабочего диагностирования, учитывая оперативный характер его противостояния неисправностям и нацеленность на поддержание достоверности вычисляемых результатов.

Для двухрежимных ВС такая задача усложняется тем, что кроме контроля достоверности текущих результатов необходимо оценивать достоверность результатов, вычисляемых в критическом режиме, используя для этого возможности штатного режима. Оценивая эти возможности, следует отметить, что цифровые компоненты в штатном и критическом режимах работают на различных множествах входных данных. Это создает проблему ограниченной контролепригодности цифровых компонентов, которая состоит в риске накопления скрытых неисправностей в штатном режиме при работе на одних входных словах и их проявлении в аварийном режиме при поступлении новых слов. Таким образом, одной отказоустойчивости цифровых компонентов оказывается недостаточно для получения достоверных результатов в критическом режиме. Необходимо также учитывать контролепригодность цифровых компонентов.

Можно выделить два основных типа ВС критического применения, различаемые по выполнению основного объема вычислений над точными или приближенными данными.

Представителями первого типа могут служить ВС, используемые в системах безопасности атомных электростанций, где результаты измерений от датчиков оцифровываются и поступают на компараторы для сравнения с пороговыми значениями изме-

ряемых параметров. Далее обрабатываются результаты сравнения, которые являются точными данными [5]. Второй тип ВС критического применения используется в радарах, где на цифровых компонентах обрабатываются приближенные данные, полученные от датчиков. На выходах цифровых компонентов вычисляются приближенные результаты, сравниваемые далее с пороговыми значениями, например, в блоках амплитудной селекции для различения уровней шума и полезного сигнала [6].

Оба типа ВС страдают низкой контролепригодностью цифровых компонентов в силу ограниченного множества входных слов, поступающих в штатном режиме. Для первого типа ВС это множество ограничивается стабильностью уровней измеряемых параметров, а во втором случае – низким уровнем шума.

Следует отметить, что высокие технологии, используемые в ВС критического применения, способствуют повышению стабильности уровней измеряемых параметров и понижению уровня шума, что дополнительно ограничивает множество входных слов в штатном режиме и ухудшает контролепригодность цифровых компонентов.

В [7] предложен метод оценки контролепригодности цифровых компонентов путем анализа точек их схем на управляемость и наблюдаемость в штатном и критическом режимах. Используя этот метод, показано еще одно негативное влияние высоких технологий на контролепригодность цифровых компонентов. Оно заключается в использовании однотактных цифровых компонентов, для которых точки схемы могут изменять значение на входном слове не более одного раза.

Целью данной работы является анализ контролепригодности цифрового компонента в зависимости от характера входных слов, используемых в штатном и критическом режимах. В качестве цифрового компонента рассмотрен однотактный умножитель (ОУ) двоичных кодов, используемый в ВС первого или второго типа для обработки чисел с фиксируемой точкой или мантисс. Разработана программная модель ОУ, позволяющая оценивать его контролепригодность по указанному методу.

В разделе 1 излагаются основные положения метода, использованные при построении программной модели, а в разделе 2 – описываются ее возможности.

Раздел 3 содержит результаты моделирования ОУ двоичных кодов мантисс и их осмысление.

В заключении приведены выводы и сформулировано направление дальнейших исследований.

1. Оценка контролепригодности ОУ

Контролепригодность ОУ оценивается в терминах управляемости и наблюдаемости точек цифровой схемы, определяемых для штатного и критического режимов работы.

Точка схемы ОУ 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.

Таким образом, управляемость точки ОУ может принимать три значения, в качестве которых используются номера 1, 2 и 3 соответственно для 1-управляемой, 0-управляемой и управляемой точки.

Такая нумерация использована для накопительной оценки точки как управляемой, если ею проявлены признаки и 0-управляемой и 1-управляемой точки.

Точка схемы ОУ 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. Такими точками являются разряды вычисляемого результата, подключаемые к схемам контроля при рабочем диагностировании ОУ.

Наблюдаемость точки ОУ может принимать четыре значения, в качестве которых используются номера 0, 1, 2 и 3 соответственно для ненаблюдаемой, 1-наблюдаемой, 0-наблюдаемой и наблюдаемой точки.

Для оценки контролепригодности цифрового компонента введено понятие опасной точки, для которой выполняется два условия: существует риск накопления скрытой неисправности в штатном режиме и допустимо ее проявление в критическом режиме.

Первое условие выполняется в штатном режиме в двух случаях: если точка является частично управляемой, и значение в точке совпадает со значением, диктуемым константной неисправностью, а также, если точка является ненаблюдаемой.

Второе условие выполняется в критическом режиме также в двух случаях: если точка является наблюдаемой и неуправляемой и ее значение, как неуправляемой точки, отлично от значения, диктуемого неисправностью, а, кроме того, если точка является и управляемой и наблюдаемой.

Описанные условия позволяют находить опасные точки ОУ, анализируя на истинность следующую формулу [7]:

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

где C_N и O_N – управляемость и наблюдаемость точки в штатном режиме;

C_E и O_E – управляемость и наблюдаемость точки в критическом режиме.

Контролепригодность ОУ оценивается по следующей формуле:

$$C = 1 - N_E / N_T,$$

где N_E – количество опасных точек;

N_T – общее количество точек схемы.

2. Умножитель и его модель

Рассматривается ОУ, выполненный 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 [8].

Сомножителями являются двоичные коды 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.

Для оценки контролепригодности ОУ построена его программная модель, в которой можно задать 4 параметра: базовое значение (Base Value) и диапазон изменения сомножителей (Range of Data) в штатном (Normal) и критическом (Emergency) режимах. Сомножители изменяются в одинаковом диапазоне с шагом 1, начиная с базового значения.

В критическом режиме сомножители принимают значение порога, с которого начинается аварийное состояние. Диапазон изменения сомножителей в критическом режиме позволяет анализировать работу ОУ на «размытом» пороге, который принимает несколько значений подряд. Точка является опасной, в том и только том случае, если оценена таковой на всех этих значениях.

Один из задаваемых параметров можно сделать переменным, указывая его начальное значение (From), шаг изменения (Step) и верхнюю границу (Up to). Если верхняя граница не превышена, то задается 8 различных значений параметра и проводится 8 экспериментов. В каждом из них вычисляется контролепригодность ОУ с указанием опасных точек схемы и их количества.

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

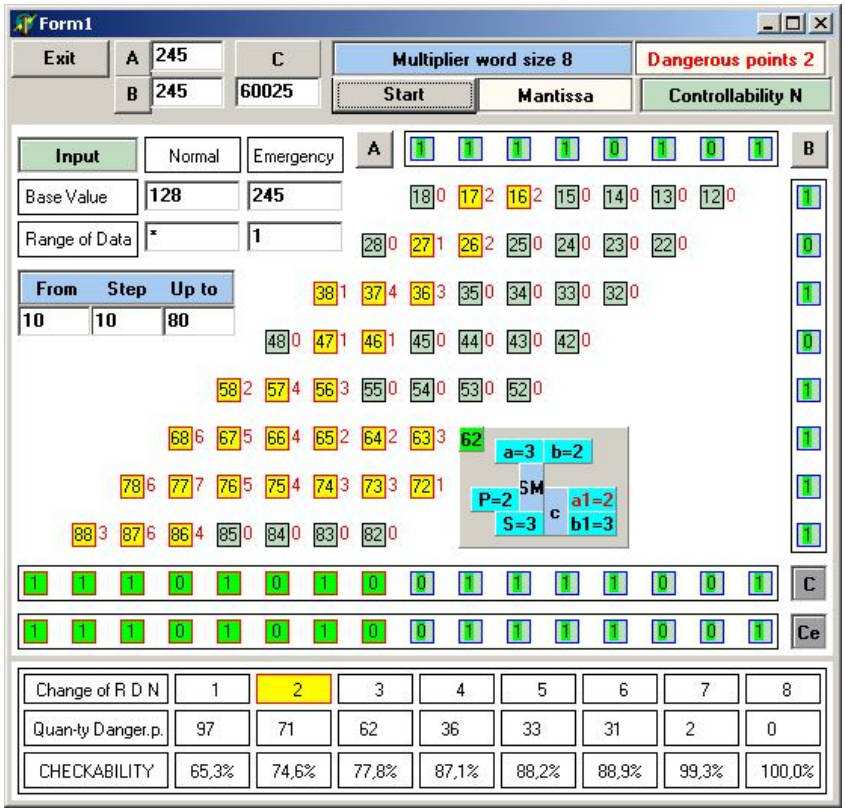

Рис. 1. Основная панель программной модели ОУ для разрядности n = 8

В данном эксперименте заданы базовые значения 128 и 245 для штатного и критического режима, соответственно. Объем диапазона в штатном режиме назначен переменным параметром, который изменяется от значения 10 с шагом 10 до верхней границы 80. Таким образом, двоичный код мантисс сомножителей изменяется в штатном режиме от 128 до 137 в первом эксперименте, до 147 во втором эксперименте и до 207 в последнем восьмом. Объем 1 диапазона в критическом режиме определяет порог на уровне базового значения 245.

Внизу панели показано количество опасных точек и значения контролепригодности, полученные по окончанию экспериментов. Они изменяются от 121 до 0 и от 70,4% до 100%, соответственно.

Показывается также матрица операционных элементов ОУ с просмотром количества содержащихся в них опасных точек для каждого эксперимента. Цветом выделяются операционные элементы, содержащие опасные точки. В данном случае выделено 29 операционных элементов из 56 по результатам проведения второго эксперимента. 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.

3. Результаты моделирования

Проведенное моделирование имело своей целью оценить уровень контролепригодности цифровых компонентов ВС критического применения и влияние на него ограниченности входных данных в штатном и критическом режимах.

Результаты первой серии экспериментов, показанных на рис. 1, приведены в табл. 1.

Таблица 1

Изменение диапазона сомножителей
в штатном режиме для разрядности n = 8

НЭ	1	2	3	4	5	6	7	8
ОД	10	20	30	40	50	60	70	80
ОТ	97	71	62	36	33	31	2	0
К,%	65,3	74,6	77,8	87,1	88,2	88,9	99,3	100

В строках таблицы показаны номера экспериментов (НЭ), объемы диапазона изменения сомножителей в штатном режиме (ОД), количество опасных точек (ОТ) и контролепригодность ОУ (К), выраженная в процентах.

Результаты моделирования показывают, что 100% контролепригодности ОУ достигается лишь при объеме диапазона в 80 значений сомножителей, что составляет 80^2 входных слов из 128^2 возможных, т.е. 39% от общего количества входных слов.

При уровне шума, обеспечивающем объем диапазона в 10 значений сомножителей и, соответственно 100 входных слов, ОУ содержит 97 опасных точек, которым соответствует контролепригодность 65,3%.

В табл. 2 приведены результаты моделирования для тех же входных данных, порога 4085 и n = 12.

Таблица 2

Изменение диапазона сомножителей
в штатном режиме для разрядности n = 12

НЭ	1	2	3	4	5	6	7	8
ОД	10	20	30	40	50	60	70	80
ОТ	374	336	333	282	277	277	220	219
К,%	43,3	49,1	49,5	57,3	58,0	58,0	66,7	66,8

Результаты моделирования показывают значительное увеличение количества опасных точек и снижение контролепригодности ОУ до 43,3% и 66,8% соответственно при объеме диапазона 10 и 80. Это можно объяснить уменьшением процента входных слов с 39% до 0,15%, т.е. в 256 раз.

Увеличение разрядности мантиссы соответствует повышению точности вычислений. Однако вместе с точностью растет также уровень шума, увеличивающий объем диапазона в штатном режиме.

В табл. 3 показаны результаты моделирования при сохранении 39% входных слов в восьмом эксперименте для порога 4085 и n = 12.

Таблица 3

Изменение увеличенного диапазона сомножителей
в штатном режиме для разрядности n = 12

НЭ	1	2	3	4	5	6	7	8
ОД	160	320	480	640	800	960	1120	1280
ОТ	165	109	102	56	53	51	2	0
К,%	75,0	83,5	84,6	91,6	92,0	92,3	99,7	100

Для этого диапазон увеличивается от начального значения 160 с шагом 160 до 1280 значений сомножителей. Результаты моделирования подтверждают достижение 100% контролепригодности при использовании 39% входных слов.

Следующие эксперименты направлены на исследование влияния на контролепригодность ОУ сближения уровня шума и уровня порога.

Такое сближение может быть выполнено двумя способами: повышением базового значения в штатном режиме и снижением базового значения в критическом режиме.

В табл. 4 показаны результаты моделирования при повышении базового значения в штатном режиме работы ОУ с разрядностью n = 12.

Таблица 4

Изменение базового значения сомножителей в штатном режиме для n = 12

НЭ	1	2	3	4	5	6	7	8
БЗ	2048	2266	2484	2702	2920	3138	3356	3574
ОТ	165	108	57	55	4	103	54	1
К,%	75,0	83,7	91,4	91,7	99,4	84,4	91,9	99,9

Результаты моделирования показывают повышение контролепригодности ОУ как общую тенденцию с возможными отклонениями. Пятый эксперимент показывает резкое повышение контролепригодности ОУ, которое не получает развития в шестом эксперименте.

Дополнительные исследования показали, что контролепригодность на уровне 99,4% (всего 4 опасные точки), показанная в пятом эксперименте сохраняется на протяжении 155 базовых значений: с 2916 по 3071. Причем, для базового значения 2916 уменьшение объема диапазона до 157 ÷ 159 и далее до 29 ÷ 156 и 13 ÷ 28 значений сомножителей снижает контролепригодность ОУ соответственно до 99,3%, 90,3% ÷ 91,6% и 83,1% ÷ 83,8%.

Для базового значения 3071 уменьшение объема диапазона до пяти значений сомножителей сохраняет контролепригодность ОУ на уровне 99,4%, На трех подряд базовых значениях 3070 ÷ 3072 и объеме диапазона штатного режима в 5 значений сомножителей, контролепригодность ОУ вычисляется на уровне 97,6%, 99,4 и 47,5%, соответственно.

Приведенные данные показывают на существенное влияние, которое оказывает выбор базового значения на контролепригодность ОУ. Резкие, внешне непредсказуемые скачки контролепригодности при минимальных смещениях базового значения сомножителей в штатном режиме указывают на целесообразность подбора базового значения путем моделирования работы ОУ.

В табл. 5 показаны результаты моделирования при снижении базового, т.е. порогового значения (ПЗ) в штатном режиме работы ОУ для n = 12.

Таблица 5

Изменение порогового значения сомножителей в штатном режиме для n = 12

НЭ	1	2	3	4	5	6	7	8
ПЗ	4085	3867	3649	3431	3213	2995	2777	2559
ОТ	165	136	74	97	47	98	52	60
К,%	75,0	79,4	88,8	85,3	92,9	85,2	92,2	90,9

Результаты моделирования также показывают повышение контролепригодности ОУ как общую тенденцию. Контролепригодность повышается волнами. Прослеживается первая волна в трех первых экспериментах, затем две волны по двум экспериментам и начало новой волны в восьмом эксперименте.

Следует отметить, что разность уровней порога и шума определяется разрядностью мантисс сомножителей: при большей разрядности разность увеличивается, а при меньшей – уменьшается, что имеет место при сохранении диапазона изменения сомножителей в штатном режиме работы ОУ. Следовательно, повышение точности обрабатываемых данных способствует понижению контролепригодности цифровых компонентов.

Таким образом, еще одно достижение высоких технологий – высокая точность обрабатываемых данных – препятствует обеспечению высокой контролепригодности цифровых компонентов в ВС критического применения.

Можно предположить, что базовое значение входных данных и их точность в значительной мере определяют уровень порога. Вместе с тем, можно допустить установку порога не в одной точке, а в некотором диапазоне значений, каждое из которых указывает на смену штатного режима на критический. Тогда возникает понятие «размытого» порога.

Возможны две противоположные оценки контролепригодности по отношению к «размытому» порогу». Уровень, сравниваемый с порогом, как правило, имеет ограниченную скорость изменения, определяемую инерционностью датчиков, аналогово-цифровых преобразователей и самого объекта управления.

Максимальный шаг изменения определяет минимальный диапазон значений «размытого» порога. Для выявления критического режима на этом рубеже точка схемы должна быть неопасной на каждом значении «размытого» порога» (логика И).

Если максимальный шаг изменения принимает минимальное значение, т.е. равен единице, то минимальный диапазон значений «размытого» порога также равен единице. Расширение диапазона порога до большего значения предъявляет к точке схемы противоположное требование: точка должна быть неопасной хотя бы на одном значении «размытого» порога» (логика ИЛИ).

В программной модели заложена логика ИЛИ, не уменьшающая контролепригодность ОУ при использовании «размытого» порога».

В табл. 6 показаны результаты моделирования при изменении диапазона значений порога (ДП) в критическом режиме работы ОУ от 1 до 8 для базового значения 2048, диапазона 160 изменения сомножителей в штатном режиме, значения порога 4085 и разрядности n = 12.

Таблица 6

Изменение диапазона значений порога в критическом режиме для n = 12

НЭ	1	2	3	4	5	6	7	8
ДП	1	2	3	4	5	6	7	8
ОТ	165	156	156	143	141	141	141	141
К,%	75,0	76,4	76,4	78,4	78,7	78,7	78,7	78,7

Результаты моделирования показывают, и это подтверждают другие эксперименты, что использование «размытого» порога» с логикой ИЛИ оценки неопасной точки повышает контролепригодность ОУ только для ее малых значений и практически не оказывает влияния на уровень 78,7% и выше.

Выводы

Традиционно, основным требованием, предъявляемым к цифровым компонентам ВС критического применения в части функциональной безопасности, является обеспечение их отказоустойчивости с использованием, как правило, мажоритарных структур и многоверсионных технологий.

Однако особенности ВС критического применения как двухрежимных систем, проектирующихся для работы в штатном и критическом режимах, обращают внимание также на контролепригодность цифровых компонентов как свойство, позволяющее противостоять риску накопления в штатном режиме скрытых неисправностей, которые могут проявиться в критическом режиме.

Такой риск не устраняется применением отказоустойчивых решений, поскольку ему подвержены все каналы мажоритарной или многоверсионной структуры на протяжении, как правило, длительного времени.

Именно благодаря достаточной контролепригодности цифровых компонентов рабочее диагностирование может в составе отказоустойчивых решений обеспечить достоверность результатов, вычисляемых в критическом режиме, используя возможности штатного режима. Поэтому важно оценить уровень контролепригодности цифровых компонентов ВС критического применения и влияющие на нее факторы. Это было сделано на примере ОУ двоичных кодов нормализованных мантисс с использованием разработанной для него программной модели.

Результаты моделирования показали, что 100% контролепригодности достигается при поступлении на ОУ 39% входных слов, что многократно превышает диапазон входных слов цифрового компонента в штатном режиме, когда он работает в диапазоне значений шума.

Повышение точности вычислений путем увеличения разрядности мантиссы сохраняет требование 39% входных слов для достижения 100% контролепригодности ОУ. Если повышение точности вычислений соответственно увеличивает диапазон значений шума, то контролепригодность ОУ не уменьшается.

Сближение уровней шума и порога, выполняемое как повышением базового значения сомножителей в штатном режиме, так и снижением порога, выявило общую тенденцию повышения контролепригодности ОУ. Вместе с тем, эксперименты показали на существенное влияние, которое оказывает базовое значение сомножителей в штатном режиме на контролепригодность ОУ, значительно повышая или снижая ее в нарушение общей тенденции.

При этом снижение контролепригодности происходит при сохранении диапазона значений шума и, по существу, является следствием повышения точности обрабатываемых данных.

Важно выявить переход цифрового компонента из штатного режима в критический режим в начале этого процесса, что требует учета максимального шага изменения величины, сравниваемой с порогом. Это изменение не должно превышать диапазон значений порога, на каждом из которых точки схемы не должны быть опасными. Это повышает требования к контролепригодности ОУ. «Размытый» порог при шаге 1 может также повышать контролепригодность ОУ, но только для ее малых значений (ниже 80%).

Следует отметить, что контролепригодность цифровых компонентов снижается при ограниченном диапазоне входных слов в штатном режиме, однотактном использовании точек схемы для вычисления результатов и значительном удалении порога от уровня шума, что является проявлением не всегда обоснованного применения высоких технологий. По-видимому, эффективные решения лежат на пути сбалансированного использования ресурсов стабильности входных данных, схемного параллелизма и точности обрабатываемых данных.

Дальнейшие исследования контролепригодности цифровых компонентов должны показать пути ее существенного повышения для ВС критического применения первого и второго типа. Основным направлением может стать поиск схемных решений по разработке цифровых компонентов.

Литература

1. Yastrebenetsky, M.A. (edit.). NPP I&Cs: Problems of Safety [Text] / M.A. Yastrebenetsky. – Ukraine, Kyiv: Technika, 2004. – 324 p.

2. Kharchenko, V. Multy-version Systems: Models, Reliability, Design Technologies [Text] / V.Kharchenko // 10th European Conference on Safety

and Reliability. – Munich, Germany. –1999. – Vol. 1. – P. 73 – 77.

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

4. Checkability of safety-critical I&Cc system components in normal and emergency modes [Text] / A. Drozd, V. Kharchenko, S. Antoshchuk, M. Drozd // Journal of Information, Control and Management Systems. – 2011. – Vol. 1, No.1. – P. 87 – 94.

5. Component-based safety-oriented on-line testing of digital systems [Text] / A. Drozd, V. Kharchenko, A. Siora, V. Sklyar // IEEE East-West Design & Test Symposium. – Peterburg, Russia. – Sept. 17-20, 2010. – P. 135 – 140.

6. Sait "Popmech.ru" [Electronic resource]. – Available to: http://www.popmech.ru/article/4954-vosmoe-chudo-sveta. - 15.01. 2012 y.

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 Sympo-sium. – Sevastopol, Ukraine. – 9-12 Sept., 2011. – P. 411 – 416.

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

Поступила в редакцию 23.02.2012

Рецензент: д-р техн. наук, проф. В.А. Твердохлебов, Институт проблем точной механики и управления РАН, Саратов, Россия.

ОЦІНКА КОНТРОЛЕПРИДАТНОСТІ ЦИФРОВИХ КОМПОНЕНТІВ ВБУДОВАНИХ СИСТЕМ КРИТИЧНОГО ЗАСТОСУВАННЯ

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

Стаття присвячена питанням забезпечення достовірності результатів, що обчислюються цифровими компонентами систем критичного застосування. Такі системи проектуються для роботи у двох режимах: штатному і критичному. Високі технології, що використовуються при їх побудові, зменшують контролепридатність цифрових компонентів. Проведені дослідження показують, як зростає ризик накопичення у штатному режимі прихованих несправностей, які можуть проявитися в критичному режимі та зменшити достовірність результатів. Такий ризик не усувається застосуванням відмовостійких рішень.

Ключові слова: Система критичного застосування, цифровий компонент, штатний і критичний режими, керованість, спостерігаємість, контролепридатність, достовірність результатів.

ASSESSMENT IN CHECKABILITY OF SAFETY-CRITICAL EMBEDDED SYSTEMS COMPONENTS

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

The paper is devoted to the problems of trustworthiness assurance for the results calculated by digital components of safety critical systems. Such systems are developed to operate in two modes: normal and emergency. The high technologies used at their designing reduce checkability of the digital components. The executed researches show growth of risk of accumulation in a normal mode of the latent faults which can appear in an emergency mode and decrease trustworthiness of results. This risk is not eliminated by the use of fault-tolerant solutions.

Key words: system of critical application, digital component, normal and emergency modes, controllability, observability, checkability, trustworthiness of results.

Дрозд Александр Валентинович – д-р техн. наук, проф., проф. кафедры компьютерных интеллектуальных систем и сетей Одесского национального политехнического университета, Одесса, Украина, 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, 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, svetlana_onpu@mail.ru.

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

Сулима Юлиан Юрьевич – аспирант кафедры компьютерных интеллектуальных систем и сетей Одесского национального политехнического университета, Одесса, Украина, mr_lemur@mail.ru.