Космічна наука і технологія. 1997. Т 3. № 5/6. С. 109—119.

УДК 681.3.014

Выбор технологии проектирования и базовых архитектур дефектоустойчивых цифровых управляющих и вычислительных систем реального времени

В. С. Харченко

Харківський військовий університет

Надійшла до редакції 28.05.96

Систематизуються технології проектування ЦКОС реального часу (РЧ) із застосуванням принципу багатоальтернативності. Пропонується векторна характеристика технологій проектування багатоальтернативних дефектостійких ЦКОС і класифікуються їх базові архітектури. Аналізуються оцінки надійності та вартості ЦКОС, які проектуються за різними технологіями. Дається загальна методика вибору технологій проектування та архітектур ЦКОС РЧ з урахуванням вимог до надійності та обмежень на габарито-масові та енергетичні характеристики.

ВВЕДЕНИЕ

Все более существенным фактором, влияющим на надежность цифровых управляющих и вычислительных систем (ЦУВС) сложных технических комплексов (летательных аппаратов, транспортных коммуникаций, энергетических систем и т. д.), работающих в реальном масштабе времени, становятся их программные средства. С одной стороны, они реализуют алгоритмы диагностирования и реконфигурации аппаратных средств при отказах, обусловленных их физическими дефектами. С другой стороны, дефекты проектирования программных средств, не выявленные при отладке и испытаниях, часто являются причиной неправильного функционирования систем. Ее весомость имеет устойчивую тенденцию нарастания, обусловливая в некоторых случаях до 50 % отказов ЦУВС (Avizienis, Laprie, 1986). Это вызвано, прежде всего, усложнением алгоритмов функционирования ЦУВС, а также ужесточением требований к срокам разработки программных средств, что исключает возможность их проверки на всем множестве исходных данных. «Традиционные» избыточные архитектуры ЦУВС не обладают свойством устойчивости к дефектам проектирования программных средств вследствие их тиражирования в однотипных резервных каналах (Кривоносов и др., 1995). Поэтому актуальной является задача разработки таких архитектур ЦУВС реального времени, которые были бы устойчивы к дефектам как аппаратных, так и программных средств, т. е. обладали бы свойством общей дефектоустойчивости (Харченко, Благодарный, 1994). Использование термина «дефектоустойчивость» представляется в этом случае более корректным, чем термина «отказоустойчивость», учитывая то обстоятельство, что в общепринятом смысле программные средства отказать не могут. Такое свойство дефектоустойчивости может быть обеспечено на основе концепции многоальтернативных (многоверсионных) систем (Харченко, Литвиненко, 1993), развивающей принцип N-версион-

ного программирования (Головкин, 1986) и предполагающей построение основных и резервных компонентов ЦУВС с использованием различных (альтернативных) программных или программно-аппаратных версий (АВ). Многоальтернативная ЦУВС $\widetilde{S}$ описывается (Харченко, 1992а) множествами входных (X), выходных (Z) и настроечных (U) сигналов, множеством выполняемых функций $\Phi = \{\varphi_i\}_{i=1}^{a}$, а также множествами версий их выполнения $V = = \{V_i = \{V_{ij}\}_{j=1}^{e_i}\}_{i=1}^{a}$ и законов (правил) $\Psi = \{\psi_i\}_{i=1}^{a}$ обработки результатов реализации этих версий $Z(V_{ij})$, т. е.

$$Z(V_i) = \Psi_i[Z(V_{i1}), ..., Z(V_{ie_i})].$$

Результаты разработки и исследования базовых архитектур двух-, трех- и четырехальтернативных ЦУВС с параллельным и последовательным выполнением версий изложены в работах Харченко, Паршина (1991) и Харченко (1992б).

Цель данной статьи — систематизация архитектур и технологий проектирования многоальтернативных ЦУВС и разработка методики их выбора.

СИСТЕМАТИЗАЦИЯ ТЕХНОЛОГИЙ СОЗДАНИЯ ЦИФРОВЫХ УПРАВЛЯЮЩИХ И ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ ПРИНЦИПА МНОГОАЛЬТЕРНАТИВНОСТИ

Область использования принципа многоальтернативности в общем случае может распространяться на этапы разработки технического задания ($f = 0$), разработки ($f = 1$), отладки ($f = 2$), производства ($f = 3$), испытаний ($f = 4$) и эксплуатации ($f = 5$) ЦУВС. Реализация принципа на этапе $f = i$ предполагает, что он используется на всех предшествующих μ-х этапах ($i \in 2, ..., 5$, $\mu \in 1, ..., i - 1$). Каждый из этапов характеризуется числом используемых альтернативных версий (тривиальных, т. е. полностью идентичных и нетривиальных, т. е. использующих различные программные или программно-аппаратные средства) и вариантом выбора версии или версий, передаваемых на следующий этап.

Технологию создания TS_ν многоальтернативной системы $\widetilde{S}$ будем описывать векторной характеристикой:

$$TS_\nu = \left\{\langle e_\nu^{(f)}\rangle, \langle e_{\overline{\text{т}}\nu}^{(f)}\rangle, \xi_{s\nu}^{(f)}\right\}_{f=1}^{F}, \qquad (1)$$

где $e_\nu^{(f)}$ — общее число альтернативных версий (АВ), используемых на f-м этапе (F — число этапов); $e_{\overline{\text{т}}\nu}^{(f)}$ — число нетривиальных АВ, используемых на f-м этапе; $\xi_{s\nu}^{(f)} = \{\xi_{s_1\nu}^{(f)}, \xi_{s_2\nu}^{(f)}\}$ — операция формирования версий, используемых на $f + 1$-м этапе.

Операция $\xi_{s\nu}^{(f)}$ может реализоваться путем выбора одной или нескольких альтернативных версий, полученных на f-м этапе:

$$\xi_{s_1\nu}^{(f)} : V^{(f)} \to \Delta V_{\text{п}}^{(f)}, \quad \Delta V_{\text{п}}^{(f)} \subseteq V^{(f)}, \qquad (2)$$

либо путем формирования одной или нескольких модифицированных версий из АВ множества $V^{(f)}$:

$$\xi_{s_2\nu}^{(f)} : V^{(f)} \to \Delta V_{\text{п}}^{*(f)}. \qquad (3)$$

Таким образом, ν-я технология создания системы определяется кортежами числа альтернативных версий и операцией их формирования для передачи на следующий этап.

Множество технологий создания многоальтернативных систем

$$MTS = \left\{TS_\nu\right\}_{\nu=1}^{\text{n}_\text{т}\,s}$$

представлено на рис. 1, где $V_{\text{т}}^{(f)}$, $V_{\overline{\text{т}}}^{(f)}$ — множества тривиальных и нетривиальных версий на f-м этапе, $\rho_\nu^{(f)}$ — операция генерации нетривиальных АВ. Оно включает:

— технологии создания одноальтернативных и тривиальных многоальтернативных систем TS_{10} и TS_{11}, в которых не используются нетривиальные АВ, т. е.

$$TS_{11(0)} =$$

$$= \left\{\langle e_\nu^{(f)} = e_{\text{т}\nu}^{(f)}(1)\rangle, \langle e_{\overline{\text{т}}\nu}^{(f)} = 0\rangle, \xi_{s\nu}^{(f)} = \xi_{s_1\nu}^{(f)}\,(\Delta V_{\text{п}}^{(f)} = V^{(f)})\right\}_{f=1}^{F};$$

— технологии создания одноальтернативных и тривиальных многоальтернативных систем TS_{20} и TS_{21}, в которых нетривиальные АВ используются только на этапе отладки ($V_{\overline{\text{т}}}^{(1)} \neq \varnothing$, $V_{\overline{\text{т}}}^{(2)} \neq \varnothing$);

— технологии создания одноальтернативных и тривиальных многоальтернативных систем TS_{30} и TS_{31} , в которых принцип многоальтернативности реализуется на этапах $f \in 1, ..., 4$;

— технологию TS_4, которая предполагает распространение принципа многоальтернативности и на этап использования системы по назначению ($f = 5$).

Множество технологий MTS может быть расширено за счет детализации границ использования принципа многоальтернативности на этапе разработки ЦУВС, который включает этапы синтеза математической модели, алгоритмов, программных и аппаратных компонентов. В этом случае множество версий программных средств может формиро-

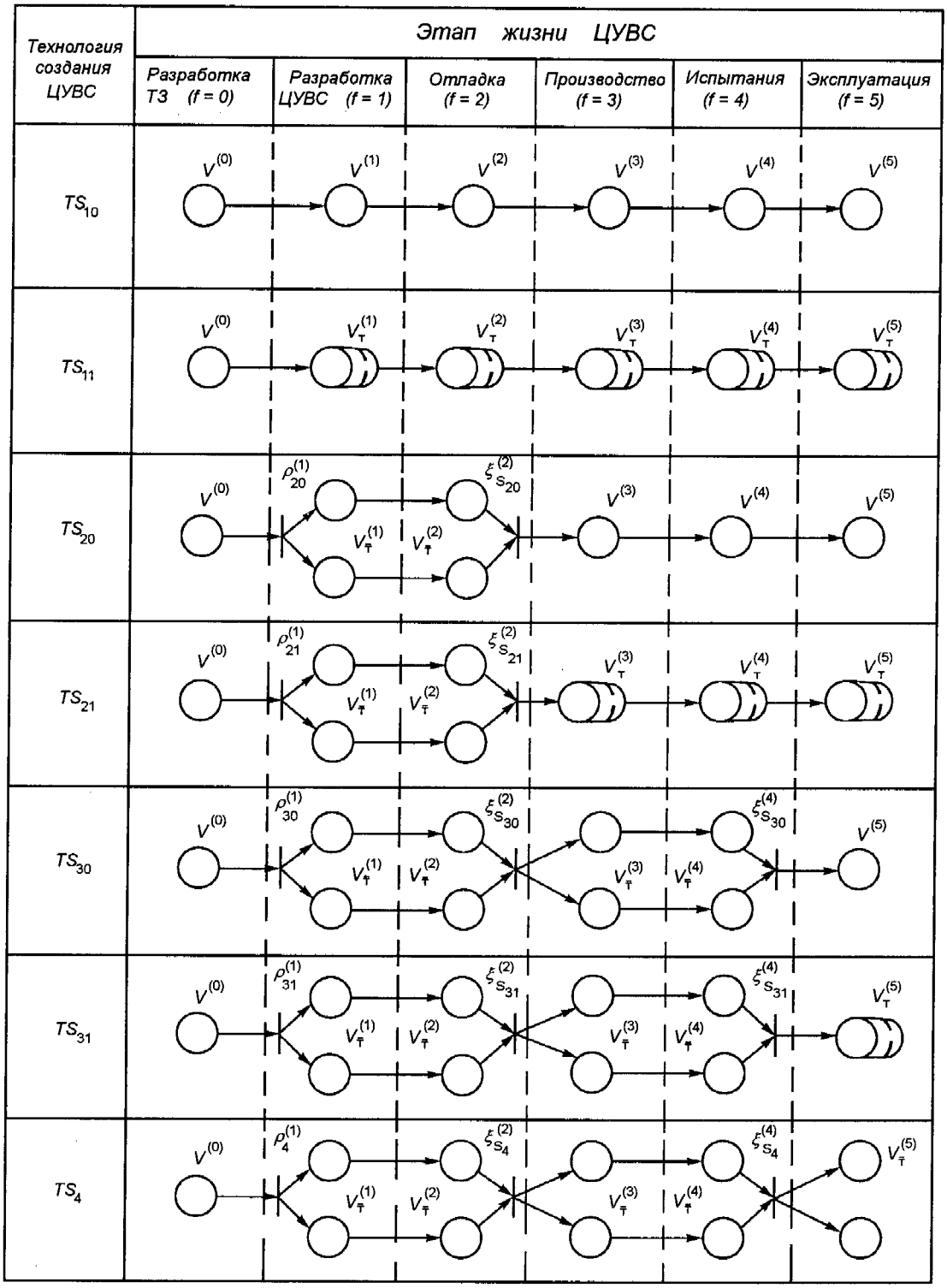

Рис. 1. Множество технологий создания многоальтернативных систем

ваться за счет использования различных субъектов разработки, тестирования и отладки языков программирования и т. д.

Каждая технология создания ЦУВС с использованием принципа многоальтернативности характеризуется суммарными затратами времени и стоимостью:

$$T_c(TS_\nu) = \sum_{f=1}^{F} \left(\max_{j \in 1,\ldots,e^{(f)}} T^{(f)}_{cv_j} + \Delta T^{(f)}_{cv} \right), \qquad (4)$$

$$C_c(TS_\nu) = \sum_{f=1}^{F} \left(e_{\overline{T}\nu} C^{(f)}_{c\overline{T}\nu} + e_{T\nu} C^{(f)}_{cT\nu} + \Delta C^{(f)}_{cv} \right), \qquad (5)$$

где $T^{(f)}_{cv_j}$ — продолжительность этапа f для технологии TS_ν по j-й нетривиальной АВ. Считаем, что эти версии на всех этапах реализуются параллельно;

$$T^{(f)}_{cv} = T(\xi^{(f)}_{sv}) + \tau^{(f)}_\nu,$$

причем $T(\xi^{(f)}_{sv})$ — продолжительность выполнения операции $\xi^{(f)}_{sv}$, а $\tau^{(f)}_\nu$ — временной параметр, связанный с параллельной реализацией нескольких нетривиальных АВ; $C^{(f)}_{c\overline{T}(T)\nu}$— стоимость создания нетривиальной (тривиальной) версии на f-м этапе для технологии TS_ν;

$$\Delta C^{(f)}_{cv} = C_c(\xi^{(f)}_{sv}) + \widetilde{C}^{(f)}_\nu,$$

причем $C_c(\xi^{(f)}_{sv})$ — стоимость реализации операции $\xi^{(f)}_{sv}$, $\widetilde{C}^{(f)}_\nu$— стоимостной параметр, связанный с параллельной реализацией нескольких нетривиальных АВ.

Величины $\tau^{(f)}_\nu$ и $\widetilde{C}^{(f)}_\nu$ в общем случае могут быть как положительны, так и отрицательны (например, при отладке нетривиальных АВ (Квирк, 1990)). Это зависит от требований, предъявляемых к надежности системы ($P_{\tilde{s}}$), сложности программных компонентов и числа версий.

Следовательно, в общем случае одному и тому же варианту создаваемой системы соответствуют несколько технологий $TS_\nu \in MTS$, отличающихся числом и номенклатурой альтернативных версий, генерируемых и анализируемых на этапе $f = i$ и передаваемых на очередной этап $f = i + 1$, $i \in 1,\ldots, F - 1$.

ОСОБЕННОСТИ ВЫБОРА АРХИТЕКТУР И ТЕХНОЛОГИЙ СОЗДАНИЯ ДЕФЕКТОУСТОЙЧИВЫХ ЦИФРОВЫХ УПРАВЛЯЮЩИХ И ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ

Процесс проектирования ЦУВС с заданным уровнем устойчивости к дефектам аппаратных и программных компонентов базируется на следующих исходных посылках.

1. Поскольку достижение теоретически возможного уровня надежности аппаратного компонента ограничивается допустимыми значениями габарито-массовых и энергетических характеристик (ГМЭХ), запасом естественной временной избыточности $\Delta\tau_{ЕИ}$, возможностью снижения качества функционирования ΔКФ, и т. д., то обеспечение требуемого уровня надежности (дефектоустойчивости) ЦУВС в целом может осуществляться за счет снижения остаточного уровня дефектов проектирования программного компонента и увеличения числа нетривиальных альтернативных версий. Другими словами, требования к надежности программного компонента определяются общими требованиями к надежности ЦУВС и достигаемыми надежностными характеристикам аппаратного компонента.

2. Специфика ряда ЦУВС рассматриваемого класса исключает или крайне ограничивает (вследствие сложности реализации и дороговизны) возможность сопровождения их программного обеспечения. Внесение изменений в программный компонент может осуществляться:

а) по результатам периодических проверок ЦУВС комплексов, которые целесообразно проводить на наборах изменяющихся (расширяемых) исходных данных, увеличивая таким образом вероятность выявления ДП;

б) при обнаружении ДП в программных компонентах или необходимости модификации выполняемых алгоритмов (например, в бортовых ЦУВС космических аппаратов, связанных телемеханическими каналами с наземными комплексами управления).

В обоих случаях изменение программного компонента может реализоваться путем введения «теневых» каналов коррекции (Харченко, 1989).

3. В процессе разработки архитектур ЦУВС параллельно осуществляется выбор (формирование) технологии их создания, поскольку варьирование ее элементами позволяет изменять (наращивать) уровень надежности программного компонента, а также влиять на стоимостные и временные характеристики. Процедура выбора архитектур и технологий создания дефектоустойчивых ЦУВС является трудноформализуемой вследствие сильной корреляции стоимостных и временных параметров отдельных этапов самого процесса проектирования, а также достигаемых надежностных характеристик создаваемой системы. Это касается, прежде всего, этапов разработки ($f = 1$) и отладки ($f = 2$) (см. рис. 1). Анализ данных, приведенных Квирком (1990), позволяет получить формулу, связываю-

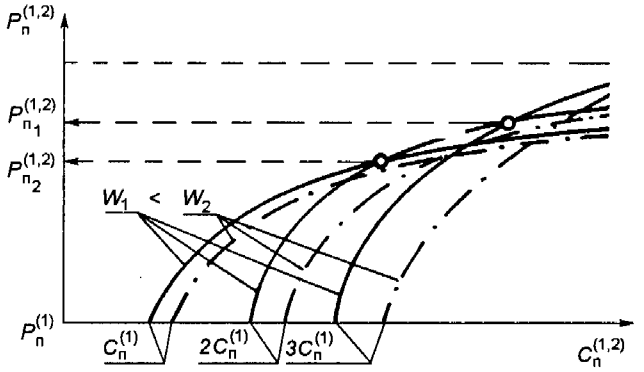

Рис. 2. Графики зависимости вероятности отсутствия дефектов проектирования в программных средствах после завершения отладки от стоимости этапов разработки и отладки

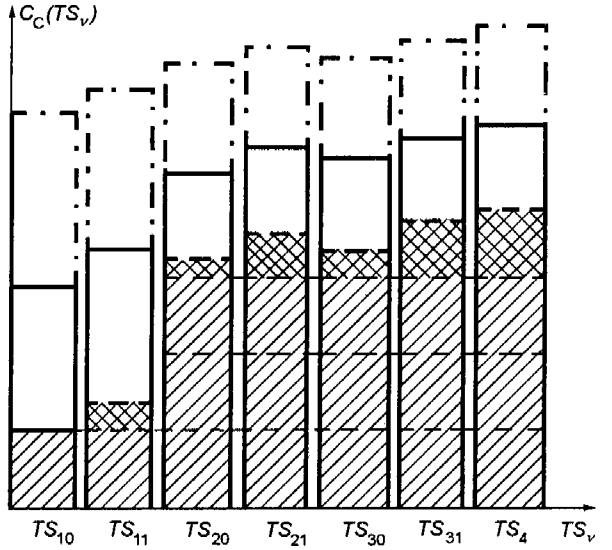

Рис. 3. Диапазоны относительного изменения стоимости создания программных средств при использовании различных технологий

щую вероятность $P_п^{(1,2)}$ отсутствия ДП в программном компоненте с суммарной стоимостью $C_п^{(1,2)}$ реализации этих двух этапов в зависимости от числа нетривиальных АВ $e_{\bar{т}}$, стоимости разработки $C_п^{(1)}$ и сложности разрабатываемой системы W:

$$P_п^{(1,2)} = 1 - [1 - P_п^{(1)}]X^{-k(w,\, e_{\bar{т}})[C_п^{(1,2)} - e_{\bar{т}}C_п^{(1)}]}, \qquad (6)$$

где X — константа процесса отладки, $X > 1$; $k(w, e_{\bar{т}})$ — коэффициент, зависящий от сложности разрабатываемой системы и числа нетривиальных версий, $k(w, e_{\bar{т}}) > 1$; $P_п^{(1)}$ — вероятность отсутствия ДП программных средств после разработки.

Графики функции $P_п^{(1,2)}[C_п^{(1,2)}, C_п^{(1)}, W, e_{\bar{т}}]$ показаны на рис. 2. Их анализ дает возможность сделать вывод о том, что увеличение числа нетривиальных версий при ужесточении требований к значению показателя $P_п^{(1,2)}$ может при возрастании сложности систем снизить суммарную стоимость $C_п^{(1,2)}$ за счет повышения интенсивности выявления ДП и сокращения времени отладки. Так, если требования к вероятности $P_п^{(1,2)}$ будут больше чем $P_{п2}^{(1,2)}$ (но меньше, чем $P_{п1}^{(1,2)}$), то для систем с уровнем сложности W_1 с точки зрения стоимости целесообразно выбрать двухверсионную технологию.

Диапазоны относительного изменения стоимости создания программных компонентов МАС при использовании различных технологий иллюстрируются рис. 3, где одинарной штриховкой отмечены затраты $C_п^{(1)}$, двойной штриховкой — затраты на операции $\psi_i \in \Psi$ и $\xi_{S1(2)}$. Незаштрихованная область соответствует стоимости реализации последующих этапов, а штрих-пунктиром — максимальное и минимальное значения общей стоимости для определенного уровня требований к надежности программного компонента.

4. Выбор архитектур из множества вариантов целесообразно осуществлять с использованием процедуры направленного перебора, основанной на формировании приоритетного ряда с учетом полученных математических оценок дефектоустойчивости и его коррекции для различных технологий, заданных требований и ограничений. Области возможных значений показателей дефектоустойчивости для базовых архитектур, образующих «поле» выбора, показаны на рис. 4.

Множество таких базовых архитектур образуют одноальтернативные нерезервированные архитектуры MS_0, многоальтернативные архитектуры $\widetilde{MS}_{\bar{т}}$ и $\widetilde{MS}_{\bar{\bar{т}}}$, использующие тривиальные и нетривиальные версии. В свою очередь, множество $\widetilde{MS}_{\bar{т}}$ включает подмножества i-ярусных архитектур ($i = 1,..., k$; ярус — участок резервирования):

— двухверсионных систем со встроенным контролем $MS_{2т}(i)$ (Харченко, 1992б);
— мажоритарных трехверсионных систем $\widetilde{MS}_{мт}(i)$ (Харченко, Паршин, 1991);
— многоканальных систем $\widetilde{MS}_{дт}(i)$, в которых каждый канал имеет двухверсионную архитектуру (Харченко, Литвиненко, 1991);
— гибридных систем $\widetilde{MS}_{дмт}$, в которых дублируются наиболее важные функции в каналах, включаемых затем по мажоритарной схеме (Харченко и др., 1992б).

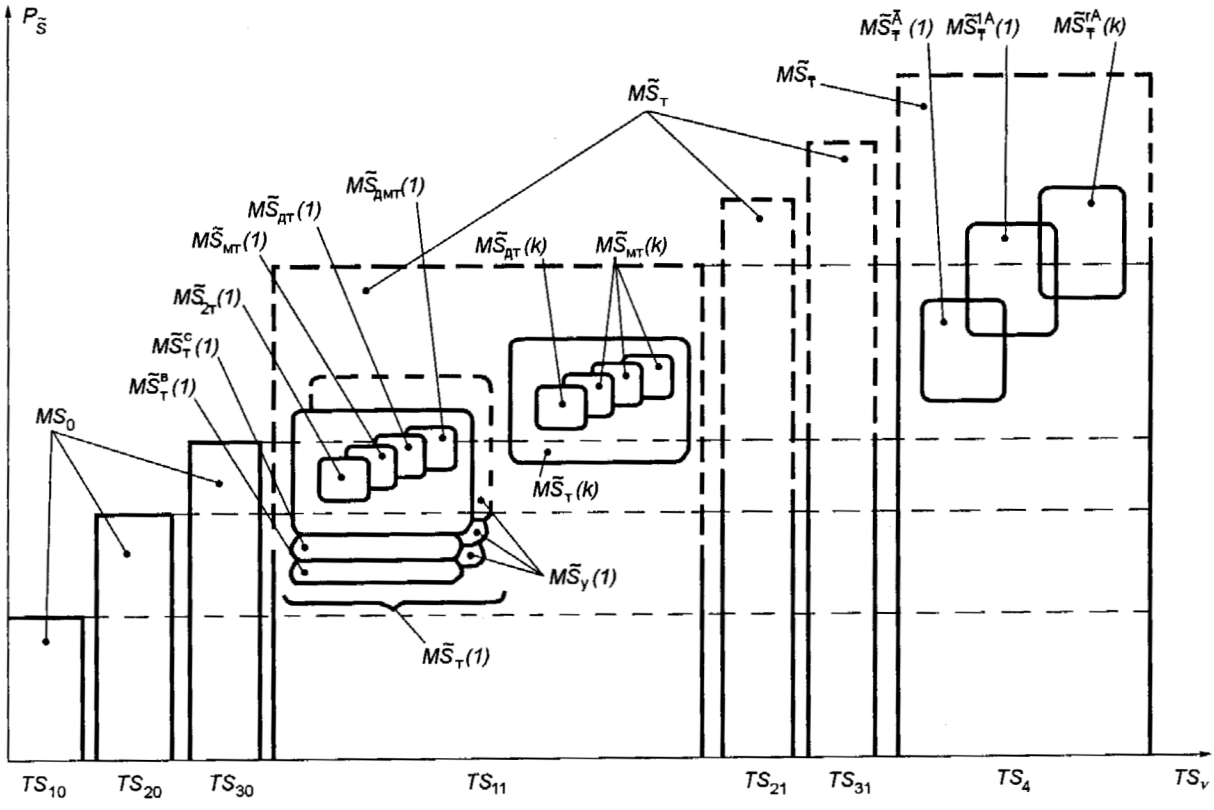

Рис. 4. Области возможных значений показателей дефектоустойчивости базовых архитектур многоальтернативных ЦУВС

Кроме того, указанное подмножество архитектур может иметь свои аналоги при последовательном ($M\tilde{S}_{\text{т}}^{\text{в}}(1)$) или параллельно-последовательном ($M\tilde{S}_{\text{т}}^{\text{с}}(1)$) выполнении версий (Харченко, Паршин, 1991), а также использовании их неполных (усеченных) вариантов $M\tilde{S}_{\text{у}}(1)$.

Множество $M\tilde{S}_{\text{т}}(i)$ включает:

— архитектуры неадаптивных систем $M\tilde{S}_{\bar{\text{т}}}^{\bar{\text{A}}}(1)$ с общим резервированием версий (Харченко, 1992а);

— архитектуры систем $M\tilde{S}_{\bar{\text{т}}}^{\text{A1}}(1)$ с однопараметрической адаптацией, в которых адаптивным параметром является пороговая функция восстанавливающего органа (Харченко, Паршин, 1991);

— архитектуры систем $M\tilde{S}_{\bar{\text{т}}}^{\text{rA}}(k)$ с многопараметрической адаптацией (r = 2, 3, ... — число адаптивных параметров). Например, такими параметрами, кроме пороговой функции, могут быть число нетривиальных версий и число ярусов резервирования, используемых в системе и изменяющихся в зависимости от числа отказов, обусловленных физическими дефектами аппаратных средств.

Такая адаптация обеспечивает минимизацию временных затрат на поиск работоспособных конфигураций при прерываниях системы, а также более полное использование резервных ресурсов по парированию последствий физических дефектов аппаратных средств. Она предусматривает переход от одноярусной многоверсионной архитектуры к многоярусной одноверсионной архитектуре по мере накопления отказов аппаратных средств.

5. Предлагаемая ниже методика строится в предположении, что выбор исходной нерезервированной архитектуры ЦУВС, для которой решается задача обеспечения дефектоустойчивости с учетом множества ограничений, произведен. В частности, предварительно отдано предпочтение либо централизованной архитектуре ЦУВС на базе мощной БЦВМ, либо децентрализованной — с использованием сети

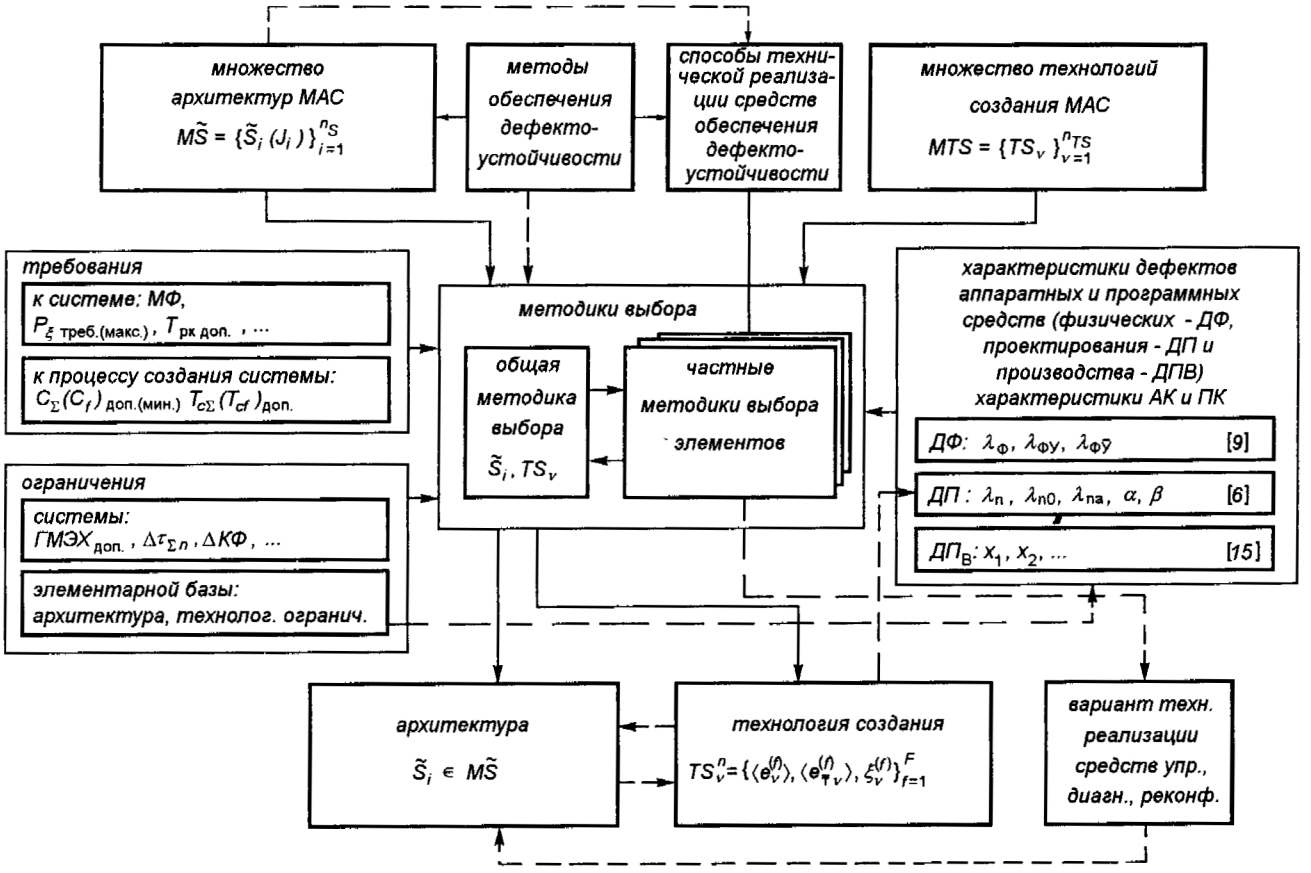

Рис. 5. Схема взаимосвязи элементов процесса создания многоальтернативных ЦУВС

микропроцессоров или микроЭВМ в соответствии с задачами, решаемыми системой (Пронин, Шохат, 1986). В первом случае дальнейшие рассуждения касаются выбора надежностной структуры центральной БЦВМ. Во втором случае объектами надежностного синтеза являются либо сетевая структура, рассматриваемая в надежностном плане как k-ярусная схема с последовательно соединенными элементами, либо сами элементы этой структуры, на которые «проецируются» требования, предъявляемые к ЦУВС в целом. Тогда по результатам оценки и выбора наилучших надежностных архитектур для случая централизованной и децентрализованной организации производится их сравнение, в результате которого может быть откорректировано исходное решение и отдано предпочтение альтернативному варианту по принципу централизации.

МЕТОДИКА ВЫБОРА АРХИТЕКТУР ДЕФЕКТОУСТОЙЧИВЫХ ЦИФРОВЫХ УПРАВЛЯЮЩИХ И ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ

Исходными элементами процесса создания многоальтернативных ЦУВС (рис. 5) являются множества архитектур МАС $M\tilde{S} = \{\tilde{S}_i(J_i)\}_{i=1}^{n_S}$ и технологий их создания $MTS = \{TS_v\}_{v=1}^{n_{TS}}$, а также принципы технической реализации средств управления, диагностирования и реконфигурации АВ при отказах (Харченко и др., 1994). В соответствии с требованиями, предъявляемыми к ЦУВС и процессу их создания, ограничениями системы и элементной базы, а также с учетом надежностных характеристик аппаратного и программного компонентов осуществляется выбор (синтез) рациональных архитектур $\tilde{S}_i^* \in M\tilde{S}$ и технологий $T\tilde{S}_v^* \in MTS$.

Алгоритм выбора включает общую и частные методики, позволяющие решать отдельные задачи создания МАС в соответствии с критериями, приведенными в работе Харченко, Благодарного (1994).

Общая методика содержит следующие основные этапы.

1. Анализ технического задания (ТЗ). В результате анализа выявляются требования, предъявляемые к ЦУВС, и основные ограничения. Кроме того, осуществляется проверка ТЗ на полноту и непротиворечивость сформулированных требований с целью снижения доли абсолютных ДП (коэффициентов α, β (Харченко, 1992а)).

2. Генерация множества архитектур одноярусных тривиальных МАС $M\widetilde{S}_{\text{т}}(1)$ и исключение из него систем $\widetilde{S}_{\text{т}\nu}$, не удовлетворяющих ограничениям по ГМЭХ, допустимой временной избыточности (это касается архитектур с последовательным $\widetilde{S}^{\text{в}}_{\text{т}}$ и параллельно-последовательным $\widetilde{S}^{\text{с}}_{\text{т}}$ выполнением версий (Харченко, Паршин, 1991), допустимому снижению достоверности или качества функционирования (при использовании систем $\widetilde{S}_{\text{у}}$ (Харченко, 1992б)).

3. Априорная оценка вероятности безотказной работы аппаратного компонента по физическим дефектам $P_{\text{ф}}(\widetilde{S}_{\text{т}i})$ и исключение систем, для которых $P_{\text{ф}}(\widetilde{S}_{\text{т}\nu}) \le P_{\widetilde{S}_{\text{тр}}}$ ($P_{\widetilde{S}_{\text{тр}}}$ — требуемое значение вероятности правильного функционирования ЦУВС). Эта оценка производится по формулам, приведенным Харченко, Литвиненко (1993) при условии, что $P_{\text{п}} = 1$.

4. Определение требований к уровню надежности программного компонента для рассматриваемого подмножества архитектур в соответствии с выражением:

$$P_{\text{п}}(\widetilde{S}_{\text{т}i}) \ge P_{\widetilde{S}_{\text{тр}}} / P_{\text{ф}}(\widetilde{S}_{\text{т}i}). \qquad (7)$$

Далее могут быть определены требования к интенсивности проявления $\lambda^{\text{тр}}_{\text{пi}}$ (остаточному уровню дефектов программных средств) и отобраны те архитектуры, для которых прогнозируемое значение $\lambda_{\text{пi}}$ при допустимом времени отладки $T^{(2)\text{доп}}_{\text{с}}$ и использовании технологии TS_{11} меньше $\lambda^{\text{тр}}_{\text{пi}}$. Для ЦУВС сложных технических комплексов требования по надежности, как правило, не могут быть выполнены в рамках одноальтернативных архитектур, поэтому технологии $TS_{\text{j}0}$, $j \in 1, 2, 3$, далее не рассматриваются.

5. Упорядочение архитектур $\widetilde{S}_{\text{т}i} \in M\widetilde{S}_{\text{т}}(1)$ в порядке нарастания стоимости их создания (или другого оптимизируемого показателя), разработка и предварительное тестирование программного компонента с целью уточнения прогноза величины $P_{\text{п}}$ и оценки вероятности правильного функционирования выбранной архитектуры в целом:

$$P_{\widetilde{S}} = P_{\text{п}} P_{\text{ф}}(S_{\text{т}i}).$$

6. Проверка соответствия найденного значения $P_{\widetilde{S}_{\text{т}}}$ требуемому уровню $P_{\widetilde{S}_{\text{тр}}}$. Если условие выполняется, то процедура завершается и выдается рекомендация по выбору архитектуры системы $S_{\text{т}i}(1)$ и технологии $T\widetilde{S}(1)$. В противном случае осуществляется выбор следующей архитектуры в порядке предпочтения (возврат к операциям 5). Если же множество архитектур систем $M\widetilde{S}_{\text{т}}(1)$ исчерпано, производится переход к следующему этапу.

7. Расширение множества анализируемых архитектур за счет использования декомпозированных многоярусных систем $M\widetilde{S}_{\text{т}}(k)$, $k \ge 2$. Из множества $M\widetilde{S}_{\text{т}}(k)$ исключаются архитектуры, не удовлетворяющие требованиям по допустимой величине времени реконфигурации $T_{\text{рк доп}}$. Для этого оцениваются временные характеристики алгоритмов поиска работоспособных конфигураций, приведенные в работе Харченко и др. (1992б).

8. Повторение операций этапов 3, 4 с учетом расширенного множества архитектур. Если

$$\exists\, \widetilde{S}_{\text{т}i}(k) \in M\widetilde{S}_{\text{т}}(k): \quad \lambda_{\text{пi}}(TS_{11}, T^{\text{доп}}_{\text{с}}) < \lambda^{\text{тр}}_{\text{пi}}, \qquad (8)$$

то далее реализуются операции этапов 5, 6 для подмножества отобранных архитектур. Их упорядочение в этом случае производится в соответствии с оценками времени и сложности средств реконфигурации. Если условия, проверяемые на этапе 6 (с учетом множества $M\widetilde{S}_{\text{т}}(k)$) или на этапе 8, не выполняются, осуществляется переход к следующему этапу.

9. Переход к технологиям $TS_{\text{j}1}$, $j \in \{2, 3\}$. Выбор (упорядочение) технологий и значений параметра $e_{\text{т}}$ для этапа $f = 2(3)$ производится с учетом временных и стоимостных ограничений процесса создания системы. Для этого используются формулы (4)—(6). Затем проверяется условие, аналогичное условию для различных технологий $TS_{\text{j}1}$ и значений $e_{\text{т}}$. Если оно выполняется, реализуются операции следующего этапа.

10. Операции данного этапа аналогичны операциям этапов 5, 6 с той разницей, что множество рассматриваемых систем охватывает и одно-, и многоярусные архитектуры $M\widetilde{S}_{\text{т}}(k')$, $k' \in 1,..., k$.

Кроме того, в процессе перебора изменяются значения числа нетривиальных АВ, используемых при отладке для уменьшения величины $\lambda_{\text{п}}$ и, если это возможно, времени и стоимости реализации

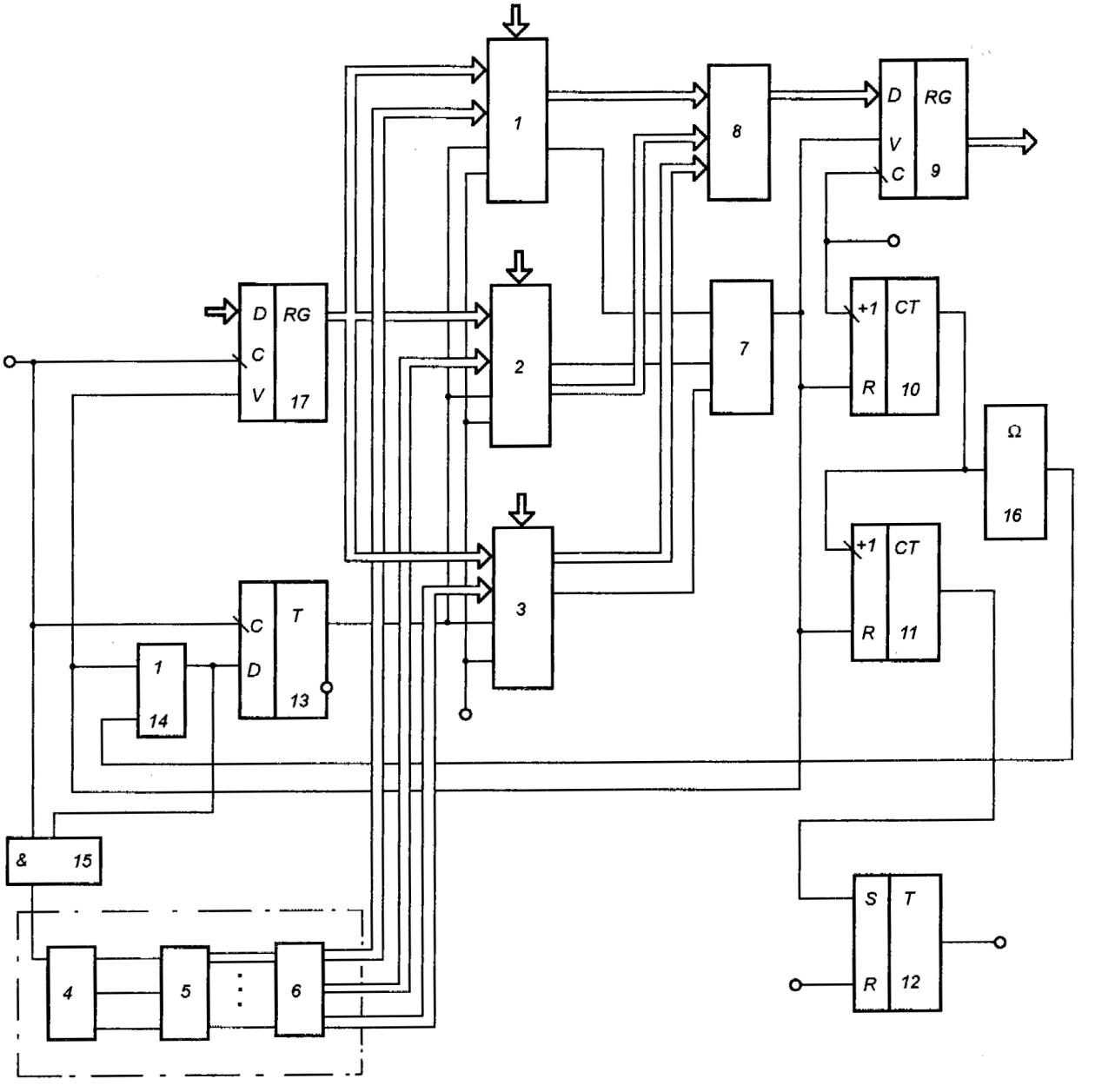

Рис. 6. Структурная схема МАС

этапа. Если после очередной итерации выполняются требования к величине $P_{\tilde{S}}$, выдается рекомендация по выбору архитектуры $\tilde{S}_{\text{п}}(k')$ и технологии TS_{j1} и работа завершается. В противном случае осуществляется переход к анализу следующей группы архитектур.

11. Генерация множества нетривиальных архитектур с однопараметрической адаптацией $M\tilde{S}_{\bar{\tau}}^{\text{A}(1\text{A})}$. Далее для этого множества повторяются операции, аналогичные операциям третьего этапа, и определяются требования к надежности программных компонентов отобранного подмножества архитектур $P_{\text{п}}(S_{\bar{\tau}}^{\text{A}(1A)})$, которые могут быть получены из выражений для оценки дефектоустойчивости с уче-

том известных величин $P_{\tilde{S}_{тр}}$ и $P_{ф}(\widetilde{S}^{\tilde{A}(1A)}_{\tilde{n}})$. Формирование множества архитектур для последующего анализа производится на основании требований к $\lambda_{п}$. При этом единственно возможной технологией для использования остается технология TS_4.

12. Блок операций этого этапа аналогичен блоку операций десятого этапа. В процессе перебора архитектур, упорядоченных по показателям стоимости (другим оптимизируемым показателям), варьируется число нетривиальных альтернативных версий. При выполнении требований к $P_{\tilde{S}}$ выдается рекомендация по оптимальной (рациональной) архитектуре $S^{\tilde{A}(1A)}_{\tilde{n}}$ и технологии TS_4. В противном случае реализуется последняя группа операций.

13. Осуществление расширения множества архитектур за счет использования методов многопараметрической адаптации. Далее проводится их анализ с учетом различных ограничений и уточняется оценка дефектоустойчивости. При наличии архитектуры, удовлетворяющей уровню $P_{\tilde{S}_{тр}}$, алгоритм завершается. Если использование многопараметрической адаптации не позволяет получить приемлемое решение, делается вывод о необходимости коррекции технического задания на ЦУВС и осуществляется возврат ко второму этапу или одному из этапов, с которых начинаются последующие итерации (этапы 7, 9, 11, 13).

ПРИМЕРЫ ТЕХНИЧЕСКОЙ РЕАЛИЗАЦИИ МАС

Особенностью технической реализации МАС является то, что при параллельном выполнении версий каналы системы работают асинхронно, поскольку длительность реализации различных версий задач может не совпадать. Следовательно, в этом случае несколько видоизменяется конструкция восстанавливающих органов. они должны содержать средства фиксации завершения выполнения фрагментов версий, когда допускается сравнение выходных данных каналов.

При последовательном выполнении версий эта особенность реализуется путем коррекции допустимой продолжительности решения задачи. Один из вариантов технической реализации архитектуры дефектоустойчивой ЦУВС приведен на рис. 6 (А. с. 1753479). В этой системе альтернативные версии задаются в вычислительных каналах (ВК *1—3*) генератором псевдонаучного кода *4*, который преобразуется блоком, выполненным на дефифраторе *5* и шифраторе *6*, в начальный код адреса версии. При реализации вычислений осуществляется логическая синхронизация меток завершения фрагментов версий элементом *7*. Выходные данные ВК *1—3* формируются блоком мажоритирования *8* и записываются в регистр *9*. Контроль зависания каналов осуществляется счетчиками *10*, *11* и триггером *12*. Синхронизация начала выполнения версий в каналах производится с использованием триггера *13*, элемента ИЛИ *14*, элемента И *15* и одновибратора *16*. Коды выполняемых задач фиксируются в регистре *17*, определяя адресное пространство программ, а данные поступают непосредственно в ВК *1—3*. При зависании каналов изменяется набор реализуемых версий и осуществляется повторный счет. Эффект от применения МАС такого типа усиливается благодаря расширению множества альтернативных версий и снижению корреляции дефектов при псевдослучайном выборе версий.

ВЫВОДЫ

1. Отличительной чертой предложенной методики является то, что она обеспечивает поиск решения на множестве архитектур ЦУВС, которое дополнено архитектурами различных вариантов многоальтернативных систем, которые обладают способностью в реальном масштабе времени парировать сбои и отказы, обусловленные не только физическими дефектами аппаратных средств, а и дефектами проектирования программных средств. Выигрыш в надежности, получаемый при использовании МАС по отношению к известным резервированным структурам, применяемых в бортовых системах (Мамедли, Соболев, 1986; Avizienis, Laprie, 1986; Кривоносов и др., 1995), зависит от соотношения безотказности аппаратных и программных средств и степени усложнения восстанавливающих органов многоальтернативных архитектур. Количественные оценки достигаемого выигрыша для двух-, трех- и четырехканальных архитектур даны в наших работах 1991—1994 гг. Так, например, при равной безотказности аппаратных и программных средств (интенсивности отказа $\sim 10^{-5}$ 1/ч) и усложнении мажоритарных элементов на 10—15 % использование трехканальных МАС обеспечивает уменьшение вероятности отказа в 2—5 раз по сравнению с традиционными одноальтернативными мажоритарными архитектурами.

2. Кроме того, данная методика в отличие от известных позволяет в рамках поставленных задач осуществлять направленный выбор не только архитектур дефектоустойчивых ЦУВС, а и технологий их создания, характеризуемых числом и порядком отбора версий на разных этапах разработки и испытаний систем.

3. Общая методика дополняется частными методиками, обеспечивающими решение локальных задач, а именно:

- декомпозиции и выбора архитектур тривиальных МАС с параллельным выполнением альтернативных версий с учетом ограничений по ГМЭХ, времени и сложности (безотказности) средств реконфигурации ЦУВС (Харченко, 1992б);
- выбора алгоритмов реконфигурации для многоярусных мажоритарных МАС и систем с матричной СБИС-архитектурой (Харченко др., 1992а), учитывающих влияние параметров средств поиска работоспособных конфигураций на вероятность правильного функционирования (функцию готовности) ЦУВС;
- выбора параметров архитектур МАС, реализующих метод гибридного резервирования, другие методы обеспечения дефектоустойчивости (Харченко, Паршин, 1991; Харченко и др., 1992б);
- оптимального резервирования локальных сетей бортовых и наземных ЦУВС в базисе дефектоустойчивых архитектур, учитывающих различные типы ограничений (Харченко и др., 1994).

Методики выбора МАС могут быть конкретизированы, если дополнить комплекс рассмотренных базовых архитектур множеством вариантов технической реализации средств обеспечения дефектоустойчивости (А. с. 1732346, 1992).

А. с. 1732346 (СССР). Устройство для контроля и отладки многоальтернативных систем / В. С. Харченко, А. В. Бек, М. А. Черныш ов и др.—Опубл. 07.05.92, Бюл. № 17.

А. с. 1753479 (СССР). Многоальтернативная вычислительная система / В. С. Харченко, Г. Н. Тимонькин, В. Л. Кукуруза и др.—Опубл. 07.08.92, Бюл. № 29.

Головкин Б. А. Многовариантное программирование и его применение // Автоматика и телемеханика.—1986.—№ 7.—С. 5—36.

Квирк У. Дж. (ред.) Проверка и утверждение программ реального времени. — Киев: Наук. думка, 1990.—216 с.

Кривоносов А. И., Байда Н. К., Харченко В. С. и др. Структурно-алгоритмическая организация и модели надежности мажоритарно-резервированных систем // Косміч. наука і технологія.—1995.—1, № 1.—С. 71—76.

Мамедли Э. М., Соболев Н. А. Концепция обеспечения отказоустойчивости СУ и безопасности экипажа «Шаттл» // Зарубеж. радиоэлектроника.—1986.—№ 8.—С. 19—32;—№ 9.—С. 21—34.

Пронин Е. Г., Шохат В. С. Проектирование технических средств бортовой ЭВА. — М.: Радио и связь, 1988.—С. 51—67.

Харченко В. С. Оперативная коррекция программ по результатам отладки. Системы отладки микропроцессорных устройств. — Харьков, 1989.—С. 120—133.

Харченко В. С. Модели и свойства отказоустойчивых многоальтернативных систем // Автоматика и телемеханика.—1992а.—№ 12.—С. 140—147.

Харченко В. С. Поиск оптимальных структур при двухальтернативном проектировании каналов УВС // Изв. ВУЗов. Приборостроение.—1992б.—№ 5.—С. 31—35.

Харченко В. С., Благодарний М. П. Організація багатоальтернативних обчислень у цифрових системах літальних апаратів і комплексів // Наука і оборона.—1994.—№ 3.—С. 153—161.

Харченко В. С., Кушнерук Ю. И., Гайворонский И. Я. Оптимальное резервирование в базисе многоальтернативных архитектур, устойчивых к дефектам программно-аппаратных средств // Надежность, живучесть и безопасность летательных аппаратов: Тез. науч. техн. семинара. — Харьков, 1994.—С. 11.

Харченко В. С., Литвиненко В. Г. Модели парирования дефектов проектирования программно-аппаратных средств в необслуживаемых системах // Электронное моделирование.—1992.—№ 3.—С. 34—39.

Харченко В. С., Литвиненко В. Г. Применение концепции многоальтернативного проектирования для построения высоконадежных и безопасных систем // Приборы и системы управления.—1993.—№ 6.—С. 8—11.

Харченко В. С., Литвиненко В. Г., Краснобаев В. А. Методы и алгоритмы реконфигурации систолических матричных систем с фиксированной размерностью и деградацией структуры // Кибернетика и системный анализ.—1992а.—№ 4.—С. 72—79.

Харченко В. С., Литвиненко В. Г., Терещенков С. В., Мельников В. А. Обеспечение устойчивости управляющих и вычислительных систем к физическим дефектам и дефектам проектирования программно-аппаратных средств // Зарубеж. радиоэлектроника.—1992б.—№ 6.—С. 18—35.

Харченко В. С., Паршин В. В. Гарантоспособные УВС с последовательным и параллельным выполнением альтернативных версий. — Харьков, 1991.—41 с.—(Препринт / АН Украины. Ин-т проблем машиностроения; № 340).

Avizienis F., Laprie J.-C. Dependable computing from concepts to desing diversity // IEEE Trans. Comput.—1986.—74.—№ 5.—P. 8—21.

CHOICE OF DESIGN TECHNOLOGIES AND BASIC ARCHITECTURES FOR THE DEFECT-TOLERANT DIGITAL CONTROL AND COMPUTING REAL-TIME SYSTEMS

V. S. Kharchenko

We analyze design technologies for the real-time digital control and computing systems (DCCS) based on the multialternative principle. We propose a vector characters of the design technologies for the multialternative defect-tolerant DCCS and a classification of their basis architectures. We assess the reliability and cost of the DCCS based on different design technologies. A method for the choice of design technologies and basic architectures of DCCS is proposed.