ISSN 1561-8889. Космічна наука і технологія. 1999. Т 5. № 5/6. С. 81—91.

УДК 681.326.7

Методы многопараметрической адаптации бортовых управляющих и вычислительных систем с раздельным мажоритарным резервированием

В. С. Харченко, А. П. Зенин, В. В. Скляр

Харківський військовий університет

Надійшла до редакції 03.08.99

Узагальнено архітектуру бортових управляючих і обчислювальних систем з роздільним мажоритарним резервуванням, в яких як адаптивні параметри використовуються не тільки порогова функція відновлюючого органу, але і кількість ярусів резервування, і кількість програмних версій (варіантів). Приведені результати досліджень систем, в яких реалізуються методи ярусно-порогової і ярусно-версійно-порогової адаптації.

1. ВВЕДЕНИЕ

Увеличение объема вводимой избыточности (структурной, программной и др.) в целях обеспечения отказоустойчивости управляющих и вычислительных систем (УВС) может дать требуемый эффект, если оно сопровождается разработкой адекватных процедур реконфигурации, учитывающих ограничения временного, стоимостного и другого характера. Это особенно важно для бортовых УВС космических аппаратов, которые работают в реальном масштабе времени и являются, как правило, необслуживаемыми или частично обслуживаемыми системами [5]. Высокие требования по их безотказности могут быть выполнены путем увеличения числа участков резервирования (ярусов) или резервируемых компонентов и введения развитых средств диагностирования и реконфигурации. В то же время поиск работоспособных конфигураций должен осуществляться достаточно быстро, несмотря на то, что их количество связано с числом ярусов показательной зависимостью [11]. Кроме того, это противоречие обостряется двумя обстоятельствами. Во-первых, усложнение процедур реконфигурации сопровождается увеличением объема и снижением безотказности соответствующих средств и УВС в целом. Во-вторых, раздельное резервирование практически исключает возможность использования версионной избыточности в многоверсионных архитектурах, устойчивых к дефектам проектирования программных средств [11].

Разрешение указанного противоречия возможно путем совершенствования механизмов адаптации архитектур отказоустойчивых УВС, обзор которых дан в [8, 13]. В наиболее распространенных УВС с мажоритарной архитектурой используются управляемые восстанавливающие органы, пороговая характеристика которых изменяется в зависимости от числа отказавших каналов [3]. В данной статье предлагается увеличить множество адаптивных параметров и таким образом расширить пространство поиска решений, удовлетворяющих требованиям к системам данного класса. К числу основных требований относятся требования безотказности системы, определяемые, как правило, величиной вероятности безотказной работы (или ее аналога — вероятности правильного функционирования при учете ненадежности программных средств). В качестве

ограничений должны учитываться, прежде всего, ограничения, диктуемые реальным масштабом времени функционирования, — допустимой продолжительностью диагностирования и реконфигурации архитектуры, а также ограничения на габаритомассовые характеристики. Далее рассматриваются УВС с мажоритированием двух типов (одноверсионные и многоверсионные системы (МВС), обладающие свойствами устойчивости к физическим дефектам аппаратных средств (ДФ-устойчивости), дефектам проектирования программных средствам (ДП-устойчивости) и общей дефектоустойчивости (Д-устойчивости). При этом используются основные понятия и результаты, изложенные в работе [6]. В частности, под версией понимается эквивалентный программный (программно-аппаратный) вариант выполнения функций.

2. ОБЩАЯ ХАРАКТЕРИСТИКА УВС С МНОГОПАРАМЕТРИЧЕСКОЙ АДАПТАЦИЕЙ. ПОСТАНОВКА ЗАДАЧИ

Рассмотрим систему $\widetilde{S}$, характеризующуюся множеством параметров $\text{МП}_{\widetilde{S}}$, которые могут изменяться в процессе функционирования. К их числу отнесем общее число версий e, число нетривиальных (нетождественных) версий $e_{\overline{\text{Т}}}$, порог срабатывания мажоритара $e_{\text{П}}$, число ярусов резервирования k и др.

Если в процессе функционирования системы при отказах элементов компонентов ее версий работоспособность сохраняется путем изменения значения одного из параметров $\text{П}_1 \in \text{МП}_{\widetilde{S}}$, будем называть ее системой с однопараметрической адаптацией, а соответствующий параметр — адаптивным. Системы с однопараметрической адаптацией по порогу $e_{\text{П}}$ срабатывания восстанавливающего органа исследованы в [7]. Порог $e_{\text{П}} = 1, \ldots, (e+1)/2$ является функцией числа отказавших версий e_{d}. Функцию $e_{\text{П}} = f(e_{\text{d}})$ назовем функцией адаптации.

Если в процессе функционирования изменяется два и более параметров из множества $\text{МП}_{\widetilde{S}}$, назовем такие системы системами с многопараметрической адаптацией. Следовательно,

$$\text{МП}_{\widetilde{S}} = \text{МП}^{\text{А}}_{\widetilde{S}} \cup \text{МП}^{\overline{\text{А}}}_{\widetilde{S}}, \quad \text{МП}^{\text{А}}_{\widetilde{S}} \cap \text{МП}^{\overline{\text{А}}}_{\widetilde{S}} = \varnothing,$$

где $\text{МП}^{\text{А}(\overline{\text{А}})}_{\widetilde{S}}$ — множество адаптивных (неадаптивных) параметров. Для систем с многопараметрической адаптацией (МПА) $\text{card}\,\text{МП}^{\text{А}}_{\widetilde{S}} \geq 2$. Таким образом, каждая система с МПА характеризуется множеством $\text{МП}^{\text{А}(\overline{\text{А}})}_{\widetilde{S}}$ и множеством функций адаптации $\text{М}f^{\text{А}}$ для всех $\text{П}_1 \in \text{МП}^{\text{А}}_{\widetilde{S}}$.

Проанализируем возможные варианты систем с многопараметрической адаптацией.

1. Одноверсионные системы с ярусно-пороговой адаптацией, $S^{2\text{A}}_{\text{Т}}$, для которых

$$\begin{cases} \text{МП}^{\text{А}}_{\widetilde{S}} = \{e_{\text{П}}, k\}, \quad k = 1,\ldots, k_{\Phi}, \quad e_{\overline{\text{Т}}} = 0, \\ e_{\text{П}} = f^{\text{А}}_{\text{П}}(e_{\text{d}}), \quad k = f^{\text{А}}_{\text{k}}(e_{\text{d}}, r_{\varphi}), \end{cases} \tag{1}$$

где r_{φ} — булева переменная, определяемая режимом функционирования системы, причем $r_{\varphi} = 0$ при выполнении $\varphi_{\text{i}} \in \Phi$ и $r_{\varphi} = 1$ при поиске работоспособных конфигураций; k_{Φ} — число ярусов, определяемых безотказностью аппаратного компонента по физическим дефектам.

2. Многоверсионные системы с ярусно-версионной адаптацией $S^{2\text{A}}_{\overline{\text{Т}}1}$, такие что

$$\begin{cases} \text{МП}^{\text{А}}_{\widetilde{S}} = \{e_{\overline{\text{Т}}}, k\}, \\ e_{\overline{\text{Т}}} = \begin{cases} e_{\overline{\text{Т}}0}, & \text{если } e_{\text{d}} \leq e - e_{\text{П}}, \\ 0, & \text{если } e_{\text{d}} > e - e_{\text{П}}, \end{cases} \\ k = \begin{cases} 1, & \text{если } e_{\text{d}} \leq e - e_{\text{П}}, \\ (>1)\ \&\ (\leq k'_{\Phi}), & \text{если } e_{\text{d}} > e - e_{\text{П}}, \end{cases} \end{cases} \tag{2}$$

$e_{\overline{\text{Т}}0}$ — начальное значение параметра $e_{\overline{\text{Т}}}$ в системе.

Варьирование значениями параметров $e_{\overline{\text{Т}}}$ и k позволяет сохранить конфигурацию нетривиальной системы до отказа элементов аппаратного компонента одной или нескольких ($e_{\text{d}} \leq e - e_{\text{П}}$) версий. Функция адаптации для параметра k может зависеть также от параметра r_{φ}.

Если возможна совместная декомпозиция программного и аппаратного компонентов на $k_{\text{П}} \leq k_{\Phi}$ ярусов, то функция адаптации $f^{\text{А}}_{\text{k}}$ выглядит следующим образом:

$$k = \begin{cases} k_{\text{П}}, & \text{если } e_{\text{d}} \leq e - e_{\text{П}}, \\ (>k_{\text{П}})\ \&\ (\leq k'_{\Phi}), & \text{если } e_{\text{d}} > e - e_{\text{П}}, \end{cases} \tag{3}$$

Системы такого типа будем обозначать $\widetilde{S}^{2\text{A}}_{\overline{\text{Т}}2}$.

3. МВС-системы с ярусно-версионно-пороговой адаптацией $\widetilde{S}^{3\text{A}}_{\overline{\text{Т}}1}$, $\widetilde{S}^{3\text{A}}_{\overline{\text{Т}}2}$, для которых $\text{МП}^{\text{А}}_{\widetilde{S}} = \{e_{\text{П}}, e_{\overline{\text{Т}}}, k\}$. Функции адаптации параметров $e_{\text{П}}$, $e_{\overline{\text{Т}}}$, k аналогичны рассмотренным выше для систем $S^{2\text{A}}_{\text{Т}}$ и $\widetilde{S}^{2\text{A}}_{\overline{\text{Т}}1}$.

Исследование различных вариантов систем с многопараметрической адаптацией включает в себя ряд частных задач:

а) оптимальная декомпозиция версий в одноверсионных системах на ярусы по показателю безотказности аппаратных компонент с учетом характеристик средств диагностирования и реконфигурации — ДФ-декомпозиция;

б) анализ целесообразности варьирования ярусности версий в зависимости от ограничений на время реконфигурации;

в) оценка эффекта, получаемого при варьировании ярусности в МВС;

г) разработка научно-методического аппарата совместной надежностной и содержательной декомпозиции версий систем, описываемых различными математическими моделями.

Остановимся на результатах решения первых трех задач применительно к мажоритарным МВС, поскольку четвертая задача носит самостоятельный характер [12]. При этом следует учесть, что:

1) вероятность правильного функционирования является возрастающей функцией числа ярусов на всем интервале от 1 до k только при идеальных средствах выполнения функции мажоритирования ξ. Кроме того, возможности увеличения k ограничиваются архитектурными и технологическими особенностями элементной базы;

2) с увеличением числа ярусов k может существенно увеличиваться время $T_{\text{рк}}$ поиска работоспособных конфигураций МВС, на которое накладываются жесткие ограничения в системах реального масштаба времени;

3) интервал времени, на котором многие типы МВС имеют преимущество в Д-устойчивости перед одноверсионными системами, ограничен [11];

4) аппаратные компоненты операционной среды, в которой реализуются различные версии, могут быть идентичными.

3. ДФ-ДЕКОМПОЗИЦИЯ МАЖОРИТАРНЫХ УВС

Получим решение задачи ДФ-декомпозиции для трехканальных мажоритарных систем двух типов — с централизованным и децентрализованным управлением средствами контроля и реконфигурации ($S^{\text{Ц}}$ и $S^{\text{Д}}$), которое, в отличие от известных [4], позволяет учесть характеристики этих средств.

1. Исследуемые системы с централизованными средствами контроля и реконфигурации $S^{\text{Ц}}$.

Поскольку безотказность входных и выходных средств коммутации и значения вероятности непроявления (проявления) дефектов программных средств $P_{\text{П}}(Q_{\text{П}})$ не влияют на результат данной задачи, будем в дальнейшем ими пренебрегать. Тогда для вероятности отказа систем $S^{\text{Ц}}_{\text{Т}}$ справедливо

$$Q(\widetilde{S}^{\text{Ц}}_{\text{Т}}) \approx (1 - Q_{\xi\text{ц}})k\,[3Q^2_{\text{фф}} - 2Q^3_{\text{фф}} - 3Q^2_{\text{фф}}(1 - Q_{\text{фф}})D_{\text{кф}}] + Q_{\xi\text{ц}}k\,[P^3_{\text{фф}} + 3P^2_{\text{фф}}(1 - P_{\text{фф}})] \times [3Q^2_{\text{фф}} - 2Q^3_{\text{фф}}], \quad (4)$$

где $D_{\text{кф}}$ — вероятность достоверного контроля аппаратного компонента; $Q_{\xi\text{ц}}$ — вероятность отказа централизованных средств контроля и реконфигурации (общего ядра средств выполнения функции ξ);

$$P_{\text{фф}} = P_{\text{фэ}}P_{\xi\text{э}}, \quad Q_{\text{фф}} \cong Q_{\text{фэ}} + Q_{\xi\text{э}} \quad (5)$$

— вероятности безотказной работы и отказа аппаратных компонентов фрагмента (канала) яруса, причем $P_{\text{фэ}}$ ($Q_{\text{фэ}}$) — вероятность безотказной работы (отказа) собственно фрагмента, $P_{\xi\text{э}}$ ($Q_{\xi\text{э}}$) — вероятность безотказной работы (отказа) мажоритарного элемента (для систем с сетевым мажоритированием).

При справедливости экспоненциального закона выражение (5) преобразуется к виду

$$Q_{\text{фф}} \approx \left(\frac{n_{\text{ф}}}{k} + n_{\xi\text{э}}\right)\lambda_{\text{фэ}}t, \quad (6)$$

$$P_{\text{фф}} \approx \left(1 - \frac{n_{\text{ф}}}{k}\lambda_{\text{фэ}}t\right)(1 - n_{\xi\text{э}}\lambda_{\text{фэ}}t), \quad (7)$$

где $n_{\text{ф}}$, $n_{\xi\text{э}}$, $\lambda_{\text{фэ}}$ — число элементов и интенсивность отказов.

Продифференцируем функцию $Q(\widetilde{S}^{\text{Ц}}_{\text{Т}}) = f(k)$ по аргументу k, исключив слагаемые, содержащие величину $(\lambda_{\text{фэ}}t)^i$, $i > 4$, с учетом (4—7), а также того, что

$$Q_{\xi\text{ц}} \cong a_{\text{ц}}(1 + b_{\text{ц}}k)\lambda_{\text{фэ}}t, \quad (8)$$

где $a_{\text{ц}}$ и $b_{\text{ц}}$ — соответствующие коэффициенты сложности средств контроля и конфигурации.

После ряда преобразований получим уравнение

$$k^3 + c_1k + c_0 = 0, \quad (9)$$

где

$$c_1 = 3n^2_{\text{ф}}(2\lambda_{\text{фэ}}tn_{\xi\text{э}} + D_{\text{кф}} - 1)/(3n^2_{\xi\text{э}} - 2\lambda_{\text{фэ}}tn^3_{\xi\text{э}}),$$

$$c_0 = 2\lambda_{\text{фэ}}tn^3_{\text{ф}}(2 - D_{\text{кф}})/(3n^2_{\xi\text{э}} - 2\lambda_{\text{фэ}}tn^3_{\xi\text{э}}).$$

Анализ дискриминанта уравнения (9) показывает, что оно имеет три действительных корня, причем только один из них не меньше единицы. Оптимальное значение k для систем $S^{\text{Ц}}_{\text{Т}}$ вычисляется по формуле

$$k_{\text{opt}}(\widetilde{S}^{\text{Ц}}_{\text{МТЗ}}) = 2\,(n_{\text{ф}}/n_{\xi\text{э}})\sqrt{\rho_1/\rho_2}\cos(\varphi/3), \quad (10)$$

где $\varphi = f(\lambda_{\text{фэ}}, t, n_{\xi\text{э}}, D_{\text{кф}})$.

Результаты исследований функций (4) и (10) иллюстрируются рис. 1. Их анализ позволяет заключить, что:

а) величина $k_{\text{opt}}(\widetilde{S}^{\text{Ц}}_{\text{МТЗ}})$ является возрастающей функцией от сложности версий $n_{\text{ф}}$, убывающей

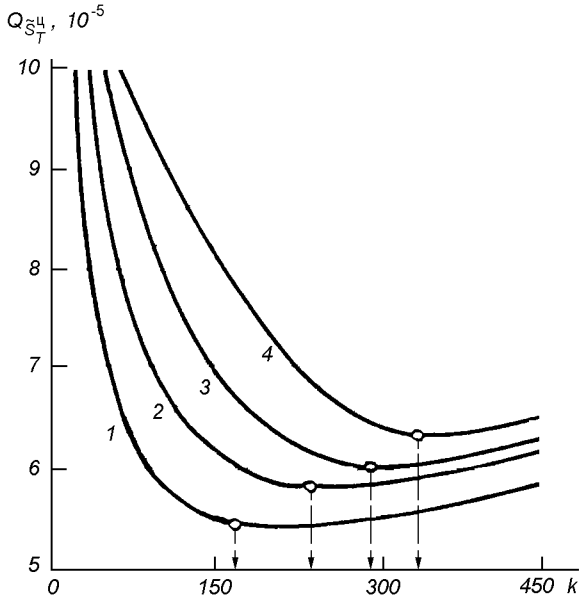

Рис. 1. Зависимости вероятности отказа систем $\tilde{S}_T^{Ц}$ от числа ярусов при $\lambda_{фэ}t = 5 \cdot 10^{-5}$, $P_П = 1$, $n_ф = 1500$, $n_{ξэ} = 2$, $a_ц = 50$, $b_ц = 0.001$. Кривые *1*—*4* — для $D_{кф} = 0.95$, 0.9, 0.85 и 0.8 соответственно

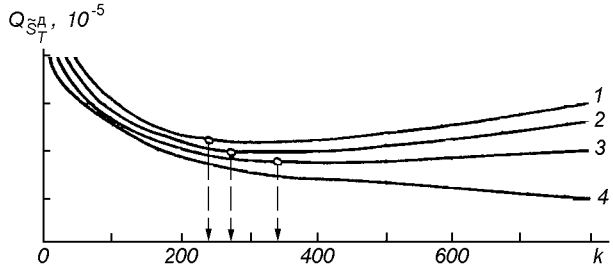

Рис. 2. Зависимости вероятности отказа систем $\tilde{S}_T^{Д}$ от числа ярусов k при $\lambda_{фэ}t = 5 \cdot 10^{-5}$, $P_П = 1$, $n_ф = 1500$, $n_{ξэ} = 2$, $b_Д = 2$, $n_{ξДЦ} = 5$, $D_{кф} = 0.8$. Кривые *1*—*4* — для $Q_A = 3$, 5, 7, 10 соответственно

функцией от достоверности контроля $D_{кф}$ и сложности мажоритарных элементов и практически не зависит от вероятности $\lambda_{фэ}t$ отказа элементов, на которых строится версия;

б) на участке $k \in [1, k_{opt}]$ значения функции $Q(S_{МТЗ}^{Ц})$ резко уменьшаются, а при $k > k_{opt}$ медленно растут;

в) увеличение коэффициентов сложности ядра ($a_ц$) и оболочки ($b_ц$) средств контроля и реконфигурации ведут к увеличению вероятности отказа и вызванному этим незначительному увеличению величины k_{opt}.

2. Исследуем системы с децентрализованными средствами контроля и реконфигурации $S_T^{Д}$. Каждый из ярусов имеет индивидуальные средства, которые могут быть реализованы в виде микрореконфигураторов [9]. Вероятность их отказа вычисляется по формуле

$$Q_{ξэ} \approx \lambda_{фэ}t\left(a_д + \frac{b_д}{k}\right), \qquad (11)$$

где $a_д$ и $b_д$ — коэффициенты сложности, аналогичные коэффициентам a и b выражения (8).

Тогда вероятность отказа системы $S_T^{Д}$ определится следующим образом

$$Q(\tilde{S}_T^{Д}) \cong (1 - kQ_{ξэд})k\,[3Q_{фф}^2 - 2Q_{фф}^3 - 3Q_{фф}^2(1 - Q_{фф})D_{кф}] + kQ_{ξэд}\,[P_{фф}^3 + 3P_{фф}^2(1 - P_{фф})] \times [3Q_{фф}^2 - 2Q_{фф}^3] + Q_{ξдц}, \qquad (12)$$

где $Q_{ξДЦ}$ — вероятность отказа аппаратных компонентов, координирующих взаимодействие индивидуальных средств контроля и реконфигурации ярусов.

Целесообразность использования систем $\tilde{S}_T^{Д}$ (по сравнению с системами $\tilde{S}_T^{Ц}$) определяется значением величины $Q_{ξДЦ}$. Исследования показывают, что приемлемые результаты могут быть получены при мажоритировании средств реализации $\xi_{ДЦ}$.

Анализ функции $Q(\tilde{S}_T^{Д}) = f(k)$ (рис. 2) показывает, что:

а) характер зависимости оптимального числа ярусов от параметров $n_ф$, $n_{ξэ}$, $D_{кф}$, $\lambda_{фэ}$, t в системах $\tilde{S}_T^{Д}$ аналогичен системам $\tilde{S}_T^{Ц}$;

б) вероятность отказа системы $\tilde{S}_T^{Д}$ и результаты определения k_{opt} весьма чувствительны к вариации параметров индивидуальных средств контроля и реконфигурации, в частности значения $a_д$;

в) усложнение мажоритарных органов в системах $\tilde{S}_T^{Д}$ в области минимальных значений вероятности отказа оказывает на него значительно меньшее влияние, чем в системах $S_T^{Ц}$, поэтому при увеличении разрядности выходной информации предпочтительность выбора систем $S_T^{Д}$ растет;

г) очевидным является преимущество систем $\tilde{S}_T^{Д}$ по показателю времени контроля и реконфигурации, а также Д-диагностируемости. Выбор системы по показателю безотказности определяется знаком разности ΔQ, вычисляемой с учетом (4) и (12) и формулы

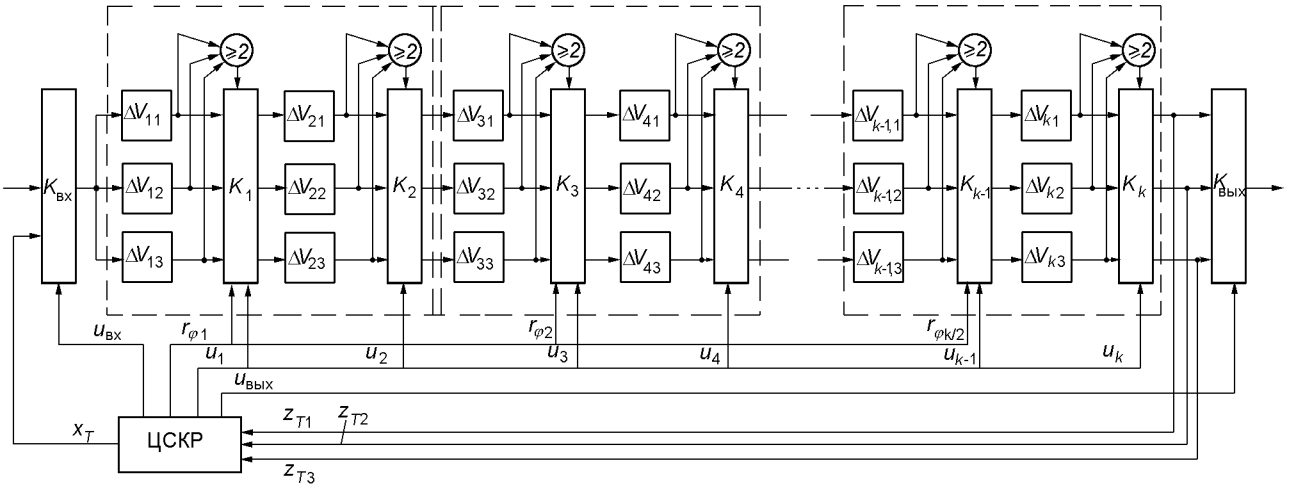

Рис. 3. Архитектура системы с ярусно-пороговой адаптацией

$$\Delta Q = Q(\widetilde{S}_{\text{Т}}^{\text{Ц}}) - Q(\widetilde{S}_{\text{Т}}^{\text{Д}}) =$$

$$= (Q_{\text{А}} - Q_{\bar{\text{А}}})(P_{\xi\text{ц}} - P_{\xi\text{д}}) - Q_{\xi\text{дц}}, \qquad (13)$$

где $Q_{\text{А}}$, $Q_{\bar{\text{А}}}$ — вероятности отказа адаптивной и неадаптивной структур систем $\widetilde{S}_{\text{Т}}$ соответственно:

$$P_{\xi\text{Ц}} = 1 - Q_{\xi\text{Ц}}, \quad P_{\xi\text{Д}} = 1 - kQ_{\xi\text{Д}}.$$

Поскольку разность $Q_{\text{А}} - Q_{\bar{\text{А}}}$ всегда меньше нуля, то знак ΔQ без учета $Q_{\xi\text{ДЦ}}$ зависит только от знака разности $P_{\xi\text{Ц}} - P_{\xi\text{Д}}$.

4. ЯРУСНО-ПОРОГОВАЯ АДАПТАЦИЯ МАЖОРИТАРНЫХ УВС

Результаты ДФ-декомпозиции позволяют получить максимальные значения показателей безотказности систем, выбрать оптимальное число ярусов, которое может быть весьма велико (сотни ярусов). В системах $S_{\text{Т}}^{\text{Ц}}$ это приводит к резкому увеличению длительности процесса поиска работоспособной конфигурации, что неприемлемо для УВС реального времени. Исследуем способ снижения влияния данного фактора на безотказность одноверсионных систем на основе использования систем с ярусно-пороговой адаптацией $S_{\text{Т}}^{2\text{А}}$ (см. п. 2). Поскольку время восстановления (реконфигурации) является возрастающей функцией k во всем диапазоне изменения числа ярусов, то предлагается варьировать значением k в зависимости от режима функционирования системы (r_φ):

$$k = \begin{cases} k_{\text{opt}}, & \text{при } r_\varphi = 0, \\ k_{\text{opt}}/x, & \text{при } r_\varphi = 1, \end{cases} \qquad (14)$$

где $1 \le x \le k_{\text{opt}}$. Величина x выбирается согласно неравенству

$$T_{\text{рк}}(x, k_{\text{opt}}) \le T_{\text{рк}}^{\text{доп}}.$$

На рис. 3 показан пример архитектуры системы с ярусно-пороговой адаптацией и централизованными средствами управления контролем и реконфигурацией (ЦСКР). В этой системе в режиме поиска работоспособной конфигурации путем подачи тестовых сигналов x и анализа выходных реакций $z_{\text{Т}j}$, $j = 1, 2, 3$, число ярусов может быть уменьшено в x раз ($x = 2$) за счет перевода средств коммутации K_ρ ($\rho = 2\varepsilon - 1$, $\varepsilon = 1, \ldots, k/2$) в состояние транзита сигналами $r_{\varphi\rho} = 1$. Конфигурация ярусов, состоящих из фрагментов ΔV_{ij}, $i = 1, 2, \ldots, k$ задается управляющими сигналами u_{i}. Ярусы могут иметь три конфигурации: мажоритарную (до появления второго отказа), одноканальную (после отказов двух каналов яруса и завершения диагностирования) и транзитную (в процессе диагностирования).

Обратимся к первому слагаемому $Q_{\text{А}}$ формулы (4), в котором коэффициент $3k$ в вычитаемом в скобках указывает на максимально возможное число одноканальных конфигураций. Перейдем к выражению для вероятности правильного функционирования:

$$P(\widetilde{S}_{\text{Т}}^{\text{Ц}}) = P_{\text{П}}P_{\xi\text{ц}}\prod_{\text{i}=1}^{k}[3P_{\text{ффi}}^2 - 2P_{\text{ффi}}^3 +$$

$$+ 3P(1 - P_{\text{ффi}})^2P_{\xi\text{яi}}P_{\text{ксi}}P_{\text{рki}}], \qquad (15)$$

где $P_{\xi\text{яi}}$ — вероятность безотказной работы средств управления реконфигурацией i-го яруса; $P_{\text{ксi}}$ — вероятность правильной классификации состояния

i-го яруса; $P_{\text{рк}i}$ — вероятность того, что реконфигурация i-го яруса будет выполнена за время, не превышающее $T_{\text{рк}}^{\text{доп}}$. Эта вероятность может вычисляться следующим образом:

$$P_{\text{рк}i} = \begin{cases} 1, & \text{если } T_{\text{рк}i} \le T_{\text{рк}}, \\ 0, & \text{если } T_{\text{рк}i} > T_{\text{рк}}^{\text{доп}}, \end{cases} \qquad (16)$$

Вероятности $P_{\xi\text{я}i}$, $P_{\text{кс}i}$ от k зависят слабо, в то время как значение $P_{\text{рк}i}$ зависит от числа ярусов, определяющего количество возможных конфигураций. Тогда при справедливости допущения о равнонадежности ярусов выражение (15) может быть преобразовано к виду:

$$P(\widetilde{S}_{\text{Т}}^{\text{Ц}}) = P_{\text{П}} P_{\xi\Sigma\text{ц}} \sum_{\text{j}=1}^{\text{k}} \{(3P_{\text{фф}}^2 - 2P_{\text{фф}}^3)^{\text{k}-\text{j}} \times$$

$$\times [P_{\text{фф}}(1 - P_{\text{фф}})^2]^{\text{j}} \sum_{\text{v}=1}^{\text{M(j,k)}} P_{\text{рк}\text{v}}\}, \qquad (17)$$

где $P_{\xi\Sigma\text{ц}} = P_{\xi\text{ц}} P_{\xi\text{я}}^{\text{k}}$, $M(i, k)$ — число одноканальных конфигураций k-ярусной системы с j ярусами, содержащими два отказавших фрагмента. Формула (17) дает нижнюю оценку при $P_{\xi\text{я}} = P_{\xi\text{я}i}$, $P_{\text{кс}i} = P_{\text{кс}} = 1$.

При отсутствии ограничений на время восстановления $T_{\text{рк}}$ справедливо

$$\sum_{\text{v}=1}^{\text{M(j,k)}} P_{\text{рк}\text{v}} = C_{\text{k}}^{\text{j}} 3^{\text{j}}. \qquad (18)$$

При наличии ограничений на время $T_{\text{рк}}^{\text{доп}}$ будет проверено $M_{\text{доп}} = \lceil T_{\text{рк}}^{\text{доп}} / \tau \rceil$ конфигураций (τ — время проверки одной конфигурации, $\lceil a \rceil$ — ближайшее целое число, не меньшее, чем a), и выражение (18) преобразуется следующим образом:

$$\sum_{\text{v}=1}^{\text{M(i,j)}} P_{\text{рк}\text{v}} = \begin{cases} C_{\text{k}}^{\text{j}} 3^{\text{j}}, \text{ если } \dfrac{T_{\text{рк}}^{\max}(j, k)}{\tau} \le M_{\text{доп}}, \\ C_{\text{k}}^{\text{j}} 3^{\text{j}}, \text{ если } \dfrac{T_{\text{рк}}^{\max}(j, k)}{\tau} > M_{\text{доп}}, \\ \qquad \text{и } C_{\text{k}}^{\text{v}} 3^{\text{v}} \le M_{\text{доп}}, \\ C_{\text{k}}^{\text{j}} 3^{\text{j}} - (C_{\text{k}}^{\text{v}} 3^{\text{v}} - M_{\text{доп}}), \text{ если } \dfrac{T_{\text{рк}}^{\max}(j, k)}{\tau} > M_{\text{доп}}, \\ \qquad \text{и } \sum_{\text{v}=1}^{\text{j}} C_{\text{k}}^{\text{v}} 3^{\text{v}} > M_{\text{доп}}, \\ 0, \text{ если } C_{\text{k}}^{\text{j}} 3^{\text{j}} - (C_{\text{k}}^{\text{v}} 3^{\text{v}} - M_{\text{доп}}) \le 0 \text{ и } j \ge 1, \\ 1, \text{ если } C_{\text{k}}^{\text{j}} 3^{\text{j}} - (C_{\text{k}}^{\text{v}} 3^{\text{v}} - M_{\text{доп}}) \le 0 \text{ и } j = 0, \end{cases} \qquad (19)$$

где $T_{\text{рк}}^{\max}(j, k)$ — максимально возможное число конфигураций, которое необходимо проверить при отказе двух фрагментов в j ярусах. Следует подчеркнуть, что формулы (17)—(19) учитывают не только уровень безотказности всех элементов системы, но и динамические характеристики средств диагностирования и реконфигурации путем уменьшения числа слагаемых, определяющих прибавку в безотказности за счет перехода в одноканальную конфигурацию.

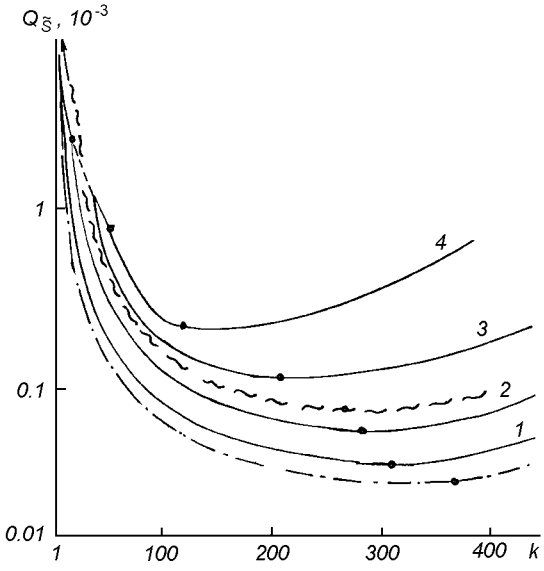

Рис. 4. Зависимости вероятности отказа систем с одно- и двупараметрической адаптацией от числа ярусов при различных ограничениях на время реконфигурации при $\lambda_{\text{фэ}} t = 5 \cdot 10^{-5}$, $P_{\text{П}} = 1$, $n_{\text{ф}} = 1500$, $a_{\text{ц}} = 50$, $b_{\text{ц}} = 0.01$. Кривая *1* — для $S_{\text{Т}}^{1\text{A}}$, сплошные кривые — для $Q(S_{\text{Т}}^{1\text{A}})$ ($n_{\xi\text{э}} = 2$), штрих-пунктирная — $Q(S_{\text{Т}}^{1\text{A}})$ ($n_{\xi\text{э}} = 1.5$), $\Delta M = 0$, волнистая — $Q(S_{\text{Т}}^{2\text{A}})$ ($n_{\xi\text{э}} = 2$), $\Delta M = 0$. Кривые *1*—*4* — для $\Delta M = 0$, 50, 100, 150 соответственно

Результаты исследования функции $Q(\widetilde{S}_{\text{Т}}^{\text{Ц}}) = 1 - P(\widetilde{S}_{\text{Т}}^{\text{Ц}})$, проведенного в соответствии с формулами (17) и (19) с учетом выражений (4)—(8), иллюстрируются рис. 4. Их анализ позволяет установить, что:

а) уменьшение величины $M_{\text{доп}}$ (увеличение $\Delta M = C_{\text{k}}^{\text{v}} 3^{\text{v}} - M_{\text{доп}}$) ведет к снижению безотказности системы и уменьшению значения k_{opt};

б) введение механизма ярусно-пороговой адаптации позволяет уменьшить минимальное значение вероятности отказа системы практически при том же значении k_{opt}. Снижения ярусности системы в x раз эквивалентно пропорциональному уменьшению значения ΔM;

в) незначительное (до 30 %) увеличение сложности управляемых мажоритарных элементов для обеспечения режима транзита и укрупнения ярусов при поиске работоспособных конфигураций не при-

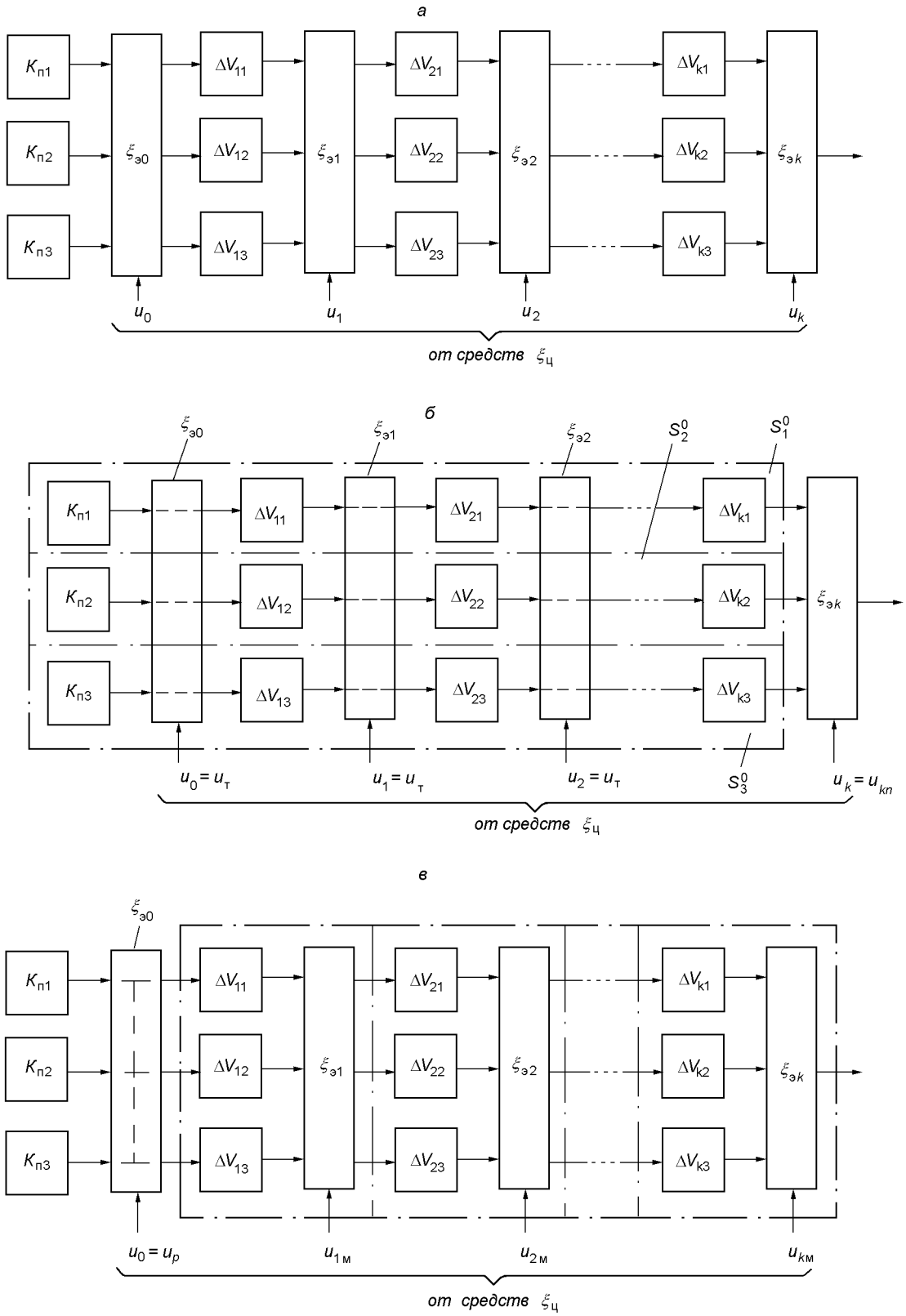

Рис. 5. Архитектура системы с ярусно-версионно-пороговой адаптацией: общая (*а*), для первого (*б*) и второго (*в*) режимов

водит к значительному увеличению вероятности отказа и уменьшению k_{opt};

г) каждому значению ΔM соответствует величина k^*, при которой становится невозможным реализация пороговой адаптации по ярусам, что эквивалентно переходу систем в режим неадаптивного функционирования.

5. ЯРУСНО-ВЕРСИОННО-ПОРОГОВАЯ АДАПТАЦИЯ МАЖОРИТАРНЫХ УВС

Ярусно-пороговая адаптация не позволяет реализовать свойство ДП-устойчивости, поскольку предполагает наличие многоярусной архитектуры, а следовательно, исключает возможность параллельного выполнения разных версий. Однако идея изменения ярусности может быть применена для повышения ДФ-устойчивости или увеличения ДП-устойчивости МВС. При разработке способа ярусно-версионной адаптации МВС учтено три обстоятельства: во-первых, такие системы при появлении физического дефекта аппаратного компонента любой версии теряют частично или полностью (при $e = 3$) свойство ДП-устойчивости; во-вторых, в них исключается возможность раздельного резервирования аппаратных компонентов, осуществляющих обработку данных по единому алгоритму; в-третьих, область выигрыша в ДП-устойчивости МВС по отношению к одновариантным системам ограничена во времени, и тем больше, чем надежнее их аппаратные компоненты [11]. Следовательно, необходим механизм адаптации, позволяющий на некотором начальном этапе применения УВС функционировать в многоверсионной конфигурации, а затем по мере накопления дефектов аппаратных компонентов переходить к работе по однотипным версиям. Суть метода ярусно-версионной (ярусно-версионно-пороговой) адаптации иллюстрируется архитектурой системы с ЦСКР (рис. 5). Ее общий вид показан на рис. 5, *а*, где $K_{\Pi j}$, $j = 1, 2, 3$ — программные компоненты версий, $\xi_{эi}$ — средства мажоритирования и коммутации, управляемые централизованными средствами $\xi_{ц}$ с помощью сигналов u_i.

В первом режиме система функционирует как МВС (рис. 5, *б*), которые реализуются подсистемами $S_j^0 = \{\Delta V_{ij}\ (i = 1, ..., k), K_{\Pi j}\}$. При этом средства выполнения функций $\xi_{эi}$ переводятся в режим транзита ($u_v = u_T$, $v = 0, ..., k - 1$) образуя независимые подсистемы S_j^0, выходные сигналы которых мажоритируются средствами $\xi_{эк}$ ($u_к = u_{iм}$).

При появлении первого физического дефекта фрагментов ΔV_{ij}, исключающего возможность парирования ДП, система переводится в многоярусную конфигурацию (рис. 5, *в*), в которой все каналы системы реализуют одну версию, задаваемую, например, компонентом $K_{\Pi 1}$ с помощью сигнала $u_р$. Конфигурация ярусов формируется затем с учетом состояния фрагментов ΔV_{ij} сигналами $u_{iм}$ аналогично тому, как это описано выше для систем с ярусно-пороговой адаптацией.

Рассмотренным конфигурациям при условии справедливости экспоненциальных законов возникновения ДФ и проявления ДП соответствуют структурные схемы надежности, показанные на рис. 6. В первой конфигурации фильтруются последствия относительных ДП, проявляющихся с интенсивностью $\lambda_{ПОj}$, во второй — последствия ДФ раздельно мажоритируемых аппаратных компонентов (интенсивность их возникновения по фрагментам равна $\lambda_{ффi}$). Во второй конфигурации в одном из ярусов имеется отказавший фрагмент. Вероятность правильного функционирования системы $\widetilde{S}_T^{3A}$ с ярусно-версионно-пороговой адаптацией равна

$$P(\widetilde{S}_T^{3A}) = (P_I P_{\tilde{S}I} + P_{II} P_{\tilde{S}II}) P_{\xi ц}, \qquad (20)$$

где P_I (P_{II}) — вероятность нахождения системы в первой (второй) конфигурации; $P_{\tilde{S}I}$($P_{\tilde{S}II}$) — вероятность правильного функционирования системы в первой (второй) конфигурации.

Формула (20) дает нижнюю оценку с учетом того, что она получена при условии, что любой отказ ЦСКР ведет к отказу системы.

Для случая равнонадежных и идеальных фрагментов ярусов имеем

$$P_I = P_{фф}^{3k}, \qquad (21)$$

$$P_{\tilde{S}I} = (3P_{по}^2 - 2P_{по}^3) P_{па} P_{\xi эк}, \qquad (22)$$

$$P_{II} = 3k(1 - P_{фф}) P_{фф}^{3k-1}, \qquad (23)$$

$$P_{\tilde{S}II} = [P_{фф}^2 + 2P_{фф}(1 - P_{фф}) D_{кф}] [3P_{фф}^2 - 2P_{фф}^3 + 3P_{фф}(1 - P_{фф})^2 D_{кф}]^{k-1} P_{по} P_{па}, \qquad (24)$$

где $P_{по} \approx 1 - \alpha\beta\lambda_ф t$, $P_{па} \approx 1 - \alpha(1 - \beta)\lambda_ф t$, α и β — коэффициенты ДП и абсолютных ДП соответственно [8].

С учетом (20)—(24) получим

$$P(\widetilde{S}_T^{3A}) = P_{фф}^{3k} P_{\xi ц} P_{па} \{(3P_{по}^2 - 2P_{по}^3) P_{\xi эк} + 3k(1 - P_{фф})[P_{фф} + 2(1 - P_{фф}) D_{кф}] [3P_{фф}^2 - 2P_{фф}^3 + 3P_{фф}(1 - P_{фф})^2 D_{кф}]^{k-1} P_{по}\}. \qquad (25)$$

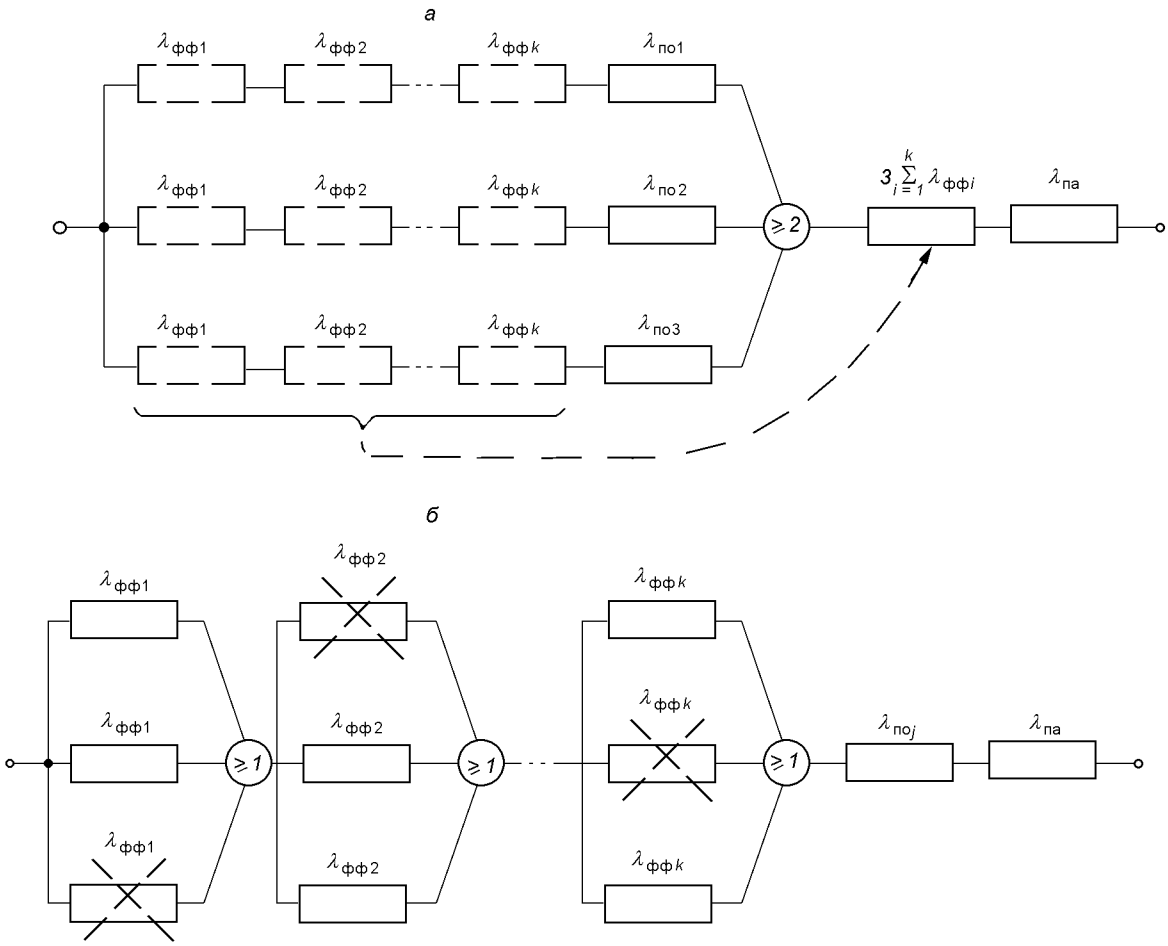

Рис. 6. Структурные схемы надежности системы с ярусно-версионно-пороговой адаптацией для первого (*а*) и второго (*б*) режимов

Исследуем зависимость вероятности $P(\widetilde{S}_{\text{Т}}^{\text{3А}})$ от основных аргументов, учитывая формулы (6)—(8). Исследование функции (25) показывает, что:

а) характер изменения значения k_{opt} в системах с ярусно-версионной адаптацией в зависимости от сложности альтернативных версий $n_{\text{ф}}$ и мажоритарных ярусов $n_{\xi_{\text{э}}}$ аналогичен системам с однопараметрической пороговой адаптацией. С увеличением $n_{\text{ф}}$ и уменьшением $n_{\xi_{\text{э}}}$ величина k_{opt} в системах $\widetilde{S}_{\text{Т}}^{\text{3А}}$ увеличивается;

б) увеличение коэффициентов α и β снижает Д-устойчивость систем $S_{\text{Т}}^{\text{3А}}$, оптимальное число ярусов при переходе во вторую конфигурацию при этом не изменяется;

в) в отличие от систем с однопараметрической адаптацией изменение (уменьшение) параметра $\lambda_{\text{фэi}}$ в системах $S_{\text{Т}}^{\text{3А}}$ влияет на величину k_{opt} (вызывает его увеличение);

г) использование систем с ярусно-версионно-пороговой адаптацией обеспечивает существенное (при определенных условиях в 3—5 раз) увеличение Д-устойчивости (устойчивости к дефектам как аппаратных, так и программных средств), проигрывая им незначительно в ДФ-устойчивости (безотказности).

На рис. 7 показан график зависимости вероятности отказа $Q(\widetilde{S}_{\text{Т}}^{\text{2А}})$ системы, реализующей два режима аналогично системе $\widetilde{S}_{\text{Т}}^{\text{3А}}$ с той разницей, что в первом режиме, как и во втором, выполняются одинаковые версии. Проигрыш в ДФ-устойчивости показан штриховкой;

д) системы с ярусно-версионно-пороговой адаптацией целесообразно использовать в бортовых УВС с длительным периодом функционирования, разделяемым на два этапа — с реализацией более сложных алгоритмов на первом (относительно непродолжительном) этапе, когда выполняются раз-

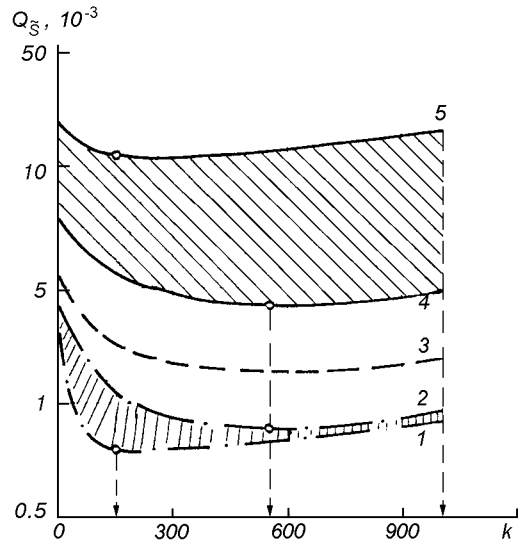

Рис. 7. Зависимости вероятности отказа систем с одно- и многопараметрической адаптацией от числа ярусов при $\lambda_{\text{фэ}}t = 5 \cdot 10^{-5}$, $n_{\text{ф}} = 1000$, $n_{\tilde{\text{ф}}\text{э}} = 3$, $D_{\text{кФ}} = 0.8$, $a_{\text{ц}} = 50$, $b_{\text{ц}} = 0.01$. Кривые *1* и *5* — для $S_{\text{T}}^{1\text{A}}$, *2* — для $S_{\text{T}}^{2\text{A}}$, *3* и *4* — для $S_{\text{T}}^{3\text{A}}$; кривые *1* и *2* — для $\alpha = \beta = 0$; *3* — для $\alpha = 0.1$, $\beta = 0.01$; *4* и *5* — для $\alpha = 0.3$, $\beta = 0.1$

личные версии и обеспечивается парирование ДП, и переходом к многоярусной одноверсионной архитектуре на более продолжительном втором этапе, на котором нейтрализуются последствия ДФ фрагментов путем пороговой адаптации. При наличии жестких ограничений на время восстановления во втором режиме следует использовать метод ярусно-пороговой адаптации. Возможны и другие стратегии выбора способа адаптации в зависимости от режима, продолжительности функционирования и задач бортовых УВС.

6. ЗАКЛЮЧЕНИЕ

1. При решении задачи ДФ-декомпозиции МВС, являющейся составной частью общей задачи оптимального резервирования, должны учитываться не только характеристики безотказности аппаратных компонентов версий, но и характеристики средств контроля и реконфигурации, поскольку от их значений существенно зависит оптимальное число ярусов (фрагментов) и минимальные значения вероятности отказа. Переход к МВС с децентрализованными (или групповыми) средствами следует производить при превалировании ограничения на время реконфигурации.

2. Отличительной особенностью предложенных методов многопараметрической адаптации является управляемое варьирование значениями нескольких параметров, влияющих на Д-устойчивость и другие свойства МВС в зависимости от режима функционирования, числа и номенклатуры дефектов. Это дает возможность реализации различных версий на начальном этапе с последующим переходом к многоярусной тривиальной архитектуре, обеспечивающей максимальную ДФ-устойчивость и минимизирующей временные затраты на поиск работоспособной конфигурации. Количественные оценки Д-устойчивости (ДФ-устойчивости) систем с ярусно-пороговой и ярусно-версионной адаптацией позволяют определить достигаемый эффект при различных значениях параметров аппаратных и программных компонентов и уточнить области целесообразного применения. Для приведенных в статье исходных данных вероятность отказа при использовании предложенных методов уменьшается на 40—50 %.

3. Системы с многопараметрической адаптацией по аналогии с контролепригодными системами могут быть названы реконфигуропригодными. Степень реконфигуропригодности определяется мощностью множеств формируемых конфигураций и качеством соответствующих алгоритмических и технических средств.

4. Техническая реализация средств контроля и реконфигурации для рассмотренных адаптивных мажоритарных систем (рис. 3) может быть осуществлена на основе устройств, описанных в авторских свидетельствах [1, 2]. Это позволяет в 1.3—1.8 раз уменьшить среднее время и в 2—5 раз — максимальное время реконфигурации.

5. Учитывая особенности современной элементной базы, используемой при проектировании бортовых УВС, (ПЛИС, микропроцессорные БИС и СБИС, матричные многопроцессорные СБИС и другие), ярусы резервирования могут полностью или частично реализовываться на внутрикристаллическом уровне, причем число ярусов и кратность резервирования уменьшается. Вследствие этого:

а) более целесообразным является использование версионно-пороговой и версионной адаптации;

б) при выборе и реализации вариантов многопараметрической адаптации необходимо учитывать зависимость между отказами элементов, относящихся к одному или нескольким ярусам;

в) возможна многопараметрическая адаптация, для которой функция адаптации связывает число задач, реализуемых, например, в систолической матричной СБИС, с числом отказавших элементов (процессоров).

1. А. с. 1633233 СССР, МКИ G06F9/22, 11/18. Устройство для управления диагностированием и восстановлением цифровых систем / В. И. Свищ, Н. Ф. Сидоренко, В. С. Харченко и др. — Опубл. 28.01.91, Бюл. № 4.
2. А. с. 1741295 СССР, МКИ G06F9/22. Система для программного управления резервированными объектами / Н. К. Байда, В. С. Харченко, Г. Н. Тимонькин и др. — Опубл. 14.06.92, Бюл. № 22.
3. Доманицкий С. М. Построение надежных логических устройств. — М.: Энергия, 1971.—279 с.
4. Колесников В. Н. Оптимальный синтез многоканальных структур ЦВМ. — М.: Сов. радио, 1976.—176 с.
5. Кривоносов А. И., Байда Н. К., Харченко В. С. и др. Структура, организация и модели мажоритарно-резервированных систем // Космическая наука и технология.—1996.—№ 1.—С. 71—76.
6. Харченко В. С. Модели и свойства отказоустойчивых многоальтернативных систем // Автоматика и телемеханика.—1992.—№ 12.—С. 140—147.
7. Харченко В. С. Теоретические основы дефектоустойчивых цифровых систем с версионной избыточностью. — Харьков: Изд-во ХВУ, 1995.—506 с.
8. Харченко В. С. Выбор технологии проектирования и базовых архитектур дефектоустойчивых цифровых управляющих и вычислительных систем реального времени // Космічна наука і технологія.—1997.—3, № 5/6.—С. 109—119.
9. Харченко В. С., Кукуруза В. Л. Многоальтернативные отказоустойчивые системы со встроенными микрореконфигураторами // Методы и системы диагностики. — Саратов: Сар. гос. ун-т, 1990.—С. 41—43.
10. Харченко В. С., Литвиненко В. Г. Модели парирования дефектов проектирования программно-аппаратных средств в необслуживаемых системах // Электронное моделирование.—1992.—№ 3.—С. 34—39.
11. Харченко В. С., Литвиненко В. Г., Терещенков С. В. Обеспечение устойчивости управляющих и вычислительных систем к физическим дефектам и дефектам проектирования программно-аппаратных средств // Зарубежная электроника.—1992.—№ 6.—С. 18—35.
12. Харченко В. С., Никольский С. Б., Сазонов А. Е. Один подход к синтезу микроконтроллерных сетей // Автоматика и вычислительная техника.—1989.—№ 4.—С. 87—95.
13. Laprie J.-C. Dependability Handbook // Laboratory for Dependability Engineery. LAAS Report.—1998.—N 98-346.—365 p.

METHODS OF THE MULTIPARAMETRIC ADAPTATION OF SPACEBORNE CONTROL AND COMPUTING SYSTEMS WITH SEPARATE MAJORITY RESERVATION

V. S. Kharchenko, A. P. Zenin, and V. V. Sklyar

We generalize the architectures of spaceborne digital fault-tolerant systems (FTS) with separate majority reservation (SRM) and three adaptive parameters (the threshold of recovering unit, number of reservation levels and number of software versions). The results of the studies of the SRM FTS with the level-threshold and level-version-threshold adaptation are presented.