Космічна наука і технологія, 1995, 1, № 1

УДК 621.03

Структурно-алгоритмическая организация и модели надежности мажоритарно-резервированных систем

А. И. Кривоносов[1], А. А. Кулаков[1], Н. К. Байда[1], В. С. Харченко[2], Н. П. Благодарный[2]

[1]НВО «Хартрон», Харків
[2]Харківский військовий університет

Надійшла до редакції 21.06.95

В статье приводятся результаты исследований по структурной организации бортовых управляющих вычислительных систем с мажоритарной архитектурой, влиянию объема универсального оборудования на надежностные характеристики неадаптивных мажоритарных архитектур. Приводятся надежностные оценки адаптивных мажоритарных структур с межканальным и внешним контролем, сведения о реализации этих структур при разработке специализированных ЭВМ в КБ Хартрон-ВИЭТ (Харьков).

ВВЕДЕНИЕ

Стремительный рост размерности задач, решаемых на борту космических аппаратов, и исключительно высокая цена отказов бортовых вычислительных средств делают проблему обеспечения надежности бортовых управляющих вычислительных систем (БУВС) одной из важнейших. Надежностные характеристики БУВС должны удовлетворять следующим требованиям:

— высокая вероятность безотказной работы БУВС в течение заданного времени;
— отказ одного элемента не должен приводить к отказу БУВС в целом;
— отказ оборудования одного из информационных каналов не должен приводить к потере всей информации;
— низкая вероятность возникновения сбоя при передаче информации;
— принципиальная возможность исключения отдельных режимов (деградация) при отказах элементов.

Наиболее эффективным подходом к удовлетворениям этих требований является многоярусное 3-канальное резервирование БУВС (Половко, 1964). В ряде случаев резервирование сопровождается адаптацией (перестройкой на исправный канал при двух отказавших каналах) на наиболее сложных по оборудованию ярусах (Кривоносов, 1990).

В настоящее время актуальными вопросами развития теории и практики мажоритарно-резервированных структур (МРС) БУВС КА являются:

— исследование влияния на надежностные характеристики соотношения универсального и функционального оборудования;
— определение надежностных характеристик адаптивных МРС.

Рассмотрению этих вопросов и посвящается работа.

СТРУКТУРНО-АЛГОРИТМИЧЕСКАЯ ОРГАНИЗАЦИЯ МРС

Организация МРС в наиболее общем случае различается по уровню, на котором проводится мажори-

тирование и по наличию адаптации. По уровню мажоритирования МРС подразделяются на:

— структуры с мажоритированием на уровне каналов (структуры I типа);
— структуры с мажоритированием на уровне блоков (структуры II типа);
— структуры с мажоритированием на уровне функциональных узлов (структуры III типа);
— комбинированные структуры (структуры IV типа), в которых использованы решения структур II и III типов.

По наличию адаптации МРС подразделяются на:

— структуры без адаптации;
— структуры с адаптацией на всех уровнях мажоритирования;
— комбинированные структуры с адаптацией на отдельных уровнях.

В зависимости от способа организации управления средствами контроля и реконфигурации (СРК) и от степени доступа управляющих воздействий к аппаратным средствам каналов существует несколько типов адаптивных МРС (АМРС) (рис. 1). Применение конкретной структуры определяется сложностью каналов МРС, СКР, временем тестирования.

МАТЕМАТИЧЕСКИЙ АППАРАТ ИССЛЕДОВАНИЙ

Обозначим через T общее время функционирования МРС, которое состоит из n равных промежутков t_k, каждый из которых соответствует шагу исследуемого процесса. При проведении в моменты 1,2,..., контроля объекта получим последовательность экспериментов. Каждый эксперимент имеет конечное число возможных исходов l. Тогда МРС может быть описана простой цепью Маркова (Кривоносов, 1990).

Для описания процесса воспользуемся векторно-матричной формой записи. Чтобы полностью определить марковскую цепь с возможными состояниями, нужно задать стохастическую матрицу вероятностей перехода $\mathbf{A}$ l-го порядка и l-мерный вектор начальных условий

$$\mathbf{A} = \left| a_{ij} \right| = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1l} \\ a_{21} & a_{22} & \dots & a_{2l} \\ \dots & \dots & \dots & \dots \\ a_{l1} & a_{l2} & \dots & a_{ll} \end{vmatrix},$$

$$\overline{P}(0) = \left| P_1(0), P_2(0), \dots, P_n(0), \dots, P_l(0) \right|,$$

где a_{ij} — условные вероятности перехода объекта из состояния i в состояние j; $P_i(0)$ — безусловная вероятность нахождения объекта в i-м состоянии в начальный момент времени.

Матрица $\mathbf{A}$ характеризует процесс снижения надежности за время t_k.

Так как объект внутри периода не контролируется и не восстанавливается,то переход из состояния с большим номером в состояние с меньшим номером невозможен и $\mathbf{A}$ является верхней треугольной стохастической матрицей, то есть

$$a_{ij} = 0 \quad \text{при } i > j,$$

$$0 < a_{ij} \le 1 \quad \text{при } i \le j,$$

$$\sum_{j=1}^{l} a_{ij} = 1.$$

На любом n-м шаге процесса вектор-строка $\overline{P}(n)$ определяется выражениями

$$\overline{P}(n) = \overline{P}(n-1)A^n = \overline{P}(0)A^n$$

— для однородной цепи Маркова,

$$\overline{P}(n) = \overline{P}(0)\prod_{i=1}^{n} A_i^n$$

— для неоднородной цепи Маркова.

Расположим компоненты вектора $\overline{P}(n)$ и строк матрицы $\mathbf{A}$ в порядке увеличения количества отказавших элементов (то есть номеру 1 соответствует состояние, когда все элементы исправны, номеру 2 — состояние, в котором один элемент отказал, а остальные исправны и т. д.). Тогда вероятность $P_{МРС}(n)$ исправного состояния МРС на n-м шаге процесса определяется вероятностями нахождения в состояниях подмножества x_1

$$P_{МРС}(n) = \sum_{i=1}^{\eta} P_i(n),$$

где $P_i(n)$ — компоненты вектора-строки $\overline{P}(n)$.

Обозначим через X_1 подмножество благоприятных состояний ($x_1 = \{1, 2, \dots, \eta\}$), а через X_2 — подмножество неблагоприятных состояний ($x_2 = \{\eta + 1, \eta + 2, \dots, l\}$).

МОДЕЛИ НАДЕЖНОСТИ МРС

Введем определения универсального и функционального оборудования МРС.

Универсальное оборудование (УО) — совокупность средств канала, отказ которых не допускает наличия отказов в любом оборудовании остальных каналов МРС.

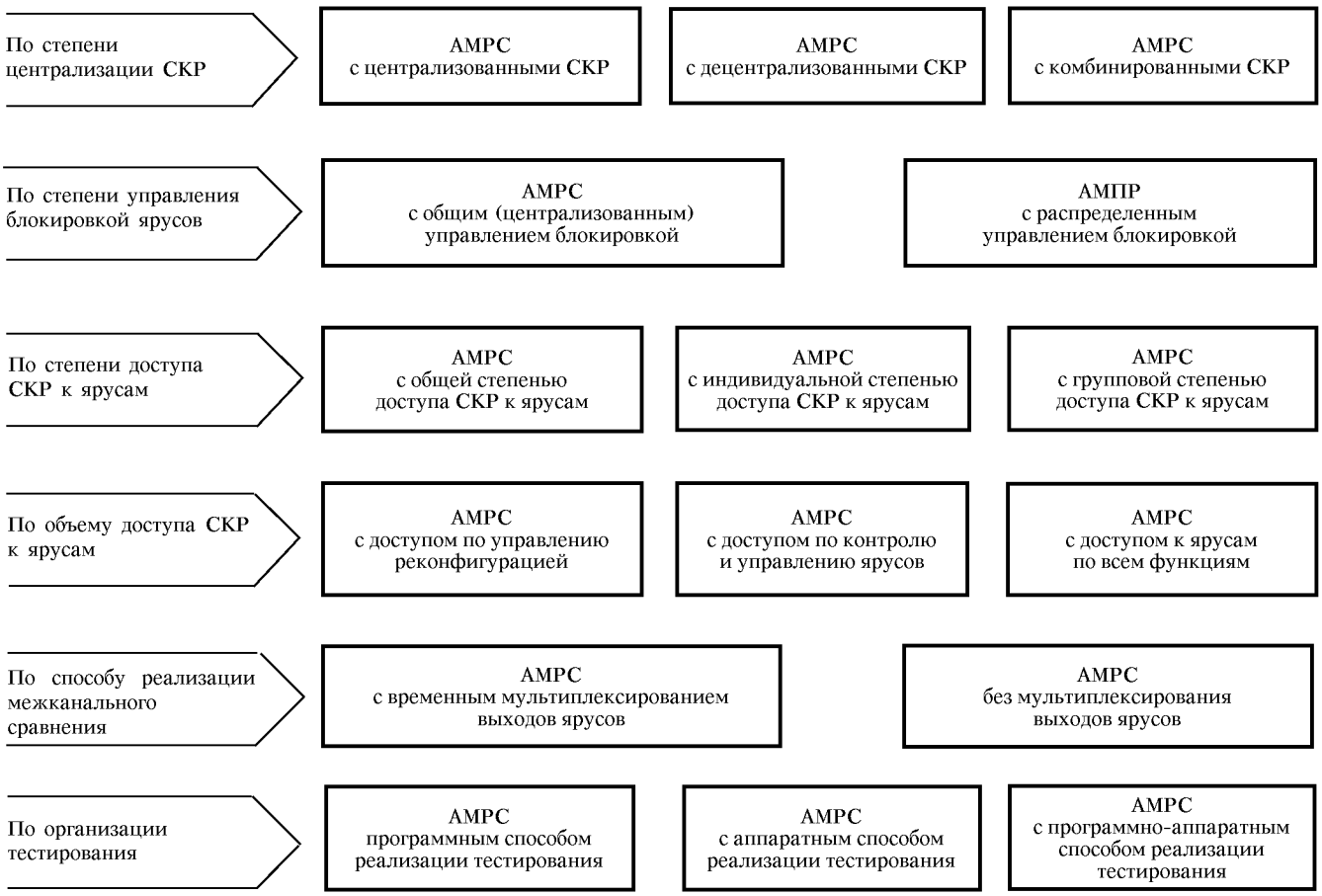

Рис. 1. Классификация типов адаптивных мажоритарно-резервированных структур (АМРС)

Функциональное оборудование (ФО) — совокупность средств, отказ которых в одном канале допускает еще наличие отказов в функциональном оборудовании других каналов, выполняющем другие функции (например, отказы различных разрядов выходных регистров каналов при наличии обмена снимаемой с них информации являются отказами функционального оборудования. В то же время отказ цепи синхронизации регистра — отказ универсального оборудования).

Структуры I типа (рис. 2) содержат в каждом канале только УО, так как мажоритарный орган находится на выходе процессора и любые отказы в двух каналах приводят к неработоспособности структуры. Структуры II типа (рис. 3) содержат в своем составе как УО, так и ФО. Структуры III типа являются с точки зрения надежности частным случаем структур II типа (в ярусе полностью отсутствует УО).

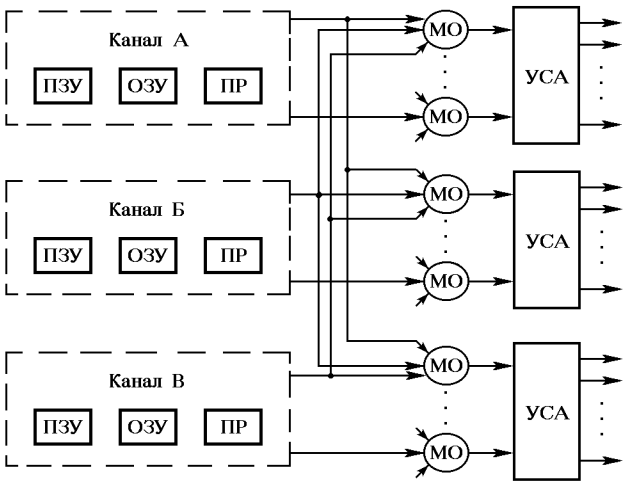

Рис. 2. Структуры I типа

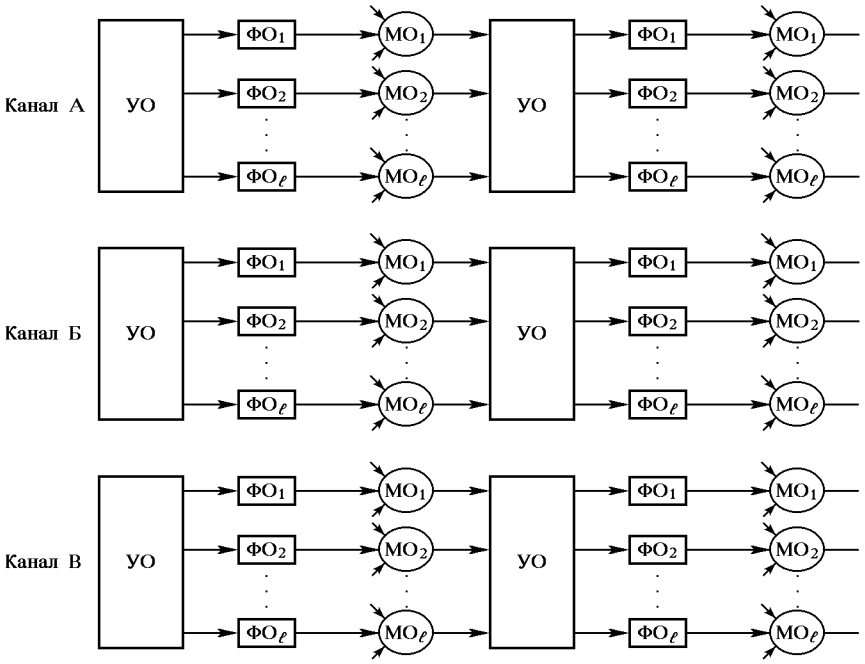

Рис. 3. Структуры II типа

Для структур I типа матрица A определяется выражением

$$\mathbf{A} = \begin{vmatrix} p^3 & 3p^2q & 3q^2p & q^3 \\ 0 & p^2 & 2pq & q^2 \\ 0 & 0 & p & q \\ 0 & 0 & 0 & 1 \end{vmatrix}.$$

Тогда вероятность $P_{\text{I}}(n)$ исправного состояния структуры I типа определяется выражением:

$$P_{\text{I}}(n) = \sum_{i=1}^{\eta} p_i(n) = \sum_{i=1}^{2} p_i(n) = p^3 + 3p^2q,$$

где $p = p(n)$ — вероятность безотказного функционирования канала ($q = 1 - p$).

С точки зрения надежности отдельные ярусы структуры II типа можно считать независимыми. Тогда вероятность исправного состояния МРС в целом на n-м шаге процесса функционирования (то есть вероятность отсутствия искажения информации на выходе одноименных разрядов ФО) определится выражением:

$$P_{\text{II}}(n) = \prod_{j=1}^{m_{\text{ЯР}}} P_{\text{ЯР}j}(n),$$

где $m_{\text{ЯР}}$ — число ярусов МРС; $P_{\text{ЯР}j}(n)$ — вероятность безотказного функционирования яруса.

Значение $P_{\text{ЯР}j}(n)$ определится выражением

$$P_{\text{ЯР}j}(n) = \sum_{i=1}^{\eta} P_{\text{УО}ji}(n) U_{ji}(n),$$

где $P_{\text{УО}ji}(n)$ — компонента вектора-строки $P_{\text{УО}j}(n)$, характеризующая вероятность нахождения УО j-го яруса в i-м состоянии; $U_{ji}(n)$ — i-я компонента вектор-столбца $U_j(n)$, характеризующая условную вероятность исправного состояния ФО j-го яруса при нахождении УО данного яруса в i-м состоянии.

Если в процессе эксплуатации осуществляется полный контроль, то $P_{\text{ЯР}j}(n)$ определится выражением

$$P_{\text{ЯР}j}(n) = P^3_{\text{УО}j}(n) \prod_{l=1}^{L} (P^3_{\text{ФО}jl}(n) + 3P_{\text{ФО}jl}(n) q_{\text{ФО}jl}) +$$

$$+ 3P^2_{\text{УО}j}(n) q_{\text{УО}j} \prod_{l=1}^{L} P^2_{\text{ФО}jl},$$

где L — количество разрядов ФО, $P_{\text{ФО}ji} = P_{\text{ФО}ji}(n)$ — вероятность исправного состояния i-го разряда ФО в j-м ярусе.

Из уравнения для $P_{\text{ЯР}j}(n)$ видно, что надежность яруса существенно зависит от доли κ УО в данном ярусе

$$\kappa = \frac{\Lambda_{\text{УО}_{\text{ЯР}}}}{\Lambda_{\text{УО}_{\text{ЯР}}} + \Lambda_{\text{ФО}_{\text{ЯР}}}} = \frac{\Lambda_{\text{УО}_{\text{ЯР}}}}{\Lambda_{\text{ЯР}}},$$

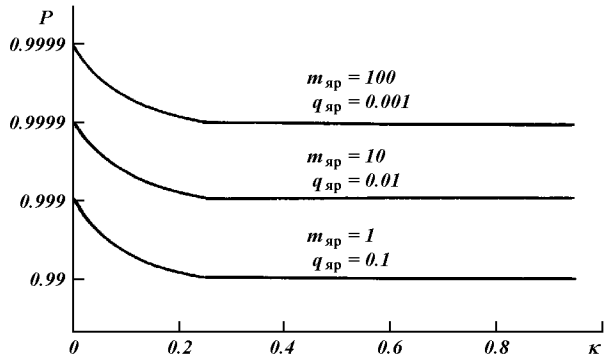

Рис. 4. Зависимость $P_{\text{II}}(n)$ от n при $L = 16$.

где $\Lambda_{\text{ЯР}}$ — интенсивность отказов оборудования яруса; $\Lambda_{\text{УО(ФО)ЯР}}$ — интенсивность отказов универсального (функционального) оборудования яруса.

На рис. 4 приведена зависимость $P_{\text{II}}(n)$ от n при $L = 16$. Очевидно, что увеличение доли УО ($к$) с 0.1 до 0.5 приводит к увеличению вероятности отказа яруса $Q_{\text{ЯР}}$ примерно в три раза. Следовательно, повышение надежности яруса может быть достигнуто уменьшением доли УО (в пределе его исключением (переход к структурам III типа).

В структурах III типа разряды ФО становятся независимыми и разряды одного яруса можно рассматривать как самостоятельные ярусы в системе. При этом в сравнении со структурой II типа количество ярусов вырастет до величины $M_{\text{ЯР}}$,

$$M_{\text{ЯР}} = m_{\text{ЯР}} n_{\text{р}},$$

где $m_{\text{ЯР}}$ и $n_{\text{р}}$ — количество ярусов и разрядов ФО в структуре III типа и вероятность $P_{\text{III}}(n)$ определяется произведением

$$P_{\text{III}}(n) = \prod_{i=1}^{M_{\text{ЯР}}} p_{\text{ЯР}_i}(n).$$

Для процесса эксплуатации с полным контролем и без учета сбоев

$$p_{\text{ЯР}_i}(n) = p_{\text{ЯР}}(n) = p^3 + 3P^2 q.$$

Поскольку количество оборудования в ярусе в сравнении со структурами I и II типов резко сократилось, то даже простой по реализации мажоритарный орган (МО) составляет ощутимую долю в оборудовании ярусов. Кроме того, общее количество МО также возрастает. Эти обстоятельства приводят к необходимости специального учета надежности МО в структуре III типа. Так как отказ МО равноценен отказу любого элемента в канале яруса, то надежность МО может быть учтена путем соответствующего увеличения вероятности отказа канала яруса q до величины q_1:

$$q_1 \approx q + q_{\text{МО}} = q(i + K_{\text{МО}}),$$

где $q_{\text{МО}}$ — вероятность отказа МО в канале яруса; $K_{\text{МО}}$ — коэффициент, учитывающий долю оборудования МО в канале яруса.

Тогда значение $P_{\text{ЯР}}(n)$ определится выражением

$$p_{\text{ЯР}}(n) = p_1^3 + 3p_1^2 q_1.$$

Снижение уровня мажоритирования позволяет повышать уровень надежности за счет более полного использования избыточности 3-канальной структуры. Однако реализация этого направления наталкивается на ряд ограничений:

— увеличивается оборудование каналов за счет дополнительных МО;

— появляется значительное число дополнительных связей между каналами;

— уменьшается быстродействие за счет задержек сигналов на МО;

— ухудшается возможность полного контроля.

НАДЕЖНОСТНЫЕ МОДЕЛИ АДАПТИВНЫХ МРС

Теоретически адаптация может быть реализована в любой из структур. Практически же реализация адаптации на всех уровнях мажоритирования в структурах II и III типов является очень сложной задачей в связи с резким усложнением оборудования. Поэтому реализуются комбинированные структуры с наличием адаптации на уровнях с наименьшей надежностью.

Для адаптации МРС в общем случае предусматривается два варианта алгоритма перестройки (Кривоносов, 1990):

— после 1-го отказа система перестраивается на работу по одному каналу («рабочий канал»), второй исправный канал остается в горячем резерве («запасной канал») (алгоритм 3-1-1);

— перестройка на один исправный канал производится только после отказа двух каналов (алгоритм 3-3-1).

Как показано в работе Кривоносова (1990), целесообразность использования алгоритмов 3-1-1 и 3-3-1 растет по мере увеличения полного контроля. Выбор одного из алгоритмов адаптации зависит от требований к достоверности функционирования и безотказности средств мажоритирования.

Следует заметить, что в многоярусных АМРС с

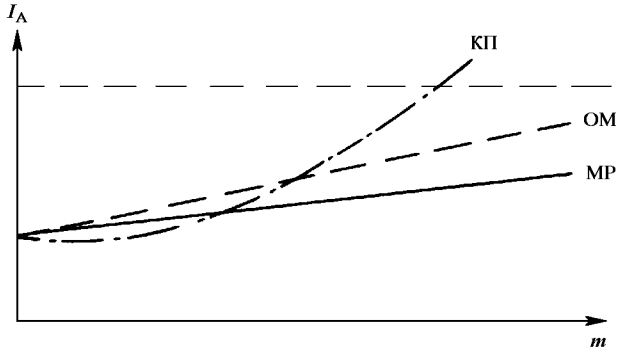

Рис. 5. Зависимость предельных времен и объема оборудования от числа ярусов

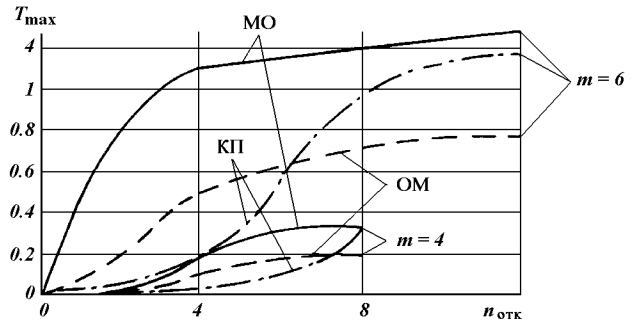

Рис. 6. Зависимость предельных времен и объема оборудования от числа отказавших фрагментов

индивидуальным доступом по управлению и общим доступом по контролю (см. рис. 1) возникает задача синтеза алгоритмов поиска работоспособных конфигураций и оценки влияния их характеристик на надежность системы. Эта задача актуальна также при разработке БУВС СУ КА, функционирующих в условиях экстремальных воздействий, когда необходимо в ограниченное время реализовать процесс «реанимации» системы. Его сердцевиной является процедура выбора работоспособной конфигурации и инициализации системы. Операционный реконфигурационный базис для синтеза алгоритмов образуют процедуры перебора (Харченко, 1992):

— от мажоритарных к одноканальным конфигурациям (МО) с максимальным временем —

$$T_{max}^{MO} = 4^m(\tau_T + \Delta\tau),$$

где τ_T — время тестирования одной конфигурации; $\Delta\tau$ — время формирования следующей конфигурации;

— от одноканальных к мажоритарным конфигурациям (ОМ), для которых

$$T_{max}^{MO} = (3^m + m)(\tau_T + \Delta\tau),$$

а также их последовательные и параллельные модификации (Харченко, 1992). Выбор процедур осуществляется с учетом ограничений на допустимое время реконфигурации и характеристик вычислительной сложности и безотказности средств аппаратно-программной поддержки. Графики зависимости предельных времен и объема оборудования от числа ярусов и числа отказавших фрагментов для процедур МО, ОМ и комбинированной процедуры (КП) показаны на рис. 5 и 6 соответственно.

ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ

В НПО «Хартрон» накоплен большой практический опыт создания высоконадежных БУВС с использованием рассмотренных стратегий резервирования. Последняя из разработок, специализированная ЭВМ М-186, обладает такими характеристиками:

Центральный процессор	на базе 80C186XL (математический сопроцессор 80C187)
Емкость ОЗУ	0.5 Мбайт
Емкость Flash-памяти	128 кбайт
Быстродействие	2.5—5 млн. коротких операций в секунду
Разрядность адрес/данные	20/16
Производительность по смеси Шаттл	350—700 тыс. оп./с
Быстродействие, Мфлопс	0.25—0.5 (определяется сопроцессором 80C187)
Совместимость с IBM PC XT/AT	снизу вверх
Обеспечение надежности	троированная структура с адаптацией на уровне магистралей, синхронная
Связь с объектами контроля и управления	дублированная шина ISA

Кривоносов А. И. Методические вопросы проектирования и эксплуатации СЦВМ. — Харьков, НПО «Электроприбор», 1990.—123 с.

Половко А. М. Основы теории надежности. — М.: Наука, 1964.—446 с.

Харченко В. С. Структурная организация отказоустойчивых и живучих систем летательных комплексов. — Харьков, 1992.—112 с.

Харченко В. С., Литвиненко В. Г., Терещенков С. В. Обеспечение устойчивости УВС к физическим дефектам и дефектам проектирования программно-аппаратных средств // Зарубежная радиоэлектроника.—1992.—№ 6.—С. 18—35.