УДК 621.396.6.019.3+519.87

Б.Ю. ВОЛОЧІЙ, Л.Д. ОЗІРКОВСЬКИЙ, О.В. МУЛЯК, М.М. ЗМИСНИЙ

Національний університет «Львівська політехніка», Україна

НАДІЙНІСНА МОДЕЛЬ ВІДМОВОСТІЙКОЇ ПРОГРАМНО-АПАРАТНОЇ СИСТЕМИ НА ОСНОВІ МАЖОРИТАРНОЇ СТРУКТУРИ З КОВЗНИМ РЕЗЕРВУВАННЯМ ТА АВТОМАТИЧНИМ ПЕРЕЗАВАНТАЖЕННЯМ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

В статті запропоновано надійнісну модель відмовостійкої програмно-апаратної системи, яка реалізована як відмовостійка система з мажоритарною структурою типу "3 з 5" та з автоматичним перезавантаженням програмного забезпечення, в роботі якого можливі збої викликані збоями апаратних засобів. До складу відмовостійкої системи входять: програмно-апаратні системи робочої конфігурації; програмно-апаратні системи ковзного резерву; мажоритарний елемент; детектор розузгодження, призначений для виявлення порушень працездатності програмно-апаратної системи; комутаційний пристрій. Модель призначена для розв'язання задач надійнісного проектування відмовостійких програмно-апаратних систем.

Ключові слова: *надійність, програмно-апаратна система, відмовостійка система, мажоритарна структура.*

Вступ

Проблема надійності програмно-апаратних систем (ПАС) довготривалого і безперервного використання, для яких недопустимими є збої в роботі, вирішується шляхом використання мажоритарних структур (МС) [1 – 3]. Ця проблема має свою специфіку, так як необхідно передбачити захист від відмов апаратних засобів (АЗ) та збоїв АЗ, які спричиняють збої програмного забезпечення (ПЗ). Відновлення працездатності ПАС в таких випадках здійснюється шляхом перезавантаження ПЗ. В практиці проектування ПАС з МС довготривалого і безперервного використання властивість відмовостійкості АЗ забезпечують використанням МС з фіксованим правилом прийняття рішень і ковзним резервуванням системи [1, 2], або реконфігурацією ядра МС [7]. Щоб уникнути однотипних збоїв у всіх ПАС ядра МС, використовуються версії ПЗ від різних розробників [4]. Такі відмовостійкі системи використовуються: в системі аварійного захисту на атомних електростанціях; в системах централізованого контролю об'єктів метрополітену або промислових підприємств [2]; в бортовій керуючій обчислювальній системі [3].

У відмовостійких ПАС з МС, виникають відмови та збої АЗ, а також збої ПЗ. У відомих дослідженнях вважається, що показники надійності ПАС мають комплексні значення [5] АЗ та ПЗ, що унеможливлює досліджувати відмовостійкі ПАС з врахуванням відновлення працездатності ПЗ. Щоб забезпечити таку можливість в розпорядженні проектанта повинні бути відповідні надійнісні моделі відмовостійких ПАС з МС.

У відомих публікаціях відсутні надійнісні моделі відмовостійких ПАС з МС з врахуванням автоматичного перезавантаження ПЗ, збої якого викликані збоями АЗ. Вищесказане обумовлює актуальність задачі розробки надійнісної моделі такої ПАС.

1. Відмовостійка система на основі мажоритарної структури

Структурна схема відмовостійкої ПАС з МС показана на рис. 1.

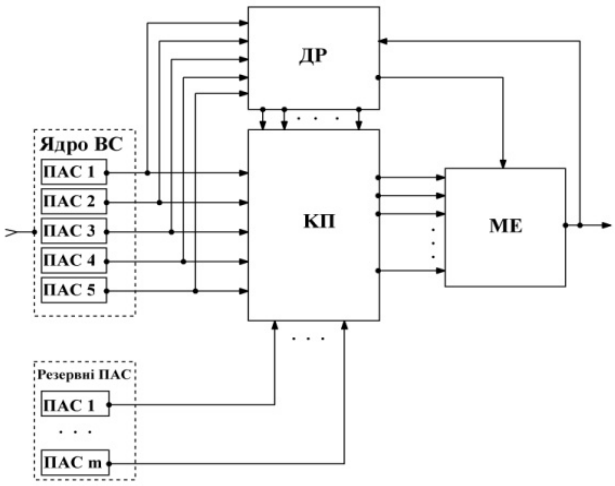

Рис. 1. Структурна схема відмовостійкої ПАС на основі мажоритарної структури з фіксованим правилом прийняття рішення

До її складу входить: ядро відмовостійкої системи (ВС), яке складають 5 ПАС робочої конфігурації; ПАС ковзного резерву, серед яких одна ПАС в гарячому резерві (з завантаженим ПЗ) та декілька ПАС холодного резерву (з не завантаженим ПЗ); мажоритарний елемент (МЕ); детектор розузгодження (ДР), на який покладені функції контрою та діагностики; комутаційний пристрій (КП), який виконує відключення несправних ПАС з ядра ПАС та підключення справних ПАС в нього.

2. Опис підходу до оцінки показників надійності програмно-апаратної системи

В ПАС, що розглядається, присутні відмови та збої АЗ. В свою чергу збої АЗ породжують збій в роботі ПЗ, що виправляється шляхом його перезавантаження. Якщо перезавантаження ПЗ відновлює працездатність ПАС, то це свідчить, що в системі відбувся збій АЗ. У випадку не успішного перезавантаження ПЗ вважається, що відбулася відмова АЗ.

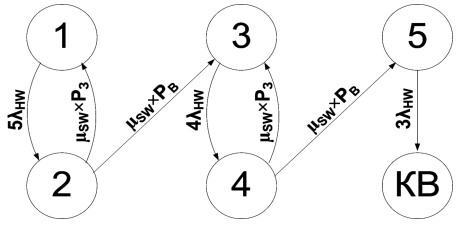

Рис. 2. Макромодель відмовостійкої програмно-апаратної системи на основі мажоритарної структури

Макромодель відмовостійкої ПАС у вигляді дискретно-неперервної стохастичної системи представлена на рис. 2, яка враховує наступні її стани, а саме:

стан 1 – справні 5 ПАС;

стан 2 – справні 4 ПАС, 1 ПАС знаходиться в непрацездатному стані, проводиться процедура перезавантаження ПЗ;

стан 3 – справні 4 ПАС і одна ПАС несправна, так як перезавантаження ПЗ не було успішним;

стан 4 – справні 3 ПАС, 1 ПАС знаходиться в непрацездатному стані, проводиться процедура перезавантаження ПЗ;

стан 5 – справні 3 ПАС; стан КВ – стан критичної відмови.

Програмно-апаратні системи, з яких сформована відмовостійка система, втрачають працездатність з інтенсивністю

$$\lambda_{АЗ}=\lambda''_{АЗ}+\lambda'_{АЗ},$$

де $\lambda''_{АЗ}$ – інтенсивність відмов АЗ, $\lambda'_{АЗ}$ – інтенсивність збоїв АЗ. Збої АЗ, приводять до збоїв у роботі ПЗ. Тому інтенсивність збоїв ПЗ, викликаних збоями АЗ, має значення $\lambda_{ПЗ} = \lambda'_{АЗ}$. Після чергової відмови система переходить в інший стан з інтенсивністю $r\cdot\lambda_{АЗ}$, (r = 5, 4, 3 – кількість справних ПАС в ядрі). З імовірністю $P_З$ в системі появляються збої АЗ та з імовірністю $P_В$ відмови АЗ. Відповідно процедура перезавантаження програмного забезпечення відбувається успішно з інтенсивністю $\mu_{ПЗ}\cdot P_З$ та не успішно з інтенсивністю $\mu_{ПЗ}\cdot P_В$, де $\mu_{ПЗ}=1/T_{resm}$, T_{resm} – середнє значення тривалості перезавантаження ПЗ. Коли в системі присутні 3 справні ПАС, то при наступній відмові система попадає в стан критичної відмови з інтенсивністю $3\cdot\lambda_{АЗ}$.

3. Модель відмовостійкої системи з мажоритарною структурою з врахуванням автоматичного перезавантаження програмного забезпечення

Метод розробки надійнісної моделі відмовостійкої ПАС з МС у вигляді графа станів та переходів, описаний у монографії [7], передбачає формалізоване представлення об'єкта дослідження у вигляді структурно-автоматної моделі. Для побудови структурно-автоматної моделі необхідно виконати наступні завдання: сформувати вербальну модель об'єкту дослідження; визначити базові події; визначити компоненти вектора стану, якими можна описати стан системи в довільний момент часу; сформувати множину параметрів, якими можна описати систему; сформувати дерево правил модифікації компонент вектора стану.

3.1. Перелік процедур, які формують поведінку відмовостійкої програмно-апаратної системи з мажоритарною структурою

Процедура 1. Виявлення несправної ПАС в ядрі та її відключення.

Процедура 2. Підключення ПАС з гарячого резерву в ядро.

Процедура 3. Підключення ПАС із холодного резерву в гарячий резерв. Ця процедура характеризується тривалістю, яку визначає затрати часу на завантаження ПЗ.

Процедура 4. Автоматичне перезавантаження програмного забезпечення ПАС, в яких відбувся збій ПЗ викликаний збоями АЗ.

3.2. Визначення базових подій програмно-апаратної системи з мажоритарною структурою

Відповідно до визначених процедур, які визначають поведінку ПАС з мажоритарною структурою, складається перелік подій, які відбуваються в даній

відмовостійкій системі. Події відображають парами, що відповідає початку і закінченню часового інтервалу, який представляє певний стан системи. З цього переліку подій для структурно-автоматної моделі вибираються базові події [7, с. 65]. В результаті проведеного аналізу визначено сім базових подій, а саме:

Подія 1 – «Відмова ПАС в ядрі МС»;

Подія 2 – «Збій ПЗ ПАС в ядрі МС»;

Подія 3 – «Відмова резервної ПАС (гарячий резерв)»;

Подія 4 – «Збій ПЗ резервної ПАС (гарячий резерв)»;

Подія 5 – «Закінчення процедури підключення ПАС з гарячого резерву в ядро МС»;

Подія 6 – «Закінчення процедури підключення ПАС з холодного резерву в гарячий резерв»;

Подія 7 – «Закінчення процедури автоматичного перезавантаження ПЗ в ПАС».

3.3. Структура вектора стану відмовостійкої системи

Представимо компоненти вектора стану, якими можна описати стан системи в довільний момент часу. Для опису стану системи використано чотири компоненти:

V1 – відображає поточне значення кількості працездатних ПАС в ядрі;

V2 – відображає наявність ПАС в гарячому резерві;

V3 – відображає поточне значення кількості ПАС в "холодному" резерві;

V4 – відображає поточне значення кількості ПАС, що перебувають на перезавантаженні.

3.4. Параметри відмовостійкої системи, які враховані в її моделі

При формуванні надійнісної моделі ВС її склад і окремі складові необхідно представити відповідними параметрами, а саме:

n – початкова кількість ПАС в ядрі МС;

k – кількість ПАС в гарячому резерві; m – початкова кількість резервних ПАС з незавантаженим ПЗ;

λ_{SW} – інтенсивність збоїв програмного забезпечення ПАС;

λ_{HW} – інтенсивність відмов ПАС в ядрі МС або в гарячому резерві;

T_h – середнє значення тривалості заміни несправної ПАС в ядрі на ПАС з гарячого резерву;

T_c – середнє значення тривалості підключення ПАС з холодного резерву в гарячий резерв;

T_{stm} – тривалість завантаження ПЗ в ПАС, що переключена з холодного в гарячий резерв;

T_{resm} – тривалість перезавантаження ПЗ в ПАС, що перебуває в непрацездатному стані в ядрі з ознакою збою ПЗ;

$P_З$ і $P_В$ – імовірності появи збоїв та відмов АЗ відповідно.

3.5. Дерево правил модифікації компонент вектора стану

Відповідно до технології аналітичного моделювання [7] та на підставі визначених базових подій, визначених компонент вектора стану та параметрів, якими описується ПАС, проведено розробку дерева правил модифікації компонент вектора стану ПАС, фрагмент якого представлено в табл. 1.

Таблиця 1

Дерево правил модифікації компонент вектора стану

Базові події	Опис ситуацій, в яких відбуваються базові події	Формула розрахунку інтенсивності базової події	Правило модифікації компонент вектора стану
1.Відмова ПАС в ядрі МС	(V1>=3)	$V1\cdot\lambda_{HW}$	V1:=V1-1
2.Збій ПЗ ПАС в ядрі МС	(V1>=3)	$V1\cdot\lambda_{SW}$	V1:=V1-1; V4:=V4+1
3. Відмова резервної ПАС (гарячий резерв)	(V2>0)	$V2\cdot\lambda_{HW}$	V2:=V2-1
4. Збій ПЗ резервної ПАС (гарячий резерв)	(V2>0)	$V2\cdot\lambda_{SW}$	V2:=V2-1; V4:=V4+1
----------			
7. Закінчення процедури перезавантаження ПЗ в ПАС	(V4>0)	$(1/T_{resm})\cdot P_З$	V3:=V3+1; V4:=V4-1
		$(1/T_{resm})\cdot P_В$	V4:=V4-1
Критерій критичної відмови	(V1<3)		

3.6. Формування аналітичної моделі відмовостійкої системи з мажоритарною структурою

Розроблена структурно-автоматна модель дає можливість згідно алгоритму побудови графа станів та переходів [7, с. 89] автоматично побудувати графи станів та переходів. Граф станів та переходів, в якому враховані наступні параметри відмовостійкої системи з мажоритарною структурою: n=5, k=0, m=0, λ_{HW}, λ_{SW}, T_h, T_c, T_{stm}, T_{resm}, $P_З$=1, $P_В$=0, представлено на рис. 3. При зміні конфігурацій відмовостійкої системи з мажоритарною структурою розмірність графів зростає і вони будуть мати параметри, які представлено в табл. 2.

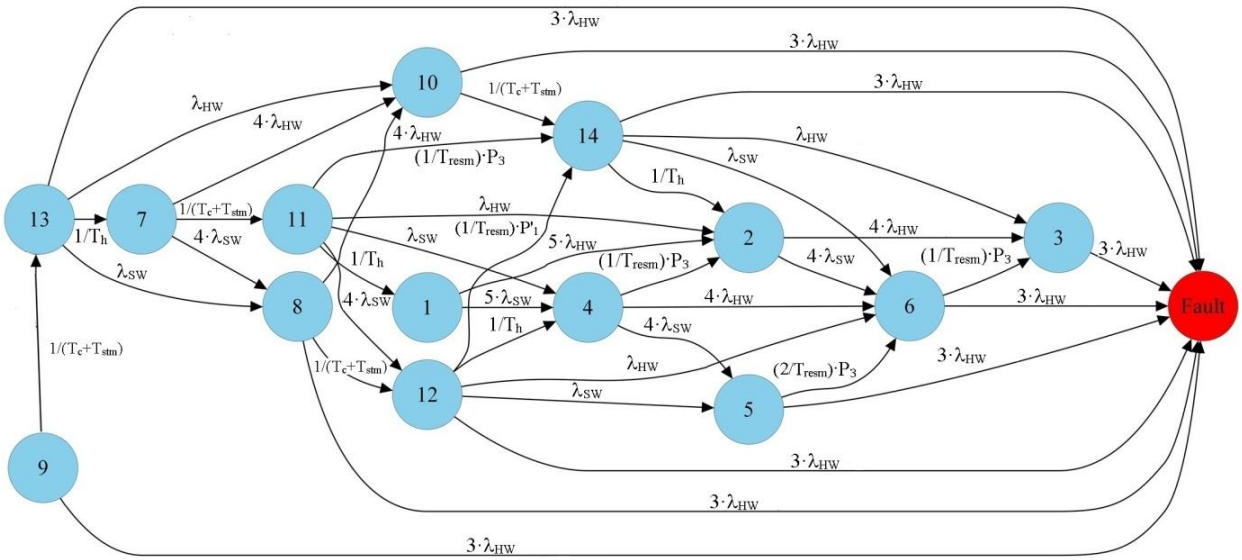

Рис. 3. Модель відмовостійкої ПАС у вигляді графа станів та переходів

На основі побудованого графа станів та переходів (рис. 3) сформована система лінійних диференційних рівнянь:

$$\frac{dP_1(t)}{dt} = -(5\lambda_{HW} + 5\lambda_{SW}) \cdot P_1(t) + \frac{1}{T_h} \cdot P_{11}(t);$$

$$\frac{dP_2(t)}{dt} = 5 \cdot \lambda_{HW} \cdot P_1(t) - (4\lambda_{HW} + 4\lambda_{SW}) \cdot P_2(t) +$$

$$+ \frac{1}{T_{resm} \cdot P_З} \cdot P_4(t) + \lambda_{HW} \cdot P_{11}(t) + \frac{1}{T_h} \cdot P_{14}(t);$$

$$\frac{dP_3(t)}{dt} = 4 \cdot \lambda_{HW} \cdot P_2(t) - 3 \cdot \lambda_{HW} \cdot P_3(t) +$$

$$\frac{1}{T_{resm}} \cdot P_3 \cdot P_6(t) + \lambda_{HW} \cdot P_{14}(t); \qquad (1)$$

……

$$\frac{dP_{14}(t)}{dt} = \frac{1}{T_c + T_{stm}} \cdot P_{10}(t) + \frac{1}{T_{resm}} \cdot P_1' \cdot P_{11}(t) +$$

$$+ \frac{1}{T_{resm}} \cdot P_3 \cdot P_{12}(t) - \left(4\lambda_{HW} + \lambda_{SW} + \frac{1}{T_h}\right) \cdot P_{14}(t);$$

$$\sum_{i=1}^{15} P_i(t) = 1.$$

Розв'язання даної системи рівнянь дає можливість провести оцінку показників надійності відмовостійкої ПАС першої конфігурації поданої в табл. 2.

Таблиця 2

Параметри графа станів та переходів при різних конфігураціях відмовостійкої системи

Параметри конфігурації ВС	Кількість станів	Кількість переходів
n=5; k=0; m=0	15	40
n=5; k=1; m=1	34	117
n=5; k=1; m=2	61	234
n=5; k=1; m=3	97	397

4. Приклад використання моделі

Необхідно порівняти значення показників надійності ПАС, отриманих за допомогою відомих моделей та розробленої моделі. Порівнювалися значення тривалості безперервної роботи ПАС, при якій ймовірність безвідмовної роботи відмовостійкої системи на основі мажоритарної структури з врахуванням автоматичного перезавантаження ПЗ на ПАС відповідає такій умові: $P_{б.р.} \geq 0{,}99$. Дослідження проведено при наступних вхідних параметрах: n=5 (кількість ПАС основної конфігурації), k=1 (кількість ПАС гарячого резерву), m=0 (кількість ПАС холодного резерву), $\lambda_{HW}=1\cdot10^{-5}$, $\lambda_{SW}=1\cdot10^{-4}$.

На рис. 4 представлені залежності ймовірності безвідмовної роботи відмовостійкої ПАС з МС від тривалості її експлуатації, отримані за допомогою моделей з різним ступенем адекватності, а саме:

крива 1 – отримана за допомогою моделі ПАС без врахування збоїв програмного забезпечення (розрахунки проведені згідно моделі, поданої в [8]);

крива 2 – отримана за допомогою моделі ПАС з врахуванням збоїв програмного забезпечення та без відновлення працездатності ПЗ (розрахунки проведені згідно моделі, поданої в [6]);

крива 3 – отримана за допомогою запропонованої моделі ПАС з врахуванням збоїв програмного забезпечення та його відновлення шляхом автоматичного перезавантаження.

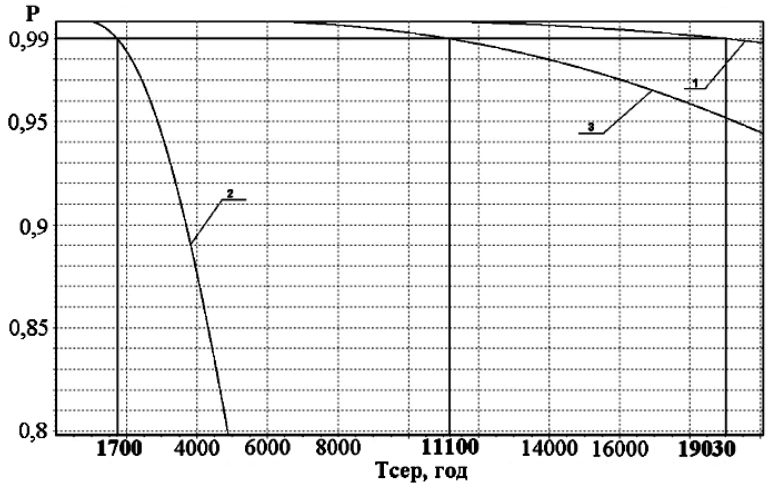

Рис. 4. Залежність ймовірності безвідмовної роботи відмовостійкої ПАС з мажоритарною структурою від тривалості її експлуатації

З результатів поданих на рис. 4 видно, що:

неврахування збоїв програмного забезпечення (крива 1) дає завищене значення показника надійності ПАС;

врахування збоїв програмного забезпечення без можливості його відновлення шляхом автоматичного перезавантаження (крива 2) занижує значення показника надійності ПАС;

запропонована модель (крива 3) показує різницю при визначенні показника надійності, яку дають відомі надійнісні моделі ПАС.

Висновки

В статті запропонована надійнісна модель відмовостійкої програмно-апаратної системи з мажоритарною структурою з відновленням працездатності апаратних засобів, шляхом автоматичного перезавантаження програмного забезпечення, збій в роботі якого був викликаний збоєм в роботі апаратного засобу. Модель відмовостійкої програмно-апаратної системи з мажоритарною структурою дає змогу проектанту вирішувати задачі надійнісного аналізу та синтезу, а саме: визначити параметри конфігурації ПАС з МС для забезпечення необхідного рівня надійності, визначити вимоги до надійності програмного забезпечення та вимоги до обмеження тривалості перезавантаження програмного забезпечення.

В подальших дослідженнях можна врахувати відмови ПЗ, які викликані дефектами у коді програмного забезпечення та тривалість його "ремонту".

Література

1. Danecek, V. The Fault-tolerant Control System Based on Majority Voting with Kalman Filter [Text] / V. Danecek, P. Silhavy // Telecommunications and Signal Processing. – 2011. – P. 472 – 477.

2. Панченко, С.В. Дослідження мажоритарної структури системи з відновленням [Текст] / С.В. Панченко, Н.Г. Панченко, А.А. Меліхов // Інформаційно-керуючі системи на залізничному транспорті. – 2010. – №5. – С. 62 – 68.

3. Структурно-алгоритмическая организация и модели надежности мажоритарно-резервированных систем [Текст] / А.И. Кривоносов, Н.К. Байда, А.А. Кулаков, В.С. Харченко, Н.П. Благодарный // Космічна наука і технологія. – 1995. – № 1. – С. 74 – 79.

4. Белый, Ю.А. Модели отказов и оценка надежности мультидиверсных систем [Текст] / Ю.А. Белый // Радіоелектронні і комп'ютерні системи. – 2008. – № 5 (32). – С. 62 – 66.

5. Поночовный, Ю.Л. Вибір методу комплексування показників надійності компонент інформаційних систем за похибкою, що вноситься [Текст] / Ю.Л. Поночовный // Системи озброєння і військова техніка. – 2008. – № 4 (16). – С. 156 – 158.

6. Friedman, M.A. Reliability techniques for combined hardware and software systems [Text] / M.A. Friedman, P.Y. Tran, P.L. Goddard / Final technical report. Rome Laboratory Air Force Systems Command, Griffiss Air Force Base. NY – 1992. – 286 p.

7. Волочій, Б.Ю. Технологія моделювання алгоритмів поведінки інформаційних систем [Текст] /

Б.Ю. Волочій. – Львів: Вид-во НУ "Львівська політехніка", 2004. – 220 с.

8. Засуха, С.А. Модель готовности двухканальной информационно-управляющей системы космического аппарата с оперативной верификацией программных средств [Текст] / С.А. Засуха, Ю.Л. Поночовный // Наука і техніка. Повітряних сил Збройних сил України: науково-технічний журнал. – 2011. – № 2(6). – С. 144 – 150.

Надійшла до редакції 14.02.2013, розглянута на редколегії 6.03.2013

Рецензент: д-р техн. наук, проф., зав. каф. комп'ютерних систем і мереж В.С. Харченко, Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ», Харків, Україна.

НАДЕЖНОСТНАЯ МОДЕЛЬ ОТКАЗОУСТОЙЧИВОЙ ПРОГРАММНО-АППАРАТНОЙ СИСТЕМЫ НА ОСНОВЕ МАЖОРИТАРНОЙ СТРУКТУРЫ СО СКОЛЬЗЯЩИМ РЕЗЕРВИРОВАНИЕМ И АВТОМАТИЧЕСКОЙ ПЕРЕЗАГРУЗКОЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Б.Ю. Волочий, Л.Д. Озирковский, А.В. Муляк, М.М. Змысный

В статье предложена надежностная модель отказоустойчивой программно-аппаратной системы, реализованной как системы с мажоритарной структурой "3 из 5" и с перезагрузкой программного обеспечения, в работе которого возможны сбои, вызванные сбоями в аппаратных средствах. В состав отказоустойчивой системы входят: программно-аппаратные системы рабочей конфигурации; программно-аппаратные системы скользящего резерва; мажоритарный элемент; детектор рассогласования, предназначенный для обнаружения нарушений работоспособности программно-аппаратной системы; коммутационное устройство. Модель предназначена для решения задач надежностного проектирования отказоустойчивых программно-аппаратных систем.

Ключевые слова: надежность, программно-аппаратная система, отказоустойчивая система, мажоритарная структура.

RELIABILITY MODEL OF THE FAULT-TOLERANT HARDWARE/SOFTWARE SYSTEM BASED ON MAJORITY STRUCTURE WITH SOFTWARE AUTOMATIC RESTART

B.Yu. Volochiy, L.D. Ozirkovsky, O.V. Mulyak, M.M. Zmysnyi

This paper outlines a reliability model of a fault-tolerant hardware/software system built on a majority structure 3 of 5, with hot and cold standby and software restart. Software failures caused by hardware failures require restart. The fault-tolerant system features consist: hardware/software systems which is in working order, hardware/software systems in sliding redundancies, adaptive voter, detector of the deviation a system in hardware and software parts, switching device. The model is delivered to systems solving a problem of reliable developments of the fault-tolerant hardware/software systems.

Key words: reliability, hardware/software systems, fault-tolerant systems, majority structure.

Волочій Богдан Юрійович – доктор техн. наук, професор кафедри теоретичної радіотехніки та радіовимірювань Національного університету «Львівська політехніка» e-mail: bvolochiy@ukr.net.

Озірковський Леонід Діонісійович – канд. техн. наук, доцент кафедри ТРР Національного університету «Львівська політехніка» e-mail: lozirkovsky@lp.edu.ua.

Муляк Олександр Володимирович – аспірант кафедри ТРР Національного університету «Львівська політехніка» e-mail: mulyak.oleksandr@gmail.com.

Змисний Михайло Михайлович – асистент кафедри ТРР Національного університету «Львівська політехніка» e-mail: zmysnyim@gmail.com.