УДК 081.32-192

Ю.П. БУЦЕНКО[*], Ю.Г. САВЧЕНКО[*]

ПОКАЗНИКИ НАДІЙНОСТІ КЛАСТЕРІВ ВИСОКОЇ ДОСТУПНОСТІ ЯК РЕЗЕРВОВАНИХ СИСТЕМ ІЗ СТРУКТУРНОЮ НАДЛИШКОВІСТЮ

[*]Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ, Україна

Анотація. *Розглянуто проблему забезпечення надійності електронних систем за умови обмеженої надійності компонентів, використаних при побудові системи. Ця проблема виникла давно і, про що свідчить досвід застосування існуючих методів її вирішення, може бути розв'язана лише на основі введення апаратурної надлишковості. Проведений ретроспективний аналіз характерних реалізацій таких методів свідчить, що в останнє десятиріччя відбулося помітне та суттєве розширення сфери застосування електронних відмовостійких систем. Якщо раніше ця сфера була обмежена, головним чином, апаратурою та системами оборонного й промислового призначення, то сьогодні відмовостійкі системи широко застосовуються в комерційній та банківських сферах, де зникають жорсткі масо-габаритні та навіть вартісні обмеження, а типовими компонентами стають окремі сервери і комп'ютери. Наприклад, термін «High-availalability clusters (HA)» – кластери високої готовності – виник порівняно недавно і використовується для опису банківських систем збереження даних, комп'ютерних систем керування комерційними мережами, телекомунікаційними мережами тощо, хоча у традиційній термінології це, по суті, не що інше, як резервовані структури з навантаженим резервом. Узагальнюючи існуючі процедури відновлення інформації в надлишкових структурах, можна стверджувати, що на сьогодні використовуються лише три алгоритми відновлення: 1) мажоритарний, 2) адаптивний мажоритарний, 3) 2-парної обробки даних із миттєвим відключенням пари, яка відмовила. У статті на основі проведеного аналізу наводяться узагальнюючі розрахункові співвідношення для оцінки основних варіантів структур із апаратурною надлишковістю та алгоритмів відновлення даних при відмові частини компонентів структури. Отримані співвідношення зв'язують імовірність безвідмовної роботи кластера, рівень надлишковості та функції розподілу ймовірності безвідмовної роботи компонентів. Показано, що в залежності від призначення резервованої системи, зокрема, для систем, які працюють у реальному часі, основним показником надійності разом із часом напрацювання до відмови стає ймовірність безпомилкової роботи системи, яка, по суті, визначає рівень безпеки автоматизованого керування.*

Ключові слова: *резервування, надійність, кластери, показники.*

Аннотация. *Рассматривается проблема обеспечения надежности электронных систем в условиях ограниченной надежности составляющих систему компонентов. Эта проблема возникла давно и, как показывает опыт применения существующих методов ее решения, может быть решена лишь на основе введения аппаратурной избыточности. Проведенный ретроспективный анализ характерных реализаций таких методов показывает, что в последнее десятилетие произошло весьма заметное расширение сферы применения электронных отказоустойчивых систем. Если раньше эта сфера ограничивалась, в основном, системами и аппаратурой промышленного и оборонного назначения, то в настоящее время отказоустойчивые системы повсеместно используются в коммерческой и банковской сферах, где исчезают серьезные масса-габаритные и даже стоимостные ограничения, а типичными компонентами систем становятся отдельные серверы и компьютеры. Например, термин «High-availalability clusters (HA)» – кластеры высокой доступности – возник сравнительно недавно и используется для описания банковских систем сохранения данных, компьютерных систем управления торговыми и коммерческими сетями, телекоммуникационными системами и т.д. В традиционной терминологии это, по сути, резервированные структуры с нагруженным резервом. Обобщая существующие процедуры восстановления информации в избыточных структурах, можно утверждать, что на сегодня существуют только три алгоритма восстановления: 1) мажоритарный, 2) адаптивный мажоритарный и 3) 2-парной обработки данных с моментальным отключением отказавшей пары. В статье на основе проведенного анализа приводятся обобщающие соотношения для оценки показателей надежности основных*

ISSN 1028-9763. Математичні машини і системи, 2018, № 4

вариантов структур с аппаратной избыточностью и алгоритмов восстановления данных при отказе части компонентов структуры. Полученные соотношения связывают вероятность безотказной работы кластера, уровень избыточности и функции распределения вероятности безотказной работы компонентов. Показано, что в зависимости от назначения резервированной системы, в частности, для систем управления реального времени основным показателем надежности наряду со временем наработки до отказа становится вероятность безошибочной работы, которая, фактически, определяет уровень безопасности автоматизированного управления.
Ключевые слова: *резервирование, надежность, кластеры, показатели.*

Abstract. *The problem of ensuring the reliability of electronic systems in conditions of limited reliability of their components is considered. This problem arose long ago and, as experience of application of existing methods for solving it shows, can be solved on the basis of the introduction of hardware redundancy only. A retrospective analysis of the characteristic realizations of such methods shows that in the last decade there has been a very noticeable expansion of the scope of electronic fault-tolerant systems. If earlier this sphere was limited mainly to systems and equipment for defense and industrial purposes, nowadays fault-tolerance systems are widely used in spheres of commerce and banking so. In these cases, serious mass-dimensional and even cost restrictions disappear and computers and servers become typical components of the system. For example, the term "high-availability cluster" has emerged relatively recently and is used to describe banking data storage systems, computer systems for managing commercial networks, telecommunication systems and etc. Moreover, from the point of view of traditional terminology, in all these cases we are dealing with redundant systems with a loaded reserve. Summarizing existing data recovery procedures in redundant structures, it can be stated, that nowadays there are only three types of algorithms for their functioning: 1) majority, 2) adopted majority, 3) double-pair processing with instantaneous disconnections of failed pairs. In the paper, based on analysis carried out, the computational relationships are calculated to estimate the reliability indexes of the basic versions of structures with hardware redundancy and data recovery algorithms for the failure of part of structure components. The relationships obtained allow us to establish connections between the probability of failure-free operation of the cluster, the level of redundancy and probability distribution functions for the components. It is shown that for redundant systems various purposes (in particular-real time control systems), the main indicator of reliability along with time to failure is the probability of error-free operation It is this indicator, in fact, that determines the level of security of automated control.*
Keywords: *redundancy, reliability, clusters, indicators.*

1. Вступ

Проблема забезпечення надійності електронних систем при обмеженій надійності компонентів, з яких складається система, виникла одночасно з першими застосуваннями таких систем для керування реальними об'єктами оборонного призначення, в промисловості, на транспорті тощо. Тобто у всіх випадках, коли відмова системи є надзвичайною подією, яка потенційно може призвести до небезпечних наслідків для персоналу або довкілля та до неприпустимих економічних втрат. Вирішити цю проблему за рахунок використання більш надійних (і дорогих) компонентів у більшості випадків неможливо, оскільки надійність електронних елементів і пристроїв обмежена сучасним станом технології на фізичному рівні (наприклад, наявність небажаних домішок у матеріалах), що жорстко визначає межу для надійності, яка може бути досягнута сьогодні. У такій ситуації обмеження надійності компонентів є об'єктивним і невідворотним фактором при проектуванні електронних систем.

Термін «High-availability clusters (HA)» – кластери високої доступності – виник порівняно недавно й використовується в основному для резервованих комп'ютерних телекомунікаційних систем, банківських систем збереження даних (СЗД), комп'ютерних систем керування комерційними та торговельними мережами. У традиційних термінах це резервовані системи із апаратною надлишковістю і в більшості випадків мова йде про використання так званого гарячого резервування (навантаженого резерву). Для електронних сис-

тем класичним прикладом можна вважати мажоритарний метод Дж. фон Неймана [1] та методи, які широко використовуються фірмою TANDEM для створення так званих промислових комп'ютерів. У будь-якому варіанті мова йде про заміну одного об'єкта (електронної схеми, пристрою, комп'ютера, сервера мережі) n однаковими (однотипними, еквівалентними за функціями) об'єктами та утворення результату шляхом оброблення сигналів (даних) з n виходів. Варіанти розрізняються рівнем надлишковості ($n = 2,3,4,...$) та логічними правилами оброблення сигналів, по суті, алгоритмом керування кластером.

Метою статті є узагальнення підходів до побудови відмовостійких електронних систем з урахуванням сучасних реалізацій та застосувань у нових сферах їх використання.

2. Основна частина

Одним із широко розповсюджених методів підвищення надійності до цього часу залишається мажоритарний метод, який у класичному вигляді передбачає наявність деякої кількості n ідентичних за призначенням пристроїв, реалізацію ними паралельно однакових завдань та вибір як найбільш вірогідного того результату, який «підтримується» більшістю $k \geq \frac{n+1}{2}$ для непарного n та $k \geq \frac{n}{2}+1$ для парного. У випадку, якщо пристрої ідентичні за своїми показниками надійності та ймовірність адекватного виконання кожним із них поставленого завдання дорівнює p, маємо такий вираз для ймовірності P формування вказаної більшості:

$$P = \sum_{k=\rho}^{n} C_n^k p^k (1-p)^{n-k}, \qquad (1)$$

де ρ відповідає мінімальній більшості з n компонентів структури.

Зауважимо, що аналогічна процедура використовується і у випадках, коли прогнозується функціонування системи в умовах невизначеності (пристрої обробляють дані відповідно до варіантів, які передбачаються у майбутньому) або при діагностуванні складних систем із великою кількістю рецепторів (датчиків).

Треба зазначити, що на час виникнення, наприклад, мажоритарного методу (1952 р.) його практична реалізація була проблематичною, оскільки мінімальний рівень необхідної надлишковості потребував потроєння масогабаритних параметрів апаратури, що у більшості випадків виходило за межі реальних можливостей, наприклад, для бортової апаратури, саме, де вимоги до надійності в той час були найбільш критичними.

На сьогодні ситуація змінилася докорінним чином завдяки досягненням мікро- та наноелектроніки, з одного боку, а з іншого, широкому застосуванню відмовостійких електронних систем у банківській та комерційних сферах, для автоматичного керування наземними транспортними та технологічними об'єктами, де немає критичних обмежень на габарити та вагу. До того ж, для деяких застосувань навіть вартість додаткового обладнання не є критичною, оскільки плата за надійність (відмостійкість) набагато вища за збитки при виникненні відмови. Загалом, у будь якому випадку рівень надлишковості, прийнятний для реальних застосувань електронних систем, сьогодні не є критичним. Наприклад, досить популярне на даний час обладнання серії NetApp FAS8000, не зважаючи на досить велику вартість таких систем, яке використовується в банківській сфері для створення відмовостійких СЗД. Важливою є також можливість нарощування кластера до 24 вузлів і 57 ПБайт дискового простору, а додавання або заміна компонентів проводиться без переривання роботи системи, а сам процес розширення не потребує спеціально відведеного часу на технічне обслуговування [2].

Наведені міркування спонукають до перегляду та спроби узагальнення існуючих методів побудови відмовостійких електронних систем з точки зору впливу рівня надлишковості та деяких інших факторів на показники надійності кластерних структур.

Узагальнюючи, можна стверджувати, що будь-яка відмовостійка система може бути представлена групою (кластером) однакових або однотипних об'єктів, що виконують однакові функції, та деякими додатковими апаратними або програмними засобами для керування кластером. Функції цього умовного додатку полягають у прийнятті рішень у випадку відмови частини кластера на основі аналізу сигналів на виходах об'єктів, що утворюють кластер. Отже, яку функцію має виконувати цей додатковий орган? Очевидно, у найзагальнішому випадку це збереження виконання функцій системою у разі виникнення будь-яких передбачуваних відмов частини кластера. Ці функції залежать від призначення системи і для кожної системи мають конкретне визначення та критерії правильного (безпомилкового) їх виконання.

Наведемо характерні приклади.

1. Система збереження даних державного або критичного з точки зору безпеки чи економіки рівня.

2. Система керування у реальному часі потенційно небезпечними (для персоналу або довкілля) об'єктами та технологічними процесами.

Перший приклад є типовим для широкого кола застосувань, де критерієм введення апаратної надлишковості є вага втрат внаслідок переходу системи в непрацездатний стан. У широкому розумінні непрацездатний стан – це неможливість надати послуги, для яких призначена система. Тобто, наприклад, для банку це відмова у виконанні транзакцій чи інших банківських операцій. Якщо такий стан не занадто тривалий, то втрати можуть бути некритичними. Але ж непрацездатний стан може бути таким, що система втратить дані, які зберігались в її пам'яті, або вони будуть спотворені. Очевидно, вага таких втрат стає неприпустимою і зрозуміло, що наслідки виникнення цих ситуацій суттєво різні.

Характерними для другого прикладу є комп'ютерні системи керування технологічними процесами або потенційно небезпечними об'єктами, наприклад, атомними станціями чи транспортними мережами. У цих випадках ціна виникнення непрацездатного стану може виявитися надто великою, що вимагає застосування спеціальних заходів для уникнення таких ситуацій (наприклад, миттєвого блокування керуючих сигналів, що надходять від системи на об'єкт керування).

Після цих попередніх зауважень перейдемо безпосередньо до вибору показників надійності структур означеного класу. Відповідно до визначення, сформульованого одним із фундаторів теорії відмовостійкості А.Авіженісом [3], «надійність характеризують наданням системою послуг, які визначені призначенням системи (або, що еквівалентно напрацюванню до відмови), яке відраховується від певного моменту». У свою чергу, напрацювання до відмови у більшості випадків це середній час або математичне сподівання часу безвідмовної роботи відповідного об'єкта. Ця величина безпосередньо залежить від функції розподілу ймовірності безвідмовної роботи $P(t)$ для кластерних структур із апаратною надлишковістю. У свою чергу, $P(t)$ залежить від функцій розподілу складових кластера $p_i(t), i = 1, 2....n$, рівня надлишковості n та способу організації структури, тобто від алгоритму нейтралізації відмов складових кластера.

Зазначимо, що ймовірність $P(t)$ може трактуватись як у апріорному сенсі (як імовірність того, що система адекватно виконує поставлену задачу, починаючи її виконання в момент часу t), так і у апостеріорному (до моменту часу t обладнання не зазнавало деградаційних або руйнівних впливів).

Алгоритм нейтралізації відмов реалізується деякими додатковими компонентами (апаратними або програмними), що оброблюють сигнали на виходах складових кластера.

У мажоритарних структурах цю функцію виконують так звані відновлюючі органи, в яких здійснюється «голосування» сигналів. У загальному випадку ці додаткові засоби можна об'єднати терміном «керуючий орган» (КО). Різноманіття алгоритмів функціонування таких КО насправді зовсім невелике.

Мажоритарний алгоритм. Результат оброблення сигналів (інформації) утворюється на основі «голосування» сигналів n складових кластера, який співпадає із сигналами більшості:

$$y = y_1 \# y_2 \# ... \# y \ ,$$

де через # позначена так звана мажоритарна логічна функція. У найпростішому випадку для двійкових змінних та $n = 3$ вона має вигляд

$$y = y_1 y_2 \vee y_1 y_3 \vee y_2 y_3 .$$

Сигнали, значення яких не співпадають із більшістю, ігноруються.

Сьогодні в системах фірми Tandem (клас Integrity) для маскування (нейтралізації) помилок використовують саме 3-кратну апаратну надлишковість, що забезпечує продовження безперервної роботи в умовах збоїв. Найчастіше системи цього класу застосовують у телефонних та стільникових мережах, а також у торговельних закладах та банках. Важливою перевагою систем із апаратною надлишковістю є також можливість проведення ремонтно-профілактичних робіт без переривання системою виконання своїх функцій та розширення (масштабування). Така можливість опосередковано еквівалентна реальному збільшенню напрацювання до відмови.

Із зрозумілих причин у обох вказаних вище випадках функція $P(t)$ є спадною, тобто $P'(t) < 0$. Запровадивши часовий параметр у формулу (1), дослідимо характер монотонності величини $P(t)$. Він не є очевидним, оскільки функція $1 - p(t)$ є зростаючою, а $P(t)$ – сума доданків, сформованих як добутки спадних та зростаючих функцій. Опускаючи досить громіздкі проміжні перетворення, для похідної $P(t)$, можна записати

$$P'(t) = p'(t) \frac{(2n+1)!}{n!n!} (p(t)(1-p(t)))^n , \qquad (2)$$

тобто можна стверджувати, що величина $P(t)$ також спадна за часом. Варто зазначити також, що у випадку високонадійних складових системи ($p(t)$ близьке до 1) швидкість спадання для невеликих значень n зменшується. Асимтотично, при великих значеннях n швидкість спадання зростає (у найбільшій мірі при $p(t)$ близьких до $1/2$).

Слід зауважити, що не завжди доцільно вибирати мінімальне значення $k = n+1$. У випадках, коли необхідно забезпечити максимальну вірогідність (певність у результаті або гарантію відсутності помилки), керуючий орган повинен утворювати результат не на базі більшості, а консенсусом. Цю вірогідність можна оцінити виразом

$$\tilde{P}(t) = p_{ко}(t) \prod_{k=1}^{n} p_k(t), \qquad (3)$$

де $p_{ко}(t)$ – імовірність безвідмовної роботи керуючого органу, який формує результуючий сигнал роботи n пристроїв (не обов'язково непарної кількості, на відміну від «чисто» мажоритарного методу), $p_k(t), k = 1, 2, ..., n$ – імовірності безвідмовної роботи відповідних складових структури, які в загальному випадку можуть мати різні характеристики надійності.

Із (3) видно, що гарантія безпомилковості (фактично, у багатьох випадках це рівень безпеки) не може бути досягнута за рахунок напрацювання до відмови. Тобто збільшення

рівня гарантування безпомилковості веде до зменшення ймовірності безвідмовної роботи кластера. Це відбувається внаслідок того, що при збільшенні n у формулі (3) збільшується кількість співмножників, менших 1 (хоча й близьких до максимуму для високонадійних складових системи).

Розглянемо деякі випадки поповнення комплексу структури деякими іншими складовими, можливо, з іншими показниками надійності, але дешевшими за основних. Цікаво, чи варто це робити з огляду на потенційну можливість збільшити надійність комплексу. Зауважимо спочатку, що метою такого поповнення може бути не лише збільшення ймовірності прийняття узгодженого рішення (наявність більш ніж половини працездатних складових, наприклад, кластера серверів), але й забезпечення достатньої сумарної продуктивності сегмента кластера. Також важливим є випадок доповнення існуючих пристроїв з надійністю p_1 іншими (наприклад, дешевшими або більш надійними) з надійністю p_2. Можливі такі варіанти.

1+1. Ціль – збільшення ймовірності наявності хоча б одного працездатного пристрою: від p_1 до $p_1 + p_2 - p_1 p_2 = p_1 + p_2(1 - p_1) > p_1$.

1+2. Ціль – можливість реалізації мажоритарної процедури. Розглянемо різницю ймовірності наявності хоча б двох працездатних із трьох та ймовірності єдиного наявного:

$$p_1 p_2^2 + (1 - p_1) p_2^2 + 2 p_1 p_2 (1 - p_2) - p_2 = (1 - 2 p_1) p_2^2 + 2 p_1 p_2 - p_1$$

– квадратична функція відносно p_2.

а) $p_1 \le 1 \backslash 2$, тобто маємо $1 - 2 p_1 \ge 0$, max виразу досягає при $p_2 = 1$ (що нереально), дорівнює $1 - p_1$. На практиці це означає, що найбільший ефект такого поповнення досягається при високонадійних додаткових пристроях;

б) $p_1 > 1 \backslash 2$, у цьому випадку max виразу матиме місце при $p_2 = \dfrac{p_1}{2 p_1 - 1}$, причому це значення, очевидно, не повинно перевищувати 1: $\dfrac{p_1}{2 p_1 - 1} \le 1$ та $p_1 \le 2 p_1 - 1$, тобто $p_1 > 1$, що неможливо.

Таким чином, слід стверджувати, що реального виграшу можна досягти в усіх випадках, але за умови, коли ймовірність p_2 близька до 1. Аналогічний результат було отримано й при аналізі інших варіантів «поповнення» структури. Так, наприклад, у випадку 3+2 тенденція зберігається практично повністю.

При іншому алгоритмі [4], коли використовується так званий відновлюючий орган із пам'яттю, сигнал, значення якого не співпадає із більшістю сигналів у кластері, усувається з подальшого аналізу, що еквівалентно зменшенню n на 1. Таким чином, вираз (1) залишається без змін, але для цього випадку $\eta = 2$, що збільшує $P(t)$ при $n > 3$.

Алгоритм, що використовується фірмою Tandem у системах класу NonStop. У цьому випадку кластер утворюється двома парами об'єктів. Сигнали з виходів у кожній парі неперервно порівнюються. У разі виникнення неспівпадіння пара миттєво вимикається і на загальний вихід проходить лише сигнал (дані) від пари, де сигнали співпадають. У системах класу NonStop для забезпечення відновлення апаратури та помилок ПЗ після збоїв ці системи використовують механізм передавання повідомлень між складовими системи процесорними парами. Усі апаратні компоненти системи NonStop побудовані на основі принципу «швидкого виявлення несправності (fail fast design), у відповідності з якими кожен компонент повинен або функціонувати правильно, або миттєво зупинитися, щоб не заважати.

Для такої конфігурації можна записати:

$$P(t) = p_{ко}(t)\{p(t)^4 + 2p(t)^2[1 - p(t)^2]\}. \quad (4)$$

З (3) та (4) видно, що суттєвим фактором, який обмежує надійність кластерів з апаратною надлишковістю, є множник $p_{ко}(t)$. Дійсно, при будь-якому рівні надлишковості керуючий орган залишається «вузьким місцем». Його відмова призводить до відмови кластера в цілому незалежно від технічного стану його інших складових. Очевидним шляхом для подолання цього недоліку є резервування не лише основних складових кластера, але й КО, як це було запропоновано ще Дж. фон Нейманом у вигляді так званих багатолінійних структур [1], для яких

$$P(t) = \sum_{j}^{n} C_n^j [p(t)p_{ко}(t)]^j [1 - (p(t)p_{ко}(t))]^{n-j}. \quad (5)$$

З чого видно, що для таких структур зникає обмеження для зростання надійності кластера при збільшенні n. Але й у цьому випадку залишається проблема «останньої ланки» структури, тобто необхідності прийняття кінцевого рішення щодо достовірності результату.

Таким чином, узагальнюючи, можна стверджувати, що на сьогодні існує лише три процедури відновлення інформації (керування кластером) при відмові частини складових кластера: 1) мажоритарна, 2) адаптована мажоритарна та 3) 2-парна з відсіченням пари, що відмовила.

У всіх випадках, що розглянуті вище, основною змінною є ймовірність безвідмовної роботи одного компонента кластера в деякий фіксований момент часу $p(t)$, тобто цю величину попередньо потрібно обчислити для заданої функції розподілу ймовірності безвідмовної роботи компонентів певного класу. Для електронних компонентів за таку функцію традиційно приймають експоненціальний розподіл. Для цього випадку можна показати, що будь-яке збільшення рівня надлишковості (додавання до кластера нових складових навіть з відносно низькою надійністю) завжди гарантовано поліпшує показники надійності кластера в цілому. Але у практичній площині виникає питання про оптимальний рівень надлишковості з точки зору вартості кластера. Отже, можна сформулювати одну із двох традиційних задач оптимізації:

1) Знайти мінімальний за вартістю склад кластера при обмеженні знизу ймовірності безвідмовної роботи системи за заданий (фіксований) проміжок часу, тобто

2) Визначити склад кластера, що забезпечує максимальні показники надійності при обмеженні зверху сумарної вартості системи.

В інших випадках, коли складові кластера не є виключно електронними пристроями, стає сумнівним припущення щодо обґрунтованості використання експоненціального розподілу ймовірності безвідмовної роботи компонентів кластера. Зазначимо, що насправді майже завжди такі компоненти (комп'ютери, ноутбуки, комутатори тощо) мають у своєму складі неелектронні складові, наприклад, дисководи, клавіатуру, елементи індикації та ін., тому функції розподілу ймовірності безвідмовної роботи яких відрізняються від експоненціального закону. Очевидно, якщо для складових кластера

$$p_i = f_i(t), i = 1, 2, ..., n,$$

де функції f_i відповідають тому чи іншому конкретному розподілу, то, наприклад, для розподілу Вейбулла функція розподілу для ймовірності безвідмовної роботи кластера в цілому у випадку мажоритарної процедури відновлення буде мати інший вигляд.

3. Висновки

Таким чином, на сьогодні застосування електронних і, зокрема, комп'ютерних систем із структурною надлишковістю не є чимось особливим. Це, скоріше, природне рішення для досягнення заданих показників надійності або продуктивності. У багатьох випадках надійність і продуктивність тісно пов'язані, а надлишковість можна розглядати як деякий аналог поняття запасу міцності у механічних системах і конструкціях. Насправді, ці два поняття (надійність – запас міцності) за своєю сутністю споріднені: механічна система, яка має великий запас міцності навіть на інтуїтивному рівні, є більш надійною, ніж механізм із меншим запасом міцності. Більшість автомобілістів, мабуть, погодяться, що потужне авто є більш надійним транспортним засобом, ніж малопотужне. Це ж саме можна сказати й про продуктивність у широкому сенсі цього поняття.

З точки зору конкретно показників надійності, основним слід вважати ймовірність безвідмовної роботи за певний час і як параметр цього показника час напрацювання до відмови. Такий показник є досить універсальним і найбільш зрозумілим для користувача. Так, фірма Tandem презентує свої системи як такі, що мають імовірність безвідмовної роботи за рік 0,99999 («п'ять дев'яток»), що еквівалентно п'яти хвилинам непрацездатності за рік (!) неперервної роботи.

Але ж це в певному сенсі «звичайні» системи. Інша справа, коли мова йде про системи, відмова яких пов'язана з ризиком для життя людини або масштабною загрозою довкіллю. Наприклад, пасажира авіалайнера не дуже, скоріш за все, буде хвилювати показник середнього часу безвідмовної роботи приладу з назвою автопілот 10000 або 20000 год. Його хвилюють, напевне, найближчі 2–4 години польоту. Тому у цьому випадку головним стає ймовірність безпомилкової роботи усієї системи керування польотом, а саме ефективність засобів оперативного контролю технічного стану складових (апаратних і програмних) системи в цілому.

І на завершення слід зауважити, що вже зараз ми починаємо жити у світі систем із структурною надлишковістю. Найбільш сучасні електронні системи – це типові резервовані системи, по суті, із структурною надлишковістю (Грід-структури, суперкомп'ютери, різноманітні кластери, системи, що використовують так звані «хмарні» обчислення та пам'ять).

СПИСОК ДЖЕРЕЛ

1. Neumann V.J. Probabilistic Logics and Synthesis of Reliable Organisms from Unreliable Components. *in Automata Studies* / eds. C. Shannon, J. McCarthy. Princeton: Princeton University Press, 1956. P. 43–98.
2. Dubrova E. Fault-Tolerant Design. New York: Springer, 2013. 185 p.
3. Avizienis A. Fault-Tolerant Systems. *IEEE Transactions on Computers*. 1976. Vol. 25, N 12. P. 1304–1312.
4. Савченко Ю.Г. Цифровые устройства, нечувствительные к неисправностям элементов. М.: Советское радио, 1977. 169 с.

Стаття надійшла до редакції 27.06.2018