УДК 519.711.2:681.326.7

ПРО РЕАЛІЗАЦІЮ СПОСОБУ ПІДВИЩЕННЯ ВІДМОВОСТІЙКОСТІ УПРАВЛЯЮЧИХ ПРОГРАМ

Бережний А.Г., Куркчі А.П., Ларгін В.А.

ABOUT REALIZATION OF A WAY FOR IMPROVING THE FAULT TOLERANCE OF GOVERNING PROGRAMS

Berezhnii A.G., Kurkchi A.P., Largin V.A.

У статті розглянуті питання підвищення відмовостійкості управляючих програм шляхом застосування принципу мультиверсійності при виконанні програм на мультиядерних мікропроцесорах. Запропоновано спосіб організації відмовостійкого обчислювального процесу в керуючому контролері шляхом впровадження і практичної реалізації трьохверсійного програмування в процес створення ПЗ.

Ключові слова: *відмовостійкість, мультиверсійність, програмне забезпечення, функціональні блоки*

Вступ. Однією з основних проблем при розробці систем управління критичними об'єктами є створення високонадійного програмного забезпечення (ПЗ) керуючих контролерів [1]. При розробці ПЗ повинні вирішуватися два основні завдання:

– створення надійного (безпомилкового) базового програмного забезпечення;

– проектування і включення програмних засобів для забезпечення живучості при програмних, інформаційних і апаратних відмовах.

Відомим методом підвищення достовірності розроблювального ПЗ є застосування об'єктно-орієнтованого і структурного підходів до програмування, перш за все шляхом зменшення числа проектних помилок. При налагодженні написаних програм важливо ретельно провести їх тестування [2]. Повне тестування програми зазвичай нездійсненно на практиці, а експериментальне тестування програм може бути доказом наявності помилок, але ніколи не доведе їх відсутності. Тому підвищення достовірності обчислювального процесу з урахуванням можливих прихованих помилок в програмі є актуальним завданням.

Аналіз останніх досліджень і публікацій. Проблема відмовостійкості в керуючих системах розглядалися в таких роботах: R.T. Wood [3] - розглянуто використання диверсійності у ядерній промисловості, В.С. Харченко [4-6] - проаналізовано моделі багатоверсійних інформаційно-управляючих систем, М.А. Ястребенецького [7], В.В. Скляра [8] - переглянуто можливі способи адаптації у багатоверсійних мажоритарно-резервованих комп'ютерних системах управління, А.В Волкова [9], Ю.Н. Соколова [10] - проаналізовано метод оцінки надійності програмно-технічних комплексів, Є.В. Брежнєва та В.С. Харченко [11] - розглянуто метод оцінки безпеки критичної енергетичної інфраструктури, А.В. Федухіна [12], Н.В. Якимця [13] - розглянуто моделі проектування відмовостійких цифрових систем та ін.

Попри значний внесок в розвиток теорії і практики відмовостійкості керуючих систем, проблема підвищення достовірності розроблювального ПЗ вимагає подальших досліджень з урахуванням додаткових можливостей, що надаються новими розробками електронних компонентів і інформаційних технологій.

Постановка проблеми. Найбільш імовірним джерелом систематичних відмов систем управління є приховані дефекти програмних засобів, внесені при розробці, що не виявлені при тестуванні і верифікації і які з'являються при певному наборі вхідних даних або характеристиках фізичних або інформаційних середовищах. Резервування системи з виконанням ідентичних програмних додатків не вирішує проблему усунення таких дефектів, оскільки вони тиражуються і з'являються одночасно, викликаючи фатальну відмову.

Існує кілька методів мінімізації помилок в програмному забезпеченні. Одним з них є мультиверсійне програмування [14], що являє собою незалежну генерацію $N \geq 3$ функціонально еквівалентних програм (мультіверсій) відповідно до ідентичних вихідних специфікацій на проектування. Для цих N програм надані засоби конкурентного виконання, по ходу якого в певних точках контролю

("cc-points" от cross-check points, точки перехресного контролю) програмами генеруються вектори порівняння ("c-vectors" від comparison vectors, вектори порівняння). Складові векторів порівняння і контрольні точки генерації "с-векторів" попередньо визначені ще на етапі вихідних специфікацій. Застосування мультиверсійного програмування дозволяє знизити ризики систематичних відмов, оскільки в разі проектних дефектів зменшується ймовірність одночасної й однотипної відмови різних версій ПЗ. Тому практична реалізація принципу мультіверсійного програмування є актуальним завданням.

Метою даної статті є висвітлення способу організації надійного відмовостійкого обчислювального процесу в керуючому контролері шляхом впровадження і практичної реалізації принципів мультиверсійного програмування в процес створення ПЗ.

Виклад основного матеріалу В даний час в системах управління широкого поширення набули контролери з мікропроцесорами фірми Intel. Поява високошвидкісних багатоядерних мікропроцесорів (англ. Multi-core) створило передумови для практичної реалізації мультиверсійного обчислювального процесу шляхом апаратної та тимчасової надмірності. Реалізація надійного обчислювального процесу буде розглянуто на прикладі програмного забезпечення, що виконується в контролері з чотирьохядерним процесором за схемою «2 із 3». Вибір схеми обробки за схемою «2 із 3» обумовлений наступним фактором: схеми типу «1 із N» (N=1,2,…) не відповідають вимогам відповідних стандартів (наприклад, [15]) і не можуть застосовуватися в системах управління реального часу (не володіють функціональною безпекою).

Схеми типу «N із N» (N = 1,2, ...) не мають великої надійності. Наприклад, користуючись [16], можна розрахувати, що в схемі «2 із 2» при ймовірності появи прихованого дефекту в циклі управління $p=10^{-7}$ в одній з двох гілок програми середній час напрацювання на відмову системи управління рівне $T_{ср}\approx 14$ h при часу циклу t = 0,01 s.

Схема «2 із 3» при тій же ймовірності появи прихованого дефекту забезпечує середній час напрацювання на відмову $T_{ср}\approx 5285$ років. Застосування схеми «2 із 3» (на відміну від схеми «2 із 2») дозволяє також однозначно визначати гілку програми з проявленим дефектом і міняти результат виконання цієї гілки на вірний. Застосування схем «2 із N» (N = 4,5, ...) недоцільно, тому що на практиці не потрібно такі наднадійні системи і вони складні в реалізації.

Програмне забезпечення систем управління, що функціонує в контролерах, складається з двох блоків - системного і функціонального програмного забезпечення (ФПЗ).

Ядром системного ПЗ є спеціалізована операційна система (ОС) реального часу. Операційна система визначає:

– підтримку функціонування ФПЗ відповідно до налаштованих модулів операційної системи на конфігурацію конкретного виконання і необхідний набір функцій;

– обмін інформацією з зовнішніми абонентами по лініях зв'язку мережевих контролерів;

– обмін інформацією з модулями зв'язку з об'єктами за допомогою введення даних і формування керуючих впливів на об'єкт;

– контроль і захист від несанкціонованого доступу;

– забезпечує можливість паралельного в часі функціонування в рамках одного мікроконтролера (на трьох ядрах) трьох ідентичних по функції гілок однієї програми з процедурами порівняння результатів виконання цих гілок і прийняттям рішень щодо подальшого функціонування за результатами порівняння. Даний режим функціонування забезпечує диверсійність реалізації ФПЗ; контроль працездатності технічних і програмних засобів в процесі функціонування;

– перехід в безпечний режим функціонування при відмові.

ФПЗ реалізує функції системи управління. Воно складається з пакетів програм, що реалізують типові функції:

– управління об’єктом;

– перевірка умов безпеки;

– контроль над об’єктом.

ФПЗ можна умовно розділити на кілька типових програм, що вирішують основні функції та функції взаємодії з персоналом і обладнанням.

База даних включає наступні групи параметрів:

– дані про поточний стан об'єктів;

– команди управління від користувача;

– параметри функціонування програм, сформовані на попередньому такті роботи;

– узагальнені дані про поточний стан об'єктів і результати їх контролю;

– дані результатів перевірки умов безпеки;

– команди управління для об'єктів;

– параметри функціонування програм, сформовані для наступного такту роботи.

Аналіз варіантів побудови ФПЗ показує, що для забезпечення захисту систем управління від систематичних відмов доцільно застосування варіанту, який заснований на принципі «Різні алгоритми, логіка й програмна структура» із залученням трьох незалежних між собою програмістів. При виборі мов трьохверсійного програмування необхідно керуватися стандартом IEC 61131-3 [17], загальновизнаного у світі стандарту по мовах технологічного програмування для програмованих контролерів.

IEC 61131-3 підтримує засоби для паралельного виконання різних фрагментів програми. На основі аналізу IEC 61131-3 до практичної реалізації можна рекомендувати для

першої версії ПЗ - асемблер (IL), другою версією - C++ (клас ST), третій - відповідає класу FBD.

Робота мультиверсійного програмування демонструється на прикладі реалізації функціональних блоків (ФБ) (рис. 1).

До операційної системи входить диспетчер ФБ. Диспетчер ФБ запускає паралельно три функціонально ідентичних ФБ. Для очікування закінчення виконання трьох ФБ використовується команда типу «Multiple wait» (очікування декількох подій). Диспетчер ФБ визначає мажоритарним методом «2 із 3» вірний результат. У разі невідповідності результату одного ФБ відповідне повідомлення передається підсистемі верхнього рівня (для повідомлення оператору, архівації та ін.). Вірний результат виконання записується в базу даних (БД), процес триває, на відміну від двухверсійного варіанту, коли система управління повинна перейти в безпечний стан.

Виконуваний модуль ФБ являє собою фрагмент коду, який запускається диспетчером переходом по таблиці ФБ згідно з номером блоку - першим словом структури поточної викликаючої послідовності. Старший байт слова - номер групи - відповідає функціональному призначенню диспетчера, молодший - вказує безпосередньо на місце адреси модуля блоку в таблиці.

Алгоритм виконання циклу ПЗ наступний (рис. 2):

– запуск трьох модулів ФБ в мікроконтролері;

– виконання модулів ФБ;

– формування результату по принципу мажорірованія «2 із 3»;

– сповіщення оператора, якщо на одному з ланок знайдено помилку;

– запис результату в БД;

– установ покажчика в списку викликів на наступний ФБ.

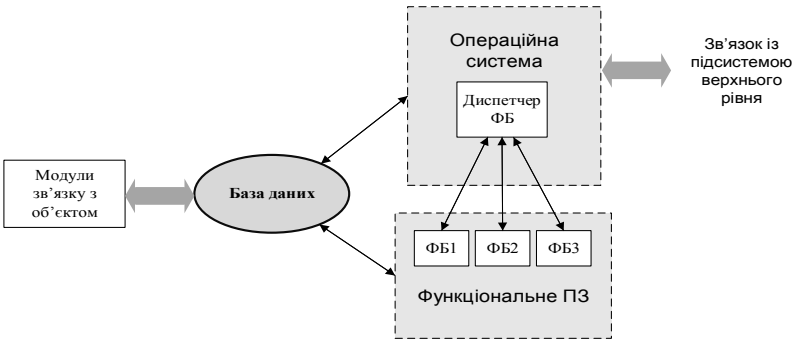

Рис. 1. Структура ПЗ

Рис. 2. Виконання циклу ПЗ

Висновок У статті розглянуто спосіб практичної реалізації трехверсійного керуючого обчислювального процесу в багатоядерному мікропроцесорі керуючого контролера. Даний спосіб дозволяє знизити ризики відмов від прихованих помилок, оскільки в разі проектних дефектів зменшується ймовірність одночасної і однотипної відмови різних версій ПЗ. При застосуванні даного методу також підвищується відмовостійкість ПЗ шляхом реалізації принципу мажорірования «2 із 3» й підвищується коефіцієнт готовності керуючої системи. У системах управління з високими вимогами до надійності розглянутий спосіб може застосовуватися разом з традиційними способами резервування апаратури, наприклад, в контролерах з трьома мікропроцесорами.

Література

1. Єлісєєв В.В., Ларгін В.А., Пивоваров Г.Ю. Програмно-технічні комплекси АСУ ТП: Навч. посібник - К.: Видавничо-поліграфічний центр «Київський університет», 2003.
2. Якість програмного забезпечення глава 10 [Електронний ресурс]: ISO / IEC TR 19759: 2005 Режим доступу: https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:19759:ed-2:v2:en. (Дата звернення: 01.10.2018)
3. Р. Т. Вуд Різноманітні стратегії, спрямовані на пом'якшення наслідків вразливості, що виникла внаслідок загальних причин. Сьоме американське ядерне товариство Міжнародне місце зустрічі з ядерних установок інструменти, контрольні та людських-машинних інтерфейсних технологій NPIC & HMIT 2010, Лас-Вегас, штат Невада, 7-11 листопада 2010 року на CD-ROM, Американське ядерне товариство, Парк LaGrange, IL (2010).
4. Харченко В. С., Скляр В. В., Токарев В. І. Моделі відмовобезпечних структур цифрових систем контролю і управління // Системи ОБРОБКИ інформації.-Х .: ХВУ.-2003 Вип. - 2003. - Т. 4. - С. 200-205.
5. Харченко В.С. Інформаційна технологія підтримки визначення компонентних функціональних структур живучих бортових інформаційно-керуючих систем / В.С. Харченко, Н.П. Бородавка // Збірник наукових праць Харківського національного університету Повітряних Сил. - 2007. - № 1 (13). - С. 82-86.
6. Харченко В.С. Автоматні моделі багатоверсійних інформаційно-керуючих систем / В.С. Харченко, В.В. Скляр, В.А. Головір // Системи ОБРОБКИ інформації. - 2007. - № 1 (59). - С. 108-109.
7. М.А. Ястребенецький, В.Н. Васильченко, С.В. Виноградська та ін. Безпека атомних станцій: Інформаційні управляючі системи: монографія /; під ред. М.Я. Ястребенецький. К.: Техніка, 2004. 472 с.
8. В. В. Скляр, В. С. Харченко, "Відмовостійкі комп'ютерні системи управління з версійно-порогової адаптацією: способи адаптації, оцінка надійності, вибір архітектури", Автомат. і телемех., 2002 № 6, 131-145; Autom. Remote Control, 63: 6 (2002), 991-1003
9. Волкової А.В. та ін. Масштабовані багатоверсійні технології для критичних додатків. Лекції та практикум / Харченко В.С. (Редактор). - МОН України, ХАІ, 2013. - 202с.
10. Соколов Ю.М. Інструментальне оцінювання надійності програмно-технічних комплексів при зростанні інтенсивності відмов / Ю.М. Соколов, В.С. Харченко, Ю.Л. Поночовний // Системи ОБРОБКИ інформації. - 2014. - № 2 (118). - С. 205-211.
11. Брежнєв Є.В. Метод оцінювання безпеки критичної енергетичної інфраструктури з урахуванням надійності цифрової підстанції / Є.В. Брежнєв, В.С. Харченко // Наука і техніка Повітряних Сил Збройних Сил України. - 2014. - № 3 (16). - С. 138-143.
12. А.В. Федухін, А.А. Муха. Забезпечення живучості систем протиаварійної автоматики на гідроелектростанціях. Математичні машини і системи, 2018, № 2. Стор. 169- 194.
13. Якимець Н.В. Відмовостійкі цифрові системи керування з програмованою логікою на основі частково працездатних автоматів: моделі та реалізація / Н.В. Якимець, В.С. Харченко // Системи ОБРОБКИ інформації. - 2007. - № 4 (62). - С. 134-138.
14. Авізеніс, А. Про реалізацію N-версії програмування програмного відмовостійкості під час виконання. / А. Авізеніс, Л. Чен. В Proc. IEEE COMPSAC 77, с. 149-155, 1977.].
15. IEC 61508: 1-6: 2012. Функціональна безпека електричних / електронних і програмованих електронних систем. Частина 3. Вимоги до програмного забезпечення
16. Гнеденко Б.В., Бєляєв Ю.К., Соловйов А.Д., Каштанов В.А. Математичні методи в теорії надійності. 2013. Книжковий дім «ЛІБРОКОМ». М. 550 с.
17. Програмувальні контролери - Частина 3: Мови програмування [Електронний ресурс]: IEC 61131-3:2013 Режим доступу: https://webstore.iec.ch/publication/4552. (Дата звернення: 04.10.2018)

References

1. Eliseev V.V, Largin V.A., Pivovarov G.Y. “Program-technical complex of industrial control system: Navch. School - K.: Vidavnicho-Polygraphic Center "Kyiv University", 2003
2. Software quality chapter 10 [Electronic resource]: ISO / IEC TR 19759: 2005 Mode of access: https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:19759:ed-2:v2:en (Applying Date: 10/01/2018)
3. Wood R. T. Diversity strategies to mitigate postulated common cause failure vulnerabilities. Seventh American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies NPIC&HMIT 2010, Las Vegas, Nevada, November 7-11, 2010, on CD-ROM, American Nuclear Society, LaGrange Park, IL (2010).
4. Kharchenko V.S., Sklyar V.V., Tokarev V.I. Models of the fail-safe structures of digital monitoring and control systems // Sistemki informatsi. – Kh .: KhVU. – 2003. – Vip. - 2003. - V. 4. - pp. 200-205.
5. Kharchenko V.S. Information technology to support the definition of component functional structures of robust on-board information management systems / V.S. Kharchenko, N.P. Wart / / / Zbirnik naukovih prats of Kharkiv National University of the Seventh Force. - 2007. - № 1 (13). - pp. 82-86.
6. Kharchenko V.S. Automaton models of multi-version information control systems / V.S. Kharchenko, V.V. Sklyar, V.A. Golovir // Processing Systems Information. - 2007. - № 1 (59). - pp. 108-109.

7. Yastrebenetsky, M.A. Vasilchenko V.N, Vinogradskaya S.V.. Safety of nuclear power plants: Information control systems: monograph /; by ed. M.Y. Yastrebenetsky. K.: Tehnika, 2004. 472 p.
8. Sklyar V.V., Kharchenko V. S., "Fault-tolerant computer control systems with version-threshold adaptation: methods of adaptation, reliability estimation, choice of architectures", Avtomat. and telemeh., 2002, No. 6, 131-145; Auto Remote Control, 63: 6 (2002), 991-1003
9. Volkovoy A.V. and others. Scalable multi-version technologies for critical applications . Lectures and practical work / Kharchenko V.S. (editor). - MES of Ukraine, KhAI, 2013. - 202s.
10. Sokolov Y.N. Instrumented assessment of the reliability of software and hardware complexes with an increase in the failure rate / Yu.N. Sokolov, V.S. Kharchenko, Yu.L. Ponochovny // Processing Systems Information. - 2014. - № 2 (118). - p. 205-211.
11. Brezhnev E.V. Method for assessing the safety of a critical energy infrastructure taking into account the reliability of a digital substation / E.V. Brezhnev, V.S. Kharchenko // Science and Technology of the Forces of the Forces of Ukraine. - 2014. - № 3 (16). - p. 138-143.
12. Feduhin A.V., Muha Ar.A.. Ensuring the survivability of emergency control systems at hydroelectric power plants. Mathematical Machines and Systems, 2018, No. 2. Page. 169-194.
13. Yakimets N.V. Fault-tolerant digital control systems with programmable logic based on partially working automata: models and implementation / N.V. Yakimets, V.S. Kharchenko // Processing Systems Information. - 2007. - № 4 (62). - p. 134-138.
14. Avizienis, A. On the implementation of N-version programming for software fault-tolerance during execution. / A. Avizienis, L. Chen. In Proc. IEEE COMPSAC 77, c. 149-155, 1977.].
15. IEC 61508: 1-6: 2012. Functional safety of electrical / electronic and programmable electronic systems. Part 3. Software Requirements
16. Gnedenko BV, Belyaev Yu.K., Solovyov A.D., Kashtanov V.A. Mathematical methods in the theory of reliability. 2013. The book house "LIBROKOM". M. 550 s.
17. Programmable Controllers - Part 3: Programming Languages [Electronic Resource]: IEC 61131-3: 2013 Access Mode: https://webstore.iec.ch/publication/4552. (Date of appeal: 10.4.2018)

Бережной А.Г., Куркчи А.П., Ларгин В.А. Про реализацию способа повышения достоверности выполнения управляющих программ

В статье рассмотрены вопросы повышения отказоустойчивости управляющих программ за счет применения принципа мультиверсионности при выполнении программ на мультиядерном микропроцессоре.

Ключевые слова: *отказоустойчивость, мультиверсионность, программное обеспечение, функциональные блоки*

Berezhnoy A.G., Kurkchi A.P., Largin V.A. About realization of a way for improving the fault tolerance of governing programs

The article deals with the issues of increasing the failure rate of control programs by applying the principle of multiversionality when executing programs on the multicore microprocessor.

Key words: *fault tolerance, multiverse, software, functional blocks*

Бережной Анатолій Геннадійович – студент, anatoliy.berg95@gmail.com
Куркчі Антон Павлович – студент, mexanikoooo77777@gmail.com
Ларгін Віктор Анатолійович – к.т.н., доцент СНУ ім. В. Даля, viktorlargin1@gmail.com

Рецензент: д.т.н., проф. ***Рач В.А.***

Стаття подана 11.10.2018