УДК 004.052.42

Б. М. КОНОРЕВ[1], В. В. СЕРГИЕНКО[1], В. С. ХАРЧЕНКО[1], Г. М. ЖОЛТКЕВИЧ[2]

[1] Национальный аэрокосмический университет им. Н. Е. Жуковского "ХАИ", Украина
[2]Харьковский национальный университет им. В. Н. Каразина, Украина

ПРОГНОЗИРОВАНИЕ ВЕРОЯТНОСТИ СКРЫТЫХ ДЕФЕКТОВ КРИТИЧЕСКОГО ПО С ЗАДАННОЙ ТОЧНОСТЬЮ

Для количественной оценки надежности и функциональной безопасности критических систем одной из ключевых характеристик является прогноз вероятности скрытых дефектов. В статье представлен метод прогнозирования вероятности скрытых дефектов критического программного обеспечения (ПО) с заданной (управляемой) точностью результатов. Для рамочной оценки скрытых дефектов предложена модель остаточных и скрытых дефектов. Приведена процедура экспериментальной калибровки чувствительности к дефектам и степени разнообразия методов контроля бездефектности исходных кодов ПО.

Ключевые слова: *программное обеспечение, model-checking верификация, инварианты, вероятность скрытых дефектов, инъекция дефектов.*

Введение

Возможный ущерб от проявления дефекта ПО на системном уровне при эксплуатации информационно-управляющих систем (ИУС) критического применения может лежать в диапазоне «материальные потери – ущерб окружающей среде - угроза здоровью и жизни человека». Скрытые дефекты (не обнаруженные при тестировании) в критическом ПО являются существенными факторами риска, поскольку могут привести к отказу ИУС при выполнении функций, связанных с безопасностью. Поэтому прогноз вероятности скрытых дефектов – одна из важнейших задач квалификационных испытаний и регулирования рисков эксплуатации систем, связанных с безопасностью.

В данный момент для проверок характеристик надежности и функциональности критического ПО все более широко используется model-checking подход [1]. Проверки на моделях могут быть реализованы в режиме статического анализа [2]. Для подтверждения отсутствия скрытых дефектов может быть использован полимодельной model-checking подход [3, 4]. Данный подход заключается в проверках исходных кодов критического ПО на инвариантно-ориентированных моделях. Для проверки корректности каждого программного инварианта (неизменного свойства или атрибута ПО) в режиме статического анализа исходных кодов ПО формируются инвариантно-ориентированные модели. Каждая такая модель проверяемого проекта ПО содержит все необходимые данные для контроля конкретного инварианта. Далее методы измерения инвариантов, используя инвариантно-ориентированные модели как входные данные, реализуют алгоритм контроля значений конкретных инвариантов. Каждый метод измерения инвариантов либо подтверждает неизменность инварианта, либо обнаруживает нарушения. Доказательность подхода заключается в использовании принципа разнообразия, - для обнаружения скрытых дефектов используются различные (диверсные) методы измерения инвариантов, имеющие в общем случае различную чувствительность к дефектам (степень диверсности - степень отличия между собой). Для оценки чувствительности и степени разнообразия методов может быть использована процедура искусственного внесения дефектов[5].

В статье предложен подход прогнозирования вероятности скрытых дефектов основанный на оценке чувствительности и степени разнообразия методов измерения инвариантов.

Основой для прогнозирования вероятности скрытых дефектов является теоретико-множественная модель скрытых и остаточных дефектов ПО, которая позволяет получить рамочную оценку вероятности скрытых дефектов. Для параметризации модели используется процедура экспериментальной калибровки чувствительности и степени разнообразия методов измерения инвариантов, основанная на использовании «точечной» инъекции тестовых дефектов.

В результате обработки собранных в ходе калибровки данных, может быть определена степень разнообразия используемых методов измерения ин-

вариантов, произведена оценка полноты покрытия исходного кода проверками и установлена область остаточных дефектов и граничная область нахождения скрытых дефектов.

1. Модель остаточных и скрытых дефектов ПО

Для оценки эффекта от использования различных методов измерения инвариантов предлагается теоретико-множественная модель остаточных и скрытых дефектов ПО для композиции методов измерения инвариантов (см. рис. 1).

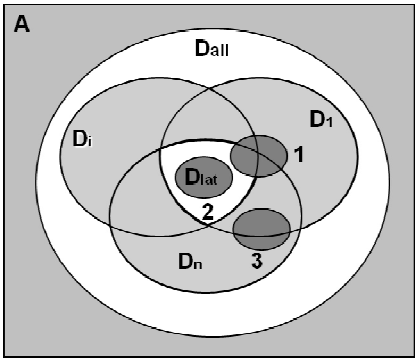

Рис. 1. Модель скрытых дефектов для диверсных методов измерения инвариантов:
D_{all} – множество возможных дефектов в пространстве адресов программного обеспечения A; D_i – множество дефектов, не обнаруживаемых методом измерения i-го типа инварианта; D_{lat} – множество скрытых дефектов

Скрытый (латентный) дефект – некорректность программного кода или документации, которая может привести к одному или более отказам компонента системы или всей системы, не выявленная при разработке и тестировании. Именно на устранении или определении области нахождения данного типа дефектов должны быть сосредоточены усилия при квалификационных испытаниях, включающих независимую верификацию ПО. Прогноз вероятности скрытых дефектов предлагается получить опосредовано, исходя из данных об остаточных дефектах. Остаточные дефекты для методов измерения инвариантов – дефекты, не обнаруживаемые использованными методами измерения инвариантов. Область нахождения остаточных дефектов может быть установлена экспериментально в результате процедуры калибровки используемых методов измерения инвариантов для конкретного проекта.

Модель, представленная в виде диаграммы Эйлера – Венна на рис. 1, иллюстрирует возможные взаимные расположения множеств остаточных и скрытых (латентных) дефектов и позволяет оценить выигрыш от использования методов измерения инвариантов для различных вариантов взаимного расположения (суперпозиции) множеств остаточных дефектов.

Индикатором оценки достигаемого эффекта от последовательной реализации композиции методов измерения инвариантов при независимой верификации является величина (в %), на которую уменьшается граничное, рамочное значение вероятности скрытых (латентных) дефектов P_{lat}:

$$I = \frac{\left| D_{lat} \setminus \bigcap_{i=1}^{n} D_i \right|}{\left| D_{lat} \right|} * P_{lat}, \qquad (1)$$

где n – количество использованных методов.

Пересечение подмножеств остаточных дефектов представляет рамочную оценку вероятности скрытых дефектов, которая может быть использована как прогноз.

Абсолютный выигрыш от использования методов измерения инвариантов определяется степенью разнообразия методов измерения инвариантов в условиях конкретного проекта. При этом можно выделить 3 варианта:

а) теоретически возможный случай уменьшения вероятности скрытых дефектов на 100% (I=1, позиция 3):

$$\left(\bigcap_{i=1}^{n} D_i \right) \cap D_{lat} = \varnothing, \qquad (2)$$

б) максимально неблагоприятный вариант (I=0, позиция 2):

$$D_{lat} \subset \bigcap_{i=1}^{n} D_i, \qquad (3)$$

в) общий случай ($I \in (0,1)$, позиция 1):

$$\left(\bigcap_{i=1}^{n} D_i \right) \cap D_{lat} \neq \varnothing. \qquad (4)$$

Если при независимой верификации не будут обнаружены скрытые дефекты (элементы множества D_{lat}), то, хотя индикатор достигаемого эффекта I=0, подмножество $\bigcap_{i=1}^{n} D_i$ может использоваться как граничная область нахождения скрытых дефектов (является рамочной оценкой вероятности скрытых дефектов). Устанавливается область (множество), где дефекты гарантированно отсутствуют – $\overline{\bigcap_{i=1}^{n} D_i}$. Для улучшения или уточнения оценки усилия необходимо сосредоточить на анализе (поисках дефектов внутри) области $\bigcap_{i=1}^{n} D_i$.

Таким образом, предложенная теоретико-

множественная модель, позволяет определить область нахождения скрытых дефектов и установить выигрыш при использовании диверсных методов измерения инвариантов для различных вариантов расположения оцениваемого множества скрытых дефектов.

2. Процедура калибровки

Для численного прогноза вероятности скрытых дефектов конкретного проекта ПО в соответствии с предложенной моделью остаточных и скрытых дефектов (см. рис. 1) необходимо получить экспериментальные данные по чувствительности и степени разнообразия используемых методов измерения инвариантов. Параметризация модели осуществляется с помощью процедуры экспериментальной калибровки используемых методов измерения инвариантов методом «точечной» инъекции тестовых дефектов. Предлагаемый метод представляет «точечную» (капельную) инъекцию тестового дефекта определенного типа в выбранное место ПО, бинарную оценку чувствительности методов измерения инвариантов (обнаружение/необнаружение внесенного дефекта) и возврат ПО в исходное состояние (удаление тестового дефекта). Под «точечной» инъекцией понимается единичное внесение дефекта, что гарантирует отсутствие взаимного влияния и появления вторичных дефектов из-за интерференции и мутации внесенных дефектов.

Для оценки полноты тестового покрытия и чувствительности методов для каждого шага (слоя) калибровки необходимо выполнить следующие действия:

1. Формирование профиля тестовых дефектов, используя результаты синтаксического и семантического разбора в режиме статического анализа исходного кода ПО.

2. Последовательный выбор типа дефекта и внесение в проверяемое ПО единичного дефекта выбранного типа.

3. Проверка всеми методами измерения инвариантов.

4. Фиксация обнаружения/необнаружения внесенного тестового дефекта для каждого метода.

5. Возврат ПО к исходному начальному состоянию (до инъекции дефекта) и повтор процедуры с п.2.

Процедура выполняется циклически для всех типов дефектов, возможных для конкретного проекта.

Необходимое количество инъектируемых дефектов (количество шагов) для каждого типа дефектов определяется исходя из требуемой точности (достоверности, степени неопределенности) результатов.

Экспериментальная калибровка чувствительности каждого метода и интегральной чувствительности композиции диверсных методов производится в контексте пространства калибровочных испытаний P_{cal}, представляющего Декартово произведение

$$P_{cal} \subseteq N \times M \times T, \quad (5)$$

где $N=\{n_i\}$ – множество инъекций тестовых дефектов, реализованных при калибровке;

$M=\{m_j\}$ – множество калибруемых методов измерения инвариантов;

$T=\{t_k\}$ – множество типов инъектируемых тестовых дефектов или профиль тестовых дефектов (ПТД). ПТД для конкретного проекта определяется используемым составом языковых конструкций. Каждая конструкция может быть искажена определенными типами дефектов, инъекция которых не приведет к нарушению синтаксиса и семантики программы (т.е. внесение дефекта не приведет к ошибке при компиляции). Именно эти типы дефектов формируют ПТД конкретного проекта.

P_{cal} определяет множество (кортеж) исходов – результатов экспериментов при калибровке. Значение элемента P_{cal} с координатой $(n_i; m_j; t_k)$ принимает значение 0, если тестовый дефект не обнаружен, или 1, если тестовый дефект обнаружен.

Инъекция кортежа $T=\{t_k\}$ при калибровке метода $M=\{m_j\}$ представляет шаг или слой калибровки в пространстве P_{cal}.

Каждый шаг калибровки (приращение по оси N) можно представить как «секущую плоскость»: выполняется инъекция дефектов из профиля тестовых дефектов и производится проверка всеми методами.

На каждом шаге «секущей плоскости» могут быть определены:

1. Дизъюнкция необнаруженных дефектов тестового профиля для каждого M_i

$$D_{fault\_i} = \bigcup_{j=1}^{m} D_j. \quad (6)$$

2. Конъюнкция необнаруженных дефектов по каждому типу дефектов тестового профиля для всех M_i

$$D_{t\_k} = \bigcap_{i=1}^{n} D_i. \quad (7)$$

3. Парциальная чувствительность каждого метода $P_{part\,ji}$ по каждому типу дефекта.

По результатам калибровки определяется:

1. Интегральная чувствительность каждого метода для выбранного ПТД:

$$P_j = \bigcup_{i=1}^{k} P_{part\,ji}, \quad (8)$$

где k – общее количество типов дефектов;

$P_{part\ ji}$ – парциальная чувствительность j–го метода к i-му типу дефекта (чувствительность к конкретному типу дефекта);

2. Попарно для всех M_i (каждого с каждым) абсолютная и относительная степень разнообразия:

$$m_{ijabs} = \left|P_i \Delta P_j\right| = \left|P_i \cup P_j\right| \setminus \left|P_i \cap P_j\right|, \quad (9)$$

$$m_{ij} = 1 - \frac{\left|P_i \cap P_j\right|}{\left|P_i \cup P_j\right|}, \quad (10)$$

где i и j принимают значения от 1 до n;

n – количество использованных методов.

Используя полученные данные может быть определен набор методов измерения инвариантов, обеспечивающий достижение заданного значения полноты тестового покрытия и достоверности (с заданной точностью) прогноза вероятности скрытых дефектов.

3. Обработка результатов калибровки

Обработка собранных в ходе калибровки данных позволяет вычислить ряд метрик.

Численное выражение парциальной чувствительности метода к каждому типу дефекта определяется как:

$$S_{partij} = \frac{n_{det\,ij}}{n_i} * 100\%, \quad (11)$$

где n_i – общее количество измерений по i-му типу дефектов;

$n_{det\ ij}$ – количество измерений, в которых j-й метод обнаружил i-й тип дефекта.

Минимально необходимое количество измерений n рассчитывается исходя из установленных требований достоверности результатов. При этом гарантируется, что расхождение между истинным и рассчитанным средним измеренным значением не превысит допустимое отклонение.

Процент обнаруженных дефектов по каждому типу $S_{det\ i}$.

$$S_{deti} = \frac{n_{det\,i}}{n_i} * 100\%, \quad (12)$$

где $n_{det\ i}$ – количество измерений, в которых хоть один метод обнаружил i-й тип дефекта.

Процент обнаруженных дефектов для каждого метода S_j.

$$S_j = \frac{\sum_{i=1}^{k} n_{det\,ij}}{\sum_{i=1}^{k} n_{det\,i}} * 100\%, \quad (13)$$

где k – количество типов дефектов.

Примечание: возможен случай, когда 2 метода обнаруживают один и тот же тип дефектов, но не имеют общих обнаруженных конкретных дефектов (нашли дефект в разных местах инъекции). В этом случае для повышения степени покрытия необходимо использовать оба метода.

В итоге вероятность наличия скрытых дефектов P_{lat} определяется как:

$$P_{lat} = \frac{\sum_{i=1}^{k} (S_{deti} * r_i / 100)}{\sum_{i=1}^{k} r_i} * 100\%, \quad (14)$$

где r_i – количество конструкций в коде, в которых возможен i-й тип дефекта.

4. Апробация

Апробация представленного подхода прогнозирования вероятности скрытых дефектов была выполнена в ходе проекта Украинского научно-технологического центра #4726, а также при экспертизе программно-технических комплексов разработки ЧАО «СНПО «Импульс». Model-checking верификация была реализована в режиме статического анализа исходных кодов ПО на платформе IDE Eclipse. Разработанный Мобильный инструментальный комплекс позволил выполнить проверки сохранности значений ряда инвариантов, в том числе:

– инвариантов потока управления (сводимость потока управления, потенциальная достижимость и «живость» операторов);

– инвариантов использования оперативной памяти в конкретном проекте ПО;

– специфических инвариантов ИУС на компонентах FPGA.

Была обеспечена возможность проведения независимой верификации при модернизации и доработках критического ПО непосредственно на объектах заказчика без вмешательства (останова) в технологические процессы (например, при модернизации критического ПО ИУС для АЭС).

Заключение

Предложенный подход для прогнозирования вероятности скрытых дефектов позволяет при независимой верификации критического ПО выполнить оценку (прогноз) вероятности скрытых дефектов с контролируемой (требуемой) точностью. Точность является управляемой величиной при практической реализации процедуры калибровки и определяется полнотой профиля тестовых дефектов и принятым количеством внесений тестовых дефектов.

Предложенная модель остаточных и скрытых дефектов позволяет выполнить рамочную оценку остаточных дефектов, оценить область нахождения скрытых дефектов и полноту тестового покрытия.

Предложенный метод разработан в рамках инвариантно-ориентированного model-checking подхода к верификации критического ПО, но сфера его использования может быть расширена и на другие подходы (модели).

Литература

1. Peled, D. Model Checking [Text] / D. Peled, P. Pelliccione, P. Spoletini // Wiley Encyclopedia of Computer Science and Engineering, 2009. – С. 1904–1920.

2. Moiseev, M. Static Analysis Approach for Defect Detection in Multithreaded C/C++ Programs. [Text]/ M. Moiseev // Материалы 5-го Междунар. семинара Software Engineering for Resilient Systems (SERENE 2013). – Springer LNCS. Vol. 8166. 2013. - С. 169-183.

3. Инвариантно-ориентированная оценка качества программного обеспечения космических систем [Текст] : монография / Б. М. Конорев, В. С. Харченко, Ю. Г. Алексеев, Ю. С. Манжос, В. В. Сергиенко, Г. Н. Чертков / Под ред. Б. М. Конорева, В. С. Харченко. – Харьков, 2009. – 224 с.

4. Konorev, B. The Evidential Independent Verification of Software of Information and Control Systems, Critical to Safety: Functional Model of Scenario. [Text] / B. Konorev, V. Sergiienko, G. Chertkov // Proceedings of IEEE East-West Design & Test Symposium (EWDTS'2011). – Kharkov : KNURE, 2011. – С. 263-266.

5. *Cotroneo, D. Introduction to Software Fault Injection. [Text] / D. Cotroneo, H. Madeira // Innovative Technologies for Dependable OTS-Based Critical Systems Challenges and Achievements of the CRITICAL STEP Project. – Springer Milan, 2013. – С. 1-15.*

Поступила в редакцию 10.03.2014, рассмотрена на редколлегии 24.03.2014

Рецензент: д-р техн. наук, проф. В. О. Мищенко, Харьковский национальный университет, Харьков, Украина.

ПРОГНОЗУВАННЯ ІМОВІРНОСТІ ПРИХОВАНИХ ДЕФЕКТІВ КРИТИЧНОГО ПЗ ІЗ ЗАДАНОЮ ТОЧНІСТЮ

Б. М. Конорев, В. В. Сергієнко, В. С. Харченко, Г. М. Жолткевич

Для кількісної оцінки надійності та функціональної безпеки критичних систем однією з ключових характеристик є прогноз ймовірності прихованих дефектів. У статті представлений метод прогнозування ймовірності прихованих дефектів критичного ПЗ із заданою (керованою) точністю результатів. Для рамкової оцінки прихованих дефектів запропонована модель залишкових і прихованих дефектів. Наведена процедура експериментального калібрування чутливості до дефектів і ступеню різноманітності методів контролю бездефектності кодів ПЗ.

Ключові слова: програмне забезпечення, model - checking верифікація, інваріанти, ймовірність прихованих дефектів, ін'єкція дефектів.

ESTIMATING OF CRITICAL SOFTWARE LATENT FAULTS WITH REQUIRED TRUSTWORTHINESS

B. M. Konorev, V. V. Sergiyenko, V. S. Kharchenko, G. N. Zholtkevych

The estimation of latent faults probability is a key indicator for quantitative assessment of critical systems reliability and safety. The article presents the method of latent faults probability estimating for critical software with a required (controlled) trustworthiness. Compositional set-theoretical model of residual and latent faults is proposed for framework assessment of latent faults. The procedure of the experimental calibration of faults sensitivity and diversity degree of inspection methods of source software faultlessness is presented.

Key words: critical software, model-checking, invariants, latent faults probability, fault injection.

Конорев Борис Михайлович – д-р техн. наук, проф., профессор кафедры инженерии программного обеспечения Национального аэрокосмического университета им. Н. Е. Жуковского «ХАИ», г. Харьков, Украина, e-mail: bkonorev@gmail.com.

Сергиенко Владимир Владимирович – канд. техн. наук, руководитель испытательной лаборатории Сертификационного центра АСУ, г. Харьков, Украина, e-mail:admin@scasu.com.

Харченко Вячеслав Сергеевич – д-р техн. наук, профессор, заведующий кафедрой компьютерных систем и сетей Национального аэрокосмического университета им. Н. Е. Жуковского "ХАИ", г. Харьков, Украина, e-mail: V.Kharchenko@khai.edu.

Жолткевич Григорий Николаевич – д-р техн. наук, профессор, декан механико-математического факультета, заведующий кафедрой теоретической и прикладной информатики Харьковского национального университета им. В. Н. Каразина, г. Харьков, Украина, e-mail: g.zholtkevych@karazin.ua.