ДИВЕРСИТЕТНЫЕ АКСИОМАТИЧЕСКИЕ БАЗИСЫ ДЛЯ РАЗРАБОТКИ БЕЗОПАСНЫХ И ОТКАЗОУСТОЙЧИВЫХ СИСТЕМ

Б.В. Сивко
Кафедра микропроцессорной техники и информационно-управляющих систем,
Белорусский государственный университет транспорта
Гомель, Республика Беларусь
E-mail: {bsivko}@gmail.com

Представлено логическое основание для общего подхода в проектировании безопасных и отказоустойчивых систем, заключающееся в рассмотрении понятия диверситета аксиоматических базисов. Приведено описание того, как при разработке аппаратно-программных комплексов на основании диверситетных аксиоматических базисов можно формализовать условия диверситета и защиты от отказа по общей причине. Рассматриваются особенности и преимущества проектирования и последующего анализа на безопасности в сравнении с классическим доказательством безопасности.

Введение

В настоящее время одной из актуальных задач является разработка методов и средств, позволяющих проектировать и верифицировать отказоустойчивые микроэлектронные системы. Данная необходимость обусловлена высокими требованиями по безопасности и надежности исполнения аппаратно-программных комплексов (АПК), которые относятся к критически важным объектам информатизации (КВОИ). Отказоустойчивые микроэлектронные системы, связанные с безопасностью, используются в таких отраслях промышленности, как железнодорожный и морской транспорт, авиация, медицина, атомная энергетика, космос, опасное химическое производство и др. [1, 2] Считается, что для обеспечения безопасности требуется применять комплексный подход, заключающийся в проведении множества мероприятий на всех этапах жизненного цикла АПК. Одним из таких способов, рекомендованных стандартом IEC 61508 [3], является создание диверситетных аппаратных и программных средств, что позволяет защититься от отказов по общей причине (common cause failure, CCF).

I. Актуальность

К методам создания диверситета относятся N-версионное программирование, привлечение независимых экспертов, выбор различных компиляторов и используемого программного обеспечения (ПО) и др. [4, 5] Разработка и верификация КВОИ ведется на основании стандарта IEC 61508, согласно которому для оценки уровня диверситета могут быть использованы BETA-метод и модель BETAPLUS [3]. Однако в настоящее время все диверситетные методы являются экспертными и существует необходимость их формализации.

Основной проблемой существующих методов является то, что само допущение того, что ошибки совершаются независимо, неверно [2, 6]. Второй проблемой CCF является несовершенство существующих моделей, которое заключается в их ограничениях, в неполном отражении зависимости процессов и во влиянии человеческого фактора [7].

Дополнительной необходимостью разработки формализованных диверситетных методов является сложность решения проблемы для ПО. Для обеспечения аппаратного диверситета широко используется физическое разделение компонентов и защита от всевозможного влияния друг на друга [2, 7]. В случае верификации ПО такие подходы применять невозможно.

II. Диверситетные аксиоматические базисы

От каждого устройства, относящегося к КВОИ, требуется доказательство безопасности его функционирования. В общем случае оно представляет собой цепь дедуктивных умозаключений, базирующихся на аксиоматическом базисе, результатом которых должен быть вывод о целевом качестве рассматриваемой системы.

Под аксиоматическим базисом (далее базис) будем понимать некоторое множество формализованных утверждений. Если данные утверждения выполняются для системы в рассматриваемом состоянии, то будем считать, что базис истинен для состояния данной системы.

Примеры утверждений базиса:

- все инструкции микропроцессора выполняются согласно его спецификации;
- тактовая частота генератора микропроцессора находится в заданных конкретных пределах;
- изменения ячеек памяти из-за агрессивной электромагнитной обстановки происходят не чаще заданного предела по времени и не больше некоторого предела бит.

Сами утверждения могут быть любыми, но они задают уровень абстракции таким образом, чтобы в рамках данной аксиоматики верифи-

Библиотека БГУИР

цировать свойства системы. Так, вышеописанные утверждения базиса позволяют верифицировать АПК, который работает в условиях сложной электромагнитной обстановки, а базис Хоара [8] позволяет верифицировать алгоритм работы ПО.

Ряд утверждений базиса может подразумеваться неявно, но использоваться при доказательстве безопасности. Например, если рассматривается базис в рамках спецификаций языка программирования, то он перестает выполняться в случае, если у микропроцессора произошел отказ тактового генератора и исполняемая программа будет остановлена. Данная проблема показывает потенциальную вероятность проявления CCF и должна решаться либо с помощью более высокоуровневой абстракции, либо посредством применения других подходов. Кроме того важно отметить, что выбор базиса не всегда может быть полным, но при этом является важным для решения проблем валидации [9].

Предлагаемый метод заключается в рассмотрении нескольких диверситетных аксиоматических базисов, которые являются независимыми друг от друга.

III. Применение

Предполагается, что описываемый подход с диверситетными аксиоматическими базисами будет использован на ранних этапах разработки. Проектирование и разработка просходит таким образом, что система одновременно выполняет некоторую функцию как в некотором базисе A, так и в некотором базисе B, и при этом базисы являются диверситетными. Особенностью такой реализации является то, что в случае нарушения одного из условий, независимых от одного из базисов, АПК остается в состоянии, когда выполняется другой базис, и тем самым система продолжает выполнять свою функцию. Как результат, АПК обладает определенным формализованным свойством защиты от CCF исходя из свойств выбранных базисов.

В общем случае считается, что подход, позволяющий создавать систему, устойчивую к заданному типу отказов, является хорошей стратегией по обеспечению защиты от CCF для отказоустойчивых и безопасных систем [7]. Это особенно актуально для микропроцессорных систем, в которых один и тот же элемент может использоваться множество раз для различных операций, и, как следствие, отказ такого элемента приводит к CCF всех функций, которые от него зависят [4].

Следует отметить, что данный подход дает возможность задать уровень диверситета на ранних этапах разработки, наделить рассматриваемый АПК целевыми свойствами и доказать её отказоустойчивость и безопасность.

Заключение

В докладе представлено описание логического основания и общего подхода для проектирования безопасных и отказоустойчивых систем на основании диверситетных аксиоматических базисов. Данный подход предлагает общую теоретическую основу, позволяющую проводить формализацию аппаратного и программного диверситета на этапе проектирования АПК.

В докладе рассматривается:

- классическое доказательство безопасности;
- диверситетные аксиоматические базисы и их свойства;
- задачи разработки отказоустойчивых систем на основании диверситетных аксиоматических базисов;
- примеры типовых решений с применением диверситетных аксиоматических базисов;
- общая методика применения диверситетных аксиоматических базисов для проектирования отказоустойчивых систем.

Данный подход прошел апробацию, которая показывает, что с помощью него возможно создание отказоустойчивых систем, что позволяет поднять их уровень надежности и безопасности.

1. Neumann, P.G. Computer-Related Risks / Peter G. Neumann, Addison Wesley. – 1995.
2. Leveson, N. Safeware: System Safety and Computers / Nancy Leveson, Addison-Wesley. – 1995.
3. David Smith, J. «Safety Critical Systems Handbook. A Straightforward Guide to Functional Safety, IEC 61508 and Related Standards, Including Process IEC 61511 and Machinery IEC 62061 and ISO 13849» / J. David Smith, G. L. S. Kenneth // Elsevier Ltd. – 2010.
4. Бочков, К. А. Микропроцессорные системы автоматики на железнодорожном транспорте : учеб. пособие / К. А. Бочков, А. Н. Коврига, С. Н. Харлап; М-во образования Респ. Беларусь, Белорусский государственный университет транспорта. – Гомель. – 2013.
5. Chen, L. N-Version Programming: A Fault-Tolerance Approach to Reliability of Software Operation / Chen L., Avizienis, A., Proceedings of the Eighth Annual International Conference on Fault Tolerant Computing. – Toulouse, France. – PP.3-9. – June 1978.
6. Knight, C. K. An Experimental valuation of the Assumption of Independence in Multiversion Programming / John C. Knight and Nancy . Leveson. // IEEE Transactions on Software Engineering. – Vol. SE-12, No.1. – January, 1986.
7. Parry, G. W. Common Cause Failure Analysis: A Critique and Some Suggestions / Gareth W. Parry, Reliability Engineering and System Safety. – Vol. 34, Is. 3. – 1991. – PP. 309–326.
8. Hoare, C. A. R., An axiomatic basis for computer programming / C. A. R. Hoare // Communications of the ACM. – Is. 12(10):576—580, 583 October, 1969.
9. Бочков К.А., Выбор и определение функции безопасности при верификации микропроцессорных систем железнодорожной автоматики и телемеханики / Бочков К.А., Сивко Б. В. // ООО Издательский Дом «Технологии», Надёжность. – Минск. – 2014. – №2(49).

Библиотека БГУИР