ПРИМЕНЕНИЕ АКСИМАТИКО-БАЗИСНОГО ПОДХОДА ДЛЯ РАЗРАБОТКИ БЕЗОПАСНЫХ И ОТКАЗОУСТОЙЧИВЫХ СИСТЕМ

Б. В. Сивко
Лаборатория «Безопасность и электромагнитная совместимость технических средств»,
Белорусский государственный университет транспорта
Гомель, Республика Беларусь
E-mail: bsivko@gmail.com

Рассмотрены основные положения аксиоматико-базисного подхода и основанная на нем разработка безопасных и отказоустойчивых систем. Показано, что применение диверситетных аксиоматических базисов во время проектирования позволяет формализованно и целенаправленно усиливать диверситет, что позволяет решать проблему отказов по общей причине. Также рассматривается взаимная проверка аксиоматических базисов, предоставляющая способ создания безопасных систем и улучшения показателей их отказоустойчивости. Утверждения подхода проверены посредством имитационных испытаний. На примерах показывается практика разработки и верификации систем с помощью описываемого подхода.

Введение

Для современных систем, связанных с безопасностью, актуальной задачей является создание методов и средств, позволяющих решать ключевые проблемы безопасности и отказоустойчивости. Необходимость обусловлена высокими требованиями исполнения, так как данные системы относятся к критически важным объектам информатизации, которые используются в таких отраслях промышленности, как железнодорожный и морской транспорт, авиация, медицина, атомная энергетика, космос, опасное химическое производство и др. [1] В настоящее время считается, что для обеспечения требуемого уровня безопасности и отказоустойчивости требуется применять множество методов и средств на всех этапах жизненного цикла [2]. Как следствие, практикуются комплексные решения, включающие в себя разные подходы, концепции, стратегии обеспечения безопасности и т.д. [3, 4] Отказы по общей причине (common cause failure, CCF) являются одной из ключевых проблем, для решения которой, согласно стандарту IEC 61508 [5], рекомендуется создание диверситетных аппаратных и программных средств. Однако, рекомендованные стандартом подходы являются экспертными, что ограничивает эффективность и глубину решения, и поэтому существует необходимость формализации.

Рассматриваемый аксиоматико-базисный подход (АБП) [6] позволяет проводить разработку и верификацию безопасных и отказоустойчивых систем в формализованном виде. В настоящее время показано и подтверждено результатами имитационных испытаний, что АБП позволяет формализованно и целенаправленно усиливать диверситет, определять факторы CCF и выявлять их, формализованно разрабатывать средства самотестирования и доказывать их полноту.

I. Положения подхода

Аксиоматическим базисом (далее базис) считается некоторое множество утверждений (условий) [6]. Если они выполняются для системы в рассматриваемом состоянии, то считается, что базис истинен (выполняется) для состояния данной системы. Например, в качестве утверждений могут выступать корректность выполнения инструкций микроконтроллера, условия выполнения некоторого протокола, частота отказов аппаратных средств и т.д.

АБП строится на следующих положениях [6]:

- безопасность и отказоустойчивость системы является функцией от базиса;
- отказ в системе рассматривается как нарушение одного из утверждений базиса.

Основным понятием при анализе является базис, на который опираются функции системы. Соответственно, в случае отказа та функциональность, разработка или доказательство которой основывались на истинности нарушенных утверждений, может перестать выполняться. Но та часть системы, которая не зависит от нарушенных утверждений, останется в работоспособном состоянии.

Основными задачами АБП являются:

- защита аксиом – выбор наименее подверженных отказам базисов и их защита;
- проверка базисов – процедуры определения выполнимости базиса как для доказательства безопасности и отказоустойчивости систем, так и для их проверки в реальном времени;
- разработка методов и средств на основе базисов – поиск эффективных решений, позволяющих оперировать базисами таким образом, чтобы улучшать показатели безопасности и отказоустойчивости.

В рамках АБП в настоящее время показано, как можно сравнивать системы на отказоустойчивость и безопасность, улучшать соответствующие показатели, оперировать базисом как степенью свободы, выполнять интеграцию и диверсификацию систем, а также обнаруживать отказы средствами самодиагностики [6].

II. Диверситетные аксиоматические базисы

Целевая задача диверситетных базисов [7] заключается в их выборе или изменении таким образом, чтобы базисы были наиболее сильными относительно диверситета. В результате таких действий общий базис должен стать как можно меньшим. АБП говорит о том, что отказы, не затрагивающие общий базис, будут проявляться в диверситетных каналах по-разному. Как следствие, проблему обнаружения отказов и защиты от них в диверситетных базисах можно решать соответствующими средствами (например, сравнением выходных сигналов). В то же время, общий базис должен быть проверен вне доказываемой теории (с привлечением внешних средств, которые, например, в случае выявления отказа, влияющего на общий базис, переводят систему в безопасное состояние с помощью специальных аппаратных схем защиты). При этом данная проверка формализована в рамках АБП, когда предоставляется определенный набор утверждений, который требуется проверить, например, с помощью самотестирования или самопроверки.

Таким образом, диверситетные аксиоматические базисы позволяют формализованно и целенаправленно усиливать диверситет, а также выполнять его верификацию.

III. Взаимная проверка аксиоматических базисов

Взаимная проверка аксиоматических базисов [8] заключается в рассмотрении диверситетных базисов, в которые встроены процедуры проверки друг друга. Другими словами, система может на основании утверждений одного базиса определить истинность утверждений другого и соответственно отреагировать на обнаруженную проблему. Применение АБП в таком ключе позволяет выполнять самодиагностику, доказывать её полноту и решать проблему обнаружения маскируемых отказов. Показано, что для эффективного решения необходимо выделять отдельные базисы как для проверки условий выполнимости другого базиса, так и для выполнения функциональности системы. Отделение первых базисов от вторых позволяет облегчить разработку и процедуру верификации, и в то же время идет разделение задач обеспечения безопасности и отказоустойчивости.

Таким образом, взаимная проверка аксиоматических базисов позволяет формализованно создавать и верифицировать системы, которые способны обнаруживать факт отказа и, как следствие, переходить в безопасное состояние или самовосстанавливаться.

Заключение

В настоящее время АБП и его методы диверситетных базисов и взаимной проверки базисов прошли апробацию на решении типовых задач систем железнодорожной автоматики и телемеханики с последующей проверкой результатов посредством имитационного моделирования, которое выполнялось с помощью программного комплекса КИИБ [9]. В докладе представлены:

- АБП как логическое основание и общий подход для проектирования безопасных и отказоустойчивых систем;
- диверситетные аксиоматические базисы, их свойства и общая методика применения;
- взаимная проверка аксиоматических базисов — формализованное проектирование, принципы выбора базисов и их взаимной проверки;
- практика применения АБП на этапах проектирования, разработки, верификации и имитационного моделирования.

1. Leveson, N. Safeware: System Safety and Computers / Nancy Leveson; New York, NY, USA, Addison-Wesley. – 1995.
2. 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.
3. Шубинский, И. Б. Функциональная надежность информационных систем. Методы анализа. / И. Б. Шубинский; Ульяновск: Изд-во журнала «Надежность». – 2012. – 216 с.
4. Шубинский, И. Б. Структурная надежность информационных систем. Методы анализа. / И. Б. Шубинский; Ульяновск: Типография «Печатный двор». – 2012. – 216 с.
5. 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; Oxford, UK, Elsevier Ltd. – 2010.
6. Сивко, Б. В. Аксиоматико-базисный подход для разработки безопасных и отказоустойчивых систем. / Б. В. Сивко; Автоматика на транспорте: Санкт-Петербург. – 2015. – № 4.
7. Сивко, Б. В. Диверситетные аксиоматические базисы для разработки безопасных и отказоустойчивых систем / Вестник БелГУТа: Наука и Транспорт. – 2014. – №1(28). – С. 19-23.
8. Сивко, Б. В. Разработка безопасных и отказоустойчивых систем на основе взаимной проверки аксиоматических базисов / Вестник БелГУТа: Наука и Транспорт. – 2015. – №1(30).
9. Бочков К. А. Методы и средства доказательства функциональной безопасности микроэлектронных систем железнодорожной автоматики // К. А. Бочков, С. Н. Харлап, Д. Н. Шевченко / Електромагнітна сумісність та безпека на залізничному транспорті, Д. : ДНУЗТ. – 2011. – №2. – С. 73-81.