Стандартизация и сертификация

УДК 004.052.2

Б. В. Сивко
Научно-исследовательская лаборатория «Безопасность и ЭМС технических средств»,
Белорусский государственный университет транспорта

АКСИОМАТИКО-БАЗИСНЫЙ ПОДХОД ДЛЯ РАЗРАБОТКИ БЕЗОПАСНЫХ И ОТКАЗОУСТОЙЧИВЫХ СИСТЕМ

Предложен подход на основе аксиоматических базисов, позволяющий формализовать решение ряда проблем разработки и верификации отказоустойчивых и безопасных систем. Сформулированы положения и задачи аксиоматико-базисного подхода. Показано, что подход согласуется с опытом инженерии безопасных и отказоустойчивых систем; позволяет повышать их отказоустойчивость и безопасность; сравнивать отказоустойчивость систем; сохранять баланс между отказоустойчивостью и сложностью разработки и верификации; применять формальные методы для доказательства; формализовать интеграцию систем; повышать и оценивать уровень диверситета без привлечения независимых групп разработчиков и экспертов; формализованно проектировать и верифицировать системы, обнаруживающие собственные отказы. Вместе с тем подход позволяет решать актуальные проблемы отказоустойчивых и безопасных систем, такие как формализация методов внутрипроцессорного контроля и разработка условий его проведения, а также доказательство достаточности диверситета разрабатываемых и верифицируемых систем.

отказоустойчивость, доказательство безопасности, формальные методы, формализация, диверситет, обнаружение отказов

Введение

Одной из актуальных задач для современных систем, связанных с безопасностью, является создание эффективных методов и средств, позволяющих выполнять их разработку и верификацию. Данные системы используются в таких отраслях промышленности, как железнодорожный и морской транспорт, гражданская авиация, атомная энергетика, медицина, космос, телекоммуникации, опасное химическое производство и др. [1]. Они относятся к системам, критичным к безопасности, к которым предъявляются повышенные требования, так как они отвечают за управление ответственными технологически-

ми процессами. Концепции построения систем данного типа имеют общую основу, закрепленную в стандарте ГОСТ Р МЭК 61508:2012 (IEC 61508) [2].

В настоящее время считается, что для обеспечения надлежащего уровня безопасности и надежности функционирования на всех этапах жизненного цикла систем требуется комплексно применять известные методы и средства для обеспечения этих свойств [3]. Практикуются функциональный, структурный и другие подходы, применяются программные и аппаратные средства защиты, используются различные концепции и стратегии обеспечения безопасности и т. д. [3–5].

Одной из проблем при решении ряда задач по разработке и верификации систем, критичных к безопасности, является отсутствие формализованных подходов. По этой причине используются экспертные методы. В качестве примера можно рассмотреть влияние фактора отказа по общей причине (common cause failure, CCF), из-за которого происходит большое количество катастроф [6–8]. Для решения возможно создание диверситетного аппаратного и программного обеспечения с помощью N-версионного программирования, привлечение независимых экспертов, выбор различных компиляторов и др. Для оценки уровня диверситета могут быть использованы BETA-метод и модель BETAPLUS, которые рекомендованы стандартом IEC 61508 [2]. Однако все существующие в настоящее время диверситетные методы являются экспертными, что ограничивает их эффективность и глубину решения, поэтому существует необходимость их формализации.

В статье предлагается подход на основе аксиоматических базисов (аксиоматико-базисный подход, АБП), который позволяет рассмотреть вопросы разработки и верификации безопасных и отказоустойчивых систем в формализованном виде. Он сформулирован на основе обобщения диверситетных аксиоматических базисов, позволяющих решить проблему формализации диверситета и CCF, что в настоящее время представляется его актуальным применением [9]. Подход базируется на общих свойствах дедуктивной логики и поэтому претендует на высокую степень обобщения. Разработка и апробация АБП проводились на микропроцессорных системах автоматики и телемеханики.

Опыт разработки и верификации в лаборатории показывает, что АБП имеет особенности применения, зависящие от проекта, поставленной задачи и рассматриваемой функциональности. В статье рассматриваются положения АБП, опирающиеся на общую основу построения систем, критичных к безопасности и надежности функционирования.

1 Аксиоматико-базисный подход

Аксиоматическим базисом (далее базис) будем считать некоторое множество утверждений (условий). Если они выполняются для системы в рассматриваемом состоянии, то будем считать, что базис истинен (выполняется) для состояния данной системы. Пример условий базиса:

– все инструкции микропроцессора выполняются согласно его спецификации;

– тактовая частота генератора находится в заданных конкретных пределах;

– отказы элементов из-за агрессивной электромагнитной обстановки происходят не чаще заданного предела по времени.

С точки зрения формализации данные условия можно рассмотреть как некоторое утверждение (логическую функцию от системы или ее состояния), которое как для рассматриваемого примера, так и в общем случае на практике удобно представить в виде конъюнкции (логического «И») более простых утверждений. Другими словами, если рассматривается некоторая система в состоянии x и при этом имеется множество утверждений $A_1(x), A_2(x), \ldots, A_n(x)$, которые являются истинными, то базисом будет являться $A(x)$, определенное по формуле

$$A(x) \equiv A_1(x) \wedge A_2(x) \wedge \ldots \wedge A_n(x), \qquad (1)$$

а система в данном состоянии будет считаться удовлетворяющей данному базису.

В качестве утверждений (условий) базиса могут рассматриваться изначальные базовые положения, на которые опирается разработчик или верификатор, и те возможности, которые ему предоставлены. Это могут быть условия функционирования, а для существующих систем, с которыми происходит взаимодействие, – их свойства.

Условия базиса должны быть формализуемыми, т. е. каждое из них можно однозначно записать в виде математического условия $A_i(x)$. Сами же условия могут быть любыми, но они задают уровень абстракции таким образом, чтобы в рамках данной аксиоматики можно было бы верифицировать свойства системы.

АБП предполагает, что утверждения $A_i(x)$ обладают некоторой степенью независимости с точки зрения отказоустойчивости. Поэтому рассмотрение базиса в виде множества утверждений, логически объединенных через конъюнкцию, удобно тем, что в случае отказа или нарушения некоторых условий оставшиеся будут выполняться и система сохранит некоторое свое свойство. Важной задачей для повышения отказоустойчивости является также уменьшение количества условий и увеличение области их определения.

Любое формализованное доказательство свойств системы, в том числе доказательство безопасности, можно представить так, как показано на рис. 1.

Доказательство базируется на утверждениях аксиоматического базиса и представляет собой цепь дедуктивных умозаключений, результатом которых должен быть вывод о целевом качестве рассматриваемой системы. Изначально принимается, что утверждения аксиоматического базиса истинны. Далее с помощью правил вывода (логики) делается попытка установить истинность верифицируемых свойств системы. В случае успеха система считается удовлетворяющей проверяемым свойствам.

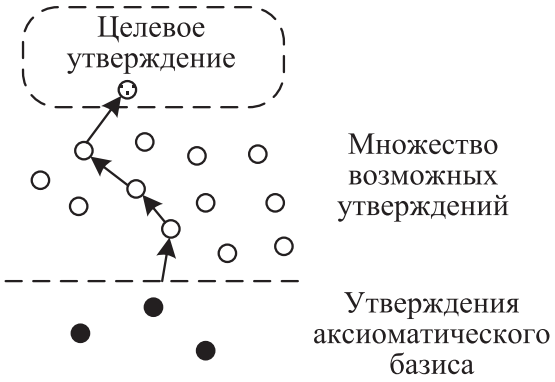

Рис. 1. Доказательство целевого утверждения

Аналогичным образом строится разработка, при которой изначально предполагается, что будущая система будет работать на основании того, что выполняются некоторые определенные утверждения. Например, при разработке безопасных схем на базе реле первого класса считается, что фронтовые контакты не могут быть замкнуты ни при каких обстоятельствах в случае, если обесточена обмотка. Данное свойство реле обеспечивается конструкционно, а в системе ответственные команды выполняются через фронтовые контакты. Или для программных средств может предполагаться, что спецификации языка программирования выполняются. Это обеспечивается безошибочностью работы аппаратуры и корректностью компиляции. Таким образом, разработка основана на истинности условий базиса и подразумевает ряд шагов, посредством которых разрабатываемая система должна перейти в такое состояние, при котором целевое утверждение становится истинным.

В рамках АБП важны оба аспекта – как доказательство свойств системы, так и процесс ее разработки.

Следует отметить, что логические правила определяются той теорией, в рамках которой выполняется доказательство или разработка. Другими словами, в процессе доказательства или проектирования разработчик или верификатор могут использовать различные математические аппараты, и АБП не налагает никаких ограничений на методы дедукции, которые могут быть применены.

АБП строится на следующих положениях:

– безопасность и отказоустойчивость системы является функцией от аксиоматического базиса;

– отказ в системе рассматривается как нарушение одного из утверждений аксиоматического базиса.

Основным понятием при анализе является аксиоматический базис, на который опираются функции системы. Соответственно в случае отказа та часть системы, разработка или доказательство которой основывались на истинности нарушенных утверждений, может перейти в состояние оказа. Но работоспособность тех функций системы, которые не зависят от нарушенных утверждений, не будет нарушена.

Как правило, базис формируется на основе экспериментальных данных или рассматривается в рамках другой теории, которая предоставляет готовые к применению условия базиса. Например, при построении безопасных схем на основе реле первого класса их можно сформулировать в терминах дискретной логики, уровень абстракции которой скрывает конкретную реализацию. Вместе с тем можно сформулировать условия базиса таким образом, чтобы оперировать вероятностными характеристиками конкретных устройств, о которых имеются экспериментальные данные.

Следует отметить, что любая функция системы выполняется тогда, когда являются истинными определенные утверждения (т. е. базис). В данном случае аксиоматический базис показывает свою двойную природу, когда, с одной стороны, налагаемые условия позволяют реализовывать требуемую функциональность, а с другой стороны, их нарушение из-за отказов приводит систему в опасное или неработоспособное состояние.

Отличительной особенностью АБП является его формализованность. Например, если нарушается базис, то можно определить условия его нарушения и целенаправленно искать решение проблемы. Или если базис усиливается, то можно определить, для каких случаев система становится более отказоустойчивой и безопасной и т. д.

Основными задачами АБП являются:

– защита аксиом – выбор таких аксиоматических базисов, которые наименее подвержены отказам, а также мероприятия по защите выполнимости утверждений базисов;

– проверка аксиоматических базисов – процедуры, позволяющие определить, выполняется базис или нет, что предоставляет возможность как доказывать безопасность и отказоустойчивость существующих систем, так и проверять их работоспособность в реальном времени;

– разработка методов и средств на основе аксиоматических базисов – поиск эффективных решений, позволяющих оперировать аксиоматическими базисами таким образом, чтобы улучшать показатели безопасности и отказоустойчивости.

2 Отказоустойчивость и безопасность систем

Система в процессе работы может изменять свое состояние и соответственно может измениться выполнимость базиса. Например, в состоянии x базис A выполняется, а в состоянии y базис A не выполняется. Тогда, если система спроектирована или верифицировалась на основании базиса A, в результате перехода из состояния x в состояние y система может перестать выполнять свою функцию. Исходя из этого можно сделать вывод о том, что одной из задач при разработке отказоустойчивых и безопасных систем является выбор

такого базиса, который является наиболее устойчивым (при котором множество $A(x)$ является как можно большим), а переход из $A(x)$ в $A(y)$ как можно менее вероятным.

Таким образом, выбирать нужно такие утверждения для базиса, которые сложно нарушить, а разработку систем вести таким образом, чтобы заданная функция выполнялась как можно в большем количестве состояний и при этом переход в некорректное состояние был бы как можно менее вероятным.

Примером сильного базиса может служить реле первого класса, для которого свариваемость фронтовых контактов маловероятна, и на этом можно строить высоконадежные системы. Примером уменьшения количества состояний, при которых не выполняются условия безопасности системы, является расчет контрольной суммы кода выполняемой программы, изменение которой приводит к переходу в безопасное состояние.

АБП обращает внимание на защиту утверждений базиса. Если функционирование реле первого класса зависит от необходимости отпадания якоря под действием силы притяжения и соответственно от его геометрического расположения, требуется обеспечивать соответствующие условия и проверять их. Если производится расчет контрольной суммы памяти, требуется обосновать утверждение о том, что произвольный отказ приводит к равновероятному изменению контрольной суммы.

3 Сравнение аксиоматических базисов

Рассмотрим два аксиоматических базиса – A и B относительно друг друга. Если выполняются нижеприведенные условия, будем считать, что базис A сильнее базиса B (соответственно B является более слабым, чем A):

$$\forall x \quad B(x) \rightarrow A(x); \tag{2}$$

$$\exists x \quad A(x) \wedge \overline{B(x)}. \tag{3}$$

Другими словами, всегда, когда выполняется базис B, выполняется базис A, но существует хотя бы одно состояние, при котором выполняется базис A, но не выполняется базис B. Например, если принять, что $A(x) \equiv x > 0, B(x) \equiv x = 1$, то выполнимость базисов и факт того, что A сильнее B, можно продемонстрировать так, как показано на рис. 2.

Во время усиления базиса относительно составляющих утверждений всегда можно выразить более слабый базис B через более сильный A следующим образом:

$$B(x) \equiv A(x) \wedge C(x). \tag{4}$$

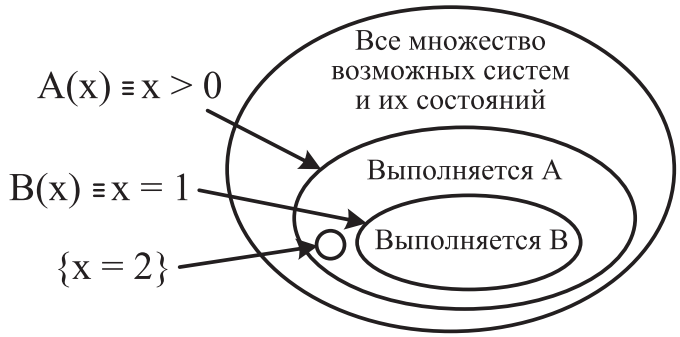

Рис. 2. Базис *A* сильнее базиса *B*

Здесь $C(x)$ включает в себя как минимум одно состояние исходя из (3) и описывает утверждения, которые являются разностью между базисами *A* и *B*.

При работе с базисами удобно рассматривать их не только с точки зрения систем, которые им удовлетворяют, но и относительно аксиоматических утверждений (см. рис. 1), которые базисы включают в себя согласно (1). Данная разница и связь между способами рассмотрения показана на рис. 3.

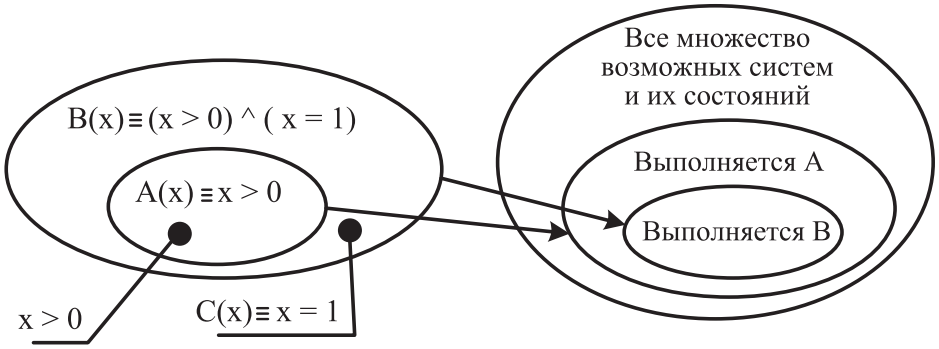

Рис. 3. Относительность усиления базиса

4 Сравнение систем на безопасность и отказоустойчивость

Рассмотрим две системы – *p* и *q* относительно некоторых базисов *A* и *B*. Если выполняется $A(p)$ (т. е. система выполняет свою функцию при выполнимости базиса *A*), выполняется $B(p)$ и $A(q)$, но не выполняется $B(q)$, то из этого можно сделать заключение о том, что система *p* более отказоустойчива, чем система *q*. Это проиллюстрировано на рис. 4. Отсюда следует вывод о том, что можно таким образом сравнивать системы на безопасность или отказоустойчивость. Однако, по ситуации, показанной на рис. 4, нельзя однозначно сказать, какой из базисов более сильный, *A* или *B*, даже несмотря на то, что есть пример системы *q*, которая может не работать на основании базиса *B* и работает на основании базиса *A*. Это происходит потому, что безопасность и отказоустойчи-

вость зависят не только от системы, но и от базиса. И с точки зрения базисов может получиться так, что имеется условие, которое выполняется в базисе B, но не выполняется в A, и соответственно существует другая пара систем p и q или их состояний, для которых ситуация противоположна (выполняется $A(p)$, $B(p)$ и $B(q)$, но не выполняется $A(q)$). Поэтому для сравнения систем на безопасность и отказоустойчивость необходимо доказательство того, что базис A сильнее базиса B.

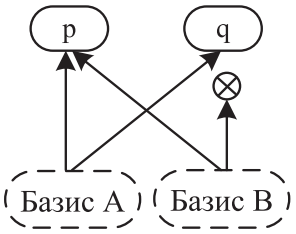

Рис. 4. Относительность усиления базиса

На основании вышеизложенного делается вывод о том, что любое формализованное сравнение на отказоустойчивость всегда относительно тех базисов, на которые оно опирается, т. е. если система выполняет свою функцию как в условиях A, так и в условиях B, то она устойчива относительно этих условий, но в других условиях ситуация может быть иной. Поэтому важной задачей является разработка и верификация отказоустойчивых и безопасных систем, которые наиболее близки в предметной области и предполагаемым условиям функционирования [10]. Второй задачей является поиск наиболее вероятных отказов и целенаправленная защита от них, что согласуется с общей практикой инженерии безопасных систем [11].

Следует отметить, что изменение свойств безопасности и отказоустойчивости систем является одним из основных факторов, приводящих к авариям и катастрофам [1, 8].

Таким образом, АБП объясняет, почему отказоустойчивость и безопасность не являются абсолютными понятиями, а должны рассматриваться относительно тех условий, в которых эксплуатируется система. АБП также показывает, почему при переносе системы в другие условия характеристики ее безопасности и отказоустойчивости изменяются.

5 Повышение безопасности и отказоустойчивости систем

АБП дает возможность повышения устойчивости систем с помощью усиления аксиоматического базиса: если в нашем распоряжении находится система, разработанная на основании некоторого базиса (B), то можно повысить отказо-

устойчивость системы таким образом, чтобы она выполняла свои функции при более сильном базисе (*A*). Верификация такой системы показана на рис. 5.

Аналогично, если рассматривается уже верифицированная система, можно доказать ее безопасность или надежность на более строгом уровне, приведя доказательство для более сильного базиса. Данная операция может быть полезна для адаптации эксплуатируемой системы к новым условиям.

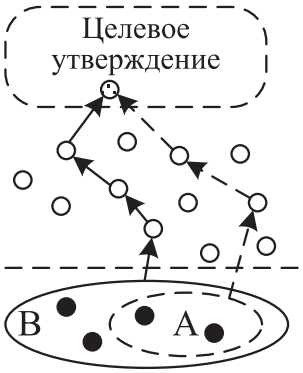

Рис. 5. Доказательство на основании более сильного базиса

Важно отметить, что вышеприведенные рассуждения применимы не только для системы в целом, но и для ее текущего состояния, которое в процессе работы может изменяться. Поэтому доказательства безопасности и отказоустойчивости на основании АБП могут приводиться для переходов системы между ее состояниями. Это может иметь место, в том числе, и с необходимым усилением базиса, например, переход в безопасное состояние может осуществляться при сопутствующем усилении базиса.

Описанный способ не обязательно применять для всей системы. Усиление базиса возможно только для отдельной ответственной функции, работоспособность которой определяет отказоустойчивость или безопасность системы.

Следует отметить, что рассмотрение двух систем относительно некоторых базисов позволяет сравнивать системы на отказоустойчивость, т. е. если одна из систем выполняет свою функцию на более сильном базисе, то она более отказоустойчива.

Таким образом, АБП дает возможность улучшать показатели отказоустойчивости формализованно и целенаправленно, а также сравнивать системы на отказоустойчивость.

6 Пример повышения отказоустойчивости с помощью усиления базиса

Допустим, требуется разработать систему, выполняющую следующую логическую функцию:

$$F(a,b,c) \equiv (a \wedge b) \vee \bar{c}. \quad (5)$$

Функция (5) является требованием к системе как ее свойству, т. е. формирует целевое утверждение, показанное на рис. 5.

Рассмотрим первый базис D, представляющий собой корректность проведения логических операций:

$$D \equiv A_{and} \wedge A_{or} \wedge A_{not}, \quad (6)$$

где A_{and} – безошибочность выполнения операции AND («И») и соответственно A_{or} для OR («ИЛИ») и A_{not} для NOT («НЕ»).

Здесь с точки зрения отказоустойчивости предполагается, что логические операции одного и того же типа более подвержены отказу, а разного типа происходят более независимо. Это может происходить, например, в случае повторного использования одних и тех же элементов (что является общей характеристикой микропроцессорных систем [3]), или тогда, когда имеется CCF для аппаратных средств одного и того же типа.

В случае, когда разработчику предоставлены возможности A_{and}, A_{or} и A_{not} для проведения логических операций, то можно получить результат, показанный на рис. 6, *а*.

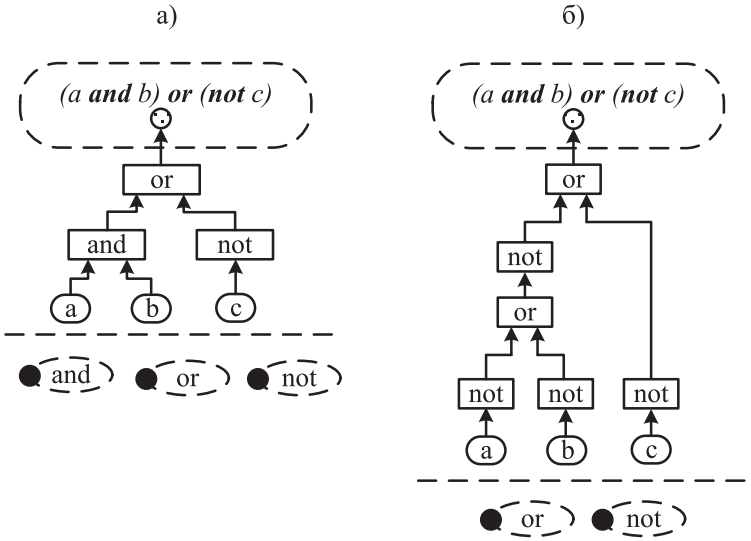

Рис. 6. Разработка (*а*) и усиление (*б*) аксиоматического базиса

Но с точки зрения АБП можно ограничить выбор действий таким образом, чтобы не использовать логическую операцию AND, т. е. исключить условие A_{and}. В этом случае будет получен более сильный базис E:

$$E \equiv A_{or} \wedge A_{not}. \quad (7)$$

Реализация системы, при которой использован более сильный базис E, может выглядеть так, как показано на рис. 6, *б*.

Таким образом, из базиса было удалено условие A_{and}, и теперь, в случае его нарушения, система продолжит выполнять свою функцию. Можно также сказать, что исключен фактор CCF для операции AND.

7 Аксиоматический базис как степень свободы

Изменение базиса отражается на сложности разработки системы или доказательства ее безопасности и надежности таким образом, что при усилении базиса сложность либо не изменяется, либо увеличивается. Как можно видеть в предыдущем примере, базис был усилен, а реализация функции усложнилась. Соответственно является верным и обратный процесс – при ослаблении базиса систему проще разрабатывать или доказывать ее свойства. С точки зрения АБП изменение базиса как степень свободы показана на рис. 7.

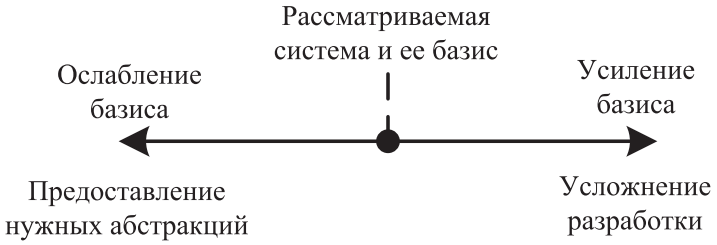

Рис. 7. Изменение базиса как степень свободы

Примером разности базисов может служить разность подходов для RISC- и CISC-процессоров, первые из которых имеют небольшой набор команд, а вторые спроектированы так, чтобы выполнять задачу с минимальным количеством строк кода [12, 13]. В качестве второго примера можно рассмотреть разницу в решении некоторой задачи на языке высокого уровня с применением готовых библиотек (предоставляющих разработчику множество удобных абстракций) и решение той же задачи на языке Ассемблер. В случае, когда задача более близка к предоставляемым абстракциям, разработка является более простой. Но при этом отказоустойчивость для первых зависит не только от аппаратных средств, но и от библиотек и компилятора.

Для создания безопасных и надежных систем усиление базиса не является целью. Важно понимание того, что усиление базиса позволяет уменьшать зависимость от внешних условий. Однако при большой сложности системы это усложняет ее разработку и верификацию, что выражается в увеличении затрат и в том, что система становится более подверженной ошибкам. Поэтому с практической точки зрения необходим поиск баланса.

Одним из способов улучшения показателей отказоустойчивости может являться поиск таких условий базиса, соблюдение которых несущественно влияет на разработку. Например, в случае, когда в системе присутствует функциональ-

ность, которая основана на условиях базиса A_m, но может быть с минимальными затратами реализована на других условиях базиса (для всех A_i при $i \neq m$), как следствие, A_m из базиса можно исключить.

С точки зрения АБП рассмотрение базиса как отдельного понятия позволяет отделить предоставляемые разработчику или верификатору отказоустойчивые абстракции от непосредственного процесса разработки или верификации и тем самым влиять на их сложность.

8 Дедуктивный анализ с помощью аксиоматических базисов

Поскольку АБП формализует поведение и разработку систем, можно проводить их дедуктивный анализ, т. е. логически доказывать целевые свойства. Например, если известно, что для базисов A и B и систем p и q выполняется $A(p)$ и $B(q)$, а также что базис A сильнее базиса B, то можно утверждать, что выполняется $B(q)$.

Дедуктивный анализ не исключает широкого применения логики как математического аппарата для доказательства. Рассмотрим в качестве примера систему в состоянии x, построенную на базисе A, и некоторое утверждение $g(x)$. Если теория непротиворечива, любое утверждение, как $g(x)$, может являться истинным (всегда выполняться), ложным (никогда не выполняться) или невыводимым (не являться истинным либо ложным в рассматриваемом базисе). Если воспользоваться доказательством от противного, то для некоторого $g(x)$ можно доказать, что оно ложно. Это означает: если условия базиса выполняются (надежно защищены) и в логике не было ошибок, то $g(x)$ никогда не может быть истинным. Другими словами, система никогда не будет находиться в состоянии, при котором $g(x)$ истинно.

Если на практике требуется выполнение $g(x)$, но мы доказываем, что оно ложно, то, скорее всего, имеется проблема в базисе A и его нужно изменить. Но возможна и обратная ситуация, когда требуется, чтобы в базисе A утверждение $g(x)$ никогда не выполнялось, что может быть полезно в случае, когда $g(x)$ описывает опасное или неработоспособное состояние.

Таким образом, АБП предоставляет возможность широкого использования формальных подходов, позволяющих доказывать безопасность и надежность систем с помощью математических средств.

9 Интеграция систем

Во время интеграции двух систем, построенных на базисах A и B соответственно, может быть логически определен базис результирующей системы. Рассмотрим два различных варианта интеграции.

Если интеграция происходит для совместного выполнения некоторой задачи, то базис определяется объединением базисов A и B через конъюнкцию. При этом получаемый в результате объединения базис либо ослабляется, либо остается прежним (в случае, если базисы A и B равны). Например, если базисы определяются как

$$A \equiv (x > 0) \wedge (x < 20) \tag{6}$$

и

$$B \equiv (x > 10) \wedge (x < 30), \tag{7}$$

то результирующий базис считается их конъюнкцией:

$$A \wedge B \equiv (x > 10) \wedge (x < 20). \tag{8}$$

Вывод на основе АБП заключается в том, что подсистемы, работающие в комплексе для выполнения общей задачи, нужно разрабатывать таким образом, чтобы они имели как можно больший общий базис. В этом случае преобразование (8) приведет к минимальному ослаблению базиса и соответственно сохранению свойств отказоустойчивости и безопасности. Если базис не согласован, то для таких систем доказательство безопасности будет затруднено, а показатели надежности могут ухудшиться.

Вторым вариантом интеграции является построение диверситетных систем, когда каждая из подсистем полноценно выполняет заданную функцию. В данном случае базис получается из A и B через дизъюнкцию

$$A \vee B \equiv (x > 0) \wedge (x < 30). \tag{9}$$

При таком объединении базис либо не изменяется (если базисы равны), либо усиливается.

Как результат, система становится защищенной от одиночных отказов в состояниях, когда один из базисов, A или B, перестает выполняться, а второй сохраняет свою истинность.

Разработка и верификация систем в данном варианте интеграции в АБП рассматриваются относительно диверситетных аксиоматических базисов [9]. Здесь вводятся функции Indep и Common:

$$\text{Indep}\,(A, B) \equiv A \wedge \overline{B}; \tag{10}$$

$$\text{Common}\,(A, B) \equiv A \wedge B. \tag{11}$$

Первая функция (10) показывает множество условий базиса A, которые независимы от базиса B. Вторая функция (11) показывает множество условий, нарушение любого из которых приводит к нарушению как базиса A, так и базиса B, т. е. того, что является общим базисом A и B.

При таких определениях диверситетная система будет защищена от одиночных отказов в состояниях, определенных по формуле

$$\text{Indep}(A,B) \vee \text{Indep}(B,A) \equiv ((x>0) \wedge (x<10)) \vee ((x>20) \wedge (x<30)) \quad (12)$$

и будет уязвимой для отказов, определенных по формуле (11).

Выражения (11) и (12) можно считать формализацией отказоустойчивости диверситетных систем.

АБП формализует задачи диверситета для повышения отказоустойчивости и безопасности, к которым относятся [9]:

– определение базисов с наибольшей степенью диверситета (увеличение области действия Indep (A, B) и Indep (B, A));

– определение базисов с минимальным влиянием CCF (уменьшение Common (A, B));

– удержание внимания на решаемых задачах, т. е. помещение в Indep (A, B) и Indep (B, A) таких условий, которые наиболее важны для функционирования;

– реализация на рассматриваемых базисах функций, непосредственно влияющих на безопасность или надежность (например, ключевые действия для самодиагностики или восстановления системы после сбоев).

Более подробно диверситетные аксиоматические базисы рассмотрены в работе [9].

Важно отметить, что АБП позволяет усиливать диверситет без привлечения независимых групп во время разработки. При этом факт повышения уровня диверситета доказывается формальными методами и согласуется с условиями функционирования, позволяя выполнять задачу целенаправленно и адаптировать решение к конкретной ситуации. Конечно, АБП не отменяет необходимости привлечения независимых разработчиков для создания систем, критичных к безопасности, но вместе с тем предоставляет инструмент для выхода на уровень более высокого качества.

Таким образом, АБП формализует интеграцию систем и показывает, как можно целенаправленно улучшать показатели безопасности и отказоустойчивости.

10 Обнаружение отказов и проверка аксиоматического базиса

Важной задачей для безопасных и отказоустойчивых систем является обнаружение отказов с последующей реакцией, позволяющей перевести систему в безопасное состояние или запустить процесс ее восстановления. Данная проблема в АБП решается относительно базисов.

Для системы, выполняющей функцию f, для обнаружения отказов вводится функция корректности работы s, которая принимает истинное значение в случае, когда система находится в безопасном и работоспособном состоянии.

Рассмотрим систему, которая разрабатывается или верифицирована на базисе A_f, состоящем из трех утверждений A_1, A_2 и A_3, и ситуацию, когда может произойти отказ, в результате которого нарушится базис A_3. Ключевой идеей АБП для обнаружения отказа является то, что в результате нарушения базиса утверждение $\overline{A_3}$ станет истинным, а на этом основании можно построить функциональность так, что отказ будет обнаружен. Проверка базиса с обнаружением отказа показана на рис. 8.

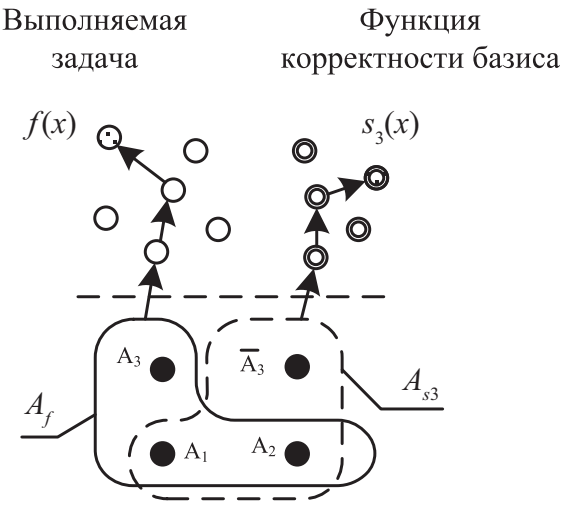

Рис. 8. Проверка базиса

Таким образом, могут быть сформированы функции s_i, проверяющие соответствующий базис A_i.

АБП вводит понятие полноты проверки. Рассмотрим систему, работающую на основании n базисов A_i, а также функции s_i, проверяющие соответствующий базис A_i, и базисы A_{si}, на основании которых реализованы соответствующие функции s_i. Для полноты проверки необходимо, чтобы выполнялись два условия:

1. Если перестал быть истинным базис A_i, то должен выполняться проверяющий его базис A_{si}.

2. Каждая функция $s_i(x)$ должна быть реализуема в предоставляемом базисе A_{si}.

В случае выполнения полной проверки система реализует свойство самопроверяемости в рамках рассматриваемой теории. Другими словами, если аксиоматические допущения надежно защищены, а разработка и верификация прошли без ошибок, то система всегда обнаружит отказ.

Следует отметить, что выполнение условия полной проверки является идеальным конечным результатом, который говорит о факте полной самопроверяемости системы в рамках рассматриваемых допущений. Иными словами, данное условие можно использовать как целевое утверждение, подлежащее выполнению.

Доказательство полноты проверки в статье не рассматривается. В настоящее время, исходя из опыта работы с конкретными устройствами, предполагается, что возможно получение инструментария доказательства полноты и корректности базиса для устройств с определенными свойствами.

Более подробно обнаружение отказов и проверка аксиоматического базиса рассмотрены в работе.

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

Заключение

АБП согласуется с опытом разработки и эксплуатации безопасных и отказоустойчивых систем – он объясняет, почему показатели системы зависят от условий эксплуатации и предоставленных для разработки средств, а также обосновывает сложность создания универсальных методов. Вместе с тем АБП формализует понятия предметной области, требующие согласования, и подтверждает необходимость внимания к характерным отказам для условий эксплуатации и аппаратных средств.

В статье показано, что с помощью АБП можно:

– повышать отказоустойчивость систем;

– сравнивать системы на отказоустойчивость;

– усиливать и ослаблять базис системы, тем самым сохранять баланс между отказоустойчивостью и сложностью разработки и верификации;

– применять формальные методы и доказывать свойства безопасности и отказоустойчивости систем математически;

– формализовать интеграцию систем и улучшать ее с точки зрения отказоустойчивости;

– улучшать диверситет без привлечения независимых групп разработчиков;

– формализованно проектировать и верифицировать системы, позволяющие обнаруживать отказы, переходить в безопасное состояние и самовосстановление.

АБП может быть применен для решения ряда актуальных проблем. Одной из них является отсутствие формальных методов внутрипроцессорного контроля, а АБП позволяет выполнить для него разработку соответствующих условий. Другой проблемой является отсутствие формальных средств доказательства достаточности диверситета разрабатываемых и верифицируемых систем. Для этой проблемы существуют только экспертные рекомендации, но отсутствует проверка как обратная связь по оценке уровня диверситета. АБП позволяет как оценить диверситет, так и сформировать достаточный его уровень во время разработки.

Таким образом, АБП позволяет выйти на новый уровень формализации разработки и верификации безопасных и отказоустойчивых систем, что дает возможность улучшать их показатели формализованно и целенаправленно.

Библиографический список

1. Levenson N. Safeware: System Safety and Computers / N. Levenson. – N. Y. : Addison-Wesley, 1995. – 680 p.
2. Smith D. 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 / D. J. Smith, Simpson Kenneth G. L. – Oxford, UK, Elsevier Ltd, 2010. – 270 p.
3. Бочков К. А. Микропроцессорные системы автоматики на железнодорожном транспорте : учеб. пособие / К. А. Бочков, А. Н. Коврига, С. Н. Харлап. – Гомель : БелГУТ, 2013. – 254 с.
4. Шубинский И. Б. Функциональная надежность информационных систем. Методы анализа / И. Б. Шубинский. – Ульяновск : Изд-во журнала «Надежность», 2012. – 216 с.
5. Шубинский И. Б. Структурная надежность информационных систем. Методы анализа / И. Б. Шубинский. – Ульяновск : Типография «Печатный двор», 2012. – 216 с.
6. Weil V. Professional Responsibility for Harmful Actions / V. Weil, B. Ferry. – Kendall Hunt, Dubuque, Iowa, 1984. – Pp. 402–411.
7. Sagan S. D. The Limits of Safety: Organizations, Accidents, and Nuclear Weapons / S. D. Sagan. – N. Y.: Princeton University Press, Princeton, 1993. – 302 p.
8. Neumann P. G. Computer-Related Risks / P. G. Neumann. – N. Y. : Addison-Wesley Professional, 1995. – 384 p.
9. Сивко Б. В. Диверситетные аксиоматические базисы для разработки безопасных и отказоустойчивых систем / Б. В. Сивко // Вестник БелГУТа: Наука и транспорт. – 2014. – № 1 (28). – С. 19–23.
10. Smith D. J. Developments in the Use of Failure Rate Data and Reliability Prediction Methods for Hardware / D. J. Smith. – Delft : Delft University of Technology, Aerospace Engineering, Dissertation, 2000. – 175 p.
11. Parry G. W. Common Cause Failure Analysis: A Critique and Some Suggestions / G. W. Parry. – Gaithersburg, Maryland, USA, Reliability Engineering and System Safety. – 1991. – Vol. 34. – Issue 3. – Pp. 309–326.
12. Касперски К. RISK vs. CISC / К. Касперски [Электронный ресурс]. – Компьютерра, 1999. – № 36 (314). – Режим доступа : http://old.computerra.ru/1999/314/3211/, свободный. – Загл. с экрана (дата обращения: 17.07.2015).
13. Орлов С. А. Организация ЭВМ и систем / С. А. Орлов, Б. Я. Цилькер. – СПб. : Питер, 2011. – 688 с.

Boris V. Sivko
Research laboratory
«Safety and Electromagnetic Compatibility of Technical Facilities»,
Belorussian State University of Transport, Gomel

Axiomatic-based approach for development of trustworthy and fault-tolerant systems

The article proposes an approach on the ground of axiomatic bases, that allows to formalize a solution of number of problems of development and verification of fault-tolerant and trustworthy systems. The article states the provisions and objectives of this axiomatic-based approach. It is shown that the approach is consistent with the experience of fault-tolerant and trustworthy systems engineering, and allows to improve its fault tolerance and safety, to carry out a comparison of system fault tolerance, to maintain the balance between the fault tolerance and the complexity of development and verification, to apply formal methods of prove, to formalize the integration of systems, to improve and to evaluate the level of diversity without the involvement of independent groups of developers and experts, and to formalized develop and verify system, detecting its own failures. Moreover, the approach makes it possible to solve the current problems of fault-tolerant and trustworthy systems, such as the formalization of methods for intraprocessor control, and of development of its realization conditions, as well as the proof of sufficiency of the diversity of developed and verifiable systems.

fault tolerance, safety proof, formal methods, formalization, diversity, failure detection

References

1. Leveson N. Safeware: System Safety and Computers. N. Y., Addison-Wesley, 1995, 680 p.
2. Smith D. J., Simpson Kenneth G. L. 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. Oxford, UK, Elsevier Ltd, 2010, 270 p.
3. Bochkov K. A., Kovriga A. N., Kharlap S. N. Railway transport microprocessor automation systems : textbook. Gomel, BelGUT, 2013, 254 p.
4. Shubinsky I. B. Functional reliability of data systems. Methods of analysis. Ul'yanovsk, Publishing house «Nadezhnost'», 2012, 216 p.
5. Shubinsky I. B. Structural reliability of data systems. Methods of analysis. Ul'yanovsk, Printing office «Pechatny dvor», 2012, 216 p.
6. Weil V., Ferry B. Professional Responsibility for Harmful Actions. Kendall Hunt, Dubuque, Iowa, 1984, pp. 402–411.
7. Sagan S. D. The Limits of Safety : Organizations, Accidents, and Nuclear Weapons. N. Y., Princeton University Press, Princeton, 1993, 302 p.
8. Neumann P. G. Computer-Related Risks. N. Y., Addison-Wesley Professional, 1995, 384 p.

9. Sivko B. V. Diversity axiomatic bases for development of trustworthy and fault-tolerant systems. Bulletin of BelGUT, Science and transport (Nauka i transport), 2014, № 1 (28), pp. 19–23.
10. Smith D. J. Developments in the Use of Failure Rate Data and Reliability Prediction Methods for Hardware. Delft, Delft University of Technology, Aerospace Engineering, Dissertation, 2000, 175 p.
11. Parry G. W. Common Cause Failure Analysis: A Critique and Some Suggestions. Gaithersburg, Maryland, USA, Reliability Engineering and System Safety, 1991, vol. 34, Issue 3, pp. 309–326.
12. Kaspersky K. RISK vs. CISC [digital resource] : Komp'yuterra. 1999, № 36 (314). Electronic version of printed publication. Access mode : http://old.computerra.ru/1999/314/3211/, free. Title (accessed date : 17.07.2015).
13. Orlov S. A., Cil'ker B. Ya. Computer and system organization. St. Petersburg, Piter, 2011, 688 p.

Статья представлена к публикации членом редколлегии Д. С. Марковым
Поступила в редакцию 08.04.2015, *принята к публикации 23.06.2015*

СИВКО Борис Витальевич – инженер-программист, магистр технических наук, сотрудник научно-исследовательской лаборатории «Безопасность и ЭМС технических средств» Белорусского государственного университета транспорта.
e-mail: bsivko@gmail.com