УДК 656.26

С. Н. ХАРЛАП, кандидат технических наук, Белорусский государственный университет транспорта, г. Гомель

ПРИМЕНЕНИЕ ДИВЕРСИТЕТА ДЛЯ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ МИКРОЭЛЕКТРОННЫХ СИСТЕМ

Рассмотрены подходы к применению диверситета в микроэлектронных системах железнодорожной автоматики и телемеханики. Приведены примеры функционального диверситета и диверситета технологий для обеспечения независимости отказов и повышения устойчивости к систематическим отказам. Сформулированы основные проблемы применения диверситета для повышения безопасности движения поездов.

Настоящее время микроэлектронные системы нашли широкое применение в различных системах управления и контроля на транспорте, в том числе в системах, связанных с обеспечением безопасности движения поездов. Примером таких систем могут служить современные системы железнодорожной автоматики и телемеханики. Одной из важнейших задач, решаемых этими системами, является обеспечение безопасности движения поездов. В отличие от релейных систем, безопасность которых базируется на свойствах специального реле I класса надежности, в микроэлектронных системах используются разнообразные методы обеспечения безопасности, которые рекомендованы международными стандартами [1–2]. Это связано с высокой сложностью микроэлектронных систем, разнообразием применяемых аппаратных средств и широким использованием программных средств для реализации безопасных функций.

Концепция обеспечения безопасности. Основные принципы обеспечения безопасного функционирования систем управления определяются концепцией, принятой разработчиком. Наибольшее распространение получила следующая концепция обеспечения безопасности [3]: «Одиночные отказы аппаратных и программных средств не должны приводить к опасным отказам и должны обнаруживаться при рабочих и тестовых воздействиях до того, как в системе произойдет второй отказ».

Основным способом реализации данной концепции является параллельное выполнение ответственных функций в нескольких вычислительных каналах (многоканальная обработка) с последующим сравнением результатов. Если результаты вычислений в различных каналах совпадают, то считается, что система исправна и правильно выполняет свои функции. Если наблюдается расхождение, то принимается решение о наличии отказа в системе и выполняется ее отключение (переход в защитное состояние). При таком подходе любые одиночные отказы не могут привести к опасному отказу, т. к. выработка опасного управляющего воздействия блокируется вторым исправным каналом. Переход в защитное состояние при обнаружении отказа гарантирует, что к опасным последствиям не приведут последующие отказы. Многоканальная обработки нашла широкое применение в различных системах железнодорожной автоматики, например, системах микропроцессорной централизации Ebilock 950, ESA 44-BC, «I-путь», «Днепр» и др.

Ограничения многоканальной обработки. Безопасность многоканальных систем базируется на следующих предположениях.

1 *Независимость случайных отказов в однотипных элементах функционально избыточных структур.* Предполагается, что любой одиночный отказ аппаратных средств вызывает некорректную работу некоторых функциональных модулей только одного из каналов. Аналогичные функциональные модули второго канала должны оставаться исправными. Одновременный отказ в обоих каналах модулей, выполняющих одинаковые функции, считается опасным отказом, если оба модуля формируют одинаковые неправильные управляющие воздействия. Одной из причин такого поведения при отказе могут быть отказы по общей причине (*common cause failure*) [4].

2 *Исключение возможности накопления отказов.* Предполагается, что все одиночные отказы обнаруживаются контрольными средствами, которые обеспечивают переход системы в защитное состояние. Появление сложных микроэлектронных и микропроцессорных элементов привело к выделению нового класса отказов – маскируемых. Отказы аппаратных средств, которые не приводят сразу к нарушению функционирования системы, называются *маскируемыми* и могут быть обнаруживаемыми и не обнаруживаемыми в зависимости от реализации средств диагностики. Не обнаруживаемые отказы могут приводить к накоплению отказов и, как следствие, к возможности появления опасных отказов.

3 *Устойчивость к систематическим отказам.* В соответствии с [4] выделяют случайные отказы аппаратных средств и систематические отказы. Причинами систематических отказов являются ошибки человека при проектировании, изготовлении (реализации) и эксплуатации аппаратных средств и программного обеспечения. Предполагается, что в безопасных многоканальных структурах отсутствуют систематические отказы. Однако на практике полностью исключить систематические отказы невозможно, и в этом случае любой систематический отказ может стать опасным.

Нарушение любого из этих предположений может привести к нарушению концепции обеспечения безопасности и, как следствие, к снижению уровня полноты безопасности системы в целом.

Методы обеспечения независимости случайных отказов. В соответствии с [1] к основным методам обеспечения независимости отказов относят:

– функциональное разнообразие (*diversity* – диверситет): использование различных подходов для достижения тех же результатов;

– разнообразие (диверситет) технологий: использование различных типов аппаратного обеспечения и программного обеспечения для достижения тех же результатов;

– отсутствие общих компонентов: обеспечение отсутствия общих компонентов или систем поддержки (например, электропитания), отказ которых может привести к опасному виду отказа всей системы;

– отсутствие общих процедур: обеспечение отсутствия общих процедур при эксплуатации, техническом обслуживании или тестировании.

Таким образом можно выделить два основных направления обеспечения независимости отказов вычислительных каналов в многоканальных системах: использование различных видов диверситета и обеспечение отсутствия общих элементов и процедур.

Как уже было сказано выше, опасным является одновременный отказ в обоих каналах модулей, выполняющих одинаковые функции, если оба модуля формируют одинаковые неправильные управляющие воздействия. В случае, если аппаратное и программное обеспечение обоих модулей идентично, то с большой вероятностью одно и то же внешнее воздействие вызовет одинаковые отказы в этих модулях. Поэтому все отказы по общей причине считаются опасными.

Подход, связанный с обеспечением отсутствия общих элементов и процедур базируется на физическом разделении каналов между собой. При этом снижается вероятность отказов по общей причине, а интенсивность одновременного отказа двух независимых модулей будет равна произведению интенсивностей отказов этих модулей. При средних значениях интенсивности отказов одного модуля 10^{-7}–10^{-6} 1/ч, интенсивность опасного отказа будет меньше 10^{-12} 1/ч, что соответствует требованиям нормативных документов.

Следует отметить, что не всегда возможно полностью исключить общие элементы и процедуры в каналах многоканальной структуры. Такие функции, как синхронизация работы каналов, сравнение результатов работы каналов, обмен данными между каналами, подразумевает наличие общих элементов: каналов передачи данных, устройств синхронизации, компараторов и др. Это накладывает определенные ограничения на использование данной группы методов обеспечения независимости отказов.

Более универсальным методом является использование диверситета, который может быть использован практически во всех ситуациях. Этот подход базируется на том, что модули разных каналов, выполняющие одинаковые функции, реализуются разными способами. В этом случае внешние воздействия, вызвавшие отказ одного из модулей, либо не повлияют на работу второго модуля, либо приведут к тому, что последствия отказов в разных модулях будут различны. При достаточном уровне диверситета даже при одновременных отказах этих модулей, вызванных общими причинами, модули сформируют различные управляющие воздействия, что будет обнаружено внешней схемой сравнения и вызовет переход в защитное состояние. Таким образом, отказы по общей причине переводятся из категории опасных в защитные.

Однако использование диверситета предполагает значительное увеличение затрат на разработку и техническое обслуживание системы, что является основным сдерживающим фактором его широкого использования.

Функциональный диверситет. Как было сказано выше, виды диверситета можно условно разделить на две категории: функциональный диверситет и диверситет технологий.

Функциональный диверситет предполагает использование различных подходов для достижения одних и тех же результатов. При этом каждая функция выполняется несколько раз различными способами. Например, если нам требуется опросить три дискретных датчика A, B и C и включить исполнительный объект Y в случае, когда датчики A или C включены, а датчик B – выключен, то эту функцию можно описать следующим образом:

$$Y = (A \vee C)\overline{B}. \qquad (1)$$

Реализовать эту функцию можно несколькими способами, которые представлены на рисунке 1. Вторая реализация функции Y (см. рисунок 1, *б*) выполнена преобразованием исходной функции с использованием теорем Де-Моргана для сложения и умножения [5].

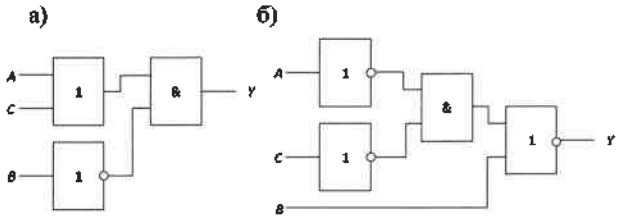

Рисунок 1 – Разные способы реализации функции Y

В качестве примера влияния отказов по общей причине на работу полученных диверситетных модулей рассмотрим последствия одновременных отказов в обоих модулях элементов «И», при которых на выходах элементов формируется значение логической единицы независимо от значений входных логических переменных (отказ вида «константная 1»). Как видно из рисунка 1, первая схема сформирует на выходе значение «1», а вторая – значение «0».

Программная реализация этой функции также может быть диверситетной. На рисунке 2 представлены алгоритмы реализации этой функции разными способами. Первый вариант реализации (см. рисунок 2, *а*) предполагает непосредственное вычисление функции Y с помощью логических операторов. Второй способ, получивший название «метод бинарных программ» [6] (см. рисунок 2, *б*), основан на проверке ряда условий и получения результата логической функции без ее вычисления. Так, для нашего примера, при значении B, равном единице, значение функции Y равно нулю при любых значениях оставшихся переменных A и B.

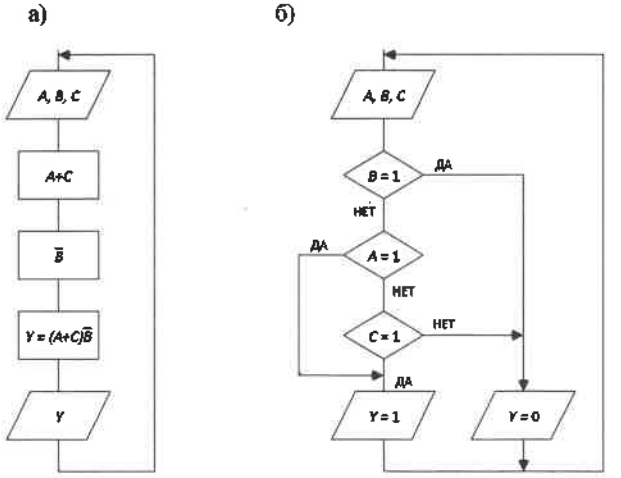

Рисунок 2 – Программная реализация функции Y

Такой метод часто используется при разработке программного обеспечения безопасных систем и получил названия «многовариантное программирование», «*N*-версионное программирование», «диверситетное программирование».

Целью данного метода является обнаружение и маскирование ошибок программных средств для предотвращения критичных для безопасности отказов системы и продолжения ее правильной работы. При многовариантном программировании заданная программная спецификация проектируется и реализуется различными способами *N* раз. Одни и те же входные значения поступают в *N* версий с последующим сравнением результатов. Если результат определяется как правильный, он поступает на выходы системы управления.

Важным требованием является то, что в некотором смысле *N* версий должны быть независимы друг от друга, поэтому они не все одновременно должны перестать правильно работать по общей причине. *N* версий могут выполняться параллельно на различных компьютерах, либо все версии могут выполняться последовательно на одном компьютере с последующим сравнением полученных результатов на том же компьютере.

Как видно из рисунка 2, для защиты от отказов по общей причине диверситет программных реализаций достигается не только разными алгоритмами, но и различными ресурсами, необходимыми для выполнения этих алгоритмов. Поэтому отказы по общей причине, приводящие невозможности использования определенных ресурсов, повлияют только на одну из реализаций. Например, неправильное вычисление логической операции «ИЛИ» может исказить результат выполнения первой программы, но никак не повлияет на вторую, а отказ флага сравнения, по которому осуществляется условный переход, исказит работу второго алгоритма, но не повлияет на первый. Таким образом обеспечивается независимость отказов в разных каналах.

Диверситет технологий. Диверситет технологий предполагает использование различных типов аппаратного обеспечения и программного обеспечения для достижения тех же результатов. Аппаратный диверситет может быть реализован применением в различных каналах компонентов с различными частотами и типами отказов. Примерами аппаратного диверситета могут служить построение различных каналов на базе:

– электронных и релейных компонентов;

– цифровых и аналоговых элементов;

– жесткой и программируемой логике;

– микроконтроллеров и программируемых логических интегральных схем (ПЛИС);

– микроконтроллеров, использующих различные (CISC, RISC или MISC) архитектуры и т. п.

Приведенные примеры аппаратного диверситета упорядочены по убыванию степени различия технологий. Наиболее сильным аппаратным диверситетом является реализация одного канала на базе электронных компонентов, а второго – с помощью релейной логики. Примеры таких реализаций функции (1) приведены на рисунках 1 и 3.

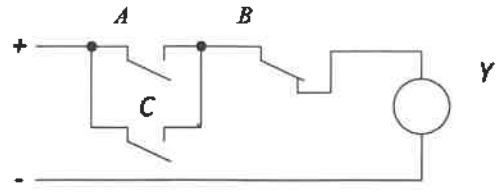

Рисунок 3 – Релейная реализация функции *Y*

В качестве примера диверситета на базе аналоговых и цифровых элементов можно привести пример различных реализаций инвертора (рисунок 4).

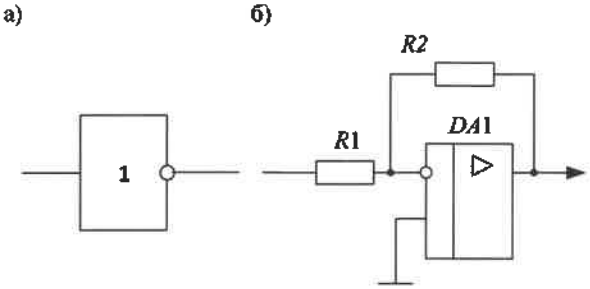

Рисунок 4 – Реализация цифрового (*а*) и аналогового (*б*) инверторов

В качестве примера реализации функции (1) на жесткой логике можно рассмотреть схему на рисунке 1, а в качестве программируемой логики можно взять любой микроконтроллер и реализовать на нем программу по любому алгоритму из рисунке 2.

При аппаратном диверситете защита от отказов по общей причине обеспечивается в первую очередь тем, что используемые диверситетные компоненты обладают различной чувствительностью к внешним воздействиям и реакцией на эти воздействия. Поэтому отказ по общей причине диверситетных модулей приведет к различиям в поведении этих модулей, что будет обнаружено при сравнении результатов их работы. Таким образом, отказ по общей причине не приводит к опасным последствиям и может быть классифицирован как защитный.

Программный диверситет технологий может быть достигнут использованием:

– различных языков программирования;

– различных сред разработки;

– различных операционных систем.

Использование этих методов позволяет частично защититься от отказов по общей причине за счет использования различных ресурсов вычислительных каналов, хотя их эффективность не так очевидна, как при использовании аппаратного диверситета.

Методы обеспечения устойчивости к систематическим отказам. Перечислить каждую причину систематических отказов, источники которых возникают на протяжении всех стадий жизненного цикла, и каждое средство защиты не представляется возможным по следующим причинам [1]: влияние систематических ошибок зависит от стадии жизненного цикла, на которой они вносятся, и эффективность любой конкретной меры

или средства по предотвращению отказов зависит от их применения.

В то же время в соответствии с [1] при проектировании безопасной системы управления должна быть обеспечена устойчивость:

– к любым остаточным ошибкам проектирования аппаратных средств, если вероятность ошибок проектирования аппаратных средств не может быть исключена;

– внешним влияниям, включая электромагнитные воздействия;

– ошибкам человека-оператора при эксплуатации системы;

– любым остаточным ошибкам в программном обеспечении;

– любым ошибкам, возникающим в результате выполнения любого процесса передачи данных.

В связи с этим основными источниками систематических отказов принято считать:

– отказы, вызванные ошибками человека, возникающими на этапах разработки и изготовления системы (например, ошибки спецификации, ошибки программного обеспечения; ошибки при проектировании и изготовлении аппаратных средств);

– отказы, вызванные ошибками, возникающими во время эксплуатации системы (например, отказы, вызванные неправильным использованием оборудования).

Для предотвращения таких отказов или уменьшения их влияния на безопасность (если они происходят) обычно требуется применение большого числа различных средств. Далее мы рассмотрим только влияние диверситетных методов на устойчивость к систематическим отказам.

Влияние различных видов диверситета на устойчивость к систематическим отказам. Опасным отказом в многоканальных системах считается отказ, при котором несколько каналов одновременно сформируют одинаково неверные управляющие воздействия. Это может быть вызвано как отказами по общей причине, которые мы рассматривали выше, так и систематическими отказами. Например, если в вычислительных каналах используется одинаковое программное обеспечение, то любая ошибка будет проявляться одинаково и не будет обнаружена схемами сравнения. Таким образом, ошибка человека на стадиях разработки и изготовления системы становится опасной, если она проявится в нескольких каналах одинаковым образом.

Для исключения таких последствий существует два основных подхода:

– многоступенчатый контроль всех стадий разработки аппаратных и программных средств;

– обеспечение достаточной независимости разработки аппаратных и программных средств для различных каналов многоканальной системы. В этом случае предполагается, что допущенные при разработке ошибки человека проявят себя в разных каналах по-разному, что позволит при сравнении результатов работы каналов их обнаружить и обеспечить переход в защитное состояние.

Для достижения достаточной независимости разработки аппаратных и программных средств для различных каналов многоканальной системы в целом используют те же подходы, что и для обеспечения независимости случайных отказов аппаратных средств:

– функциональный диверситет;

– диверситет технологий;

– отсутствие общих процедур проектирования, разработки и изготовления каналов.

Рассмотрим эти методы с точки зрения влияния на устойчивость к систематическим отказам.

Применение функционального диверситета приводит к разработке различных спецификаций для каждого канала, отличающихся набором функций, алгоритмами, схемными решениями. Любая ошибка, возникшая при разработке спецификации, коснется только одного вычислительного канала и не будет перенесена во второй канал. То же самое произойдет и при проектировании, программировании и изготовлении каналов, т. к. каждый канал будет разрабатываться по отдельным спецификациям.

Данный метод не устраняет ошибок, не выявленных при проектировании, а также ошибок в интерпретации спецификации, однако он является средством для обнаружения и маскирования ошибок, прежде чем они смогут повлиять на безопасность.

Недостатком такого подхода является как минимум удвоение затрат на разработку.

Диверситет технологий кроме применения методов, рассмотренных выше, практически всегда дополняется правилом, что аппаратные и программные средства различных каналов должны разрабатывать различные группы разработчиков. В этом случае предполагается, что даже отталкиваясь от одной и той же спецификации требований, если разные разработчики и допустят ошибки, то эти ошибки проявятся по-разному и будут обнаружены при сравнении работы каналов. Использование различных языков и сред программирования только усиливает этот эффект. Как и в случае с функциональным диверситетом, этот метод очень затратен, т. к. подразумевает финансирование еще одной параллельной разработки.

На практике часто объединяют эти подходы, когда каналы проектируют различные группы разработчиков по отличающимся спецификациям (функциональный диверситет) с применением различных операционных систем, языков и сред программирования (диверситет технологий).

Проблемы применения диверситета. Следует учитывать, что в стандартах предлагаются только общие подходы к достижению диверситета, рассмотренные в этой статье. К сожалению, эксперименты и аналитические исследования показывают, что применение диверситета не всегда столь эффективно, как хотелось бы. Независимость версий, являющуюся основой для диверситета, на практике довольно трудно достичь и продемонстрировать. Даже если используются различные функциональные элементы и алгоритмы, привлекаются различные коллективы разработчиков, разные версии аппаратного и программного обеспечения слишком часто имеют одинаковые реакции при проявлении внутренних ошибок или искажении внешних данных.

В последнее время получил распространение комплексный подход, при котором одновременно используются как аппаратный, так и программный диверситеты. В этом случае в разных каналах обработки информации используются различные аппаратные средства, с загруженными в них диверситетными программами. Такой подход позволяет объединить достоинства обоих методов и защититься как от отказов по общей причине аппаратных средств, так и от ошибок программного обеспечения.

До настоящего времени не существует эффективного метода, количественно оценивающего уровень разнообразия (диверситета) различных версий, и, как следствие, методов оценки достаточности полученного диверситета для заданного уровня полноты безопасности.

Выводы. Основными преимуществами использования диверситета являются:

– повышение стойкости к систематическим отказам в процессе проектирования, реализации, эксплуатации и технического обслуживания аппаратных и программных средств;

– снижение риска возникновения отказов по общей причине.

К недостаткам использования диверситета можно отнести:

– значительное увеличение стоимости разработки системы;

– сложность подтверждения различного поведения диверситетных каналов при возникновении случайных отказов аппаратных средств, систематических отказов (ошибок) проектирования, реализации аппаратных средств и ошибок в программном обеспечении;

– независимо от подхода в настоящее время нет эффективного метода, оценивающего уровень разнообразия (диверситета).

Однако следует отметить, что альтернативные методы решения задачи повышения стойкости к систематическим отказам и снижения риска возникновения отказов по общей причины не менее затратны и сложны. При этом каждый из альтернативных методов в отличии от диверситета решает только часть описанных выше проблем. Поэтому, несмотря на эти недостатки, применение диверситета в безопасных микроэлектронных системах является полностью оправданным.

Список литературы

1 **СТБ IEC 61508-2–2014.** Функциональная безопасность электрических, электронных, программируемых электронных систем, относящихся к безопасности. Часть 2. Требования к электрическим, электронным, программируемым электронным системам, относящимся к безопасности. – Введ. 2015-06-01.

2 **СТБ IEC 62425–2011.** Железный дороги. Системы связи, сигнализации и обработки данных. Электронные системы сигнализации, связанные с безопасностью. – Введ. 2011-08-01.

3 **РТМ 32 ЦШ 1115842.01–94.** Руководящий технический материал. Безопасность железнодорожной автоматики и телемеханики. Методы и принципы обеспечения безопасности микроэлектронных СЖАТ. – СПб., 1994. – 120 с.

4 **СТБ IEC 61508-4–2014.** Функциональная безопасность электрических, электронных, программируемых электронных систем, относящихся к безопасности. Часть 4. Термины и определения и сокращения. – Введ. 2015-06-01.

5 Теория дискретных устройств железнодорожной автоматики, телемеханики и связи : учеб. / В. В. Сапожников [и др.] ; под ред. Вл. В. Сапожникова. – М. : ФГБОУ «УМЦ ЖДТ», 2016. – 339 с.

6 Методы построения безопасных микроэлектронных систем железнодорожной автоматики / В. В. Сапожников [и др.] ; под ред. Вл. В. Сапожникова. – М. : Транспорт, 1995. – 272 с.

7 **СТБ IEC 61508-3–2014.** Функциональная безопасность электрических, электронных, программируемых электронных систем, относящихся к безопасности. Часть 3. Требования к программному обеспечению. – Введ. 2015-06-01.

Получено 30.08.2020

S. N. Kharlap. Applying diversity to increase safety microelectronic systems.

Approaches to the use of diversification in microelectronic systems of railway automation and telemechanics are considered. Examples of functional diversification and diversification of technologies for ensuring the independence of failures and increasing resistance to systematic failures are given. The main problems of using diversification to improve the safety of train traffic are formulated.