Риски нужно контролировать постоянно. И качественно выполненная и документированная первая оценка может существенно упростить последующую деятельность.

Для небольшого предприятия допустимо рассматривать всю информационную инфраструктуру. Однако, если предприятие крупное, всеобъемлющая оценка может потребовать неприемлемых затрат времени и сил. В таком случае следует сосредоточиться на наиболее важных сервисах, заранее соглашаясь с приближенностью итоговой оценки. Если важных сервисов все еще много, выбираются те из них, риски для которых заведомо велики или неизвестны.

Очень важно выбрать разумную методологию оценки рисков. Целью оценки является получение ответа на два вопроса: приемлемы ли существующие риски, и если нет, то какие защитные средства экономически выгодно использовать.

Выбирая подходящий способ защиты, необходимо учитывать возможность покрытия одним сервисом безопасности сразу нескольких других сервисов. Важным обстоятельством является совместимость нового средства со сложившейся операционной и аппаратно-программной структурой предприятия и его подразделений.

Реализацию и проверку новых сервисов безопасности следует предварительно спланировать. Необходимо составить план тестирования, в котором учесть и наличие финансовых средств, и сроки обучения персонала. Когда намеченные меры приняты, необходимо проверить их действия и убедиться, что остаточные риски приемлемы. Если это на самом деле так, значит, все в порядке и можно спокойно намечать дату ближайшей переоценки. В противном случае придется проанализировать допущенные ошибки и провести повторный сеанс управления рисками.

Все эти мероприятия и есть основная часть управленческих мер обеспечения информационной безопасности.

Список литературы

1 **Демуськов, А. Б.** Проблемы информационной безопасности в компьютерных сетях / А. Б. Демуськов, Г. И. Большакова, Т. П. Бышик // Известия Гомельского госуниверситета им. Ф. Скорины. – 2003. – № 3 (18).

2 **Демуськов, А. Б.** Политики информационной безопасности предприятий / А. Б. Демуськов, В. А. Короткевич, Л. И. Короткевич // Известия Гомельского госуниверситета им. Ф. Скорины. – 2003. – № 4 (19).

3 **Герасименко, В. А.** Основы защиты информации / В. А. Герасименко, А. А. Малюк. – М. : МИФИ, 1997.

4 Научная сессия МИФИ-2003. Проблемы информационной безопасности в системе высшей школы : X Всероссийская науч. конф. : сб. науч. тр. – М. : МИФИ, 2003. – 256 с.

5 Гостехкомиссия России. Руководящий документ. Концепция защиты СВТ и АС от НСД к информации. – М., 1992.

6 **Гайкович, В. А.** Безопасность электронных банковских систем / В. А. Гайкович, А. Першин. – М. : Единая Европа, 1994.

УДК 004.052.32+681.518.5

МЕТОДЫ СИНТЕЗА САМОПРОВЕРЯЕМЫХ ЛОГИЧЕСКИХ УСТРОЙСТВ НА ОСНОВЕ ПОЛИНОМИАЛЬНЫХ КОДОВ

Д. В. ЕФАНОВ
Российский университет транспорта (МИИТ), г. Москва

Р. Б. АБДУЛЛАЕВ
Петербургский государственный университет путей сообщения Императора Александра I, Российская Федерация

В современном мире все более прогрессивнее происходит переход от использования выполнения операций вручную к применению автоматизированных и автоматических систем управления в выполнении задач любых сложностей [1]. Такие системы для выполнения различных задач проектируются с разным уровнем надежности. Для систем с высоким уровнем надежности на этапе их проектирования используют различные методы обеспечения отказоустойчивости, к примеру, в системах микропроцессорного исполнения широко используют резервирование и диверсифицирование блоков и узлов системы для обнаружения в их структуре сбоев и отказов, для реализации отдельных схем используют высоконадежные логические составляющие и т. п. [2]. Дублирование узлов и компонентов подразумевает многократное увеличение аппаратных средств при построении системы. Для сокращения показателей структурной избыточности системы в целом при сохранении

свойств обнаружения внутренних неисправностей в контролируемых блоках и узлах широко используют методы синтеза самопроверяемых встраиваемых схем контроля [3]. С такой целью схемы встроенного контроля реализуются с применением помехоустойчивых кодов по структуре, изображенной на рисунке 1.

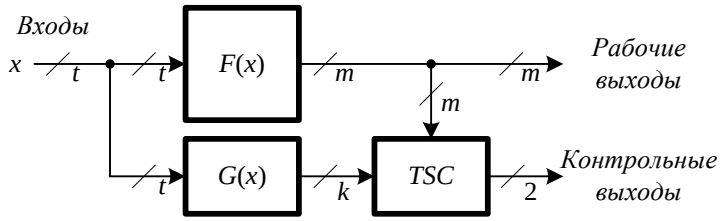

Рисунок 1 – Структурная схема организации контроля логического устройства на основе помехоустойчивого кода

На рисунке 1 блок $F(x)$ является диагностируемым устройством с количеством выходов, равным m. Блок $G(x)$ является контрольной схемой, вырабатывающей контрольные функции k от значений входных переменных x. Блок *TSC* представляет собой тестер, состоящий из кодера используемого помехоустойчивого кода и компаратора. На входы кодера подаются комбинации длиной m от рабочих функций блока $F(x)$, а на выходах формируются контрольные векторы длиной k заранее выбранного кода. Функции блока $G(x)$ и кодера, как правило, реализуются взаимно инверсными, а компаратор реализуется на основе элементарных модулей сжатия парафазных сигналов [4]. Тестер снабжается двумя выходами, на которых формируется сигнал контроля: при отсутствии неисправностей и ошибок в вычислениях формируется парафазный сигнал, установка непарафазного сигнала свидетельствует о наличии ошибок.

Выигрыш такой системы на основе помехоустойчивого кода по аппаратурным затратам по сравнению с дублированием достигается благодаря использованию в схемах сравнения меньшего по длине контрольного вектора. Однако уменьшение числа контрольных разрядов влияет на характеристики обнаружения ошибок на выходах логических устройств. В практических реализациях, однако, часть ошибок определенных видов и кратностей формируется не всегда, что определяет и возможности применения избыточного кодирования для контроля логических устройств. Рассмотрим методы синтеза самопроверяемых устройств на основе широко известных полиномиальных кодов [5].

1 Метод синтеза схемы контроля на основе подбора образующего полинома. Образующие полиномы определяют значение k и характеристики обнаружения ошибок кодом. Для построения схемы контроля с обнаружением полного множества ошибок на выходах контролируемых объектов анализируются виды и кратности проявляющихся на их выходах ошибок при внесении неисправностей из заданного класса. Затем определяются полиномы, позволяющие идентифицировать полученные виды ошибок.

Эксперименты с большим числом контрольных схем показывают, что представленный метод позволяет в ряде случаев синтезировать полностью самопроверяемые устройства. Если для устройства не удается построить схему контроля за счет подбора образующего полинома, то применяют следующие методы.

2 Метод синтеза схемы контроля на основе полиномиальных кодов, обнаруживающих определенные кратности ошибок. В зависимости от структуры исходного устройства кратности ошибок на его выходах могут быть различными. Полиномиальными кодами не обнаруживаются полностью все кратности ошибок, но при этом обнаруживаются полностью определенные кратности ошибок, в основном, ошибки малых кратностей. Это свойство можно учесть при синтезе схемы контроля. В таком случае для обнаружения полного множества ошибок на выходах устройства предлагается разбиение его выходов на группы контролепригодных выходов по полиномиальным кодам. Для этого подбирается полиномиальный код, обнаруживающий все ошибки до определенной кратности d. На множестве выходов схемы осуществляется поиск подмножеств таких выходов, на которых при внутренней неисправности в объекте диагностирования возможно одновременное проявление ошибок. Определяется число r таких выходов в каждом подмножестве. Очевидно, что при $r > d$ для искомых подмножеств не гарантируется обнаружение полного множества ошибок на выходах устройства. В таком случае, если число $r > d$ для некоторого подмножества, то из данного подмножества «исключают» несколько выходов и включают их в другое подмножество или формируют новое подмножество выходов с таким расчетом, чтобы в каждом подмножестве выходов вы-

полнялось условие $r \leq d$. Подмножества выходов можно объединять в одну группу, если на данных подмножествах выходов одновременное проявление ошибок при внутренних неисправностях исключено. Для каждой контролируемой группы реализуется своя схема контроля, а затем выходы различных схем контроля объединяются на входах самопроверяемого компаратора.

3 Метод синтеза схемы контроля на основе полиномиальных кодов, обнаруживающих определенные виды ошибок. Согласно классификации ошибок в кодовых векторах могут возникать следующие виды ошибок: одиночные, монотонные, симметричные и асимметричные ошибки [4]. Одиночные ошибки связаны с искажениями только одного разряда, монотонные, симметричные и асимметричные – двух и более. Если искажаются только нулевые или только единичные разряды, то ошибка считается монотонной, иначе – симметричной или асимметричной. Симметричная ошибка имеет четную кратность и связана с одинаковым числом искажаемых нулевых и единичных значений. Асимметричная ошибка – это ошибка, связанная с неравным количеством искажений нулевых и единичных разрядов. В ходе исследования полиномиальных кодов установлено, что некоторые образующие полиномы позволяют строить коды с полным обнаружением ошибок определенных видов [5]. В таком случае, для построения схемы контроля с идентификацией полного множества ошибок анализируются все возможные виды ошибок на выходах устройства. Далее формируются группы контролепригодных по полиномиальным кодам выходов устройства. Для этого из множества выходов выделяются такие, на которых проявляются только симметричные или только асимметричные ошибки. Выходы с одноименным видом ошибок помещаются в одну группу. Для каждой сформированной группы реализуется своя контрольная схема.

В конечном счете, при проектировании систем на основе рассмотренных методов выбирается метод, позволяющий синтезировать самопроверяемое устройство с минимальной структурной избыточностью.

Приведенные выше методы синтеза схем встроенного контроля на основе полиномиальных кодов позволяют получать устройства, имеющие свойство обнаружения полного множества ошибок с наименьшими аппаратурными затратами.

Список литературы

1 Control Systems: Theory and Applications / V. Kuntsevich [et al.] // River Publishers Series in Automation, Control and Robotics, 2018.

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

3 Надежность и эффективность в технике: Справочник в десяти томах. Т. 9: Техническая диагностика / под ред. В. В. Клюева и П. П. Пархоменко. – М. : Машиностроение, 1987. – 352 с.

4 **Сапожников, В. В.** Коды с суммированием для систем технического диагностирования : [монография] / В. В. Сапожников, Вл. В. Сапожников, Д. В. Ефанов. – Т. 1: Классические коды Бергера и их модификации. – М. : Наука, 2020. – 383 с.

5 **Abdullaev, R.** Polynomial Code with Detecting the Symmetric and Asymmetric Errors in the Data Vectors / R. Abdullaev [et al.]. // Proceedings of 17th IEEE East-West Design & Test Symposium (EWDTS`2019), Batumi, Georgia, September 13–16. – 2019. – P. 157–161. – DOI: 10.1109/EWDTS.2019.8884451.

УДК 658.56

ОСОБЕННОСТИ ПРОВЕДЕНИЯ FMECA МИКРОЭЛЕКТРОННЫХ СИСТЕМ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ

И. О. ЖИГАЛИН, С. И. ХОМЕНКО, И. В. ЛОГВИНЕНКО
Белорусский государственный университет транспорта, г. Гомель

FMECA (Failure Mode, Effects and Criticality Analysis) – это инструмент для анализа потенциальных отказов, их последствий и критичности. Метод применяется при оценке соответствия требованиям по функциональной безопасности и предназначен для выявления потенциальных отказов, причин их возникновения и последствий при эксплуатации [1]. Эффективность FMECA заключается в том, что, благодаря усилиям на начальной стадии, можно добиться соответствия заданным ТНПА требованиям по функциональной безопасности на последующих этапах жизненного цикла продукта. Кроме того, исключение потенциальных отказов позволяет существенно снизить количество доработок до соответствия требованиям по функциональной безопасности.