– штатный алгоритм (при наличии одной (первой) из числа установленных кодовых комбинаций дешифратор не должен давать сбоя (изменения показания локомотивного светофора) при условии нормальной регулировки его реле и времени замедления реле СР 5,0 с (минимально допускаемое));

– возможный алгоритм (при наличии одной из установленных кодовых комбинаций дешифратор не должен давать сбоя при условии нормальной регулировки реле и времени замедления реле СР свыше 5,0 с);

– алгоритмы низкой помехоустойчивости (если временные параметры реле схемы декодирования кодовых комбинаций не соответствуют норме или замедление реле СР не соответствует установленным параметрам).

На основании представленных алгоритмов работы реле СР оказывается возможным произвести классификацию дешифраторов (или комплектов аппаратуры, в том числе микропроцессорных) по степени их помехоустойчивости. Если не выполняется хотя бы один штатный алгоритм, то такой уровень соответствует низкой помехоустойчивости. Если выполняются все штатные алгоритмы, то дешифратор или комплект аппаратуры имеет номинальный уровень помехоустойчивости. Выполнение всех возможных алгоритмов работы реле СР подразумевает высокий уровень помехоустойчивости работы.

Внедрение полученных тестовых сигналов в рамках предлагаемой технологии проверки локомотивной аппаратуры АЛСН позволит исключить выпуск в эксплуатацию так называемых «сбойных» локомотивов, а также сократит время и затраты на техническое обслуживание. Повышается производительность труда и культура персонала, что позволяет повысить, в конечном итоге, безопасность движения поездов.

На базе вышеуказанного алгоритма в настоящее время специалистами АО «НИИАС» разрабатываются технические средства контроля и диагностики локомотивной аппаратуры в условиях контрольных пунктов АЛС депо.

УДК 656.25

ПРИМЕНЕНИЕ ДИВЕРСИТЕТА ДЛЯ ПОВЫШЕНИЯ УРОВНЯ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ МИКРОЭЛЕКТРОННЫХ СИСТЕМ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ

С. Н. ХАРЛАП

Белорусский государственный университет транспорта, г. Гомель

Важнейшей задачей, стоящей перед разработчиками микроэлектронных систем железнодорожной автоматики, является достижение заданного уровня полноты функциональной безопасности (УПБ или SIL). Методы обеспечения функциональной безопасности определены международными стандартами IEC61508:2010 (ГОСТ Р МЭК 61508–2012), EN50128:2011 и EN50129:2018.

В соответствии с этими стандартами основным методом обеспечения безопасности в настоящее время является многоканальная обработка информации (дублированные или троированные мажоритарные структуры). Безопасность при этом обеспечивается в предположении, что одиночный отказ аппаратных средств или одиночные ошибки в программном обеспечении не могут привести к опасному отказу, а вероятность накопления нескольких отказов ниже допустимого нормативного значения.

Однако при использовании данного метода необходимо в первую очередь подтвердить:

– что интенсивность отказов по общей причине не превышает допустимого значения интенсивности опасного отказа;

– система обладает требуемой стойкостью к систематическим отказам, т. е. отказам, связанным с какой-либо причиной, которая может быть исключена только путем модификации проекта либо производственного процесса, операций, документации, либо других факторов (ГОСТ Р МЭК 61508-4–2012).

Примерами причин систематических отказов являются ошибки человека:

– в спецификации требований к безопасности;

– при проектировании, изготовлении, установке или во время работы аппаратных средств;

– при проектировании и реализации программного обеспечения.

Для снижения риска возникновения отказов по общей причине и для повышения стойкости к систематическим отказам в процессе проектирования, реализации, эксплуатации и технического

обслуживания аппаратных средств стандартами рекомендованы одинаковые подходы, которые заключаются в определении следующих общих требований к каналам обработки информации в многоканальных системах:

1) каналы должны быть независимыми настолько, чтобы вероятность одновременного отказа двух или более функциональных модулей была низкой по сравнению с требуемой полнотой безопасности;

2) каналы должны быть функционально различными (т. е. использовать совершенно различные подходы для достижения одних и тех же результатов);

3) должны основываться на различных технологиях (т. е. в них должно использоваться оборудование различных видов для достижения одних и тех же результатов);

4) не должны иметь общих частей, систем сервиса или поддержки (например, источников питания), отказ которых может привести к опасному отказу всей системы.

Второе и третье требования предполагают наличие разнообразия (диверситета) между реализациями каналов обработки информации. При этом можно выделить два направления реализации диверситета:

– функциональное разнообразие – использование различных подходов для достижения тех же результатов;

– разнообразие технологий – использование различных типов оборудования для достижения тех же результатов.

Первый подход получил широкое распространение при разработке программного обеспечения 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 на одном компьютере с последующим сравнением полученных результатов на том же компьютере. Данный метод не устраняет ошибок, не выявленных при проектировании программ, а также ошибок в интерпретации спецификации, однако он является средством для обнаружения и маскирования ошибок прежде чем они смогут повлиять на безопасность.

К сожалению, эксперименты и аналитические исследования показывают, что N-вариантное программирование не всегда столь эффективно, как хотелось бы. Независимость версий, являющуюся основой для многовариантного программирования, на практике довольно трудно достичь и продемонстрировать. Даже если используются различные алгоритмы, то разнообразные версии программного обеспечения слишком часто имеют одинаковые реакции при проявлении внутренних ошибок или искажении внешних данных. В стандартах предлагаются только общие подходы к достижению диверситета, такие как привлечение для разработки различных версий независимых коллективов программистов, использование различных операционных систем и языков программирования и т. п. Однако до настоящего времени не существует эффективного метода, оценивающего уровень разнообразия (диверситета) различных версий программ, и, как следствие, методов оценки достаточности полученного диверситета для заданного уровня полноты безопасности.

Второй подход основан на разнообразии (диверситете) аппаратных средств. Целью данного подхода является обнаружение систематических отказов при выполнении операций с использованием разнообразных компонентов с различными частотами и типами отказов. При этом для разных каналов многоканальной системы, связанной с безопасностью, используются различные типы компонентов. Это снижает вероятность появления отказов по общей причине и повышает вероятность обнаружения таких отказов.

В последнее время получил распространение комплексный подход, при котором одновременно используются как аппаратный, так и программный диверситет. 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.

Таким образом, 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 причине не менее затратны и сложны. При этом каждый из альтернативных методов, в отличие от диверситета, решает только часть описанных выше проблем. Поэтому, несмотря на эти недостатки, применение диверситета в микроэлектронных системах автоматики и телемеханики является полностью оправданным.

УДК 681.518.5+004.052.32

ОБОБЩЕННАЯ ФУНКЦИЯ ПРЕДПОЧТЕНИЯ ДЛЯ ОПТИМИЗАЦИИ ВОПРОСНИКОВ МЕТОДОМ КОРНЕВОГО ВОПРОСА

В. В. ХОРОШЕВ

Российский университет транспорта (МИИТ), г. Москва

Системы железнодорожной автоматики и телемеханики (СЖАТ) подвергаются постоянным нагрузкам в процессе эксплуатации. Для их бесперебойного функционирования необходимо производить процедуры обслуживания и диагностики. В связи с современными тенденциями постепенно переходят от периодического обслуживания объектов СЖАТ к обслуживанию по состоянию: постепенно происходит внедрение систем мониторинга [1]. Для обеспечения автоматизации диагностирования объектов СЖАТ в программных средствах систем мониторинга возможно применение различных способов: от экспертной оценки и самообучающихся компонентов до применения динамических способов формирования последовательностей расследования инцидентов. Последний вариант является, по мнению автора, весьма перспективным и может быть реализован с использованием теории вопросников [2, 3].

В теории вопросников основной задачей является оптимизация исходного вопросника по цене обхода. Для оптимизации применяются различные методы, самыми известными из которых являются метод динамического программирования, метод ветвей и границ, метод корневого вопроса и эвристические [3, 4]. Все методы имеют свои ограничения; например, в методе динамического программирования экспоненциально возрастает сложность с увеличением количества вопросов в вопроснике. Более простым способом оптимизации является метод корневого вопроса, но и данный метод оптимизации содержит ограничения, он работает в случае, когда между вопросами имеются отношения сравнения. Два вопроса y_1 и y_2 находятся в отношении сравнения в том случае, если подмножество какого-либо исхода одного из них является собственным подмножеством какого-либо исхода другого вопроса. Ранее А. Ю. Арженко и его учениками было проведено исследование отношений сравнения между вопросами бинарного вида [4] и выведена функция предпочтения двух сравниваемых бинарных вопросов. Данная работа освещает результаты исследований отношений сравнения различных типов сравниваемых вопросов (не только бинарных). Производится поиск отношений сравнения между бинарным и тернарным вопросом, между тернарными вопросами. Автором на основе проведенных изысканий получена обобщенная функция предпочтения, которая может быть применима для любых типов сравниваемых вопросов (как бинарных, так и q-арных).

При проведении исследований было получено, что между бинарным и тернарным вопросом возможны только три варианта отношений сравнения. Установим изначальные условия. Имеется