где λ_{ao} – интенсивность аварий по причине опасных отказов МПЦ; $\lambda_{ан}$ – интенсивность аварий по причине неопасных (защитных) отказов МПЦ; λ_{oo} – интенсивность опасных отказов ($\lambda_{oo} = 10^{-12}$–10^{-9} 1/ч, обеспечивается на этапе разработки системы); P_{co} – вероятность наличия неблагоприятной поездной ситуации в момент опасного отказа МПЦ; $P_{п}$ – вероятность парирования опасной технологической ситуации ДСП; $\lambda_{но}$ – интенсивность неопасных отказов (причем, $\lambda_{но} = 10^{-8}…10^{-4}$ 1/ч); $P_{сн}$ – вероятность наличия неблагоприятной поездной ситуации в момент неопасного отказа МПЦ; $P_{од}$ – вероятность ошибочных действий ДСП (имеет порядок $P_{од} = 10^{-3}…10^{-2}$ и зависит от многих факторов, таких как время суток, интенсивность работы, физиологическое состояние и др. В нештатных стрессовых ситуациях она может увеличиваться до 10^{-2}–10^{-1}).

Анализируя факторы, влияющие на интенсивность аварий λ_a, видно, что второе слагаемое в выражении (1) имеет преимущественный вклад, а меры повышения надежности и безопасности функционирования МПЦ в первую очередь должны быть связаны с уменьшением вероятности $P_{од}$ ошибочных действий ДСП.

Для снижения риска возникновения аварийных ситуаций в системах критичных к безопасности находят все более широкое применение интеллектуальные надстройки в виде систем поддержки принятия решений оперативным персоналом.

Для облегчения работы ДСП во внештатных ситуациях в МПЦ «іпуть» реализована интеллектуальная система поддержки принятия решений (СППР), задачей которой является предоставление дежурному по станции порядка действий при возникновении нештатных ситуаций и контроль его выполнения. Новизна технических решений МПЦ подтверждена патентами на изобретения в Республике Беларусь и РФ. Таким образом, интеллектуализация функций МПЦ путем интеграции в неё СППР повышает уровень безопасности движения поездов за счет значительного уменьшения ошибочных действий ДСП.

Анализ влияния интеллектуализации функций МПЦ на повышение безопасности движения поездов помимо этого дает возможность обоснования и количественной оценки необходимости «глубины» резервирования подсистем МПЦ.

УДК 004.312.466

АНАЛИЗ НА БЕЗОПАСНОСТЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ МИКРОПРОЦЕССОРНЫХ УСТРОЙСТВ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ

К. А. БОЧКОВ, Б. В. СИВКО
Белорусский государственный университет транспорта, г. Гомель

Современные микропроцессорные системы железнодорожной автоматики и телемеханики (СЖАТ) относятся к критически важным объектам информатизации с повышенными требованиями по уровню безопасности и надежности функционирования. Данные системы являются аппаратно-программными комплексами (АПК), в которых программное обеспечение (ПО) является неотъемлемым компонентом и оно подлежит анализу на безопасность, как и аппаратные средства СЖАТ. В настоящее время отсутствуют общепризнанные и универсальные методы проведения анализа на безопасность ПО, и одним из актуальных вопросов является разработка инструментария, позволяющего эффективно проводить мероприятия по обеспечению необходимого уровня качества ПО и последующему доказательству безопасности.

Согласно мировой практике, мнению экспертов и стандартам разработки критически важных объектов информатизации, верификация данных устройств должна проводиться независимо от коллектива разработчиков. Проводимый анализ на безопасность представляет собой полный цикл обратной разработки (reverse engineering), во время которой независимой организацией необходимо определить доказываемые свойства системы и проверить их на корректность. Для верификации систем, управляющими ответственными технологическими процессами, первым шагом является определение функции безопасности (ФБ), выполнение которой верифицируется в последующем.

Определение ФБ имеет ряд особенностей и проблем. Прежде всего, при доказательстве безопасности должна быть определена ФБ независимой организацией для последующего анализа корректности предоставленных разработчиками доказательных документов.

Во время верификации ключевой и опорной информацией является исходный код ПО и конкретные схемные решения АПК.

В процессе анализа ПО может оказаться, что принятая ФБ не является необходимой или достаточной. Во время последующего анализа на безопасность может быть выяснено, что заданные рамки слишком строги и доказательство безопасности провести невозможно, или напротив, слишком слабы, из-за чего уменьшается вероятность нахождения ошибок ПО.

Обратная разработка является трудоемким процессом, поэтому актуальным вопросом является создание и применение эффективных методов и средств, позволяющих проводить анализ на безопасность с приемлемыми затратами как времени, так и ресурсов.

Опыт верификации ПО СЖАТ существующих АПК, которые анализировались на безопасность в НИЛ «Безопасность и ЭМС технических средств» (БЭМС ТС) Белорусского государственного университета транспорта, говорит о том, что выбор функции безопасности существенно сказывается на качестве верификации и является проблемой, требующей особого внимания.

В докладе рассматриваются следующие рекомендации и подходы для работы с функцией безопасности:

1 Определение функции безопасности на основании:

1.1 Используемой стратегии обеспечения безопасности.

1.2 Требований безопасности к интерфейсам взаимодействия.

1.3 Требований безопасности к рассматриваемому АПК.

2 Изменение функции безопасности для более эффективной верификации:

2.1 Ослабление и усиление функции безопасности.

2.2 Выбор менее сложной функции.

2.3 Выбор функции, определяющей более детерминированное поведение системы.

3 Использование контрольного списка особенностей ПО.

В докладе рассматривается необходимость и условия применения описанных рекомендаций, позволяющих сделать эффективный и качественный выбор функции безопасности.

Выполненные в НИЛ «БЭМС ТС» Белорусского государственного университета транспорта работа по доказательству безопасности ПО микропроцессорных СЖАТ показали правильность принятого подхода определения ФБ для конкретных систем.

УДК 681.325.3

МОДЕЛИРОВАНИЕ В ПРОЦЕССЕ ИССЛЕДОВАНИЯ ПРОПУСКНОЙ СПОСОБНОСТИ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ С КОММУТАЦИЕЙ ПАКЕТОВ

П. М. БУЙ, Д. Е. ГОНЧАРОВ, К. М. ЛЕВШУНОВА

Белорусский государственный университет транспорта, г. Гомель

Исследование пропускной способности сетей передачи данных с коммутацией пакетов проще всего проводить на базе адекватной модели сети, позволяющей моделировать появление дополнительной нагрузки и новых источников нагрузки, а также выход из строя узлов или каналов связи. Такая модель разработана в виде компьютерной программы, которая позволяет создать любую сеть, состоящую из источников нагрузки и сетевых узлов с уникальными параметрами. Созданная сеть хранится в виде файла xml-формата (рисунок 1, *а*). В процессе настройки сети могут изменяться параметры источников нагрузки (адресаты и объем исходящей информации), сетевых узлов (объем памяти) и каналов связи (пропускная способность). На первом этапе модель предполагает использование виртуальных каналов, которые задаются в процессе создания сети. В дальнейшем планируется реализовать датаграмный режим, при котором каждый сетевой узел будет принимать решение о направлении передачи пакетов.

Внешний вид программы моделирования работы сети передачи данных с коммутацией пакетов представлен на рисунке 1, *б*.

В левой части рабочего окна расположена панель управления для загрузки и исследования сети. В центральной части представлено графическое изображение сети с указанием параметров источ-