

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-

ников и сетевых узлов. Графическое изображение сети является интерактивным и позволяет при нажатии левой клавишей мыши на том или ином объекте изменять его параметры в специально загрузаемом окне. Правая часть рабочего окна программы отображает результаты исследования сети. Представленная здесь статистика описывает общее количество пакетов, которые были отправлены источниками в сеть и поступили в приемники, а также положение пакетов, которые еще не дошли до приемников.

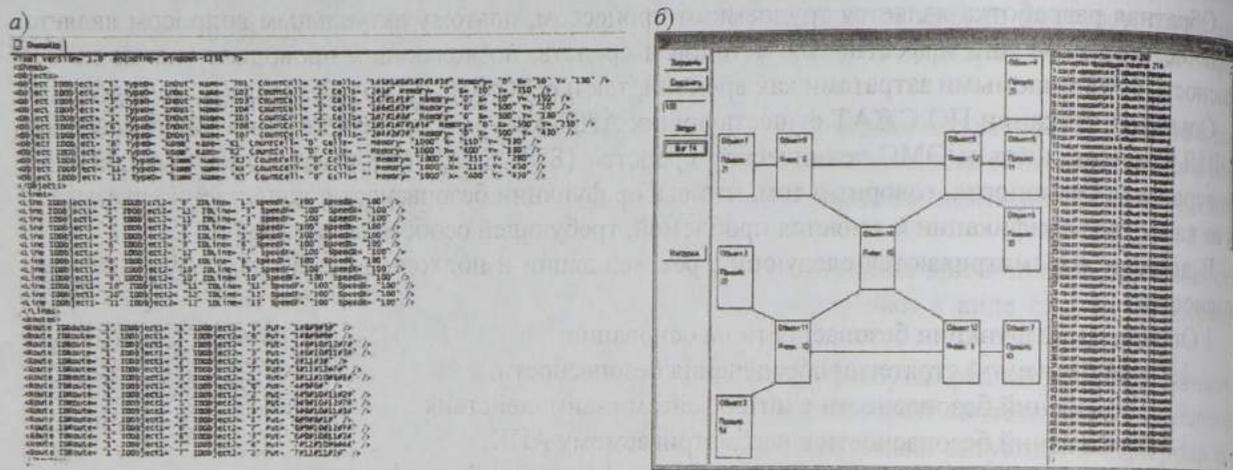


Рисунок 1 – Структура сети передачи данных в формате xml (а) и внешний вид программы моделирования работы сети (б)

Процесс исследования предполагает пошаговый или мгновенный прогон заданного количества «жизненных циклов» сети, на каждом из которых информационные пакеты делают один шаг на пути от источника к приемнику. Статистика, отображаемая на графическом изображении сети и в правой части рабочего окна, позволяет оценивать самое «узкое» звено сети, которое формирует очереди пакетов. Изменяя параметры узлов сети можно и повторяя эксперимент можно добиться оптимального согласования пропускной способности каналов и объема информации, поступающей от источников. При моделировании какой-либо существующей сети можно исследовать характер возникающих в ней задержек пакетов и определить наиболее «слабое» звено сети, ограничивающее общую скорость передачи пакетов от источника к приемнику.

УДК 656.257:681.32

УСОВЕРШЕНСТВОВАНИЕ ТЕХНИЧЕСКОГО КОНТРОЛЯ СИСТЕМЫ МИКРОПРОЦЕССОРНОЙ ЦЕНТРАЛИЗАЦИИ ПУТЁМ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ЕЁ ФУНКЦИОНАЛЬНЫХ ИСПЫТАНИЙ

А. Ю. КАМЕНЕВ

Украинская государственная академия железнодорожного транспорта, г. Харьков

Гарантирование безопасности применения системы микропроцессорной централизации стрелок и сигналов (МПС) достигается техническим контролем её характеристик и параметров на этапах производства, эксплуатации и ремонта. Эффективным средством его осуществления является активное воздействие на систему, достигаемое путём функциональных испытаний, которые призваны, согласно ГОСТ 16504-81, подтвердить её соответствие заданным показателям назначения. С учётом недостатков существующих методов и средств технического контроля, выполняемого с помощью данного вида испытаний, автором проведено научно-прикладное исследование, направленное на повышение их эффективности, которое вошло в его диссертационную работу. В результате получены следующие научные положения и технические средства: