УДК 004.312.466

ПРОЕКТИРОВАНИЕ БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ МИКРОПРОЦЕССОРНЫХ УСТРОЙСТВ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ

Б. В. СИВКО

Белорусский государственный университет транспорта, г. Гомель

Современные микропроцессорные системы железнодорожной автоматики и телемеханики (СЖАТ) отвечают за управление ответственными технологическими процессами. Программное обеспечение (ПО) данных систем является их неотъемлемой частью и к нему предъявляются такие же требования по уровню безопасности и надежности функционирования, как и к системе в целом. В связи с этим одним из актуальных вопросов является обеспечение необходимого уровня качества ПО с использованием различных средств и методов на всех этапах проектирования.

Опыт верификации микроэлектронных СЖАТ говорит о том, что в ряде случаев даже в ПО небольшой сложности, спроектированных подготовленными специалистами с использованием концепций обеспечения безопасности, при этом эксплуатируемого в течение длительного времени, могут содержаться ошибки, которые проявляются в редких случаях и их обнаружение затруднено в силу особенностей тестирования и эксплуатации. Ошибки такого рода могут быть выявлены с помощью различных подходов с разной вероятностью, но их обнаружение незначительно повышает уровень надежности и безопасности системы. Для существенных результатов по улучшению качества ПО необходимо использовать различные принципы и методы на более ранних этапах разработки, на таких как проектирование и формализация требований ко всему аппаратно-программному комплексу (АПК).

В настоящее время накоплен опыт верификации ПО СЖАТ с помощью формальных методов, с помощью которого были выявлены некоторые ошибки существующих АПК, которые проходили верификацию в лаборатории «Безопасность и ЭМС технических средств» Белорусского государственного университета транспорта. Анализу подвергались микроэлектронные устройства с ПО небольшой сложности (сотни и тысячи команд низкого уровня), отвечающие за управление ответственными технологическими процессами. На основании данного опыта были выявлены характерные особенности рассматриваемых типов устройств, найдены потенциальные источники ошибок,а также выработаны рекомендации, согласно которым можно улучшить качество ПО микроэлектронных СЖАТ на этапе проектирования всего АПК.

В качестве рекомендаций и подходов проектирования ПО АПК в докладе рассматриваются:

- разделение выхода работы системы в рабочий режим и выполнения основной функциональности;
- разделение получения входной информации, выполнения логики работы ПО и установки выходных значений;
- разработка ПО, имеющего конечное время выполнения алгоритма;
- необходимость задания контрольных точек ПО, выполнение которых необходимо на каждом витке цикла штатного режима;
- тактирование работы системы и её особенности.

УДК 625.151.3

МИКРОПРОЦЕССОРНАЯ ЦЕНТРАЛИЗАЦИЯ СТРЕЛОК И СИГНАЛОВ МПЦ-И

И. Г. ТИЛЬК, В. В. ЛЯНОЙ

Научно-производственный цент «Промэлектроника» г. Екатеринбург, Российская федерация

МПЦ-И предназначена для реконструкции действующих и строительства новых станций любого класса и со всеми видами поездной и маневровой работы. МПЦ-И обладает развитыми коммуникационными средствами и гибкой архитектурой, что позволяет интегрировать в МПЦ смежные системы железнодорожной автоматики (например, переездную сигнализацию, полуавтоматическую и автоматическую блокировки, линейные пункты ДЦ, центры радиоблокировки и т. п.), использовать современные сети передачи данных и создавать экономически оправданные конфигурации системы для станций различных классов.

Функционально МПЦ-И состоит из следующих элементов:

- управляющий контроллер централизации (УКЦ);
- телекоммуникационный шкаф ШТК;
- система гарантированного электропитания СГП-МС. Представляет собой линейку питающих установок мощностью от 10 до 30 кВА и временем резервирования от 10 мин до 8 ч;