

## МЕТОД ВЕРИФИКАЦИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ УСТРОЙСТВ УПРАВЛЕНИЯ ОТВЕТСТВЕННЫМИ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ

Б. В. СИВКО

*Белорусский государственный университет транспорта*

Современные микроэлектронные системы управления ответственными технологическими процессами связаны с обеспечением безопасности, и их некорректное поведение может привести к большому экономическому ущербу, а в ряде случаев – к гибели и потере здоровья людей. В связи с этим к ним предъявляются повышенные требования безопасности функционирования и разрабатываются методы и средства по их обеспечению.

В научно-исследовательской и испытательной лаборатории «Безопасность и ЭМС технических средств» Белорусского государственного университета проводилась верификация программного обеспечения ряда устройств по управлению технологическими процессами посредством доказательства правильности. На основании накопленного опыта была выявлена необходимость введения инварианта при анализе на безопасность систем такого рода.

В технологических процессах программное обеспечение крайне редко работает по линейному алгоритму. Чаще всего алгоритм представляет собой циклический процесс и предшествующий ему запуск системы. Запуск фактически производит инициализацию устройства (служит для установления начального инварианта), а во время циклической работы установленный инвариант должен сохраняться на каждом витке цикла.

При общем решении доказательства правильности требуется, чтобы необходимые условия в таких системах создавались на каждом шаге выполнения программы. В описываемом подходе доказательство правильности разбивается на две соответствующие части: то, что система выходит на нужный режим работы, и то, что этот режим работы при любых условиях сохраняется. При таком подходе во время верификации необходимо выделение контрольных точек алгоритма (а лучше всего – одной точки), в которой необходимо проверять истинность инварианта на каждом витке цикла. При этом желательно установление такой точки ещё на этапе проектирования.

Вышеописанные действия позволяют получить точное ограничение времени цикла посредством правил вывода. В результате, используя данную характеристику, можно вычислить вероятностные оценки критериев безопасности исходя из минимального времени обнаружения отказа и установленного периода контроля.

В докладе рассматриваются особенности и преимущества применения установления инварианта и контрольных точек в программном обеспечении устройств управления ответственными технологическими процессами.

УДК 656.256

## ПРИМЕНЕНИЕ ТЕХНОЛОГИИ СЧЕТА ОСЕЙ

И. Г. ТИЛЬК, В. В. ЛЯНОЙ, М. А. КРИВДА

*НПЦ «Промэлектроника»*

Одним из направлений совершенствования систем железнодорожной автоматики и телемеханики (СЖАТ) является создание многоуровневых систем, в которых технические характеристики устройств различного иерархического уровня должны быть оптимально согласованы между собой, а межсистемные интерфейсы – еще на этапе разработки. Таким примером может служить комплекс технических средств управления движением поездов с использованием Системы контроля свободности участков железнодорожного пути методом счета осей подвижного состава (ЭССО), разработанный научно-производственным центром «Промэлектроника».

Система ЭССО предназначена для контроля свободности участков пути любой сложности и конфигурации как на станциях, так и на перегонах, в том числе на участках с металлическими шпалами и стяжками, на целнометаллических мостах. ЭССО контролирует свободность участков приближения к переездам, блокучастков при автоматической блокировке, стрелочных секций и приемоотправочных путей на станциях, стрелочных и бесстрелочных участков в системах горочных автоматических централизаций, осуществляет контроль прибытия поезда в полном составе при полуавтоматической блокировке. ЭССО применяется как на участках с автономной тягой, так и на участках с электротягой любого рода тока.



Система ЭССО сертифицирована на соответствие российским требованиям к устойчивости и прочности в условиях воздействия климатических, механических факторов и электромагнитных помех, а также требованиям безопасности, которые соответствуют требованиям CENELEC уровня SIL4. Применяемые в системе ЭССО технологии и алгоритмы защищены патентами РФ.

С 1995 г. по настоящее время эксплуатируется более 10 000 счетных пунктов системы ЭССО на всех железных дорогах сети "ОАО РЖД" и на подъездных путях крупнейших промышленных предприятий РФ и ближнего зарубежья.

Технология счета осей используется:

- при полуавтоматической блокировке (ПАБ) – в качестве устройств контроля прибытия поезда в полном составе, что позволит автоматически формировать блок-сигнал прибытия и включить участки, оборудованные ПАБ, в ДЦ;

- при ПАБ с организацией АБП для увеличения пропускной способности участка – в качестве устройств контроля состояния участков между станциями и автоматическим блок постом;

- на переездах – для контроля участков извещения, что позволит устанавливать переездные сигнализации поверх любых систем путевой блокировки без привязки к границам блок-участков, тем самым оперативно менять длину участков извещения, т. е. время извещения при изменении предельных скоростей движения по участку;

- при автоматической блокировке (АБ) – для контроля состояния блок-участков, расположенных на мостовых мостах, в тоннелях и на загрязненных участках;

- на станциях – в качестве основного средства контроля второстепенных путей и стрелочных секций, а также маневровых зон, где не применяется АЛС с использованием рельсовой линии;

- на станциях – в качестве устройств резервирования кодируемых рельсовых цепей (РЦ) главных путей и стрелочных секций с целью повышения надежности работы РЦ на главных направлениях;

- на сортировочных горках – для контроля состояния разветвленных и не разветвленных участков с совмещением функции контроля проследования длиннобазных вагонов;

- на сортировочных горках – в качестве устройств контроля заполнения подгорочных путей.

УДК 656.259.1

## ДОКАЗАТЕЛЬСТВО БЕЗОПАСНОСТИ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ МИКРОПРОЦЕССОРНОЙ ЦЕНТРАЛИЗАЦИИ «ПУТЬ»

*С. Н. ХАРЛАП, А. В. ЛОГВИНЕНКО*

*Белорусский государственный университет транспорта*

Обязательным этапом разработки и внедрения современных микроэлектронных и компьютерных систем железнодорожной автоматики и телемеханики является доказательство безопасности их функционирования. Доказательство представляет собой специальный документ, в котором разработчик подтверждает соответствие основных показателей системы требованиям к надежности и безопасности функционирования. При этом используются различные методы: экспертиза, имитационное моделирование и испытания.

Разработанная в БелГУТе система микропроцессорной централизации стрелок и сигналов (МПЦ) «Путь» представляет собой комплекс устройств, обеспечивающих установку, замыкание, размыкание маршрутов на станции и проверку выполнения требуемых взаимозависимостей. Она должна обеспечивать безопасность движения поездов и надежную работу системы в течение всего срока эксплуатации.

Структура системы строится по иерархическому принципу с выделением трех основных уровней иерархии. *Верхний уровень* включает в себя автоматизированные рабочие места дежурного по станции (АРМ ДСП) и электромеканика СЦБ (АРМ ШН), средства организации передачи информации между элементами верхнего и среднего уровней ПРЦ посредством локальной сети Ethernet (локальная сеть верхнего уровня), средства организации передачи информации между ПРЦ и другими информационными системами (сервер ДЦ).

*Средний уровень* (уровень реализации логических зависимостей) состоит из двух резервированных двуканальных ядра (сервера) централизации, каждое из которых включает в себя два промышленных компьютера с технологическим прикладным программным обеспечением для данной станции, реализующих функции центральных зависимостей и блокировок ЭЦ.

*Нижний уровень* включает в себя блоки телеуправления ТУ8Б и телесигнализации ТС16Б, предназначенные для безопасного включения и контроля состояния исполнительных реле, средства организации передачи информации между элементами нижнего и среднего уровней ПРЦ посредством локальной сети RS-485 (локальная сеть нижнего уровня), релейные схемы увязки с использованием реле I класса надежности.