

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 электромеханика 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 двухканальных 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.

Система построена таким образом, что основные функции по обеспечению безопасности возлагаются на средний и нижний уровни системы, что позволяет расширять ее возможности путем подключения новых информационных подсистем или независимых систем без проведения дополнительных испытаний на безопасность функционирования. Таким образом осуществляется подключение системы поддержки принятия решений (СППР), съем и передача информации в систему ДЦ «Неман».

Безопасность технических средств ядра системы обеспечивается двухканальной обработкой информации, независимостью дублированных частей каналов, регулярным сравнением всех релевантных по безопасности данных, обнаружением неисправностей за короткий промежуток времени, что позволяет переключиться на резерв, не нарушая условий безопасности, специальным регламентом восстановления системы после перехода на резерв, специальными мерами по обнаружению недетектированных (не проявляющихся) неисправностей, тестированием аппаратных средств в каждом цикле программного обеспечения.

Безопасность программного обеспечения обеспечивается диверсифицированным программным обеспечением каждого канала ядра, постоянным обновлением (отдельно в каждом канале) и периодической проверкой целостности наборов данных, программной синхронизацией алгоритмов, хранением программных данных таким образом, что искажение любого бита или байта при адресации не приводит к наложению одних данных на другие.

Безопасность подключения устройств сопряжения с объектами (локальная сеть нижнего уровня) обеспечивается использованием отдельных физических каналов для подключения блоков УСО к ядрам МПЦ, привязкой блока к колодке и невозможностью передачи информации на блок ТУ-ТС, подключённый к другой колодке.

Безопасность устройств согласования с объектами (блоков ТУ-ТС) обеспечивается параллельной обработкой информации в двух каналах, постоянным программным сравнением идентичности работы каналов, ограничением по времени актуальности команд, использованием безопасных схем для формирования управляющего воздействия и ввода информации.

Безопасность релейных схем увязки подтверждается использованием специальных железнодорожных реле I класса надежности, экспертизой схемных решений, проведенной специалистами Службы Ш и КТЦ Белорусской железной дороги.

Выполненные расчеты показателей надежности и безопасности подтвердили их соответствие установленным нормам: коэффициент готовности системы составил 0,9999998, а интенсивность опасных отказов –  $10^{-13}$  1/ч.

Система соответствует всем требованиям технического задания, прошла полный цикл приемочных испытаний, что подтверждено соответствующими протоколами. В мае 2007 г. система «ИПуть» введена в опытную эксплуатацию на станции Ипуть Гомельского отделения Белорусской железной дороги. При этом в качестве резерва была сохранена существующая релейная система ЭЦ.

Результаты опытной эксплуатации подтвердили высокую надежность и безопасность системы. За время опытной эксплуатации не было зафиксировано ни одного опасного отказа системы, а также отказов, вызвавших выключение системы и переключение на резервную релейную систему ЭЦ. В настоящее время выполняются работы по демонтажу резервной релейной системы ЭЦ. При дальнейшем система МПЦ «ИПуть» будет проектироваться с полной заменой существующих релейных систем ЭЦ.

УДК 519.21

## ОБ ОДНОМ КЛАССЕ СЛУЧАЙНЫХ ЯВЛЕНИЙ

*Д. Н. ШЕВЧЕНКО*

*Белорусский государственный университет транспорта*

Анализ дерева отказов (АДО) один из распространенных методов моделирования надежности технических систем и технологических процессов на стадии проектирования. Он состоит в построении и анализе логико-вероятностной модели причинно-следственных связей отказов системы с отказами его элементов, другими событиями и воздействиями. Традиционно АДО применяется для качественного анализа надежности восстанавливаемых систем с независимыми отказами элементов, в некоторых случаях – для количественного анализа с определением вероятности отказа системы.

Вместе с тем возможно использование АДО для определения показателей надежности систем с восстанавливаемыми элементами; а также с учетом: последовательности отказов (актуальным при анализе безопасности функционирования систем); зависимости между отказами (и другими событиями); частичных и множественных отказов. Для этого необходимо рассмотрение случайных величин времени до наступления каждого из базовых, промежуточных и результирующего события дерева отказов. Такой подход, кроме прочего, позволит определять среднюю и гамма-процентную наработку системы до отказа и другие показатели надежности. В частном случае, задаваясь некоторой наработкой, можно прийти к традиционному подходу определения вероятности отказа.