УДК 656.2.08

КОНЦЕПЦИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ МПЦ СТАНЦИИ ИПУТЬ

А. В. ЛОГВИНЕНКО

Белорусский государственный университет транспорта

Построение современных микропроцессорных систем ЖАТ требует нового, принципиально отличного от релейных систем, подхода.

Существует несколько подходов в проектировании безопасных систем. Наиболее распространенный и известный в мировой практике подход основан на использовании мажоритарного принципа два из трёх. Он позволяет обеспечить режим одновременного штатного функционирования основного и резервных каналов, исключает применение специальных коммутационных узлов, устраняющих взаимное влияние основного и резервных каналов друг на друга. При этом отказ основного или резервного канала не влияет на работу оставшихся исправных элементов. Однако эксплуатационная готовность, безопасность таких систем ниже, чем применяемый в современных системах железнодорожной автоматике принцип два из двух. На данном принципе построена концепция безопасности МПЦ Ипуть.

МПЦ имеет следующую структуру: ядро МПЦ состоит из 4 промышленных компьютеров; компьютеры сгруппированы по парам в 2 комплекта – основной и резервный (представлено на рисунке 1).

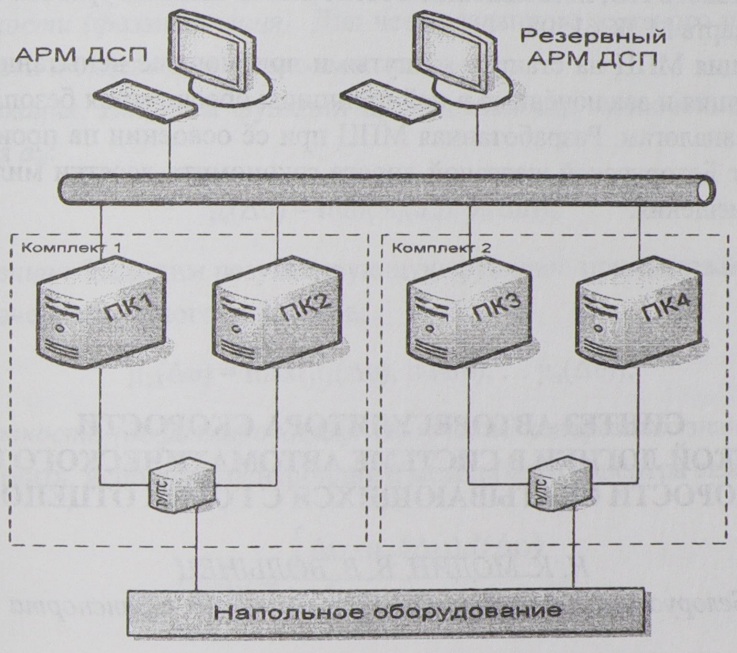

Рисунок 1 – Структурная схема подключения ядра МПЦ

Второй комплект находится в горячем резерве и повторяет все функции основного комплекта. После выхода из строя основного комплекта резервный автоматически начинает выполнять операции управления. Такая схема позволяет повысить надёжность и эксплуатационную готовность работы системы. В каждом комплекте используются два компьютера, контролирующих работу друг друга. При некорректной работе одного из них второй осуществляет переключение на резерв, с отключением отказавшего комплекта.

Обеспечение заданного уровня безопасности основывается на следующих принципах: дублированные части являются независимыми; все релевантные данные по безопасности регулярно сравниваются; предполагаемые неисправности определяются в течение короткого промежутка времени, позволяющего переключиться на резерв, не нарушая безопасности; определен регламент восстановления системы после перехода на резерв или при запуске остановленной части оборудования системы; определены меры для обнаружения недетектированных (не проявляющихся) неисправностей; в каждом цикле программное обеспечение проводит тестирование аппаратных средств (таких,

как регистры общего назначения и память); хранение программных данных реализовано таким образом что искажение любого бита или байта при адресации не приводит к наложению одних данных на другие.

Неодновременное проявление отказа позволяет обнаружить одиночный отказ до появления второго, это достигается за счёт диверсификации ПО ядер двух параллельных каналов. Программы ядра одного и второго каналов скомпилированы разными компиляторами. Внутренние циклы выполнения всех алгоритмов различны, что создаёт диверситет при выполнении одинаковых по внешним проявлениям алгоритмов СЦБ.

Для минимизации влияния структуры микропроцессора основные алгоритмические места программы ядра МПЦ написаны в ассемблерном коде, что транслируются в тривиальный байт-код, позволяющий свести выполнение алгоритма МПЦ к тривиальным логическим операциям AND, OR, EQU (и, или, равенство) и практически исключить операции условного перехода, в которых отказ одного бита приводит к необнаружимому неправильному функционированию.

Целостность и корректность передачи проверяется контрольной суммой и маркером владельца.

Защита информации внутри ядра МПЦ осуществляется следующим образом: все бинарные данные закодированы 32-битным словом с кодовым расстоянием не менее 16. При выполнении действий над ними, если результат не является верным, происходит выставление ошибки. Все адреса данных выровнены таким образом, что имеют кодовое расстояние не менее 4 и не имеют в себе более 8 подряд стоящих 0 или 1, в младшей, значащей части адреса, данные адресные пространства формируются различным образом для всех четырёх ядер каналов МПЦ.

Таким образом, в разработанной МПЦ «Ипуть» реализованы все современные методы как в аппаратной реализации, так и в ПО, позволяющие обеспечивать высший уровень SIL4 по требованиям международного стандарта МЭК 61508.

Опытная эксплуатация МПЦ на станции «Ипуть» и приёмочные испытания свидетельствуют о том, что данная концепция и заключённые в ней принципы обеспечения безопасности соответствуют лучшим западным аналогам. Разработанная МПЦ при её освоении на производстве и широком её внедрении позволит Белорусской железной дороге сэкономить десятки миллионов долларов по программе импортозамещения.

УДК 656.222.3: 656.21

СИНТЕЗ АВТОРЕГУЛЯТОРА СКОРОСТИ НА ОСНОВЕ НЕЧЕТКОЙ ЛОГИКИ В СИСТЕМЕ АВТОМАТИЧЕСКОГО РЕГУЛИРОВАНИЯ СКОРОСТИ СКАТЫВАЮЩИХСЯ С ГОРКИ ОТЦЕПОВ

Н. К. МОДИН, В. В. ВОЛЫНЕЦ
Белорусский государственный университет транспорта

Комплекс автоматического регулирования скорости (АРС) осуществляет интервальное и прицельное регулирование скорости скатывающихся вагонов на сортировочной горке, используя в качестве исполнительных органов вагонные замедлители. Недостатки алгоритмов функционирования существующих систем АРС, а также невозможность получения достоверной информации об объекте управления являются основными причинами опасных ситуаций, приводящих к нарушению безопасности функционирования комплекса АРС.

При необходимости реализовать заданную скорость выхода $\upsilon_з$ оттормаживание замедлителей должно начинаться в момент, когда отцеп имеет скорость $\upsilon_{от} = \upsilon_з + \Delta\upsilon$, где $\Delta\upsilon$ – опережение скорости оттормаживания. Упреждение по скорости при оттормаживании определяют с учетом инерционности Δt горочных замедлителей

$$\Delta\upsilon = a_{зi}\,\Delta t, \tag{1}$$

где $a_{зi}$ – интенсивность торможения.

Для расчета фактической величины $a_ф$ системы управления требуется определить функцию изменения интенсивности торможения $a_з(t)$ на временном интервале $[t_1;\ t_1 + \Delta t]$, причем значение $a_ф$