УДК 656.2.08

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 цельнометаллических мостах. ЭССО контролирует свободность участков приближения к переездам, блок-участков 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.