УДК 621.3.019.3

Ар.А. МУХА[*]

ПРАКТИЧЕСКИЕ АСПЕКТЫ ГАРАНТОСПОСОБНОСТИ КОНТРОЛЬНО-ИНФОРМАЦИОННОЙ СИСТЕМЫ ДЛЯ ЖЕЛЕЗНОДОРОЖНЫХ ПЕРЕЕЗДОВ «БЛАГОВЕСТ»

[*]Институт проблем математических машин и систем НАН Украины, г. Киев, Украина

Анотація. *У даній статті розглянуті питання інжинірингу гарантоздатних комп'ютерних систем. Проведено аналіз технічних засобів і рішень з реалізації атрибутів гарантоздатності. Як приклад, було розглянуто проблему безпечного перетину залізничних переїздів, яка в даний час є особливо актуальною для всіх промислово розвинених країн у зв'язку з ростом інтенсивності і швидкості руху поїздів. Це пов'язано з тим, що сучасні системи автоматичної переїзної сигналізації і автоматичних шлагбаумів мають ряд ідеологічних і технічних недоліків, які не дозволяють забезпечити високий рівень безпеки руху автотранспорту на переїздах. Базою для прикладу стала контрольно-інформаційна система для залізничних переїздів серії «Благовіст». Система «Благовіст» передбачає підвищення безпеки руху автотранспорту через переїзди за рахунок підвищення інформованості учасників руху про поїзну ситуацію на переїзді і його ділянках наближення за допомогою впровадження сучасних інформаційних технологій. У статті детально описуються апаратні і технічні рішення, які були впроваджені при розробці системи для залізничних переїздів. Продемонстровано, як у процесі розробки контрольно-інформаційної системи на базі платформи відмовостійкості реалізовувалися основні вимоги до гарантоздатних комп'ютерних систем. Згідно з прикладом описаної системи, проводиться обґрунтування стратегії реалізації часткової відмовостійкості, відмовобезпеки. У відповідності зі стратегією відмовобезпеки розглянуті технічні, програмні засоби та алгоритм роботи системи. У статті наводиться атрибутивна модель гарантоздатності комп'ютерних систем. Згідно з наведеною моделлю, розглянуті основні методи, завдяки впровадженню яких стало можливим підвищення рівня відповідних атрибутів.*
Ключові слова: *гарантоздатність, атрибутивна модель, відмовобезпека.*

Аннотация. *В данной статье рассмотрены вопросы инжиниринга гарантоспособных компьютерных систем. Проведен анализ технических средств и решений по реализации атрибутов гарантоспособности. В качестве примера была рассмотрена проблема безопасного пересечения железнодорожных переездов, которая в настоящее время является особенно актуальной для всех промышленно развитых стран в связи с ростом интенсивности и скорости движения поездов. Это связано с тем, что современные системы автоматической переездной сигнализации и автоматических шлагбаумов обладают рядом идеологических и технических недостатков, которые не позволяют обеспечить высокий уровень безопасности движения автотранспорта на переездах. Базой для примера стала контрольно-информационная система для железнодорожных переездов серии «Благовест». Система «Благовест» предусматривает повышение безопасности движения автотранспорта через переезды за счет повышения информированности участников движения о поездной ситуации на переезде и его участках приближения при помощи внедрения современных информационных технологий. В статье детально описываются аппаратные и технические решения, которые были внедрены при разработке системы для железнодорожных переездов. Продемонстрировано, как в процессе разработки контрольно-информационной системы на базе платформы отказоустойчивости реализовывались основные требования к гарантоспособным компьютерным системам. Согласно примеру описанной системы, производится обоснование стратегии реализации частичной отказоустойчивости, отказобезопасности. В соответствии со стратегией отказобезопасности рассмотрены технические, программные средства и алгоритм работы системы. В статье приводится атрибутивная модель гарантоспособности компьютерных систем. Согласно приведенной модели, рассмотрены основные методы, благодаря внедрению которых стало возможным повышение уровня соответствующих атрибутов.*
Ключевые слова: *гарантоспособность, атрибутивная модель, отказобезопасность.*

ISSN 1028-9763. Математичні машини і системи, 2018, № 4

Abstract. *The paper considers the questions of engineering of dependable computer systems. The analysis of technical equipment and solutions on the implementation of the attributes of the dependability was carried out. As an example, the problem of the safe crossing of railway crossings was considered, which is now particularly relevant for all industrialized countries in connection with the increase in the intensity and speed of train traffic. This is due to the fact that modern systems of automatic crossing signaling and automatic barriers have a number of ideological and technical deficiencies that do not allow ensuring a high level of traffic safety for crossings. The basis for this example was the control and information system for railway crossings of the "Blagovist" series. The "Blagovist" system provides for increasing traffic safety through crossings, by raising the awareness of traffic participants about the train situation at the crossing and its approaching areas by introducing modern information technologies. The paper describes in details the hardware and technical solutions that were introduced under the development of the system for railway crossings. It was demonstrated both during the development of the control and information system, based on the fault tolerance platform, the basic requirements for secure computer systems were implemented. According to the example of the described system, the strategy of implementation of partial fault tolerance is substantiated, - fail-safety. In accordance with the fail-safety strategy, technical, software and algorithm of the system operation are considered. The paper provides an attributive model of the computer systems' reliability. According to the above model, the main methods are considered, thanks to the introduction of which it became possible to increase the level of the corresponding attributes.*
Keywords: *Dependability, attributive model, fail-safety.*

1. Введение

В настоящее время человеческое общество становится все более зависимым от высокого качества услуг, предоставляемых динамично развивающимися информационными технологиями (ИТ). По мере развития общества возрастают требования к услугам, предоставляемым ИТ. Очень важным аспектом в этом вопросе является уровень надежности, достоверности, готовности, целостности и безопасности сервисов и систем, базирующихся на ИТ. Это обусловлено тем, что недостаточный уровень надежности и безопасности компьютерных систем (КС) как средств, реализующих ИТ, приводит либо к значительным материальным потерям и снижению конкурентоспособности производств и продукции для бизнес – критических приложений, а для КС критического применения – к техногенным и экологическим катастрофам и человеческим жертвам. На сегодня основным средством гарантируемого оказания обслуживания, согласно выше перечисленным показателям системы, является гарантоспособность. Поэтому *целью* статьи является анализ методов обеспечения атрибутов гарантоспособности систем специального предназначения.

В качестве примера рассмотрим решение проблемы безопасного пересечения железнодорожных переездов, которая в настоящее время является особенно актуальной для всех промышленно развитых стран в связи с ростом интенсивности и скорости движения поездов. Пересечения автомобильных и железных дорог характеризуются не только экономическими потерями, связанными с простоями автотранспорта, а наиболее острой проблемой являются дорожно-транспортные происшествия на переездах, часто сопровождающиеся особо тяжкими последствиями и человеческими жертвами.

Анализ аварий на переездах показывает, что в настоящее время в 98% случаев они происходят по вине водителей. В год на каждом переезде в среднем фиксируется по восемь нарушений правил дорожного движения. Наиболее остро эта проблема существует на неохраняемых и необорудованных автоматикой переездах. Это связано с тем, что современные системы автоматической переездной сигнализации (АПС) и автоматических шлагбаумов (АШ) обладают рядом идеологических и технических недостатков, которые не позволяют обеспечить высокий уровень безопасности движения автотранспорта на переездах [1, 2].

2. Контрольно-информационные системы (КИС) для железнодорожных переездов

Решение рассматриваемой проблемы по повышению безопасности движения автотранспорта через переезды представляется возможным за счет повышения информированности участников движения о поездной ситуации на переезде и его участках приближения при помощи внедрения современных информационных технологий, обеспечивающих высокий уровень гарантоспособности – надежности, достоверности и безопасности [3].

В сложившейся ситуации решение вопроса повышения безопасности движения автотранспорта на переездах представляется возможным за счет повышения информированности участников движения о ситуации на контролируемом объекте (информационный подход) [4]. Основным достоинством такого подхода является то, что разрабатываемые КИС являются на порядок более дешевыми, чем традиционные АПС и АШ нового поколения. Они являются автономными, не требуют схемной увязки с действующими системами АПС, АШ и автоматической блокировки (АБ), могут устанавливаться независимо от их наличия и на них не распространяются требования по функциональной безопасности, предъявляемые к системам железнодорожной автоматики, связанным с обеспечением безопасности движения поездов.

К такому классу систем относятся КИС серии «Благовест», разработанные в ИПММС НАН Украины. Более подробно с системами серии «Благовест» можно ознакомиться в [5–7].

Коротко рассмотрим основные функции и техническую реализацию базовой версии «Благовест 1.0».

Повышение информированности водителей автотранспортных средств достигается за счет использования электронного светодиодного табло, на котором в реальном масштабе времени воспроизводится информация о:

- приближении подвижного состава (поезда, локомотива, дрезины и т.п.) к переезду;
- занятости подвижным составом участка приближения к переезду;
- направлении движения подвижного состава через переезд;
- скорости движения подвижного состава;
- оставшемся времени до прохождения подвижного состава через переезд;
- освобождении контрольного участка за переездом;
- дорожной ситуации на переезде в виде бегущей информационной строки.

Источником информации является микропроцессорный комплекс технических средств, реализующий особый алгоритм функционирования. Входящая информация о движении подвижного состава снимается с четырех путевых датчиков счета осей (по два на пути в каждом направлении движения), устанавливаемых непосредственно вблизи рельса. Каждый датчик имеет два чувствительных элемента, которые регистрируют прохождение реборды колеса подвижного состава над датчиком. Датчики расположены как на участках приближения к переезду (на расстоянии до 2,5 км), так и в самой близости к переезду, до и после него в каждом направлении движения. Связь с удаленными датчиками счетных пунктов осуществляется по беспроводному радиоканалу. С целью защиты КИС от импульсных помех по сети питания, вызванных грозовыми разрядами, удаленные счетные пункты системы имеют автономное электроснабжение от солнечных батарей. Кроме того, центральный пункт КИС, расположенный на переезде, снабжен резервным источником бесперебойного питания.

Так как данная КИС связана с безопасностью движения поездов, то проанализируем ее реализацию с позиции обеспечения требований по гарантоспособности.

3. Атрибутивная модель гарантоспособности компьютерных систем

В процессе разработки КИС, начиная с эскизного проектирования и формирования технического задания, на платформе отказоустойчивости реализовывались основные требования к гарантоспособным КС, сформулированные в виде атрибутов гарантоспособности, а именно:

• *безотказность* – свойство системы непрерывно сохранять работоспособное состояние в течение некоторого времени или наработки;

• *готовность* – способность системы выполнять необходимые функции при определенных условиях эксплуатации и технического обслуживания в заданный момент или фиксированный интервал времени при условиях обеспечения необходимыми внешними ресурсами;

• *достоверность* – вероятность того, что значение вычисляемого параметра, отражаемое информацией и/или управляющим воздействием, производимыми КС, отличается от истинного значения этого параметра в пределах требуемой точности;

• *живучесть* – свойство системы сохранять или восстанавливать способность выполнять основные функции в определенном объеме и на протяжении заданной наработки при изменении условий эксплуатации, структуры системы и (или) алгоритмов;

• *целостность* – свойство системы быть неизменной при функционировании в условиях случайных или преднамеренных искажений или разрушающих воздействий извне системы (внешним агентом);

• *конфиденциальность* – свойство системы обеспечивать защиту от несанкционированного использования информации или технического средства, от подмены информации или технического средства, от повреждения информации или технического средства изнутри системы (внутренним агентом);

• *обслуживаемость* – способность системы подлежать техническому обслуживанию, модификации и ремонту;

• *функциональная безопасност*ь – способность системы при наличии отказа не причинять опасных (катастрофических) воздействий на человека (пользователя) или окружающую среду его обитания.

Технические и программные средства и алгоритм работы системы разрабатывались в соответствии со стратегией отказобезопасности [8, 9], основанной на замене реализации дорогостоящей полной отказоустойчивости на реализацию частичной отказоустойчивости, названной отказобезопасностью, основанной на исключении опасных ситуаций по вине КИС как при исправном, так и при неисправном ее состоянии. При моделировании алгоритма системы [10] производился контроль работоспособности алгоритма КИС на недопущение опасных искажений информации на выходе системы при возникновении отказов в работе.

При анализе КИС на наличие опасных ситуаций, которые могут возникать на переезде, было установлено, что без введения дополнительной избыточности даже при полностью исправной аппаратуре вероятность их появления достаточно высока.

Сбой в работе КИС может привести к кратковременной ошибке в расчете остаточного времени до момента проследования подвижным составом переезда, но такая ситуация не является опасной, так как вследствие динамического режима работы она исправляется в следующем такте работы системы.

Отказ системы теоретически может привести к ошибочной оценке остаточного времени, вследствие чего может быть выдана ложная информация на электронное табло, причем выдача более продолжительного промежутка времени является более опасной, чем выдача укороченного. В связи с этим была принята парадигма построения гарантоспособной системы из негарантоспособных составных частей [11], при которой любой отказ системы следует считать опасным и решение проблемы безопасности необходимо решать в

рамках одноканальной КС алгоритмическими, программными и другими средствами (динамическим режимом, автоматическим контролем, самодиагностикой и д.р.).

Рассмотрим следующие понятия.

Опасное состояние (Hazardous State) – неработоспособное состояние системы, при котором значение хотя бы одного параметра, характеризующего способность выполнять заданные функции по обеспечению безопасности, не соответствует требованиям НТД и (или) КД. Например, постоянная выдача ложной информации об остаточном времени проследования подвижного состава через переезд.

Защитный отказ (Protective Failure) – событие, заключающееся в нарушении работоспособного состояния системы при сохранении защитного состояния. Например, сбой в радиосвязи, отказ путевого датчика, приводящий к отсутствию информации на электронном табло.

Опасный отказ (Hazardous Failure) – событие, заключающееся в нарушении работоспособного и защитного состояний системы, приводящее ее в опасное состояние.

В системе предусмотрен режим защитного состояния (Protective State), при котором табло либо не работает, либо на него выводится предупредительная информация, которая позволяет своевременно уведомить водителей автотранспорта об опасности. Выбранная структура системы и ее алгоритм функционирования позволяют осуществлять объективный контроль состояний системы и идентифицировать события в соответствии с их значимостью в отношении отказобезопасности.

4. Практическая реализация атрибутов гарантоспособности в системе «Благовест»

Безотказность

Атрибут безотказность обеспечивается использованием всего комплекса методов классической теории надежности, включая использование высоконадежных современных элементов (микропроцессоров, микросхем, полупроводниковых приборов и т.п.), структурных методов резервирования, методов информационной избыточности и помехозащищенного кодирования информации. Использование в системе виброзащищенных путевых датчиков нового образца с дублированным чувствительным элементом и возможностью контроля электрических цепей позволяет разрабатывать счетные пункты с высоким уровнем отказоустойчивости.

Готовность

Для обеспечения данного атрибута был предпринят ряд мер, а именно: в системе осуществляется непрерывный контроль цепей путевых датчиков, выполняется циклический опрос канала радиосвязи, производится контроль заряда батареи блока бесперебойного питания, что положительно сказывается на снижении времени восстановления системы и повышении ее коэффициента готовности.

Живучесть

Для обеспечения данного атрибута в системе предусмотрены следующие конструкционные решения:

• датчики системы выполнены в корпусах из ударопрочной пластмассы для защиты от механических повреждений при внешних воздействиях;

• аппаратура счетных пунктов и центрального пункта размещена в металлических шкафах для защиты от несанкционированного доступа и атмосферного влияния в случае непогоды и природных катаклизмов;

• выполнено дублирование путевых датчиков, которое позволяет продолжать работу системы при отказах их элементов;

•реализован алгоритм контроля неисправностей, при реализации которого отслеживаются отказы датчиков, модулей связи, источника бесперебойного питания;

• применены гальванические развязки оборудования для повышения стойкости системы к скачкам напряжений по цепям питания при нестандартных режимах работы.

Достоверность

С целью повышения уровня достоверности работы системы производится проверка и осуществляется контроль:

• алгоритма работы системы (система вычисляет решение по двум сценариям и принимает решение только при совпадении решений);

• вычисление скорости движения подвижного состава по двум источникам данных (сигналы с разных чувствительных элементов одного датчика и сигнал с разных датчиков, производится сравнение результата);

• определение направления движения подвижного состава (сигналы с разных чувствительных элементов одного датчика и сигнал с разных датчиков, производится сравнение результата).

В процессе работы системы осуществляется многократная передача радиосигнала от счетного пункта на центральный пункт. Для повышения достоверности работы системы осуществляется счет осей проходящего подвижного состава на входном и выходном датчиках. При несовпадении результатов подсчета система переводится в защитное состояние с выдачей на табло предупредительной информации.

Обслуживаемость

Для обеспечения необходимого уровня обслуживаемости системы используются приведенные ниже технические решения. Каждый блок системы снабжен световой индикацией, а именно:

• блок бесперебойного питания – индикатор включения и работы в разных режимах;

• блок заряда аккумулятора и режима питания – световая индикация работы в разных режимах (зарядка, ошибка зарядки, аккумулятор заряжен);

• вычислительный блок счетного пункта – световая индикация работы в разных режимах, связь с датчиками, срабатывание датчиков, наличие питания;

• радиопередатчики – световая индикация включения и работы в разных режимах, индикатор наличия связи между устройствами;

• информационное табло – вывод технической информации в виде кодов ошибок.

Система имеет блочную конструкцию, все блоки соединены разъемами и могут быть заменены в случае выхода из строя.

Целостность

Для обеспечения необходимого уровня целостности системы используются следующие технические решения:

• при передаче сигналов по проводному каналу от центрального пункта к информационным табло используется специально разработанный протокол, который включает в себя проверку контрольных сумм посылки.

• при передаче по радиоканалу используется специальный внутренний протокол связи, который учитывает механизмы проверки целостности сообщения (Integrity) и проверки его подлинности (Authentication).

Конфиденциальность

Система данного типа является режимной, то есть ручное управление и контроль в ней могут осуществляться электромехаником только при открытии замка на шкафу с оборудованием и подключении специального сервисного компьютера. Также, поскольку в системе

используется радиосвязь, для обеспечения атрибута конфиденциальность предусмотрено шифрование передаваемых данных в радиоканале с помощью алгоритма AES с длиной ключа 128 бит.

Функциональная безопасность

Для обеспечения атрибута функциональная безопасность в системе был произведен анализ возможных неисправностей и реакций системы на них и приняты соответствующие меры при проектировании. Например, при отказах путевых датчиков отслеживаются такие ситуации: отсутствие сигнала, слабый сигнал, ложный сигнал.

Поскольку в системе для идентификации поезда используется дублированный каскад двухканальных ПД, это решение позволяет, в случае отказа одного датчика из пары либо одного из каналов каждого датчика, переходить в режим, при котором система остается работоспособной. В этом случае расчет скорости при движении поезда по направлению отказавшего датчика не производится, а значение скорости на информационном табло маскируется максимально допустимым значением скорости для поездов, курсирующих на данном железнодорожном участке. В системе выделены состояния, при которых производится ее переход в безопасное состояние с уведомлением участников движения информацией на табло.

5. Заключение

Анализ реализации атрибутов гарантоспособности показал, что при проектировании системы «Благовест» применен системный подход к инжинирингу компьютерных систем критического применения. Производя контроль реализации атрибутивной модели при проектировании и реализации компьютерных систем, становится возможным достижение необходимого уровня гарантоспособности. Контроль уровня гарантоспособности рекомендуется проводить на каждом этапе жизненного цикла разработки, начиная с выработки концепции системы и кончая этапом рабочего проектирования и производства. В дальнейшем, производя более подробную детализацию атрибутивной модели на метрики, представляется возможным определение конкретных количественных параметров гарантоспособности, которые дадут возможность оценить количественный уровень гарантоспособности разрабатываемой КС и выбрать наиболее предпочтительный вариант реализации.

СПИСОК ИСТОЧНИКОВ

1. Поздняков В.А., Тюпкин Ю.А. Безопасность на железнодорожных переездах. URL: http://www.css-rzd.ru/zdm/03-2000/00039.htm.
2. Соловьев А.Л., Чеблаков В.А., Петров А.Ф. Микропроцессорная переездная сигнализация с аппаратурой счета осей. *Автоматика, связь, информатика*. 2008. № 6. С. 2–10.
3. Федухин А.В., Сеспедес Гарсия Н.В. Атрибуты и метрики гарантоспособных компьютерных систем. *Математичні машини і системи*. 2013. № 2. С. 195–201.
4. Федухин А.В., Муха Ар.А. Информационный подход к повышению безопасности движения по железнодорожным переездам. *Математичні машини і системи*. 2015. № 4. С. 145–151.
5. Федухин А.В., Муха Ар.А. Беспроводные микропроцессорные системы для железнодорожных переездов серии «Благовест». *Приборы и системы. Управление, контроль, диагностика*. 2015. № 2. С. 1–5.
6. Федухин А.В., Муха Ар.А. Радиомикропроцессорные информационные системы для железнодорожных переездов серии «Благовест». *Математичні машини і системи*. 2014. № 2. С. 137–141.
7. Федухин А.В., Муха Ар.А. Беспроводные микропроцессорные системы для железнодорожных переездов серии «Благовест». *Молодий вчений*. 2014. № 11. С. 16–19.
8. Федухин А.В., Муха Ар.А. Стратегия отказобезопасности как альтернатива полной отказоустойчивости при проектировании гарантоспособных компьютерных систем. Ч. 1. *Молодий вчений*. 2016. № 8 (35). С. 169–173.

9. Федухин А.В., Муха Ар.А. Стратегия отказобезопасности как альтернатива полной отказоустойчивости при проектировании гарантоспособных компьютерных систем. Ч. 2. *Молодий вчений*. 2016. № 10 (37). С. 23–27.
10. Муха Ар.А. Моделирование и разработка алгоритма работы АПС-РМПГ средствами пакета Matlab Similink+Statefolw. *Молодий вчений*. 2014. № 5 (8). С. 10–14.
11. Харченко В.С. Эволюция Фон-Неймановской парадигмы: гарантоспособные системы из негарантоспособных компонент. *Системи обробки інформації*. 2004. Вип. 8 (36). С. 11–19.

Стаття надійшла до редакції 17.10.2018