Надежность и безопасность железнодорожной автоматики и телемеханики

Шалягин Д.В.,

Шубинский И.Б.

Появление в последние годы на сети российских железных дорогах нового поколения средств автоматики и телемеханики (ЖАТ), основанного на микроэлектронной элементной базе и вычислительной технике, цифровых сетях передачи информации, поставило и новые требования к определению их надежностных характеристик и показателей безопасности.

Более надежная элементная база, структурное и элементное резервирование, введение параметрической и информационной избыточности, применение средств диагностики и другие меры приводят к тому, что вероятность отказов в новых устройствах ЖАТ меньше, чем в традиционных релейных устройствах.

Повышая надежность элементов, вводя избыточность в аппаратуру, применяя взаимозаменяемость и восстановление, мы обеспечиваем безотказность системы, т.е. ее способность функционировать без отказов в течение определенного времени, и отказоустойчивость аппаратуры, т.е. ее способность правильно выполнять все или некоторые основные свои функции даже при наличии отказов ее элементов (до определенного их количества).

Однако именно для сложных систем (а современные средства ЖАТ являются сложными системами) характерна возможность и сложных многократных комбинаций событий, вероятность каждого из которых мала, а в сумме таких событий, казалось бы, невероятных, набирается немало. Работа таких систем зависит подчас от деятельности нескольких операторов, включая обслуживающий персонал, от их квалификации и мастерства. При дальнейшем внедрении современной техники вопросы ее надежности и безопасности, дисциплины и организованности персонала приобретают первостепенное значение.

Повышение отказоустойчивости системы необходимо, но оно не обеспечивает безопасность. Даже специально создаваемые «безопасные» системы, ориентированные на простой перебор возможных опасных ситуаций, не могут гарантировать защиты системы от произвольных комбинаций отказов, нарушений правил эксплуатации, запредельных воздействий внешней среды, человеческого фактора и иных неблагоприятных воздействий.

Теория надежности развивается уже несколько десятков лет, изданы сотни книг, учебников и статей, созданы научные школы и защищено множество диссертаций. Однако успехи в области теории безопасности несравненно скромнее и менее известны, хотя крупнейшие аварии и катастрофы в мире, в том числе на железных дорогах, выявили существенную роль и значимость развития теории безопасности.

Недостаточный уровень надежности изделий и систем приводит к большим экономическим потерям. Но могут быть такие последствия ненадежности, которые нельзя или сложно оценить экономическими показателями. Безопасность функционирования – это комплексная проблема,

включающая кроме структурно-технических, также вопросы деятельности человека, его дисциплинированности, организации труда, обучения персонала.

Несмотря на солидный возраст теории надежности и наличие серии международных и отечественных стандартов, напомним все же основные ее понятия.

Под надежностью первоначально понимали только безотказность. Затем в нее включили понятия ремонтопригодности, долговечности и сохраняемости, а некоторые авторы – даже живучесть, безопасность и устойчивость. Такое расширенное понимание надежности в научном отношении сомнительно, а в практическом смысле приносит только вред.

Проблема обеспечения надежности аппаратно-программных комплексов (АПК) ЖАТ, как и любой другой системы, использующей АПК, состоит в обеспечении процесса их функционирования в течение заданного времени при воздействии внутренних возмущающих факторов: отказов и сбоев аппаратных средств, ошибок в алгоритмическом и программном обеспечении, искажений входной информации, ошибок операторов внутри системы (человеческий фактор). Эти факторы уменьшают время безотказной работы АПК, снижают уровень его готовности к выполнению предусмотренных задач и, как следствие, ухудшают показатели его технического использования. Внешняя среда также оказывает определенное негативное влияние на уровень надежности АПК ЖАТ. Поэтому на всех этапах жизненного цикла системы это влияние учитывается и должно компенсироваться.

Надежность управляющих систем принято оценивать рядом показателей, среди которых различают единичные и комплексные. К основным единичным показателям относятся:

- интенсивность отказов технических средств;
- вероятность безотказной работы исправного в момент включения устройства в течение определенного времени;
- среднее время наработки устройства на отказ;
- среднее время обнаружения отказа и среднее время восстановления отказавшего устройства (ремонтопригодность устройства), зависящие от интенсивности обнаружения отказов в устройстве и интенсивности восстановления отказавшего устройства.

К комплексным показателям надежности относят коэффициенты готовности, оперативной готовности и технического использования устройства или системы, показывающие вероятности ее исправного состояния, возможности решения конкретной оперативной задачи за заданное время и того, что в данный момент времени система не ремонтируется и не обслуживается. Другими словами, показатели надежности определяют вероятность того, что в данный момент времени устройство или система исправны и могут выполнять возложенные на них задачи.

Теория безопасности должна изучать комплекс вопросов, связанных с определением возможности возникновения аварий и катастроф в результате отказов технических средств, действий персонала или недопустимых воздействий внешней среды и с разработкой методов защиты от таких

событий и борьбы с их последствиями. При этом должно рассматриваться не только поведение системы в экстремальных ситуациях, но и категории угроз безопасности (в том числе военные, экологические, социальные), методы снижения негативных последствий от катастроф, правовое и экологическое регулирование безопасности и другие вопросы, так или иначе связанные с безопасностью перевозочного процесса. Исходя из сказанного, можно сформулировать понятие безопасности движения поездов, как антропотехническое понятие, определяющее совокупность свойств технических и технологических средств железнодорожного транспорта, окружающей среды и целенаправленной деятельности человека, обеспечивающих исключение (предупреждение) ситуаций, опасных для движения поездов, постоянных сооружений, окружающей среды и людей.

При возникновении отказов, связанных с нарушением безопасности движения поездов, часто возникает вопрос, кто виноват в их возникновении. Для некоторых причин отказов можно ответить на этот вопрос (см. табл. 1).

Последняя причина допустима лишь в том случае, если последствия отказа не привели к нарушению безопасности и могут быть устранены при проведении планового или непланового ремонта, т.е. при обслуживании устройств. Если же отказ может привести к тяжелым последствиям, и тем более стать причиной аварийной ситуации, то он является недопустимым и возникает по вине разработчика. Поэтому при разработке системы и на стадии ее проектирования необходимо провести следующие исследования.

Таблица 1

Причина отказа	Кто виноват в возникновении отказа
1. Неправильный расчет ресурса изделия, неправильно установлены ТУ на параметры изделия	Разработчик
2. Нарушение ТУ при изготовлении и испытании изделия	Изготовитель
3. Нарушение режимов и условий эксплуатации, указанных в ТУ	Эксплуатационник
4. Допускаемая ТУ вероятность возникновения отказа	Никто

- Провести анализ возможности возникновения аварийной ситуации, рассмотреть и описать сценарии их развития, классифицировать возможные последствия аварий, установить вероятности получения каждой степени поражения.
- Установить перечень выходных параметров системы, которые претерпевают существенные изменения в процессе аварии. По

возможности выявить те показатели, изменение которых предшествует критическому состоянию и по изменению значения которых можно предотвратить (прогнозировать) возможность аварии.

- Установить потенциально опасные узлы и элементы системы, нарушение работоспособности которых может иметь недопустимые последствия.
- Установить предельно допустимые условия эксплуатации и режимы работы системы. Оценить возможную продолжительность работы системы в экстремальных условиях, в том числе при потере работоспособности ее отдельных узлов и элементов.
- Рассмотреть возможные действия пользователей системы и обслуживающего ее персонала и проработать способы защиты от их ошибок (как умышленных, так и неумышленных), которые могли бы привести к недопустимым последствиям.

Эти исследования должны проводиться при подготовке «Доказательства безопасности», которое является основой для разработки конструкции системы, ее структуры и схем отдельных узлов, алгоритмического и программного обеспечения, т.е. разработки безопасной системы, устойчивой к возникновению «нештатных» ситуаций.

Методы обеспечения безопасности весьма разнообразны, но могут быть сведены к двум основным принципам.

Первый принцип связан с введением избыточности в создаваемые элементы, узлы, устройства и системы. Избыточность может быть параметрической (введение в состав узла запаса прочности), схемной (введение в состав устройства так называемых безопасных логических элементов, компараторов, ключей и т.д.), структурной или аппаратной (дублирование, троирование и т.д. в устройстве или в системе аппаратных средств, функциональных узлов и элементов), программной (решение задачи двумя независимыми программными продуктами), функциональной (создание возможности решения одной и той же задачи путем реализации полной или упрощенной функции, но с меньшей точностью), информационной (кодирование информации внутри системы с последующим декодированием и проверкой ее безошибочности перед использованием), временной (увеличение времени восприятия или выдачи воздействия), комбинированной (при использовании нескольких из перечисленных методов). Таким образом, требования безопасности накладывают дополнительные условия на комплектующие изделия и материалы, на конструкцию, на схемные решения и структуру системы, на представление информации в ней и т.д.

В соответствии со *вторым принципом* обеспечение безопасности достигается применением средств, локализующих развитие неблагоприятных процессов, защищающих систему от выдачи неправильных воздействий, предупреждающих о возможном наступлении экстремальных ситуаций, управляющих функционированием объекта в критических случаях (парирующих развитие отказа и переводящих объекты управления в защитное состояние). Для этих целей используются контролирующие и диагностирующие устройства, которые оценивают значения выходных параметров системы и значения специальных диагностических признаков, а в необходимых случаях и окружающей среды (вибрации, температура,

электромагнитная обстановка и др.). Сравнение измеренных сигналов с их заданными значениями, обработка информации и принятие решения о необходимых действиях для предотвращения аварийной ситуации должны осуществляться устройствами, которые сами обладают высокой достоверностью, т.е., в данном случае, отвечающих требованиям безопасности.

Естественно, возможно и одновременное использование обоих методов реализации требований безопасности при построении одной системы.

Основным направлением всех работ и исследований в области безопасности является принцип исключения возможности появления потенциально опасной ситуации (или сведению вероятности появления этого события к минимально допустимой величине). Поэтому достижение безопасности функционирования устройств и систем управления движением поездов должно базироваться на следующих основополагающих принципах:

- обеспечение безопасного функционирования системы управления;
- обеспечение качественного изготовления устройств системы и ее программного обеспечения;
- принцип допущения худшего случая, при котором система даже при маловероятном сочетании поражающих факторов должна исключать появление потенциально опасной ситуации;
- организация непрерывного контроля функционирования устройств в процессе эксплуатации;
- осуществление непрерывного мониторинга состояния устройств системы методами диагностики.

Требования к средствам управления движением поездов с учетом безопасности должны заключаться в следующем:

- вероятность появления потенциально опасные ситуации, а тем более аварии, по вине самих технических средств должна быть минимальной, не выше заданной;
- при возникновении потенциально опасной ситуации система должна парировать ее (переходить в защитное состояние), а при возникновении аварии – обеспечивать минимальный материальный ущерб и отсутствие человеческих жертв.

Использование для целей управления движением поездов информационных ресурсов (систем передачи и обработки информации) в современных системах обусловило появление проблемы обеспечения информационной безопасности при функционировании таких систем, в том числе устройств автоматики и телемеханики. Основное внимание в теории и практике обеспечения информационной безопасности (это относится как к управляющим, так и к информационным системам) сосредоточено на их защите от несанкционированного доступа в целях сохранения конфиденциальности информации (недопущение хищений и несанкционированного использования), ее целостности (недопущение злоумышленных разрушений и искажений информационных массивов), доступности разрешенным пользователям. Для этого предусматриваются

организационные и технические средства разграничения доступа к системе, аутентификации и идентификации пользователей, антивирусной защиты, а также защиты от целенаправленной перегрузки трафика сетей передачи данных, криптографии, аудита и мониторинга состояния защищенности систем, их проверок на недекларированные возможности (наличие аппаратных и/или программных «закладок») и т.д. Для однозначного разделения понятий и требований информационной безопасности и безопасности движения поездов, обеспечиваемой устройствами и системами управления, для последней применяется новый термин – функциональная безопасность.

Проблемы функциональной безопасности систем ЖАТ рассматриваются в ряде международных стандартов [1 - 5], в соответствии с которыми к основным понятиям функциональной безопасности относятся следующие:

- система, связанная с безопасностью;
- функция безопасности и полнота безопасности;
- уровень полноты безопасности;
- состояния безопасности;
- отказы.

Система, связанная с безопасностью, обеспечивает выполнение функций безопасности, необходимых для достижения или поддержания безопасного состояния объекта управления, и предназначена для достижения необходимой полноты безопасности – самостоятельно или совместно с другими связанными с безопасностью средствами, как встроенными в систему, так и внешними по отношению к ней, в том числе средствами снижения риска. Необходимо отметить, что система, связанная с безопасностью, включает в себя не только аппаратные средства, но и программное обеспечение, кроме того, человек – оператор также может являться частью такой системы. При этом под средствами снижения риска понимаются специальные меры, предпринимаемые без использования систем, связанных с безопасностью.

Функция, реализуемая связанной с безопасностью системой, целью которой является обеспечение или поддержание безопасного состояния применительно к конкретному опасному состоянию называется *функцией безопасности*.

Полнота безопасности – это уровень удовлетворительного выполнения системой, связанной с безопасностью, требуемых функций безопасности при всех заданных условиях в течение заданного периода времени. Чем выше уровень полноты безопасности систем, связанных с безопасностью, тем меньше вероятность отказа этих систем при выполнении ими требуемых функций безопасности. При определении полноты безопасности учитываются все причины отказов, ведущих к опасному состоянию (отказы аппаратуры, программного обеспечения, электромагнитное влияние и др.), многие из них могут быть оценены количественными показателями, но для ряда факторов возможна лишь их качественная оценка.

Состояния безопасности включают исправное (выполняются все требования нормативно-технической документации), неисправное (не обеспечивается выполнение хотя бы одного требования нормативно-технической документации), работоспособное (выполняются все требования

нормативно-технической документации, характеризующие способность выполнять заданные функции), неработоспособное (значение хотя бы одного параметра, характеризующего способность выполнять заданные функции, не соответствует требованиям нормативно-технической документации), защитное (выполняются все предусмотренные функции безопасности, реализуемые, например, путем отключения от объекта управления), опасное (неработоспособное состояние, при котором не выполняется хотя бы одна функция безопасности), неопасное (работоспособное и защитное состояния).

Естественно, защитное состояние может быть только в системах, связанных с безопасностью.

Отказ – это событие, заключающееся в нарушении работоспособного состояния системы. Отказы в свою очередь могут быть защитными (при попадании системы в защитное состояние), опасными (при нарушении работоспособного или защитного состояний).

Особенно необходимо остановиться на понятии полноты безопасности. В стандарте IEC 61508 приводятся четыре уровня полноты безопасности (табл. 2).

Таблица 2

Уровень полноты безопасности	Интенсивность опасных отказов (1/час)
УПБ 4	$\geq 10^{-9}$ до $< 10^{-8}$
УПБ 3	$\geq 10^{-8}$ до $< 10^{-7}$
УПБ 2	$\geq 10^{-7}$ до $< 10^{-6}$
УПБ 1	$\geq 10^{-6}$ до $< 10^{-5}$

УПБ 1 достигается относительно легко при условии применения на всех стадиях разработки и производства требований стандартов качества.

УПБ 2 достигается не на много сложнее, чем предыдущий, однако для его обеспечения требуется большее число проверок и испытаний, что приводит к повышению стоимости системы.

Для достижения УПБ 3 требуются более существенные усилия и более высокая компетенция разработчиков, чем в случаях УПБ 1 и УПБ 2. Важными факторами являются стоимость и время разработки, выбор исполнителей становится ограниченным, так как не многие их них способны обеспечить этот уровень.

УПБ 4 требует проведения разработки «на грани искусства», включая применение «формальных методов» [7]. Стоимость проекта будет предельно большой и при создании потребуется исключительно высокая компетентность. В ряде случаев удается избегать применения УПБ 4, дополнительно используя уровни защиты.

Для систем, связанных с безопасностью, применяют несколько количественных показателей функциональной безопасности. Так, на железнодорожном транспорте распространены такие показатели, как

интенсивность опасных отказов, вероятность опасных отказов, вероятность безопасной работы за заданное время, средняя наработка до опасного отказа и некоторые другие. При этом рекомендуется определять эти параметры экспериментально, расчетным путем или с помощью моделирования. Однако необходимо отметить, что появление опасного отказа – редкое событие, и для определения его вероятностных параметров экспериментальными методами потребуется время, значительно превышающее время жизни исследуемого устройства. Кроме того, появление такого редкого события, как опасный отказ, нельзя описывать известными законами распределения случайных событий, поддающимися аналитическим исследованиям, а, следовательно, расчетные методы для получения всех перечисленных характеристик безопасности не могут быть адекватны фактическим параметрам устройства.

Математическое моделирование процессов появления опасных отказов является мощным инструментом исследования устройств и систем управления на соответствие требованиям безопасности, но для его реализации необходимо создание соответствующего математического описания объекта исследования – процесса появления опасных отказов, что не может быть в полной мере реализовано в силу высказанных выше причин.

Для создания сложных многоуровневых СЖАТ на микропроцессорных компонентах возникает необходимость в выработке комплексного подхода к рациональному использованию аналитических и экспериментальных способов и методов доказательства безопасности, объединения разнородной информации для получения достоверных оценок доказательства функциональной безопасности СЖАТ. С этой целью целесообразно сочетать результаты математического моделирования с ускоренными натурными испытаниями, с результатами экспертизы технической и конструкторской документации, испытаниями имитационных моделей программно - аппаратных средств, стендовыми испытаниями, а также с оценками безопасности по статистическим данным об отказах в процессе эксплуатации.

Использованная литература:

1. IEC 61508: 1-6. Functional safety of electrical / electronic / programmable electronic safety – related systems. 1998 – 2000. Функциональная безопасность электрических /электронных/ программируемых электронных систем безопасности.
2. CENELEC EN 50126: Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS). 1998. Применения на железнодорожном транспорте - Спецификация и демонстрация надежности, доступности,
3. CENELEC EN 50126-2: Railway Applications: Dependability for Guided Transport Systems. Part 2: Safety. 1999. Применения на железнодорожном транспорте - Согласованность для управляющих транспортных систем - часть 2. Безопасность.
4. CENELEC EN 50128: Railway Applications – Communications, signaling and processing systems - Software for Railway Control and Protection Systems. 2000. Применения на железнодорожном транспорте - Программное обеспечение для систем управления и обеспечения безопасности на железнодорожном транспорте.

5. CENELEC EN 50129: Railway Applications - Safety-related Electronic Systems for Signaling. 2000. Применения на железнодорожном транспорте - Электронные системы железнодорожного управления и защиты, связанные с безопасностью.
6. Смит Д., Симпсон К. Функциональная безопасность (Простое руководство по применению стандарта МЭК 61508 и связанных с ним стандартов) / Пер. с англ. под ред. проф. И.Б. Шубинского – М.: Изд. Дом «Технологии», 206 с., 2004.