УДК 621.38

ВЛИЯНИЕ ИНТЕЛЛЕКТУАЛИЗАЦИИ ФУНКЦИЙ МИКРОПРОЦЕССОРНОЙ ЦЕНТРАЛИЗАЦИИ НА ПОВЫШЕНИЕ БЕЗОПАСНОСТИ ДВИЖЕНИЯ ПОЕЗДОВ НА СТАНЦИИ

К. А. БОЧКОВ, А. Н. КОВРИГА, Д. В. ШЕВЧЕНКО
Белорусский государственный университет транспорта, г. Гомель

Интеллектуализация функций является преобладающей мировой тенденцией встраиваемых компьютерных систем управления, ответственных за технологические процессы. Микропроцессорные системы управления движением поездов являются стратегическими объектами и по классификации США относятся к критическим системам инфраструктуры, классификации Российской Федерации – к критическим системам информации, по классификации Республики Беларусь – к критически важным объектам информации.

Микропроцессорные централизации стрелок и сигналов (МПЦ) являются составной частью автоматизированных систем управления движением поездов на станции, в контуре управления которых находится дежурный по станции (ДСП). В штатном режиме функционирования МПЦ основные функции по обеспечению безопасности движения поездов обеспечиваются аппаратно-программным комплексом МПЦ. При возникновении нештатных ситуаций на время восстановления системы МПЦ часть функций по обеспечению безопасности движения поездов принимает на себя ДСП. В связи с этим представляет особый интерес анализ влияния интеллектуализации функций МПЦ в составе автоматизированных систем на повышение безопасности движения поездов на станциях.

Как и любые другие системы, построенные на современной элементной базе, МПЦ подвержены отказам, которые в зависимости от возможных последствий подразделяют:

– на опасные, нарушающие условия безопасности движения поездов на станции и создающие потенциальную опасность для жизни и здоровья людей при наличии неблагоприятной поездной ситуации на время опасного отказа и не парирования опасного отказа машинистом, ДСП, ШН;

– защитные, которые непосредственно не нарушают условия безопасности, т.к. переводят МПЦ в защитное состояние. Эти отказы должны обнаруживаться с заданной вероятностью на рабочих или тестовых воздействиях не позднее, чем в системе возникнет следующий отказ.

Отказы аппаратно-программного комплекса МПЦ, как правило, носят случайный характер, и идентифицировать их предотказное состояние практически не представляется возможным.

Безотказность современных систем МПЦ, определенная из принципа замещения рисков, должна быть по показателю интенсивности опасных отказов не ниже $1{,}8\times10^{-7}$ 1/ч (для крупных станций – $7{,}7\times10^{-9}$ 1/ч на одну централизованную стрелку). С целью увеличения коэффициента готовности при защитном отказе в некоторых МПЦ предусмотрен вспомогательный ручной режим управления, в котором проверка условий безопасности и принятие решений возлагаются исключительно на дежурного по станции.

Анализ крушений и браков в работе систем ЖАТ показывает, что в большинстве случаев события, приводящие к тяжелым последствиям, развиваются по следующему сценарию:

– вначале следует отказ технических средств ЖАТ, и как следствие, возникает нештатная ситуация, приводящая к полной или частичной потери функции по управлению и контролю над объектами дежурным по станции;

– затем основные функции по обеспечению безопасности движения поездов, на время устранения нештатной ситуации, принимает на себя ДСП.

Таким образом, в нештатных ситуациях на время восстановления системы МПЦ уровень обеспечения безопасности движения поездов на станции значительно снижается и на первый план выступает человеческий фактор. К чему это может приводить известно из многочисленных фактов аварий и крушений.

Предполагая поток отказов МПЦ простейшим, интенсивность аварий на железнодорожной станции (по причине отказов МПЦ) определяется выражением

$$\lambda_{а} = \lambda_{ао} + \lambda_{ан} = \lambda_{оо} P_{со} \left(1 - P_{п}\right) + \lambda_{но} P_{си} P_{од}, \qquad (1)$$

где λ_{ao} – интенсивность аварий по причине опасных отказов МПЦ; $\lambda_{ан}$ – интенсивность аварий по причине неопасных (защитных) отказов МПЦ; λ_{oo} – интенсивность опасных отказов ($\lambda_{oo} = 10^{-12}$–10^{-9} 1/ч, обеспечивается на этапе разработки системы); P_{co} – вероятность наличия неблагоприятной поездной ситуации в момент опасного отказа МПЦ; $P_{п}$ – вероятность парирования опасной технологической ситуации ДСП; $\lambda_{но}$ – интенсивность неопасных отказов (причем, $\lambda_{но} = 10^{-8}…10^{-4}$ 1/ч); $P_{сн}$ – вероятность наличия неблагоприятной поездной ситуации в момент неопасного отказа МПЦ; $P_{од}$ – вероятность ошибочных действий ДСП (имеет порядок $P_{од} = 10^{-3}…10^{-2}$ и зависит от многих факторов, таких как время суток, интенсивность работы, физиологическое состояние и др. В нештатных стрессовых ситуациях она может увеличиваться до 10^{-2}–10^{-1}).

Анализируя факторы, влияющие на интенсивность аварий λ_a, видно, что второе слагаемое в выражении (1) имеет преимущественный вклад, а меры повышения надежности и безопасности функционирования МПЦ в первую очередь должны быть связаны с уменьшением вероятности $P_{од}$ ошибочных действий ДСП.

Для снижения риска возникновения аварийных ситуаций в системах критичных к безопасности находят все более широкое применение интеллектуальные надстройки в виде систем поддержки принятия решений оперативным персоналом.

Для облегчения работы ДСП во внештатных ситуациях в МПЦ «іпуть» реализована интеллектуальная система поддержки принятия решений (СППР), задачей которой является предоставление дежурному по станции порядка действий при возникновении нештатных ситуаций и контроль его выполнения. Новизна технических решений МПЦ подтверждена патентами на изобретения в Республике Беларусь и РФ. Таким образом, интеллектуализация функций МПЦ путем интеграции в неё СППР повышает уровень безопасности движения поездов за счет значительного уменьшения ошибочных действий ДСП.

Анализ влияния интеллектуализации функций МПЦ на повышение безопасности движения поездов помимо этого дает возможность обоснования и количественной оценки необходимости «глубины» резервирования подсистем МПЦ.

УДК 004.312.466

АНАЛИЗ НА БЕЗОПАСНОСТЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ МИКРОПРОЦЕССОРНЫХ УСТРОЙСТВ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ

К. А. БОЧКОВ, Б. В. СИВКО
Белорусский государственный университет транспорта, г. Гомель

Современные микропроцессорные системы железнодорожной автоматики и телемеханики (СЖАТ) относятся к критически важным объектам информатизации с повышенными требованиями по уровню безопасности и надежности функционирования. Данные системы являются аппаратно-программными комплексами (АПК), в которых программное обеспечение (ПО) является неотъемлемым компонентом и оно подлежит анализу на безопасность, как и аппаратные средства СЖАТ. В настоящее время отсутствуют общепризнанные и универсальные методы проведения анализа на безопасность ПО, и одним из актуальных вопросов является разработка инструментария, позволяющего эффективно проводить мероприятия по обеспечению необходимого уровня качества ПО и последующему доказательству безопасности.

Согласно мировой практике, мнению экспертов и стандартам разработки критически важных объектов информатизации, верификация данных устройств должна проводиться независимо от коллектива разработчиков. Проводимый анализ на безопасность представляет собой полный цикл обратной разработки (reverse engineering), во время которой независимой организацией необходимо определить доказываемые свойства системы и проверить их на корректность. Для верификации систем, управляющими ответственными технологическими процессами, первым шагом является определение функции безопасности (ФБ), выполнение которой верифицируется в последующем.

Определение ФБ имеет ряд особенностей и проблем. Прежде всего, при доказательстве безопасности должна быть определена ФБ независимой организацией для последующего анализа корректности предоставленных разработчиками доказательных документов.