

УДК 656.25

Функциональная безопасность тягового железнодорожного подвижного состава

В.А. КУЧУМОВ, Р.В. МУРЗИН, Н.Б. НИКИФОРОВА, М.С. ХАЗОВ, А.А. АКИШИН

Акционерное общество «Научно-исследовательский институт железнодорожного транспорта» (АО «ВНИИЖТ»), Москва, 129626, Россия

Аннотация. Изложены подходы к определению понятия функциональной безопасности на железнодорожном транспорте. Показана важность соблюдения требований к функциональной безопасности в условиях повсеместного использования программируемых контроллеров и микропроцессорных систем управления. С позиции функциональной безопасности рассмотрен электровоз, приведена его структурная схема, по которой проводят соответствующие проверки. Рассмотрены источники опасных событий, связанные с наличием программного обеспечения и представляющие угрозу нарушения требований безопасности, к которым относятся как отказы некоторых составных частей электровоза, так и внешние воздействия, в том числе ошибочные действия локомотивной бригады.

Рассмотрено понятие риска нарушений требований безопасности, приведен подход для оценки уровня риска, который предполагает качественную и количественную оценки вероятности и последствий риска. Показана необходимость учета при оценке рисков возможного ущерба здоровью людей и окружающей среде, а также финансовых потерь.

Показана необходимость определения функций безопасности тягового железнодорожного подвижного состава, направленных на противодействие внешним и внутренним опасностям. Представлена методика определения уровней полноты безопасности для различных функций безопасности.

Изложена методика по определению фактического уровня полноты безопасности для функций безопасности, реализованных контурами безопасности, основанная на использовании графа безопасности и заключающаяся в анализе устройств, входящих в этот контур.

Подробно рассмотрен пример выполнения проверки соответствия одной из функций безопасности электровоза требованиям функциональной безопасности.

Ключевые слова: функциональная безопасность; уровень полноты безопасности (УПБ); оценка рисков; функция безопасности; микропроцессорные системы

1. Актуальность. Микропроцессорные системы управления широко применяются на разных типах железнодорожного подвижного состава (ПС): локомотивах, электропоездах и на некоторых типах пассажирских вагонов, например системы Тальго. По мере увеличения на ПС количества микропроцессорных систем управления увеличивается число отказов, ошибок и сбоев функционирования программного обеспечения (ПО). Возможно выделить события, связанные с безопасностью, т. е. такие, которые могут привести к травмированию людей, значительным

материальным потерям или нанести ущерб окружающей среде [1].

Для предотвращения таких событий, согласно стандарту ОАО «РЖД» 02.049 – 2014 «Автоматизированные системы управления технологическими процессами и техническими средствами железнодорожного транспорта. Требования к функциональной и информационной безопасности программного обеспечения. Порядок оценки соответствия», необходимо предусматривать специальные средства, соответствующие требованиям функциональной безопасности (ФБ). Действующий стандарт [2, ч. 4] дает следующее определение ФБ: «Функциональная безопасность — это часть общей безопасности, обусловленная применением управляемого оборудования (УО), системы управления УО и зависящая от правильности функционирования электрических, электронных, программируемых электронных систем, связанных с безопасностью, и других средств по снижению риска». УО — это оборудование, машины, аппараты или установки, используемые для производства, обработки, транспортировки и т. д. Система управления УО представляет собой отдельное, отличное от УО понятие.

2. Постановка задачи. Для исследования ФБ сложного объекта с распределенной архитектурой целесообразно представить его в виде структурной схемы (рис. 1). Центральная система управления принимает управляющие команды по интерфейсу управления от оператора, информационные сигналы от блокировок, датчиков и специальных информационных систем,

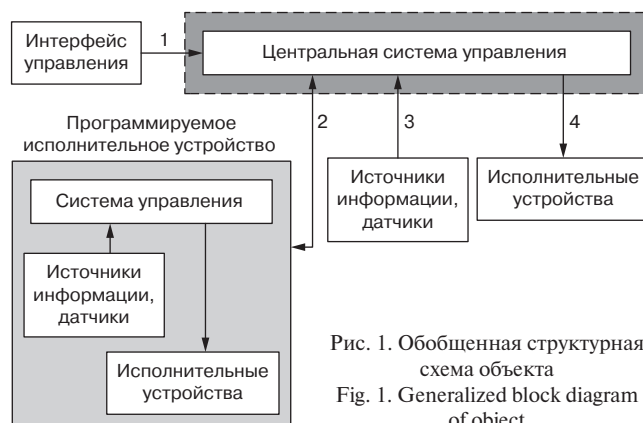


Рис. 1. Обобщенная структурная схема объекта
Fig. 1. Generalized block diagram of object

■ E-mail: khazov.maksim@vniizht.ru (М.С. Хазов)

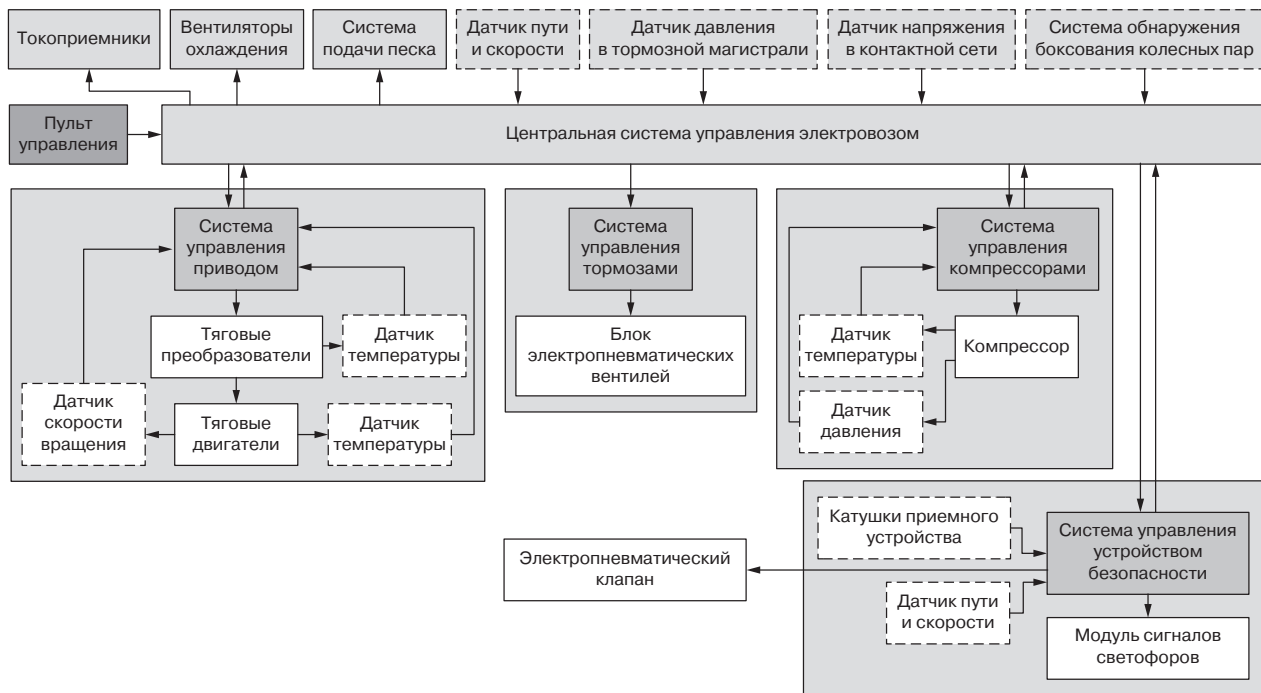


Рис. 2. Структурная схема электровоза с позиции ФБ
Fig.2. Structural electric scheme from the position of FS

формирует и передает команды управления на исполнительные устройства. Программируемые исполнительные устройства выделены сплошной линией; они содержат в своем составе системы управления конкретным оборудованием ПС. На границе центральной системы управления ПС (штриховая линия на рис. 1) имеются четыре порта 1–4, т.е. зажимы, разъемы, клеммы, стыки связи и т.д. Именно на этих портах необходимо рассматривать появление опасных событий, вызванных нештатными режимами работы, отказами исполнительных устройств, источников информации, датчиков, интерфейсов управления. Когда объект содержит исполнительные устройства с собственными программируемыми системами управления, то сначала отдельно рассматривается ФБ этих устройств в качестве автономно работающих объектов.

На современных электровозах имеется несколько иерархически подчиненных систем управления — например, тяговым приводом, тормозной системой, системой кондиционирования воздуха, системами высоковольтного и низковольтного питания и т.д. (рис. 2).

Процесс управления ПС предусматривает информационное взаимодействие с датчиками, органами и объектами управления, выполненными по разным техническим принципам [3, 4]. Алгоритмы управления должны не только обеспечивать правильное выполнение предусмотренных функций, но и сохранять безопасное состояние при воздействиях, приводящих к возникновению опасных состояний [5]. Опасности приводят к неправильной реализации функций управления.

В качестве основных источников опасности (рис. 3) согласно ГОСТ Р 51897–2011 (Руководство ИСО 73:2009) «Менеджмент риска. Термины и определения» рассмотрены аппаратура управления, управляемое и измерительное оборудование, ошибки обслуживающего персонала, воздействие окружающей среды и др. [6].

Аппаратура и программная часть систем управления могут быть источниками опасности при сбоях, отказах, ошибках.

Такие понятия, относящиеся к отказам, используются в соответствии с рекомендациями национального,

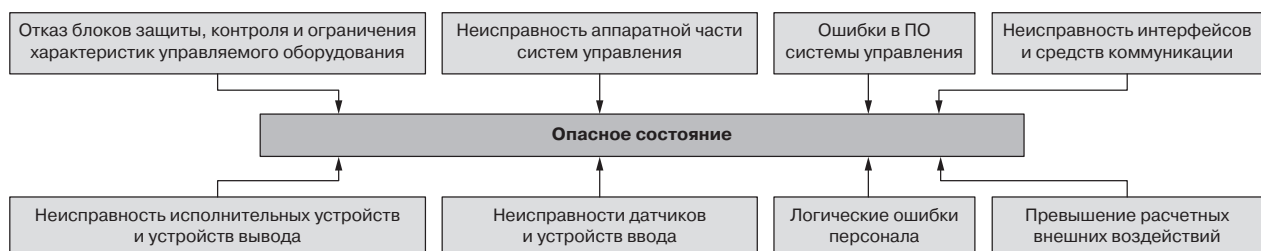


Рис. 3. Источники возникновения опасных состояний электровоза
Fig. 3. Sources of dangerous states of electric locomotive

идентичного международному, стандарта [2, ч. 4]. Неисправность интерфейсов, средств коммуникации также может служить источником опасности, так как при отказе, например обрыве провода, поступают ошибочные данные и на их основании будут выработаны опасные управляющие воздействия.

Отказ блоков защиты, контроля и ограничения характеристик управляемого оборудования (главный (быстродействующий) выключатель, дифференциальное реле и др.) также может привести к опасной ситуации, если нет специальных защитных мер.

Также к опасным последствиям могут привести отказы в работе исполнительных блоков управляемого оборудования (контакты, двигатели), датчиков и измерительных устройств (датчики скорости, датчики напряжения контактной сети, переключатели грузовых режимов и т. д.).

К источникам опасных ситуаций, которые должны быть учтены при создании системы управления, относятся также ошибки и некорректные действия локомотивной бригады.

При разработке системы управления оговариваются допустимые внешние воздействия. Однако бывают опасные ситуации при превышении величины внешних воздействий, когда оборудование может отказать, но опасное состояние ПС должно быть предотвращено.

По отношению к конкретному опасному событию (сход с рельсов, самоход и т. д.) необходимо предусмотреть создание функции безопасности, которая будет ему противодействовать. Создание спецификации функций безопасности, т. е. перечня функций безопасности, которые должна выполнять система управления, согласно ГОСТ Р 54504 – 2011 «Безопасность функциональная. Политика, программа обеспечения безопасности. Доказательство безопасности объектов железнодорожного транспорта» должно предусматриваться еще на этапе разработки технического задания. Функция безопасности может реализовываться различными способами: начиная от сообщения оператору о появлении какой-либо опасности и заканчивая автоматическим принятием мер по недопущению опасного состояния ПС. Совокупность технических и алгоритмических средств, реализующих конкретную функцию безопасности, представляет собой контур безопасности. Оператор тоже может быть одним из элементов контура безопасности. Основным требованием обеспечения ФБ электровоза является наличие необходимых функций безопасности, направленных на противодействие возможным опасным событиям.

Для каждой потенциальной опасности необходимо провести оценку риска. Поскольку риск — событийное понятие, для его численной оценки вводится отдельный показатель — оценка или уровень риска (УР) [1]. УР — это вероятность того, что опасность реализуется

и приведет к нанесению ущерба. Таким образом, УР является функцией двух аргументов: вероятности проявления риска $p_j(t)$ и объема ущерба от его проявления C_j . Вероятность проявления риска $p_j(t)$ должна отражать возможность появления опасного события и его негативные последствия. Эта вероятность может выражаться различными способами, например как пропорция (один случай на тысячу), как периодичность (10 случаев в год) или как качественная оценка (несущественно или существенно).

Описание последствий риска зависит от типа и объема нанесенного ущерба. Тип ущерба зависит от объекта, которому был нанесен урон. Такими объектами могут являться: человек (ущерб здоровью), объект железнодорожной техники, инфраструктуры и т. д. (материальный ущерб), окружающая среда (экологический ущерб). Также ущерб может быть комплексным [1]. Материальный ущерб оценивается в соответствии с потерями холдинга ОАО «РЖД» из-за проявления риска.

В общем случае последствия определяются простыми описаниями, например «побочные», «малой тяжести», «тяжелые», «катастрофические». Для примера можно указать, что в ГОСТ Р 54505 – 2011 «Безопасность функциональная. Управление рисками на железнодорожном транспорте» для тележек грузовых вагонов в 2012 г. введены следующие оценки: менее 500 тыс. руб. — «незначительный ущерб», более 2500 тыс. руб. — «катастрофический ущерб».

Для возможности перехода от оценок риска к соответствующим требованиям к функциям безопасности при наличии столь разнообразных оценок рисков в стандарте [2, ч. 1] введено четыре уровня полноты безопасности (УПБ) от первого (самого низкого) до четвертого (самого высокого). Понятие УПБ использовалось достаточно давно для оценки отказоустойчивости аппаратных средств [7], при этом в соответствии с регламентированной надежностью оценивалась интенсивность отказов. УПБ определяется для функций безопасности системы, т. е. для защитных мер, принимаемых для адекватного снижения риска конструктором или пользователем.

В общем случае УПБ показывает, какая интенсивность реализации опасного события, приводящего к нанесению ущерба, допускается для системы. Задание УПБ имеет значение на всех этапах жизненного цикла создания систем управления [8], начиная от технических требований к новому электровозу и системе управления. Выполнение заданного УПБ необходимо учитывать при проектировании архитектуры системы, при интеграции ее с объектом управления. Для готового локомотива проводится проверка ФБ, включающая следующие основные этапы:

1. Проверка обоснованности спецификации функций безопасности рассматриваемого объекта;

Значения допустимой интенсивности проявления рисков для УПБ

The values of the permissible intensity for displaying risks for SIL

Уровень полноты безопасности (УПБ)	Допустимая интенсивность проявления опасностей λ_p , ч ⁻¹	Допустимая интенсивность проявления опасностей λ_p , год ⁻¹
1	$10^{-6} \leq \lambda_p < 10^{-5}$	$10^{-2} \leq \lambda_p < 10^{-1}$
2	$10^{-7} \leq \lambda_p < 10^{-6}$	$10^{-3} \leq \lambda_p < 10^{-2}$
3	$10^{-8} \leq \lambda_p < 10^{-7}$	$10^{-4} \leq \lambda_p < 10^{-3}$
4	$10^{-9} \leq \lambda_p < 10^{-8}$	$10^{-5} \leq \lambda_p < 10^{-4}$

2. Проверка выполнения системой требуемого УПБ к этим функциям;

3. Проверка выполнения функций безопасности при моделировании возникновения рисков.

Достижение заданного УПБ осуществляется многоуровневой структурой построения объекта. Для обеспечения стабильности работы ПО при создании программного кода должны выполняться требования к архитектуре, средствам поддержки и т.д. этого кода, соответствующие заданному УПБ. Иными словами, при создании ПО должны соблюдаться допустимые для данного УПБ методы программирования в соответствии с [2, ч. 3].

Для оценки аппаратных средств существуют численные оценки интенсивности отказов для разных УПБ (таблица) [2, ч. 1]. Если к функции безопасности не предъявляются требования по ограничению наибольшей интенсивности проявления опасностей

(ведущих к нанесению ущерба), то для нее УПБ не определяется. Первый уровень полноты безопасности (УПБ = 1) предъявляет к функциям системы требования по ограничению наибольшей интенсивности проявления риска.

Максимально допустимая интенсивность проявления опасностей λ_p в час в системах с УПБ = 1 не должна превышать значение из диапазона $10^{-6} \leq \lambda_p < 10^{-5}$ или $10^{-2} \leq \lambda_p < 10^{-1}$ отказов в год. Интенсивность проявлений риска в защищенной системе может быть меньше, чем заданное требованиями к УПБ, но не должна его превышать. Как правило, первый уровень полноты безопасности назначается системам, ущерб от проявления риска в которых велик при низкой вероятности проявления ущерба, или системам, вероятность проявления риска в которых велика, но его последствия не являются существенными.

Остальные уровни полноты безопасности УПБ = 2, УПБ = 3 и УПБ = 4 отличаются от первого только ограничением на наибольшую интенсивность проявления рисков, допустимую для системы (см. таблицу).

3. Пути решения задачи. Для определения необходимого УПБ контура безопасности, реализующего конкретную функцию безопасности, возможно применять как количественный, так и качественный подходы. Одним из методов определения УПБ в [2, ч. 5] указывается метод графа риска. Граф риска позволяет определить требования по УПБ для функций

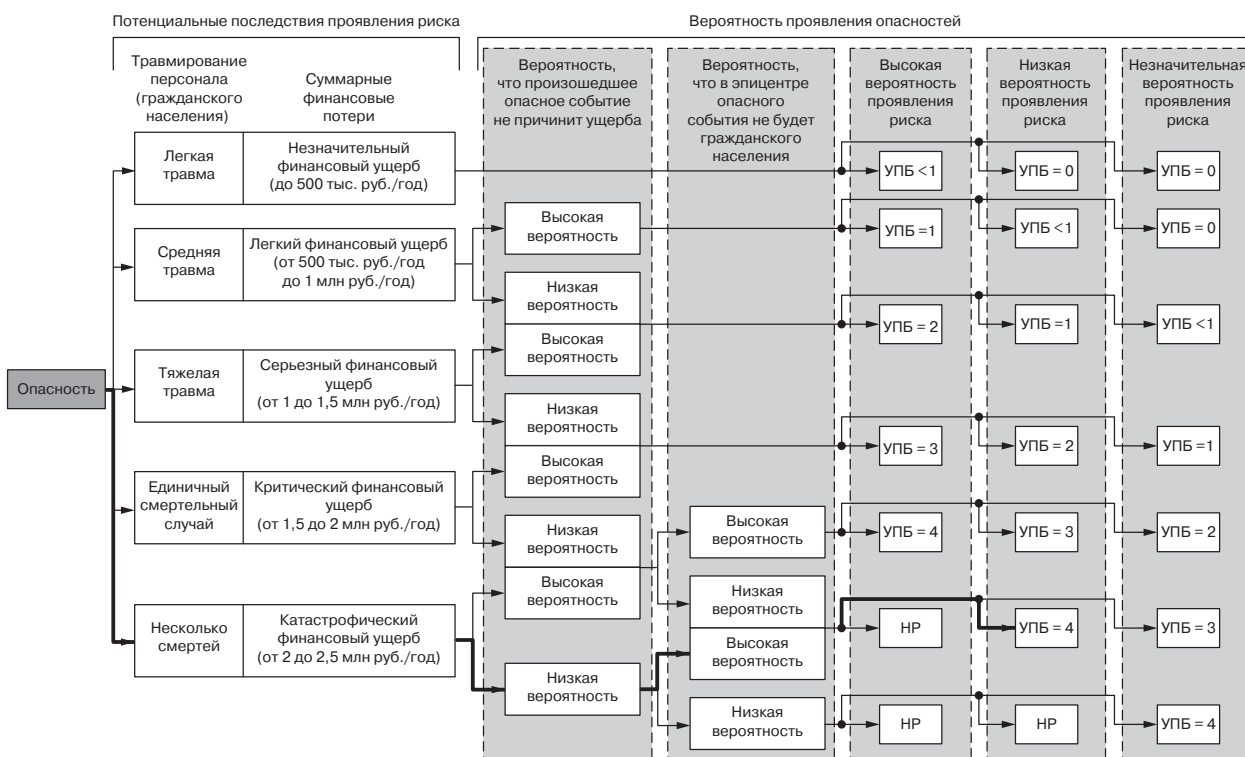


Рис. 4. Граф риска для определения УПБ железнодорожного подвижного состава (жирная линия для случая, рассматриваемого в примере)

Fig. 4. Graph risk for determining SIL of railway rolling stock (thick line for the case under consideration in the example)

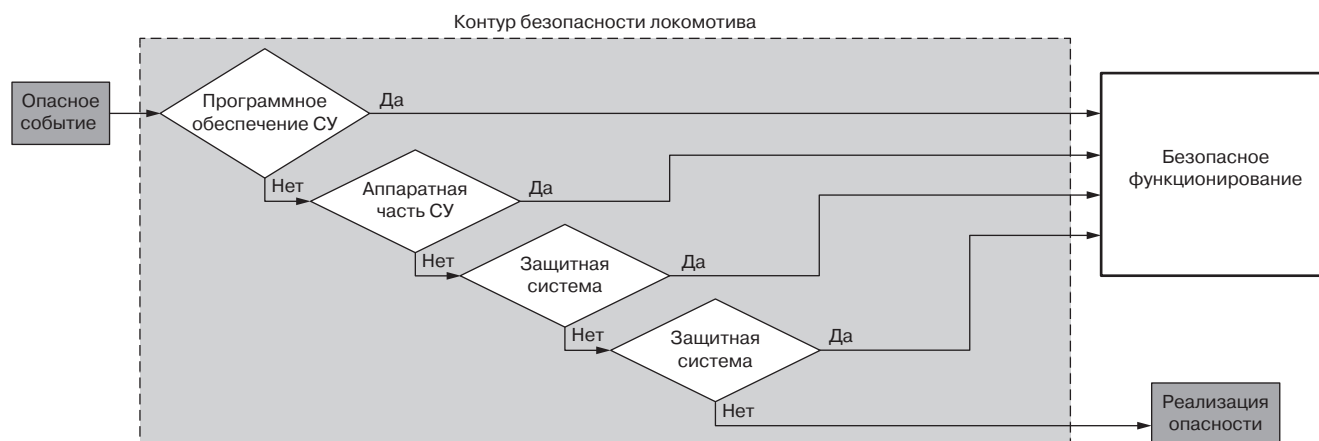


Рис. 5. Контур безопасности
Fig. 5. Safety contour

безопасности, в системах для которых вероятность проявления риска определить затруднительно. Граф риска направлен на уточнение вероятности проявления риска за счет рассмотрения предотвращающих или смягчающих риск факторов (рис. 4).

С использованием графа риска для рассматриваемой опасности производится определение потенциальных последствий проявления риска, которые могут быть оценены в людских или материальных потерях или совместно в том и другом. На следующем этапе графа риска оценивается, какова вероятность того, что опасное событие не причинит ущерба (так, например, если пассажира зажмет автоматическими дверями и «протащит» по платформе, есть высокая вероятность того, что серьезных травм ему удастся избежать при своевременной остановке поезда). Далее учитывается, могут ли при аварии пострадать окружающие, не участники перевозочного процесса.

Следующий этап использования графа — учесть, насколько часто встречаются подобные ситуации. Градация «высокая вероятность» оценочно соответствует выражению частоты события: «об этих случаях говорят», или в числовом эквиваленте: $\lambda_{вз} \approx 1$ (один случай в год). «Низкая вероятность» соответствует выражению частоты события «такие случаи были» ($\lambda_{вз} \approx 0,1 \text{ год}^{-1}$). И понятие «незначительная вероятность» соответствует высказыванию «либо не были вообще, либо о них все забыли» ($\lambda_{вз} \approx 0,01 \text{ год}^{-1}$). Безусловно, этот граф представляет экспертную оценку с соответствующей долей субъективизма, но четыре диапазона УПБ достаточно широкие и позволяют пользоваться такими понятиями.

На графе риска (см. рис. 4) финансовые потери могут быть вызваны двумя факторами: *выход из строя* частей ПС (пробой изоляции тягового двигателя, обрыв автосцепки и т. д.) и железнодорожной инфраструктуры (при сходах с рельсов и т. д.) и сопутствующее этому *невыполнение основной функции* — перевозки грузов или пассажиров (простой на перегонах, вынужденное

движение по перегону с минимальной скоростью по причине аварии). При этом необходимо учитывать, что простой одного поезда на перегоне приводит к простоям следующих за ним поездов, тем самым увеличиваются общие финансовые потери. При этом к «катастрофическим» финансовым потерям могут привести как одно значительное крушение, так и несколько длительных остановок на перегоне из-за отказов, не позволяющих продолжить движение. Денежные потери, безусловно, должны соотноситься с курсом рубля, в данном случае приведены финансовые потери, актуальные на начало 2012 г.

Достижение заданного УПБ реализуется за счет многоуровневого построения контура безопасности, содержащего выполненные на различных принципах системы. В контур безопасности (рис. 5) для примера могут входить средства, программно выполняющие функции безопасности (1-й уровень), контролирующие и предотвращающие нежелательные события (2-й уровень). И наконец, 3-й и 4-й уровни — защитные системы выявления опасности, способные с определенной долей вероятности не дать риску проявиться за счет использования автоматических или ручных защитных мер.

На этапе проверки ПС на ФБ необходимо доказать выполнение функциями безопасности (а следовательно, контурами безопасности) требований по интенсивности их отказов, определенных на этапе распределения УПБ для этих контуров.

Интенсивность отказа контура λ_k — это вероятность того, что в течение заданного времени контур безопасности не реализует функцию безопасности из-за одновременного отказа всех устройств этого контура, что приведет к возникновению опасности. Поэтому λ_k определяется перемножением вероятности отказа каждого из i устройств, входящих в контур безопасности: $\lambda_{k\Sigma} = \lambda_{k1} \cdot \lambda_{k2} \cdot \dots \cdot \lambda_{ki}$ (см. рис. 5).

Далее оценивается, насколько часто при появлении риска происходит неблагоприятное событие, т. е.

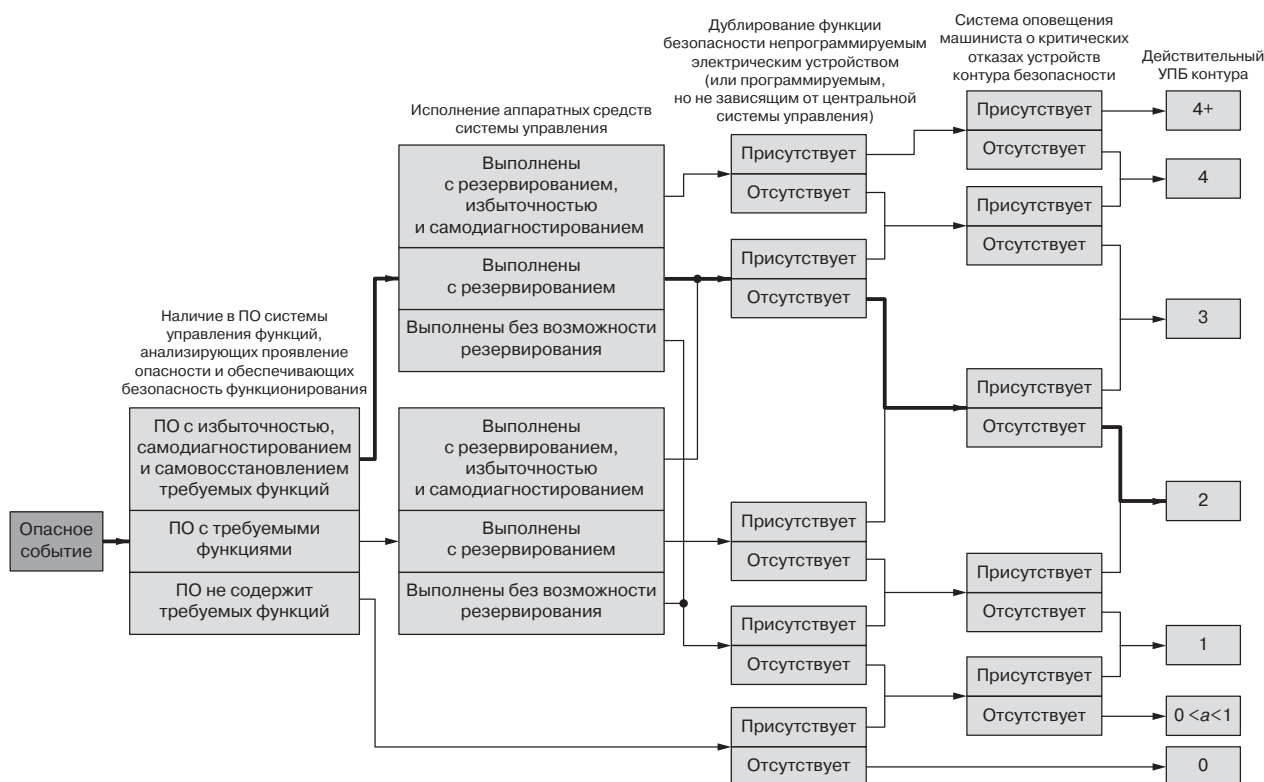


Рис. 6. Граф безопасности (жирная линия для случая, рассматриваемого в примере)

Fig. 6. Safety graph (thick line for the case under consideration in the example)

отношение k проявления риска к количеству отказов функции безопасности. Например, при $k = 0,1$ только один из десяти отказов контура защиты приводит к проявлению риска. Таким образом, интенсивность проявления риска для ПС вычисляется как $\lambda_p = k\lambda_k$.

Полученное значение λ_p сравнивается с приведенными в таблице для УПБ, определенного для функции безопасности ПС. При больших значениях λ_p интенсивность нанесения ущерба будет больше максимально приемлемой, следовательно, контур безопасности не выполняет заданную функцию безопасности и требует совершенствования. При меньших значениях λ_p , наоборот, интенсивность нанесения ущерба будет меньше максимально приемлемой, следовательно, контур безопасности не требует дальнейшего совершенствования.

Для определения реализованного УПБ контура безопасности разработан типичный граф безопасности функций безопасности электроваза (рис. 6). С помощью этого графа можно вычислить УПБ контура безопасности, используя:

- примерную оценку отказов ПО и программируемых устройств, не имеющих аналогов в эксплуатации;
- более точную оценку отказов электрических и электронных устройств, интенсивность отказов которых можно спрогнозировать исходя из полученных при эксплуатации статистических данных.

Для первого уровня контура безопасности действительный УПБ определяется свойствами ПО системы

управления, реализующей функции безопасности. Если в ПО присутствуют защитные меры, то это ПО возможно классифицировать по принципам противодействия внутренним ошибкам, определяющим интенсивность отказа контура [9]:

- «ПО с избыточностью, самодиагностированием и самовосстановлением требуемых функций» — это наиболее отказоустойчивое ПО, способное выполнять требуемую функцию безопасности. Отказоустойчивость может достигаться наличием в нем средств предупреждения и обнаружения ошибок (избыточность, взаимное недоверие компонентов и т.д.) и средств, обеспечивающих устойчивость к ошибкам (динамическая избыточность, самовосстановление, самодиагностирование) [9]. Используя рекомендации, приведенные в [2], а также имеющийся опыт применения таких систем [3], интенсивность критических отказов ПО в этом случае для примера можно принять такой же, как и аппаратной части устройств системы управления, реализующих данное ПО. Таким образом, получается $\lambda_k \approx 0,3 \text{ год}^{-1}$, что соответствует наработке ПО на отказ 20000 ч при коэффициенте использования ПС $k_u = 0,7$;

- «ПО с требуемыми функциями» — это ПО, также способное выполнять требуемую функцию безопасности, но не защищенное от внутренних ошибок и имеющее интенсивность критических отказов выше, чем предыдущее; оценим интенсивность отказов $\lambda_k \approx 0,9 \text{ год}^{-1}$;

• «ПО не содержит требуемых функций» — в ПО системы управления не содержится защитных мер от отказов, ошибок и сбоев ПО; оценим интенсивность отказов $\lambda_k \approx 120 \text{ год}^{-1}$.

Для второго уровня контура безопасности реализованный УПБ определяется исполнением аппаратной части систем управления ПС, противодействующих опасности. Интенсивность отказов этих устройств может быть определена расчетным способом [2, ч. 6]. Архитектуру исполнения аппаратной части возможно классифицировать как:

- выполнение с резервированием, избыточностью и самодиагностированием — ориентировочно наработка на отказ составляет 20 000 ч, что при коэффициенте использования подвижного состава $k_{\text{и}} = 0,7$ позволяет получить интенсивность отказов в год $\lambda_k \approx 0,3 \text{ год}^{-1}$;

- выполнение с резервированием — после отказа резервируемых составляющих общая надежность значительно снижается, и любой последующий отказ может привести к реализации опасного события; из-за отсутствия средств самодиагностирования возможен отказ средств холодного резервирования. Интенсивность отказов таких контуров возможно оценить в раз-
мере $\lambda_k \approx 0,9 \text{ год}^{-1}$;

- выполнение без резервирования — интенсивность отказов этих контуров возможно оценить в раз-
мере $\lambda_k \approx 120 \text{ год}^{-1}$.

Для третьего и четвертого уровней контуров безопасности с целью определения действительного УПБ контура рассматриваются устройства, реализующие защитные меры, которые способны работать параллельно с центральной системой управления. Это могут быть непрограммируемые электрические устройства (главный (быстродействующий) выключатель, блокировки шкафов с оборудованием, блокировки дверей в электропоездах, газовые реле) или программируемые при условии, что их система управления может функционировать без связи с центральной. Опыт проектирования и создания электропоездов показал, что опасные отказы электрических устройств и аппаратов происходят примерно раз в три года, следовательно, интенсивность опасных отказов электрических устройств защиты можно принять в раз-
мере $\lambda_k \approx 0,33 \text{ год}^{-1}$.

Далее учитывается способность локомотивной бригады обеспечить безопасность функционирования электропоезда в случае отказа всего контура безопасности или некоторых его составляющих. Отсутствие необходимых действий локомотивной бригады приравнивается к отказу одного из уровней.

При учете влияния человеческого фактора учитываются следующие положения [10]. Вероятность ошибок локомотивной бригады не является постоянной величиной и зависит от времени суток, продолжительности смены и т. д. По статистике зафиксированных

происшествий на Западно-Сибирской железной дороге в 2012, 2013 и 2014 гг., количество опасных отказов, возникших по вине человека, примерно в 10 раз меньше, чем из-за неисправности технических средств. Таким образом, при отсутствии специальных средств оповещения машиниста об отказах устройств контура безопасности с учетом влияния человеческого фактора интенсивность того, что машинист не применит защитные меры при возникновении угрозы, составляет $\lambda_k \approx 0,033 \text{ год}^{-1}$. Однако при применении специальных средств оповещения (например, звуковое оповещение об отказе системы управления с рекомендацией усиленного контроля за параметрами движения поезда и выполнения перезагрузки ПО системы в ручном режиме) интенсивность опасных событий, которые машинист не предупредил, может быть снижена до $\lambda_k \approx 0,001 \text{ год}^{-1}$.

4. Применение результатов (экспериментальная часть). Для примера проанализируем проверку безопасности выполнения одной из функций безопасности грузового электропоезда при отказе системы управления и, как следствие, отсутствии замещения рекуперативного торможения пневматическим. Одна из возможных реализаций данной опасности — сход электропоезда с рельсов при движении в кривой, на других участках ограничения скорости и т. д. Поэтому реализация данной опасности приводит к «катастрофическому» финансовому ущербу (2 и более млн рублей) от разрушения электропоезда и разрушения пути, а также может нанести непоправимый ущерб жизни людей. Следовательно, используя граф риска для железнодорожного ПС (см. рис. 4), в группе блоков «Потенциальные последствия проявления риска» выбирается нижний блок «Несколько смертей».

Вероятность того, что произошедшее опасное событие (неконтролируемое увеличение скорости) не причинит ущерба, мала, из чего следует выбор блока «Низкая вероятность», последовательно соединенно-
го с блоком «Несколько смертей».

Вероятность того, что при реализации риска не будет пассажиров и гражданского населения (в случае наличия в данном месте на путях других транспортных средств с людьми), велика, поэтому выбираем блок «Высокая вероятность», связанный последовательно с выбранным ранее блоком «Низкая вероятность». То есть по графу риска определено, что при низкой вероятности такого отказа контур безопасности должен иметь УПБ = 4.

После этого определяется контур безопасности электропоезда, направленный на применение защитных мер (см. рис. 5). Первым уровнем в контуре безопасности являются программные средства, вторым — аппаратные средства системы управления. Если после отключения или при опасном отказе ПО системы управления происходит срыв рекуперативного торможения

без замещения пневматическим, то для остановки поезда возможно применить пневматическое торможение, используя кран машиниста или кнопку экстренного торможения — третий уровень контура безопасности, который может быть активирован вручную локомотивной бригадой.

Четвертым уровнем контура безопасности является безопасный локомотивный объединенный комплекс БЛОК, который применяет пневматическое торможение при превышении скорости движения поезда, разрешенной на данном участке, или при проезде запрещающего сигнала светофора.

Далее с использованием графа безопасности (см. рис. 6) определяется действительный УПБ контура безопасности, для этого классифицируется каждое устройство i -го уровня контура безопасности в соответствии с предложенной для графа безопасности классификацией.

Пусть в ПО системы управления электровоза присутствуют команды, направленные на активацию пневматического торможения при срыве рекуперативного торможения, и ПО содержит средства самовосстановления, самодиагностирования и т. д., что обеспечивает его высокую отказоустойчивость. Тогда по графу безопасности на рис. 6 должен быть выбран блок «ПО с избыточностью, самодиагностированием и самовосстановлением требуемых функций».

Аппаратная часть системы управления электровоза выполнена с возможностью резервирования, но без возможности самовосстановления отказавших модулей и без аппаратной избыточности. При отказе одного модуля системы управления она полностью лишается резервирования, и последующий ее отказ приведет к опасному отказу электровоза. Аппаратные средства такой системы управления возможно классифицировать по графу безопасности как «выполнены с резервированием».

Предположим, что на электровозе отсутствуют устройства безопасности, активирующие пневматическое торможение при разборе схемы рекуперативного торможения при неработающей системе управления, и отсутствуют системы оповещения локомотивной бригады о потере работоспособности системы управления. Тогда можно сделать вывод, что действительный уровень контура безопасности электровоза составляет УПБ = 2 при требовании УПБ = 4, что свидетельствует о невыполнении электровозом требований УПБ = 4.

Для того чтобы данная функция безопасности электровоза соответствовала УПБ = 4, необходимо, например, реализовать функцию звукового оповещения локомотивной бригады об отказе рекуперативного торможения и добавить в аппаратную часть системы управления возможность самовосстановления отказавших модулей и аппаратную избыточность.

5. Заключение. Для тягового подвижного состава рассмотрены вопросы функциональной безопасности, начиная от принципов определения рисков и функций безопасности и заканчивая анализом определения требований и фактической реализации УПБ для одной из функций безопасности электровоза. Такое изложение позволяет иллюстрировать важность вопросов функциональной безопасности для безопасности тягового подвижного состава.

СПИСОК ЛИТЕРАТУРЫ

1. Фортон В.Е., Махутов Н.А. Научное обоснование критериев эффективности, безопасности и рисков эксплуатации железнодорожного транспорта // Научное обеспечение инновационного развития и повышения эффективности деятельности железнодорожного транспорта: коллективная монография членов и научных партнеров Объединенного научного совета ОАО «РЖД». М.: Mittel Press, 2014. С. 13 – 15.
2. ГОСТ Р МЭК 61508 – 2012. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. М.: Стандартинформ, 2014.
3. Никифорова Н.Б., Худорожко М.В., Рогожников О.В. Задача обеспечения функциональной безопасности при разработке микропроцессорных систем управления // Вопросы развития железнодорожного транспорта в условиях рыночной экономики: сб. науч. трудов / под ред. Ю.М. Черкашина, Г.В. Гогричани. М.: Интекст, 2007. С. 69 – 75.
4. Никифорова Н.Б., Худорожко М.В., Рогожников О.В. Анализ функциональной безопасности системы управления электровозом // 7-я международная научно-техническая конференция «Кибернетика и высокие технологии XXI века»: сборник докладов. Т. 1. Воронеж: НПФ «САКВЕЕ», 2006. С. 26 – 30.
5. Рудановский В.М. Методика определения причинно-следственных связей нарушений безопасности движения // Вестник ВНИИЖТ. 2014. № 3. С. 17 – 23.
6. Юренко К.И., Юренко И.К. Повышение информационной и функциональной безопасности бортовых систем управления локомотивов нового поколения // Вестник Всероссийского научно-исследовательского и проектно-конструкторского института электровозостроения. 2009. № 2 (58). С. 260 – 264.
7. Смит Д.Дж., Кеннет Симпсон Дж. Л. Функциональная безопасность. Простое руководство по применению стандарта МЭК 61508 и связанных с ним стандартов. М.: Издательский Дом «Технологии», 2004. 208 с.
8. P. Low, R. Pabst, E. Petry. Funktionale Sicherheit in der Praxis. Anwendung von DIN EN 61508 und ISO/DIS 26262 bei der Entwicklung von Serienprodukten. dpunkt Verlag, 2010. 355 S.
9. Шубинский И.Б. Методы обеспечения функциональной надежности программ // Надежность. 2014. № 4 (51). С. 87 – 94.
10. Репина И.Б. Учет влияния человеческого фактора на организационно-технологическую надежность производственных процессов инфраструктуры железных дорог: дисс. на соиск. уч. степ. канд. техн. наук. 2015. 211 с.

ИНФОРМАЦИЯ ОБ АВТОРАХ

КУЧУМОВ Владислав Алексеевич,
д-р техн. наук, профессор, главный научный сотрудник,
отделение «Тяговый подвижной состав», АО «ВНИИЖТ»

МУРЗИН Роман Вилорьевич,
канд. техн. наук, заведующий лабораторией «Электровозы»,
отделение «Тяговый подвижной состав», АО «ВНИИЖТ»

НИКИФОРОВА Нина Борисовна,

канд. техн. наук, ведущий научный сотрудник, отделение
«Тяговый подвижной состав», АО «ВНИИЖТ»

ХАЗОВ Максим Сергеевич,

канд. техн. наук, ведущий научный сотрудник, отделение
«Тяговый подвижной состав», АО «ВНИИЖТ»

АКИШИН Александр Александрович,

канд. техн. наук, ведущий инженер, отделение «Тяговый
подвижной состав», АО «ВНИИЖТ»

Статья поступила в редакцию 9.02.2016 г., актуализирована
20.04.2016 г., принята к публикации 25.04.2016 г.,

Functional safety of traction railway rolling stock

V.A. KUCHUMOV, R.V. MURZIN, N.B. NIKIFOROVA, M.S. KHAZOV, A.A. AKISHIN

Joint Stock Company "Railway Research Institute" (JSC "VNIIZhT"), Moscow, 129626, Russia

Abstract. The article describes approaches to the definition of functional safety in railway transport. The importance of compliance with requirements for functional safety in the context of widespread use of programmable controllers and microprocessor control systems is shown. Electric locomotive is considered from the point of functional safety, as well as its structural scheme which is used to carry out necessary checks. Main sources of threats for railway rolling stock were described, which include the malfunction of some component parts of the electric locomotive and external influences, including erroneous actions of locomotive crew.

This article discusses the concept of risk of breaching safety requirements as well as demonstrates approach for assessing the level of risk, which involves quantitative and qualitative assessment of the probability and consequences of risk. Necessity of considering potential damage to human health, environmental damage and financial losses when performing risk assessment is shown.

The article shows the necessity of determining safety features of railway rolling stock targeted to counteraction to external and internal threats. Methods of determining safety integrity levels for the various safety functions is demonstrated on the base of using risk graph, which takes into account the probability of a hazardous event and damage caused to them. Necessity of using different devices to achieve required safety integrity level is shown.

Method for determining the actual safety integrity level of the safety contour based on the use of the "graph of safety" is shown and includes analysis of devices in this contour. This method allows determining the safety integrity level of the safety contour rolling stock on the basis of experience in the production and usage of devices of control and diagnosis.

An example of compliance one of the safety functions of the electric locomotive to the requirements of functional safety is closely considered in the article. In the example is shown, what measures are possible to apply to increase the functional safety of the electric locomotive to meet the requirements for safety integrity level.

Keywords: functional safety; safety integrity level (SIL); risk assessment; safety function; microprocessor systems

REFERENCES

1. Fortov V.E., Makhutov N.A. *Nauchnoe obosnovanie kriteriev effektivnosti, bezopasnosti i riskov ekspluatatsii zheleznodorozhnogo transporta* [Scientific justification of criteria of efficiency, safety and risks of operation of railway transport]. Nauchnoe obespechenie innovatsionnogo razvitiya i povysheniya effektivnosti deyatelnosti zheleznodorozhnogo transporta: kollektivnaya monografiya chlenov i nauchnykh partnerov Ob'dinenennogo nauchnogo soveta OAO "RZhD" [Scientific support for innovative development and improve the efficiency of railway transport: collective monograph of members and research partners of the Joint Scientific Council of JSC "Russian Railways"]. Moscow, Mittel Press Publ., 2014, pp. 13 – 15.
2. GOST EIC 61508 – 2012 *Functional safety of electrical, electronic, programmable electronic and safety-related systems*. Moscow, Standartinform Publ., 2014, 58 p. (in Russ.)
3. Nikiforova N.B., Khudorozhko M.V., Rogozhnikova O.V. *Zadacha obespecheniya funktsional'noy bezopasnosti pri razrabotke mikroprocessornykh sistem upravleniya* [Task of ensuring functional safety in the development of microprocessor control systems]. Voprosy razvitiya zheleznodorozhnogo transporta v usloviyakh rynochnoy ekonomiki: Sb. tr.

uchenykh OAO "VNIIZhT" [Issues of development of railway transport in terms of market economy. Coll. of works of JSC VNIIZhT (Railway research institute) scientists]. Moscow, Intext Publ., 2007, pp. 69 – 75.

4. Nikiforova N.B., Khudorozhko M.V., Rogozhnikova O.V. *Analiz funktsional'noy bezopasnosti sistemy upravleniya elektrovozom* [Analysis of functional safety of electric locomotive control system]. 7 mezhduarodnaya nauchno-tehnicheskaya konferentsiya: "Kibernetika i vysokie tekhnologii XXI veka". Sbornik dokladov, T.1. [7th International Scientific Conference: "Science and High Technologies of the XXI century". Collection of reports. Vol.1]. Voronezh, NPF "SAKVEE" Publ., 2006, pp. 26 – 30.

5. Rudanovskiy V.M. *Metodika opredeleniya prichinno-sledstvennykh svyazey narusheniy bezopasnosti dvizheniya* [Method for determining causal relationships for violations of traffic safety]. Vestnik VNIIZHT [Vestnik of the Railway Research Institute], 2014, no. 3, pp. 17 – 23.

6. Yurenko K.I., Yurenko I.K. *Povyshenie informatsionnoy i funktsional'noy bezopasnosti bortovykh sistem upravleniya lokomotivov novogo pokoleniya* [Increased informational and functional safety of board control systems of locomotives of new generation]. Vestnik vserossiyskogo nauchno-issledovatel'skogo i proektno-konstruktorskogo instituta elektrovostroyeniya [Bulletin of the Russian Research and Design Institute of Electric Locomotive Engineering], 2009, no. 2, pp. 260 – 264.

7. Smit D.J., Kennet Simpson J.L. *Funktsional'naya bezopasnost'. Prostoe rukovodstvo po primeneniyu standarta MEK 61508 i svyazannykh s nim standartov* [Functional safety. Simple guidance on the application of IEC 61508 and related standards]. Moscow, Izdatel'skiy Dom "Tekhnologii" Publ., 2004, 208 p.

8. P. Low, R. Pabst, E. Petry. *Funktionale Sicherheit in der Praxis. Anwendung von DIN EN 61508 und ISO/DIS 26262 bei der Entwicklung von Serienprodukten*, Dpunkt.verlag GmbH, 2010, 355 p. (in Germ.).

9. Shubinskiy I.B. *Metody obespecheniya funktsional'noy nadezhnosti program* [Methods of ensuring functional reliability program]. Nadezhnost' [Reliability], no. 4, 2014, pp. 87 – 94.

10. Repina I.B. *Uchet vliyaniya chelovecheskogo faktora na organizatsionno-tehnologicheskuyu nadezhnost' proizvodstvennykh protsessov infrastruktury zheleznnykh dorog*. Kand. tekhn. nauk diss. [The influence of the human factor on the organizational and technological reliability of production processes of infrastructure of railways. Cand. tehn. sci. diss.]. Novosibirsk, 2015, 211 p.

ABOUT THE AUTHORS

KUCHUMOV Vladislav Alekseyevich,

Dr. Sci. (Eng.), Professor, Chief Researcher, Department "Traction rolling stock", JSC "VNIIZhT"

MURZIN Roman Vilor'evich,

Cand. Sci. (Eng.), Head of Laboratory "Electric locomotives", Department "Traction rolling stock", JSC "VNIIZhT"

NIKIFOROVA Nina Borisovna,

Cand. Sci. (Eng.), Leading Researcher, Department "Traction rolling stock", JSC "VNIIZhT"

KHAZOV Maksim Sergeyevich,

Cand. Sci. (Eng.), Leading Researcher, Department "Traction rolling stock", JSC "VNIIZhT"

AKISHIN Aleksandr Aleksandrovich,

Cand. Sci. (Eng.), Leading Engineer, Department "Traction rolling stock", JSC "VNIIZhT"

Received 9.02.2016

Revised 20.04.2016

Accepted 25.04.2016

■ E-mail: khazov.maksim@vniizht.ru (M.S. Khazov)