УДК656.25

АНАЛИЗ НОРМАТИВНЫХ ПОКАЗАТЕЛЕЙ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ В СТАНДАРТАХ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ

В. Ф. КУСТОВ
Украинский государственный университет железнодорожного транспорта, г. Харьков

Одним из важнейших этапов доказательства безопасности систем железнодорожной автоматики (СЖА) является расчет нормативных показателей функциональной безопасности (ФБ), значения которых должны быть научно обоснованными. При этом необходимо учитывать, что более жесткие нормативы по ФБ будут приводить к усложнению разработки СЖА и к их удорожанию, а менее жесткие – приводить к железнодорожным авариям и катастрофам. В международных и европейских стандартах регламентируют допустимые вероятности опасных отказов в час или интенсивности опасных отказов в расчете на одну функцию безопасности, которые обозначают SIL1–SIL4 [1, 2]. Необходимо отметить, что для систем управления с малым числом функций безопасности эти требования могут быть приемлемыми, но при большом числе ответственных функций требования по ФБ к системе снижаются пропорционально их числу, т. к. невыполнение любой функции безопасности приводит к опасному состоянию всей системы в целом. Например, для микропроцессорных систем централизации стрелок и сигналов (МПЦ) в среднем на одну централизуемую стрелку приходится более десяти ответственных функций, поэтому для МПЦ с числом стрелок 100 европейские нормы по уровням полноты безопасности (SIL1–SIL4) будут в тысячу раз менее жесткими, чем требования вышеуказанных стандартов. Так, расчетная вероятность опасных отказов на систему МПЦ (1000 функций безопасности) для уровня SIL4 (10^{-9}–10^{-8}) согласно стандартов EN50129 и IEC 61508 [1, 2] за 10 лет работы составит 0,0839–0,5835, а за 20 лет работы – 0,1607–0,8266. Очевидно, что такие требования к СЖА являются недопустимыми и требуют пересмотра норм ФБ, приведенных в базовых стандартах EN и IEC.

В докладе предлагаются следующие методы обоснования нормативов ФБ [3].

1 Обоснование допустимой интенсивности опасных отказов функций безопасности по методу сравнения уровней безопасности с безопасностью железнодорожных реле 1-го класса надежности.

Учитывая, что релейные СЖА обеспечивают приемлемую безопасность движения поездов, а реле 1-го класса надежности успешно выполняют ответственные функции безопасности, допустимую интенсивность опасных отказов в расчете на одну функцию безопасности для наиболее жесткой нормы SIL4 можно установить по эксплуатационной (фактической) интенсивности опасных отказов реле 1-го класса надежности: $\lambda_{\text{оп.доп}} \le \lambda_{\text{оп.реле1}}$.

По данным эксплуатации за 5 лет на железных дорогах бывшего СССР у 16 млн электромагнитных реле 1-го класса надежности было зафиксировано девять опасных отказов, т.е. допустимая интенсивность опасных отказов функций безопасности составляет величину $\lambda_{\text{оп.доп}} \le 0{,}128 \cdot 10^{-10}$1/ч.

2 Обоснование допустимой интенсивности опасных отказов функций безопасности по методу сравнения с допустимым числом опасных отказов за определенный период эксплуатации систем.

Допустимая интенсивность опасных отказов для уровней безопасности SIL1–SIL4 определяется по допустимому числу опасных отказов за период эксплуатации систем:

$$\lambda_{\text{оп.доп}} = \frac{n_{\text{оп.доп}}(t)}{tN_{\text{оф}}}, \qquad (1)$$

где $n_{\text{оп.доп}}(t)$ – допустимое число опасных отказов функций безопасности за время t для каждого нормируемого уровня SIL1–SIL4; t – период эксплуатации системы; $N_{\text{оф}}$ – число функций безопасности при серийной эксплуатации систем (должно быть статистически достаточным для приемлемой доверительной вероятности получаемых результатов).

3 Обоснование допустимой интенсивности опасных отказов функций безопасности по методу полного исключения опасных отказов за определенный период эксплуатации системы.

Допустимая интенсивность опасных отказов ответственных функций для исключения опасных отказов за определенный период эксплуатации систем (появления менее 1-го опасного отказа) будет определяться следующим выражением:

$$\lambda_{\text{оп.доп}} \le \frac{1}{tN_{\text{оф}}}. \qquad (2)$$

Так, на железных дорогах Украины (14-е место в мире по протяженности железных дорог) эксплуатируется около 45 тысяч централизованных стрелок, соответственно 450 тысяч ответственных функций в системах управления стрелками и сигналами. Для исключения возможности появления в них опасных отказов за период эксплуатации 20 лет (175200 ч) допустимое их значение для нормируемого уровня SIL4, с учетом формулы (2), $\lambda_{\text{оп.доп}} = 0{,}127 \cdot 10^{-10} 1/\text{ч}$. Указанное значение является практически аналогичным результату, приведенном в п.1 и стандарте ДСТУ 4178 по ФБ.

4 Обоснование допустимой интенсивности опасных отказов функций безопасности по нормируемой интенсивности опасных отказов систем.

Межгосударственные стандарты (МГС) нормируют ФБ на систему в целом или условный измеритель, например, на малую или крупную железнодорожную станцию, систему путевой блокировки, 1 км протяженности линии, один переезд и т. п. Учитывая, что количество ответственных функций $N_{\text{оф}}$ в таких системах будет отличаться и даже значительно, предлагается определять допустимую интенсивность опасных отказов в расчете на одну функцию безопасности следующим образом:

$$\lambda_{\text{оп.доп}} \le \frac{\lambda_{\text{оп.доп.общ}}}{N_{\text{оф}}}, \qquad (3)$$

где $\lambda_{\text{оп.доп.общ}}$ – допустимая нормативная интенсивность опасных отказов в расчете на систему в целом или условный измеритель.

5 Обоснование допустимой интенсивности опасных отказов функций безопасности по методу замещения рисков.

Допустимую интенсивность опасных отказов функции безопасности предлагается определять на основании данных статистики числа опасных отказов эксплуатируемых систем с приемлемой для общества безопасностью:

$$\lambda_{\text{оп.доп}} \le \frac{n_{\text{оп.э}}(t)K}{100tN_{\text{оф.э}}}, \qquad (4)$$

где $n_{\text{оп.э}}(t)$ – число опасных отказов большого числа эксплуатируемых систем за определенный период эксплуатации t; K – процент опасных отказов функций безопасности, вызванных конструктивными особенностями комплектующих элементов, от общего числа опасных состояний системы по данным их эксплуатации; $N_{\text{оф.э}}$ – число ответственных функций, находящихся в эксплуатации (статистика должна обеспечить высокий уровень доверительной вероятности).

В докладе приводятся результаты расчета допустимой интенсивности опасных отказов функции безопасности для указанных методов с учетом межгосударственных, европейских и международных стандартов по функциональной безопасности СЖА, на основании которых дается вывод о недостатках нормативов ФБ в принятых стандартах и пути усовершенствования их.

В докладе приводятся результаты обоснования допустимой наработки до опасного отказа отдельных каналов резервирования СЖА в зависимости от всех возможных способов резервирования, допустимых уровнях ФБ, законах распределения опасных отказов каналов резервирования и максимально допустимых периодах диагностирования и устранения опасных отказов. Такой этап подтверждения ФБ на этапе эксплуатации позволяет выявить ошибки, объективно существующие на каждом этапе доказательства безопасности СЖА, и исключить катастрофические последствия, связанные с ними. В случае появления опасного отказа в любом отдельном канале резервирования

раньше допустимого нормативного значения принимается решение о недостоверности доказательства безопасности СЖА и срочном выявлении причин появления опасного отказа, которыми могут быть дестабилизирующие факторы, которые не были учтены в полной мере при вводе СЖА в эксплуатацию (неточные данные по безопасности комплектующих элементов, новые источники электромагнитных помех от мобильной связи, электротяги и т. п.).

Список литературы

1 IEC 61508-1:1998. Functional safety of electrical/electronic/programmable electronic safety-related systems. – Part 1: General requirements.

2 CENELEC-EN 50129. Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signaling, 2018.

3 Ensuring railroad's digital automation systems resistance to dangerous states / S. Panchenko [et al.] // ICTE in Transportation and Logistics. ICTE Tol 2019, LNITI. – 2020. – P. 120–128.

УДК 656.25

АВТОМАТИЗИРОВАННОЕ РАБОЧЕЕ МЕСТО ДЛЯ РАСЧЕТА И АНАЛИЗА ПАРАМЕТРОВ РЕЛЬСОВЫХ ЦЕПЕЙ

Д. Д. МЕДВЕДЕВ
Белорусский государственный университет транспорта, г. Гомель

Рельсовые цепи являются базовыми элементами современных систем железнодорожной автоматики и телемеханики, выполняя ответственные функции путевых датчиков и телемеханических каналов. Надежная работа рельсовых цепей во многом определяет нормальное функционирование систем железнодорожной автоматики и телемеханики, обеспечивая тем самым безопасность движения поездов и регулярность перевозочного процесса.

Надежная работа рельсовой цепи во всех режимах обеспечивается за счет правильного расчета параметров рельсовой цепи при определенных параметрах рельсовой линии и выполняется при проектировании и модернизации участков железной дороги.

При анализе и расчете рельсовых цепей предполагается, что рельсовая линия и элементы аппаратуры являются линейными, то есть их параметры не зависят от протекающих токов. Для упрощения расчетов рельсовых цепей представляют соответствующей математической моделью (схемой замещения) для каждого режима. В зависимости от вида применяемой схемы замещения различают четырехполюсные и многополюсные модели. Классический метод расчета основан на использовании четырехполюсных моделей [1, 2].

Разработанное автоматизированное рабочее место позволяет решить следующие задачи:

– выполнить расчет рельсовой цепи во всех режимах функционирования;

– построить регулировочные таблицы при новом проектировании или модернизации участка пути;

– анализировать выполнение требований функционирования рельсовой цепи во всех режимах для наихудших условий как элементов рельсовой цепи, так и параметров рельсовой линии;

– накапливать статистическую информацию о влиянии параметров элементов рельсовой цепи и рельсовой линии на надежность функционирования рельсовой цепи;

– хранить информацию о схеме замещения рельсовой цепи;

– хранить информацию о элементах, входящих в рельсовую цепь;

– оперативно строить и анализировать схемы замещения рельсовой цепи.

Автоматизированное рабочее место состоит из нескольких взаимосвязанных модулей.

Модуль ввода элемента в эквивалентную схему релейного или питающего конца позволяет добавлять в базу элементов новый четырехполюсник, частично отредактировать существующий (с ограниченными правами доступа редактирования). Выбрать существующий элемент из базы с параметрами его функционирования: частота, коэффициент трансформации и схема включения. Простейшие элементы, такие как индуктивность, сопротивление, емкость со схемами их включения, могут быть автоматически представлены в виде четырехполюсника с рассчитанными параметрами. Также автоматизированное рабочее место может быть дополнено модулем связи с микропроцес-