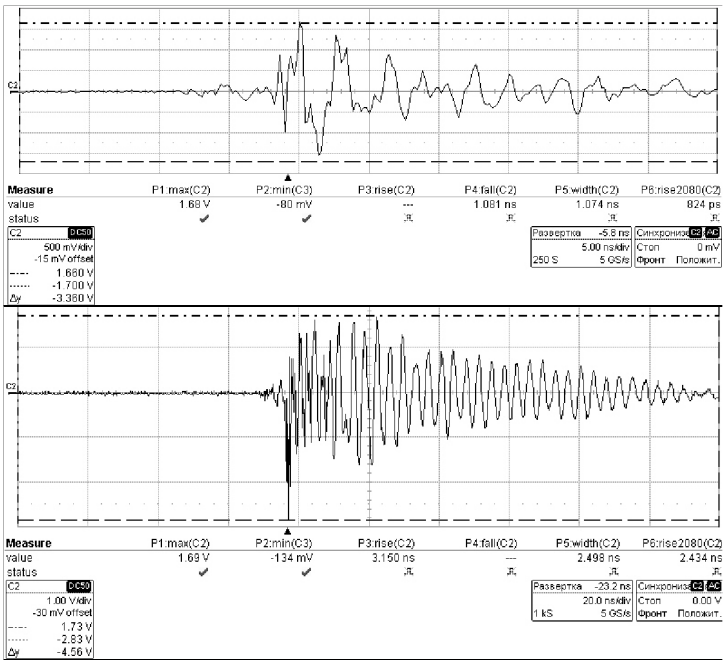

Рисунок 1 – Осциллограммы импульсов

Достоинство описанного метода определения порога чувствительности МСЖАТ с помощью генератора ЭСР заключается в том, что исходные данные для прогнозирования воздействия генераторов ЭИПВ можно получить без проведения разрушающих испытаний МСЖАТ с помощью уникальных дорогостоящих генераторов ЭИПВ.

Таким образом, третий метод, основанный на использовании условий эквивалентности импульсов помех и полученных аналитических моделей механизма проникновения электромагнитных наносекундных импульсов помех, позволяет на ранних этапах разработки и изготовления опытных образцов МСЖАТ прогнозировать их устойчивость к ЭИПВ и определять параметры периметров охраны объектов расположения МСЖАТ.

Список литературы

1 **Фоминич, Э. Н.** Электромагнитный терроризм. Новая угроза для информационно-управляющих систем / Э. Н. Фоминич, Д. Р. Владимиров // Военный инженер. – 2016. – № 2. – С. 10–17. – EDN YLYICP.

2 **Бочков, К. А.** Прогнозирование устойчивости микроэлектронных систем железнодорожной автоматики и телемеханики к электромагнитным импульсам преднамеренного воздействия / К. А. Бочков, Д. В. Комнатный, И. О. Жигалин // Вестник БелГУТа: Наука и транспорт. – 2022. – № 2(45). – С. 11–14.

3 **Бочков, К. А.** Элементы моделирования электромагнитной совместимости устройств железнодорожной автоматики и телемеханики / К. А. Бочков, Д. В. Комнатный. – Гомель : БелГУТ, 2013. – 185 с.

4 **Костин, А. В.** Методика измерения помех в цепях бортовой аппаратуры комических аппаратов, вызванных электромагнитным полем электростатического разряда / А. В. Костин, М. Н. Пиганов // Известия Самарского научного центра Российской академии наук. – 2015. – Т. 17, № 2-4. – С. 804–810. – EDN UMEJIL.

УДК 656.25

ПРОБЛЕМЫ ОЦЕНКИ ПОКАЗАТЕЛЕЙ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ СИСТЕМ ТЕХНИЧЕСКОГО ЗРЕНИЯ

К. А. БОЧКОВ, С. Н. ХАРЛАП
Белорусский государственный университет транспорта, г. Гомель

В настоящее время наблюдается активное использование систем технического зрения (СТЗ) в системах железнодорожной автоматики и телемеханики (СЖАТ). Типовыми задачами СТЗ являются: распознавание, идентификация, обнаружение, восстановление 3*D*-формы по 2*D*-изображениям, оценка траектории движения объекта. В СЖАТ решение этих задач может быть частью функций

безопасности, таких как обнаружение и распознавание препятствий движению железнодорожного транспорта, определение расстояния до препятствия, определение скорости и направления движения объектов, не выполнение которых может стать причиной опасного отказа системы автоматики.

Так как требования функциональной безопасности закреплены в соответствующих нормативных документах – МЭК 61508, *EN* 50126, *EN* 50129, ГОСТ 34012, являются обязательными для систем управления ответственными технологическими процессами, к числу которых относятся и СЖАТ, то для подтверждения выполнения этих требований разработчик предоставляет на экспертизу документ «Доказательство безопасности». Чаще всего требования функциональной безопасности задаются в виде уровня полноты безопасности (УПБ или *SIL*) и/или интенсивности либо вероятности опасных отказов.

Типовыми причинами нарушения требований функциональной безопасности, делающими невозможным выполнение функций безопасности, могут быть:

– отказы аппаратуры;

– искажения информации (при хранении или передаче);

– внешние влияния (электромагнитные, механические, климатические и т. д.), вызывающие отказы и сбои аппаратуры и искажения информации;

– ошибки человека при проектировании аппаратного и/или программного обеспечения;

– ошибки человека при эксплуатации оборудования.

Оценку влияния отказов принято выполнять по следующему алгоритму:

1 На основе анализа рисков, функциональной (принципиальной) схемы устройства, алгоритмов работы системы и средств диагностики выполняется анализ *FMECA*, в результате выполнения которого оцениваются последствия отказов (как одиночных, так и множественных). Последствия классифицируют по следующим категориям: опасные, защитные, обнаруживаемые и необнаруживаемые диагностикой, маскируемые (не влияющие на безопасность), отказы системы диагностики.

2 Строятся деревья опасных отказов (для каждой функции, критерия опасного отказа, отдельного функционального модуля или устройства в целом) и выполняется расчет интенсивности опасных отказов.

3 Выполняется оценка (сравнение с нормативными значениями для установленного УПБ или требованиями ТЗ).

Хотя алгоритм оценки влияния отказов хорошо проработан, но при практическом использовании очень часто возникают проблемы с определениями базовых интенсивностей отказов элементов, участвующих в расчетах показателей безопасности. Одной из распространенных ошибок разработчиков как раз и является желание все эти отказы оценить одним и тем же общим методом через вычисление интенсивности опасных отказов.

С интенсивностями отказов аппаратуры обычно проблем не возникает, т. к. их можно получить из различных источников: стандарта *MIL-HDBK*-217, справочника «Надежность ЭРИ», от производителей компонентов. Интенсивность искажений информации при передаче по различным интерфейсам также можно достаточно точно оценить на основании данных из нормативных документов и открытых источников. А вот с определением интенсивности ошибок человека при проектировании и при эксплуатации часто возникают проблемы.

Часто чтобы решить эти проблемы, разработчики начинают вводить множество допущений, пытаясь оценить такие отказы количественно (через интенсивность или вероятность отказов), используя в том числе различные статистические методы. Однако необходимо помнить, что статистические данные допускается использовать для обоснования (выбора) УПБ (например, принцип GAMAB), но не для подтверждения достигнутого уровня, т. к. в этом случае статистическая выборка предоставляет усредненное значение отказов для различных действующих систем, выполняющих аналогичные функции. Причем для новой разработки показатели ее работы не включены в выборку, т. к. для нее еще нет статистики отказов. А конкретная система может иметь показатели как значительно лучше, так и значительно хуже. Исключением является случай использования оборудования, для которого ранее уже был подтвержден УПБ.

Стандартом допускается использование адекватных статистических данных по отказам системы при эксплуатации (принцип «Доказано практикой»), однако, чтобы подтвердить достигнутый УПБ для доверительного интервала 70 %, необходимо продемонстрировать работу системы без опасных отказов в течение 12 лет для УПБ1 (12 тысяч лет для УПБ4), что для новой системы является недо-

стижимым. Поэтому такое применение статистических методов для оценки функциональной безопасности некорректно.

Рассмотрим теперь систему технического зрения, применяемую для выполнения функций безопасности, например, для обнаружения препятствий перед транспортным средством. В общем случае система технического зрения с точки зрения функциональной безопасности состоит из следующих функциональных модулей:

– датчики (камеры, радары, лидары и т. д.);

– устройства первичной обработки информации, выполняющие фильтрацию первичных данных и позволяющие исключить из дальнейшей обработки объекты, обнаруженные вне контролируемой зоны и иные постоянно обнаруживаемые объекты, характерные для конкретного применения, например, определенные объекты инфраструктуры, набор которых определяется на этапе начальной калибровки системы технического зрения;

– устройства обработки информации, которые выполняют функции классификации обнаруженного объекта (нейронная сеть), вычисления количественных характеристик (расстояние, местоположение, скорость и направление движения и т. д.);

– устройство управления, которое принимает решение о наличии препятствия (т. е. является ли препятствием обнаруженный объект или нет).

При этом критерием опасного отказа является необнаружение (пропуск) препятствия в зоне контроля при его фактическом наличии в этой зоне.

Рассмотрим возможные отказы функциональных модулей, которые могут привести к опасному отказу. Условно все эти отказы можно разделить на две категории:

– случайные отказы, например, аппаратный отказ датчика, искажения информации, отказы по общей причине;

– систематические отказы, возникающие до установки или в период установки системы, например, неправильный выбор датчиков, неправильная установка датчика, ошибки в программном обеспечении датчика, недостаточность средств защиты информации от искажений, и систематические отказы, возникающие во время эксплуатации, например, неверные конфигурационные данные, изменение параметров установки датчика.

При определении уровня полноты безопасности должны учитываться все причины отказов как случайных, так и систематических. В связи с этим, общая оценка соответствия системы требованиям функциональной безопасности заключается в проверке как соответствия количественных показателей (интенсивности случайных опасных отказов), так и соответствия применяемых мер защиты от систематических отказов (стойкость к систематическим отказам (*systematic capability*).

При этом надо помнить, что методы оценки показателей функциональной безопасности для случайных и систематических отказов значительно отличаются. Это связано с тем, что стандарт декларирует, что систематические отказы (влияние человеческого фактора) невозможно оценить количественно. Защита от систематических отказов обеспечивается на качественном уровне за счет выполнения различных мероприятий на разных стадиях жизненного цикла, начиная с анализа рисков и заканчивая подтверждением соответствия и приемкой в эксплуатацию, что закреплено в специальном документе «Программа обеспечения безопасности». Соответственно для каждой категории в соответствии с МЭК61508 необходимо применять разные группы методов защиты и желательно их не смешивать между собой.

Все мероприятия по защите от систематических отказов в соответствии с МЭК 61508 (приложения А и В) имеют рекомендации по применению для различных уровней УПБ (*M, HR, R, NR*) и требуемый уровень эффективности (*L, M, H*). Соответственно процедура подтверждения соответствия УПБ состоит в том, что разработчик должен подтвердить применение всех рекомендованных стандартом для этого УПБ методов и средств по защите от систематических отказов.

К сожалению, для систем технического зрения практически невозможно выполнить разработку «с нуля». В любом случае будут использоваться готовые изделия сторонней разработки: камеры, лидары, нейронные сети, вычислители и т. д. Соответственно систематические ошибки в этих изделиях будут зависеть от тех мероприятий, которые выполнял их разработчик, и повлиять на них в сторону усиления мы уже не можем. Таким образом, эти изделия уже имеют собственный УПБ, который и надо учитывать при подтверждении соответствия всей системы в целом.

При этом надо учитывать, что МЭК 61508 прямо говорит, что одноканальное исполнение без специальных архитектурных решений может обеспечить максимум УПБ2. Поэтому разработки сторонних организаций (если обратное не подтверждается соответствующим сертификатом) не могут иметь УПБ выше УПБ2 (а чаще ограничиваются УПБ1). Достижение более высокого УПБ должно базироваться на специальных архитектурных методах, например, дублировании. Однако при этом надо помнить, что если несколько элементов с различными УПБ участвуют в выполнении функции безопасности последовательно, то результирующий УПБ будет равен наименьшему УПБ.

Повысить УПБ можно, только используя многоканальное построение (например, дублирование). В этом случае УПБ системы в наилучшем случае (при выполнении всех мероприятий по защите от систематических отказов) может достигать суммы УПБ отдельных каналов. Но при этом следует учитывать, что на результат оказывают сильное влияние отказы по общей причине. В многоканальной структуре такие отказы принято считать опасными. Интенсивность отказов по общей причине обычно составляет 1–5 % от интенсивности опасных отказов аналогичной одноканальной системы, поэтому без дополнительных мероприятий максимум чего можно достичь, это увеличения большего УПБ на единицу. Дополнительного повышения УПБ можно достичь, например, применением диверситета, который позволяет значительно снизить влияние отказов по общей причине на общую безопасность системы.

Таким образом, можно сформулировать основные подходы к оценке показателей функциональной безопасности систем технического зрения:

1) оценка правильности выбора УПБ системы и компонентов, оценка полноты и корректности критериев опасных отказов и требуемых количественных показателей функциональной безопасности (могут быть использованы статистические методы, например, принцип GAMAB, и требования нормативных документов);

2) оценка полноты перечня мероприятий по защите от систематических отказов, выполняемых на каждом этапе ЖЦ (для системы в целом в соответствии с установленным УПБ);

3) оценка корректности определения УПБ сторонних компонентов (при отсутствии сертификата – не более УПБ2), и оценка полноты перечня мероприятий по защите от систематических отказов на уровне отдельных разрабатываемых компонентов (в соответствии с установленным УПБ для компонента);

4) оценка влияния систематических отказов для системы, определение стойкости к систематическим отказам (*systematic capability*);

5) оценка влияния случайных отказов (выполнение анализа *FMECA*, построение деревьев отказов и расчет количественных показателей функциональной безопасности на уровне одноканальных компонентов);

6) оценка влияния отказов по общей причине для многоканальных компонентов;

7) оценка влияния случайных отказов для системы в целом (расчет общих количественных показателей функциональной безопасности и сравнение количественных показателей с нормативными значениями для установленного УПБ или требованиями технического задания);

8) принятие решения о соответствии системы заданному УПБ (стойкость к систематическим отказам соответствует УПБ, количественные показатели соответствуют УПБ).

УДК 621.314

ДИАГНОСТИКА ТРАНСФОРМАТОРОВ С ПОМОЩЬЮ НЕЙРОННЫХ СЕТЕЙ

И. Л. ГРОМЫКО, Д. В.МИРОШ, К. Я. ШАБЛОВСКИЙ, И. Е. МОНАРХОВИЧ
Белорусский государственный университет транспорта, г. Гомель

На сегодняшний день более 50 % трансформаторов системы электроснабжения железнодорожной отрасли страны отработали 25 лет – установленный согласно [1] срок службы. Многие из таких трансформаторов могут эксплуатироваться еще длительное время, однако в этом случае должны предъявляться повышенные требования к методам диагностики их технического состояния.