В заключение следует отметить, что для эффективной оценки рисков кибератак достаточно обоснованным является использование методов анализа риска, получивших широкое применение при оценке функциональной безопасности. В частности, можно воспользоваться матрицей рисков, для составления которой необходимо предварительно выявить последствия и частоты наступления опасных событий. Для повышения эффективности оценки рисков необходимо совершенствовать способы оценки частот опасных событий.

Список литературы

1 PDCLC/TS 50701:2023 Railway applications. Cybersecurity. – BSI, 2023. – P. 164.

2 **Гордейчик, С. В.** Кибербезопасность микропроцессорных систем управления на железнодорожном транспорте / С. В. Гордейчик. – М. : Горячая линия – Телеком, 2021. – 120 с.

3 ГОСТ 33433–2015. Безопасность функциональная. Управление рисками на железнодорожном транспорте. – Введ. 2016-09-01. – М. : Стандартинформ, 2020. – 34 с.

4 Bug Bounty [Электронный ресурс] // Википедия. Свободная энциклопедия. – Режим доступа : https://ru.wikipedia.org/wiki/Bug_Bounty. – Дата доступа : 10.10.2024.

УДК 681.5.09

ПОДХОДЫ К ДОКАЗАТЕЛЬСТВУ БЕЗОПАСНОСТИ ИННОВАЦИОННЫХ СИСТЕМ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ, ТЕЛЕМЕХАНИКИ И СВЯЗИ

Н. А. БОЯРИНОВА, Н. Г. ПЕНЬКОВА, В. В. БАТРАЕВ, Е. С. РОДИМАНОВА
Научно-исследовательский и проектно-конструкторский институт информатизации, автоматизации и связи на железнодорожном транспорте (АО «НИИАС»), г. Москва, Российская Федерация

Стратегия и методология доказательства функциональной безопасности беспилотных систем управления движением на железнодорожном транспорте находится в начальной стадии развития как в России, так и за рубежом. Кроме того, информационных материалов по этой теме значительно меньше, чем в автомобильной отрасли.

Действующая в области железнодорожной автоматики нормативная база предполагает в качестве обязательного условия для допуска системы, отвечающей за безопасность движения, в опытную и постоянную эксплуатацию наличие положительного независимого экспертного заключения по документу «Доказательство безопасности». Назначение Доказательства безопасности, а также основные требования к порядку его разработки, структуре и содержанию определены в межгосударственном стандарте ГОСТ 33432–2015 «Безопасность функциональная. Политика, программа обеспечения безопасности. Доказательство безопасности объектов железнодорожного транспорта». В соответствии с указанным стандартом обозначенный документ предназначен для аккумулирования всей совокупности материалов доказательного характера и отражения результатов работ по обеспечению требований безопасности на всех этапах жизненного цикла.

В процессе разработки системы управления движением поездов на Московском центральном кольце (МЦК) специалисты АО «НИИАС» столкнулись с отсутствием в действующих стандартах требований безопасности к некоторым новым функциям. Вопросы обеспечения функциональной безопасности хорошо развиты для традиционных систем микропроцессорной централизации, автоблокировки, локомотивной сигнализации. Для инновационных систем вопросы нормирования показателей безопасности и доказательства их выполнения проработаны не достаточно. Текущее исследование посвящено методам и подходам, которые могут быть использованы для доказательства безопасности систем, требования к которым не определены в нормативных документах отрасли.

В качестве примера рассматриваются системы интервального регулирования с использованием технического зрения, включая 4-й уровень автоматизации по ГОСТ Р 70059–2022 « Национальный стандарт Российской Федерации. Системы управления и контроля железнодорожного транспорта для перевозок пассажиров в пригородном сообщении. Принципы построения и основные функциональные требования».

Всего существует 4 уровня автоматизации (УА). Причем первые два уровня – частичная и условная автоматизация – широко развиты и применяются на железных дорогах (например, системы автоведения), в то время как перед разработчиками систем с УА3 (уровень, когда машинист находится в локомотиве) и УА4 (уровень, когда движение полностью автономно) стоит сложнейшая задача создания эффективных современных методов обеспечения и доказательства безопасности, которые полностью гармонизированы с принятыми принципами нормирования безопасности, правилами и стандартами разработки и внедрения систем.

Система управления движением на МЦК обладает множеством сценариев эксплуатационной работы, как технологических, так и ситуационных. Первым шагом разработки системы с УА4 был пересмотр всего технологического процесса ввиду отсутствия машиниста в кабине. При традиционном способе управления движением на машиниста было возложено выполнение множества функций и ответственность за их реализацию. При исключении оператора движения и переходе на уровень автоматизации 4 ответственность за выполнение данных функций легла на автоматику. Среди сценариев эксплуатационной работы были выделены те, где выполнение части функций машиниста было возложено на системы, в том числе использующие техническое зрение.

В результате для реализации беспилотного вождения на МЦК была создана многоуровневая система управления движением. Для 4-го уровня автоматизации она представляет собой многокомпонентный комплекс, подсистемы которого работают в условиях большого количества взаимосвязей. Каждая подсистема системы управления движением на МЦК в автоматическом режиме включает в себя множество различных датчиков, поэтому требуется выполнение комплексного анализа для принятия единого решения по данным от всех элементов. Вопросы надежности датчиков и правильности алгоритмов обработки данных напрямую связаны с выдачей конечного результата для обеспечения функциональной безопасности.

Предваряющим этап подтверждения безопасности является процесс установления требований безопасности как для каждой подсистемы в целом, так и для её составных частей. Требования безопасности к некоторым, ранее выполняемым машинистом, функциям, таким как обнаружение препятствия и людей на пути следования, контроль закрытия дверей при посадке пассажиров, не были нормированы в действующих стандартах, поэтому стояла задача по их определению. Для этого был проведен анализ рисков.

Анализ рисков для инновационных систем, в том числе использующих техническое зрение, – это комплексный процесс, направленный на выявление, оценку и контроль потенциальных угроз безопасности, надежности и эффективности работы системы в конкретной середе.

При нормировании требований к подсистемам технического зрения прежде всего необходимо определить допустимый уровень риска с учетом вида ущерба, возникающего в результате отказа системы. В случае если ущерб является материальным (повреждение объектов инфраструктуры, нарушение графика движения), то в качестве допустимого принимается ущерб, вычисленный по статистическим данным о происшествиях с аналогичными последствиями или приемлемый для заказчика. В случае если ущербом является травмирование или гибель человека (пассажиров, работников железных дорог), то нормирование риска производится по принципу МЕМ (минимальной эндогенной смертности).

Опыт применения для нормирования метода МЕМ показал, что существенным аспектом при его использовании в системах, в том числе с техническим зрением, является частота возникновения неблагоприятного сценария, которая тесно связана с конкретной средой эксплуатации данной системы. В частности с пассажиропотоком, состоянием инфраструктуры, доступностью попадания человека на путь следования поезда и т. п.

В результате анализа рисков подсистемы технического зрения получены следующие требования к допустимой частоте отказов – вероятность необнаружения человека не должна превышать 10^{-2} для каждого типа датчика. Следует отметить, что это значение не коррелируется с определенными в стандарте ГОСТ Р МЭК 61508–2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью» количественными показателями для уровня полноты безопасности УПБ4, хотя по значению ущерба от отказов данная подсистема должна классифицироваться как система с самым высоким уровнем безопасности УПБ4. То есть в некоторых случаях оправдан подход, когда интенсивность опасного отказа изделия не привязывается к количественным показателям УПБ, при этом методы по защите от систематиче-

ских отказов применяются для того УПБ, который определен тяжестью ущерба, в нашем случае для подсистемы технического зрения это УПБ 4.

Если для систем, использующих жесткую логику для определения частоты нежелательного события, можно было воспользоваться традиционными вероятностными расчетами надежности и безопасности исходя из структуры изделия, то для систем, использующих техническое зрение, потребовалось применить расчетно-экспериментальный метод. Это вызвано необходимостью оценки эффективности работы алгоритмов работы нейронных сетей, которую можно выполнить только путем проведения испытаний и получения выборки достаточного объема.

В ходе планирования испытаний был рассмотрен каждый конкретный сценарий эксплуатации исследуемой системы и определены возможные опасности, свойственные данному сценарию. Это позволило при проведении испытаний смоделировать конкретную ситуацию для сбора статистики по способности системы снижения риска реализации данной опасности в реальной среде, а именно на Московском центральном кольце, с целью подтверждения соответствия требованиям.

Таким образом, используя метод МЕМ и полученную статистику, мы выполнили нормирование требований безопасности к системе технического зрения в конкретном сценарии и сформировали минимальное требование к подсистеме, удовлетворяющее всем сценариям, а также подтвердили выполнение этих требований. Опыт применения данного метода показал, что он может быть использован в инновационных системах, для которых стандартизованные требования безопасности отсутствуют.

УДК 62-567.5:536.7

ВНЕДРЕНИЕ МОБИЛЬНОГО РАБОЧЕГО МЕСТА КАК ФАКТОР ПОВЫШЕНИЯ БЕЗОПАСНОСТИ УСЛОВИЙ ТРУДА РАБОТНИКОВ ХОЗЯЙСТВА АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ

Ю. А. ГЕНВАРЕВА, О. Ю. МАЛАХОВА
Оренбургский институт путей сообщения – филиал Приволжского государственного университета путей сообщения, Российская Федерация

Надежность устройств железнодорожной автоматики и телемеханики носит приоритетный характер, определяет степень безопасности производственного процесса для персонала и окружающей среды. Для осуществления технического процесса ремонта и обслуживания устройств для каждого предприятия железнодорожного транспорта разрабатываются свои графики и вводятся системы диагностики. Современные тенденции цифровизации и автоматизации применяются не только в повседневной нашей жизни в качестве использования гаджетов и всевозможных приложений, но и активно внедряются в производственную сферу.

На сегодняшний день в большинстве дистанций хозяйства автоматики и телемеханики график обслуживания устройств не автоматизирован, а реализуется на бумажном носителе. В данной научной статье нами рассматривается вопрос внедрения мобильного рабочего места (МРМ) электромеханика хозяйства автоматики и телемеханики. Благодаря мобильному рабочему месту работники могут получать информацию о состоянии оборудования в реальном времени, проводить диагностику и обслуживание удаленных объектов без необходимости нахождения на месте. Это позволяет избежать опасных ситуаций и минимизировать риск возникновения чрезвычайных ситуаций. Важным преимуществом мобильного рабочего места выступает быстрый доступ к инструкциям по безопасной эксплуатации оборудования. Работники получают возможность быстро реагировать на любые потенциально опасные ситуации и принимать необходимые меры по предотвращению аварий.

Мобильное рабочее место электромеханика устройств сигнализации, централизации и блокировки (СЦБ) (МРМ) является одним из средств обслуживания пути и устройств СЦБ, что подразумевает практическое внедрение цифровых технологий в хозяйстве автоматики и телемеханики в части:

– совершенствования технологических процессов хозяйства;
– минимизации рутинных операций;
– соблюдения норм содержания технических средств;
– обеспечения автоматизированного контроля за выполнением работ.