

Автономное вождение. О способах применения принципов безопасности

Хендрик Шебе, TÜV Rheinland InterTraffic GmbH, Кельн, Германия



Хендрик Шебе

Резюме. В статье обсуждаются принципы обеспечения безопасности автономного вождения автомобилей. Прежде всего, мы проводим сравнение между принципами и опытом применения автономных или автоматических систем на железнодорожном и автодорожном транспорте. Автоматические поезда метро эксплуатируются в контролируемой и четко определенной среде, пассажиры и посторонние лица отделены от поездов ограждениями, туннелями и т.д. Автомобиль эксплуатируется в гораздо более сложной среде. Далее мы затрагиваем принципы безопасности. Применение принципов обеспечения безопасности (например, отказоустойчивость или безопасный ресурс) обеспечивает разработку и реализацию безопасной системы, которая будет соответствовать положениям стандартов функциональной безопасности. Различия в ответственности живого водителя и технической системы управления на разных уровнях автоматизации процесса вождения требуют применения принципов обеспечения безопасности. Мы рассматриваем подлежащие применению принципы обеспечения безопасности исходя из общих принципов обеспечения безопасности и анализа соответствующего уровня автоматизации по классификации SAE на основе опыта осуществления ряда проектов, предусматривавших реализацию пяти уровней автоматизации вождения согласно классификации SAE. В зависимости от уровня автоматизации технические системы реализуются на основе принципов отказа без последствий, отказоустойчивости или безопасного ресурса.

Ключевые слова: архитектура безопасности, автономное вождение, автомобили.

Формат цитирования: Шебе Х. Автономное вождение. О способах применения принципов безопасности // Надежность. 2019. №3. С. 21-33. DOI: 10.21683/1729-2646-2019-19-3-21-33

Введение

Средства автономного управления автомобилем [2] набирают популярность. Первые системы-демонстраторы уже находятся в эксплуатации [4, 10, 21]. При этом автоматические поезда метро и системы транспортировки людей успешно работают уже много лет.

В настоящей статье мы сравниваем различные уровни автоматизации согласно классификациям UITP [23] и SAE [22] и их влияние на работу системы в целом. Также рассматриваются резервные ручные режимы вождения.

Для автомобильного транспорта в настоящее время доступно множество систем содействия, способных справиться с рядом конкретных ситуаций. Может создаться впечатление, что такие автомобили действуют самостоятельно.

В большинстве случаев автомобили эксплуатируются в гораздо более сложной среде, чем поезда.

Мы приводим описание различий в процедурах допуска для поездов метро, автомобилей и так называемых автоматически управляемых транспортных средствах (АУТС). Рассмотрены юридические требования допуска автомобилей согласно положениям Конвенции о дорожном движении, а также их влияние на свойства системы и поведение водителя.

Автономное вождение к настоящему времени стало важным предметом исследования; осуществляются первые пилотные проекты. В технологиях обеспечения безопасности применение принципов обеспечения

безопасности, например, отказоустойчивости или безопасного ресурса, представляет собой весьма важный инструмент при разработке и реализации безопасной системы, которая будет соответствовать положениям стандартов функциональной безопасности. Принципы обеспечения безопасности для управляемых транспортных систем, в том числе с нематериальными системами наведения, описаны и применяются.

В более ранних работах принципы обеспечения безопасности были описаны и затем применены к управляемому вождению.

В настоящей статье мы проводим систематическое рассмотрение того, какие принципы обеспечения безопасности необходимо применять на различных уровнях систем автономного вождения по SAE, а также показываем способы построения автономной системы. Работа была проведена отчасти на основе общих принципов обеспечения безопасности, отчасти – путем анализа соответствующих уровней SAE на основе опыта реализации ряда проектов.

Согласно резолюции ООН [24] или SAE [22], средства автономного вождения автомобилей классифицируются по пяти различным уровням:

- 0 – Без автоматизации;
- 1 – Помощь водителю;
- 2 – Частичная автоматизация;
- 3 – Условная автоматизация;
- 4 – Высокая степень автоматизации;
- 5 – Полная автоматизация.

На уровнях с 0 по 2 водитель несет полную ответственность за вождение. Начиная с уровня 3, состояние транспортного средства контролируется оборудованием автоматизированного вождения.

Данное различие в мере ответственности между живым водителем и технической системой управления требуют применения принципов обеспечения безопасности. В настоящей статье мы проводим систематическое рассмотрение того, какие принципы обеспечения безопасности необходимо применять на различных уровнях и показываем способы построения такой системы.

Эта задача решается отчасти на основе общих принципов обеспечения безопасности, отчасти – путем анализа соответствующих уровней.

В качестве отправной точки мы используем абстрактную модель системы и показываем, что существует ряд различных возможностей реализации автономного вождения. К важным выводам можно отнести необходимость наличия схемы разрешения конфликтов, которая обеспечивала бы возможность отмены живым водителем решений автономной системы в целях выполнения юридических требования.

Для каждого из пяти уровней автоматизированного вождения согласно классификации SAE [22] в статье выводятся свои принципы обеспечения безопасности. На уровнях с 0 по 2 водитель несет полную ответственность за вождение, но, начиная с уровня 3, состояние транспортного средства контролируется оборудованием автоматизированного вождения. Для того чтобы обеспечить водителю возможность вмешаться в процесс управления, система должна отвечать соответствующему уровню полноты обеспечения безопасности, а у водителя должно быть достаточно времени для перехвата управления. Последнее в значительной мере зависит от уровня автоматизации и скорости, а также окружающей обстановки.

В зависимости от уровня автоматизации технические системы реализуются на основе принципов отказа без последствий или безопасного ресурса. Есть также исключения – технические системы, реализованные на основе принципа отказоустойчивости, при котором автомобиль всегда можно безопасно остановить, например, при движении с малой скоростью или на технически адаптированном участке.

Мы рассматриваем две основных функции – управление и торможение/ускорение – и их роль применительно к автономному вождению. Кроме того, освещены вопросы обнаружения и реагирования на подвижные и неподвижные препятствия.

Согласно двум основополагающим требованиям к автономным системам, они должны быть разработаны в соответствии с положениями действующих стандартов функциональной безопасности и отвечать требованиям определенного уровня УПБА, т.е. уровень полноты безопасности автомобильный ASIL (или УПБ т.е. уровень полноты безопасности SIL), а технические возможности системы автономного вождения должны быть, по меньшей мере, не хуже аналогичных способностей живого водителя.

Отметим, что Вахенфельд [26] предлагает стохастический подход для демонстрации соответствия автономной системы определенному уровню функциональных возможностей или безопасности. Это, однако, может рассматриваться в качестве дополнительных доводов. В качестве основного доказательства безопасности системы выступает соответствующая архитектура безопасности, реализованная согласно правилам функциональной безопасности (см. ИСО 26262 [17]).

В настоящей статье мы проводим общий обзор существующих технических возможностей и технических решений автоматизированного вождения. Особое внимание уделено возможностям и ограничениям искусственного интеллекта. Мы также приводим общий план дальнейших действий.

Текущее состояние вопроса применительно к метрополитенам, системам транспортировки людей и автомобилям

2.1. Метрополитены и системы транспортировки людей

Во многих городах уже эксплуатируются автоматизированные поезда метро и системы транспортировки людей.

Приведем несколько примеров:

- Линия «Канарси» оператора Brooklyn-Manhattan Transit Corporation Нью-Йоркского метрополитена;
- Линии «Центральная», «Северная», «Джубили» и «Виктория» Лондонского метрополитена, на которых реализовано автоведение;
- В метрополитене Нюрнберга существующая линия U2 и новые линии U3 переоборудованы с реализацией автоведения;
- В метрополитене Барселоны на линиях L9 (самая длинная в Европе линия автономного движения), L10 и L11 реализовано автоведение;
- Группа Rio Tinto получила разрешение на введение автономного управления на своей железорудной линии;
- Система Tren Urbano (Сан-Хуанский метрополитен, Пуэрто-Рико) оборудована комплексом автоматизированного управления Siemens, которая обеспечивает эксплуатацию подвижного состава в полностью автоматическом режиме;
- Система SkyTrain в г. Ванкувере;
- Система Skyline Аэропорта Франкфурта-на-Майне;
- Копенгагенский метрополитен;
- В Миланском метрополитене на красной линии M1 реализовано автоведение;
- В Системе скоростного транспорта Сингапура на всех действующих линиях с 1987 функционируют средства автоведения.

На метрополитенах и системах транспортировки людей реализован принцип разграничения: Автоматизированные поезда отделены от всего прочего движения, они передвигаются в тоннелях, открытые участки пути

огорожены, на платформах пассажиры отделены от поездов автоматическими дверями. Это значительно упростило условия эксплуатации.

Автоматизированная система управления и обеспечения безопасности движения поезда (АСУБДП) используется для предотвращения столкновений и сходов с рельсов. Ее использование также позволяет эксплуатировать поезда с ручным управлением на той же сети.

Нормальным требованием безопасности для АСУБДП является соответствие четвертому уровню полноты безопасности (УПБ 4). При этом предусматривается наличие резервных ручных режимов управления. На борту присутствуют проводники для оказания помощи пассажирам, особенно в случае эвакуации.

Для метрополитенов и систем транспортировки людей UITP [24] установил 5 уровней автоматизации. Это означает, что между ручным и автоматизированным вождением существует еще ряд вариантов. Автоматизация представляет собой поэтапный процесс. UITP [24] установлено пять следующих уровней:

- УА 0: управление поездом по условиям видимости подобно тому, как трамвай передвигается по улице (Полное отсутствие автоматизации);

- УА 1: ручное ведение поезда, при котором машинист управляет началом и прекращением движения, дверьми, а также отвечает за реагирование на чрезвычайные происшествия и иные непредвиденные обстоятельства;

- УА 2: полуавтоматическое ведение поезда (ПАВП), при котором начало и прекращение движения автоматизированы, а машинист управляет дверьми, по необходимости осуществляет ведение поезда и отвечает за реагирование на чрезвычайные происшествия. Многие системы автоведения соответствуют уровню УА 2;

- УА 3: безэкипажное ведение поезда (БЭВП), при котором начало и прекращение движения автоматизированы, при этом проводник управляет дверьми и в крайних случаях осуществляет ведение поезда;

- УА 4: безлюдное ведение поезда (БЛВП), при котором управление началом и прекращением движения, дверьми, а также реагирование на чрезвычайные происшествия полностью автоматизированы при полном отсутствии поезда бригады.

Дополнительно отметим, что автоматические поезда метро и системы транспортировки людей UITP могут рассматриваться в качестве полностью сложившихся транспортных средств. При этом нельзя упускать из виду, что они эксплуатируются в простых и контролируемых условиях.

2.2. Автомобили

Необходимо различать две ситуации:

- а) движение по дороге и
- б) движение по частной территории.

Не останавливаясь на вопросе подробно, отметим лишь необходимость понимать, что при движении по дороге согласно требованиям Конвенции водитель обязан постоянно находиться в автомобиле, что отражено в национальных законодательствах почти всех стран

мира. Правила дорожного движения не распространяются на частные территории. Автомобиль считается самодвижущейся машиной. Тем не менее, в такой эксплуатационной среде также необходимо придерживаться определенных правил безопасности. Упомянутый тип транспортных средств называется автоматически управляемыми транспортными средствами (АУТС).

Общее представление о том, как работает автономное вождение, в значительной мере было определено автомобилями Google [14] и Tesla [9], а также другими системами, появившимися в тот же период. К более простым системам относятся средства автоматизированной парковки, которая осуществляется водителем, находящимся вне автомобиля, при помощи мобильного телефона. Исследования автономного вождения проводились в присутствии водителя в автомобиле в целях испытания или демонстрации. В закрытых зонах или в составе промышленных транспортных систем также применяются автоматически управляемые транспортные средства. Последние в строгом смысле этого слова – не автомобили, а самодвижущиеся машины.

В качестве примера можно рассмотреть автомобиль Google [14]. Он представляет собой двухместное транспортное средство наподобие Smart, по виду которого можно легко судить о том, что оно управляется автономно.

К сожалению, имело место дорожно-транспортное происшествие, и Google заявил, что несет «некоторую долю ответственности» после того, как автомобиль столкнулся с рейсовым автобусом в Маунтин-Вью, шт. Калифорния [14]. Это значит, что столкновение произошло по вине автомобиля Google. В таком случае ответственность лежит на автомобиле и, соответственно, его изготовителе. Однако водителя и его ответственность также нельзя оставлять без внимания.

Еще один пример – автомобиль Tesla, врезавшийся в грузовой полуприцеп. Водитель, положившись на систему автоматизированного вождения, не среагировал на ситуацию и погиб в результате столкновения. Важно, что система вождения автомобиля Tesla оказалась неспособна обнаружить полуприцеп. Встает вопрос о том, кто несет ответственность за ДТП. Безусловно, водитель был должен постоянно наблюдать за поведением автоматической системы, и не известно, был ли он достаточно хорошо проинструктирован. Также необходимо обсудить, имел ли водитель возможность остановить автомобиль или перехватить управление. В данном контексте помимо свойств технической системы необходимо также рассматривать время реакции человека.

SAE [22] и ООН [24] выделяют следующие уровни.

- 0 – Без автоматизации;
- 1 – Помощь водителю;
- 2 – Частичная автоматизация ;
- 3 – Условная автоматизация;
- 4 – Высокая степень автоматизации;
- 5 – Полная автоматизация.

Подробные сведения по уровням приведены в Таблице 1.

Таблица 1 – Обзор уровней автоматизации [22]

Уровень по SAE	Наименование	Словесное определение	Рулевое управление и ускорение/торможение	Контроль органов управления	Резервирование функций вождения	Возможность системы (режимы вождения)
Живой водитель наблюдает дорожную обстановку						
0	Без автоматизации	Непрерывное выполнение живым водителем всех составляющих динамического процесса вождения даже при наличии систем оповещения и вмешательства	Живой водитель	Живой водитель	Живой водитель	нет сведений
1	Помощь водителю	Выполнение системой содействия водителю управления направлением движения или ускорением/торможением в зависимости от текущего режима вождения на основе информации о дорожной обстановке. Предполагается, что живой водитель выполняет все остальные составляющие динамического процесса вождения	Живой водитель и система	Живой водитель	Живой водитель	Некоторые режимы вождения
2	Частичная автоматизация	Выполнение одной или несколькими системами содействия водителю и управления направлением движения и ускорением/торможением в зависимости от текущего режима вождения на основе информации о дорожной обстановке. Предполагается, что живой водитель выполняет все остальные составляющие динамического процесса вождения	Система	Живой водитель	Живой водитель	Некоторые режимы вождения
Автоматизированная система вождения («система») контролирует органы управления автомобиля						
3	Условная автоматизация	Выполнение автоматизированной системой вождения управления всеми составляющими динамического процесса вождения. Предполагается, что живой водитель должным образом отреагирует на требование вмешаться	Система	Система	Живой водитель	Некоторые режимы вождения
4	Высокая степень автоматизации	Выполнение автоматизированной системой вождения управления всеми составляющими динамического процесса вождения, даже если живой водитель должным образом не реагирует на требование вмешаться	Система	Система	Система	Некоторые режимы вождения
5	Полная автоматизация	Непрерывное выполнение автоматизированной системой вождения всех составляющих динамического процесса вождения при любой дорожной обстановке, с которой может справиться живой водитель	Система	Система	Система	Все режимы вождения

Существующие в настоящее время системы преимущественно предназначены для помощи водителю. Система содействия помогает в простых ситуациях, однако ответственность всегда лежит на водителе. Приведем несколько примеров:

- Помощь в соблюдении дистанции;
- Формирование автоколонн;
- Помощь в движении по полосе;
- Шоссейный автопилот для грузовиков.

Беглого взгляда достаточно для того, чтобы заметить различия в процедурах допуска:

- Автоматизированные поезда метро оцениваются согласно положениям стандартов EN 50126 [6], EN 50128 [7], EN 50129 [8], а допуск получают согласно местным законодательным актам о метрополитенах, которые в каждой стране свои;

- В странах Европейского Союза автомобили получают Европейское разрешение на эксплуатацию согласно правилам ЕСЕ. В Германии эти задачи возложены на Федеральное управление по вопросам транспортных средств (КВА), в Нидерландах – на Государственную службу дорожного движения (RDW);

- АУТС – не автомобили и не поезда. Они считаются автоматизированными машинами и сертифицируются согласно Директиве 2006/42/ЕС о безопасности машин и оборудования [19] и стандарту МЭК 61508 [16].

Новое законодательство в области омологации автомобилей в Германии разрешает автоматизированное вождение в ряде случаев (отметим, что речь не идет о системах помощи водителю), но предусматривает приоритет водителя над системой.

Это соответствует Конвенции о дорожном движении [3], согласно которой:

- статья 8, 1: «Каждое транспортное средство или состав транспортных средств, которые находятся в движении, обязаны иметь водителя».

- статья 8, 3: «Водитель обязан обладать необходимыми физическими и психическими качествами, и его физическое и умственное состояние должно позволять ему управлять транспортным средством».

- статья 8, 5: «Водитель (погонщик) должен быть всегда в состоянии управлять своим транспортным средством или направлять своих животных».

В настоящее время эти принципы реализованы в рамках соответствующих национальных законодательств.

Исходя из изложенного, мы можем заключить, что опыт эксплуатации и принципы безопасности автоматических метрополитенов неприменимы напрямую к автомобильному транспорту. Это связано с различиями, во-первых, в нормативном регулировании, во-вторых, в вопросах стандартизации, и в-третьих, в эксплуатационной среде. Автоматические метрополитены характерны наличием подконтрольной и четко заданной эксплуатационной среды, которая делает возможным автоматическое управление подвижным составом. Пассажиры отделены от движущихся систем, в частности, при помощи защитных дверей на платформах, которые

ведут непосредственно внутрь состава. В большинстве случаев с автомобилями ситуация иная.

3. Общие принципы безопасности и уровни полноты безопасности

В данном разделе мы приводим краткий обзор основных принципов безопасности (см. Гюлькер и Шебе [15], Гайен и Шебе [11, 12], Грефлинг и Шебе [13]) и уровней полноты обеспечения безопасности.

Отказоустойчивость: Если система имеет состояние защитной остановки, т.е. защитное состояние, в котором автомобиль не работает, а такое состояние устойчиво и достигается достаточно быстро, может быть реализован принцип отказоустойчивости. Это означает, что система приходит в такое состояние в случае неприемлемого отказа. Этот принцип может быть реализован как внутренняя отказоустойчивость, реактивная отказоустойчивость или составная отказоустойчивость.

Безопасный ресурс (многоотказность): Если система не имеет состояния защитной остановки, которое достигается достаточно быстро, необходимо реализовать функцию безопасности. Этого, главным образом, добиваются при помощи резервирования.

Отказ без последствий: Принцип отказа без последствий применяется к функциям, потеря которых приемлема ввиду того, что речь идет либо о вспомогательной, либо резервированной функции. В таком случае отказ функции не должен иметь значимых последствий для безопасного функционирования системы. Это значит, что система с отказом без последствий должна обнаруживать свои отказы и возможные опасные состояния и отключаться, не оказывая небезопасного влияния на другие системы.

Во всех случаях, когда функция может причинить вред, т.е. несет угрозу здоровью и жизни людей, имуществу, окружающей среде, необходимо применение мер функциональной безопасности. Иными словами, риск, обусловленный возможным функциональным отказом, должен быть снижен до приемлемого уровня.

Для этого задаются уровни полноты безопасности. Согласно ИСО 26262 [17] они могут быть УК (QM), от УПБА А до УПБА D, причем УПБА D – самый строгий. Такая система обязательна к применению в отношении автомобилей. Стандарт МЭК 61508 [16], предусматривает уровни полноты безопасности с 1 по 4 и распространяется на самодвижущиеся машины.

На практике это означает, что для всех функций вождения и всех подсистем вождения необходимый уровень безопасности (УПБА или УПБ) определяется при помощи анализа риска.

Уровни полноты обеспечения безопасности (УПБ/УПБА) определены в стандартах функциональной безопасности. МЭК 61508 и EN 50129 определяют уровни от УПБ 1 до УПБ 4. Для автомобильного транспорта стандартом ИСО 26262 [17] установлены уровни УПБ (УПБА) от А до D.

УПБ/УПБА включает в себя два основополагающих требования:

- Максимальная допустимая интенсивность опасных отказов, которую превышать нельзя;
- Меры противодействия систематическим отказам (верификация, отслеживаемость требований, конкретные технические решения).

4. Абстрактная модель системы

В [18] Лотц предложил архитектуру, состоящую из трех уровней: навигационного, маневрового и управляющего. Мы постараемся рассмотреть как можно более простую модель реализации такой архитектуры.

Для систем с автоматическим, частично автоматическим или автономным вождением мы определим следующую очень простую структуру. Система должна иметь не только живого водителя, но и техническую систему вождения, которая выполняет соответствующую функцию.

Очень абстрактно автомобиль имеет в своем составе такие подсистемы вождения, как система рулевого управления, торможения, ускорения и т.д. Они могут представлять собой очень простые техническим средства, например, механическую систему рулевого управления, пневматическую систему торможения и т.д. Вождение осуществляется живым водителем с непосредственным использованием таких подсистем вождения.

Маневровый и навигационный уровни согласно Лотцу [18] в данном случае объединены в одну систему (живой водитель/техническая система вождения).

Если автомобиль управляется технической системой вождения, которая осуществляет соответствующие функции вместо живого водителя, либо содействует ему, то система должна иметь доступ к подсистеме вождения. Это возможно только при использовании контроллера и привода. Это означает, что системы подобного типа должны присутствовать в составе конструкции автомобиля, чтобы обеспечить возможность вождения под управлением технической системы.

В таком случае живой водитель также имеет доступ к подсистеме вождения за счет наличия контроллеров вождения.

Таким образом, существует несколько вариантов управления указанными подсистемами:

а) Водитель имеет прямой доступ к подсистеме вождения, т.е. рулевое колесо механически соединено с осью управления;

б) Водитель взаимодействует с подсистемой вождения при помощи контроллера и привода, который управляет подсистемой электронными средствами. Типичным примером такой системы является электрический стояночный тормоз;

в) Техническая система вождения взаимодействует с подсистемой вождения при помощи контроллера и привода.

Из Рисунка 1 очевидна необходимость наличия средств разрешения конфликтов между командами, поступающими от живого водителя и технической системы вождения.

Разрешение конфликтов может осуществляться на различных уровнях:

а) подсистемы вождения.

В данном случае силы, прикладываемые контроллером и приводом должны быть настолько малы, чтобы водитель мог в любой момент перехватить управление. Однако, водитель будет должен либо отключить контроллер и привод вручную, либо эти системы должны иметь встроенную функцию обнаружения вмешательства водителя и отключаться сами;

б) контроллер и привод вождения.

В данном случае контроллер имеет два ввода с различным приоритетом. Ввод высокого приоритета используется водителем, ввод низкого приоритета используется технической системой вождения. Разрешение конфликтов осуществляется контроллером, который обнаруживает перехват управления живым водителем и отключает входной сигнал от технической системы вождения. Многие контроллеры в современных автомобилях (контроллер тормозной системы, рулевого управления и т.д.) имеют дополнительный ввод для систем содействия водителю, выполняя, таким образом, указанное требование. При таком подходе предполагается, что живой водитель управляет автомобилем электромеханическим способом за счет соответствующих контроллеров;

в) техническая система вождения.

Разрешение конфликтов происходит на уровне живого водителя и технической системы вождения. Если живой водитель перехватывает управление у техниче-

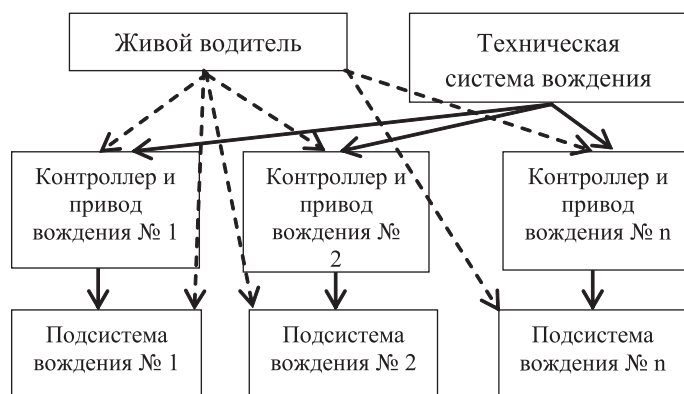


Рисунок 1 – Схема автомобиля с функциями автоматического вождения

ской системы вождения, последняя не вырабатывает собственных сигналов, а лишь передает сигналы живого водителя на контроллер вождения.

Выбор в пользу того или иного подхода зависит от производителя автомобиля. Однако, этот выбор имеет прямое отношение к поставщикам контроллеров и приводов вождения. В своих контроллерах им необходимо реализовывать различные системные архитектуры.

В случае а) они должны обеспечивать обнаружение вмешательства водителя и отключать привод.

В случае б) они должны иметь два входа с различным приоритетом и обеспечивать разрешение конфликтов.

В случае в) необходим лишь один вход и в разрешении конфликтов необходимости нет.

Как видим для реализации решений б) и в) необходимо наличие средств электромеханического управления.

Дальнейшее рассмотрение будет проводиться исходя из требования полностью автономного вождения, при котором живой водитель может в любое время перехватить управление.

5. Анализ уровней

5.1. Уровни 0 и 1

В данном разделе мы проведем анализ уровней (SAE [22]) автоматизации и сделаем выводы относительно вопроса архитектуры безопасности автомобиля.

На уровнях 0-1 за управление движением, ускорение и замедление отвечает живой водитель, он же отслеживает окружающую обстановку, а техническая система оказывает поддержку в некоторых режимах вождения (уровень 1).

Это значит, что водитель осуществляет управление, а техническая система обеспечивает лишь некоторые функции поддержки, например, выдачу предупреждения или реагирование на некоторую ситуацию, если водитель не способен этого сделать (содействие при экстренном торможении). При этом техническая система должна реализовывать принцип отказа без последствий, т.е. при ее отказе поведение автомобиля не должно измениться, либо может измениться таким образом, который не влияет на безопасность движения. Водитель при этом должен быть уведомлен об отказе системы содействия.

5.2. Уровень 2

На уровне автоматизации 2 система берет на себя ответственность в некоторых режимах вождения. Водитель отслеживает работу технической системы и боится ее. То есть все технические системы лишь оказывают поддержку, и

T1) Технически водитель должен иметь возможность вмешаться в процесс вождения, т.е. перехватить управление у технической системы. Иными словами каждый контроллер, отвечающий за ускорение, торможение и управление направлением движения, получающий сигнал от водителя и технической системы вождения, должен иметь в своем составе схему голосования, которая во всех случаях отдает приоритет водителю. Это означает, что для реализации этих функций необходимо

наличие электронной системы управления с УПБА, соответствующим функциям. В большинстве случаев речь идет об УПБА D. Такая система управления должна иметь приоритетный ввод для водителя и еще один неприоритетный ввод для технической системой вождения. Соответствующий контроллер вождения должен обеспечивать обнаружение попытки водителя перехватить управление у технической системы вождения и выполнение соответствующих действий;

T2) Водитель должен иметь в своем распоряжении достаточно времени для обнаружения неправильного поведения технической системы вождения, реагирования и возвращения автомобиля в безопасный режим вождения. Иными словами контроллеры должны ограничивать влияние технической системы вождения, т.е. ограничивать ускорение, торможение и углы поворота или угловую скорость и угловое ускорение и резкие движения таким образом, чтобы у водителя всегда было время отреагировать. Кроме того, водитель должен быть обучен пользованию этой функцией, либо контроллеры должны быть устроены таким образом, чтобы дать любому водителю достаточно времени на реагирование.

Требование T2 влечет за собой требования к системе автономного вождения:

- Торможение: автоматическая система должна осуществлять торможение медленнее, чем человек-водитель, а разница (между скоростями торможения, обеспечиваемыми системой и человеком) также должна обеспечивать возможность реагирования водителем (кривые торможения);
- Рулевое управление: расстояние до опасных объектов (другие автомобили, разделительные линии и т.д.) должна быть достаточно большой для обеспечения возможности реагирования водителя, а угол поворота должен быть ограничен. Вышеупомянутое может быть сопряжено с ограничениями скорости движения;
- Возможно, водителю понадобится особая подготовка.

На рисунке 2 показан пример кривой торможения. Видна зависимость скорости (м/с) от расстояния. Указано две кривых: одна для автоматического торможения (замедление 3 м/с^2), вторая – для торможения водителем (5 м/с^2). При этом время реакции водителя принято как 1,3 с. Начальная скорость составляет 20 м/с.

В приведенном примере водитель способен полностью остановить автомобиль вовремя, если обнаружит, что автоматическая система не в состоянии осуществить торможение. Разумеется, водитель должен реагировать и должен быть способен отреагировать за отведенные 1,3 с.

Для рулевого управления необходимо принять аналогичные требования: У водителя должно быть необходимое время на реагирование. Данное время реагирования зависит от расстояния до обочины или соседней полосы, скорости и реакции системы. Последнее включает в себя максимальные угловые скорости и ускорения, при которых система может оказаться неспособна реагировать на ситуацию соответствующим образом.

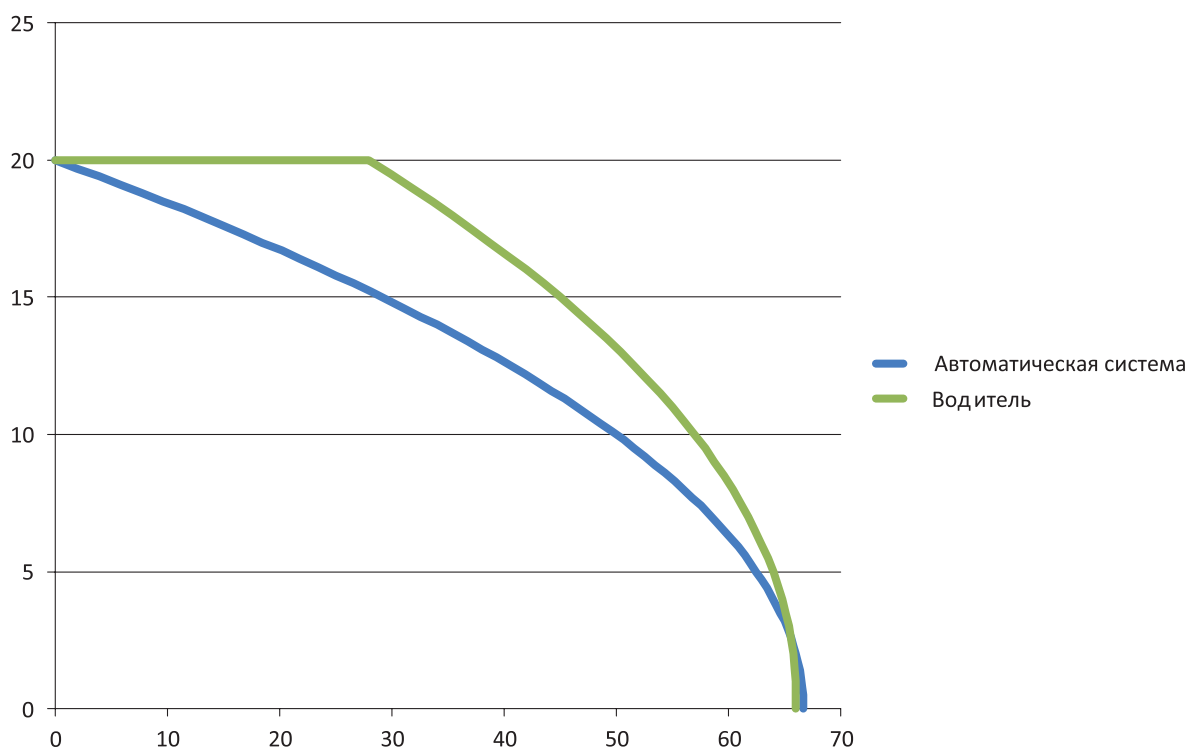


Рисунок 2 – Пример кривой торможения

Существующие технические решения реализованы на основе следующих разработанных технических средств:

- Разнообразные контроллеры или ответственные вычислительные комплексы, сертифицированные по требованиям УПБА D/УПБ 4;
- Существуют также сертифицированные на УПБ «умные датчики»;
- Разнообразные датчики (без УПБ) с перекрестной проверкой ответственным вычислительным комплексом. В качестве примеров таких датчиков можно привести камеры, лазеры, радары, инфракрасные и ультразвуковые сенсоры и т.д.;
- Разнообразие на уровне узлов и агрегатов. Использование предохранительных реле в качестве электрических компонентов, использование проверенных механических систем.

5.3. Уровень 3

Уровень 3 отличается от уровня 2 лишь в одном. Техническая система вождения отвечает за контроль соответствующего оборудования. Это означает, что система должна проводить самодиагностику и контролировать окружающую обстановку для определения того, может ли она продолжать управления, либо передать эту функцию человеку. Важно отметить следующие требования:

T3) Необходимо четко определить процедуру передачи полномочий между человеком и технической системой вождения. Либо техническая система вождения должна продолжать функционирование до принятия человеком управления, либо

T4) Предусмотрен определенный промежуток времени (например, одна секунда), в течение которого чело-

век должен перехватить управление, если техническая система вождения того потребует.

В первом случае (T3) техническая система вождения должна быть с безопасным ресурсом, во втором случае (T4) время задержки при перехвате управления человеком должно быть обеспечено техническими системами: либо свойством безопасного ресурса, либо исходя из дорожной обстановки и скорости движения. Соображения относительно временных показателей изложены в [25] (Фогельполь и др.).

5.4. Уровни 4 и 5

Уровни 4 и 5 еще сложнее. Различия между уровнями 4 и 5 относительно невелики, поскольку распределение обязанностей идентично за тем исключением, что на уровне 4 некоторые режимы вождения исключены, за счет чего возможности технической системы вождения ограничены. При этом, если система активна, она должна быть способна взять на себя полную меру ответственности.

По этой причине техническая система должна непрерывно обеспечивать безопасное вождение, реализуя принцип безопасного ресурса.

Соответствующие требования основаны на так называемом принципе GAME, который изложен, в частности, в EN 50126 [6]: “Все новые рельсовые транспортные системы должны обеспечивать общий уровень риска не хуже аналогичных существующих систем“. В данном случае под рельсовыми транспортными системами мы понимаем только транспортные средства с автономным вождением. Мы проводим сравнение классического и самоуправляемого транспортных средств. Необходимо рассматривать два аспекта:

- а) Технические показатели и
- б) Достаточная защита технической системы (транспортное средство и техническая система вождения) от опасных отказов.

Эти два аспекта рассматриваются по отдельности. С точки зрения технических показателей система вождения должна быть не хуже человека-водителя в соответствующих дорожных ситуациях (см. Мацгега и др. [20]). Если это условие нельзя соблюсти для всех дорожных ситуаций, перечень последних должен быть ограничен, и на человека-водителя должна быть возложена ответственность за наиболее сложные из них.

Вопрос безопасности можно решить, как и в любой другой технической системе, путем задания соответствующего уровня безопасности (УПБА или УПБ). Из чего следует, что

T5) Технические показатели системы вождения включают в себя время реагирования, обнаружение и отработку различных ситуаций дорожного движения и пр. При этом штатно функционирующая система должна быть не хуже человека-водителя.

T6) Техническая система вождения должна быть разработана в соответствии с разумно достаточным УПБ/УПБА.

Для уровня 4 необходимо четко определить процедуру передачи полномочий между технической системой вождения и человеком-водителем. Прежде всего, необходимо определить режимы вождения, в которых техническую систему вождения использовать нельзя по причине, например, несоответствия ее показателей поставленной задаче. Передача управления должна осуществляться во время остановки, либо техническая система вождения должна заблаговременно информировать водителя о том, что она намерена передать ему управление и он должен его принять. Если водитель не принимает управление, техническая система вождения все равно должна иметь возможность остановить транспортное средство, если она находится в режиме вождения, при котором автоматическое вождение допустимо и возможно.

В случае передачи водителем управления технической системе вождения ответственность остается на нем до тех пор, пока техническая система вождения не сообщит ему, что она приняла ответственность.

При движении по дороге, открытой для проезда, водитель несет полную ответственность за поведение транспортного средства (см. Конвенцию [3]). В этом случае, даже если техническая система вождения соответствует уровню SAE 5 с необходимым уровнем полноты безопасности, водитель должен иметь возможность вмешаться в процесс вождения. Таким образом, требования а) и б) для уровня SAE 2 должны выполняться при движении по дороге, открытой для проезда.

Действительно автономное вождение, т.е. вождение без вмешательства человека-водителя в действительности реализовано только на уровне SAE 4 (частично) или 5 (полностью). Это так, даже если законодательство требует наличия водителя в транспортном средстве.

6. Реализация принципов безопасности

6.1. Системы содействия

Ясно, что технические системы вождения уровней до 2 должны и могут быть построены по принципу отказа без последствий; и T1, и T2 обязаны выполняться для обеспечения возможности водителя принять управление на себя.

6.2. Применение принципа отказоустойчивости

Прежде всего, необходимо определить, существует ли состояние безопасной остановки, которого можно достичь достаточно быстро. Предположим, что скорость движения транспортного средства ограничена значением v , тормозное замедление составляет a , а время реакции – t , тогда транспортное средство остановится в пределах дистанции

$$s = v \cdot t + v^2 / (2a).$$

Предполагая, что рулевое управление ничем не ограничено, остановка транспортного средства будет безопасным действием в случае отсутствия препятствий в пределах дистанции s . Это пространство можно сделать еще меньше, если принимать во внимание:

- направление поворота рулевого колеса и (физические) ограничения изменения угла его поворота, а также
- физические ограничения изменения направления движения.

В таком случае техническая система вождения и контроллеры могут представлять собой полностью безаварийную систему и останавливать транспортное средство в случае обнаружения отказа.

В зависимости от наличия свободного пространства вокруг определяется скорость движения транспортного средства. Очевидно, что, чем меньше доступно свободного пространства, тем медленнее должно двигаться транспортное средство. Контроллеры вождения необходимо разработать с учетом требований соответствующих УПБ/УПБА, которые зависят от скорости движения.

6.2. Применение принципа безопасного ресурса

В таком случае, если необходимо обеспечить более высокую скорость движения транспортного средства, техническая система вождения и контроллеры должны реализовывать принцип безопасного ресурса по крайней мере во время движения.

Контроллеры вождения необходимо разработать с учетом требований соответствующего УПБ. Для тормозной системы (АБС/ЭСКУ) – это, в основном, УПБА D, для системы рулевого управления – УПБА В – УПБА D в зависимости от функции контроллера. При таких условиях большинство транспортных средств могут эксплуатироваться на скоростях до 250 км/ч.

Реализация принципов безопасности различается применительно к дорожным транспортным средствам и самодвижущимся машинам. В первом случае мы не можем предположить, что окружающая обстановка находится под контролем. Во втором случае этого добиться можно, поскольку техническая система вождения эксплуатируется на частной территории. В последнем

случае гораздо проще обеспечить наличие достаточного свободного пространства.

Ввиду этого обстоятельства ясно, что не все функции и не всегда обязаны быть реализованы с учетом максимально высокого УПБ/УПБА. Это во многом зависит от скорости движения и свойств среды. Если скорость ограничена физически или иным образом, допустимо применение более низкого УПБ или УПБА. В любом случае исходить нужно из анализа рисков, проводимого согласно требованиям ИСО 26262 [17] или МЭК 61508 [16].

Ниже указаны функции, которые необходимо учитывать в первую очередь:

- Управление.

Порядок реализации данной функции, включая аспект рулевого управления, описан в работе [1] (Бауман, Шебе и Вис). Принцип безопасного ресурса необходимо реализовать прежде всего применительно к управлению ведущим мостом, а в составе технической системы вождения необходимо использовать безопасный вычислительный комплекс, который будет отвечать за контроль угла поворота управляемых колес. Еще одна важная функция – определение местоположения, которое можно осуществить при помощи дифференциальной GPS, картографических материалов, а также ультразвуковых датчиков, радаров, лазеров или камер, либо физических меток вдоль полосы движения. Безопасный вычислительный комплекс определит действительное местоположение и сравнит его с предполагаемым исходя из предпринятых действий по управлению, а затем скорректирует поведение или остановит транспортное средство;

- Торможение и ускорение.

Предполагая, что транспортное средство движется по желаемой траектории, оно должно начать, продолжить и завершить движение. Следовательно, транспортное средство должно реагировать на соответствующие команды. Важно ограничить скорость движения, например, в кривых или на узких участках дороги и обеспечить возможность экстренной остановки в случае отказа составных частей системы. Для выполнения данной функции системе необходимо иметь информацию о текущем местоположении.

За счет двух указанных функций транспортное средство сможет лишь двигаться без учета окружающей обстановки. Любые изменения в окружающей среде могут привести к столкновениям с участием автомобиля, покидающего свою полосу;

- Реагирование на непредусмотренные события (препятствия).

Транспортное средство должно обладать способностью обнаруживать препятствия. Препятствием мы называем объект, находящийся в пределах (запланированной) или рядом с (запланированной) траекторией движения транспортного средства. Необходимо различать неподвижные и движущиеся препятствия. Изначально в качестве единственной стратегии рассматривается остановка транспортного средства перед препятствием. Вариант объезда препятствия будет рассмотрен далее применительно к случаям движущихся препятствий.

а) Неподвижное препятствие: для обнаружения препятствий техническая система вождения должна иметь в своем составе образ окружающей среды, с которым она сравнивает окружающую обстановку для выявления расхождений. Это требует наличия ряда алгоритмов обнаружения и классификации объектов. Отметим, что термины «обнаружение» и «образ» не означают, что техническая система вождения использует какие бы то ни было оптические средства. Могут использоваться как оптические средства, так и иные системы или их сочетания.

На первом этапе происходит как таковое обнаружение препятствий. Это возможно только на определенном расстоянии и занимает некоторое время. В зависимости от производительности системы скорость движения транспортного средства может быть ограничена ввиду необходимости обеспечения остановки перед препятствием.

На втором этапе техническая система вождения осуществляет классификацию препятствий как небольших. Отметим, что такая классификация может осуществляться неявно, если техническая система вождения не обнаруживает небольшие препятствия. Такая классификация присутствует всегда ввиду ограниченности возможностей системы.

Если препятствие достаточно невелико и невысоко, транспортное средство может принять решение продолжать движение.

б) Движущиеся препятствия: Движущиеся препятствия необходимо отслеживать, а их перемещение – прогнозировать на основе текущего положения и скорости. Нужно также принимать во внимание, способен ли объект ускориться и менять направление движения. Последние факторы в значительной мере зависят от природы объекта. К примеру, характеристики ускорения мотоцикла и пешехода различаются. Точное прогнозирование требует от технической системы вождения классификации движущихся объектов по подвижности. Соответственно, для каждого объекта различных групп необходимо прогнозировать будущее местоположение, и техническая система вождения должна задавать движение транспортного средства таким образом, чтобы избежать столкновения. Результатом может быть решение об остановке или дальнейшем пребывании в неподвижном положении.

В зависимости от качества работы алгоритмов группирования и прогнозирования техническая система вождения будет вести себя более или менее сдержанно. При использовании более качественных алгоритмов техническая система вождения будет останавливать транспортное средство реже. Напомним, что указанные алгоритмы и процесс торможения в ситуациях малопредсказуемой траектории движения препятствия должны обеспечивать результаты не хуже, чем человек-водитель. Это включает стратегии объезда препятствий.

в) Неподвижные препятствия, которые могут прийти в движение представляют собой сочетание указанных выше случаев а) и б). Это значит, что техническая система вождения обязана не только отслеживать движущиеся препятствия, но также быть способна классифицировать неподвижные препятствия и выносить суждение относи-

тельно того, могут ли они двигаться и с какой скоростью и в каком направлении. Наиболее безопасной стратегией, безусловно, было бы остановиться на безопасном расстоянии от любого неизвестного объекта.

Если должного реагирования со стороны транспортного средства во всех дорожных ситуациях обеспечить невозможно, перечень последних должен быть ограничен, и на человека-водителя должна быть возложена ответственность за наиболее сложные из них. Таким образом, складывается ситуация уровня SAE 4. В качестве примера можно привести стратегию, при которой техническая система вождения берет на себя управление при движении по шоссе, а человек-водитель – при движении в городе.

7. Проблемы

Вопрос автономного вождения сопряжен с рядом проблем. Мы рассмотрим лишь часть из них и постараемся описать возможные технические решения.

а) Предположим, что автономное транспортное средство не в состоянии предотвратить происшествие и должно сделать выбор, например, между материальным ущербом, экологическим ущербом и причинением вреда здоровью, либо, что еще хуже, причинением травмы или гибели пожилому человеку или ребенку, другому водителю, собственным пассажирам и др. [5].

Этот вопрос неизбежно возникает при обсуждении передачи управления от человека-водителя технической системе вождения. Соответствующая этическая проблема в рамках данного раздела решена быть не может. Очевидно, что техническое решение данной проблемы потребует механизмов распознавания людей, предметов и животных, а также различных категорий людей. Это (если это вообще возможно) потребует применения достаточно сложных алгоритмов.

Наиболее простым решением была бы реализация принципа вождения по визуальным показателям. Это означает, что автономное транспортное средство будет двигаться только с такой скоростью, при которой оно сможет остановиться перед любым препятствием, которое появляется на дороге. Соответствующие требования включают следующее:

- Обнаружение препятствий больше определенного размера,
- Прогнозирование передвижения объектов (наиболее сложная часть),
- Снижение скорости при необходимости остановки транспортного средства перед таким препятствием.

На основании подобного подхода «безопасность прежде всего» объект определенного (небольшого) размера в будущем может быть проигнорирован в целях повышения производительности и исключения остановки транспортного средства перед упавшим листом или пластиковым пакетом;

б) Дополнительные сведения.

Транспортное средство может также использовать дополнительную информацию, получаемую от ин-

фраструктуры, что может способствовать повышению безопасности.

Рассмотрим следующий пример. Транспортное средство использует информацию, полученную с уличных камер, и способно «заглянуть за угол». Таким образом оно может, например, обнаружить ребенка, внезапно выбежавшего из дома, на что человек-водитель не способен;

в) Целевые показатели безопасности.

Поскольку целевым показателем безопасности системы автономного вождения всегда является поведение человека-водителя, техническая система вождения должна удовлетворять данному важному требованию. Однако, если предположить, что в будущем автономными системами будет установлен новый целевой показатель безопасности, то возникает вопрос: Имеет ли водитель право отключить автоматическую систему и понизить уровень безопасности? Это будет в некоторой мере равносильно отключению системы интервального регулирования машинистом поезда. Этот простой пример показывает, что переход к автономному вождению будет бесповоротным, и возврата к ручному управлению не будет.

8. Возможные дальнейшие шаги

Исходя из текущей ситуации можно предположить, в каком направлении пойдет развитие автотранспорта:

- Может быть реализована функция удержания на полосе движения, например, с использованием дифференциальной GPS в сочетании с регулярно обновляемыми качественными картографическими материалами. Все места проведения дорожных работ и временно закрытые участки должны быть отмечены на карте.
- Принудительная остановка перед запрещающим сигналом светофора посредством беспроводной передачи информации на транспортные средства. При этом водитель по-прежнему обязан отслеживать действия потенциальных нарушителей, например, велосипедистов, даже, если горит зеленый сигнал.
- Обеспечение соблюдения ограничений скорости, при котором максимально допустимое значение скорости движения передается по беспроводной связи от вещающего знака, либо знак считывается камерой, также для этих целей могут применяться картографические материалы.
- Обработка простых дорожных ситуаций, например, следование полосе движения на автотрассе без осуществления обгонов.
- Автономные транспортные средства на отдельных территориях и участках сети.

Дальнейшее развитие может предполагать следующее:

- Дорога или полоса могут быть отделены двойным ограждением, образуя контролируемую среду, в которой транспортное средство может перемещаться в автоматическом режиме. При этом функции рулевого управления, торможения, вождения будут реализованы в соответствии с УПБА D;
- Транспортные средства движутся на очень коротком расстоянии друг от друга, образуя автоколонны;

- В определенных местах организован въезд и выезд с автодорожной сети. В таких местах водитель будет принимать на себя управление и вести транспортное средство вручную до места назначения;

- Функции, связанные со всей необходимой информацией, включая картографические материалы, местоположение, ограничения скорости, связь с другими автоматизированными транспортными средствами, будут реализованы на основе бортовых, а не инфраструктурных средств;

- Инфраструктура будет относительно недорогой и будет состоять из дороги и ограждения. По сравнению с железнодорожным транспортом такая инфраструктура более гибкая, не требует наличия светофоров, стрелок, балласта и шпал.

Во всех указанных случаях используемые технические системы должны иметь безопасный ресурс с уровнем безопасности до УПБА D/УПБ 4.

Система с безопасным ресурсом — это система, которая в отличие от безаварийной системы не выключается в случае отказа, и в которой функция обеспечения безопасности выполняется даже в случае одного, а иногда нескольких отказов.

В контексте путей дальнейшего развития также необходимо рассматривать возможные проблемы, которые необходимо решить для того, чтобы автоматическое или автономное автодорожное транспортное средство могло сравниться с автомобилем под управлением человека. Прежде всего такая система обязана отличать людей и животных от неподвижных объектов. Она также не должна путать высокие транспортные средства и мосты. Проблему также представляет то, что в некоторых случаях намерения человека или животного неизвестны: будет ли человек или животное переходить дорогу? Характерным примером может служить ребенок с мячом на тротуаре, роняющий мяч, который катится на проезжую часть. Таких случаев много, и они требуют интеллектуальных решений, которые скорее всего будут реализованы с применением искусственного интеллекта.

Исходя из этого, предполагаем, что автономное вождение будет реализовано на основе искусственного интеллекта. Требования согласно УПБ 4/УПБА D должны будут неукоснительно выполняться на уровне программного и аппаратного обеспечения. С другой стороны, алгоритмы искусственного интеллекта громоздки и сложны. При этом если, например, потребуется продемонстрировать выполнение требования «Алгоритм обязан отличать людей от прочих объектов», можно представить себе сложность выполнения такой задачи. И это лишь одно требование. Комплекс требований к программному обеспечению будет должен принимать во внимание множество дорожных ситуаций. Если алгоритм обладает свойством самообучения, необходимо обеспечить необходимый объем обучения в установленные сроки, что должно быть доказано применительно к требованиям стандартов МЭК 61508 [16] и (или) ИСО 26262 [17]. В качестве альтернативы можно прибегнуть к доказавшему свою состоятельность на практике критерию $3 \cdot 10^9$ часов реальной наработки (см. МЭК 61508 [16], Часть 7,

Приложение D). Из расчета 600 часов вождения в год это будет эквивалентно подконтрольной эксплуатации 5 млн транспортных средств в течение целого года. Такая эксплуатация предполагает наличие подготовленных водителей, способных перехватить управление, а также регистрацию всех событий. Число транспортных средств можно сократить за счет увеличения числа часов эксплуатации в год до, например, 6 тыс., для чего процесс вождения должен быть посменным. Тем не менее, все равно потребуется 500 тыс. транспортных средств. Кроме того, любое изменение в программном обеспечении потребует повторного процесса согласования.

Напрашивается вывод о том, что технические решения, применяемые в ответственном программном обеспечении, должны быть относительно простыми и не должны предполагать прогнозирования намерений. Решения на основе искусственного интеллекта найдут применение в составе систем содействия водителю.

9. Выводы

В настоящей статье мы рассмотрели некоторые вопросы, связанные с автоматическим (или автономным) управлением железнодорожным подвижным составом и автомобилями. Выяснилось, что автомобили эксплуатируются в гораздо более сложной среде, чем поезда. Поэтому опыт эксплуатации, например, автоматических поездов метро здесь напрямую неприменим.

В статье предлагается несколько идей для построения архитектуры обеспечения безопасности системы автономного вождения на основе известных принципов и общих требований обеспечения безопасности. Мы проанализировали уровни SAE и их смысл с точки зрения архитектуры безопасности.

Приведено описание возможных принципов реализации и обсуждены конкретные проблемы автономного вождения. Так, реализацию систем автономного вождения рекомендуется проводить согласно принципам проектирования, изложенным в главе 6. Важно понимать архитектуру безопасности автомобиля и решить, идет ли речь лишь о системе содействия (система с отказом без последствий), либо требуется реализация принципа отказоустойчивости или безопасного ресурса. Эти положения должны лежать в основе оценки безопасности автомобилей с автономным вождением.

Большинство существующих систем относятся либо к категории систем содействия, либо приспособлены для работы в условной дорожной обстановке.

Есть все основания ожидать, что первые безопасные решения в области автономного вождения будут предназначены для эксплуатации в упрощенных условиях, прежде всего там, где эксплуатационная среда контролируется или даже специально адаптирована к задачам автономного вождения. В качестве примера можно привести автоматически управляемые транспортные средства, которые осуществляют движение лишь в рамках полностью адаптированной среды, но не на дорогах общего пользования.

Библиографический список

1. **Bouwman, R.** Application of safety principles – for a guidance system in public transport [Text] / R. Bouwman, H. Schäbe, H. Vis // Proceedings of ESREL 2009, Reliability, Risk and Safety. – 2009. – Vol. 3. – P. 2275-2278.
2. **Breitinger, M.** Kabinett erlaubt teilautomatisiertes Fahren [Электронный ресурс]. – URL: <http://www.zeit.de/mobilitaet/2016-04/autonomes-fahren-gesetzentwurf-verkehrsrecht-alexander-dobrindt> (дата обращения 19.10.2017).
3. Конвенция о дорожном движении от 08.11.1968, Европейское дополнительное соглашение от 01.05.1971 и Протокол от 01.03.1973 [Текст].
4. The Mercedes-Benz Future Bus The future of mobility [Электронный ресурс]. – URL: <https://www.daimler.com/innovation/autonomous-driving/future-bus.html> (дата обращения 19.10.2017).
5. Ethik-kommission Automatisiertes und Vernetztes Fahren (нем. Комиссия по этике в области автоматизированного и дистанционного вождения), Отчет, Июнь 2017 г. [Электронный ресурс] – URL: www.bmvd.de.
6. EN 50126 Транспорт железнодорожный – спецификация и демонстрация Надежности, Доступности, Пригодности для обслуживания и Безопасности (RAMS) [Текст] – 1999.
7. EN 50129 Транспорт железнодорожный – Коммуникация, системы СЦБ и обрабатывающие системы – Программное обеспечение для железнодорожных систем управления и систем защиты [Текст] – 2011.
8. EN 50129 Железные дороги. Системы связи сигнализации и обработки данных. Электронные сигнализационные системы безопасности [Текст] – 2003.
9. Todesfall im selbstfahrenden E-Auto US-Verkehrsaufsicht prüft Teslas «Autopilot» [Электронный ресурс]. Focus. – 2016. – URL: www.focus.de/auto/elektroauto/todesfall-im-selbstfahrenden-auto-us-verkehrsaufsicht-prueft-teslas-autopilot_id_5687341.html (дата обращения 01.07.2016).
10. www.frog.nl [Электронный ресурс] (дата обращения 19.10.2017).
11. **Gayen, J.-T.** (Miss-) Konzeptionen von Sicherheitssprinzipien [Text] / J.-T. Gayen, H. Schäbe // Signal + Draht. – 2008. – Vol. 7+8. – P. 11-18.
12. **Gayen, J.-T.** (Mis-) conceptions of safety principles [Text] / J.-T. Gayen, H. Schäbe // ESREL 2008, Proceedings Safety, Reliability and Risk analysis. – 2008. – Vol. 2. – P. 1283-1291.
13. **Gräfling, S.** The agri-motive safety performance integrity level – or how do you call it? [Text] / S. Gräfling, H. Schäbe // Proceedings of ESREL 2012/PSAM 11. – 2012. – P. 10.
14. Google self-driving car hits public bus near Mountain View headquarters [Электронный ресурс]. – URL: www.mercurynews.com/2016/02/29/google-self-driving-car-hits-public-bus-near-mountain-view-headquarters (дата обращения 19.10.2017).
15. **Gülker, J.** Physical Principles of Safety, Safety and Reliability for Managing Risk [Text] / J. Gülker, H. Schäbe // Proceedings of ESREL 2006. – 2006. – P. 1045-1050.
16. **МЭК 61508.** Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Части 1 – 7 [Текст] – 2010.
17. **ИСО 26262.** Дорожные транспортные средства. Функциональная безопасность Части 1-10 [Текст] – 2014.
18. **Lotz, G.O.** Eine Referenzarchitektur für die assistierte und automatisierte Fahrzeugführung mit Fahrereinbindung: диссертация: 2017 [Text] / Lotz G.O.; [место защиты: Дармштадтский технический университет].
19. Директива № 2006/42/ЕС Европейского парламента и Европейского совета от 17 мая 2006 г. о технике, вносящая поправки в Директиву № 95/16/ЕС (исправленная версия) [Текст].
20. **Mazzega, J.** Absicherung hochautomatisierter Fahrfunktionen [Text] / J. Mazzega, F. Köster, K. Lemmer, T. Form // Automobiltechnische Zeitschrift. – 2016. – Vol. 10. – P. 48-52.
21. Weltpremiere: Daimler Buses präsentiert autonom fahrenden Stadtbus [Электронный ресурс]. – URL: www.nahverkehrs-praxis.de/news/nahverkehrspraxis-top-news/article/weltpremiere-daimler-buses-praesentiert-autonom-fahrenden-stadtbus (дата обращения 19.10.2017).
22. Классификация и определение терминов в области систем автоматизации вождения автомобильных транспортных средств. SAE J3016 [Текст]. – 2016.
23. A global bid for automation: UITP Observatory of Automated Metros confirms sustained growth rates for the coming years [Электронный ресурс] (дата обращения 19.10.2017).
24. Сводная резолюция о конструкции транспортных средств (СР.3), Пересмотр 6. Организация Объединенных Наций, Экономическая комиссия для Европы, Комитет по внутреннему транспорту, Всемирный форум для согласования правил в области транспортных средств [Текст] (дата обращения 11.07.2017).
25. **Vogelpohl, T.** Übergabe von hochautomatisiertem Fahren zu manueller Steuerung. Forschungsbericht Nr. 39 [Text] / T. Vogelpohl, M. Vollrath, M. Kühn, T. Hummel, T. Gehlert // Германский союз страховщиков. – Август 2016. – ISBN 978-3-939163-67-1.
26. **Wachenfeld, H.K.** How Stochastic can Help to Introduce Automated Driving: диссертация: 2016 [Text] / Wachenfeld H.K.; [место защиты: Дармштадтский технический университет].

Сведения об авторе

Шебе Хендрик, доктор физико-математических наук, заведующий отделом анализа рисков и опасностей, TÜV Rheinland InterTraffic, Cologne, Germany, e-mail: schaebe@de.tuv.com

Поступила 18.03.2019