РОЛЬ НАДЕЖНОСТИ И БЕЗОПАСНОСТИ В АВТОМОБИЛЕ БУДУЩЕГО

ФРАНК ВАН ДЕН БОЙКЕН (FRANK VAN DEN BEUKEN)
ПЕРЕВОД: ВЛАДИМИР РЕНТЮК, ВИТАЛИЙ ШЕШУКОВ

Автомобили эволюционируют на наших глазах, превращаясь из электромеханического устройства, действующего под контролем человека, в полностью автономное транспортное средство. Сегодня большинство новых машин оборудовано современными системами помощи водителю (англ. Advanced Driver Assistance Systems, ADAS), выполняющими такие функции, как слежение за полосами движения, независимое экстренное торможение, видеонаблюдение и др. Однако в то же время экспериментальные, полностью автономные автомобили уже способны проехать миллионы миль в тестовом режиме, и это приближает нас к переломному моменту в развитии автомобильной промышленности.

ПОВЫШЕННАЯ ФУНКЦИОНАЛЬНОСТЬ

Современные системы помощи водителю или автономного движения состоят из датчиков, сенсоров, активаторов, радарных и лидарных систем (англ. термин от Light Identification, Lidar — лазерный дальномер). Все они объединяются в единое целое через внутренние и внешние компьютерные сети и управляются микроконтроллерами, поэтому такой автомобиль можно назвать «Интернетом на колесах» (англ. Internet on Wheels). Кроме того, машины могут обмениваться данными между собой, по технологии V to V, а также с инфраструктурой (V to I) — светофорами, дорожными знаками и навигационными спутниковыми системами, например уже привычной системой глобального позиционирования, или GPS.

Для реализации этого комплекса возможностей, естественно, нужно программное обеспечение (ПО), т. е. более 100 миллионов линий кода. Сюда входят коды для различных приложений, операционные системы (ОС) и ПО для организации сетевых коммуникаций и интерфейсов с датчиками и сенсорами, приводами и водительскими экранами.

ПОВЫШЕННАЯ УЯЗВИМОСТЬ

По мере усложнения электронных систем транспортных средств (ТС) все острее становится вопрос их надежности и безопасности. Из-за обмена данными по каналу V to X (от машины к некоему объекту X) автомобили более подвержены внешним атакам. Уже бывали случаи, когда третья сторона получала контроль над, например, машиной производства компании Jeep и управляла им вместо водителя. Еще одна уязвимость добавляется со стороны владельца автомобиля. Все производители машин для мониторинга многочисленных пара-

метров двигателя и поиска неисправностей используют бортовую диагностику (англ. On Board Diagnostics, OBD). Спецификация нтерфейса соединителя OBD II сейчас общедоступна, и, если вы наберете в строке поиска Google «OBD II», он выдаст вам массу устройств с подключением по Bluetooth, которые позволяют контролировать и отслеживать состояние двигателя с помощью смартфона. Это также делает систему управления двигателем открытой для недоброжелателей. В недавней статье исследователей Мичиганского университета было описано использование прямого подключения ноутбука к OBD для перехвата управления большим грузовиком и школьным автобусом.

Кроме того, из-за огромного размера программного кода его надежность тоже является критическим параметром. К примеру, случай с непреднамеренным ускорением, произошедший с автомобилем Toyota, показал, что используемый сейчас код содержит модули, написанные очень давно и не соответствующие современным стандартам качества. Поэтому при создании кода необходимо ориентироваться на стандарты, предъявляющие более высокие требования.

ВОПРОСЫ СТАНДАРТИЗАЦИИ

В 2011 г. был издан специальный стандарт безопасности для автомобилей — ISO 26262[1] [1], являющийся адаптацией функционального стандарта безопасности IEC 61508[2] [3, 4]. Новый стандарт фокусируется на требованиях к электрическим и электронным системам, которые используются в серийном производстве легковых автомобилей, и применяется ко всем процессам, происходящим в этих системах безопасности на протяжении всего срока службы. Он также включает требования к качеству ПО.

Чтобы обеспечить анализ и определение рисков, связанных с подсистемами, этот стандарт использует подход, основанный на уровнях полноты безопасности автомобиля (англ. Automotive Safety Integrity Level, ASIL). Все подсистемы делятся на уровни от A до D, где A — наименьший уровень эксплуатационной безопасности, а D — наивысший, который содержит самые жесткие требования. Эти уровни дополняет класс управления качеством (англ. Quality Management, QM), указывающий на отсутствие требования соблюдать ISO 26262, т. е. на то, что ответственность за гарантию качества лежит на разработчике.

Также ASIL определяет параметры серьезности риска, вероятности воздействия и управляемости. Особого внимания требует последний. Параметр управляемости предполагает, что водитель находится в надлежащем состоянии для вождения, имеет водительские права, соблюдает все правовые нормы, включая требования к техобслуживанию, а также выполняет ПДД.

В скором времени правила дорожного движения необходимо будет адаптировать таким образом, чтобы в том случае, когда автоматизированная система вождения находится в действии, водителю не приходилось следить за ситуацией, пока система не потребует его вмешательства. Поэтому важнейшее значение имеет правильное функционирование системы в части своевременного и правильного уведомления водителя и передачи управления человеку. Если уведомления не приходят, водитель не будет владеть ситуацией и может попасть в аварию, как это недавно случилось с автомобилем компании Tesla. Если же не произойдет передача управления, водитель тоже не сможет избежать опасности. Такие ситуации всегда должны относиться к самому высокому классу контроля (C3), который предполагает, что не менее 90% всех водителей и других участников дорожного движения в состоянии не попасть в аварию.

Тому, как правильно разработать ПО, чтобы написать достаточно надежный код для работы в системе, соответствующей уровню ASIL, посвящена шестая часть стандарта ISO 26262[3] [7].

Существует еще один стандарт для машин — J3016[4] [9], разработанный Сообществом автомобильных инженеров, известным как SAE (англ. The Society of Automotive Engineers). В нем автоматизация управления автомобилем разделена на шесть классов, от ТС «без автоматизации» до «полной автоматизации» (таблица). Автоматизированные системы управления, отнесенные к третьему классу и выше, используют ПО, которое для того, чтобы смоделировать окружающую обстановку, собирает данные с датчиков и затем, в зависимости от задачи, решает, как помочь водителю или как управлять ТС. У этого ПО есть и другие важные задачи, такие как определение того, правильно ли функционируют датчики, когда выдавать водителю предупреждения и в каких случаях необходимо передавать управление человеку.

ЗАКОНОДАТЕЛЬСТВО

Несомненно, ПДД необходимо будет изменить с учетом применения автоматизированных систем вождения, особенно в области ответственности и конфиденциальности. Многие правительства уже предприняли определенные законодательные инициативы в этой сфере.

Национальное управление безопасностью движения на трассах министерства транспорта США (National Highway Traffic Safety Administration) предложило официальную систему классификации, которая определяет пять уровней автоматизации управления. Начиная с уровня, когда водитель полностью контролирует ТС во все время движения, и заканчивая уровнем, когда ТС осуществляет управление критически важными функциями на протяжении всей поездки, не нуждаясь во вмешательстве водителя.

Кроме того, у каждого штата США свой подход к этому вопросу. Так, Невада еще в 2011 г. стала первым штатом, разрешившим эксплуатацию автономных ТС и проведение испытаний технологий автономного вождения на дорогах общего пользования. За ней последовали Калифорния, Флорида, Мичиган, Северная Дакота, Теннесси и округ Колумбия (Washington DC).

Что касается ЕС, в январе 2014 г. стартовал европейский исследовательский проект AdaptIVe (Automated Driving Applications & Technologies for Intelligent Vehicles — «Автома-

[1] В РФ в этой области действует стандарт ГОСТ Р ИСО 26262-1-2014[2], который идентичен международному стандарту ИСО 26262-1:2011 и определяет термины в части функциональной безопасности. — Прим. пер.

[2] В РФ в этой области действуют стандарт ГОСТ Р МЭК 61508-1-2012 [5], идентичный международному стандарту МЭК 61508-1:2010, который определяет общие требования, и стандарт ГОСТ Р МЭК 61508-2-2012 [6], идентичный международному стандарту МЭК 61508-2:2010 и содержащий требования к системам. — Прим. пер.

[3] В РФ в этой области действует стандарт ГОСТ Р ИСО 26262-6-2014 [8], идентичный международному стандарту ИСО 26262-6:2011, который определяет требования к разработке ПО изделия. — Прим. пер.

[4] Текущая версия 2016-09-30, аналогов в РФ не имеет. — Прим. пер.

тизированные приложения и технологии вождения для интеллектуальных транспортных средств»). В его рамках разрабатываются различные функции автоматического вождения для ежедневного использования, которые динамически адаптируют уровень автоматизации в соответствии с дорожной ситуацией и состоянием водителя. Проект также затрагивает ряд правовых вопросов, которые могут повлиять на успешный вывод на рынок данных технологий.

Для решения этой задачи при поддержке Евросоюза было организовано движение «Автоматизация транспортных средств и дорог» (англ. Vehicle & Road Automation, VRA), которое призвано создать сообщество экспертов и других заинтересо-

ТАБЛИЦА. ШЕСТЬ КЛАССОВ АВТОМАТИЗАЦИИ УПРАВЛЕНИЯ АВТОМОБИЛЕМ

Уровень автоматизации согласно SAE	Наименование	Общее определение	Рулевое управление и управление ускорением / торможением	Мониторинг вождения	Отклик на предупреждения по обратной связи во время вождения	Возможности системы автоматики (режимы вождения)
Водитель самостоятельно отслеживает ситуацию и управляет процессом вождения						
0	Без участия автоматики	Управление режимом движения осуществляется непосредственно самим водителем при помощи системы рулевого управления или путем управления режимом ускорения / торможения, на основании воспринимаемой непосредственно им самим информации о дорожной обстановке. Водитель самостоятельно выполняет все необходимые действия в зависимости от текущей задачи по управлению ТС.	Водитель	Водитель	Водитель	–
1	Помощь водителю	Режим движения обеспечивается одной или несколькими системами поддержки водителя как в части рулевого управления, так и посредством режимов ускорения / торможения. Для этого используется информация об окружающей обстановке, которую также предоставляют системы поддержки водителя. Водитель самостоятельно предпринимает все необходимые действия для выполнения текущей задачи по управлению ТС.	Водитель и система автоматики	Водитель	Водитель	Некоторые режимы движения
2	Частичная автоматизация вождения	Частичное управление режимом движения путем применения одной или нескольких систем автоматизации и помощи водителю в части рулевого управления и режимов ускорения / торможения, с использованием информации об окружающей дорожной обстановке. Водитель самостоятельно предпринимает все необходимые действия для выполнения текущей задачи по управлению ТС.	Система автоматики	Водитель	Водитель	Некоторые режимы движения
Управление автомобилем осуществляет автоматизированная система вождения, которая контролирует процесс вождения						
3	В зависимости от условий	В зависимости от конкретной дорожной обстановки производительность автоматизированной системы управления всеми аспектами, необходимыми для вождения ТС, позволяет организовать управление ТС, даже если водитель должным образом не отвечает на запрос о необходимости принятия тех или иных конкретных мер.	Система автоматики	Система автоматики	Водитель	Некоторые режимы движения
4	Высокая автоматизация вождения	Производительность автоматизированной системы управления всеми аспектами, необходимыми для вождения ТС, позволяет организовать его управление, даже если водитель должным образом не отвечает на запрос о необходимости принятия тех или иных конкретных мер по управлению ТС.	Система автоматики	Система автоматики	Система автоматики	Некоторые режимы движения
5	Полная автоматизация вождения	Полное непрерывное управление движением ТС с помощью автоматизированной системы вождения. Осуществляется путем управления всеми режимами вождения, которыми может управлять водитель данного ТС, во всех возможных ситуациях на дороге и при любых условиях вождения.	Система автоматики	Система автоматики	Система автоматики	Все режимы движения

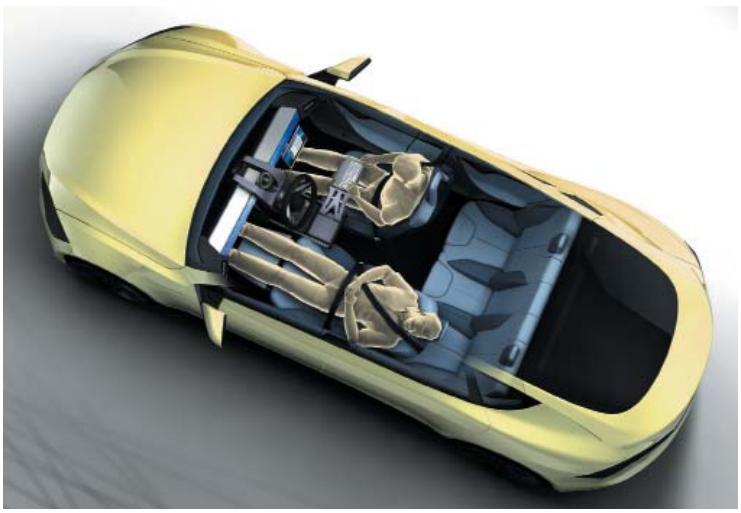
ванных сторон для развития автоматизированных ТС и сопутствующей инфраструктуры в Европе.

В этом направлении работают и некоторые компании. Так, Volkswagen принимает активное участие в формировании европейского законодательства, включая разработку прогрессивной поправки к Правилам 79 ЕЭК (ЕЭК — Европейская экономическая комиссия ООН) в отношении рулевого оборудования.

Правительство Японии тоже ведет подготовку законов, регулирующих использование автомобилей без водителя. Специалисты уже создали классификацию автоматизированного вождения: она делится на четыре класса, один из которых — это полностью автономное вождение.

В Китае компания Baidu также работает над созданием автономного автомобиля в сотрудничестве с компанией BMW. Китайское законодательство достаточно гибкое, что позволяет правительству быстро вносить необходимые изменения. Однако сложность поставленных перед ними задач не будет отличаться от других стран.

Индия тоже задумывается над проблемой автономного вождения, но ее решению мешают трудноизменяемое законодательство и сложности с внедрением нужных правил из-за различий в инфраструктуре.



ПОДХОДЫ К РАЗРАБОТКЕ

С учетом всего вышесказанного можно выделить одну из основных проблем в этой области — как же создать код ПО, который был бы и безопасным, и надежным? Как уже упоминалось, стандарт ISO 26262 запускает процесс разработки такого кода, который включает в себя стандарты кодирования и инструменты проверки кода.

Обеспечение безопасности системы начинается с разработки таких функций, как:

- Разделение приложений. Подразумевается, в частности, разделение с помощью брандмауэров на приложения с критической безопасностью (таких как рулевое управление и тормоза), менее критичные приложения и на те, которые имеют связь с окружающим миром (например, информационно-развлекательные).
- Ограничение в части коммуникации.
- Проверка и утверждение (валидация) принимаемых и передаваемых данных.

Поскольку основная часть ПО в этой отрасли пишется на языке C, хорошей отправной точкой для безопасного и надежного кода является стандарт разработки ПО на языке C в рамках стандарта MISRA C:2012 (MISRA 3)[5]. Он обеспечивает набор правил для написания программ на языке C, которые, наряду с отсутствием неопределенности поведения, включают в себя правила, улучшающие обслуживание, проверяемость, компактность и читабельность исходного кода. Также правила MISRA во многом совпадают с таблицами соответствия ISO 26262-6.

Недавно MISRA опубликовала изменение 1 к MISRA 3. Оно содержит 14 новых правил, которые позволят еще шире использовать MISRA в сфере разработки безопасных систем.

В соответствии со стандартом ISO 26262 неотъемлемой частью разработки являются и соответствующие инструменты. Так, программы статического анализа кода являются важной составляющей управления качеством кода, обеспечивая как контроль качества кода, так и его соответствие стандартам кодирования, таким как MISRA. Программы тестирования дают дополнительную уверенность в качестве ПО, а программы проверки измеряют, насколько хорошо ПО выполняет свои функции.

Таким образом, мы видим, что уже сейчас можно создавать и безопасные ТС, и надежное ПО. При этом организации, которые уже перестроили свои процессы разработки в соответствии с требованиями ISO 26262, обнаружили, что даже на начальном этапе внедрения и обучения они начинают выигрывать в части эффективности и получают от этого дополнительную прибыль. ●

ЛИТЕРАТУРА

1. ISO 26262-1:2011 «Road vehicles — Functional safety — Part 1: Vocabulary».
2. ГОСТ Р ИСО 26262-1-2014 «Дорожные транспортные средства. Функциональная безопасность. Часть 1. Термины и определения».
3. IEC 61508-1:2010 «Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 1: General requirements».
4. IEC 61508-2:2010 «Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 2. Requirements for electrical/electronic/programmable electronic safety-related systems».
5. ГОСТ Р МЭК 61508-1-2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования».
6. ГОСТ Р МЭК 61508-2-2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам».
7. ISO 26262-6:2011 «Road vehicles — Functional safety — Part 6: Product development at the software level».
8. ГОСТ Р ИСО 26262-6-2014 «Дорожные транспортные средства. Функциональная безопасность. Часть 6. Разработка программного обеспечения изделия».
9. J3016_20160 «Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems».

[5] MISRA (Motor Industry Software Reliability Association) — международная ассоциация, в числе прочего публикующая рекомендации по программированию на языках C и C++. — Прим. пер.