Онтологии и безопасность автономных (беспилотных) автомобилей

О.Н. Покусаев, В.П. Куприяновский, Д.В. Катцын, Д.Е. Намиот

***Аннотация*—В статье обсуждаются вопросы, связанные с архитектурой программного обеспечения автономных (беспилотных) автомобилей. В работе используется англоязычная аббревиатура CAV (Connected Autonomous Vehicle). Автомобильные транспортные средства имеют сегодня гораздо более сложные компьютерные системы, чем самолеты, из-за сложных взаимодействий автономных автомобилей на дорогах. Объемы кодов программного обеспечения для систем управления самолетами и CAV разняться в десятки раз. Производить такой большой код с требуемыми как функциональными, так и временными характеристиками, а также обеспечивать его безопасность старыми методами просто невозможно. В работе рассмотрены сервисы CAV и устройства, через которые они реализуются. В работе описывается процесс построения программного кода для CAV. Рассмотрение этих процессов с точки зрения мировых стандартов приводит нас к кибер-физическим системам и онтологиям. В работе описываются онтологические домены кибер-физических систем, затрагивающие CAV. Рассматриваются международные стандарты, связанные с онтологическим проектированием CAV и обеспечением безопасности. Подробно анализируются вопросы безопасности CAV, потенциальные уязвимости и возможные атаки. Также рассмотрены основные области для улучшения проектирования CAV. К ним отнесены безопасность по дизайну, предоставление обновлений программного обеспечения CAV на весь срок жизни, избежание неограниченных окон уязвимостей, а также повышение прозрачности цепочки поставок с помощью онтологических отраслевых решений и системы оценки кибербезопасности.**

***Ключевые слова*— автономные автомобили; безопасность; онтологии; программное обеспечение.**

Статья получена 30 декабря 2018. Рекомендована организационным комитетом III Международной научной конференции «Конвергентные когнитивно-информационные технологии».

Покусаев Олег Николаевич – кандидат экономических наук, исполнительный директор Российской Академии транспорта; директор Центра высокоскоростных транспортных систем РУТ (МИИТ) (email: o.pokusaev@rut.digital)

Куприяновский Василий Павлович – эксперт Центра высокоскоростных транспортных систем РУТ (МИИТ); Национальный Центр Цифровой Экономики МГУ имени М.В. Ломоносова (email: v.kupriyanovsky@rut.digital)

Катцын Дмитрий Владимирович кандидат технических наук, доцент кафедры «Высокоскоростные транспортные системы» РУТ (МИИТ) (email: kattzyn@center.rzd.ru)

Намиот Дмитрий Евгеньевич – кандидат физико-математических наук, старший научный сотрудник лаборатории Открытых информационных технологий факультета ВМК МГУ имени М.В. Ломоносова; РУТ (МИИТ) (email: dnamiot@gmail.com)

I. Введение. Архитектура беспилотных (автономных) автомобилей

Автомобильные транспортные средства имеют сегодня гораздо более сложные компьютерные системы, чем самолеты, из-за сложных взаимодействий беспилотных (автономных) автомобилей на дорогах. Далее в работе мы будем употреблять английскую аббревиатуру CAV (Connected Autonomous Vehicle). Объемы кодов программного обеспечения для систем управления самолетами и CAV сильно разнятся, и эта разница визуально показана на рисунке 1 ниже.

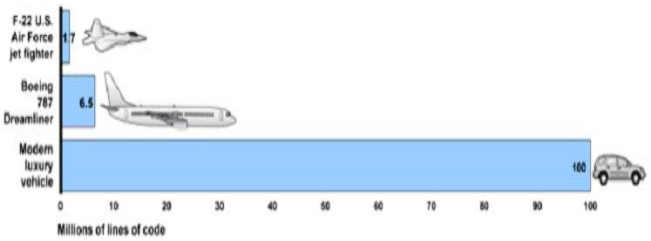


Рис. 1. Визуальная картина для оценки объема программных кодов для управления боевой авиацией, гражданской авиацией и CAV, принимая последнее за 100 % [1].

Важно другое, что производить такой код с требуемыми как функциональными, так и временными характеристиками просто невозможно старыми методами [1, 2, 3] и, тем более, обеспечивать его безопасность. Это очень сложный процесс уже на уроне бортовой сети CAV, включающий граничные сети и облачные вычисления и возможно, что в скором будущем там появятся радиокоммуникации, как они уже появляются на самолетах [4].

На рисунке 2 показаны ограничения применения старых методов (например, реляционные базы данных уже давно исключены из списка рассмотрения претендентов). Какие сервисы CAV реализуются и через какие устройства автомобиля показано на рисунке 3.

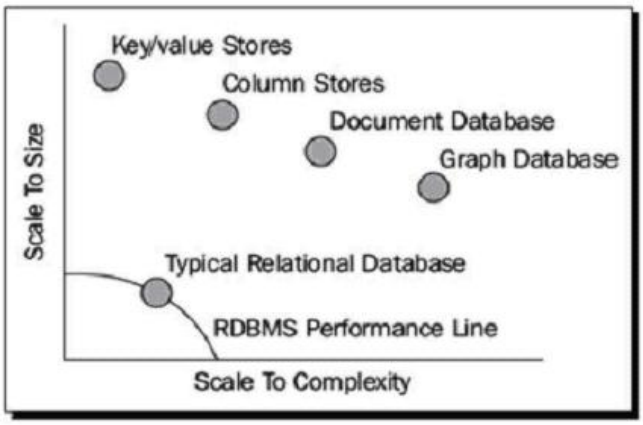


Рис. 2. Масштабируемость возможностей создания программного обеспечения в зависимости от его объема и сложности [4]

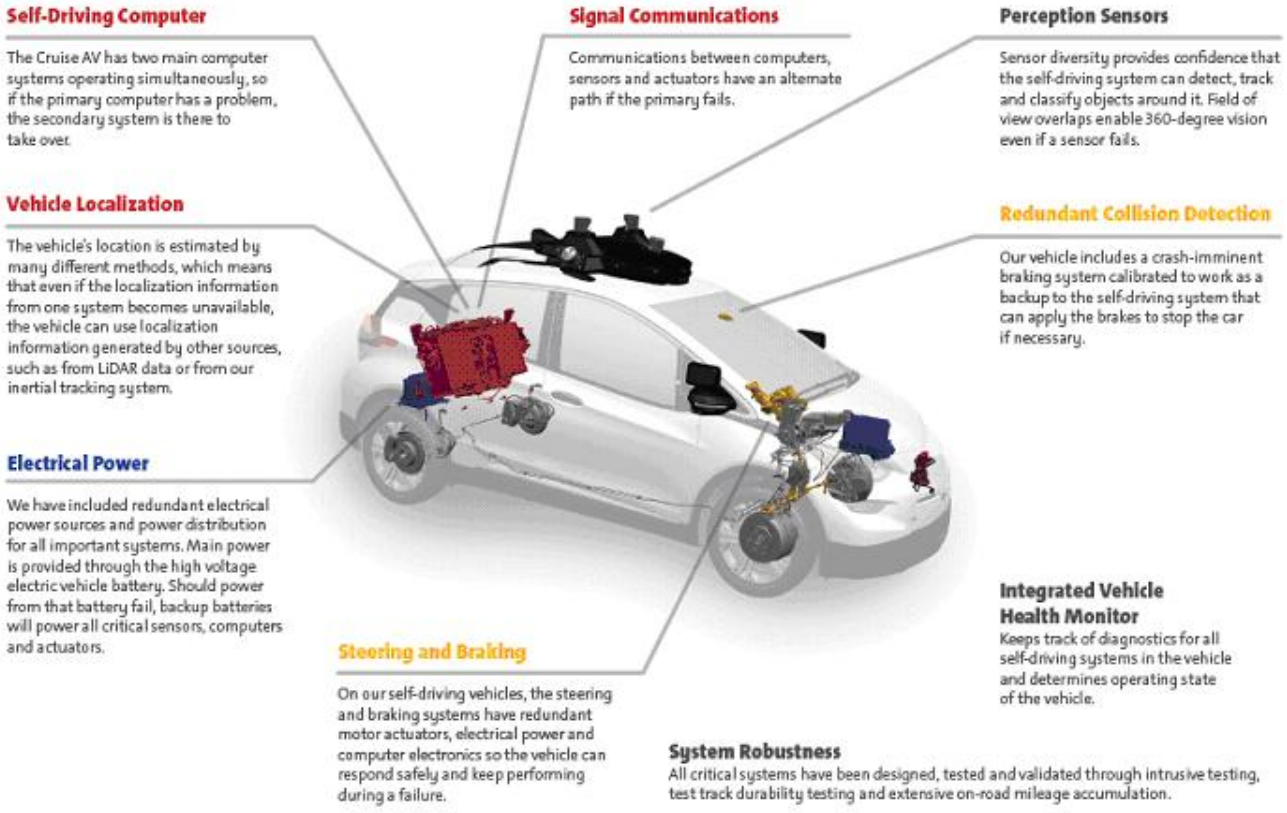


Рис. 3. Какие сервисы CAV реализуются и через какие устройства [5]

Сегодняшний верхний граф программно-информационные подсистемы CAV можно увидеть на рисунке 4, и каждый блок этого графа может быть описан множеством томов (искусственный интеллект, машинное обучение, точное цифровое картографирование и т.п.).

Отдельная часть связана с управлением автомобилем. Процесс построения систем программного кода CAV с точки зрения автомобиля сегодня можно увидеть на рисунке 5.

Рассматривая эти процессы с точки зрения мировых стандартов, мы приводим рисунок 6, и дальнейшее развитие приводит нас к системам CPS или к кибер-физическим системам [4, 6, 7, 8] и онтологиям. Рисунок 7 описывает онтологические домены CPS, затрагивающие CAV.

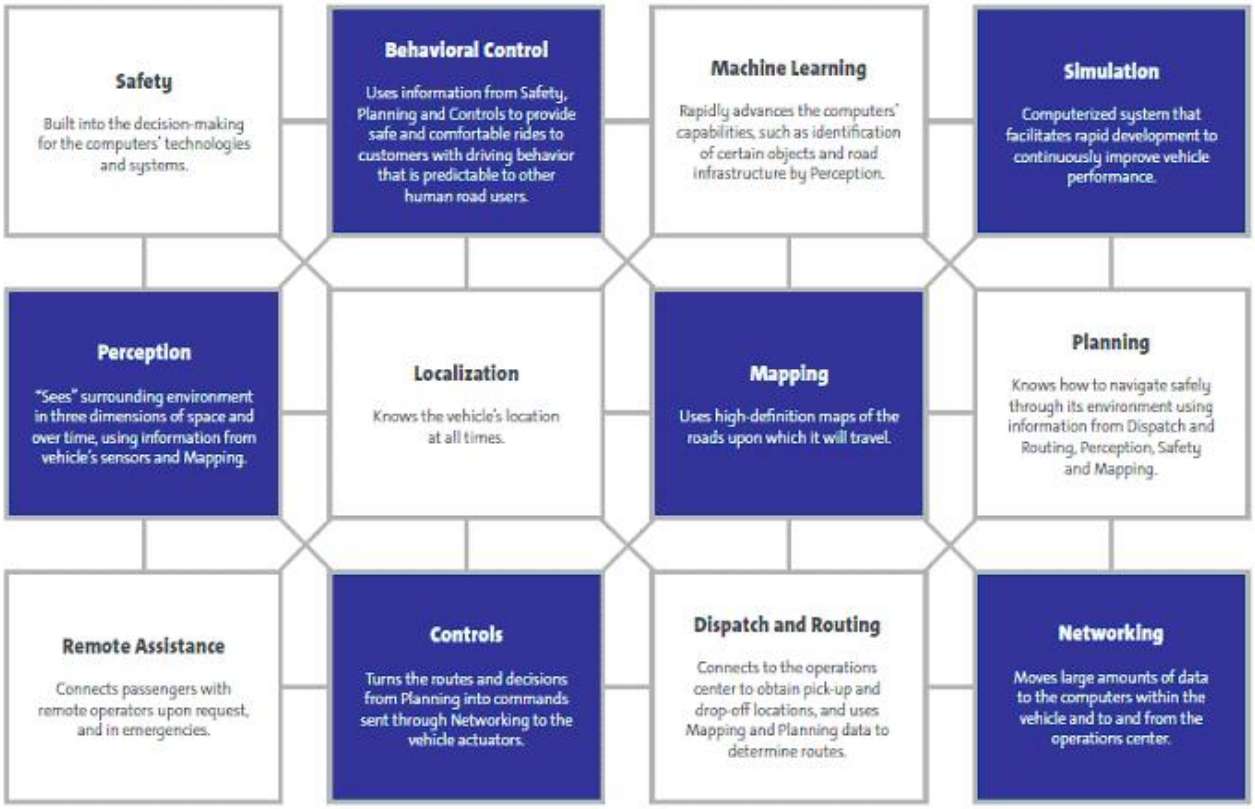


Рис. 4. Сегодняшние программно-информационные подсистемы CAV [5]

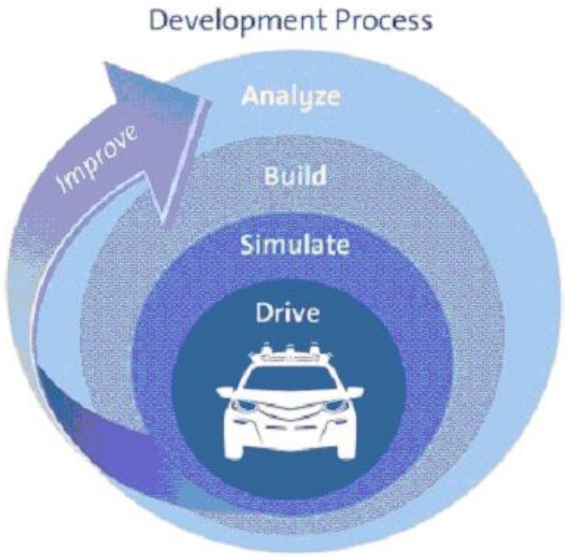


Рис. 5. Как представляется процесс построения систем программного кода CAV с точки зрения автомобиля сегодня [5]

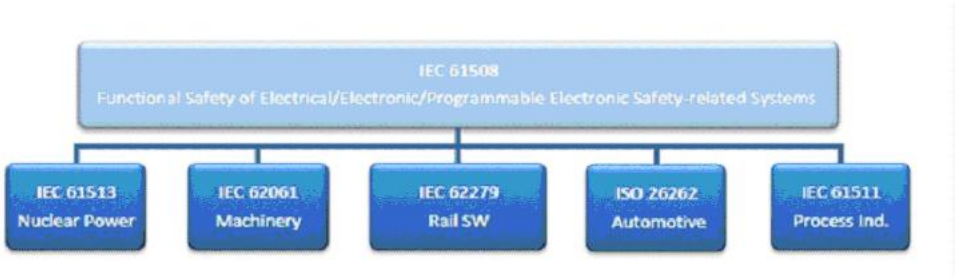


Рис. 6. IEC 61508 и соответствующие стандарты верхнего уровня применяемы для CAV [9]

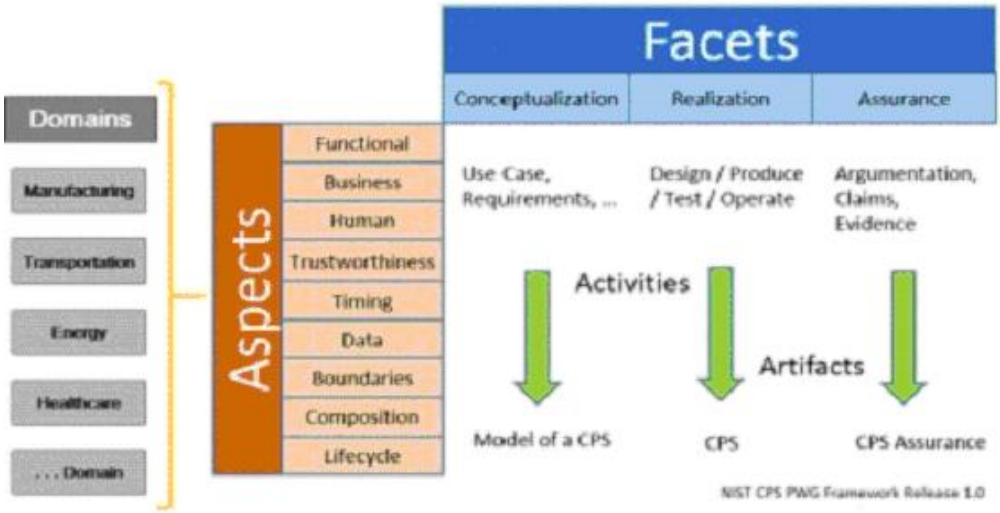


Рис. 7. Онтологические домены CPS, затрагивающие CAV [25]

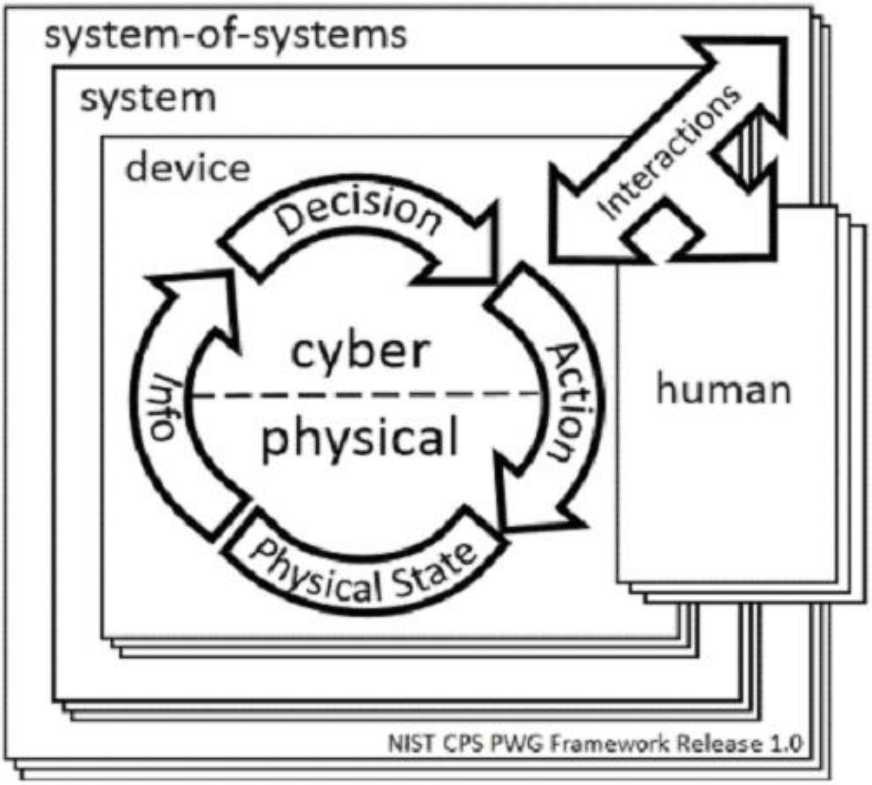


Рис. 8. Общая архитектура CPS с участием человека, интегрирующая в системе систем устройства, информацию, решения и действия, определяющие физические состояния предмета [9]

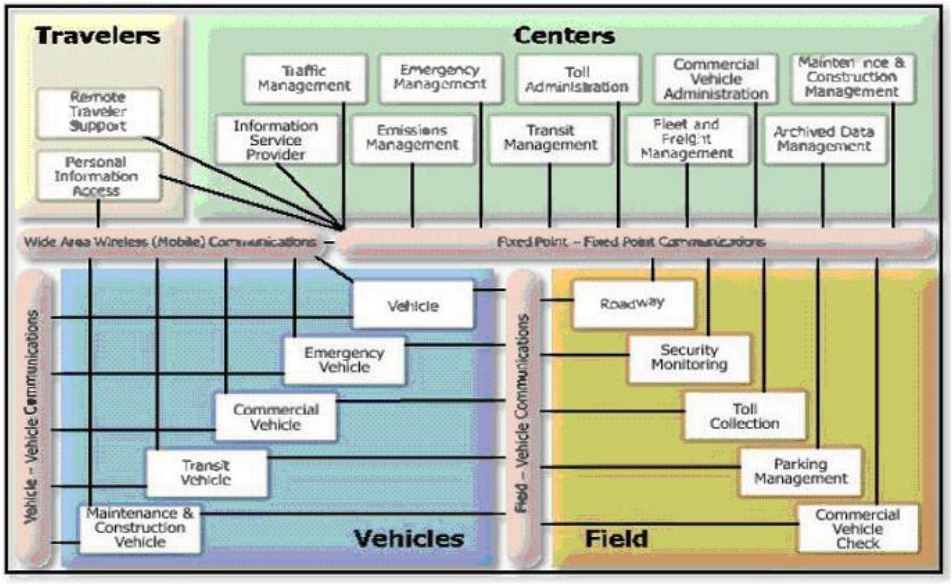


Рис. 9. Система CAV как инженерная онтология автомобиля и его окружения в CPS [9].

Общая архитектура CPS с участием человека интегрирующая в системе систем устройства, информацию, решения и действия, определяющие физические состояния предмета приведена на рисунке 8. Система CAV как инженерная онтология автомобиля и его окружение в CPS приводится на рисунке 9.

Национальный инфраструктурный план США по CAV или NIPP описывает рекомендуемую структуру управления рисками, в которой упор делается на обмен информацией между членами заинтересованных сторон для создания надежной, взаимозависимой транспортной сети. Структура была разработана так, чтобы быть гибкой для работы во всех выбранных DHS режимах CI (департамент внутренней безопасности США или DHS), но достаточно хорошо определенной, чтобы осуществлять обмен рисками, угрозами и контрмерами между членами, чтобы они были продуктивными (рисунок 10).

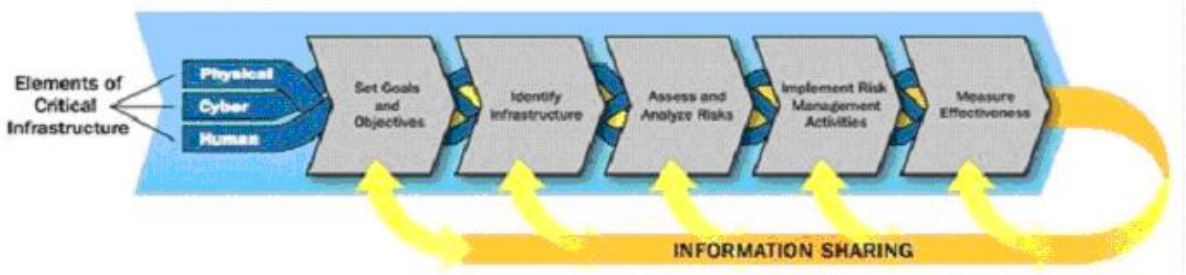


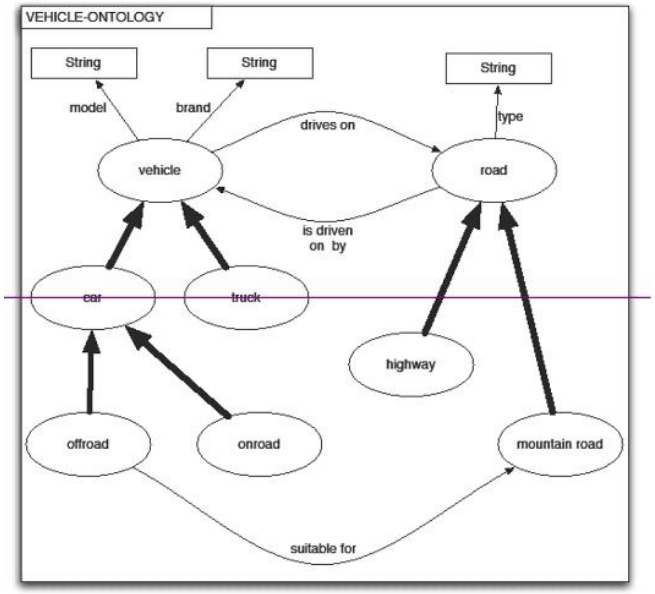
Рис. 10. Структура управления рисками NIPP и поток данных [10]

II Современное состояние автомобильной онтологии и CAV

Стандарт ISO 26262 просто необходим, как базовый для онтологии CAV. Стандарт ISO 26262 (ISO, 2011-2012 и [11]) описывает требования функциональной безопасности, применяемые к разработке бортовых электронных / электрических систем на дорожных транспортных средствах. Для понимания на рисунке 11 мы приводим совсем общий пример онтологии транспортного автомобильного средства CAV.

Этот стандарт (ISO 26262) распространяется на IEC 61508 (IEC, 2010), применяемый для обеспечения функциональной безопасности электрических / электронных / программируемых электронных систем безопасности, связанных с безопасностью. Но ISO 26262 - это не только адаптация IEC 61508 к конкретному автомобильному домену. На самом деле, новый стандарт применяется ко всем видам деятельности в течение всего жизненного цикла безопасности систем, связанных с безопасностью, состоящих из электрических, электронных и программных компонентов на дорожных транспортных средствах. Таким образом, стандарт ISO 26262 обеспечивает соответствующие требования и процессы в более общей, полной, сочлененной и самосогласованной структуре, чем IEC 61508. ISO 26262 поддерживает весь жизненный цикл безопасности автомобилей (управление, разработка, производство, эксплуатация, обслуживание, вывод из эксплуатации) и содержит автомобильную схему классификации опасностей. Ключевой вопрос ISO 26262 - это определение целей, которые компонент / система до интеграции на транспортном средстве должен выполнять для обеспечения соответствия установленным требованиям безопасности в зависимости от сценария применения (интеграция транспортного средства, характеристик транспортного средства и предполагаемого поведения и характеристик, связанных с окружающими условиями и

рабочими ситуациями).



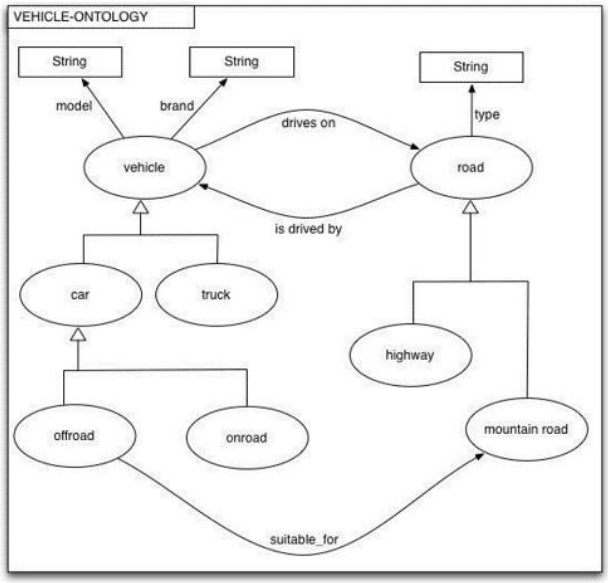


Рис. 11. Пример онтологии транспортного средства [11]

Кроме того, безопасность системы достигается с помощью ряда мер безопасности, которые реализуются в различных технологиях (например, механические, гидравлические, пневматические, электрические, электронные, программируемые электронные и т. д.) и применяется на разных уровнях процесса разработки. И хотя ISO 26262 связан с функциональной безопасностью электрических и электронных систем, его структура может применяться к системам, связанным с безопасностью, на основе других технологий.

Кроме того, его формальная и структурная полнота, от проектирования до снятия с эксплуатации транспортного средства, обеспечивает уровень ответственности (ответственности) автопроизводителя в отношении соответствия безопасности производимым автомобилям. Применение ISO 26262 в автомобильном домене направлено на предоставление необходимой документации, которая подтверждает эффективность поведения безопасности транспортного средства и его компонентов. Этот результат можно было бы признать на уровне закона, поскольку наилучшая практика, на которую ссылаются, но (до сих пор) еще не сертифицирована официальным образом организационными органами, внешними по отношению к автопроизводителям.

Стандарт ISO 26262 состоит из десяти частей, связанных друг с другом:

- Часть 1: Словарь
- Часть 2: Управление функциональной безопасностью
- Часть 3: этап концепции
- Часть 4: Разработка продукта на системном уровне
- Часть 5: Разработка продукта на аппаратном уровне
- Часть 6: Разработка продукта на уровне программного обеспечения
- Часть 7: Производство и эксплуатация
- Часть 8: Вспомогательные процессы
- Часть 9: Уровень целостности автомобильной безопасности (ASIL) - ориентированный и ориентированный на безопасность анализ
- Часть 10: Руководство по ISO 26262

III Онтологические аспекты стандарта для CAV

Терминология, описанная в части 1 (Словарь) стандарта ISO 26262, охватывает (по определению) основные темы онтологии об эксплуатационной безопасности автомобилей. Некоторые из стандартных определений являются конкретными в рабочем процессе, в то время как другие являются общими для полей приложений аппаратуры и программного обеспечения, связанных с общей автомобильной средой.

Рамки платформы CRYSTAL [11] должны иметь дело с логическими структурами, терминами и определениями в отношении систем, архитектур, инструментов и их функциональной совместимости, а в ISO 26262 [ISO, 2011-2012, часть 1]:

- элементы, связанные со структурами и элементами HW и SW в анализируемой системе (например, аппаратная часть, компонент, элемент, система, элемент, встроенное программное обеспечение, программный инструмент, модуль программного обеспечения, компонент программного обеспечения, архитектура, распределение и т. д.).
- конкретные термины, связанные с развертыванием процесса оценки функциональной безопасности автомобилей по всей цепочке разработки продукта (например, план безопасности, элемент, анализ воздействия, анализ рисков и оценка рисков, проверка, проверка, подтверждение, анализ безопасности и т. Д.).

Между ISO 26262 и общим процессом проектирования существует двунаправленная связь, как показано на рисунке 12. Оба будут влиять на онтологию автомобильных доменов CAV, но ISO влияет на процесс автомобильного проектирования, а также элементы процесса проектирования становятся актуальными в ISO, и поэтому могут быть перекрывающиеся словари, которые мы должны учитывать при построении

онтология автомобильной области.

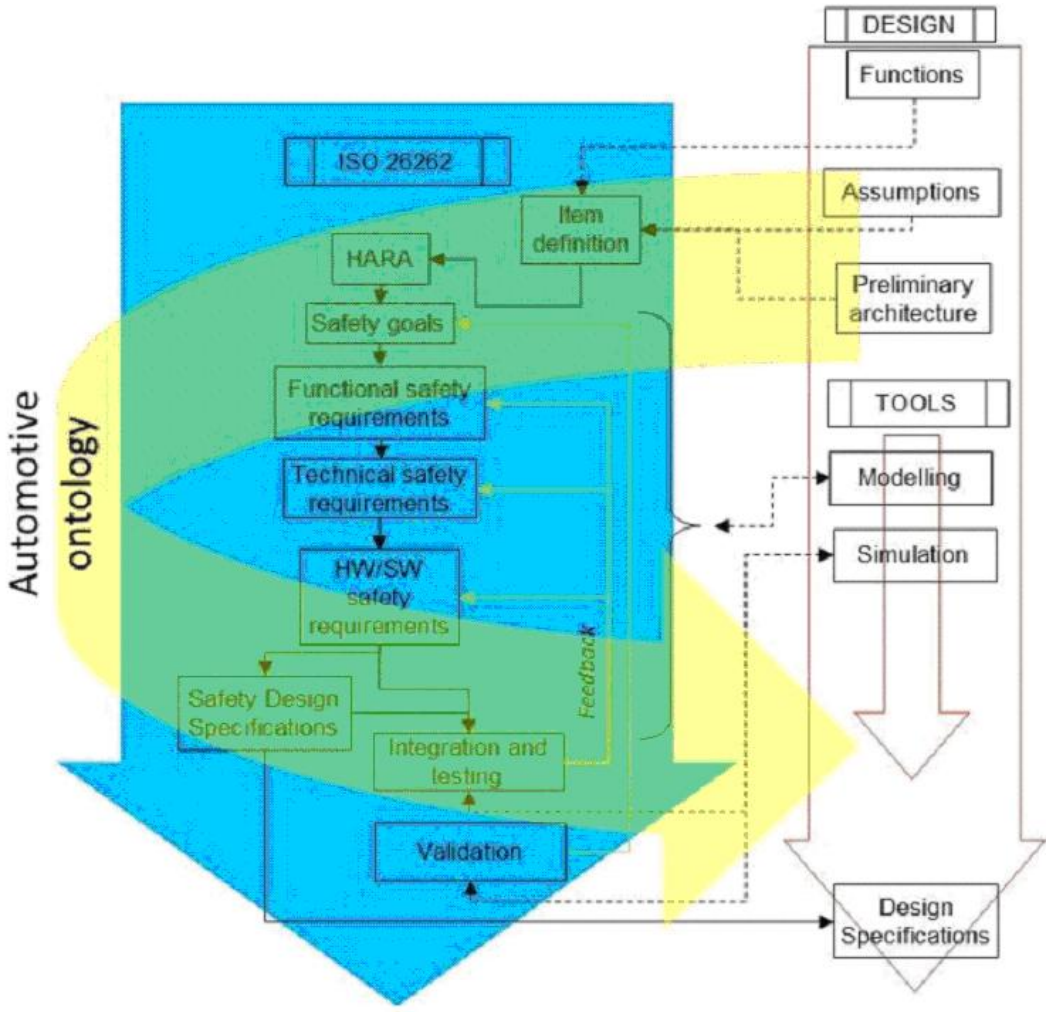


Рис. 12. Онтология ISO 26262 по сравнению с автомобильным дизайном и проектированием CAV [11]

Терминологию ИСО 26262 можно рассматривать как базовую ссылку для развертывания онтологии более высокого уровня, подходящей для моделирования более общей структуры процесса, т. е. процесса оценки функциональной безопасности автомобилей. Это будет объяснено более точно в следующем развитии и стандартизации такой как, например, европейская [12,13,14,15,16] .

IV Развитие решений безопасности CAV и стандартизация

Следуя ранее объявленным подходом максимального использования стандартов, мы опираемся на обширный пул источников [17-38], из которых, пожалуй, стоит выделить SAE J3061 и ISO / SAE 21434 опивающее начальное руководство по кибербезопасности для кибер-физических Систем транспортных средств. Эти документы обеспечивают:

- Анализ угроз и оценка рисков по сравнению с анализом опасности
- Анализ дерева атаки и анализ дерева отказов
- Контрмеры кибербезопасности должны соответствовать мерам безопасности и механизмам безопасности
- Группе безопасности кибербезопасности и функциональной безопасности необходимо взаимодействовать
- Подразумевает необходимость в аппаратных элементах для кибербезопасности.

Таблица 1. Международная стандартизация и самые значительные инициативы для CAV [17]

Body	Working Group	Objectives
SAE	Vehicle Electrical System Security Committee	Provide a Cybersecurity Guidebook for Cyber-Physical Vehicle Systems. Requirements for Hardware-Protected Security for Ground Vehicle Applications.
ISO	TC22 /SC 32/ WG11	Coordinate standardization activities with SAE Vehicle Electrical System Security Committee for Automotive security engineering.
ETSI	TC ITS WG5	Assurance of ITS solutions conformity to regulatory requirements for privacy, data protection, lawful interception and data retention.
IEEE	SCC42/SCC Type 2	Coordination of IEEE standardization activities for technologies related to transportation, especially in the areas of connected vehicles, autonomous/ automated vehicles, inter- and intra-vehicle communications, and other types of transportation electrification.

Вопросы любой безопасности и защиты всегда решаются по месту с учетом существующих в конкретном месте рисков и с безусловным соблюдением требований российского законодательств, норм и правил. Поэтому ранее приведенный перечень публикаций по этому направлению мы не считаем

окончательным и его, безусловно, надо будет расширять. В качестве первого приближения можно посмотреть российские публикации по теме безопасности инфраструктур и антитеррору [39], по онтологии безопасности [40]. На рисунках 13 и 14 приведены иллюстрации безопасности по умолчанию (заложенные при проектировании) для автомобилей CAV как многослойной онтологически связанной структуры в жизненно цикле автомобиля CAV, которые также подробно обсуждались в российской публикации [41].

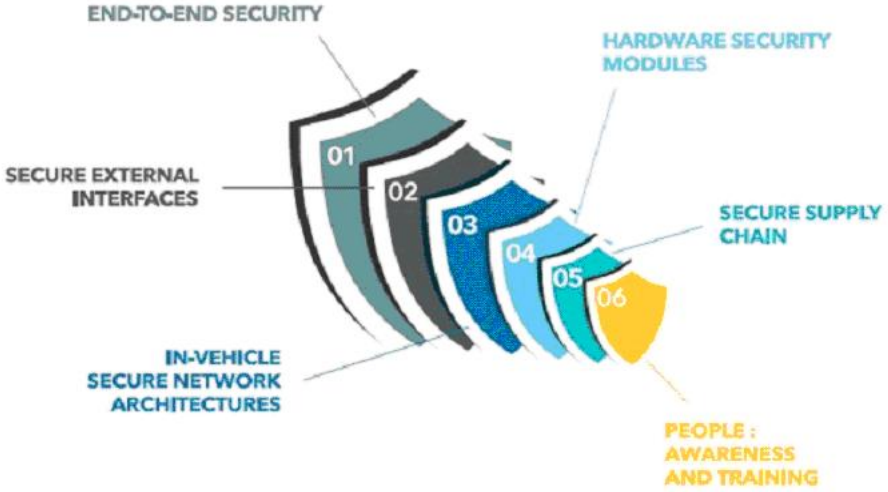


Рис. 13. Темы безопасности по умолчанию (заложенные при проектировании) для автомобилей CAV как многослойная онтологически связанная структура [17]

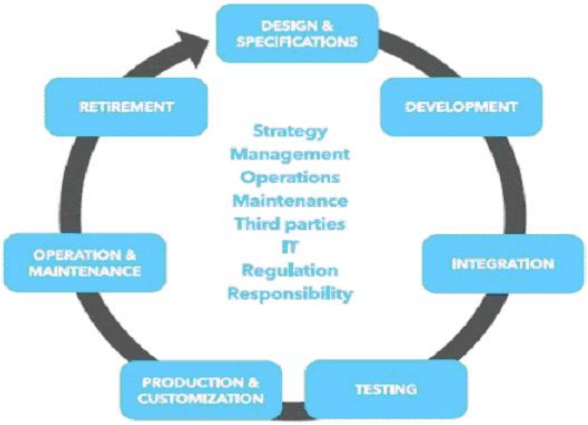


Рис. 14. Безопасность по умолчанию в жизненно цикле автомобиля CAV [17]

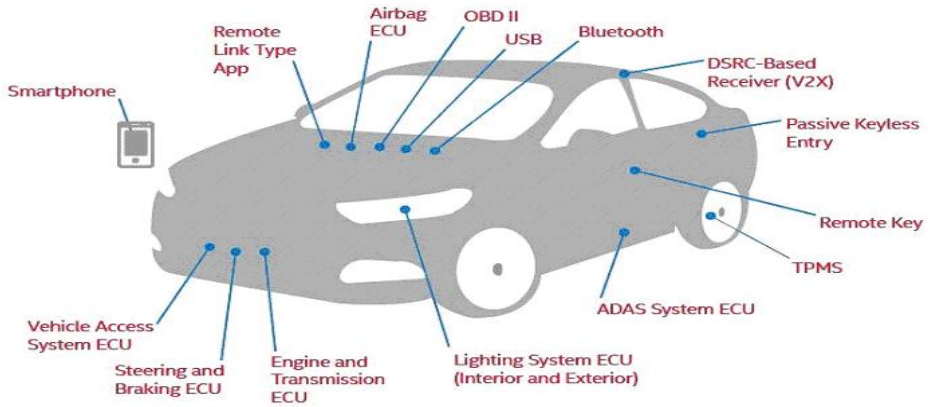


Рис. 15. Потенциальные шлюзы для атак на CAV [42]

Чтобы показать практическое применение изложенных выше подходов, мы приводим рисунок 15 о потенциальных шлюзах атак на системы безопасности

согласно [43]. Сегодня это изучение происходит на уровне текущих пониманий разработки и накопленной практики, о которой мы уже говорили выше. Эти шлюзы представляют собой:

• Электрические блоки управления (ECU)
• Подушка безопасности, усовершенствованная система помощи водителю, двигатель, рулевое управление и тормоза и т. д.
• Диагностический порт бортовой диагностики (OBD) II
• Выделенный приемник с малой дальностью связи
• USB-порты
• Пассивный Keyless Entry / Remote Key
• Приложение для удаленного соединения
• Система контроля давления в шинах (TPMS)

Далее мы даем объяснение ключей атаки, следуя [43]:

• Электронные блоки управления (ECU) - это встроенные системы, которые управляют одной или несколькими электрическими системами или подсистемами внутри транспортного средства и подключаются через внутреннюю сеть. Они управляют такими системами, как двигатель и трансмиссия, рулевое управление и тормоза, информационно-развлекательная система, освещение и т. Д. Риски возникают, когда доступ к ECU (обычно периферийным ECU, таким как информационно-развлекательная система) нарушается, а злонамеренные участники имеют доступ к некоторым ECU или всей сети. Сегодня у транспортных средств есть до 100 ECU.

• Диагностический порт OBD II. Каждый автомобиль, изготовленный после 1996 года и продаваемый в США, должен иметь OBD II. Первоначально порт был уполномочен обеспечивать мониторинг выбросов и т. д. Он все чаще используется для облегчения недиагностических функций, таких как включение Wi-Fi, или предоставления страховой компании возможности отслеживать использование посредством привязки «ключа» к порту. Эти порты могут обеспечить доступ для злоумышленников в защищенную систему.

• Приемники на основе DSRC. DSRC продвигается как способ поощрения коммуникаций V2V и транспортных средств к инфраструктуре (V2I). Коротковолновые коммуникации могут быть подвергнуты подделке и другим атакам. Теперь есть толчок, чтобы перейти к более продвинутым коммуникациям на основе 5G.

V Общие уязвимости безопасности

К общим уязвимостям относятся:

• Программные ошибки. Подключенные транспортные средства сегодня содержат более 100 миллионов строк кода. Больше кода означает больше возможностей для багов и ошибок. Внезапные отказы (Glitches), даже когда они могут быть непреднамеренными, могут быть использованы.

• Отсутствие единого источника знаний или контроль над исходным кодом. Программное обеспечение для различных компонентов подключенных транспортных средств написано разными разработчиками, и ни один источник не имеет знаний или не контролирует исходный код.

• Увеличение использования приложений оставляет уязвимость. Потребители используют все большее число приложений для смартфонов для взаимодействия со своими подключенными автомобилями, которые помогают выполнять определенные функции. Исследователи уже продемонстрировали слабые места в некоторых из этих приложений. Вероятно, вы увидите распространение в использовании вредоносного ПО.

• Потребность в постоянных обновлениях может быть пропущена - с увеличением использования подключенных функций возникает повышенная потребность в непрерывных обновлениях для исправления сбоев и защиты транспортных средств. Существует риск того, что эти обновления могут быть упущены или что злоумышленники могут заразить обычные обновления.

Угрозы и проблемы кибербезопасности CAV:

• Те же самые типы атак, которые возможны в любом подключенном устройстве, как правило, возможны в подключенных транспортных средствах после получения доступа.

• Например, атаки типа «отказ в обслуживании» (например, использование системы шины контроллера CAN), удаленный доступ и управление (например, событие «человек в середине» -MiM) и т. д.

• Разница между такими атаками против обычных устройств IoT и атак в подключенном или автономном транспортном средстве - это вероятность увеличения риска жизни и имущества в контексте транспортного средства.

Основные возможности для реализации кибербезопасности CAV сегодня это:

• Обеспечить многоуровневую защиту. Начиная с уровня отдельных ECU, продвигаясь на уровень, чтобы включить программное обеспечение для защиты внутренней сети транспортного средства, изучая все сетевые коммуникации и создавая механизмы для предотвращения атак от продвижения по сети.

• Защищать от потенциальных внешних шлюзов - Обеспечить, чтобы слабые звенья в безопасности автомобиля рассматривались как потенциальные угрозы, и защита встроена в систему. Это особенно справедливо для информационно-развлекательных или подобных внешних механизмов, которые разрабатываются или используются несколькими внешними объектами

• Обеспечить надежную защиту поставщиков и поставщиков. Подключенные и автономные транспортные средства состоят из подчастей и подсистем. Крайне важно проанализировать и контролировать политику и практику поставщиков и поставщиков.

• Содействовать своевременным обновлениям.

Компании должны своевременно и эффективно исправлять проблемы, как только будут выявлены проблемы.

Попытка добавить безопасность, вырвав прошлое и заменить его решениями, созданными с нуля, обычно не практична. Многое из того, что представлено как новое, опирается на компоненты, которые являются десятилетиями назад, и они потенциально скрывают скрытые недостатки, которые избегают даже самых бдительных инструментов и команд проверки. Современный новый код может быстро стать завтрашними «спагетти», когда команды перейдут, еще раз затрудняя усилия по реинжинирингу, если не применять онтологические подходы к проектированию и реализации CAV.

Автоматизация через онтологию может быть большой частью ответа. Многие подрядчики, поставщики управляемых услуг и интеграторы чрезмерно подчеркивают кадровые решения, а люди сегодня недостаточно надежны как носители знаний такого объема. Люди нуждаются в анализе и высокоценных задачах, но не могут наилучшим образом модифицировать миллионы строк кода для обеспечения проектирования, эксплуатации и безопасности, если задержка, проблемы с качеством или перерасход средств не встроены в структуру разбивки на работу (WBS) так четко, как их онтологический эквивалент.

Творческое использование автоматизации и онтологии является ключевым моментом, например, при применении приложений реального времени таких как Runtime Application Self Protection (RASP) или добавлений и изменений в существующие аппаратные следы или добавлении систем предотвращения вторжений в системы безопасности на основе AI (IPS) как в физические, так и в цифровые сети CAV.

Экономические преимущества подключения, автоматизации и спасения жизней являются в центре внимания OEM-производителей и поставщиков транспортных средств CAV. В то время как принципы кибербезопасности и конфиденциальности сегодня являются добровольными, они станут обязательными раньше, чем позже, если мышление программного обеспечения «бета как производство» подрывает более ориентированный на безопасность онтологический подход к машиностроению. Предотвратимые инциденты с безопасностью CAV могут потенциально подорвать доверие общественности и прогнозы масштабируемости, инвестиций и найма, на которые так много компаний полагаются. Кибербезопасность поистине проблематична. Следующие три области рассматриваются как основные CAV для улучшения:

1. Безопасность по дизайну и необходимостью уделять особое внимание внешнему объединению и тестированию на проникновение, хотя бы для того, чтобы свести к минимуму ущерб для гордости, который может понести многолетний опыт автомобильной промышленности, состоящий в союзе только с опытом работы в области кибербезопасности.

2. Предоставление обновлений программного обеспечения CAV на весь срок жизни, избежание неограниченных окон уязвимостей.

3. Повышение прозрачности цепочки поставок с помощью онтологических отраслевых решений и системы оценки кибербезопасности.

Однако не стоит никогда забывать, что всегда придется отвечать на простой вопрос: «Кто будет платить при аварии с участием CAV? (рисунок 16).

Рис. 16. Кто будет платить в случае аварии CAV? [43].

Библиография

[1] Todd Litman, Autonomous Vehicle Implementation Predictions .Implications for Transport Planning,Victoria Transport Policy Institute.24 July 2018

[2] ALESSANDRA PIERONI, NOEMI SCARPATO AND MARCO BRILLI, INDUSTRY 4.0 REVOLUTION IN AUTONOMOUS AND CONNECTED VEHICLE. A NON-CONVENTIONAL APPROACH TO MANAGE BIG DATA, Journal of Theoretical and Applied Information Technology ,15th January 2018. Vol.96. No 1, pp 10-18

[3] SAS Institute Inc., “The connected vehicle: big data, big opportunities,” SAS White Pap.,p. 10, 2016

[4] Куприяновский В. П. и др. Развитие транспортно-логистических отраслей Европейского Союза: открытый BIM, Интернет Вещей и кибер-физические системы //International Journal of Open Information Technologies. – 2018. – Т. 6. – №. 2.-С. 54-100

[5] 2018 SELF-DRIVING SAFETY REPORT GM 2018

[6] Куприяновский В. П., Намиот Д. Е., Синягов С. А. Кибер-физические системы как основа цифровой экономики //International Journal of Open Information Technologies. – 2016. – Т. 4. – №. 2. – С. 18-22.

[7] Куприяновский В. П. и др. Трансформация промышленности в цифровой экономике-проектирование и производство //International Journal of Open Information Technologies. – 2017. – Т. 5. – №. 1. – С. 50-70.

[8] Куприяновский В. П. и др. Трансформация промышленности в цифровой экономике-экосистема и жизненный цикл //International Journal of Open Information Technologies. – 2017. – Т. 5. – №. 1. – С. 34-49.

[9] CYBERSECURITY LITERATURE REVIEW AND EFFORTS REPORT .Prepared for: NCHRP Project 03-127 Cybersecurity of Traffic Management Systems, NCHRP 2018

[10] Cybersecurity in Automotive: How to stay ahead of cyber threats? Position paper, Altran 2018

[11] CRYSTAL State of the art for automotive ontology Deliverable No. D308.010 V1.1 Date 2014-06-05

[12] ETSI GR ENI 001 V1.1.1 (2018-04) Published Experiential Networked Intelligence (ENI); ENI use cases

[13] ETSI GS ENI 002 V1.1.1 (2018-04) Published Experiential Networked Intelligence (ENI); ENI requirements

[14] ETSI GR ENI 003 V1.1.1 (2018-05) Published Experiential Networked Intelligence (ENI); Context-Aware Policy Management Gap Analysis

[15] ETSI GR ENI 004 V1.1.1 (2018-05) Published Experiential Networked Intelligence (ENI); ENI General Terminology

[16] ETSI GR ENI 006 V1.1.1 (2018-05) Published Experiential Networked Intelligence (ENI); ENI Proof of Concept (PoC) Framework

[17] Cybersecurity in Automotive: How to stay ahead of cyber threats? Position paper, Altran 2018
[18] Common Criteria Recognition Arrangement, "Common Critera Portal," 3 11 2017. http://www.commoncriteriaportal.org/cc/.
[19] "Part 1: Introduction and General Model V3.1R4," Common Criteria Recognition Arrangement (CCRA), 2012.
[20] "Part 2: Security Functional Components V3.1R4," Common Criteria Recognition Arrangement (CCRA), 2012.
[21] "Part 3: Security Assurance Components V3.1R4," Common Criteria Recognition Arrangement (CCRA), 2012.
[22] International Organization for Standardization, "ISO/IEC 27000 - Information Secuity," ISO/IEC, 2013. https://www.iso.org/isoiec-27001-information-security.html.
[23] ISO/IEC, Information Technology - Security Techniques - Vulnerability Disclosure, Switzerland: ISO/IEC, 2014.
[24] Cyber Physical Systems Public Working Group, "Framework for Cyber-Physical Systems," National Institute of Science and Technology, 2016.
[25] United States Department of Homeland Security, "Cybersecurity Capability Maturity Model (C2M2) Program," United States Department of Homeland Security, https://energy.gov/oe/cybersecurity-critical-energy-infrastructure/cybersecurity-capability-maturitymodel- c2m2-program
[26] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity version 1.1 (Draft), https://www.nist.gov/cyberframework
[27] United States Department of Homeland Security, "C3 Voluntary Program FAQs," United States Department of Homeland Security, 2015. NCHRP 03-127 Task 1 - Security Literature Review and Efforts Report Cybersecurity of Traffic Management Systems Final January 12, 2018
[28] Department of Homeland Security, "Study on Mobil Device Security," 4 May 2017. https://www.dhs.gov/publication/csd-mobile-device-security-study.
[29] National Institute of Standards and Technology, "Assessing Threats to Mobile Devices & Infrastructure, The Mobile Threat Catalogue," NISTIR8144, 12 September 2016. https://csrc.nist.gov/CSRC/media/Publications/nistir/8144/draft/documents/nistir8144_draft.pdf.
[30] F. T. Adminisration, "National ITS Architecture Subsystems and Communications," Federal Transit Adminisration 2017.
[31] The Roadmap to Secure Control Systems in the Transportation Sector Working Group, "Roadmap to Secure Control Systems in the Transportation Sector," United States Department of Homeland Security, 2012.
[32] U.S. Department of Homeland Security, "Transportation Industrial Control System (ICS) Cybersecurity Standards Strategy," 2013.
[33] United States Department of Homeland Security, "NIPP 2013, Partnering for Ctitical Infrastructure Security Resilience," United States Department of Homeland Security, 2013.
[34] APTA Standards Development Program, "Cybersecurity Considerations for Public Transit," APTA Standards Development Program, Washington, D.C., 2013.
[35] Transportation Security Administration, "Surface Transportation Cybersecurity Toolkit," Department of Homeland Security, 17 11 2017. https://www.tsa.gov/for-industry/surfacetransportation-cybersecurity-toolkit.
[36] NHTSA | National Highway Traffic Safety Administration, "Cybersecurity Best Practices for Modern Vehicles," U.S. Department of Transportation, Washington, DC, 2016.
[37] E. a. M. National Academies of Sciences, Protection of Transportation Infrastructure from Cyber, Washington, DC: The National Academies Press., 2016
[38] Deliverable D4.1Initial design of 5G V2X system level architecture and security framework 5GCAR Delivery Date: 2018-04-30
[39] [Соколов И. А. и др. Умные города, инфраструктуры и их антитеррористическая устойчивость. Опыт интеграции антитеррористических стандартов США и создания программного обеспечения для цифровой безопасности //International Journal of Open Information Technologies. – 2017. – Т. 5. – №. 7. – С. 45-65.
[40] Соколов И. А. и др. Современные исследовательские проекты ЕС и онтологии цифровой безопасности Европы //International Journal of Open Information Technologies. – 2018. – Т. 6. – №. 4. – С. 72-79.
[41] Соколов И. А. и др. Цифровая безопасность умных городов //International Journal of Open Information Technologies. – 2018. – Т. 6. – №. 1. – С. 104 – 118.
[42] Telematics Wire http://telematicswire.net/cybersecurity-a-gating-issue-for-safety-in-a-connected-and-automated-vehicle-future/
[43] Autonomous Vehicles: Navigating the legal and regulatory issues of a driver less world. MCCA GLOBAL TECH FORUM. 2018

On ontology and security of autonomous (driverless) cars

Oleg Pokusaev, Vasily Kupriyanovsky, Dmitry Katzin, Dmitry Namiot

***Abstract*—The article discusses issues related to the architecture of autonomous (unmanned) car software. The work uses the English abbreviation CAV (Connected Autonomous Vehicle). Automobile vehicles today have much more complex computer systems than airplanes, due to the complex interactions of autonomous cars on the roads. The volume of software codes for aircraft control systems and CAV differ tenfold. It is simply impossible to produce such a large code with the required functional and temporal characteristics, as well as ensure its safety with the old methods. In work, the services CAV and devices through which they are realized are considered. The paper describes the process of building software code for CAV. Consideration of these processes from the point of view of world standards leads us to cyber-physical systems and ontologies. The paper describes the ontological domains of cyber-physical systems affecting CAV. International standards related to ontological CAV design and security are considered. CAV security issues, potential vulnerabilities, and possible attacks are analyzed in detail. Also reviewed are the main areas of the area for improving CAV design. These include security design, the provision of CAV software for life, avoiding unlimited vulnerability windows, and increasing the transparency of the supply chain with ontological industry solutions and a cybersecurity assessment system.**

***Keywords*— autonomous cars; security; ontologies; software.**

REFERENCES

[1] Todd Litman, Autonomous Vehicle Implementation Predictions .Implications for Transport Planning,Victoria Transport Policy Institute.24 July 2018

[2] ALESSANDRA PIERONI, NOEMI SCARPATO AND MARCO BRILLI, INDUSTRY 4.0 REVOLUTION IN AUTONOMOUS AND CONNECTED VEHICLE. A NON-CONVENTIONAL APPROACH TO MANAGE BIG DATA, Journal of Theoretical and Applied Information Technology ,15th January 2018. Vol.96. No 1, pp 10-18

[3] SAS Institute Inc., “The connected vehicle: big data, big opportunities,” SAS White Pap.,p. 10, 2016

[4] Kuprijanovskij V. P. i dr. Razvitie transportno-logisticheskih otraslej Evropejskogo Sojuza: otkrytyj BIM, Internet Veshhej i kiber-fizicheskie sistemy //International Journal of Open Information Technologies. – 2018. – T. 6. – #. 2.-C. 54-100

[5] 2018 SELF-DRIVING SAFETY REPORT GM 2018

[6] Kuprijanovskij V. P., Namiot D. E., Sinjagov S. A. Kiber-fizicheskie sistemy kak osnova cifrovoj jekonomiki //International Journal of Open Information Technologies. – 2016. – T. 4. – #. 2. – S. 18-22.

[7] Kupriyanovsky V. et al. Industries transformation in the digital economy–the design and production //International Journal of Open Information Technologies. – 2017. – T. 5. – №. 1. – С. 50-70.

[8] Kuprijanovskij V. P. i dr. Transformacija promyshlennosti v cifrovoj jekonomike-jekosistema i zhiznennyj cikl //International Journal of Open Information Technologies. – 2017. – T. 5. – #. 1. – S. 34-49.

[9] CYBERSECURITY LITERATURE REVIEW AND EFFORTS REPORT .Prepared for: NCHRP Project 03-127 Cybersecurity of Traffic Management Systems, NCHRP 2018

[10] Cybersecurity in Automotive: How to stay ahead of cyber threats? Position paper, Altran 2018

[11] CRYSTAL State of the art for automotive ontology Deliverable No. D308.010 V1.1 Date 2014-06-05

[12] ETSI GR ENI 001 V1.1.1 (2018-04) Published Experiential Networked Intelligence (ENI); ENI use cases

[13] ETSI GS ENI 002 V1.1.1 (2018-04) Published Experiential Networked Intelligence (ENI); ENI requirements

[14] ETSI GR ENI 003 V1.1.1 (2018-05) Published Experiential Networked Intelligence (ENI); Context-Aware Policy Management Gap Analysis

[15] ETSI GR ENI 004 V1.1.1 (2018-05) Published Experiential Networked Intelligence (ENI); ENI General Terminology

[16] ETSI GR ENI 006 V1.1.1 (2018-05) Published Experiential Networked Intelligence (ENI); ENI Proof of Concept (PoC) Framework

[17] Cybersecurity in Automotive: How to stay ahead of cyber threats? Position paper, Altran 2018

[18] Common Criteria Recognition Arrangement, "Common Critera Portal," 3 11 2017. http://www.commoncriteriaportal.org/cc/.

[19] "Part 1: Introduction and General Model V3.1R4," Common Criteria Recognition Arrangement (CCRA), 2012.

[20] "Part 2: Security Functional Components V3.1R4," Common Criteria Recognition Arrangement (CCRA), 2012.

[21] "Part 3: Security Assurance Components V3.1R4," Common Criteria Recognition Arrangement (CCRA), 2012.

[22] International Organization for Standardization, "ISO/IEC 27000 - Information Secuity," ISO/IEC, 2013. https://www.iso.org/isoiec-27001-information-security.html.

[23] ISO/IEC, Information Technology - Security Techniques - Vulnerability Disclosure, Switzerland: ISO/IEC, 2014.

[24] Cyber Physical Systems Public Working Group, "Framework for Cyber-Physical Systems," National Institute of Science and Technology, 2016.

[25] United States Department of Homeland Security, "Cybersecurity Capability Maturity Model (C2M2) Program," United States Department of Homeland Security, https://energy.gov/oe/cybersecurity-critical-energy-infrastructure/cybersecurity-capability-maturitymodel- c2m2-program

[26] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity version 1.1 (Draft), https://www.nist.gov/cyberframework

[27] United States Department of Homeland Security, "C3 Voluntary Program FAQs," United States Department of Homeland Security, 2015. NCHRP 03-127 Task 1 - Security Literature Review and Efforts Report Cybersecurity of Traffic Management Systems Final January 12, 2018

[28] Department of Homeland Security, "Study on Mobil Device Security," 4 May 2017. https://www.dhs.gov/publication/csd-mobile-device-security-study.

[29] National Institute of Standards and Technology, "Assessing Threats to Mobile Devices & Infrastructure, The Mobile Threat Catalogue," NISTIR8144, 12 September 2016. https://csrc.nist.gov/CSRC/media/Publications/nistir/8144/draft/documents/nistir8144_draft.pdf.

[30] F. T. Adminisration, "National ITS Architecture Subsystems and Communications," Federal Transit Adminisration 2017.

[31] The Roadmap to Secure Control Systems in the Transportation Sector Working Group, "Roadmap to Secure Control Systems in the Transportation Sector," United States Department of Homeland Security, 2012.

[32] U.S. Department of Homeland Security, "Transportation Industrial Control System (ICS) Cybersecurity Standards Strategy," 2013.

[33] United States Department of Homeland Security, "NIPP 2013, Partnering for Ctitical Infrastructure Security Resilience," United States Department of Homeland Security, 2013.

[34] APTA Standards Development Program, "Cybersecurity Considerations for Public Transit," APTA Standards Development Program, Washington, D.C., 2013.

[35] Transportation Security Administration, "Surface Transportation Cybersecurity Toolkit," Department of Homeland Security, 17 11 2017. https://www.tsa.gov/for-industry/surfacetransportation- cybersecurity-toolkit.
[36] NHTSA | National Highway Traffic Safety Administration, "Cybersecurity Best Practices for Modern Vehicles," U.S. Department of Transportation, Washington, DC, 2016.
[37] E. a. M. National Academies of Sciences, Protection of Transportation Infrastructure from Cyber, Washington, DC: The National Academies Press., 2016
[38] Deliverable D4.1Initial design of 5G V2X system level architecture and security framework 5GCAR Delivery Date: 2018-04-30
[39] Sokolov I. et al. Smart cities, infrastructure, and their anti-terrorist stability. The experience of integrating the US anti-terrorism standards and creating software for digital security //International Journal of Open Information Technologies. – 2017. – Т. 5. – №. 7. – С. 45-65.
[40] Sokolov I. et al. Modern EU research projects and the digital security ontology of Europe //International Journal of Open Information Technologies. – 2018. – Т. 6. – №. 4. – С. 72-79.
[41] Sokolov I. A. i dr. Cifrovaja bezopasnost' umnyh gorodov //International Journal of Open Information Technologies. – 2018. – Т. 6. – #. 1. – С. 104 – 118.
[42] Telematics Wire http://telematicswire.net/cybersecurity-a-gating-issue-for-safety-in-a-connected-and-automated-vehicle-future/
[43] Autonomous Vehicles: Navigating the legal and regulatory issues of a driver less world. MCCA GLOBAL TECH FORUM. 2018