



# МАШИНОСТРОИТЕЛЬНЫЕ КОМПОНЕНТЫ

УДК 62-235

Л.Г. КРАСНЕВСКИЙ, член-корр. НАН Беларуси, д-р техн. наук, проф.

главный научный сотрудник

E-mail: krasnevski\_l@tut.by

Объединенный институт машиностроения НАН Беларуси, г. Минск, Республика Беларусь

Поступила в редакцию 02.09.2016.

## АВТОМАТИЧЕСКИЕ ТРАНСМИССИИ: ТЕХНОЛОГИЯ «УПРАВЛЕНИЕ ПО ПРОВОДАМ»

*Насыщение электронными и мехатронными устройствами привело к появлению на мобильных машинах бортовых систем управления, в которых отсутствует традиционная механическая связь между оператором и управляемым объектом и управление осуществляется посредством подачи электрических сигналов с помощью технологии, обобщенно называемой «X-by-Wire» («управление по проводам»). В их числе мехатронные системы управления автоматических трансмиссий (гидромеханических, механических, гибридных электромеханических). Однако наряду с преимуществами она порождает и новые сложные проблемы, важнейшей из которых является безопасность таких систем. Рассматриваются основные проблемы создания мехатронных систем управления автоматическими трансмиссиями (АТ) «по проводам» с позиции требований стандартов по безопасности транспортных средств. Проведен анализ этапов развития таких систем, особенностей их конструкций, основных типов отказов и методов их парирования на примерах ведущих компаний-производителей АТ. Их анализ показывает, что реализация данной технологии в мехатронных системах, в особенности на тяжелых трансмиссиях, сопряжена с необходимостью существенной трансформации архитектуры всех трех составляющих подсистем — электронной, программно-алгоритмической и электрогидравлической исполнительской.*

**Ключевые слова:** автоматическая трансмиссия, гидромеханическая передача, мехатронная система управления, безопасность систем управления, мобильная техника, технология «управление по проводам»

**Введение.** Стремительное развитие техники привело к появлению систем «человек — машина», принципиальной особенностью которых является отсутствие каких-либо механических связей между оператором и управляемым объектом. Здесь управление осуществляется только посредством подачи электрических сигналов, или, по англоязычной терминологии, «по проводам» («by wire»). Число таких систем в разных областях техники возрастает, и обобщенно эту технологию управления обозначают как «X-by-Wire» («управление по проводам»).

Считается, что первоначально такие системы, называемые «Fly-by-Wire» (приблизительно — «полет по проводам»), были созданы в авиации. Насыщение электронными и мехатронными устройствами в последнее десятилетие привело

к появлению таких бортовых систем управления и на современных автомобилях. Это две системы активной безопасности — тормозная и рулевая, получившие международные обозначения «Brake-by-Wire» («торможение по проводам») и «Drive-by-Wire» («управление по проводам»). В последнее время к ним относят и электронную систему дистанционного управления дроссельной заслонкой двигателя («электронную педаль акселератора»). Часто в научных публикациях применяют более краткое обозначение «DBW system». Его русским аналогом с использованием транслитерации может быть «ДБВ система», который и будет использоваться далее.

Применение этой технологии открыло широкие возможности для совершенствования систем управления и самого объекта — автомобиля. Так,

в тормозной системе отпадает необходимость дистанционного гидропривода, а установка электропривода вместо механической передачи между рулевым колесом и управляемыми колесами позволяет реализовать функции автономного курсового управления беспилотных автомобилей, автоматической парковки и др.

Однако наряду с преимуществами данная технология порождает и сложные проблемы, важнейшей из которых является безопасность.

Требования к безопасности систем «X-by-Wire» и методология ее обеспечения уже к 1993 году были определены международным стандартом MIL-STD-882C [1], а затем IEC 61508 [2] (ГОСТы, идентичные последнему, выпущены в России). Наконец, на их основе был разработан стандарт ISO 26262 по обеспечению функциональной безопасности дорожных транспортных средств (2011 год). Идентичный ему комплекс ГОСТов Р ИСО 26262 выпущен в 2014 году в России.

К настоящему времени опубликовано большое число исследований и методических материалов по практическому его применению к бортовым электронным системам, преимущественно к системам активной безопасности — тормозным и рулевым.

Что же касается современных мехатронных систем управления по проводам (далее МСУПП) автоматических трансмиссий (АТ), то публикации, касающиеся анализа и обеспечения безопасности этой технологии в свете требований ИСО 26262, нам не известны. Эти системы в настоящее время не включены в число автомобильных систем активной или пассивной безопасности. Поэтому цель данной статьи — рассмотреть и оценить влияние МСУПП на безопасность транспортного средства с позиции требований ИСО 26262.

**Актуальность.** В свете изложенного две основные причины побудили обратиться к теме, обозначенной в заголовке. Первая — появившиеся в июле 2016 г. в русскоязычной прессе [3] сообщения о гибели голливудского актера Антона Ельчина (уроженца Ленинграда) под колесами своего Jeep Grand Cherokee из-за предполагаемой неисправности коробки передач (КП). Оставив автомобиль с работающим двигателем и нейтралью в КП, пострадавший пошел открывать ворота дачи. Автомобиль на уклоне пришел в движение и придавил его к воротам. Предполагают, что из-за неисправностей системы управления КП водитель не был предупрежден, что рычаг управления не переведен в положение «паркинг» и колеса автомобиля не заблокированы. Отмечается, что данный случай отнюдь не единичный: «внедорожники этой марки недавно попали под отзывную кампанию из-за множества аналогичных инцидентов, в которых люди получали травмы». Далее, ссылаясь на газету Daily Mail, пишут, что в 2016 году компания Fiat Chrysler отзывала автомобили выпуска 2012–2015 годов из-

за дефекта, приведшего к их самопроизвольному движению. Это модели с восьмиступенчатой АТ и так называемым моностабильным селектором управления. Селекторы с такими же алгоритмами управления имеет, например, и BMW. Тогда же, по данным Национального управления безопасностью дорожного движения на трассах (NHTSA), по этой и схожим причинам в США зафиксировано 212 аварий, 308 случаев порчи имущества и 41 инцидент, когда люди получали травмы. Отмечается, что такие инциденты регулярно происходят и в России. Так, в 2015 году в Челябинской и Калужской областях под колесами собственных автомобилей погибли два водителя автомобилей Лада Калина и Peugeot.

Даже этих фактов достаточно, чтобы оценить степень опасности внезапных отказов, неисправностей и конструктивных дефектов систем управления современных многоступенчатых АТ и особенно МСУПП. Из истории известны многочисленные случаи, когда недостатки конкретных моделей АТ приводили к десяткам смертей, сотням травм и тысячам дорожных происшествий. Поэтому автор убежден, что *МСУ АТ должна рассматриваться в общем контексте безопасности автомобиля наряду с тормозной и рулевой системами как система безопасности, а не только как локальная СУ.*

Эти проблемы приобретают особую остроту в связи с тем, что в последние годы происходит вытеснение механических приводов из бортовых автомобильных систем управления, т. е. активный переход к ДБВ системам, в том числе и переход от МСУ к МСУПП АТ.

Вторая причина заключается в следующем. Быстрое расширение мирового производства АТ способствовало росту интереса к их созданию и применению в выпускаемой отечественной технике. В то же время русскоязычные публикации по проблемам обеспечения безопасности МСУ АТ (и, тем более, МСУПП АТ) практически отсутствуют. А многолетняя мировая практика показывает, что недостаточное внимание к этим проблемам приводит к тяжелым последствиям, упомянутым выше.

**О международном стандарте ИСО 262962.** ГОСТ Р ИСО 26262 «Дорожные транспортные средства. Функциональная безопасность», выпущенный в 2014 году, применяется к связанным с безопасностью системам, включающим в себя одну или несколько электрических или электронных (Э/Э) систем, которые установлены в серийно производимых легковых автомобилях с максимальной массой до 3500 кг. Он рассматривает возможные опасности, вызванные некорректным поведением, связанных с безопасностью Э/Э систем. Это комплекс взаимосвязанных стандартов, охватывающих все стадии жизненного цикла объектов от начала проектирования до эксплуатации.

Формально стандарт распространяется только на легковые и легкие грузовые автомобили. Однако другого инструмента для эффективного анализа безопасности и методологии ее обеспечения нет.

Для дальнейшего рассмотрения важно использовать терминологию, применяемую в стандарте. Она четко оговорена в первой его части [4] с датой введения — 2015-05-01. Ниже приведены (с сохранением орфографии и пунктуации ГОСТа) некоторые термины и определения, наиболее близкие к данной теме. Жирным шрифтом, как и в стандарте, выделены те из них, по которым в нем даны формулировки.

- **Функциональная безопасность** (functional safety): Отсутствие **неоправданного риска** вследствие **опасностей**, вызванных **неправильным поведением** Э/Э систем.

- **Готовность** (availability): Способность изделия выполнять необходимую функцию в заданных условиях, в определенное время или в течение заданного периода при условии, что необходимые внешние ресурсы доступны.

- **Уровень полноты безопасности автомобиля, УПБА** (Automotive Safety Integrity Level; ASIL): Один из четырех уровней, используемых для задания необходимых для **устройства** или **элемента** требований настоящего стандарта или **мер безопасности**, чтобы предотвратить неоправданный **остаточный риск**, для которого значение УПБА, равное D, является наиболее строгим уровнем, а значение УПБА, равное A, — наименее строгим.

- **Механизм безопасности** (safety mechanism): Техническое решение, реализованное Э/Э функциями или элементами или выполненное на основе **других технологий** для обнаружения **сбоев** или управления **отказами** в целях достижения или поддержки **безопасного состояния**.

- **Другая технология** (other technology): Используемая в области применения настоящего стандарта технология, отличающаяся от Э/Э технологий.

**Пример — технология, основанная на принципах механики; технология, основанная на принципах гидравлики.**

- **Риск** (risk): Сочетание вероятности причинения вреда и тяжести этого вреда.

- **Тяжесть**: (severity): Оценка степени **вреда**, причиняемого одному или нескольким лицам, который может возникнуть в потенциально **опасных** ситуациях.

- **Отказ** (failure): Прекращение способности элемента выполнять необходимую функцию.

- **Безопасный сбой** (safe fault): **Сбой**, появление которого несущественно увеличивает вероятность нарушения **цели безопасности**.

Уже из этой краткой выборки видно, что стандарт не касается оценки надежности. Пользуясь приведенными выше терминами, можно говорить, что он оценивает степень риска нарушения функциональной безопасности, т. е. готовности из-

делия выполнять заданную ему функцию в случае возникновения отказа какого-то его элемента.

Цитируем: «Безопасность системы достигается за счет ряда мер безопасности, которые реализуются с применением различных технологий (например, механических, гидравлических, пневматических, электрических, электронных, программируемых электронных) и применяются на различных уровнях процесса разработки. Несмотря на то, что настоящий стандарт касается функциональной безопасности Э/Э систем, подход, рассматриваемый в настоящем стандарте, может быть использован для разработки связанных с безопасностью систем, основанных на других технологиях».

Таким образом, проясняется и распространение стандарта на мехатронные системы: четко указано, что технические решения, обеспечивающие функциональную безопасность, могут быть выполнены *с помощью Э/Э технологий и других технологий, например, основанных на принципах механики и гидравлики*. А это уже прямое указание на мехатронные системы, которое было введено данным стандартом. Так, в докладе на конгрессе ИФАК 2005 года [5], посвященном безопасности бортовых мехатронных и ДБВ-систем, мехатроника представлена в виде диаграммы (рисунок 1), изображающей «синергетическую интеграцию различных дисциплин — электроники, информационных технологий, механики и электро-механики». Однако анализ функциональной безопасности с позиций стандарта ИЕС 61508 выполнен в [5] только для первых двух, так как данный стандарт не распространялся на механические и электромеханические элементы. Согласно стандарту ИСО 26262 *заданный уровень УБПА для системы, влияющей на функциональную безопасность, распространяется на все ее элементы*, а значит, и на механические/электромеханические. Важность и возможные последствия этого события трудно переоценить.

**О применении бортовых ДБВ-систем.** Для реализации преимуществ бортовых ДБВ систем в области активной и пассивной безопасности автомобиля необходимо полное и всестороннее выполнение процессов обеспечения безопасности самих этих систем. В [6] приведены стандартные

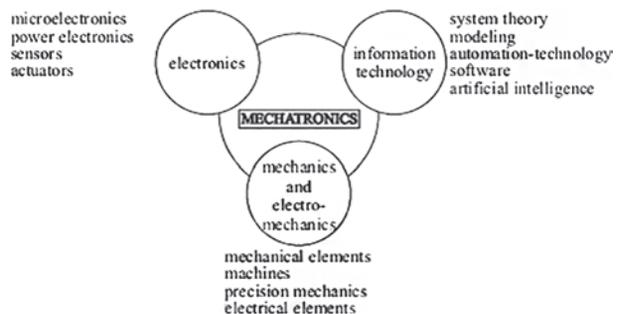


Рисунок 1 — Мехатроника: синергетическая интеграция различных дисциплин [5]

элементы таких процессов, широко применяемых в различных областях, предложен процесс анализа безопасности автомобильных ДБВ систем на примере рулевого управления.

Для обеспечения согласно ИСО 26262 уровня УПБА D критически важных для безопасности систем применяют специальные стратегии построения архитектуры входящих в них микроконтроллеров, в том числе их самодиагностику [7].

С точки зрения критичности выполняемых функций будущее автомобильных ДБВ систем обоснованно сравнивают с авиационными. Для них вероятность утраты критического УПБА не должна превышать  $5 \cdot 10^{-10}$  или же  $10^{-9}$  на систему в течение часа. Достичь такой высокой надежности очень сложно, в том числе и по экономическим ограничениям [8, 9].

При анализе надежности воздушных судов и их систем определяющим является анализ опасности, создающейся в результате каждого отказа, и установление ограничений на вероятность его возникновения в зависимости от тяжести последствий. В работе [10], посвященной гидросистемам воздушных судов, приведены следующие требования международной организации ИКАО: для умеренно вероятных событий (от  $10^{-3}$  до  $10^{-5}$ ) допускаются лишь незначительные последствия, для маловероятных (от  $10^{-5}$  до  $10^{-7}$ ) — последствия без крайней опасности, для крайне маловероятных (меньше  $10^{-7}$ ) — опасные, а катастрофические — лишь для крайне невероятных (менее  $10^{-9}$ ). Основной структурный метод обеспечения требуемого уровня надежности авиационных гидросистем — резервирование (двух-, трех-, четырехкратное).

Ноу-хау, накопленные в авиационной промышленности, могут оказать большую помощь, но необходимо разработать методологию конструирования бортовых систем, адаптированную к ограничениям автомобильной промышленности [8, 9]. Основная задача — переключить процесс разработки с интеграции подсистем на создание единой системы ввиду возрастания количества сетевых функций управления внутри бортовых МСУ. Очевидно, что это относится и к мехатронным системам, понимаемым как единый объект по рисунку 1.

Как отмечается в [11], ДБВ системы входят в число новых сложных технологий, освоение которых автомобильной промышленностью может оказать влияние на взаимоотношения производителей и поставщиков. Это обусловлено тем, что технологическая специализация создает сложную архитектуру бортовых Э/Э систем, которая порождает взаимозависимость всех участников автомобильных инновационных сетей — факт, который еще не освещен в литературе. Для более глубокого изучения приведены примеры тормозных и рулевых ДБВ-систем. Так, на рисунке 2 приведе-

на ДБВ тормозная система известной компании Delphi (2002 год, [12]) с резервированием. Она содержит два микроконтроллера 10 и 12 и три источника напряжения 4, 8, 14 — генератор, аккумуляторную батарею (или блок топливных элементов), а также накопитель электроэнергии (в гибридных автомобилях).

Другой пример — внедрение компанией John Deere в 2002 году МСУПП для бесступенчатой электрогидрообъемной трансмиссии нового семейства тракторов серии 7000 [13].

Новым важным шагом в развитии автомобильных ДБВ систем станет создание их генерации, обеспечивающей автономное вождение. Развитие архитектуры таких систем, отвечающих требованиям надежности и другим ограничениям, — ответственная задача, которая может привести к изменению парадигмы автомобильных ECS («electronics, control and software» — электроники, средств управления и программного обеспечения — обозначения в оригинале), которая приведет к созданию ECS, способных функционировать при наличии отказов [14]. Отмечается, что этот аспект особенно важен при конструировании электромобилей с интегрированными в колеса приводами и подсистемами шасси, питаемыми от аккумуляторных батарей. В таких интегрированных взаимозависимых системах многие функции требуют самого высокого УПБА.

**Развитие методов обеспечения безопасности.** Совершенствование методов защиты от последствий потенциально опасных отказов СУ неразрывно связано с развитием самих ГМП, которые исторически были первым и до настоящего времени самым массовым типом АТ. В этом процессе можно укрупнено отметить четыре этапа (подробнее см. [15]):

ЭТАП I. ГМП малой мощности с гидравлическими системами автоматического управления и механическим приводом ручного управления (для легковых автомобилей).

ЭТАП II. ГМП большой мощности с электрогидравлическими системами командного управ-

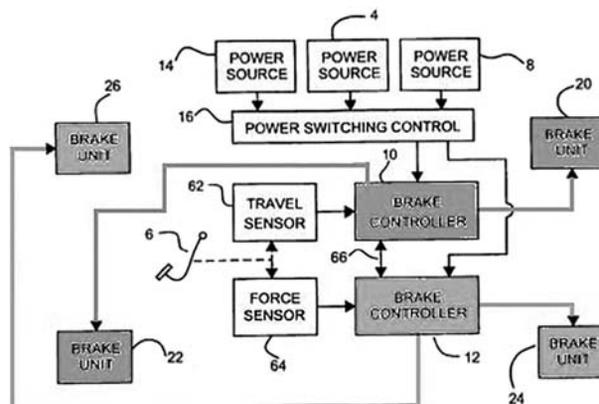


Рисунок 2 — Тормозная ДБВ система компании Delphi с двумя микроконтроллерами [12]



(особенно на переднеприводных легковых автомобилях), его применяют даже в суперсовременных легковых АТ (вместе с тем, в обоснованных случаях и ДБВ системы), в том числе на тяжелых ГМП. Система по рисунку 3 — типичный пример сочетания МСУ третьего этапа и ручного селектора, перешедшего из первого.

На втором этапе на тяжелых ГМП появились электрогидравлические системы дистанционного командного управления. На автомобилях большой мощности и грузоподъемности расстояние между рабочим местом оператора и АТ велико, а рама во время движения может упруго деформироваться. Это настолько затрудняет использование механического привода ручного управления, что изначально применяют ДБВ системы. Яркий пример — широко известная система управления ГМП Allison 6 + 2 серий DP 8000, 9000 на мощность 800–1000 л. с., выполненная по патенту США 1970 года (рисунок 4 [19]).

В данной системе связь между рычагом селектора и механизмом управления ГМП только электрическая. Ее контроллер управления имел отдельные позиции для всех ступеней плюс нейтраль. Здесь также произошел переход к двухкаскадному построению гидросхемы с малогабаритными ЭГК в пилотном каскаде. В дальнейшем она вошла в состав МСУ General Motors первого поколения (в настоящее время в производстве система пятого поколения).

Как уже говорилось, здесь запрет включения блокирующих комбинаций ЭУ реализован с по-

мощью известной логической гидросхемы. Ее структура, соответствующая рисунку 4 и патенту [19], приведенная в нашей работе [17], показана на рисунке 5.

На третьем этапе — в 80-х годах — состоялся массовый переход от гидроавтоматики к электронно-гидравлическим мехаторным системам. При этом описанная выше механическая связь оператора с АТ сохраняется, несмотря на наличие нескольких ЭГК как единственно возможного интерфейса между электроникой и механизмами управления в МСУ.

Появилась возможность реализации ряда функций, выполнявшихся механическими (гидравлическими) устройствами, с помощью электронных аппаратных и/или программных средств. В результате значительно уменьшились габариты и вес, упростились конструкции блоков механической части МСУ.

Упрощение механической части на какое-то время стало увлечением. Характерный пример — публикация сотрудников упомянутой компании Hyundai, посвященная исследованию «полностью электронного управления АТ». Здесь в хронологическом порядке приведено шесть структурных схем систем управления — от простых электрогидравлических «пассивных» систем 80-х годов к показанной на рисунке 6 предлагаемой МСУ (2000 год, [20]), реализующей «прямое активное управление». Суть предложения в том, что управление давлением в каждом из фрикционов C1, C2, C3, C4 осуществляется отдельным полнопоточным (од-

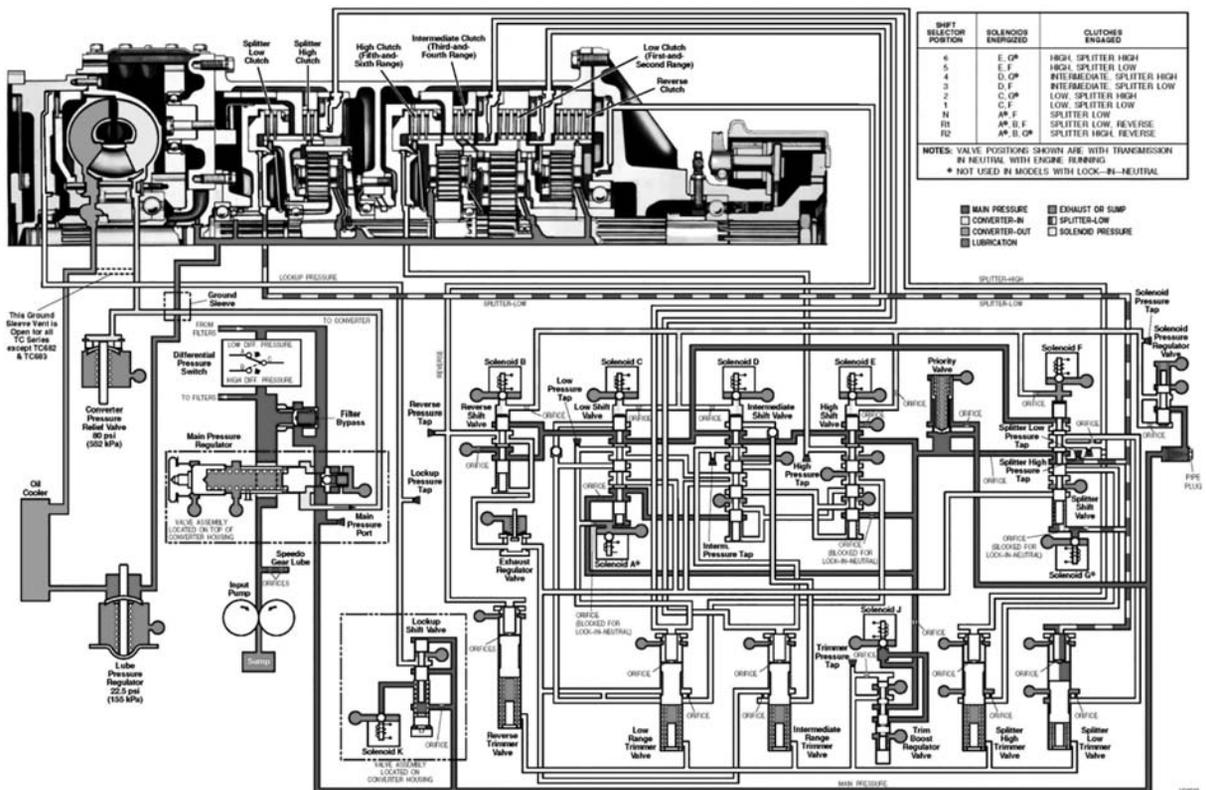


Рисунок 4 — ГМП Allison 6 + 2 с МСУ и электроприводом дистанционного ручного управления (версия 2000 года)

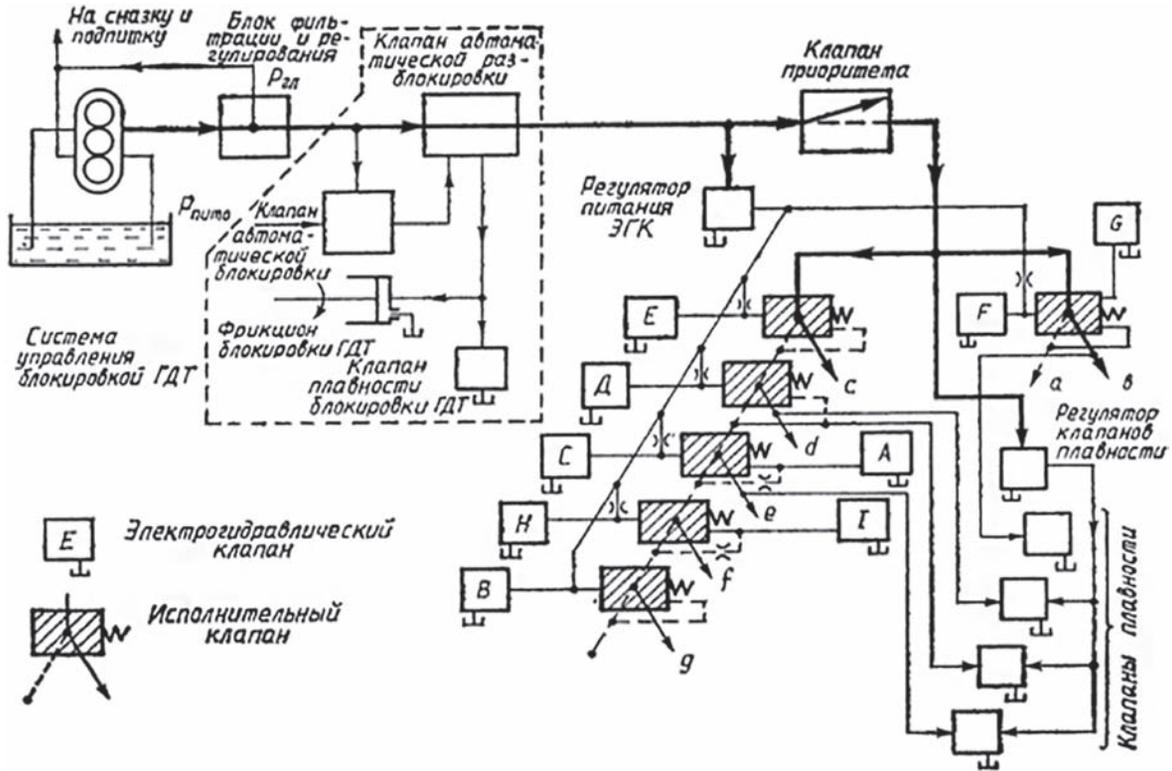


Рисунок 5 — Структурная схема системы командного управления ГМП Allison по рисунку 4

нокаскадным) пропорциональным ЭГК (на рисунке — PCSV). Эти клапаны параллельно независимо подключены к общему источнику давления, и, как видим, никаких элементов защиты на схеме нет.

С момента этой публикации прошло довольно много времени, и, судя по современным конструкциям АТ (в том числе Hyundai), данный вариант не состоялся, что и сегодня может быть полезным уроком.

Наконец, на четвертом этапе — этапе сегодняшнего дня — начался и продолжается переход к АТ с МСУ и электрической связью между контроллером и трансмиссией, т. е. к чистому «управлению по проводам» — ДБВ-системам.

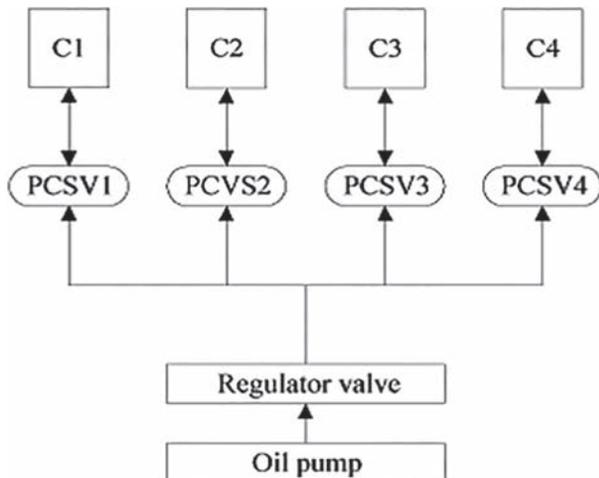


Рисунок 6 — Схема полностью электронной системы прямого активного управления АТ (2000 год [20])

Подводя итоги этих этапов развития, следует отметить следующее.

*Первое.* Появление МСУ привело к кардинальному изменению архитектуры механизма управления ГМП. Это позволило осуществить согласованное управление буксованием участвующих в каждом переключении фрикционов (в англоязычной литературе — «clutch-to-clutch shift»), что недостижимо для средств гидроавтоматики (даже в таких системах, как на рисунке 4, — одной из лучших). В результате резко снизилась динамическая нагруженность АТ и повысилась комфортабельность («плавность») переключений.

*Второе.* Наряду с повышением плавности электроника позволила обеспечить переключения без разрыва потока мощности («с перекрытием») за счет одновременного управления моментами трения выключаемого и включаемого фрикционов.

Переключение без разрыва потока мощности, в свою очередь, оказалось столь важным для повышения эксплуатационных свойств (особенно машин высокой проходимости), что поставило автоматические ГМП вне конкуренции по сравнению со всеми другими типами трансмиссий в данной области.

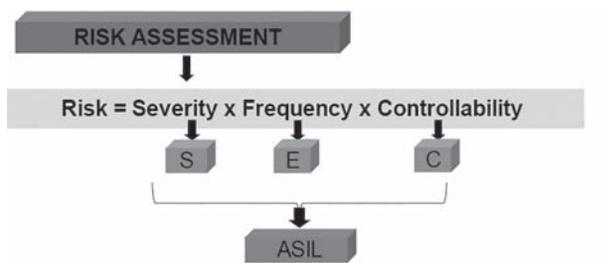
*Третье.* Но для получения плавности и перекрытия во включаемом и выключаемом фрикционах в переходном процессе должны одновременно поддерживаться давления жидкости (изменяющиеся по разным законам), т. е. они должны находиться в комбинации, которая запрещена на установленном режиме. Поэтому для осуществления

таких переключений пришлось вообще отказаться от применявшихся логических гидросхем, исключая возможность включения таких комбинаций. Вместо них пришлось установить отдельный электрогидравлический регулятор давления для каждого фрикциона.

О требованиях к обеспечению безопасности классических и ДБВ систем управления АТ. Как видно из изложенного, с позиции ИСО 26262 отказ от средств гидравлики для исключения блокирующих комбинаций сам по себе существенно снижает уровень безопасности. Для компенсации стали постепенно вводить в МСУ различные обходные решения при безоговорочном сохранении многопозиционного селектора с механической связью. Например, при каждом переключении ступеней правильность комбинации, включение которой уже началось, может определяться путем вычисления изменяющегося передаточного числа АТ и сравнения его с передаточным числом заданной комбинации, что в какой-то степени компенсирует отсутствие логических гидросхем. По мере накопления опыта массовой эксплуатации МСУ технические решения, направленные на повышение безопасности, множились, причем каждая компания в соответствии с требованиями патентной чистоты находила свои пути. В большинстве таких решений используются средства гидравлики. Понятно, что эти проблемы обостряются при переходе к ДБВ системам. Скажем только, что в практику последних нескольких лет вошло подробное описание в патентах на системы управления их поведения при отказах и мер предупреждения наиболее опасных.

Определение степени опасности отказов согласно ИСО 26262, т. е. уровня риска УПБА (ASIL), поясняется рисунком 7 [21]. Как видно из рисунка 7, уровень риска есть произведение (логическое) трех показателей, характеризующих потенциальные последствия одиночного отказа какого-либо элемента, или подсистемы, или системы в течение часа функционирования. Это следующие показатели:

- *тяжесть (severity)*: без повреждений; легкие и средние повреждения; опасные и угрожающие жизни людей повреждения (выживание возможно);



ASIL: Automotive Safety Integrity Level

Рисунок 7 — Схема оценки риска по ИСО 26262 [21]

Таблица 1 — Определение уровня риска ASIL (УПБА) в зависимости от сочетания уровней тяжести, частоты и управляемости опасного воздействия по ИСО 26262 [21]

Use Severity, Exposure, Controllability to set ASIL

|    |    | C1     | C2     | C3     |
|----|----|--------|--------|--------|
| S1 | E1 | QM     | QM     | QM     |
|    | E2 | QM     | QM     | QM     |
|    | E3 | QM     | QM     | ASILA  |
|    | E4 | QM     | ASILA  | ASIL B |
| S2 | E1 | QM     | QM     | QM     |
|    | E2 | QM     | QM     | ASILA  |
|    | E3 | QM     | ASILA  | ASIL B |
|    | E4 | ASILA  | ASIL B | ASIL C |
| S3 | E1 | QM     | QM     | ASILA  |
|    | E2 | QM     | ASILA  | ASIL B |
|    | E3 | ASILA  | ASIL B | ASIL C |
|    | E4 | ASIL B | ASIL C | ASIL D |

Source ISO/DIS 26262

угрожающие жизни повреждения (выживание неопределенно); фатальные повреждения;

- *частота (frequency)*: невероятность; очень низкая вероятность; низкая вероятность; средняя вероятность; высокая вероятность;
- *управляемость (controllability)*: полностью управляемо; просто управляемо; нормально управляемо; трудно управляемо или неуправляемо.

Каждый из названных показателей имеет четыре уровня: первый — низший, четвертый — высший. Все эти уровни трех показателей сведены в таблицу 1 [21], в которой обозначения соответствуют начальным буквам названий параметров. В клетках таблицы обозначены уровни ASIL (УПБА) A, B, C, D, соответствующие сочетаниям уровней показателей каждой клетки. Видно, что при приближении к правому нижнему углу таблицы эти уровни возрастают, а угловая нижняя правая клетка соответствует высшему уровню — ASIL D (УПБА D).

Физический смысл этой процедуры поясняет схема, показанная на рисунке 8 [22]. Предположим, объект имеет три возможных уровня защиты: нормальное состояние (верхняя плоскость),

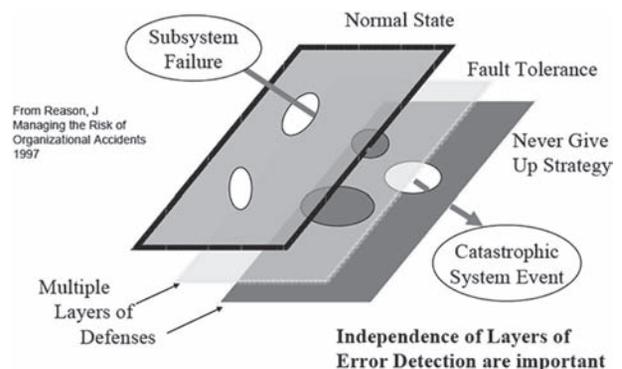


Рисунок 8 — Уровень безопасности: модель «Швейцарского сыра» [22]

устойчивое к отказу (нечувствительное, средняя плоскость) и предельное (нижняя плоскость). Если происходит отказ какой-то подсистемы (жирная стрелка), который пройдет через все три уровня, то он приведет к катастрофе объекта. Следовательно, объект должен иметь такой уровень безопасности, который не допустит преодоления защиты от данного отказа.

В соответствии с требованиями данного стандарта комплекс мероприятий по обеспечению безопасности начинается с анализа опасностей и разработки плана по их предотвращению.

Чтобы однозначно определить, какие же состояния АТ (вызванные отказами СУ) являются наиболее опасными, необходимо предварительно провести тщательный структурный анализ самой АТ. Эти вопросы применительно к автоматическим ГМП еще ранее были подробно рассмотрены в наших работах [16, с. 179–191, 17]. Проведен анализ потенциальных отказов СУ, предложена классификация последствий основных их видов в зависимости от степени тяжести для АТ и автомобиля с делением на три группы и несколько подгрупп (незначительные, средние, тяжелые, предаварийные, аварийные) в зависимости от воздействия на 10 основных компонентов МСУ. Эти результаты по смыслу близки к показанной выше таблице 1. Для анализа совместного поведения МСУ и АТ при отказах АТ рассматривается как дискретный объект с конечным числом внутренних состояний, однозначно определяемых комбинациями включения элементов управления (ЭУ) — фрикционов. При этом входящий в состав МСУ электронный блок может быть представлен как «черный ящик», внутренние дискретные состояния которого (исправное, неисправное) однозначно отображаются состояниями (значениями двоичных сигналов и их последовательностями) на его выходах. А их число равно числу ЭГК в исполнительной части МСУ. При таком представлении любые состояния двух составляющих этого мехатронного объекта — электроники и программного обеспечения (исправное и неисправное) — проявляются только в виде комбинаций двоичных чисел на выходах, которые поступают на входы механической составляющей — электрогидравлического механизма управления.

Понятно, что в результате отказа на выходе в принципе может появиться любая комбинация в виде многоразрядного двоичного числа. Число вариантов, равное факториалу числа разрядов, очень велико (см. [16]). Среди этих комбинаций есть рабочие, нейтральные и запрещенные, которые должны быть исключены. Другими словами, МСУ должна обладать способностью парировать отказы, способные вызвать включение запрещенных комбинаций ЭУ.

Как было показано выше, это свойство легко обеспечивается средствами гидравлики (логическими гидросхемами). Таким образом, приходим

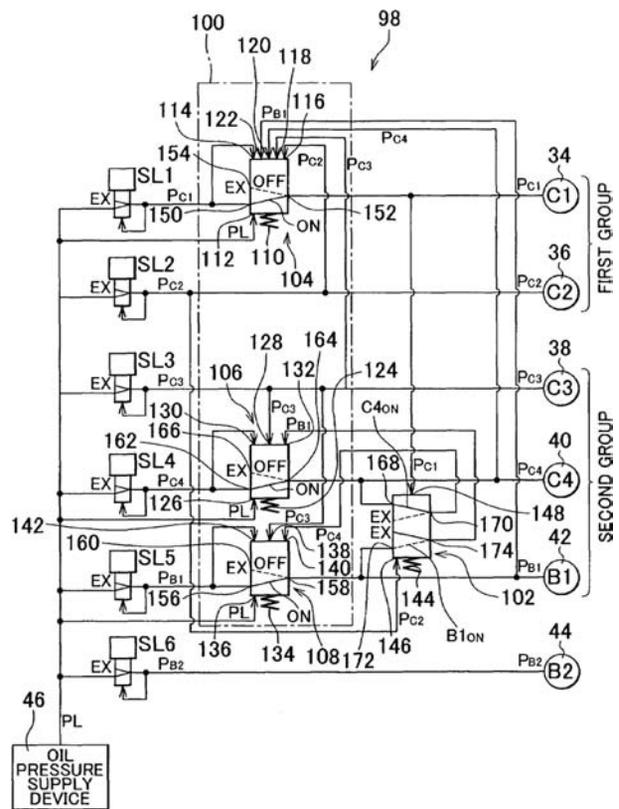


Рисунок 9 — МСУПП ГМП 8 + 2 компании Toyota (2008 год [25])

к выводу, что командные ДБВ системы и МСУПП, имеющие в своем составе такие устройства, по уровню безопасности (УПБА) были близки к будущим требованиям ИСО 26262. В [16, 23, 24] нами были предложены методы синтеза таких систем, основанные на теории дискретных устройств.

Совершенно иная ситуация складывается с УПБА МСУПП без гидравлической блокировки запрещенных комбинаций, поскольку в общем случае парирование огромного их числа должно быть возложено на электронику. Поэтому гидравлическая логика в сочетании с многопозиционными распределителями с ручным приводом применяется, хоть и в урезанном виде.

Яркий пример — ДБВ система управления автоматической ГМП Toyota 8 + 2 для легковых автомобилей (т. е. МСУПП) по патенту 2008 года [25], показанная на рисунке 9. Здесь нет гидравлической блокировки запрещенных комбинаций, как в предыдущих примерах, но фрикционы разделены на две группы, управляемые отдельными двухкаскадными электрогидравлическими распределителями, и есть гидравлическая логика в пилотном каскаде второй (нижней) группы. Однако, как принято при таких схемах, проведен анализ возможных последствий отказов во всех рабочих состояниях ГМП, результаты которого учтены при ее разработке. В таблице 2 представлены включения фрикционов этой ГМП, а в таблицах 3, 4 — анализ последствий отказов МСУПП только на второй и восьмой ступенях. Аналогично

Таблица 2 — Порядок включения фрикционов ГМП по рисунку 9 [25]

|      | C1 | C2 | C3 | C4 | B1 | B2  | F1 |
|------|----|----|----|----|----|-----|----|
| P    |    |    |    |    |    |     |    |
| Rev1 |    |    | ○  |    |    | ○   |    |
| Rev2 |    |    |    | ○  |    | ○   |    |
| N    |    |    |    |    |    |     |    |
| 1st  | ○  |    |    |    |    | (○) | ○  |
| 2nd  | ○  |    |    |    | ○  |     |    |
| 3rd  | ○  |    | ○  |    |    |     |    |
| 4th  | ○  |    |    | ○  |    |     |    |
| 5th  | ○  | ○  |    |    |    |     |    |
| 6th  |    | ○  |    | ○  |    |     |    |
| 7th  |    | ○  | ○  |    |    |     |    |
| 8th  |    | ○  |    |    | ○  |     |    |

○ : ENGAGED  
(○) : ENGAGED AT ENGINE BRAKE

Таблица 3 — Анализ последствий отказов МСУПП по рисунку 9 на второй ступени ГМП [25]

| 2nd              | 1ST GROUP |     | 2ND GROUP |     |     | AFTER FAIL-SAFE        |            |
|------------------|-----------|-----|-----------|-----|-----|------------------------|------------|
|                  | C1        | C2  | C3        | C4  | B1  | ENGAGEMENT COMBINATION | GEAR STAGE |
| NORMAL           | ○         |     |           |     | ○   |                        |            |
| C2ON ABNORMALITY | ○→×       | ●→○ |           |     | ○   | C2-B1                  | 8th        |
| C3ON ABNORMALITY | ○         |     | ●→○       |     | ○→× | C1-C3                  | 3rd        |
| C4ON ABNORMALITY | ○         |     |           | ●→○ | ○→× | C1-C4                  | 4th        |

○ : ENGAGED × : RELEASED ● : ON-ABNORMALITY

Таблица 4 — Анализ последствий отказов МСУПП по рисунку 9 на восьмой ступени ГМП [25]

| 8th              | 1ST GROUP |    | 2ND GROUP |     |     | AFTER FAIL-SAFE        |            |
|------------------|-----------|----|-----------|-----|-----|------------------------|------------|
|                  | C1        | C2 | C3        | C4  | B1  | ENGAGEMENT COMBINATION | GEAR STAGE |
| NORMAL           |           | ○  |           |     | ○   |                        |            |
| C1ON ABNORMALITY | ●→▲       | ○  |           |     | ○   | C2-B1                  | 8th        |
| C3ON ABNORMALITY |           | ○  | ●→○       |     | ○→× | C2-C3                  | 7th        |
| C4ON ABNORMALITY |           | ○  |           | ●→▲ | ○   | C2-B1                  | 8th        |

○ : ENGAGED × : RELEASED ● : ON-ABNORMALITY ▲ : NOT ENGAGED

проведен анализ на всех остальных ступенях с соответствующими пояснениями в тексте [25].

В нашей работе (15) рассмотрены технические решения, касающиеся безопасности МСУПП компаний Zahnrad Fabrik, General Motors и др. Так, последняя в [26] при переводе МСУ АТ на технологию «управление по проводам» вводит специальную подсистему ETRS (Electronic Transmission Range Selection), которая, в частности, заменяет многопозиционный селектор с механическим ручным приводом.

**Заключение.** Как видно из изложенного, насыщение современных автомобилей электрон-

ными и мехатронными устройствами в последнее десятилетие привело к появлению бортовых систем управления, принципиальной особенностью которых является отсутствие механических связей между оператором и управляемым объектом. Здесь управление осуществляется только посредством подачи электрических сигналов, или, по англоязычной терминологии, «по проводам» («by wire»). Это две системы активной безопасности — тормозная и рулевая, а в последнее время — и мехатронные системы управления автоматических трансмиссий.

Применение этой технологии открыло широкие возможности для совершенствования систем управления и самого объекта — автомобиля. Однако наряду с преимуществами она порождает и сложные проблемы, важнейшей из которых является безопасность, которая для дорожных транспортных средств определяется международным стандартом ISO 26262 (2011 год) и идентичным ему комплексом ГОСТов Р ИСО 26262 (2014 год) России.

Как показывает мировой опыт, реализация технологии «управления по проводам» в мехатронных системах управления автоматическими трансмиссиями сопряжена с необходимостью существенной трансформации архитектуры всех трех их составляющих подсистем — электронной, программно-алгоритмической и электрогидравлической исполнительной. Методология и направленность трансформации определяются требованиями к уровню приемлемой безопасности автомобиля — УПБА (ASIL) в соответствии со стандартом ISO 26262 (ГОСТ Р ИСО 26262 России).

## Список литературы

1. System Safety Program Requirements. Military standart: MIL-STD-882C. — 19.01.93.
2. Functional Safety of Electrical / Electronic / Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES): IEC 61508. — Mode of access: <https://www.pilz.com/ru-RU/knowhow/law-standards-norms/functional-safety/en-iec-61508>.
3. Актера Ельчина подвела коробка передач // Газета Ру. — 2016. — 20 июня.
4. Дорожные транспортные средства. Функциональная безопасность. Ч. 1: Термины и определения: ГОСТ Р ИСО 26262-1-2014. — Введ. 01.08.14.
5. Isermann, Rolf. Mechatronic Systems — Innovative Products with Embedded Control / Rolf Isermann. — Mode of access: [https://www.researchgate.net/publication/222668010\\_Mechatronic\\_systems-Innovative\\_products\\_with\\_embedded\\_control](https://www.researchgate.net/publication/222668010_Mechatronic_systems-Innovative_products_with_embedded_control).
6. A System-Safety Process For By-Wire Automotive Systems // SAE Technical Paper 2000-01-1056. — 2000.
7. Achieving ASIL D for Microcontroller in Safety-Critical Drive-by-Wire System // SAE Technical Paper 2009-01-0759. — 2009.
8. Trends in automotive communication systems // Proceedings of the IEEE. Special issue on industrial communication systems. — 2005. — 93(6). — Pp. 1204–1223.
9. Achieving 10-9 Dependability with Drive-by-Wire Systems // SAE Technical Paper 2003-01-1290. — 2003.
10. Надежность гидравлических систем воздушных судов / Т.М. Башта [и др.]. — М.: Транспорт, 1986. — 279 с.
11. Managing technology for highly complex critical modular systems: The case of automotive by-wire systems // International Journal of Production Economics. — April 2009. — Vol. 118, Iss. 2. — Pp. 473–485.

12. Brake by wire system with separate controllers and both position and force input sensors: US Pat. 6390565 / Delphi Technologies, Inc. — May 21, 2002.
13. Infinitely variable transmission (IVT) of John Deere 7000 TEN series tractor // IMECE2002-39347. — Pp. 123–131.
14. Architectural design and reliability analysis of a fail-operational brake-by-wire system from ISO 26262 perspectives // Reliability Engineering & System Safety. — October 2011. — Vol. 96, Iss. 10. — Pp. 1349–1359.
15. Красневский, Л.Г. Автоматическая трансмиссия как объект управления в системе безопасности современного автомобиля / Л.Г. Красневский // Актуальные вопросы машиноведения: сб. науч. тр. — 2015. — Вып. 4.
16. Красневский, Л.Г. Управление гидромеханическими многоступенчатыми передачами мобильных машин / Л.Г. Красневский. — Минск: Наука і техника, 1990. — 256 с.
17. The fundamental aspects of the structural theory of multispeed Transmissions control / L. Krasnevski // SAE 2005 – 01 – 1598.
18. Development of 4 speed electronically controlled new automatic transmission for FWD // Seoul 2000 FISITA World Automotive Congress. — June 12–15, Seoul, Korea.
19. Transmission and controls: US Pat. № 3505907 / General Motors Corp. — Apr. 14, 1970.
20. A Study on Full Electronic Control of Automatic Transmission: Direct Active Shift Control / Hyundai Motor Company // Seoul 2000 FISITA World Automotive Congress. — 2000. — June 12–15.
21. ISO 26262 Functional Safety Draft International Standard for Road Vehicles: Background, Status, and Overview // General Motors Research and Development. ISSC 2010. Minneapolis, Minnesota.
22. From a Federated to an Integrated Architecture for Dependable Embedded Systems / H. Kopetz // TU Wien. — September 2004.
23. Красневский, Л.Г. Синтез релейных гидросистем управления многоступенчатыми трансмиссиями тяжелых автомобилей / Л.Г. Красневский. — дис. ... канд. техн. наук. — Минск, 1969.
24. The Synthesis Method of Electro-Hydraulic Schemes of Mechatronic Control Systems for Hydromechanical Transmissions / Leonid Krasnevski // SAE 2003 – 01 – 0319.
25. Control apparatus of vehicular automatic transmission: US Pat. № 7419452 / Toyota Jidosha K.K. — Sep. 2, 2008.
26. Hydraulic control system for an automatic transmission having electronic transmission range selection with failure mode control: US Pat. № 8435148 / GM Global Technology Operations LLC. — May 7, 2013.

KRASNEVSKIY Leonid G., Corresponding Member of the NAS of Belarus,  
D. Sc. in Eng., Prof.

Chief Researcher

E-mail: krasnevski\_l@tut.by

Joint Institute of Mechanical Engineering of the National Academy of Sciences of Belarus, Minsk, Republic of Belarus

Received 02 September 2016.

## AUTOMATIC TRANSMISSIONS: THE TECHNOLOGY OF “X-BY-WIRE”

*An increase in the use of electronic and mechatronic devices has led to the introduction of mobile machines' on-board control systems, which are free of usual mechanical link between the operator and the object controlled, and the control is maintained with the supply of electrical signals – with the help of a technology, collectively called “X-by-Wire” (“control-by-wire”). These include mechatronic control systems of automatic transmissions (hydro-mechanical, mechanical, hybrid electro-mechanical). However, along with the advantages it gives rise to new challenges, the most important of which is the safety of such systems. The main problem of creating mechatronic control systems of automatic transmissions “X-by-Wire” from a position of requirements to the vehicles safety standards is studied. The analysis of the stages of development of such systems, characteristics of their designs, main types of failures and solution methods through the examples of the leading AT manufacturers is conducted. Their analysis shows that implementation of this technology in mechatronic systems, especially in heavy transmissions, is connected with the need to substantially transform the design of all three components of their subsystems – electronic, software and algorithmic and electrohydraulic executive.*

**Keywords:** automatic transmission, hydromechanical transmission, mechatronic control system, control systems' safety, mobile machines, technology of “X-by-Wire”

### References

1. Military standard MIL-STD-882C. *System Safety Program Requirements*. 1993.
2. *Functional Safety of Electrical / Electronic / Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES): IEC 61508*. Available at: <https://www.pilz.com/ru-RU/knowhow/law-standards-norms/functional-safety/en-iec-61508/>.
3. *Aktera Elchina podvela korobka peredach* [Transmission threw actor Yelchin over the bridge]. Available at: [https://www.gazeta.ru/auto/2016/06/20\\_a\\_8317715.shtml/](https://www.gazeta.ru/auto/2016/06/20_a_8317715.shtml/) (accessed 20 June 2016).
4. GOST R ISO 26262-1-2014. *Dorozhnyye transportnye sredstva. Funkcionalnaja bezopasnost. Ch. 1: Terminy i opredelenija*. [State Standard R ISO 26262-1-2014. Road vehicles. Functional safety. Part 1: Terms and definitions]. 2014.
5. Isermann Rolf. *Mechatronic Systems – Innovative Products with Embedded Control*. Available at: [https://www.researchgate.net/publication/222668010\\_Mechatronic\\_systems-Innovative\\_products\\_with\\_embedded\\_control](https://www.researchgate.net/publication/222668010_Mechatronic_systems-Innovative_products_with_embedded_control).
6. A System-Safety Process For By-Wire Automotive Systems. *SAE Technical Paper*, 2000.
7. Achieving ASIL D for Microcontroller in Safety-Critical Drive-by-Wire System. *SAE Technical Paper*, 2009.
8. Trends in automotive communication systems. *Proc. IEEE “Special issue on industrial communication systems”*. 2005, no. 93(6), pp. 1204–1223.
9. Achieving 10-9 Dependability with Drive-by-Wire Systems. *SAE Technical Paper*, 2003.

10. Bashta T.M. [et al.] *Nadezhnost gidravlicheskih sistem vozdukhnykh sudov* [Reliability of the hydraulic systems of aircraft]. Moscow, Transport, 1986. 279 p.
11. Managing technology for highly complex critical modular systems: The case of automotive by-wire systems. *International Journal of Production Economics*, 2009, vol. 118, no. 2, pp. 473–485.
12. *Brake by wire system with separate controllers and both position and force input sensors*. Patent US, no. 6390565, 2002.
13. Infinitely variable transmission (IVT) of John Deere 7000 TEN series tractor. *IMECE2002-39347*, pp. 123–131.
14. Architectural design and reliability analysis of a fail-operational brake-by-wire system from ISO 26262 perspectives. *Reliability Engineering & System Safety*, 2011, vol. 96, no. 10, pp. 1349–1359.
15. Krasnevskiy L.G. Avtomaticheskaja transmissija kak obekt upravlenija v sisteme bezopasnosti sovremennogo avtomobilja [Automatic transmission as a control object in security system of a modern vehicle]. *Aktualnye voprosy mashinovedenija: sb. nauch. tr.* [Topical Issues of Mechanical Engineering: collection of scientific articles], 2015, no. 4.
16. Krasnevskiy L.G. *Upravlenie gidromehanicheskimi mnogostupenchatymi peredachami mobilnykh mashin* [Managing multi-stage hydromechanical transmissions of mobile machines]. Minsk, Navuka i tjehnika, 1990. 256 p.
17. Krasnevskiy L. *The fundamental aspects of the structural theory of multispeed Transmissions control*. SAE, 2005.
18. Development of 4 speed electronically controlled new automatic transmission for FWD. *Proc. Seoul FISITA World Automotive Congress*. Seoul, 2000.
19. *Transmission and controls*. Patent US, no. 3505907, 1970.
20. A Study on Full Electronic Control of Automatic Transmission: Direct Active Shift Control. *Proc. Seoul FISITA World Automotive Congress*. Seoul, 2000.
21. *Functional Safety Draft International Standard for Road Vehicles: Background, Status, and Overview*. ISO 26262, 2010.
22. Kopetz H. *From a Federated to an Integrated Architecture for Dependable Embedded Systems*. TU Wien, 2004.
23. Krasnevskiy L.G. *Sintez relejnyh gidrosistem upravlenija mnogostupenchatymi transmissijami tjazhelyh avtomobilej*. *Diss. kand. tehn. nauk* [Synthesis of relay control multistage hydraulic transmissions of heavy vehicles. Ph.D. sci. diss.]. Minsk, 1969.
24. Krasnevskiy L. *The Synthesis Method of Electro-Hydraulic Schemes of Mechatronic Control Systems for Hydromechanical Transmissions*. SAE, 2003.
25. *Control apparatus of vehicular automatic transmission*. Patent US, no. 7419452, 2008.
26. *Hydraulic control system for an automatic transmission having electronic transmission range selection with failure mode control*. Patent US, no. 8435148, 2013.