ЛЕКЦИЯ 12
ДИАГНОСТИРОВАНИЕ И ОТКАЗОУСТОЙЧИВОЕ УПРАВЛЕНИЕ. ОБНАРУЖЕНИЕ НЕИСПРАВНОСТЕЙ ДАТЧИКОВ И ИСПОЛНИТЕЛЬНЫХ МЕХАНИЗМОВ, РЕЗЕРВИРОВАНИЕ И ПЕРЕХОД В БЕЗОПАСНЫЙ РЕЖИМ

Цель

Сформировать у обучающихся системное представление о диагностировании и отказоустойчивом управлении как о критически важных функциях интеллектуальных систем управления автомобилями. Рассмотреть классификацию и природу неисправностей, архитектуру систем диагностирования, методы обнаружения неисправностей датчиков и исполнительных механизмов, принципы резервирования и организации перехода в безопасный режим, а также требования стандартов функциональной безопасности и кибербезопасности.

Планируемые результаты

После изучения данной лекции обучающийся сможет:

- объяснять, почему диагностирование и отказоустойчивость являются критическими функциями автомобильных систем управления;
- классифицировать неисправности по природе возникновения, времени проявления и последствиям;
- описывать архитектуру систем обнаружения неисправностей и диагностирования (FDI);
- характеризовать методы аппаратного, программного и аналитического резервирования;
- объяснять принципы организации перехода в безопасный режим и аварийного функционирования;
- анализировать требования стандартов ISO 26262 и ISO/SAE 21434 к диагностированию и отказоустойчивости;
- оценивать применение методов искусственного интеллекта для прогнозной диагностики и обнаружения неисправностей.

Вопрос занятия. Современный автомобиль — это сложная киберфизическая система, в которой отказ одного датчика или сбой в программном обеспечении может привести к катастрофическим последствиям. Но как система должна отличать реальную неисправность от временного сбоя или шума? Как она должна реагировать, чтобы сохранить управляемость и безопасность? И главное — можно ли спроектировать систему, которая не только обнаруживает неисправности, но и продолжает работать, пусть и с ограничениями, даже при отказе нескольких компонентов?

1. Введение в диагностирование и отказоустойчивое управление

1.1. Почему диагностирование и отказоустойчивость критичны?

Современный автомобиль представляет собой сложную киберфизическую систему, в которой механические, электрические, электронные и программные компоненты тесно интегрированы. Современные автомобили содержат более 100 электронных блоков управления (ECU), соединённых высокоскоростными сетями связи, такими как CAN, FlexRay и Automotive Ethernet. Критически важные приложения — управление тормозами (brake-by-wire), рулевое управление (steer-by-wire), системы управления батареей (BMS) и системы помощи водителю (ADAS) — в значительной степени полагаются на встроенные системы управления, которые должны работать надёжно в условиях жёстких ограничений реального времени и безопасности.

По мере роста сложности системы возрастает и вероятность возникновения неисправностей, вызванных деградацией аппаратного обеспечения, дефектами программного обеспечения, ошибками связи или воздействием внешней среды. В критически важных областях такие неисправности могут привести к опасным событиям с серьёзными последствиями.

Именно поэтому диагностирование и отказоустойчивое управление стали не просто желательными, а **обязательными** функциями автомобильных систем управления. Требования к ним закреплены в стандартах функциональной безопасности, таких как ISO 26262, который определяет структурированный жизненный цикл безопасности, уровни целостности безопасности (ASIL) и систематические методы анализа опасностей и оценки рисков.

1.2. Ключевые понятия и определения

Прежде чем перейти к рассмотрению конкретных методов, необходимо определить ключевые понятия.

Неисправность (fault). Физическое или логическое отклонение характеристики компонента от нормального состояния. Неисправность может быть скрытой (латентной) или явной.

Ошибка (error). Проявление неисправности — неправильное состояние системы, данные или результат вычислений.

Отказ (failure). Событие, при котором система или компонент перестаёт выполнять требуемую функцию.

Диагностирование (diagnostics). Процесс обнаружения, локализации и идентификации неисправностей.

Отказоустойчивость (fault tolerance). Способность системы продолжать выполнение своих функций (возможно, с пониженной производительностью) при наличии неисправностей.

Безопасный режим (safe state). Состояние системы, в котором риск причинения вреда минимален. Переход в безопасный режим — это контролируемое снижение функциональности для предотвращения опасных последствий.

Интервал обработки неисправности (Fault Handling Time Interval, FHTI). Время, доступное для обнаружения неисправности и перехода в безопасное состояние. Включает интервал обнаружения неисправности (Fault Detection Time Interval, FDTI) и интервал реакции на неисправность (Fault Reaction Time Interval, FRTI).

Интервал отказоустойчивого времени (Fault Tolerant Time Interval, FTTI). Максимально допустимое время между возникновением неисправности и наступлением опасного события, если система не предпринимает защитных действий.

Диагностическое покрытие (Diagnostic Coverage, DC). Доля интенсивности отказов элемента аппаратных средств, которая обнаруживается применяемыми диагностическими механизмами.

2. Классификация и природа неисправностей

Для эффективного диагностирования необходимо понимать, какие типы неисправностей могут возникать и как они проявляются.

2.1. Классификация по природе возникновения

Аппаратные неисправности. Связаны с физической деградацией или отказом компонентов:

- **Постоянные (hard faults).** Необратимые отказы, например, обрыв цепи, короткое замыкание, разрушение полупроводникового перехода.
- **Временные (soft faults).** Обратимые сбои, вызванные электромагнитными помехами, перегревом, радиацией. Могут исчезать после восстановления нормальных условий.
- **Параметрические.** Постепенное изменение характеристик компонента (например, увеличение сопротивления, снижение ёмкости) в результате старения или износа.

Программные неисправности. Связаны с ошибками в программном обеспечении:

- **Ошибки логики.** Неправильная реализация алгоритмов.
- **Ошибки данных.** Неправильная инициализация, переполнение буфера, повреждение памяти.
- **Ошибки синхронизации.** Нарушение временных ограничений, состояния гонки, взаимные блокировки.

Коммуникационные неисправности. Связаны с передачей данных по бортовым сетям:

- **Потеря сообщений.** Сообщение не доставлено получателю.
- **Задержка сообщений.** Сообщение доставлено с превышением допустимого времени.
- **Повреждение сообщений.** Искажение содержимого сообщения (ошибки CRC).

- **Несанкционированные сообщения.** Поступление сообщений от непроверенного источника.

Неисправности, связанные с внешней средой. Вызванные воздействием внешних факторов:

- Электромагнитные помехи.
- Экстремальные температуры.
- Влажность, коррозия.
- Механические воздействия (вибрации, удары).

2.2. Классификация по времени проявления

Немедленные (immediate). Проявляются сразу после возникновения. Легко обнаруживаются.

Периодические (intermittent). Проявляются время от времени. Трудно обнаруживаются, особенно если интервалы между проявлениями велики.

Скрытые (latent). Не проявляются в нормальном режиме работы, но становятся заметными в определённых условиях или при совпадении с другими событиями.

2.3. Классификация по последствиям

Критические (critical). Неисправности, которые могут привести к немедленной потере управляемости, аварии или травмам.

Существенные (major). Неисправности, которые ухудшают характеристики системы, но не приводят к немедленной опасности.

Незначительные (minor). Неисправности, которые не влияют на безопасность или основные функции.

Информационные (informational). Неисправности, которые не влияют на работу системы, но требуют внимания обслуживающего персонала.

2.4. Неисправности датчиков

Датчики являются «глазами и ушами» системы управления. Их отказ может иметь серьёзные последствия. Типичные неисправности датчиков:

- **Полный отказ.** Сигнал отсутствует (обрыв) или зафиксирован на крайнем значении.
- **Дрейф.** Постепенное смещение выходного сигнала относительно истинного значения.
- **Шум.** Повышенный уровень случайных флуктуаций сигнала.
- **Зависание (stuck-at).** Сигнал зафиксирован на постоянном значении.
- **Неправильная калибровка.** Систематическая ошибка, вызванная неправильной настройкой.

2.5. Неисправности исполнительных механизмов

Исполнительные механизмы являются «мышцами» системы. Их неисправности могут проявляться как:

- **Полный отказ.** Механизм не реагирует на управляющий сигнал.
- **Зависание (stuck).** Механизм зафиксирован в одном положении.

- **Неполное срабатывание.** Механизм срабатывает частично или с задержкой.
- **Дребезг.** Нестабильное поведение при переключении.
- **Дрейф характеристики.** Изменение передаточной функции (например, износ фрикционных поверхностей).

3. Архитектура систем диагностирования и обнаружения неисправностей

3.1. Обобщённая структура FDI

Система обнаружения неисправностей и диагностирования (Fault Detection and Isolation, FDI) обычно включает следующие функциональные блоки:

Блок обнаружения (Detection). Определяет факт наличия неисправности. Это может быть превышение порога, нарушение логической связи между сигналами, отклонение от эталонной модели и т.д.

Блок локализации (Isolation). Определяет, какой именно компонент (датчик, исполнительный механизм, ECU, сеть) является источником неисправности.

Блок идентификации (Identification). Определяет тип и характер неисправности (постоянный отказ, дрейф, шум и т.д.).

Блок принятия решений (Decision). На основе информации о неисправности принимает решение о необходимых действиях: переход в безопасный режим, реконфигурация, выдача предупреждения водителю, запись в журнал событий.

3.2. Точки диагностики

Стандарт ISO 26262 определяет **точки диагностики (diagnostic points)** как выходные сигналы элемента, в которых наблюдается появление сбоев или их коррекция. Точки диагностики должны быть выбраны таким образом, чтобы обеспечивать требуемое диагностическое покрытие для каждого уровня ASIL.

3.3. Временные параметры диагностирования

Ключевым требованием к системам диагностирования является соблюдение временных ограничений. Стандарт ISO 26262 определяет **интервал обработки неисправности (Fault Handling Time Interval, FHTI)** , который включает:

- **Интервал обнаружения неисправности (Fault Detection Time Interval, FDTI).** Время от возникновения неисправности до её обнаружения системой диагностирования.
- **Интервал реакции на неисправность (Fault Reaction Time Interval, FRTI).** Время от обнаружения неисправности до перехода системы в безопасное состояние.

Сумма FDTI и FRTI должна быть меньше **интервала отказоустойчивого времени (Fault Tolerant Time Interval, FTTI)** — максимально допустимого времени между возникновением неисправности и наступлением опасного события.

Современные исследования показывают, что использование методов искусственного интеллекта позволяет достичь времени восстановления после неисправности менее 30 мс.

4. Методы обнаружения неисправностей

4.1. Аппаратные методы

Прямой контроль. Измерение параметров компонента (напряжение, ток, температура, сопротивление) и сравнение с допустимыми пределами.

Самодиагностика (Built-In Self-Test, BIST). Встроенные в компонент средства диагностирования, активируемые по команде или периодически.

Watchdog-таймеры. Аппаратные таймеры, которые сбрасываются работающей программой. Если программа зависает и не сбрасывает таймер, он генерирует сигнал сброса.

Мониторы питания. Контроль напряжения питания и его стабильности.

4.2. Программные методы

Проверка диапазона (range checking). Проверка того, что значение сигнала находится в допустимых пределах.

Проверка правдоподобности (plausibility checking). Проверка согласованности сигналов от разных датчиков. Например, если датчик скорости показывает 100 км/ч, а датчик положения дроссельной заслонки — 0%, это несоответствие указывает на неисправность одного из датчиков.

Контрольная сумма (checksum) и циклический избыточный код (CRC). Проверка целостности данных при передаче и хранении.

Программные watchdogs. Таймеры, реализованные в программном обеспечении, которые контролируют выполнение критических задач.

Анализ времени выполнения. Контроль того, что задачи выполняются в отведённые временные интервалы.

4.3. Методы аналитической избыточности

Аналитическая избыточность — это использование математических моделей для оценки ожидаемого поведения системы и сравнения с фактическим. Отклонение от модели указывает на возможную неисправность.

Модели на основе наблюдателей (observer-based). Наблюдатель состояния (например, фильтр Калмана) оценивает состояние системы на основе доступных измерений. Разница между оценкой и фактическим измерением (невязка) анализируется для обнаружения неисправностей.

Анализ остаточных сигналов (residual analysis). Генерируются остаточные сигналы — разность между фактическим выходом системы и выходом модели. Анализ остатков (сравнение с порогом, анализ частотного спектра) позволяет обнаруживать неисправности.

Метод главных компонент (Principal Component Analysis, PCA). Статистический метод для обнаружения аномалий в многомерных данных. Исследования показывают, что использование **адаптивной фильтрации Калмана (AKF)** и **вероятностного сглаживания сигналов** повышает точность обнаружения неисправностей.

Ядерный анализ главных компонент (KPCA). Нелинейное обобщение PCA, используемое для моделирования сложной динамики неисправностей в многомерных данных датчиков и исполнительных механизмов.

4.4. Методы на основе машинного обучения

Современные системы диагностирования всё чаще используют методы машинного обучения для обнаружения неисправностей.

Bi-LSTM (Bidirectional Long Short-Term Memory). Рекуррентная нейронная сеть, которая используется для оценки состояния системы (например, перемещения рейки рулевого управления) и обнаружения неисправностей датчиков. Bi-LSTM может обрабатывать данные как в прямом, так и в обратном направлении, что повышает точность оценки.

Последовательный критерий отношения вероятностей (Sequential Probability Ratio Test, SPRT). Статистический метод для обнаружения изменений в сигнале. В сочетании с Bi-LSTM позволяет своевременно обнаруживать отказы датчиков и восстанавливать стабильное состояние автомобиля.

Свёрточные нейронные сети (CNN). Используются для анализа данных датчиков в системах ADAS. Исследования показывают, что ИИ-модели могут прогнозировать аппаратные и программные неисправности до того, как они перерастут в опасные состояния.

Машины опорных векторов (SVM) и случайный лес (Random Forest). Используются для классификации типов неисправностей в инверторах и других силовых компонентах.

Цифровые двойники (Digital Twin). Технология цифровых двойников позволяет создавать виртуальные представления физических систем для прогнозного управления неисправностями. Исследования показывают, что цифровые двойники на основе KPCA обеспечивают точность обнаружения неисправностей **98,2%** при различных сценариях отказов датчиков и исполнительных механизмов.

В работе, опубликованной в 2026 году на WCX SAE World Congress, представлена **структура прогнозного управления неисправностями (Predictive Fault Management)** , которая интегрирует модели ИИ с механизмами безопасности ISO 26262. Подход демонстрирует **до 25% более высокое диагностическое покрытие** и время восстановления после неисправности менее 30 мс, сохраняя при этом соответствие требованиям ASIL-D.

Важно отметить, что в этой структуре ИИ-модель используется **исключительно как диагностическое дополнение** и не учитывается как механизм безопасности ISO 26262; все решения по безопасности и реакции на неисправности остаются под контролем детерминированной «безопасной оболочки».

5. Отказоустойчивое управление и резервирование

5.1. Принципы отказоустойчивости

Отказоустойчивое управление (Fault-Tolerant Control, FTC) обеспечивает продолжение работы системы (возможно, с пониженной производительностью) при возникновении неисправностей. Основные стратегии FTC:

Пассивное FTC (Passive FTC). Система спроектирована таким образом, чтобы быть нечувствительной к определённым типам неисправностей (робастность). Не требует перестройки структуры управления.

Активное FTC (Active FTC). Система обнаруживает неисправность и реконфигурирует структуру управления для компенсации её последствий.

Адаптивное FTC. Система адаптирует параметры управления в реальном времени для компенсации изменений, вызванных неисправностями.

5.2. Аппаратное резервирование

Аппаратное резервирование — это использование дополнительных (резервных) компонентов для обеспечения работоспособности при отказе основных.

N-модульная избыточность (N-Modular Redundancy, NMR). Система состоит из N параллельно работающих компонентов, и выход определяется голосованием. Для работы системы необходимо как минимум три компонента. Система может допускать отказы в (N-1)/2 модулях.

Тройная модульная избыточность (Triple Modular Redundancy, TMR). Частный случай NMR с N=3. Три датчика работают параллельно, и контроллер выполняет голосование по трём значениям.

Динамическое резервирование. В отличие от статической избыточности, которая требует большого числа компонентов, динамические архитектуры используют механизмы обнаружения неисправностей и реконфигурации. Резервные компоненты могут находиться в «горячем» режиме (активно обрабатывают информацию) или «холодном» режиме (ограниченная активность).

Резервирование с парами и резервом (Pair and Spare). Используется в системах brake-by-wire: два датчика активно сравниваются контроллером. При обнаружении расхождения между двумя активными датчиками включается дополнительный датчик, определяется, какой из активных датчиков неисправен, и он исключается.

Двухъядерные процессоры в режиме Lockstep. Два процессорных ядра выполняют одинаковые вычисления и сравнивают результаты. При

расхождении фиксируется ошибка. Этот метод обеспечивает диагностическое покрытие 99,9%.

Двойное резервирование (1oo2D). Два исполнительных механизма с контролем работоспособности.

5.3. Программное резервирование

Разнородное резервирование (Diverse Redundancy). Использование разных алгоритмов или разных реализаций одного алгоритма для выполнения одной функции. Если одна реализация даёт сбой, другая может продолжить работу.

N-версионное программирование (N-Version Programming). Разработка N независимых версий одного программного модуля разными командами. Все версии выполняются параллельно, и результат определяется голосованием.

Сторожевые мониторы (Watchdogs). Программные компоненты, контролирующие выполнение критических задач и корректность данных.

Безопасное переключение (Failover). Механизм автоматического переключения на резервный компонент или резервную программу при обнаружении неисправности.

5.4. Аналитическое резервирование

Аналитическое резервирование использует математические модели вместо физических резервных компонентов.

Наблюдатели состояния. Оценка недоступных для измерения переменных на основе модели и доступных измерений. При отказе датчика его значение может быть заменено оценкой наблюдателя.

Фильтры Калмана. Оптимальная оценка состояния системы в присутствии шумов. Может использоваться для обнаружения и компенсации отказов датчиков.

Нейросетевые модели. Обученная нейронная сеть может аппроксимировать поведение системы и использоваться для оценки отсутствующих сигналов.

6. Переход в безопасный режим

6.1. Понятие безопасного режима

Безопасный режим (safe state) — это состояние системы, в котором риск причинения вреда сведён к минимуму. В автомобильных системах безопасный режим может означать:

- Снижение мощности или скорости.
- Переход в аварийный режим управления с ограниченной функциональностью.
- Безопасная остановка автомобиля.
- Отключение неисправной функции и переход на резервную.
- Предупреждение водителя и передача управления человеку.

6.2. Этапы перехода в безопасный режим

Обнаружение. Система диагностирования обнаруживает неисправность. Время обнаружения (FDTI) должно быть минимальным.

Оценка. Система оценивает тяжесть неисправности и её потенциальные последствия.

Принятие решения. Система выбирает наиболее подходящий безопасный режим на основе оценки риска.

Исполнение. Система выполняет переход в безопасный режим. Время реакции (FRTI) должно быть минимальным.

Подтверждение. Система проверяет, что переход в безопасный режим выполнен успешно.

6.3. Уровни функциональности при отказах

В зависимости от тяжести неисправности система может переходить на различные уровни функциональности:

Полная функциональность (Full operation). Система работает в штатном режиме. Резервирование обеспечивает возможность работы даже при наличии скрытых неисправностей.

Ограниченная функциональность (Degraded operation). Система продолжает работу, но с ограничениями: снижение максимальной скорости, ограничение ускорения, отключение некоторых функций (например, круиз-контроля).

Аварийный режим (Limp-home mode). Система обеспечивает только базовую функциональность, достаточную для безопасного движения до места ремонта. Например, ограничение скорости до 20-30 км/ч.

Безопасная остановка (Safe stop). Система выполняет контролируемую остановку автомобиля.

Полное отключение (Shutdown). Система отключает неисправную функцию, если её работа представляет опасность.

6.4. Пример: аварийный режим инвертора электромобиля

В работе, опубликованной в 2026 году, представлена стратегия отказоустойчивого управления для пятифазного высоковольтного инвертора электромобиля. При возникновении неисправности (обрыв или короткое замыкание в одной из фаз) система:

1. Активно контролирует фазные токи и напряжения для обнаружения неисправности.
2. Изолирует неисправные компоненты, отключая управляющие импульсы.
3. Продолжает работу двигателя на оставшихся здоровых фазах.
4. Обеспечивает движение в аварийном режиме (limp mode) для безопасного достижения пункта назначения.

Это демонстрирует, как активное FTC с обнаружением, изоляцией и реконфигурацией позволяет сохранить базовую функциональность даже при отказе критических компонентов.

6.5. Двухканальные архитектуры для отказоустойчивых систем

В критически важных системах (steer-by-wire, brake-by-wire) используются двухканальные архитектуры с полным резервированием:

- **Номинальный канал (nominal channel).** Основной канал управления, включающий датчики, модули определения стратегии вождения, модули управления транспортным средством и исполнительные механизмы.
- **Резервный канал (redundant channel).** Полностью дублирует номинальный канал.

При отказе номинального канала система мгновенно переключается на резервный. Такая архитектура обеспечивает **безотказную работу (fail-operational)** — систему, которая продолжает работать даже после отказа.

7. Диагностирование и отказоустойчивость в системах трансмиссии

7.1. Диагностирование датчиков трансмиссии

В системах управления трансмиссией используются многочисленные датчики, требующие диагностирования:

Датчики скорости. Отказ датчика скорости может привести к неправильному переключению передач. Используется аналитическая избыточность: скорость оценивается по другим датчикам (ABS, датчик положения педали).

Датчики давления. В гидравлических системах управления муфтами. Отказ датчика давления может привести к неправильному управлению муфтой. Используется проверка диапазона и взаимосвязи с другими сигналами.

Датчики температуры. Контроль температуры масла, электродвигателя, инвертора. Используется проверка диапазона и скорости изменения.

Датчики положения. Датчики положения селектора передач, положения муфты. Используются методы аналитической избыточности.

7.2. Диагностирование исполнительных механизмов трансмиссии

Соленоидные клапаны. Контроль тока и напряжения, проверка реакции на управляющий сигнал.

Электрические масляные насосы. Контроль тока, скорости вращения, давления.

Муфты. Контроль пробуксовки (разница скоростей ведущей и ведомой частей), давления в гидросистеме, температуры.

7.3. Отказоустойчивое управление трансмиссией

При обнаружении неисправности в трансмиссии система может:

- Ограничить крутящий момент для защиты компонентов.
- Переключиться в аварийный режим с фиксированной передачей.
- Отключить неисправную муфту и перейти на резервную.
- Предупредить водителя и ограничить скорость.

8. Взаимосвязь функциональной безопасности и кибербезопасности

8.1. ISO 26262 — Функциональная безопасность

Стандарт ISO 26262 «Road vehicles — Functional safety» является основным документом, регламентирующим требования к функциональной безопасности автомобильных электронных систем.

Ключевые понятия ISO 26262:

Уровни целостности безопасности (Automotive Safety Integrity Levels, ASIL). От A (самый низкий) до D (самый высокий). Для каждого уровня определяются требования к диагностическому покрытию, отказоустойчивости и другим аспектам безопасности.

Анализ опасностей и оценка риска (Hazard Analysis and Risk Assessment, HARA). Систематический метод выявления потенциальных опасностей и оценки связанных с ними рисков.

Интервал отказоустойчивого времени (Fault Tolerant Time Interval, FTTI). Максимально допустимое время между возникновением неисправности и наступлением опасного события.

Диагностическое покрытие (Diagnostic Coverage, DC). Доля отказов, обнаруживаемых применяемыми диагностическими механизмами.

Механизмы безопасности (Safety Mechanisms). Технические и организационные меры для обнаружения и контроля неисправностей или для смягчения их последствий.

В стандарте ISO 26262 определены различные механизмы безопасности для обнаружения неисправностей, включая:

- Двухъядерные процессоры в режиме lockstep (диагностическое покрытие 99,9%).
- Избыточные датчики.
- Контролируемые исполнительные механизмы.
- Сторожевые таймеры.

8.2. ISO/SAE 21434 — Кибербезопасность

Стандарт ISO/SAE 21434 «Road vehicles — Cybersecurity engineering» определяет требования к кибербезопасности автомобильных систем.

Ключевые аспекты ISO/SAE 21434, связанные с диагностированием:

Обнаружение вторжений. Система должна обнаруживать попытки несанкционированного доступа и атак.

Мониторинг целостности. Контроль целостности программного обеспечения и данных.

Безопасные обновления. Механизмы проверки подлинности и целостности обновлений ПО.

Журналирование событий безопасности. Ведение защищённых журналов для расследования инцидентов.

8.3. Объединение безопасности и кибербезопасности

Современные исследования показывают необходимость **объединённого подхода** к функциональной безопасности и кибербезопасности. В работе, опубликованной в 2026 году, представлен **единый архитектурный подход**, который исследует, как механизмы функциональной безопасности ISO 26262 и механизмы кибербезопасности ISO/SAE 21434 могут быть интегрированы в зональных архитектурах ECU.

Кибербезопасность в соответствии с ISO/SAE 21434 фокусируется на защите ECU от атак и поддержании целостности системы. При этом стандарт идентифицирует **атаки с внедрением неисправностей (fault injection attacks)** как растущий риск.

Интеграция подходов позволяет:

- Обнаруживать как случайные неисправности, так и преднамеренные атаки.
- Использовать общие механизмы диагностирования для обоих типов событий.
- Обеспечивать единую стратегию перехода в безопасный режим.

9. Интеллектуальные подходы к диагностированию и отказоустойчивости

9.1. Прогнозное управление неисправностями (Predictive Fault Management)

Современные исследования предлагают **прогнозное управление неисправностями (Predictive Fault Management)** на основе ИИ. В отличие от реактивных систем, которые обнаруживают неисправность только после её возникновения, прогнозные системы анализируют данные в реальном времени и прогнозируют возможные неисправности до их возникновения.

Этот подход:

- Интегрирует прогнозные модели ИИ с механизмами безопасности ISO 26262.
- Обеспечивает адаптивную диагностику, изоляцию неисправностей и стратегии быстрого восстановления.
- Демонстрирует до 25% более высокое диагностическое покрытие.

9.2. Цифровые двойники для отказоустойчивого управления

Цифровые двойники (Digital Twins) создают виртуальные копии физических систем для мониторинга и диагностики.

В работе, опубликованной в 2025 году, представлена интегрированная структура отказоустойчивого управления на основе **KPCA (Kernel Principal Component Analysis) цифрового двойника** и **модельного прогнозирующего управления (MPC)** для автономных транспортных средств.

Структура обеспечивает:

- Обнаружение неисправностей в реальном времени.

- Оценку и реконструкцию неисправностей.
- Точность обнаружения неисправностей **98,2%**.
- Сокращение ошибки скорости на **90,5%** , ошибки бокового смещения на **91,7%** и ошибки угла на **81,1%** по сравнению с некомпенсированными неисправностями.

9.3. Отказоустойчивое управление на основе Bi-LSTM и SPRT

В работе, опубликованной в 2023 году, представлена стратегия обнаружения неисправностей и отказоустойчивого управления (FDFTC) для автономной системы рулевого управления.

Стратегия включает:

- **Оценщик перемещения рейки на основе Bi-LSTM (Bidirectional Long Short-Term Memory)** для программного резервирования датчика.
- **Последовательный критерий отношения вероятностей (SPRT)** для обнаружения отказов датчика.

Результаты показывают, что стратегия позволяет своевременно обнаруживать отказы датчиков и эффективно восстанавливать стабильное состояние автомобиля.

9.4. Скользящий режим и адаптивное обнаружение неисправностей

В работе, опубликованной в 2022 году, представлен **адаптивный метод обнаружения неисправностей и аварийного управления** для систем fail-safe с использованием подхода скользящего режима.

Метод включает:

- **Алгоритм линейного прогнозирования** для обнаружения неисправностей датчиков окружающей среды.
- **Прогнозирующий и накопительный метод** для определения допустимых границ текущих измерений.

10. Вызовы и перспективы развития

10.1. Основные вызовы

Сложность систем. Рост числа ECU, датчиков и исполнительных механизмов увеличивает сложность диагностирования.

Временные ограничения. Обнаружение неисправностей и переход в безопасный режим должны выполняться в течение миллисекунд.

Неопределённость. Различие между случайной неисправностью и преднамеренной атакой становится всё более сложной задачей.

Интеграция ИИ. Использование ИИ для диагностирования создаёт новые проблемы, связанные с объяснимостью, предвзятостью данных и дрейфом моделей.

Старение компонентов. Тепловые и механические характеристики компонентов меняются с течением времени, что требует адаптации порогов диагностирования.

10.2. Перспективы развития

Прогнозная диагностика на основе ИИ. Развитие методов прогнозирования неисправностей до их возникновения.

Цифровые двойники. Создание высокоточных виртуальных моделей для диагностирования и прогнозирования.

Федеративное обучение. Обучение моделей диагностирования на распределённых данных без их централизации для повышения приватности.

Интеграция функциональной безопасности и кибербезопасности. Разработка единых архитектур и методов для обнаружения как случайных неисправностей, так и преднамеренных атак.

Объяснимый ИИ (XAI). Разработка методов, позволяющих интерпретировать решения, принимаемые ИИ-моделями диагностирования.

Самообучающиеся системы. Разработка систем, которые адаптируют пороги диагностирования и стратегии отказоустойчивости на основе накопленного опыта.

11. Закрепление и завершение

11.1. Мини-тест

1. Что такое интервал обработки неисправности (FHTI) и из каких компонентов он состоит?
2. Каковы основные методы обнаружения неисправностей датчиков?
3. В чём отличие тройной модульной избыточности (TMR) от динамического резервирования?
4. Что такое безопасный режим и каковы его уровни?
5. Каковы основные требования стандарта ISO 26262 к диагностированию?

11.2. Эталонные краткие ответы

1. **Интервал обработки неисправности (FHTI)** — это время, доступное для обнаружения неисправности и перехода в безопасное состояние. Он включает **интервал обнаружения неисправности (FDTI)** — время от возникновения неисправности до её обнаружения, и **интервал реакции на неисправность (FRTI)** — время от обнаружения до перехода в безопасное состояние.
2. **Основные методы обнаружения:** аппаратные (прямой контроль, BIST, watchdogs), программные (проверка диапазона, проверка правдоподобности, контрольные суммы), аналитической избыточности (наблюдатели, фильтры Калмана, PCA, KPCA) и на основе машинного обучения (Bi-LSTM, SPRT, нейронные сети, цифровые двойники).
3. **Тройная модульная избыточность (TMR)** — это статическое резервирование с тремя параллельно работающими компонентами и голосованием. **Динамическое резервирование** использует механизмы обнаружения

неисправностей и реконфигурации, позволяя обходиться меньшим числом компонентов (вплоть до двух с резервным).

4. **Безопасный режим** — это состояние системы, в котором риск причинения вреда минимален. Уровни: полная функциональность, ограниченная функциональность (degraded operation), аварийный режим (limp-home), безопасная остановка (safe stop), полное отключение (shutdown).

5. **Основные требования ISO 26262:** определение уровней ASIL, проведение HARA, соблюдение FTTI, обеспечение требуемого диагностического покрытия (DC), реализация механизмов безопасности, документирование всех этапов жизненного цикла.

11.3. Итоговые положения

Диагностирование и отказоустойчивое управление являются критическими функциями автомобильных систем, обеспечивающими безопасность и надёжность.

Неисправности классифицируются по природе возникновения (аппаратные, программные, коммуникационные, внешние), времени проявления (немедленные, периодические, скрытые) и последствиям (критические, существенные, незначительные).

Системы обнаружения неисправностей и диагностирования (FDI) включают блоки обнаружения, локализации, идентификации и принятия решений.

Методы обнаружения включают аппаратные (прямой контроль, BIST, watchdogs), программные (проверка диапазона, правдоподобности, контрольные суммы), аналитической избыточности (наблюдатели, PCA, KPCA) и на основе машинного обучения (Bi-LSTM, SPRT, цифровые двойники).

Отказоустойчивое управление использует аппаратное резервирование (TMR, pair and spare, lockstep), программное резервирование (разнородное, N-версионное) и аналитическое резервирование (наблюдатели, фильтры Калмана).

Переход в безопасный режим включает этапы обнаружения, оценки, принятия решения, исполнения и подтверждения. Уровни функциональности варьируются от полной до полного отключения.

Стандарты ISO 26262 (функциональная безопасность) и **ISO/SAE 21434** (кибербезопасность) определяют требования к диагностированию и отказоустойчивости.

Интеллектуальные подходы (прогнозное управление неисправностями, цифровые двойники, Bi-LSTM, скользящее управление) обеспечивают более высокую точность и скорость диагностирования.

Перспективы развития связаны с прогнозной диагностикой на основе ИИ, цифровыми двойниками, федеративным обучением, интеграцией безопасности и кибербезопасности, объяснимым ИИ и самообучающимися системами.

Задание после лекции

Выберите один из аспектов диагностирования и отказоустойчивого управления (метод обнаружения неисправностей, стратегия резервирования, переход в безопасный режим, стандарт функциональной безопасности) и подготовьте аналитический обзор (2–3 страницы), в котором:

1. Опишите выбранный аспект и его роль в обеспечении безопасности автомобильных систем.
2. Объясните принципы работы и технические решения.
3. Проанализируйте преимущества и ограничения.
4. Приведите примеры из научных исследований или промышленности.
5. Оцените перспективы развития выбранного аспекта.

Контрольные вопросы

1. Почему диагностирование и отказоустойчивость являются критическими функциями автомобильных систем?
2. Что такое неисправность, ошибка и отказ?
3. Каковы основные типы неисправностей по природе возникновения?
4. Каковы основные типы неисправностей по времени проявления?
5. Каковы типичные неисправности датчиков?
6. Каковы типичные неисправности исполнительных механизмов?
7. Что такое интервал обработки неисправности (FHTI)?
8. Что такое интервал отказоустойчивого времени (FTTI)?
9. Что такое диагностическое покрытие (DC)?
10. Какие блоки входят в систему обнаружения неисправностей и диагностирования (FDI)?
11. Каковы основные методы обнаружения неисправностей?
12. Что такое аналитическая избыточность и как она применяется для обнаружения неисправностей?
13. Как машинное обучение применяется для обнаружения неисправностей?
14. Что такое цифровой двойник и как он применяется для отказоустойчивого управления?
15. В чём отличие пассивного FTC от активного FTC?
16. Что такое тройная модульная избыточность (TMR)?
17. Что такое динамическое резервирование?
18. Что такое двухъядерный процессор в режиме lockstep?
19. Что такое безопасный режим и каковы его уровни?
20. Каковы основные этапы перехода в безопасный режим?
21. Что такое аварийный режим (limp-home mode)?
22. Каковы требования стандарта ISO 26262 к диагностированию?

23. Каковы требования стандарта ISO/SAE 21434 к диагностированию?

24. Как интегрируются функциональная безопасность и кибербезопасность?

25. Что такое прогнозное управление неисправностями (Predictive Fault Management)?

26. Как Bi-LSTM применяется для обнаружения неисправностей?

27. Что такое последовательный критерий отношения вероятностей (SPRT)?

28. Каковы основные вызовы при разработке систем диагностирования и отказоустойчивого управления?

29. Как старение компонентов влияет на диагностирование?

30. Каковы перспективы развития диагностирования и отказоустойчивого управления?

Список рекомендуемой литературы

Основная литература

1. Robert Bosch GmbH. Automotive Handbook. 11th ed. — Chichester: Wiley, 2022. — 2047 p. — ISBN 978-1-119-91190-6.

2. Ulsoy A. G., Peng H., Çakmakcı M. Automotive Control Systems. — Cambridge: Cambridge University Press, 2012. — 407 p. — ISBN 978-1-107-68604-5. — DOI: 10.1017/CBO9780511844577.

3. Rajamani R. Vehicle Dynamics and Control. 2nd ed. — New York: Springer, 2012. — 496 p. — ISBN 978-1-4614-1432-2. — DOI: 10.1007/978-1-4614-1433-9.

Дополнительная литература

4. ISO 26262:2018. Road Vehicles — Functional Safety. Parts 1–10. — Geneva: International Organization for Standardization, 2018.

5. ISO/SAE 21434:2021. Road Vehicles — Cybersecurity Engineering. — Geneva: International Organization for Standardization, 2021.

6. Abdul Karim A. AI-Enhanced Functional Safety in ADAS Controllers: Predictive Fault Management under ISO 26262 // SAE Technical Paper. — 2026. — No. 2026-01-0036. — DOI: 10.4271/2026-01-0036.

7. KPCA Digital Twin-Enhanced Real-Time Fault-Tolerant Control for Autonomous Vehicles // ScienceDirect. — 2025.

8. Fault Detection and Fault-Tolerant Control of Autonomous Steering System for Intelligent Vehicles Combining Bi-LSTM and SPRT // ScienceDirect. — 2023.

9. Safety-Oriented Redundancy and Fault-Tolerant Control in Automotive Embedded Systems // Zenodo. — 2023.

10. Intelligent Fault-Tolerant Control Strategy for 5Phase HV Electric Vehicle Traction Inverters // IEEE Xplore. — 2026.
11. Functional Safety and Cybersecurity in Zonal ECU Architectures: A Unified Architectural and Experimental Approach // IEEE Xplore. — 2026.
12. Automating Fault Detection Time Interval in Automotive Functional Safety Using HIL Simulation // TRID. — 2025.

Электронные ресурсы

13. SAE International. SAE Technical Papers Database. — Режим доступа: https://www.sae.org/publications/technical-papers.
14. SpringerLink. Electronic Collection of Scientific and Educational Literature. — Режим доступа: https://link.springer.com.
15. IEEE Xplore. Scientific and Technical Publications Database. — Режим доступа: https://ieeexplore.ieee.org.
16. ScienceDirect. Scientific and Technical Publications Database. — Режим доступа: https://www.sciencedirect.com.