

-НАМИ-

**Выполнение положений ISO 26262
и интеграция в процессы разработки
электрических и электронных систем
ФГУП НАМИ**

Рогов П.С., Холодилин И.В., Крутько О.В., Королев А.В., Лепеева И.Б.

ЛОКАЛИЗАЦИЯ

ПП РФ №719

Больше нет:



Как гарантировать
безопасность
Э/Э систем?

Разработка электрических и электронных систем

-НАМИ-

Перечень систем в проектах

AURUS MOTO

- Силовой агрегат
- Система ВВ питания
- Система термостатирования
- Система торможения
- Система НВ питания
- Система комфорта
- Система внешнего освещения
- Внешнее звуковое оповещение
- Система идентификации
- Мониторинг давления в шинах
- Имитация звука ДВС
- Система спец. сигналов
- Система спец. связи

Всего в работе **34** системы

≈ **80%** систем имеют
HW/SW собственной разработки

AURUS

- Система управления движением
- Система управления комбинированной установкой
- Электрогидравлическая система РУ
- Электрическая система РУ
- Система ВВ питания
- Система хранения водорода
- Система контроля перестроения
- Система автоматического экстренного торможения
- Система адаптивного круиз-контроля
- Система управления матричным светом
- Система предупреждения при открытии дверей
- Система предупреждения об объектах при движении задним ходом
- Система удержания в полосе движения
- Система помощи при парковке
- Система защиты пассажиров (пассивная безопасность)
- Стояночный тормоз
- Тормозная система (ABS, EBD, TCS и пр.)
- Информационно-развлекательная система
- Комбинация приборов
- Система управления рулевой колонкой
- Система управления электропитанием/ система состояний автомобиля

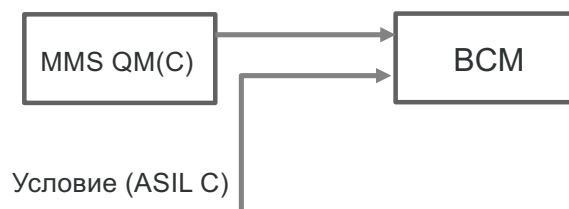
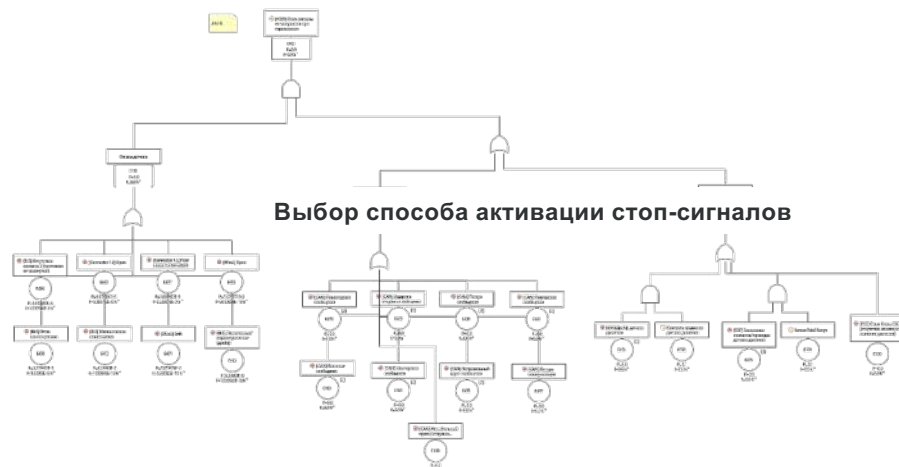


Функциональная безопасность в проектах

-НАМИ-

Стадия концепции ФБ

- декомпозиция ASIL
- выбор датчиков/способов мониторинга
- условия перехода между состояниями системы
- концептуальный функционал системы
- лучшая реакция на сбой/отказ на уровне системы



Необходимый шаг к собственной интеграции компонентов в систему

Функциональная безопасность в проектах

-НАМИ-

Стадия концепции ТБ

- Контроль и экспертиза работ поставщика компонента по ISO 26262
- Необходимый шаг к собственной разработке безопасных систем/компонентов
- Технические требования по безопасности
- Выбор механизмов безопасности
- Программа испытаний системы/компонентов

Технические требования по безопасности

Если T15 «по проводу» отсутствует и при этом CAN сигнал T15 state = active, считать T15 = вкл
Если T15 «по проводу» присутствует и при этом CAN сигнал T15 state = not active, либо есть неисправности/ошибки передачи данных CAN, считать T15 = вкл
Если сигнал отсутствует и физически и в CAN – T15 = выкл

Проверку на залипание сигнала от датчика на одном значении (stuck in range) реализовать программно за счет контроля изменения значения от датчика в течение N циклов, уведомлять водителя об обнаруженной ошибке
Проверку на зашумление сигнала от датчика (oscillations) реализовать программно: если датчик отправляет сигналы по изменению давления при скорости 0 км/ч - детектировать неисправность, уведомлять водителя об обнаруженной ошибке

Длительность нажатия кнопки должна исключать появление статуса = вкл. придребезге и залипании контактов кнопки. Минимальная длительность нажатия кнопки для статуса «вкл.» = 1.2 секунды (tbd), минимальная длительность нажатия для обнаружения залипания контактов = 5 секунд (tbd). При обнаружении залипания контактов – отправка предупреждающего сообщения для DB

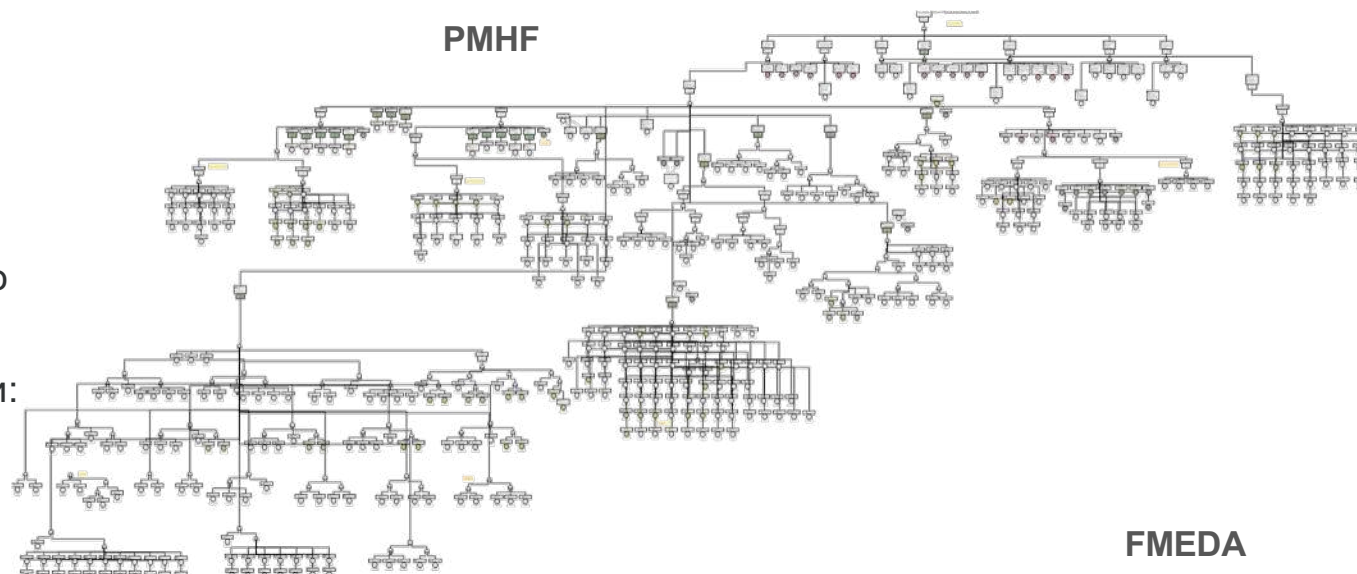
Необходимо проводить сравнение значений TPS1 и TPS2. При выявлении расхождения значений перейти на валидный сигнал (согласованный со значением TVDV). Отправить предупреждающее сообщение для IC, активировать аварийный режим с ограничением крутящего момента

Функциональная безопасность в проектах

-НАМИ-

Стадия разработки HW

- Контроль и экспертиза разработки HW/SW по ISO 26262
- Собственная разработка OEM/OES по ISO 26262 в части HW/SW
- Метрики по достижению безопасности:
 - PMHF – в части допустимых значений случайных отказов HW
 - SPFM, LFM – в части достаточного охвата диагностикой одиночных и скрытых сбоев (FMEDA)
- Уточнение механизмов безопасности
- Выбор компонентов HW
- Тестирование компонента



Имя компонента	Назначение станд. в РП	Суммарная интерьерная станд. в РП	Вспомог. интерьерная станд. в РП	Вспомог. интерьерная станд. в РП	Потенциальная оценка	Comment on this failure	Расхождение интерьерной станд. в %	Расхождение интерьерной станд. в РП	Вспомог. Дана Сбл. в %	Сопоставление станд. взаимной связности	Нормативные интерьерные	МБ предотвращает станд. не-нарушения целой безопасности	QuantSPH в %	SPH в РП	Всего SPH в РП	Значимость SPH	МБ предотвращает станд. целостности целой безопасности	МБ предотвращает серьезный инцидент
AI_V/ARL3	0,0	0,00202	✓											0,0	0,0			
AI_V/HL1_1 FO	0,0	35,70023	✓											2,670	15,79			
AI_V/MLU	0,0	12,82000	✓											2,315	15,20			
AI_V/Terminal	0,0	40,96050	✓											0,0				
Y01: TPS2ACAP-FB/7 H	14,0	14,0	✓		Shut Open Drift - Drift - Open		70,0 20,0 5,0 5,0 40,0	9,8 2,8 0,7 0,7 0,05662	0,0 2,0 0,0 0,0 0,08692198	0,0 0,0 0,7 0,7 0,04246640	0,0 0,0 0,7 0,7 0,04246640	0,0 0,0 0,0 0,0 0,0	0,0 0,0 0,0 0,0 0,0	- - - - -	0,0 0,0 0,0 0,0 0,0	0,0 0,0 0,0 0,0 0,0	✓ ✓ ✓ ✓ ✓	
RI: ACB023FR-0715 OKL	0,140	0,141555	✓		Open Drift - Drift - Open		30,0 30,0 30,0 40,0	0,04246 0,04246 0,04246 0,05662198	0,0 0,0 0,0 0,05662198	0,0 0,04246640 0,04246640 0,05662198	0,0 0,0 0,0 0,0	0,0 0,0 0,0 0,0	- - - -	0,0 0,0 0,0 0,0	0,0 0,0 0,0 0,0	0,0 0,0 0,0 0,0	✓ ✓ ✓ ✓	
RI2: ACB023FR-0713 OKL	0,140	0,141555	□		Open Drift - Drift - Open		30,0 30,0 30,0 40,0	0,04246 0,04246 0,04246 0,05662198	0,0 0,0 0,0 0,05662198	0,04246640 0,04246640 0,04246640 0,05662198	0,0 0,0 0,0 0,0	0,0 0,0 0,0 0,0	- - - -	0,0 0,0 0,0 0,0	0,0 0,0 0,0 0,0	0,0 0,0 0,0 0,0	✓ ✓ ✓ ✓	
RI3: ACB023FR-071K SL	0,140	0,141555	✓		Open Drift - Drift - Open		30,0 30,0 30,0 40,0	0,04246 0,04246 0,04246 0,05662198	0,0 0,0 0,0 0,05662198	0,04246640 0,04246640 0,04246640 0,05662198	0,0 0,0 0,0 0,0	0,0 0,0 0,0 0,0	- - - -	0,0 0,0 0,0 0,0	0,0 0,0 0,0 0,0	0,0 0,0 0,0 0,0	✓ ✓ ✓ ✓	

Эффект применения ISO 26262



	ASIL A	(ASIL B)*	ASIL C**	ASIL D**
PMHF	-	$< 1 \times 10^{-7}$ 1/ч (100 FIT)	$< 1 \times 10^{-7}$ 1/ч (100 FIT)	$< 1 \times 10^{-8}$ 1/ч (10 FIT)

*рекомендуемое требование

**обязательное требование

Оценка вероятности нарушения целей безопасности (метрика PMHF)

Цель безопасности	PMHF до мероприятий ФБ	PMHF после технических решений стадии технической концепции	PMHF после анализа ФБ на аппаратном уровне
G001 – ASIL C			
G002 – ASIL C			
G003 – ASIL B			
G004 – ASIL B			
G005 – ASIL B			

Надежность и безопасность

Эффект применения ISO 26262



Количественный анализ для блока управления и защиты электропитания

	MSIL A	(MSIL B)	MSIL C*	MSIL D**
PMHF	-	-	$< 1 \times 10^{-7}$ 1/ч (100 FIT)	$< 1 \times 10^{-7}$ 1/ч (100 FIT)

*рекомендуемое требование **обязательное требование

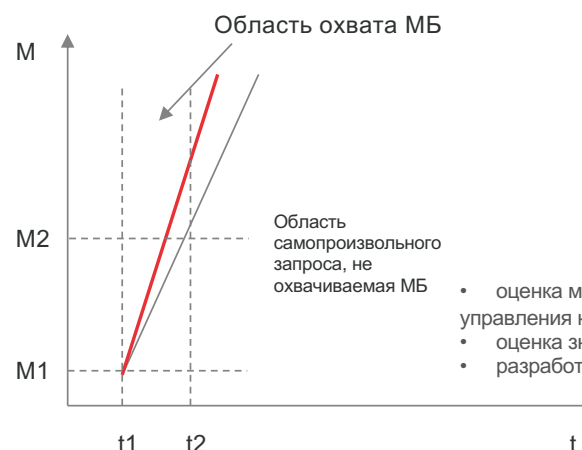
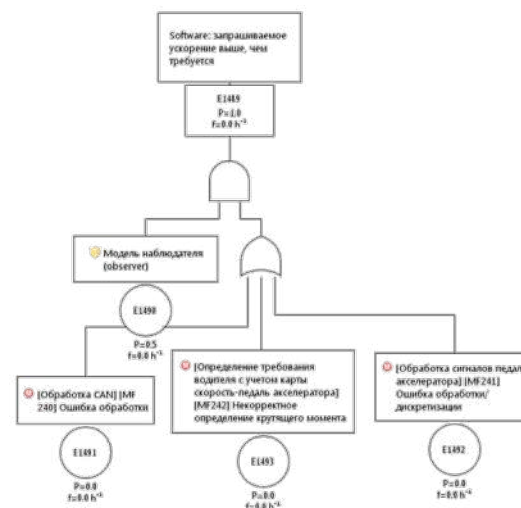
Система	ID ЦБ	PMHF	PMHF после анализа ФБ на аппаратном уровне
Внешнее освещение	ELS Moto G001 (MSIL C)		
Внешнее освещение	ELS Moto G003 (MSIL C)		
Внешнее освещение	ELS Moto G005 (MSIL C)		
Внешнее освещение	ELS Moto G006 (MSIL C)		

Надежность и безопасность

Функциональная безопасность в проектах

Стадия разработки SW

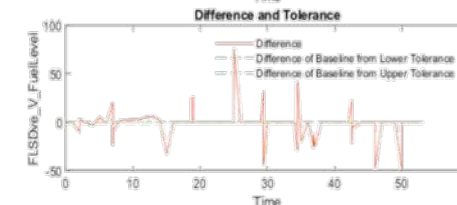
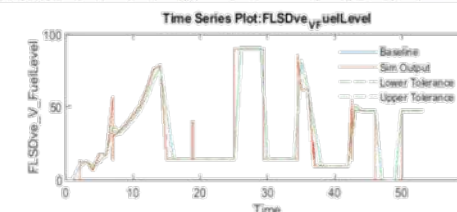
- Контроль и экспертиза разработки SW по ISO 26262
- Собственная разработка OEM/OES по ISO 26262 в части SW
- Уточнение механизмов безопасности
- Разработка концепции мониторинга SW/HW
- Тестирование SW



- оценка максимального градиента в зависимостях управления крутящим моментом
- оценка значения $(M2 - M1)/(t2 - t1)$ (с коэффициентом запаса)
- разработка/изменение SW для INC

FLSDve_V_FuelLevel	0	0	0	0	75.8	double	Continuous	T_V,1,65535,100	0,038	Triggered	linear union	Link
FLSDve_S_FuelLevelWarming	0	0	0	0	1	double	Continuous	T_BOOLEAN		Triggered	linear union	Link

Name	Abn	Rel	T	Lead	Lag	Max Diff	Data Type	Units	Sample Time	Data Type 2	Units	Sample Time	Interp	Sync
FLSDve_V_FuelLevel	0	0	0	0	75.8	double	Continuous	T_V,1,65535,100	0,038	Triggered	linear union			

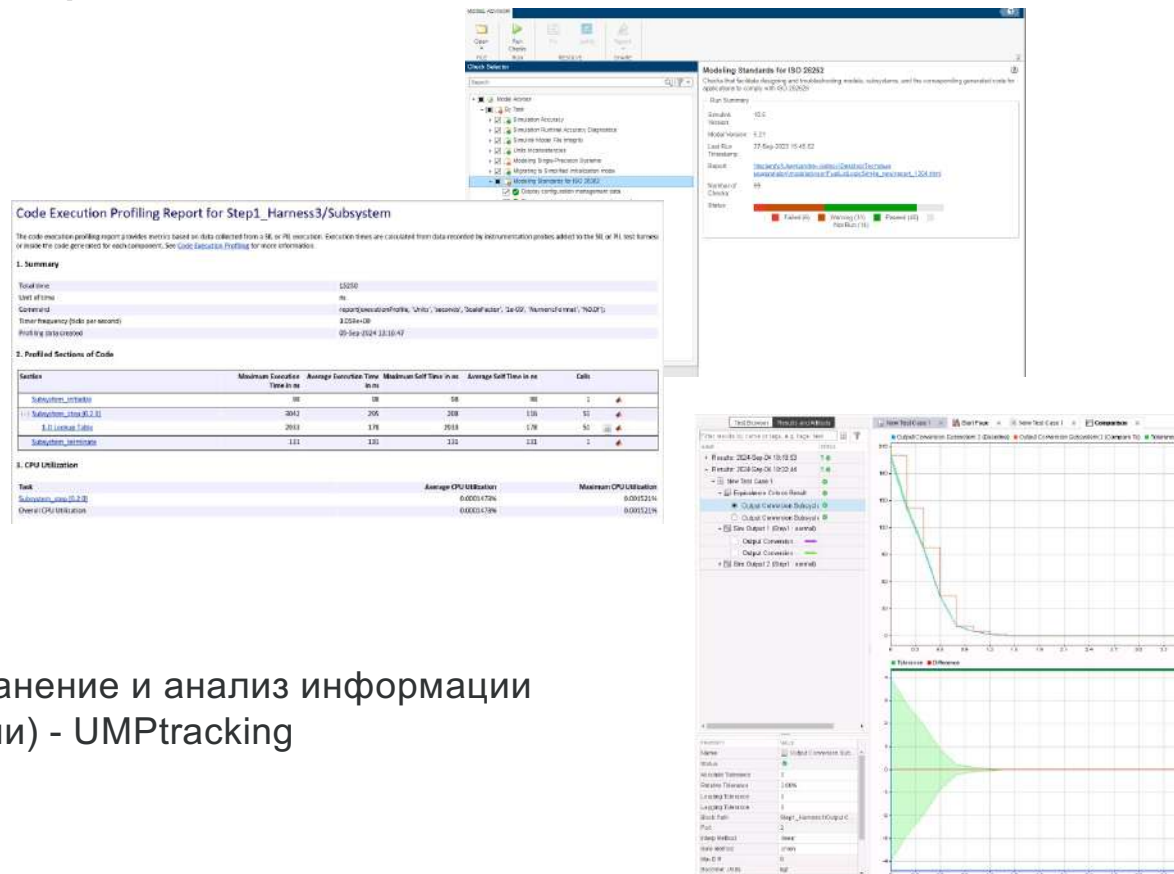


Функциональная безопасность в проектах

-НАМИ-

Тестирование и поддерживающие процессы SW

- Инспекция
- Тестирование по требованиям
- Анализ покрытия требованиями
- Статический анализ кода
- B2B comparison
- Scheduling анализ
- Управление требованиями и кодом (GitLab, Simulink Requirements)
- Система управления прошивками (сбор, хранение и анализ информации о версиях ПО, ЭБУ на сборке и эксплуатации) - UMPtracking



Менеджмент функциональной безопасности

-НАМИ-

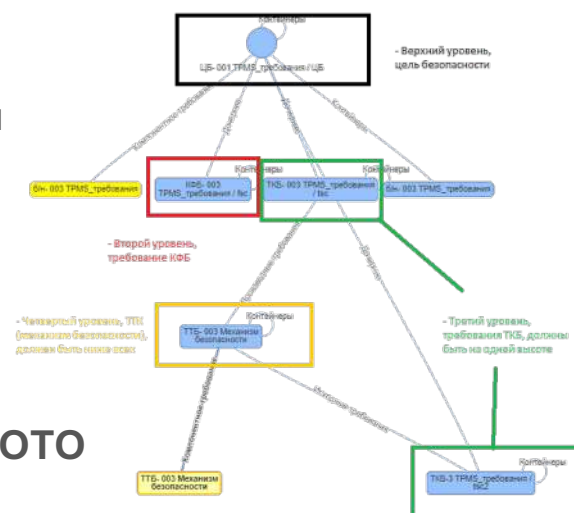
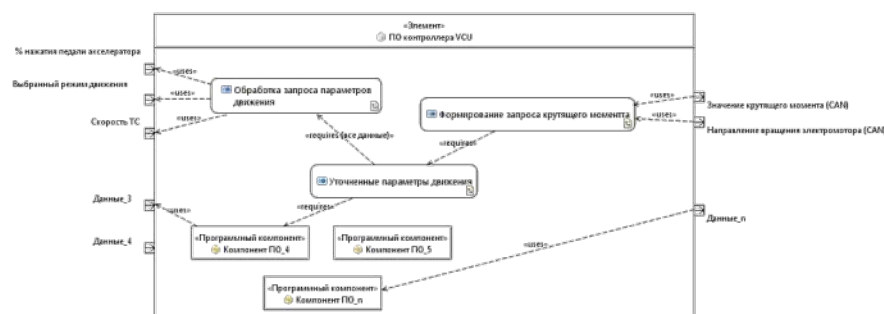
Управление требованиями/продуктом

- DevProm (разработан шаблон процесса разработки по ISO 26262 в DevProm), Polarion, GitLab

Анализ ФБ и трассировка ЦБ/требований

- Ansys medini Analyze

Все требования/артефакты анализа ФБ в AURUS MOTO полностью перенесены в DevProm



ЦБ
КФБ
ТКБ
ТТБ

КФБ-10-20502 [Передача данных о давлении 2] [MF018] Данные о давлении не передаются

КФБ-10 В работе

В

Производные требования: [КФБ-10-20563] В работе Требования концепции безопасности для системы мониторинга давления в шинах (код 10) / ОБНАРУЖИТЬ/ПРЕДОТВРАТИТЬ: [Комбинированный датчик давления и температуры 2] Out of range
[КФБ-10-20570] В работе Требования концепции безопасности для системы мониторинга давления в шинах (код 10) / ОБНАРУЖИТЬ/ПРЕДОТВРАТИТЬ: [Комбинированный датчик давления и температуры 2] Null

Менеджмент функциональной безопасности

-НАМИ-

Специальные правила и процедуры в части ФБ

- МУ 37.031.090-2023 «Общее руководство по выполнению анализа функциональной безопасности (ISO 26262) на функциональном, техническом, аппаратном и программном уровне изделия/системы»
- МУ 37.031.064–2023 «Рекомендации по проектированию аппаратной части электрических и электронных изделий с учетом положений серии стандартов ISO 26262»
- Р 37.031.091–2024 «Порядок разработки концепции функциональной безопасности электрических и электронных систем»
- Р 37.031.092–2024 «Функциональная безопасность. Порядок разработки концепции технической безопасности устройства»



Культура безопасности

-НАМИ-

- Научно-практический семинар по применению ISO 26262 для сотрудников ФГУП НАМИ (присутствовало около 100 профильных специалистов)
- Учебный курс в аспирантуре ФГУП НАМИ (с контролем полученных знаний). Проводится раз в год на постоянной основе
- Практика в части ФБ и последующее трудоустройство молодых специалистов технических ВУЗов – на постоянной основе
- Подготовка отзывов на стандарты (1 ред. ГОСТ Р ИСО 21448, 1 ред. ГОСТ «Требования к плану обеспечения безопасности» (Автонет))
- Выступления на научно-практических конференциях (МАНФ, ААИ, ММФБ) – на постоянной основе
- Программа ДПО по функциональной безопасности: обучение и выдача дипломов государственного образца

Материально - техническая база

-НАМИ-

ISO 26262 требует тщательного тестирования устройства на разных стадиях разработки

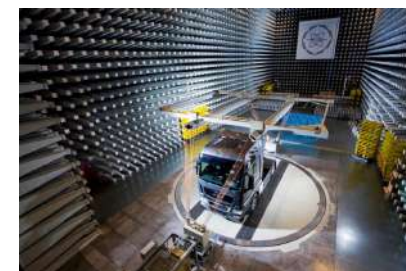
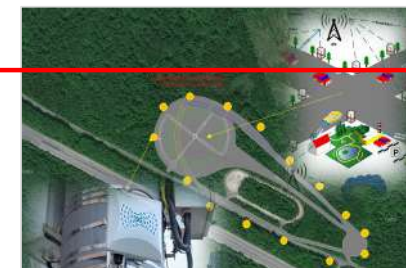
Программно-аппаратный уровень и уровень системы



Уровень транспортного средства



В перспективе



Выводы и перспективы

-НАМИ-

Применение положений ISO 26262 значительно повышает безопасность электрических и электронных систем ТС

Необходимо внедрять инструменты добровольной сертификации в автомобильной промышленности

Актуально участие организаций автомобильной промышленности в работе ТК 58

Актуальным является импортозамещение в области ПО для анализа безопасности, а также инструментов разработки и тестирования прикладного ПО

Импортозамещение и инструменты квалификации для микросхем и микроконтроллеров для соответствия положениям ГОСТ Р ИСО 26262 – наиболее актуальная из задач для повышения безопасности электрических и электронных систем ТС

-НАМИ-

Петр Рогов, к.т.н., начальник сектора ФБ ПО ФГУП НАМИ

+7-987-559-64-43

petr.rogov@nami.ru

**СПАСИБО
ЗА ВНИМАНИЕ**

nami.ru