Второй Межотраслевой форум «Функциональная безопасность»

ЭКВАРТА
инженерная компания

Тема доклада: «Особенности проведения анализа опасностей и оценки рисков в автомобильной отрасли»

Леонид Долгов
Руководитель автомобильного направления

Москва, 09 октября 2025 года

ЭКВАРТА
инженерная компания

Виды деятельности в автомобильном направлении

- Сопровождение разработки E/E систем, включая ADAS
- Анализ безопасности E/E систем с использованием методов HARA, TARA, FTA, FME(D)A и др.
- Разработка требований и концепций безопасности
- Разработка комплекта документов по ГОСТ Р ИСО 26262
- Обучение специалистов по процессам и методам функциональной безопасности
- Постановка процессов обеспечения функциональной безопасности

E/E – электронные и/или электрические системы

Для чего нужно проводить анализ опасностей и оценку рисков?

Потребительские свойства

Эксплуатация на дорогах общего пользования

Отсутствие неоправданного риска

Опасности

[Toyota Slow to See Scope of Problem Even After Fatal Crash - The New York Times]

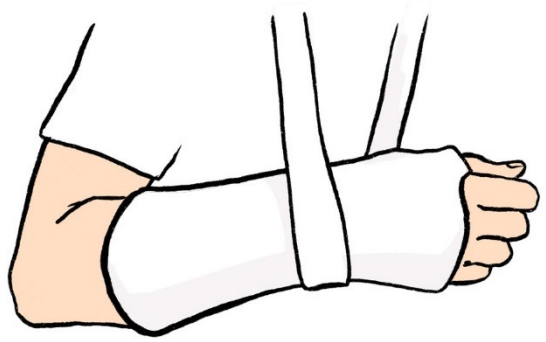
В чем заключается анализ опасностей и оценка рисков?

Некорректное функционирование
неисправного устройства

Уровень полноты безопасности транспортного средства, цели безопасности

Эксплуатационная ситуация

Управляемость



Тяжесть вреда

Идентификация источников опасностей

Определять опасности систематически

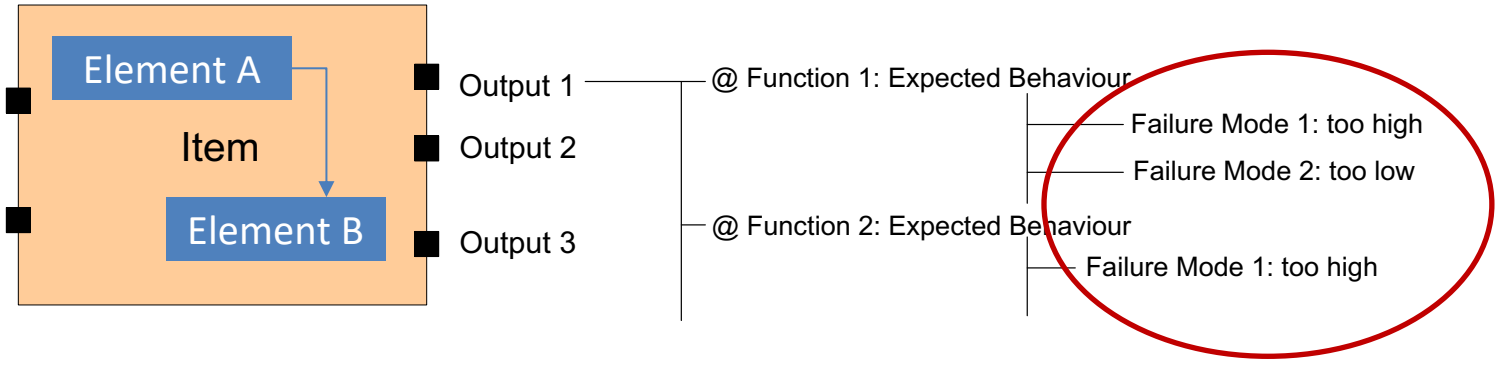
Применять мозговой штурм

Учитывать известные отказы и опасности

Индуктивные методы

Интерфейсно-ориентированные методы

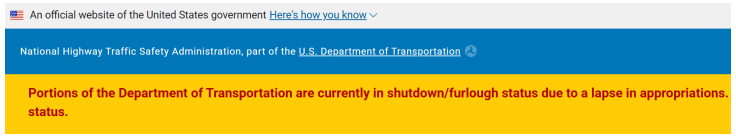
Стандарты, Правила, Технические отчеты и др.



UNECE

NHTSA

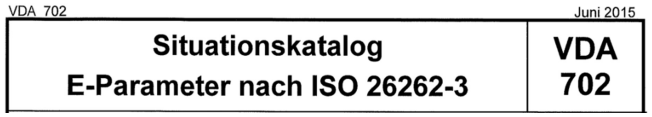
ISO



Потенциальные источники опасностей

Пример ADAS: ~50 потенциальных отказов при использовании комбинации методов

Выбор эксплуатационных ситуаций


VDA 702 Juni 2015

Situationskatalog E-Parameter nach ISO 26262-3	VDA 702

Напр.: маневрирование на высокой скорости…

Ситуации наибольшего вреда → Опасные события с высоким уровнем тяжести вреда (S-параметр)

Напр.: городской трафик, движение на перекрестках…

Наиболее частые ситуации → Опасные события с высоким уровнем вероятности воздействия (E-параметр)

Напр.: ДТП, неисправность транспортного средства

Особые ситуации → Опасные события, во многом определяющие полноту анализа

Пример ADAS: ~50 ситуаций в результате комбинирования факторов и рассмотрения особых ситуаций

ЭКВАРТА
инженерная компания

Классификация опасных событий

Тяжесть последствий

Collision Type	*Range For*	S0	S1	S2	S3
Front	Minimum speed		> 4-10 kph and	> 20-50 kph and	> 40-65 kph
	Maximum speed	< 4-10 kph*	< 20-50 kph	<= 40-65 kph	
Back	Minimum speed		> 4-10 kph and	> 20-50 kph and	> 40-60 kph
	Maximum speed	< 4-10 kph*	< 20-50 kph	<= 40-60 kph	
Side	Minimum speed		> 2-10 kph and	>= 8-30 kph and	>16-40 kph
	Maximum speed	< 2-3 kph*	< 8-30 kph	<16-40 kph	

Управляемость

Оценка способности избежать вреда водителем или другими лицами, находящимися в потенциально опасной ситуации

Можем ли рассчитывать на внешние меры?

SAE INTERNATIONAL

SURFACE VEHICLE RECOMMENDED PRACTICE	J2980™	APR2018
	Issued 2015-05 Revised 2018-04 Superseding J2980 MAY2015	
(R) Considerations for ISO 26262 ASIL Hazard Classification		

Пример ADAS: ~25 опасностей неправильного функционирования

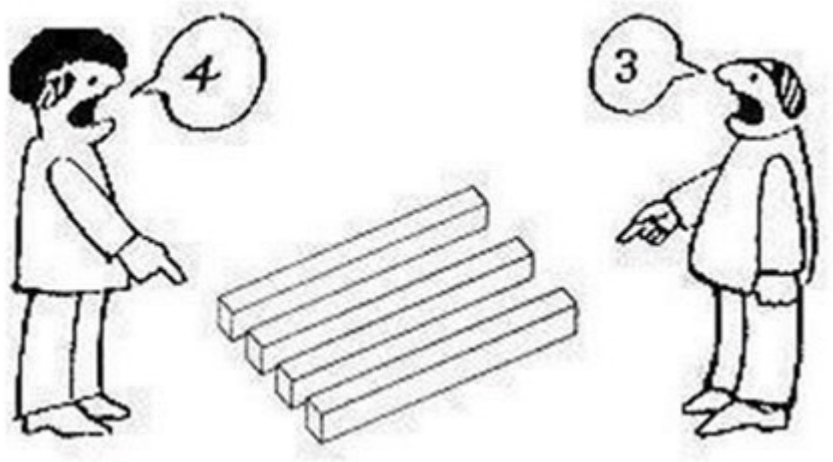
Цели безопасности

Пример ADAS: ~20 целей безопасностей

Коллективная работа

Как поступить, если мнения расходятся:

- Сравнивать аргументы, а не ощущения
- Избегать необоснованных авторитетных утверждений
- Использовать все доступные источники информации
- При прочих равных условиях придерживаться консервативной оценки



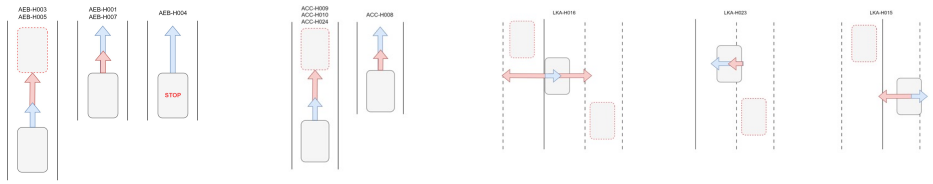
*В ISO 26262-3 требуется проверить полноту HARA. Однако **стандартом не приводятся критерии** того, что считается действительным аргументом в пользу полноты.*
*Один из методов доказательства полноты HARA состоит в том, чтобы оспорить его, пытаясь сформулировать **больше опасных событий**.*
*Если мы **не можем сформулировать какое-либо новое** опасное событие, еще не охваченное списком целей безопасности, мы можем сделать вывод, что **выполнили анализ HARA**.*

Пример ADAS: N часов обсуждений, протоколы согласования

Проверка HARA

Верификация HARA

Обеспечить подтверждение полноты, соответствия и согласованности



ID	Requirement	Scope Ri	Checked	Checker's Comment	Agreeded
6	HARA				
6.1	Цели				
6.1a	Цель выявить и классифицировать опасные события, вызванные некорректным функционированием неисправного устройства определена	must	agreed		agreed
6.1b	Цель сформулировать цели безопасности с соответствующими значениями УПБТС, связанными с предотвращением или ослаблением последствий опасных событий, во избежание необоснованного риска определена	must	agreed		agreed
6.2	Общие положения				
6.3	Входная информация				
6.3.1	Определение устройства определено, как входная информация, используется	must	agreed		agreed
6.3.2	Информация о других устройствах представлена	optional		Результаты HARA для других устройств отсутствуют, следовательно, не должны учитываться в текущем анализе	
6.4	Требования и рекомендации				
6.4.1	6.4.1 Запуск процедуры анализа опасностей и оценки рисков				
6.4.1.1	6.4.1.1 Анализ опасностей и оценка рисков должны быть основаны на определении устройства.	must	agreed		agreed
6.4.1.2	6.4.1.2 Анализ опасностей и оценка рисков устройства должны выполняться без его внутренних механизмов безопасности, то есть при анализе опасностей и оценке рисков не должны рассматриваться механизмы безопасности, предназначенные для реализации или которые уже были реализованы в предшествующих устройствах.	must	agreed		agreed
6.4.2	6.4.2 Анализ ситуации и идентификация опасности				
6.4.2.1	6.4.2.1 Должны быть описаны эксплуатационные ситуации и режимы работы, в которых некорректное функционирование устройства приводит к опасному событию как в случаях регламентированного использования транспортного средства, так и в случаях предсказуемо неправильного использования.	must	agreed		agreed

Обосновать выбор эксплуатационных ситуаций и опасных событий, правильность определения значений ASIL

Оценка подтверждения

Уровень независимости – I3 (от QM до ASIL D)

Мера подтверждения должна быть выполнена лицом, независимым от отдела, отвечающего за рассматриваемые результаты работы, от организации их выполнения, используемых ресурсов и определения полномочий

ЭКВАРТА
инженерная компания

@FACETOSAFE

Контакты:

Леонид Долгов

Руководитель автомобильного направления

+7(926)009-05-79

dolgov@ekvartagroup.ru

+7(495)222-4761

Спасибо за внимание!