ТРЕТИЙ РОССИЙСКИЙ ФОРУМ

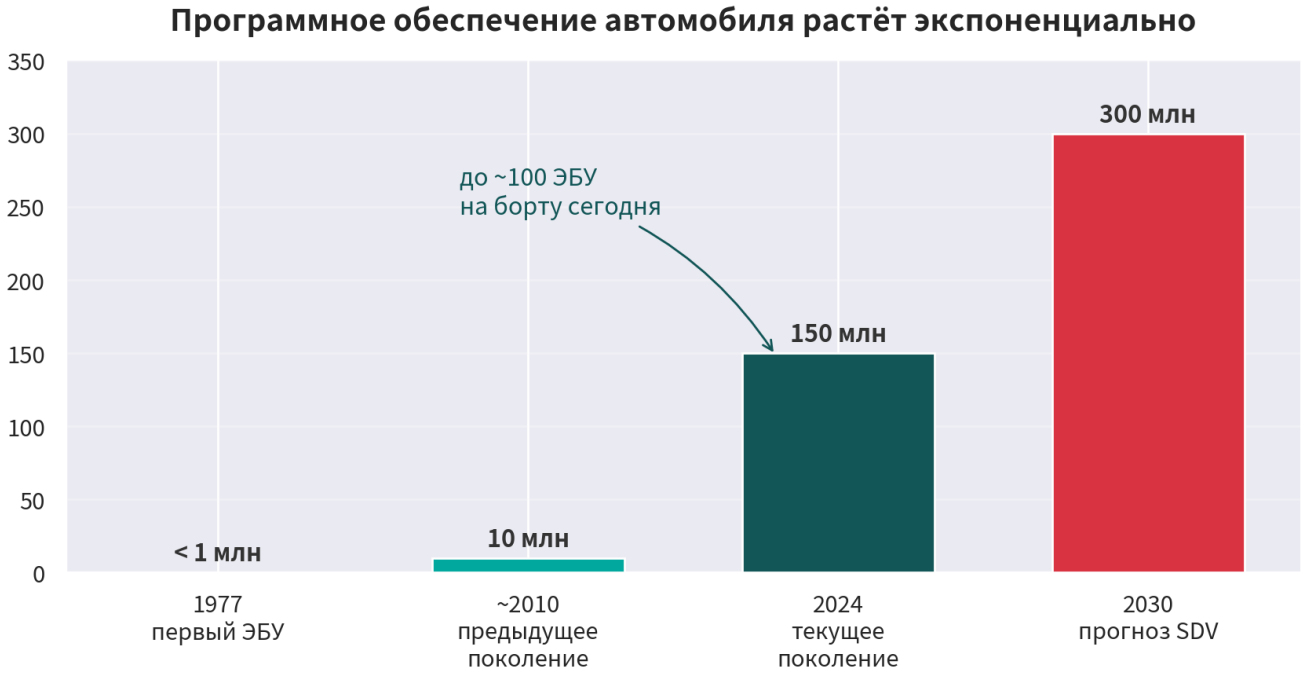
«БЕЗОПАСНОСТЬ транспортных средств»

Модельно-ориентированная оценка безопасности транспортных систем: архитектурная модель как ответ на рост сложности и изменение требований к разработке и эксплуатации

Дмитрий Пасынков
ГК «ПЛМ Урал»

ВЫЗОВ · СЛОЖНОСТЬ ИЗДЕЛИЙ

Транспортные системы стремительно меняются



≈100 ЭБУ

электронных блоков управления в современном автомобиле

150 млн строк

бортового программного кода — уже сегодня

300 млн строк

прогноз объёма бортового ПО к 2030 году

>1 ТБ в сутки

данных генерирует один подключённый автомобиль

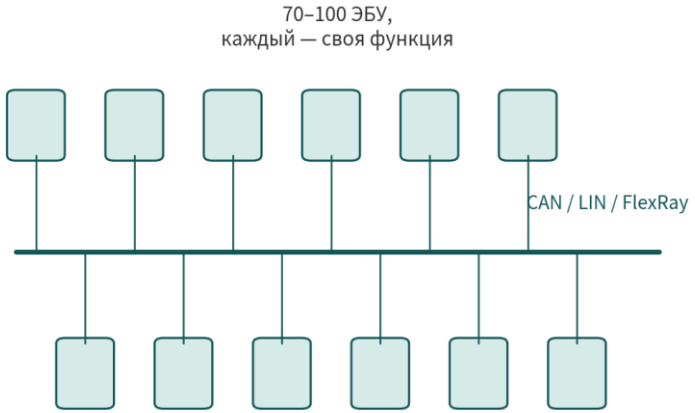
Свыше 80 % инноваций в автомобилестроении реализуются программно-интенсивными системами

Источники: отраслевые оценки (McKinsey, IEEE, BCG)

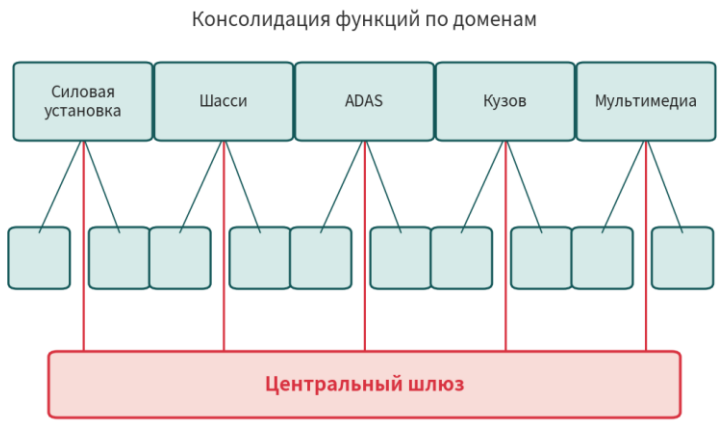
ВЫЗОВ · АРХИТЕКТУРА ИЗДЕЛИЙ

Эволюция E/E-архитектур: всё более распределённые и программно-определяемые

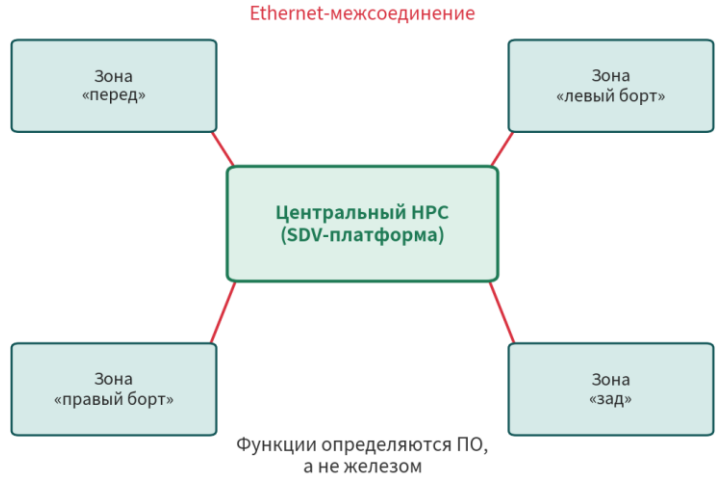
Распределённая (классическая)



Доменная



Зональная + HPC (SDV)



Авиация — интегрированная модульная авионика (IMA); ЖД и морской транспорт — распределённые системы управления; БПЛА — бортовые сети реального времени

ПРОБЛЕМАТИКА · ИСХОДНЫЕ ДАННЫЕ

Что получает специалист по безопасности

W Техническое задание	W Технические условия (покупные/готовые изделия)	W Пояснительная записка	V P Структурная схема	V P Функциональная схема
CAD Электрические схемы	X Ведомость покупных	W Руководство по эксплуатации	W Программа и методика испытаний (в части безопасности)	V P X CAD .....

Разные подразделения. Разные форматы. Разные сроки выпуска. Ни одной формальной связи между ними.

Пять проблем документо-центричного подхода



1 **Ориентир на работу с документами**

Носителем инженерного знания является документ, а не данные; перенос в модель для анализа — вручную, и повторить его невозможно; каждый интерпретирует по своему

2 **Отсутствие единого источника данных**

Единого источника данных нет: один и тот же элемент в трёх документах назван по-разному; когда в проекте происходит изменение — а оно происходит постоянно — обновляется часть документов, но не все

3 **Нет границ и сценариев**

Что является объектом оценки, где проходит его граница, с чем он взаимодействует и т.д.; ответы либо отсутствуют, либо разбросаны по разделам, либо существуют только в голове ведущего конструктора

4 **Неоднозначность языка**

Естественный язык допускает множественное толкование; типичная формулировка: «При отказе основного канала управление передаётся резервному» — при каком отказе? за какое время? и т.д.

5 **Отсутствие трассируемости**

При изменении никто не может ответить на вопрос: какие требования безопасности и какие доказательства затронуты; ответ получают экспертно — а значит, с пропусками, и пропуски эти системные, а не случайные

К чему это приводит при оценке безопасности

Поиск данных, а не оценка

Оценка безопасности превращается в реконструкцию замысла разработчика по косвенным признакам: значительная доля трудозатрат уходит не на оценку, а на сбор и сверку исходных данных

Невоспроизводимость

Результаты невоспроизводимы: повторить рассуждение по документам нельзя, можно только поверить автору

Позднее обнаружение

Оценка выполняется поздно, когда архитектура уже заморожена, поэтому она не влияет на конструкцию, а лишь констатирует её; из проектного инструмента оценка безопасности вырождается в приёмочную процедуру

Высокая цена изменений

Границы изменения не видны:

- либо перестраховываемся и переделываем оценку целиком,
- либо недооцениваем влияние, пропускаем анализ — и получаем срыв сроков и бюджета

И главное: оценка безопасности оторвана от реального изделия — она опирается на разрозненный набор документов и её полнота ничем не гарантирована

Тезис доклада

Методы анализа

FMEA, FTA, HAZOP, марковские модели — совершенствуются десятилетиями

Исходные данные

Готовятся так же, как тридцать лет назад: разрозненный набор документов

Сложность транспортных систем

Выросла многократно: ~100 ЭБУ, 150 млн строк кода, распределённые E/E-архитектуры — и продолжает расти

> **Качество оценки безопасности определяется не методом анализа, а качеством описания объекта**
> **Документо-центричный подход к исходным данным исчерпал себя — единым источником данных должна стать архитектурная модель (MBSE/MBSA)**

MBSE (Model-Based Systems Engineering) — модельно-ориентированная системная инженерия. Подход, при котором модели являются основным артефактом на всех этапах жизненного цикла системы.

MBSA (Model-Based Safety Assessment) — модельно-ориентированная оценка безопасности. Подход, при котором оценка безопасности (FMEA, FTA, и т.д.) выполняется на основе системных моделей, созданных в рамках MBSE.

ПРОБЛЕМАТИКА · ПОЧЕМУ АНАЛИЗ НУЖЕН НА РАННИХ ЭТАПАХ

Ошибку, заложенную в архитектуру, нельзя «соскрести» на поздних стадиях

Неверная архитектура



Верное решение заложено сразу



Дорого

Стоимость исправления ошибки растёт от 1× на фазе требований до 21–78× на испытаниях и 29–1500× в эксплуатации (NASA JSC)

Неэффективно

Если неверное решение было заложено в архитектуру, то на поздних стадиях его последствия не всегда удаётся полностью компенсировать: «соскрести подгоревшее» можно, но это уже будет компромисс, а не задуманный результат

Безопасность должна закладываться в архитектуру и проверяться на ранних этапах — там, где ошибки рождаются и где их исправление наименее затратно



АРХИТЕКТУРА · ОПРЕДЕЛЕНИЕ

Архитектура — это данные, а не рисунок

Архитектура (системы) — основные понятия или свойства системы в окружающей среде, воплощенной в ее элементах, отношениях и конкретных принципах ее проекта и развития

ЭЛЕМЕНТЫ	ОТНОШЕНИЯ	ОКРУЖЕНИЕ	ПРИНЦИПЫ

Не картинка и не отдельный документ, а структурированный набор данных об изделии: элементы, связи, функции, потоки, границы, состояния и режимы

Архитектура (системы) - это обо всем важном. Что бы это ни было

Ральф Джонсон

ISO/IEC/IEEE 42010:2022 «Software, systems and enterprise — Architecture description»; в РФ — ГОСТ Р 57100-2016

АРХИТЕКТУРА · НОРМАТИВНАЯ БАЗА

Архитектура уже требуется нормативно — во всех отраслях

Системная инженерия

ISO/IEC/IEEE 15288 — определение архитектуры как процесс ЖЦ;
ISO/IEC/IEEE 42010 — архитектурное описание, закрепляет архитектуру как данные;
IEC 61508 — вводит архитектурные ограничения SIL.
РФ: ГОСТ Р 57193, ГОСТ Р 57100, ГОСТ Р МЭК 61508

Модели: не напрямую — архитектура как данные

Автомобилестроение

ISO 26262 — архитектура на каждом уровне: декомпозиция ASIL, анализ зависимых отказов, FMEDA;
ISO 21448 (SOTIF); ISO/SAE 21434 + ЕЭК ООН № 155/156 — кибербезопасность как условие допуска

Модели: частично — нотации допускаются

Automotive SPICE 4.0 (2023)

Архитектурные процессы в каждом домене: SYS.3, SWE.2, HWE.2, MLE.2; «information items» вместо «work products» — данные в инструменте, а не документ; двунаправленная прослеживаемость обязательна

Модели: не напрямую — но шаг к модельным данным

Железная дорога

EN 50129: отчёт по безопасности обязан содержать описание архитектуры.
EN 50126 / 50128 / 50129 / 50657 — ЖЦ RAMS и доказательство безопасности;
РФ: ГОСТ 33432-2015, ГОСТ 33433-2015, ТР ТС 001–003/2011

Модели: явных требований нет

Авиация — отраслевой ориентир

ARP4754A/B и ARP4761/4761A: FHA — до определения архитектуры, PSSA — инструмент её выбора, SSA — подтверждение реализованной архитектуры

Модели: прямо — ARP4761A ввёл MBSA

Что это значит

От «допускаются» до «формального метода» — стандарты всё увереннее говорят о моделях. Архитектура обязательна везде; разница лишь в том, насколько формально она описана.

Вопрос не «нужна ли архитектура», а в чём она живёт: модель — или россыпь документов

О КОМПАНИИ И ПРОДУКТАХ

ГК «ПЛМ Урал»: инструменты модельно-ориентированной разработки и оценки безопасности

Группа компаний «ПЛМ Урал» разрабатывает и внедряет отечественное ПО для системной инженерии, основанной на моделях (MBSE), и модельно-ориентированной оценки безопасности (MBSA). Помогаем предприятиям переходить от документо-центричной разработки к модельно-ориентированному проектированию: инженерия требований, архитектурное проектирование, верификация и валидация — поставка, внедрение, обучение и поддержка.

ПО «АрхиП»

Архитектурное проектирование сложных систем по методу Arcadia (ГОСТ Р 57193-2025) — от анализа применения до физических компонентов

- Полная поддержка Arcadia: все уровни абстракции
- Функции, взаимодействия, режимы и состояния
- Прослеживаемость: изделие → системы → компоненты
- Проверка модели на согласованность, анализ влияния изменений
- Методологическое руководство внутри инструмента

ПО «АрхиП: Команда»

Совместная работа группы проектировщиков над единой системной моделью без конфликтов

- Одновременная работа над единой моделью
- Блокировка редактируемого элемента и его связей
- Мгновенная синхронизация изменений у всей команды
- История правок и сравнение версий
- Разграничение прав, защищённое хранилище моделей

ЛОЦМАН:PLM Архитектурное проектирование

Для предприятий на экосистеме АСКОН — инструмент архитектурного проектирования, встроенный в PLM-среду

- Интеграция в общую PLM-среду ЛОЦМАН:PLM
- Трассировка требований из ЛОЦМАН:PLM на объекты архитектурного описания
- Хранение архитектуры в виде объектов ЛОЦМАН:PLM

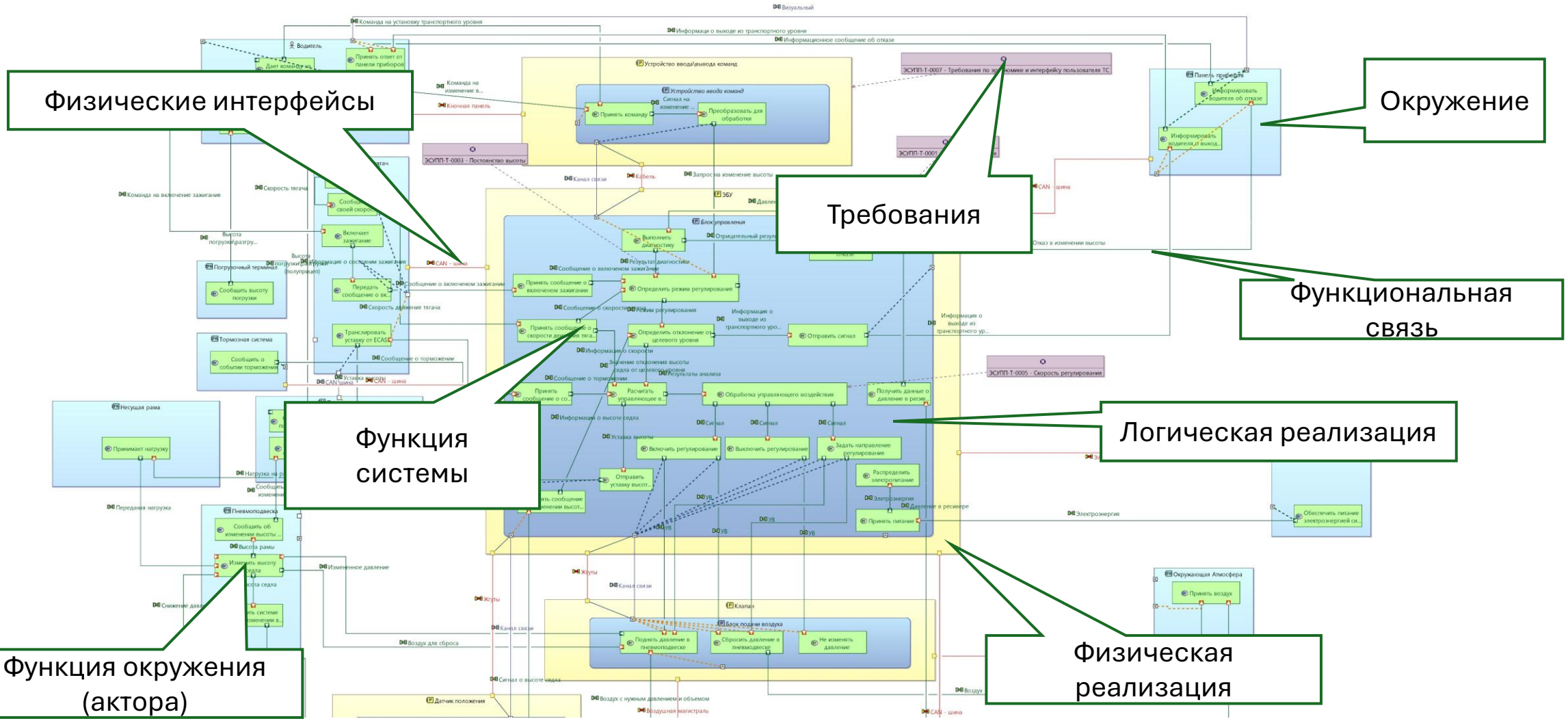
Модуль оценки безопасности

MBSA

- Расширение ПО «АрхиП»: оценка функциональных опасностей (FHA) прямо на архитектурной модели
- Сквозная прослеживаемость: требование → функция → отказ → последствие; уровни DAL
- Практический опыт внедрения в авиационной отрасли

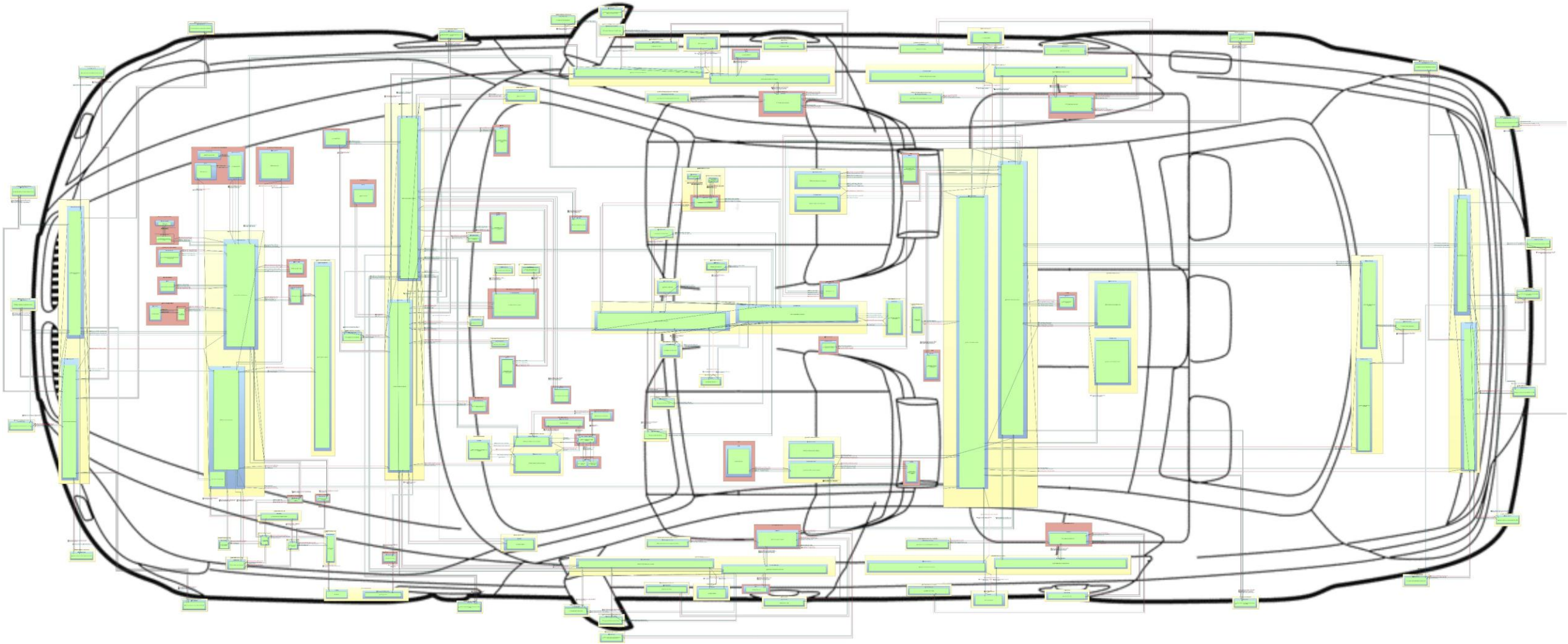
ПРИМЕР · АРХИТЕКТУРНАЯ ДИАГРАММА ВЫПОЛНЕНАЯ В ПО «АРХИП»

Пример архитектурной диаграммы для СУПП



ПРИМЕР · АРХИТЕКТУРНАЯ ДИАГРАММА ВЫПОЛНЕНАЯ В ПО «АРХИП»

Упрощенная Архитектурная диаграмма E/E



ОТ MBSE К MBSA

MBSA: единый контур оценки безопасности на базе архитектурной модели

1. Модель отказов

Архитектурная модель дополняется режимами отказов и правилами распространения ошибок

2. Формальный язык

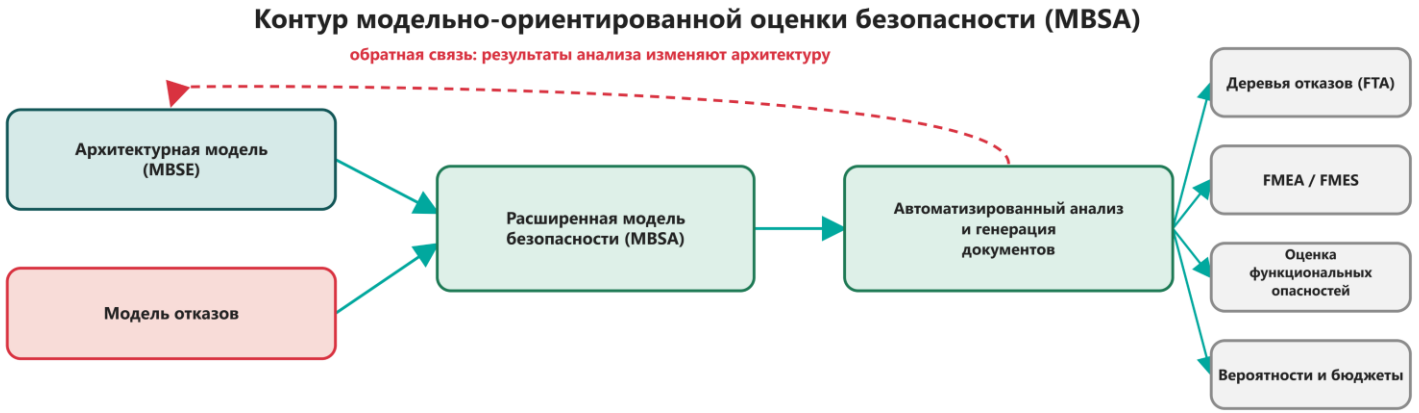
Модель безопасности описывается однозначно и машиночитаемо

3. Автоматизированный анализ

Инструмент генерирует FTA, FMEA, вероятностные оценки

4. Ранний анализ

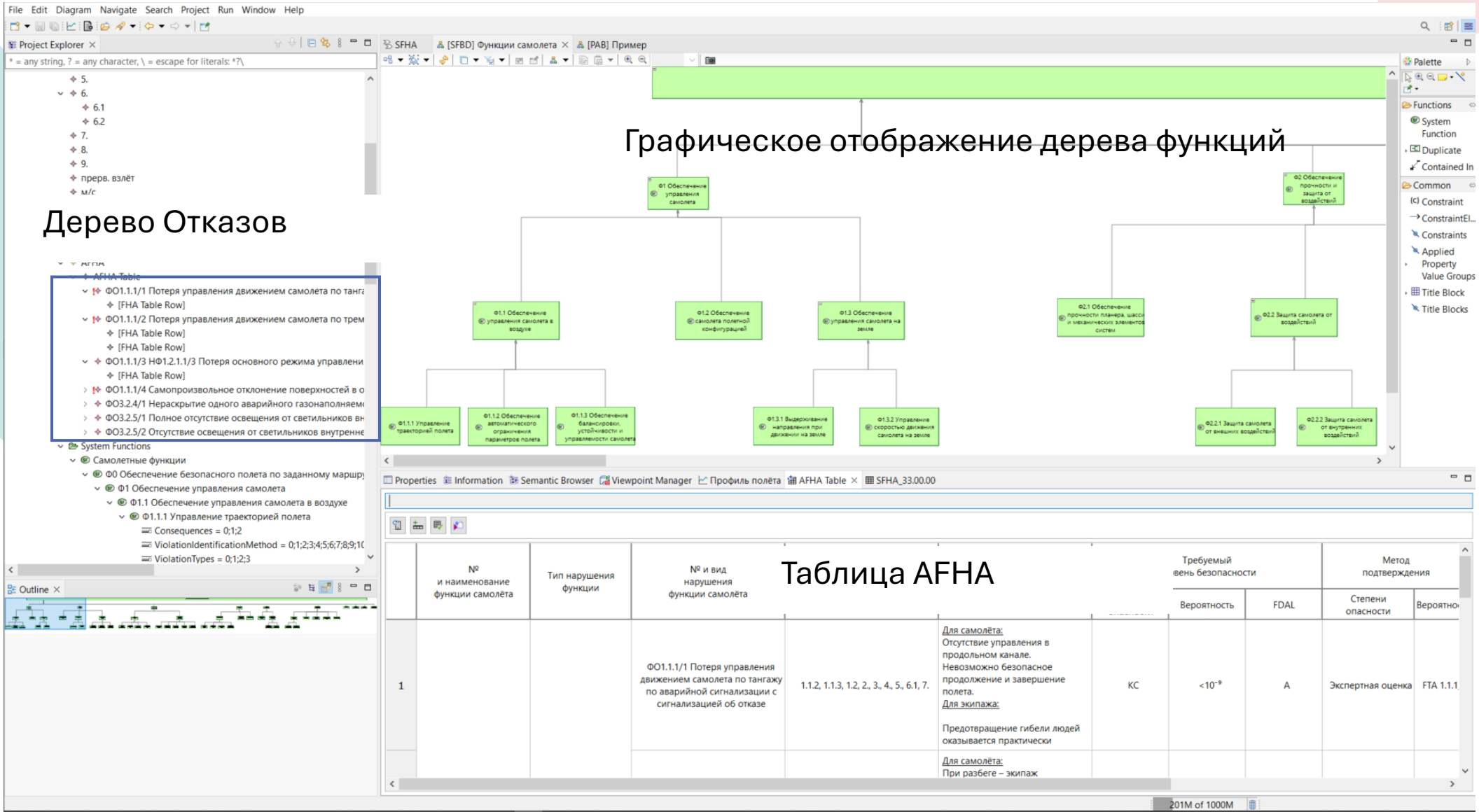
Проверка архитектуры на соответствие целям безопасности — до затрат на реализацию



Только архитектурные модели позволяют выполнять строгую оценку безопасности на самых ранних этапах — когда изменения ещё дёшевы

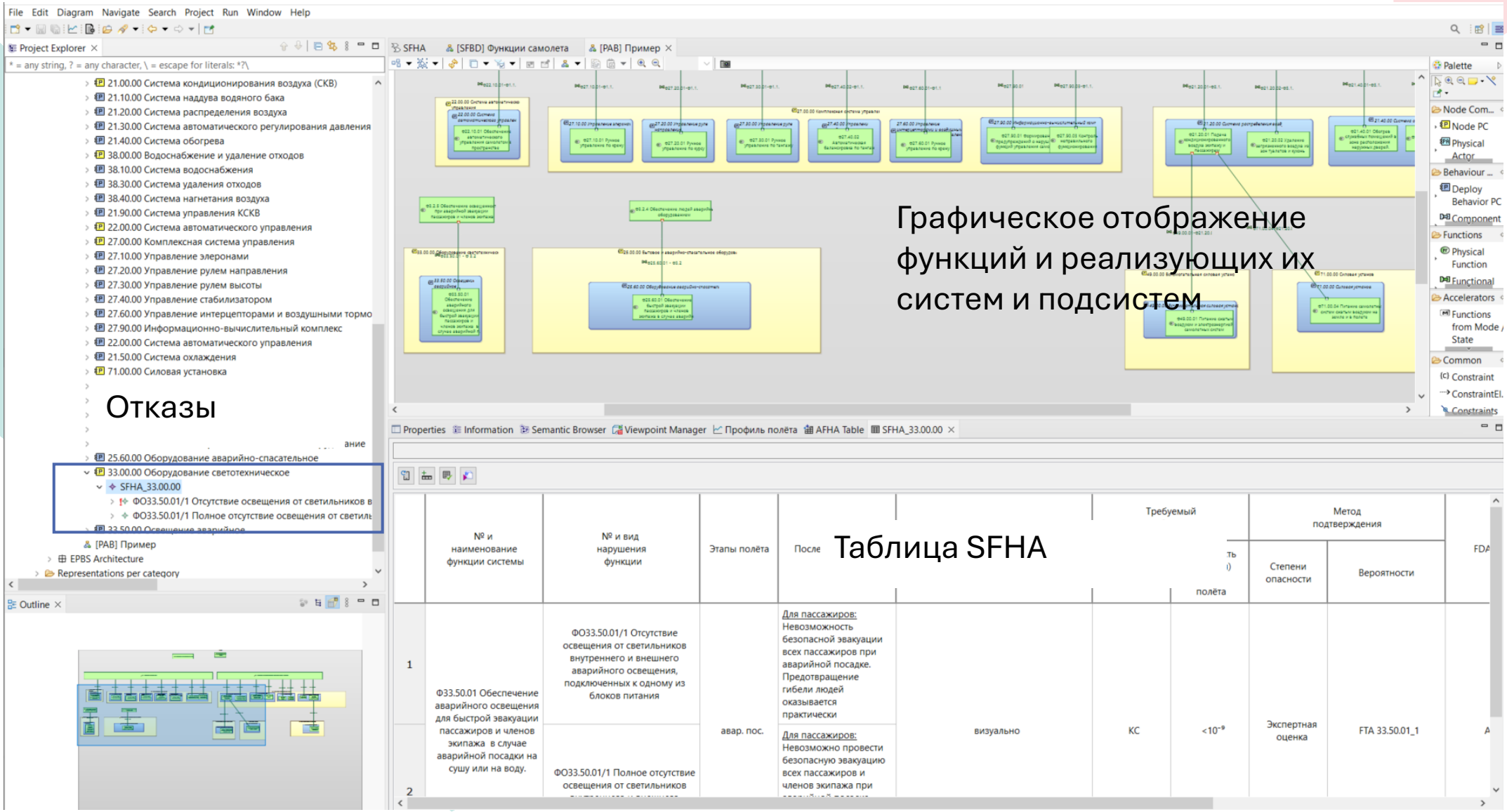
ПРИМЕР · ТАБЛИЦА AFHA ПРЕДСТАВЛЕННАЯ В ИНТЕРФЕЙСЕ ПО «АРХИП» (АВИАЦИЯ)

Оценка функциональных опасностей (Авиация)



ПРИМЕР · ТАБЛИЦА SFHA ПРЕДСТАВЛЕННАЯ В ИНТЕРФЕЙСЕ ПО «АРХИП» (АВИАЦИЯ)

Оценка функциональных опасностей (Авиация)



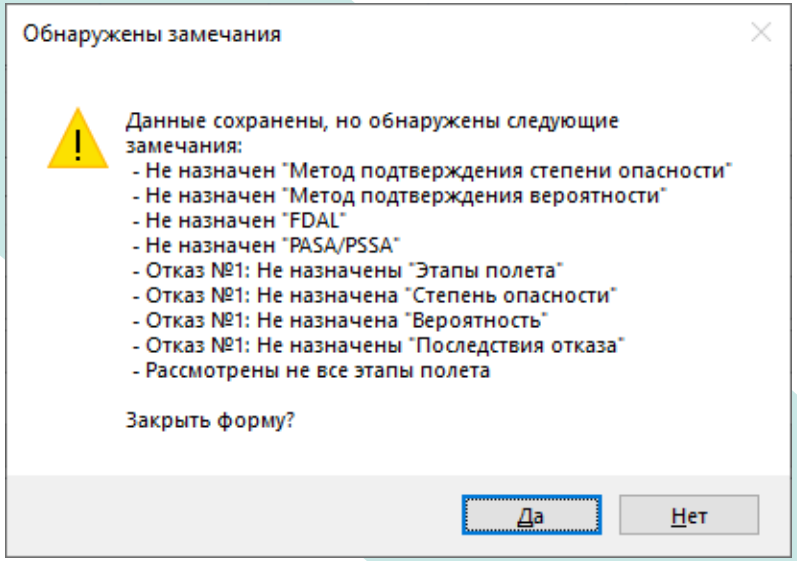
	№ и наименование функции системы	№ и вид нарушения функции	Этапы полёта	После		Требуемый		Метод подтверждения		FDA
							полёта	Степени опасности	Вероятности	
1	Ф33.50.01 Обеспечение аварийного освещения для быстрой эвакуации пассажиров и членов экипажа в случае аварийной посадки на сушу или на воду.	ФО33.50.01/1 Отсутствие освещения от светильников внутреннего и внешнего аварийного освещения, подключенных к одному из блоков питания	авар. пос.	Для пассажиров: Невозможность безопасной эвакуации всех пассажиров при аварийной посадке. Предотвращение гибели людей оказывается практически	визуально	КС	$<10^{-9}$	Экспертная оценка	FTA 33.50.01_1	A
2		ФО33.50.01/1 Полное отсутствие освещения от светильников		Для пассажиров: Невозможно провести безопасную эвакуацию всех пассажиров и членов экипажа при						

ПРИМЕР · ПРЕДУПРЕЖДАЮЩИЕ ОКНА В ПО «АРХИП» (АВИАЦИЯ)

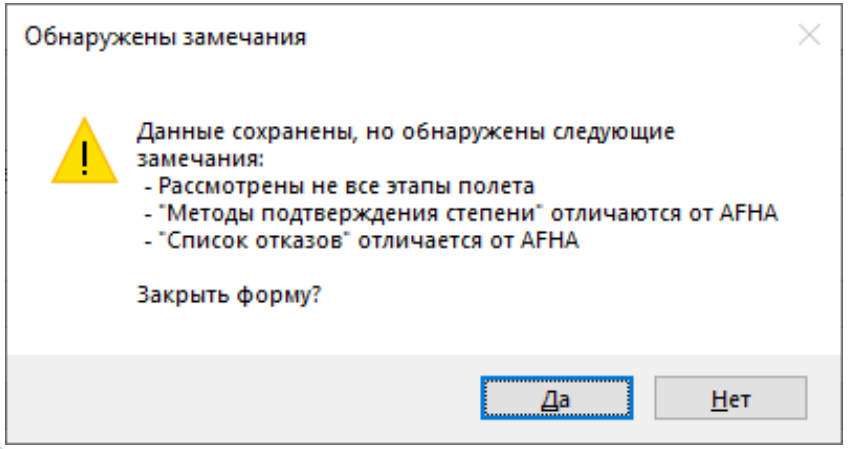
Оценка функциональных опасностей (Авиация)

Примеры проверок, которые защищают пользователя от ввода неверных данных

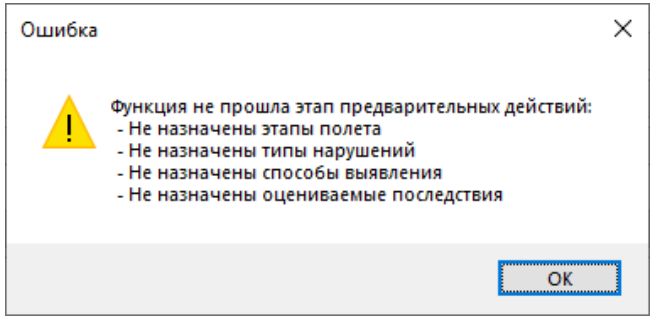
Проверка заполнения обязательных полей отказного состояния.



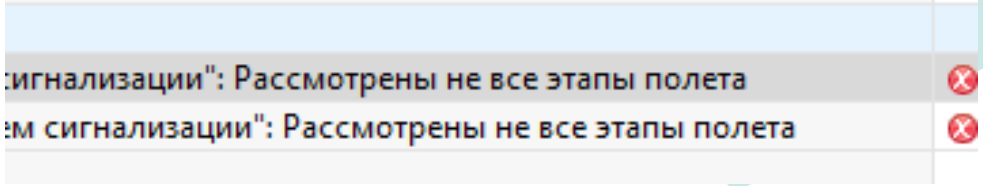
При рассинхронизации данных в AFHA и SFHA таблицах



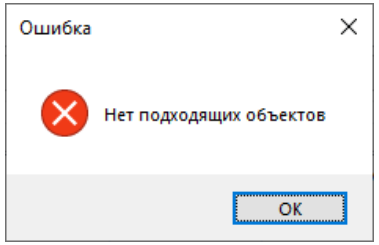
При выборе функции, для которой не в полном объёме выполнены предварительные действия



Пропущены обязательные шаги AFHA/SFHA-анализа (валидация модели)

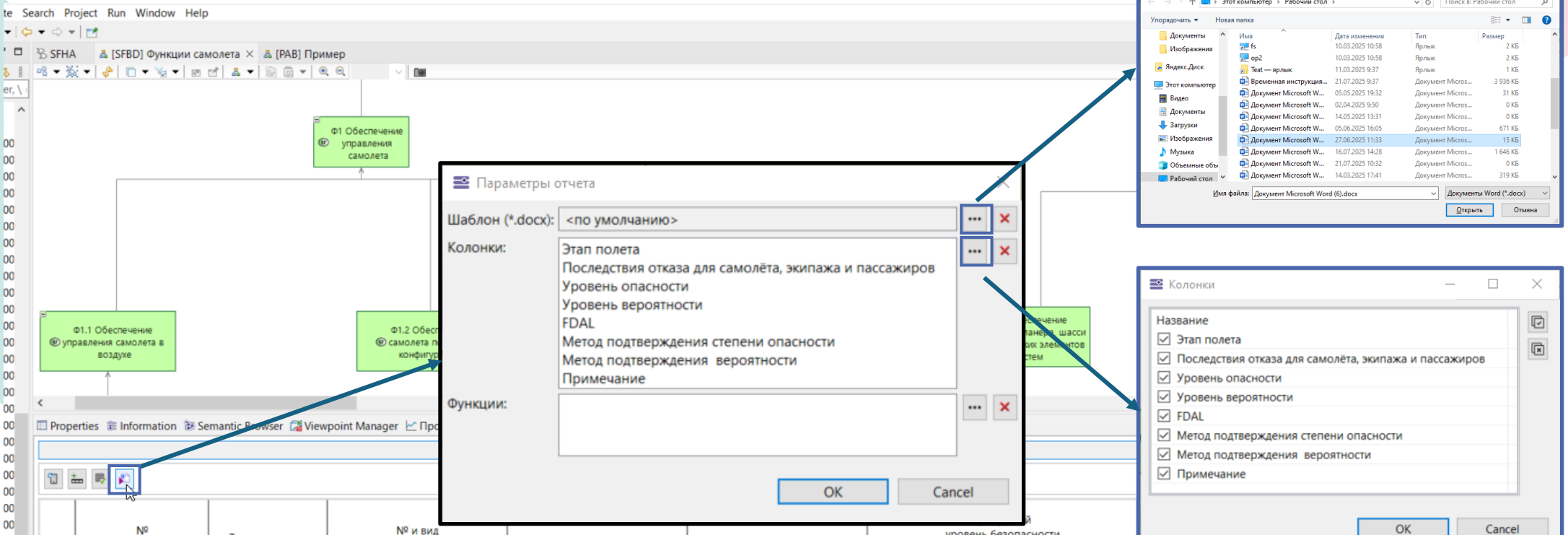


Отсутствие необходимых связей между объектами (функциями, уровнями, физическими объектами) в исходной модели



ПРИМЕР · ФОРМИРОВАНИЯ ОТЧЕТА AFHA/SFHA В ПО «АРХИП» (АВИАЦИЯ)

Оценка функциональных опасностей (Авиация)



	№ и наименование функции самолёта	Тип нарушения функции	№ и вид нарушения функции самолёта	Этапы полёта	Последствия отказа	уровень безопасности			
						Степень опасности	Вероятность	FDAL	
1			ФО1.1.1/1 Потеря управления движением самолета по тангажу по аварийной сигнализации с сигнализацией об отказе	1.1.2, 1.1.3, 1.2, 2., 3., 4., 5., 6.1, 7.	Для самолёта: Отсутствие управления в продольном канале. Невозможно безопасное продолжение и завершение полета. Для экипажа: Предотвращение гибели людей оказывается практически	КС	$<10^{-9}$	A	Экспе
2		Полная потеря функции		1.1.1, 6.2	Для самолёта: При разбеге – экипаж применяет процедуру прерванного взлета. Отсутствие возможности управления РН и СУПК от педальных постов на	АС	$<10^{-7}$		

Оценка функциональных опасностей (Авиация)

№ и наименование подфункций самолета	№ и вид нарушения функции самолета	Этап полета	Последствия отказа для самолёта, экипажа и пассажиров	Требуемый уровень безопасности:			Метод подтверждения:		Примечание
				Степень опасности	Вероятность	FDAL	Степени опасности	Вероятности	
Самолетные функции									
Ф0 Обеспечение безопасного полета по заданному маршруту в ожидаемых условиях эксплуатации									
Ф1 Обеспечение управления самолета									
Ф1.1 Обеспечение управления самолета в воздухе									
Ф1.1.1 Управление траекторией полета	Полная потеря функции:								
	ФО1.1.1/1 Потеря управления движением самолета по тангажу по аварийной сигнализации с сигнализацией об отказе	1.1.2, 1.1.3, 1.2, 2., 3., 4., 5., 6.1, 7.	Для самолёта: Отсутствие управления в продольном канале. Невозможно безопасное продолжение и завершение полета. Для экипажа: Предотвращение гибели людей оказывается практически невозможным	КС	$<10^{-9}$	A	Экспертная оценка	FTA 1.1.1_1	
	ФО1.1.1/2 Потеря управления движением самолета по трем каналам по аварийной сигнализации	1.1.1, 6.2	Для самолёта: При разбеге – экипаж применяет процедуру прерванного взлета. Отсутствие возможности управления РН и СУПК от педальных постов на больших скоростях - возможно боковое выкатывание с ВПП. Значительное увеличение рабочей нагрузки на экипаж	АС	$<10^{-7}$	A	Экспертная оценка	FTA 1.1.1_2	
		1.2, 2., 3., 4., 5., 6.1	Для самолёта: Потеря управления самолетом. Невозможно безопасное продолжение и завершение полета. Для пассажиров: Предотвращение гибели людей оказывается практически невозможным	КС	$<10^{-9}$				
	Частичная потеря функции:								
	ФО1.1.1/3 НФ1.2.1.1/3 Потеря основного режима управления самолета по трем каналам с сигнализацией об отказе по предупреждающей сигнализации с сигнализацией об отказе	1., 1.1, 1.1.1, 1.1.2, 1.1.3, 1.2, 2., 3., 4., 5., 6., 6.1, 6.2, 7.	Для самолёта: Изменение характеристик управляемости и устойчивости. Отсутствие ограничительных функций КСУ. Потеря всех режимов САУ Для экипажа: Экипаж переключится на резервный (ручной)	УУП	$<10^{-3}$	D	Стендовые испытания, Летные испытания	FTA 1.1.1_3	

ЭФФЕКТЫ МОДЕЛИ

Что архитектурная модель даёт оценке безопасности

1 Единый источник данных

Модель — база данных, а не рисунок: элемент существует в одном экземпляре, противоречие между представлениями (диаграммами) становится физически невозможным; изменение вносится один раз и автоматически отражается во всех представлениях

2 Доказуемая полнота охвата

Модель выдаёт полный перечень элементов, интерфейсов, функций и режимов — и полноту оценки можно не декларировать, а продемонстрировать численно

3 Однозначность интерпретации

Модель строится на формальном языке; формальный язык не допускает разночтений; допущения специалиста по безопасности замещаются данными разработчика

4 Сдвиг оценки влево

Архитектурная модель появляется раньше КД: варианты архитектуры сравниваем по безопасности ещё до того, как выбор сделан

5 Автоматизация анализов (MBSA)

Деревья отказов, таблицы FMEA, таблицы ОФО и прочие артефакты оценки безопасности генерируются из модели автоматически

6 Сквозная трассируемость

Связи «отказное состояние — требование безопасности — элемент архитектуры — мера снижения риска — свидетельство» являются объектами модели: при изменении элемента система сама показывает, какие требования, анализы и свидетельства подлежат пересмотру

ПРАКТИКА ПЕРЕХОДА

Переход к MBSA: преимущества и сложности

ПРЕИМУЩЕСТВА

- Единый источник данных вместо десятков «разрозненных» документов
- Автоматизация: FTA, FMEA, и другие артефакты генерируются, а не рисуются
- Гарантированная согласованность модели проекта и модели безопасности
- Мгновенный анализ влияния изменений — перегенерация вместо переделки
- Ранняя верификация архитектуры, когда изменения дёшевы

СЛОЖНОСТИ

- На старте нужны вложения: инструменты, инфраструктура, обучение
- Дефицит специалистов, владеющих модельно-ориентированными подходами к проектированию
- «Мусор на входе — мусор на выходе»: модель не исправит плохие данные по отказам
- Незрелость стандартизации за пределами авиации
- Изменение процессов и культуры: подход «купим лицензии и нарисуем всё в SysML» не работает

Переход непрост — но если не начать сейчас, создать по-настоящему безопасный транспорт не получится

итоги

Выводы

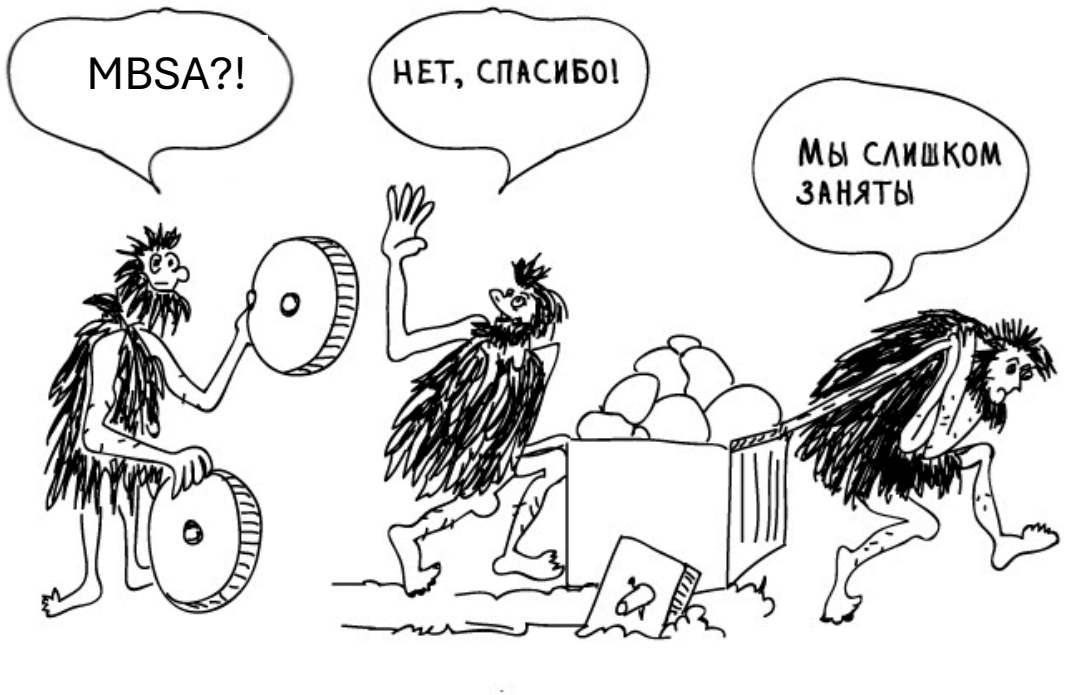
1. Сложность транспортных систем выросла многократно, а причина ошибок и трудозатрат при оценке безопасности — не в методах анализа, а в способе представления исходных данных

2. Архитектура уже требуется нормативно: ISO/IEC/IEEE 15288 и 42010, IEC 61508, ISO 26262, ISO 21448, ISO/SAE 21434, EN 5012x, ARP4754/ARP4761, ГОСТы — вопрос лишь в форме: модель или россыпь документов

3. Архитектурная модель даёт то, чего документы дать не могут: доказуемую полноту, однозначность, ранний анализ, автогенерацию артефактов (MBSA) и сквозную трассируемость

4. Инструменты для такого перехода уже существуют и работают: ГК «ПЛМ Урал» разрабатывает и внедряет ПО для мультидоменного архитектурного моделирования и модельно-ориентированной оценки безопасности. Приглашаем к сотрудничеству всех, кому тема откликнулась.

В качестве заключения



Будьте открыты новому

Спасибо за внимание!

Готов ответить на ваши вопросы

ГК «ПЛМ Урал»
620131, г. Екатеринбург,
ул. Металлургов, 16 Б

8-800-500-1993
info@plm-ural.ru
www.plm-ural.ru

