Конференция «Встраиваемые системы реального времени»
9 октября 2025 года

ENDURANCE
TEST & CERTIFICATION

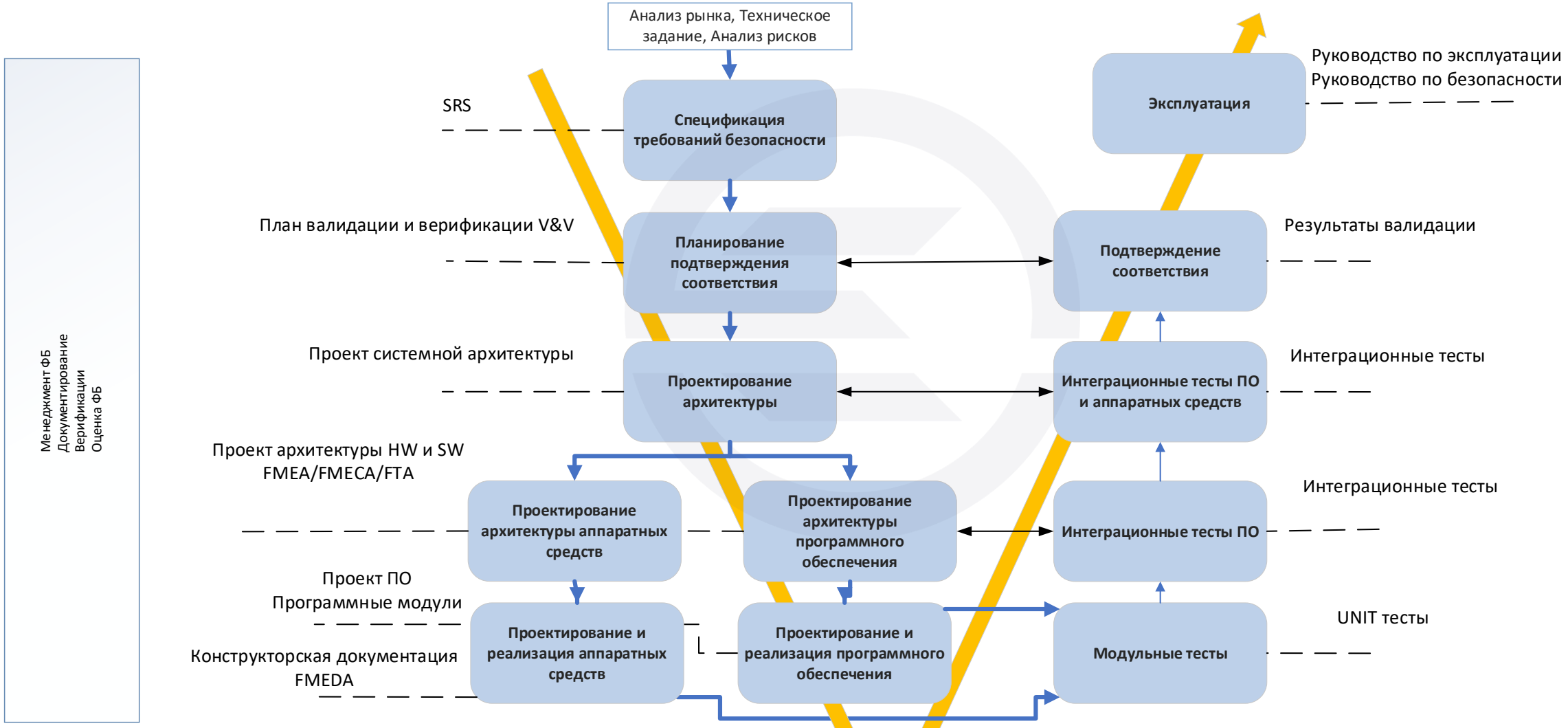
Особенности выбора инструментальных средств для поддержки жизненного цикла разработки технических средств

ЗУБРЕВ ЕВГЕНИЙ

Руководитель направления оценки и сертификации

Жизненный цикл разработки технических средств

(сокращенный и обобщенный, в соответствии с МЭК 61508)



Для чего использовать инструментальные средства?

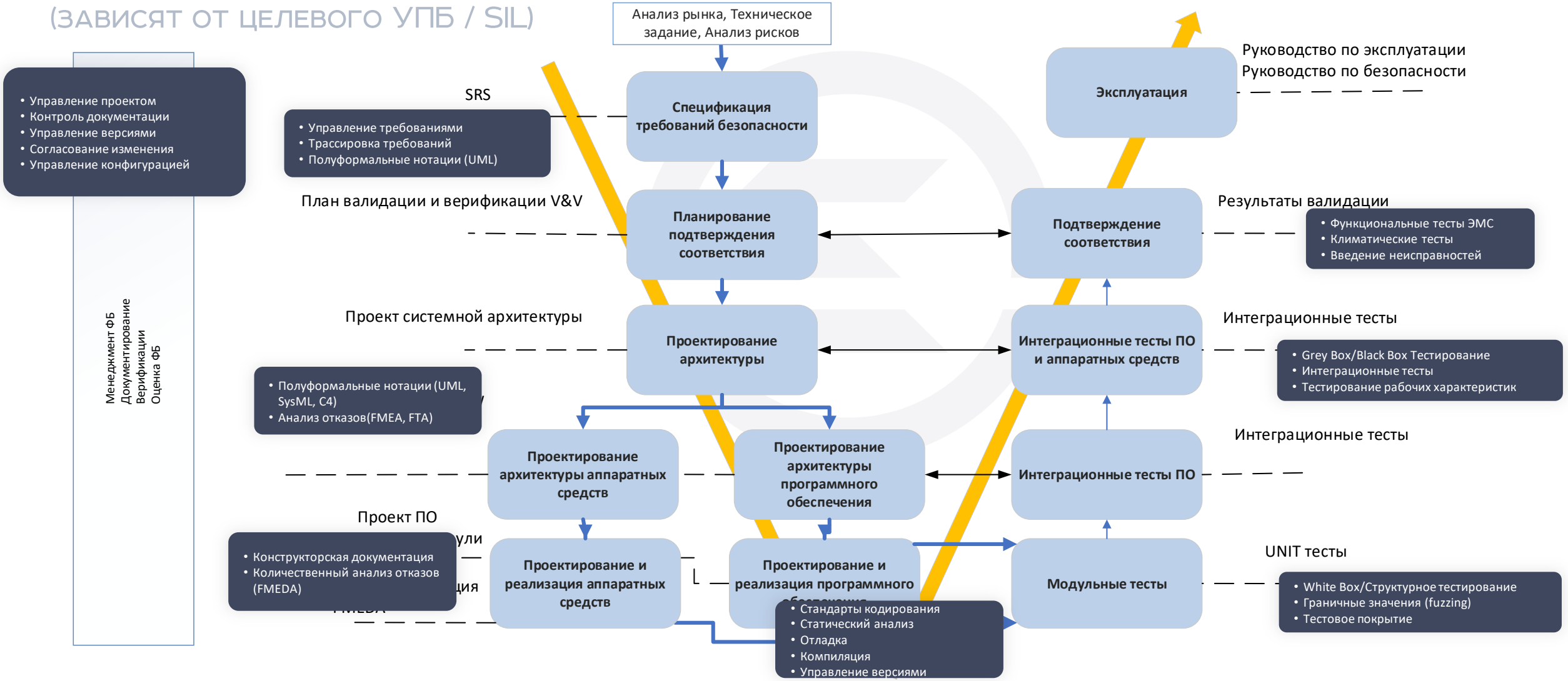
ENDURANCE
TEST & CERTIFICATION

- Поддержка жизненного цикла безопасности при разработке
- Применение методов управления систематическими отказами требуемыми стандартами функциональной безопасности
- Уменьшение человеческого фактора при разработке
- Уменьшение вероятности появления или необнаружения отказов во время разработки

Цель – снижение систематических отказов

Основные методы управления систематическими отказами на различных этапах жизненного цикла

(зависят от целевого УПБ / SIL)



Основные требования к инструментальным средствам (МЭК 61508)

1. Все инструментальные средства, которые планируется использовать в проекте функциональной безопасности, **должны быть перечислены и описаны** (например, в Плане безопасности).

2. Все инструментальные средства должны быть классифицированы в соответствии с их критичностью для разрабатываемой системы. МЭК 61508 выделяет классы инструментальных средств **T1, T2, T3.**

3. Инструментальные средства класса **T2 и T3** должны иметь документацию, в которой описано поведение средства и даны инструкции по его использованию.
   Пригодность для целевой задачи!

4. Для инструментальных средств класса **T2 и T3** должна быть проведена оценка потенциальных отказов и выработаны механизмы их ослабления (например, HAZOP/FMEA ПО)
   Инструментальные средства также могут вносить отказы!

5. Для инструментальных средств класса **T3** должно быть свидетельство о соответствие средства его документации (результаты квалификации)

Спецификация требований безопасности (SRS)

ENDURANCE
TEST & CERTIFICATION

Основные требования:

- Ясность, точность, возможность проверки требований
- Управляемость требованиями (статус, ответственный)
- Иерархическое разделение требований (ID, SR/NRS)
- Обеспечение прямой и обратной прослеживаемости (трассировка требований) – для УПБ 3 / УПБ 4
- Выражение с использованием полуформальных нотаций (например, UML) – для УПБ 3 / УПБ 4

Примеры инструментальных средств

Иностранный рынок:

IBM Rational DOORS
JAMA SOFTWARE
PTC Codebeamer
…

Отечественный рынок:

Devprom

Проектирование архитектуры

ENDURANCE
TEST & CERTIFICATION

Основные требования:

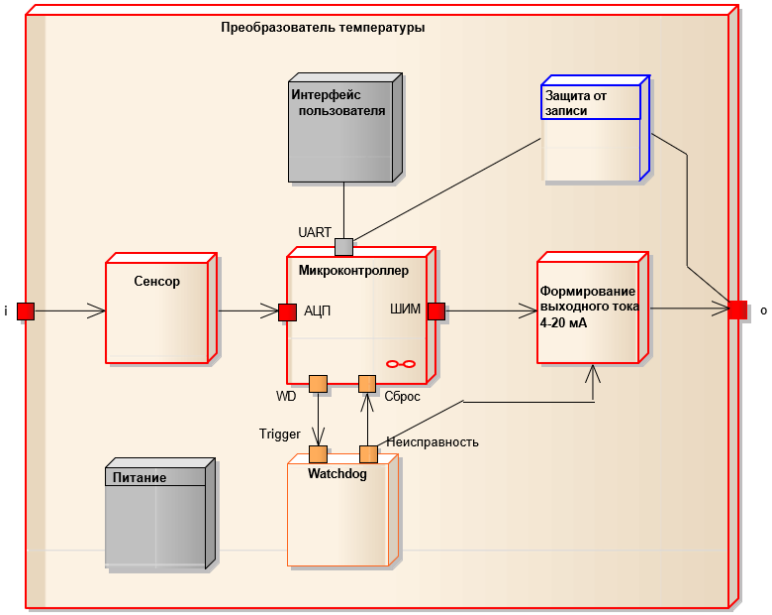
- Иерархичность, модульность
- Представление с помощью полуформальных нотаций (например, UML, SysML) – для УПБ 3 / УПБ 4
- Обеспечение трассируемости с требованиями – для УПБ 3 / УПБ 4

Примеры инструментальных средств

Иностранный рынок:
IBM Engineering Rhapsody
Enterprise Architect
PTC Integrity Modeler
…

Отечественный рынок:
—

Диаграмма развертывания преобразователя



Возможно использование средств с открытым исходным кодом:

- **Plant UML**
- **draw.io**
- **Modelio System Architect**
- **Eclipse Papyrus**

Проектирование аппаратных средств. Качественная и количественная оценка отказов

ENDURANCE
TEST & CERTIFICATION

Основные требования:

- Анализ вероятности отказов функции безопасности
- Прогнозирование показателей отказов (λ, SFF, PFDavg, PFH, SPFM, LFM)

Примеры инструментальных средств

Иностранный рынок:

Ansys medini (HAZOP, HARA, FHA, FTA, FME(C)A, FMEDA)
EnCo SOX (HAZOP, HARA, FTA, FME(C)A, FMEDA)
ISOGRAPH Reliability Workbench (модуль надежности)
…

Отечественный рынок:

—

Возможно использование средств с открытым исходным кодом:

- EMFTA (только FTA)
- Open FMEA (только FMEA)

Реализация программного кода

ENDURANCE
TEST & CERTIFICATION

Основные требования:

- Использование стандартов кодирования и подмножества языка (MISRA, AUTOSAR)
- Проведение и документирование статического анализа
- Ограничение сложности программного обеспечения, модульность

Примеры инструментальных средств

Иностранный рынок:

PC-lint
SonarQube
Parasoft C/C++test

Отечественный рынок:

PVS-Studio

Трансляторы и компиляторы

ENDURANCE
TEST & CERTIFICATION

Основные требования:

- Относятся к инструментальным средствам класса Т3
- Должно быть свидетельство о соответствие средства его документации
- Тестирование функций, влияющих на генерацию исполнимого кода

Примеры инструментальных средств

Иностранный рынок:

Arm Compiler for Embedded FuSa
IAR Embedded Workbench for Functional Safety
TI Compiler
…

Отечественный рынок:

—

Возможно использование средств с открытым исходным кодом:

- GCC, LLVM (требуется квалификация)

Тестирование программного обеспечения. Динамический анализ

ENDURANCE
TEST & CERTIFICATION

Основные требования:

- Тестирование всех программных модулей участвующих в безопасности
- Анализ тестовых сценариев на основе требований к функциям модуля
- Проведение структурных тестов (точки входа, операторы, условные переходы) → Функциональные / UNIT тесты
- Анализ метрик охвата структурных тестов (цель - 100% выбранной метрики)
- Анализ граничных значений → Фаззинг
- Документированность тестов

Примеры инструментальных средств

Иностранный рынок:
LDRAunit
Parasoft's C/C++ unit
VectorCAST/C

Отечественный рынок:
Киннор Динамика (фаззинг)

Возможно использование средств с открытым исходным кодом:

- Google Test
- ThrowTheSwitch
- Gcov

Выводы

1 | Инструментальные средства предназначены **для поддержки жизненного цикла и управления систематическими отказами**

2 | Инструментальные средства **могут вносить собственные отказы** – требуется обоснование выбора

3 | **На международном рынке** представлено **множество** инструментальных средств для различных этапов жизненного цикла безопасности

4 | **На отечественном рынке** инструментальные средства, поддерживающие жизненный цикл безопасности, **представлены ограниченно.** Для отдельных этапов жизненного цикла **отсутствуют полностью.**

ENDURANCE
TEST & CERTIFICATION

ОСТАЛИСЬ ВОПРОСЫ?

СВЯЖИТЕСЬ С НАМИ

сайт компании
https://www.endce.ru

сайт по функциональной безопасности
https://sil3.ru/

e-mail
info@endce.ru

телефон
+7 495 799-07-93

telegram
https://t.me/endurance_msc

@ENDURANCE_MSC