Взаимная трассировка требований, кода и тестов в среде АИС УЖЦ с целью безопасной разработки системного ПО

Солоделов Ю.А., Началлник лаборатории
Ветров С.О., Начальник сектора
Автоманов С.А., ведущий инженер сектора
Июнь 2022

ГосНИИАС
ГНЦ ФГУП «Государственный научно-исследовательский институт авиационных систем»

Постановка задачи

- При разработке ответственного и сложного ПО необходимо обеспечить его соответствие требованиям.
- Проверка на соответствие осуществляется с помощью тестирования, а также с помощью ряда других процедур – инспекций и анализа исходного кода, проведения испытаний и т.п.
- Задача состоит в обеспечении корректности, полноты и непротиворечивости покрытия требований кодом и тестами, а также (обратная задача) нахождения кода и тестов, соответствующих требованиям.

Теория

- Синтез системы S состоит в построении модели Ψ_b, определяющей **внутренне строение** по модели Ψ_a, определяющей **свойства** проектируемой системы путем нахождения предиката **функциональной целостности**.
- Преобразование $\Psi_a \rightarrow \Psi_b$ – называется эквивалентированием системы S в систему $S^{\sim}$. В общем виде представляет собой ориентированный граф.
- Ответственное и сложное ПО относится к классу **больших** и **сложных** систем:
  - Для сложной системы не существует взаимно однозначного соответствия между моделями Ψ_a и Ψ_b
  - Большая система не упрощается заданными вычислительными средствами.

Основные понятия

Артефакты

- Атомы из которых состоит Система
- Полезный продукт труда
- Самостоятельная ценность
- Составляют единицы конфигурации

Связи

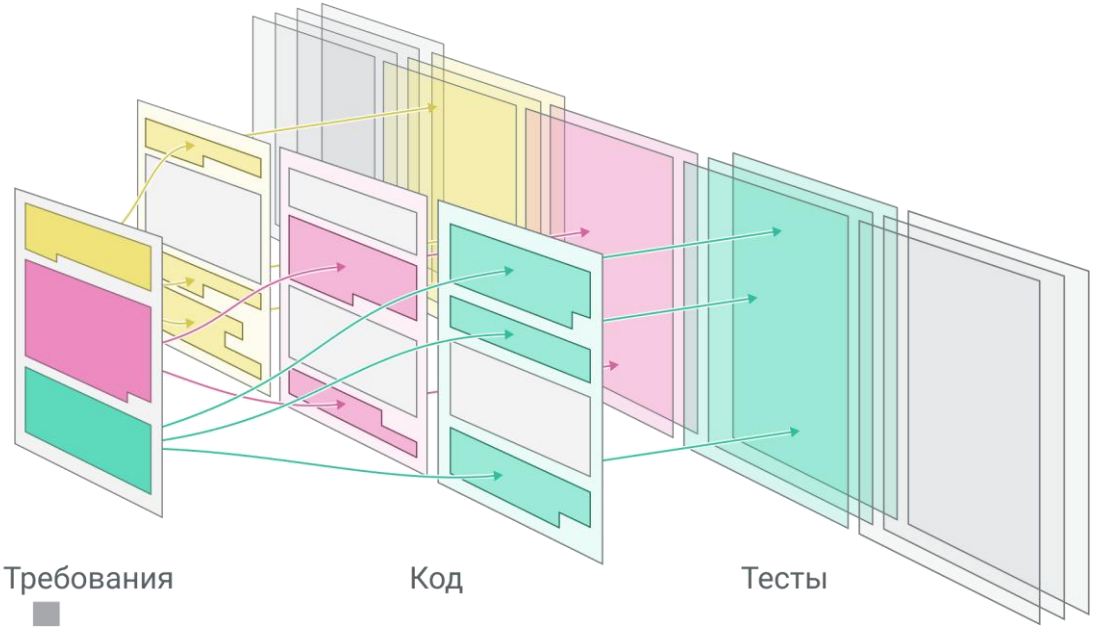
- Отражают отношения между артефактами
- Служат для согласованной обработки артефактов
- Позволяют анализировать группы артефактов

Процессы

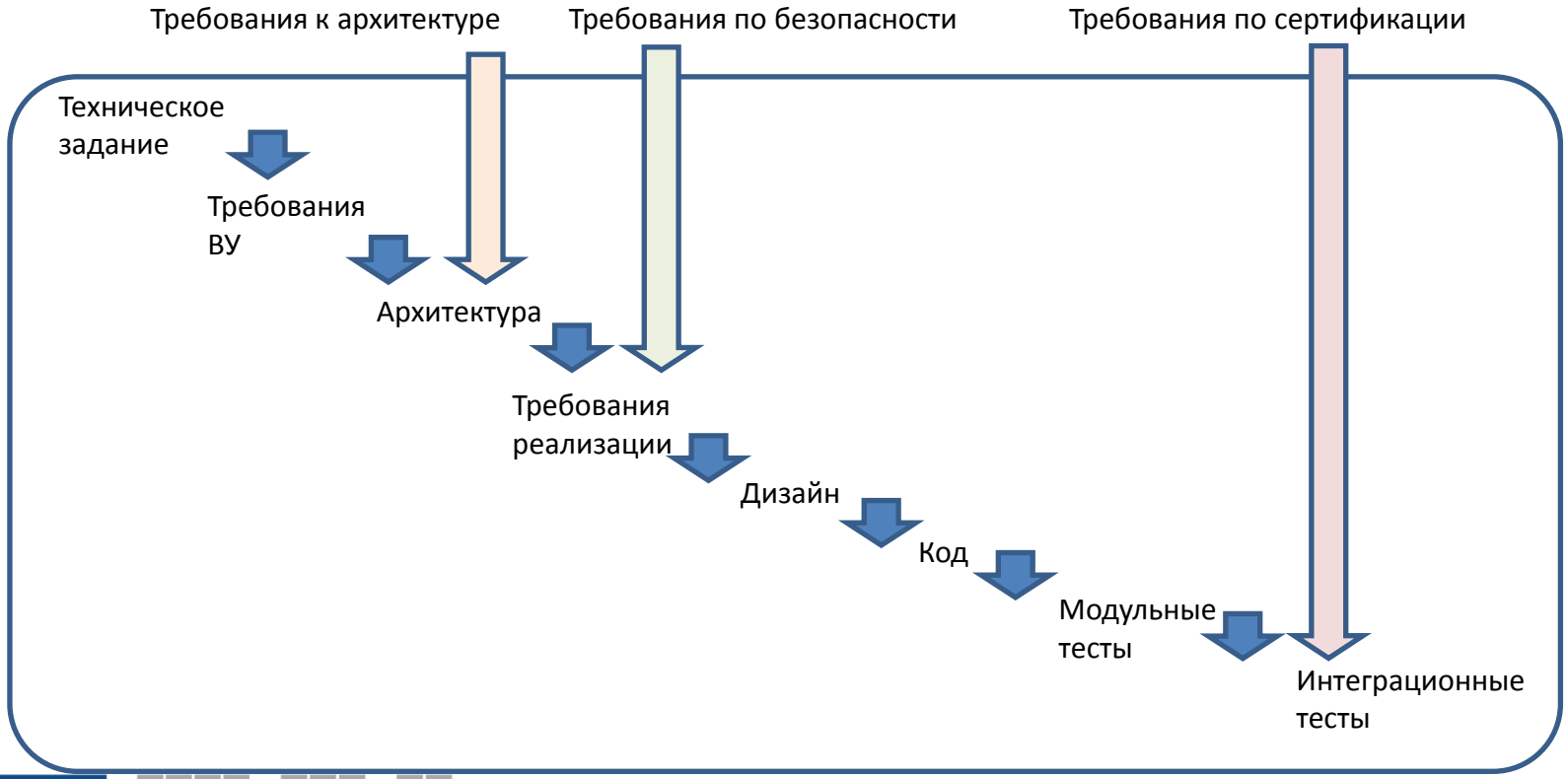
- Регламенты (правила) работы с Артефактами и Связями

Практика

- Техническое задание (Модель Ψ_a) `*.doc`
- Код (Модель Ψ_b) `*.h *.c`
- Тесты (оценка предиката функциональной целостности) `*.c`



Этапы разработки сложного ПО

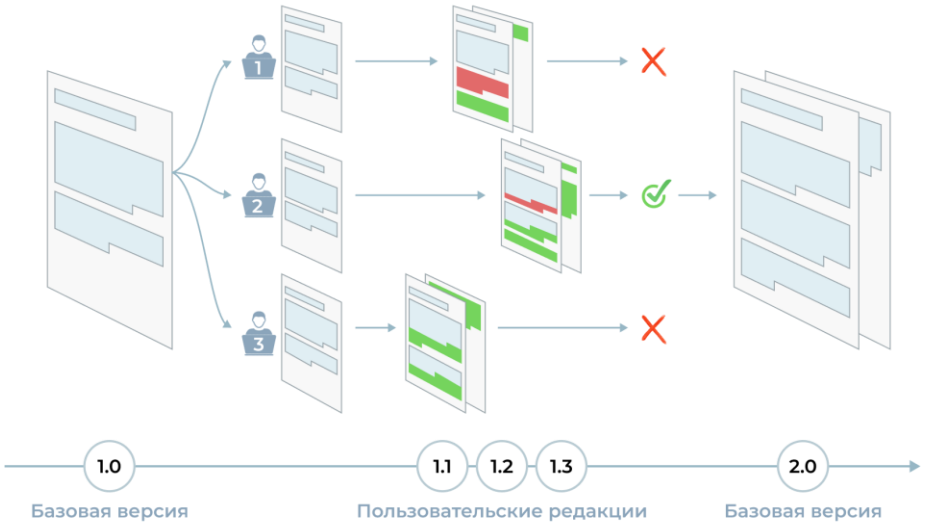


Артефакты отдельных этапов разработки ПО

- **Архитектура**
  - Требования к архитектуре
  - Описание архитектуры на AADL
  - Анализ на отказнобезопасность
  - Анализ производительности
- **Требования к реализации**
  - Используемые протоколы
  - Имитационная модель
- **Интеграционные тесты**
  - Испытательный базис
  - План испытаний
  - Тестовые случаи и тестовые процедуры

Количественная оценка объема проекта

- Последовательность эквивалентных преобразований может состоять из N*10 шагов.
- На каждом шаге свой набор артефактов
- Всего $M*10^2$ видов артефактов
- $K*10^6$ экземпляров артефактов
- $L*10^6$ связей между артефактами
- Артефакты и связи версионируются

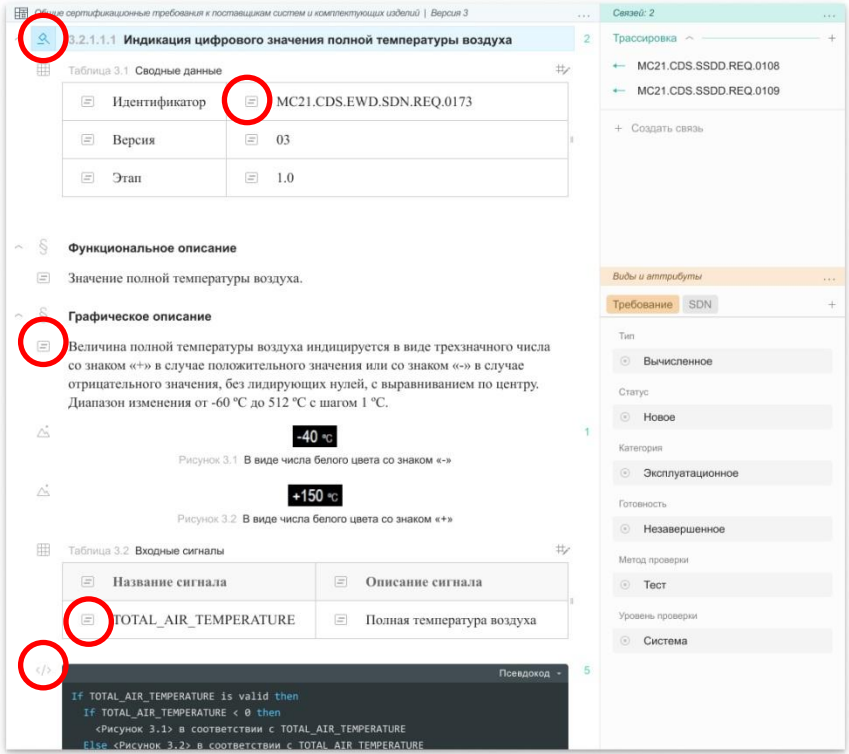


Автоматизированная информационная среда управления жизненным циклом

АИС УЖЦ

- **Управление конфигурацией**
  - Типизированные артефакты и единицы конфигурации
  - Согласованность изменений единиц конфигурации
  - Произвольная грануляция единиц конфигурации
- **Прослеживаемость**
  - Типизированные связи
  - Обеспечивает согласованное изменение связанных артефактов
  - Обеспечивает комплексный анализ Системы
  - Позволяет оценить риски изменений
- **Регламент**
  - Определяет правила изменения Артефактов
  - Обеспечивает контроль за изменениями
  - Позволяет оценивать трудоемкость и сроки работ

АИС УЖЦ: Требования



Артефакт АИС УЖЦ

АИС УЖЦ: Связи

Схемотехника

Схемотехника аналоговых и аналогово-цифровых эл... / пользовательская редакция /

5.2.1 Упрощенная схема стабилизатора

9

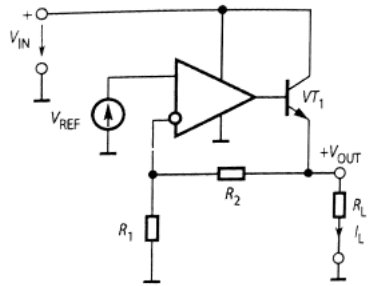


Рисунок 5.1 Схема линейного стабилизатора напряжения

2

В упрощенном виде схема линейного стабилизатора напряжения приведена на Рис.5.1 Схема состоит из ОУ, включенного по схеме неинвертирующего усилителяс отрицательной обратной связью по напряжению, источника опорного напряжения Vref и регулирующего транзистора VT1, включенного последовательно с нагрузкой.

Связей: 9

Обоснование

- MC21.CDS.SRS.REQ.0011
- MC21.CDS.SRS.REQ.0032
- MC21.CDS.SRS.REQ.0036
- MC21.CDS.SRS.REQ.0053

Описание

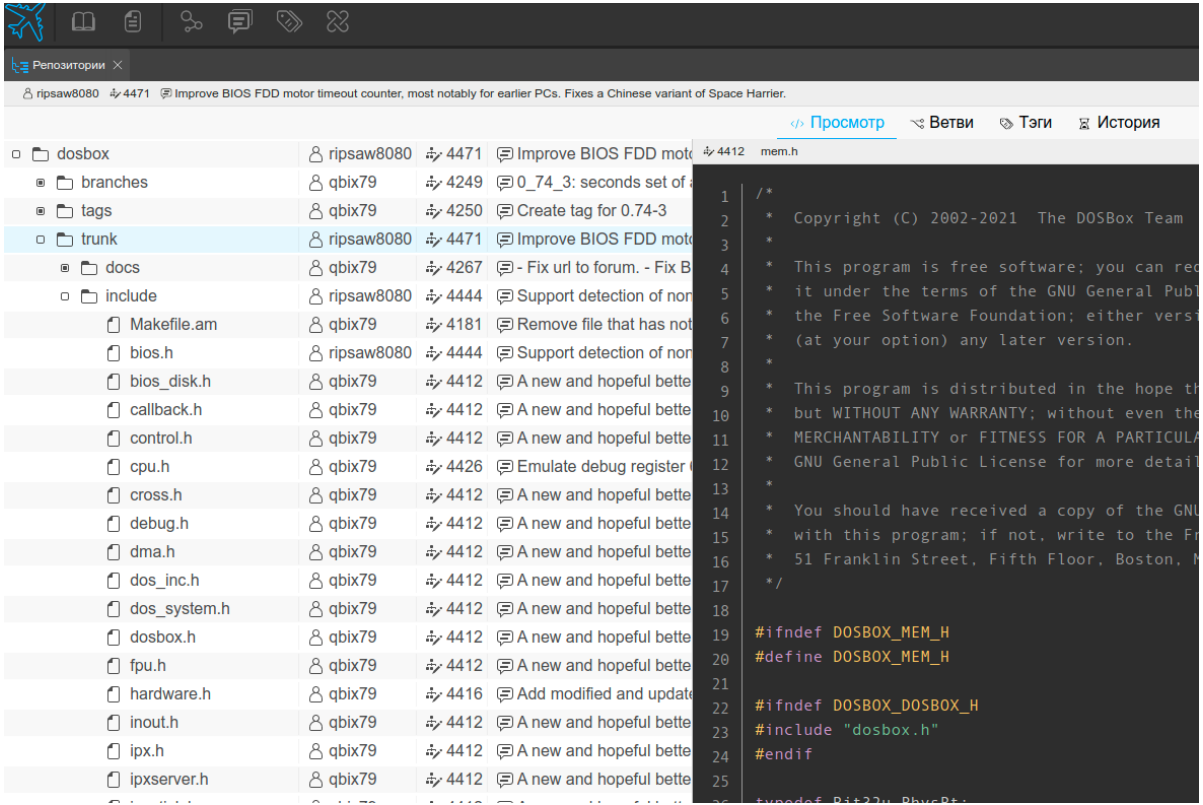
- MC21.CDS.EWD.SDN.REQ.0...
- MC21.CDS.EWD.SDN.REQ.0...

Трассировка

- MC21.CDS.SSDD.REQ.0162
- MC21.CDS.SSDD.REQ.0169
- MC21.CDS.SSDD.REQ.0175

Создать связь

АИС УЖЦ: Внешний репозиторий кода

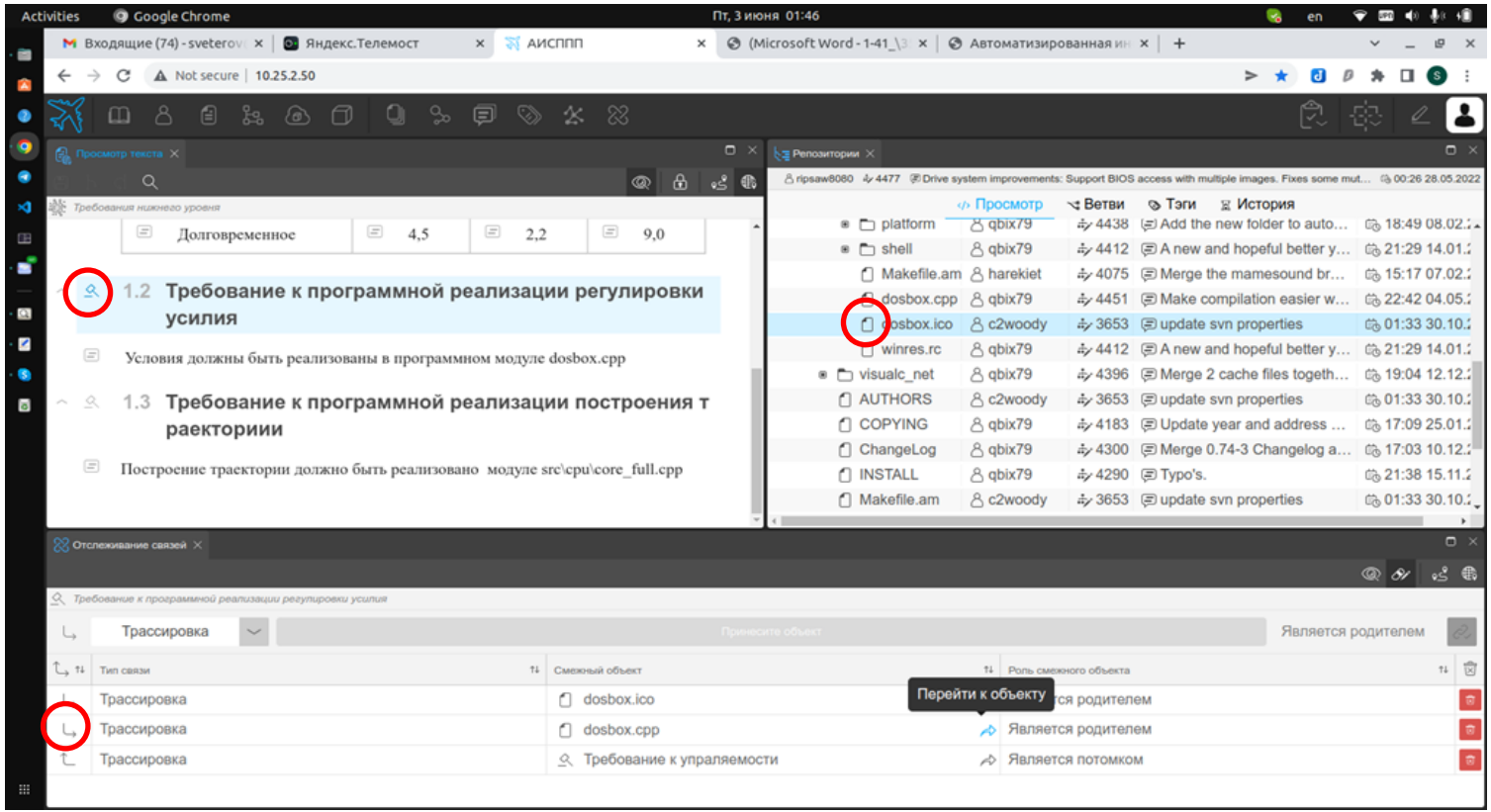


АИС УЖЦ: Анализ связей

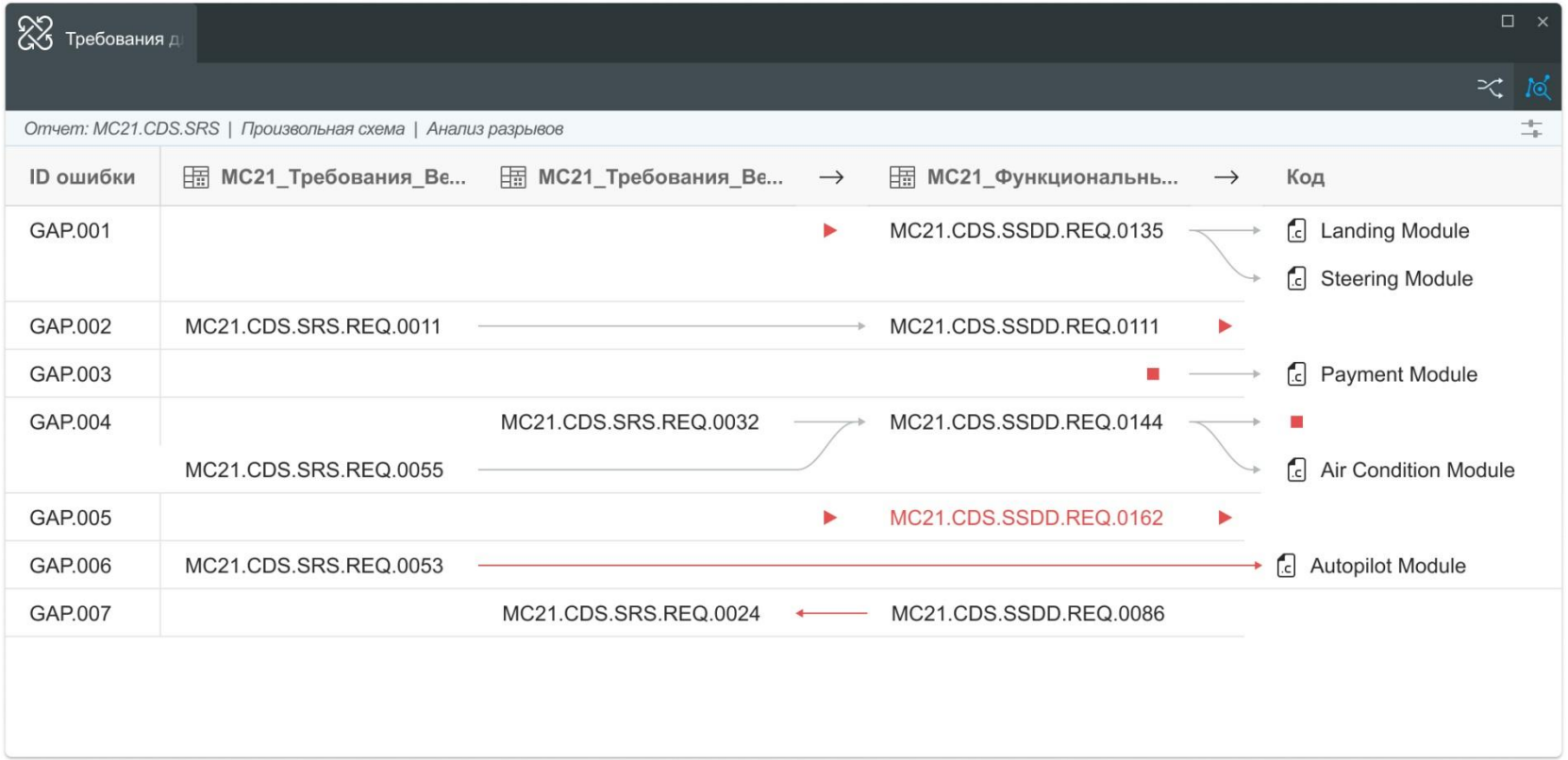
Виды формального анализа связей:

- Трассировка (прослеживаемость) – анализ согласно трассировочной схеме
- Анализ разрывов связей (GAP анализ)
- Анализ влияния
- Выход за пределы проекта

АИС УЖЦ: Анализ связей



АИС УЖЦ: GAP анализ трассировочных связей



АИС УЖЦ: облик системы

- Доступ из глобальной сети, размещение в облаке
- Совместное редактирование документов
- Хранение истории изменений (редакции, версии, варианты)
- Сборка документа из частей по шаблону и регламенту
- Документ как структура цифровых артефактов (текст, изображение)
- Автоматизированная валидация, верификация, аудит
- Доступ к внешним приложениям и базам данных
- Импорт/ экспорт файлов форматов odt, docx, pdf, ReqIF, csv
- Обработка артефактов по регламенту
- Связывание артефактов
- Организация и контроль конфигураций (вариант, сборка, система)
- Цифровая библиотека артефактов
- Единый документ с вариантами на многих языках

АИС УЖЦ: облик системы

АИС ППП осуществляет поддержку сквозной технологии разработки, модернизации и сертификации сложных технических систем

АИС УЖЦ: облик системы

Работа из глобальной сети

Библиотека цифровых артефактов

Совместное редактирование текста

Единый документ на нескольких языках

История изменений документа, его частей, требования, спецификации и конфигурации

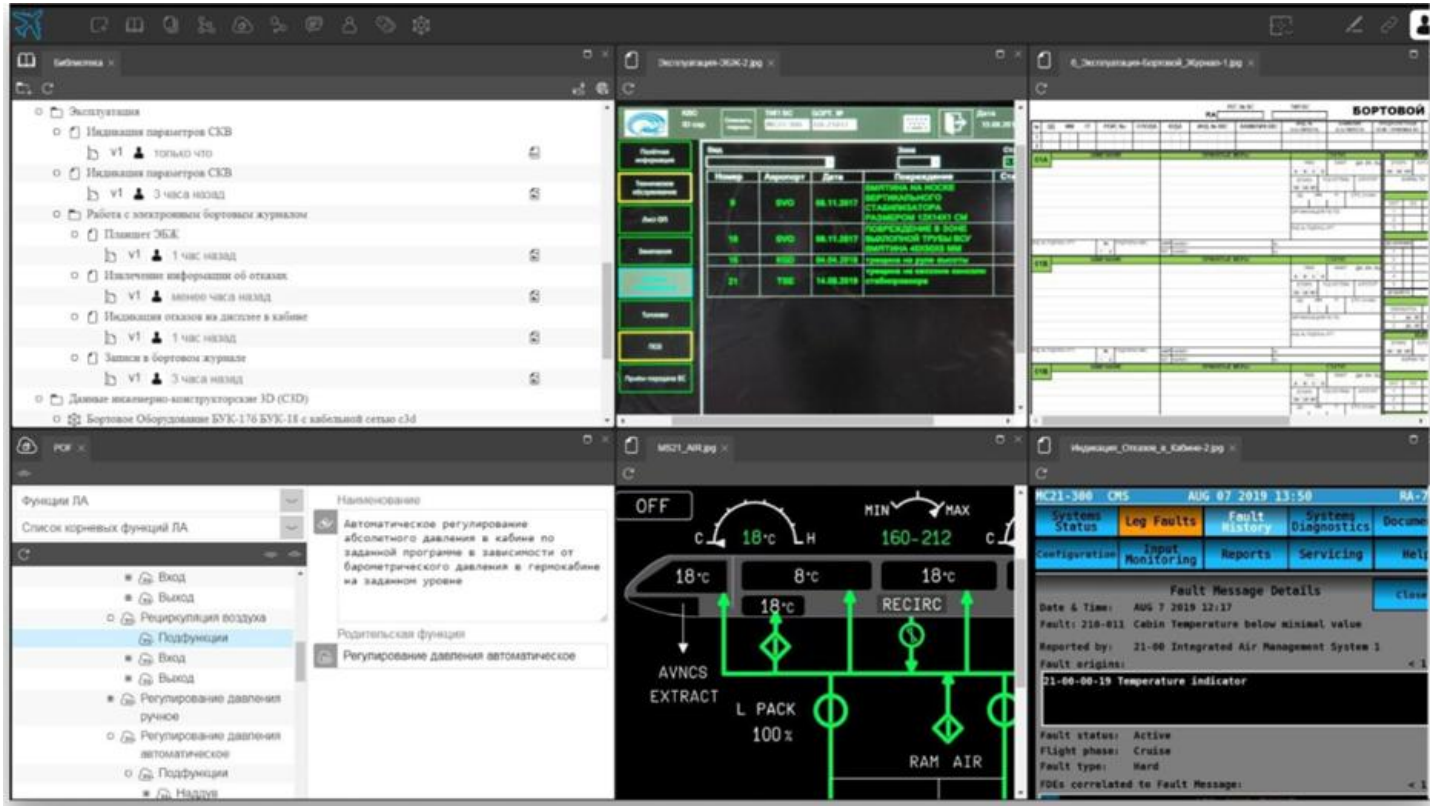
Ассоциация с приложениями и системами

Автоматизация валидации, верификации и аудита

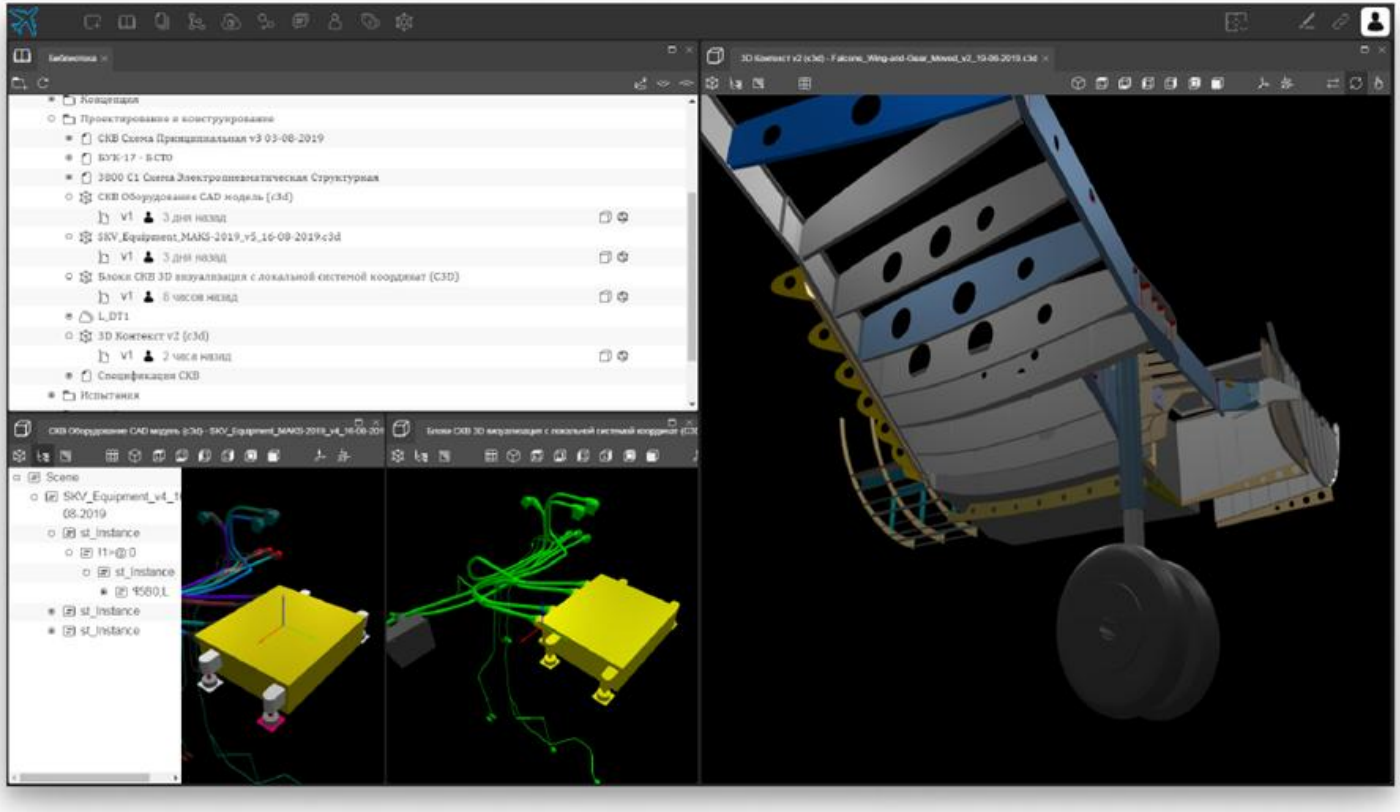
Управление заданиями, управление проектами

Выпуск документации по шаблонам

АИС УЖЦ: охват всего ЖЦ



АИС УЖЦ: совместная работа с САПР



Спасибо за внимание!