

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

Солоделов Ю.А., Начальник 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.

- 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

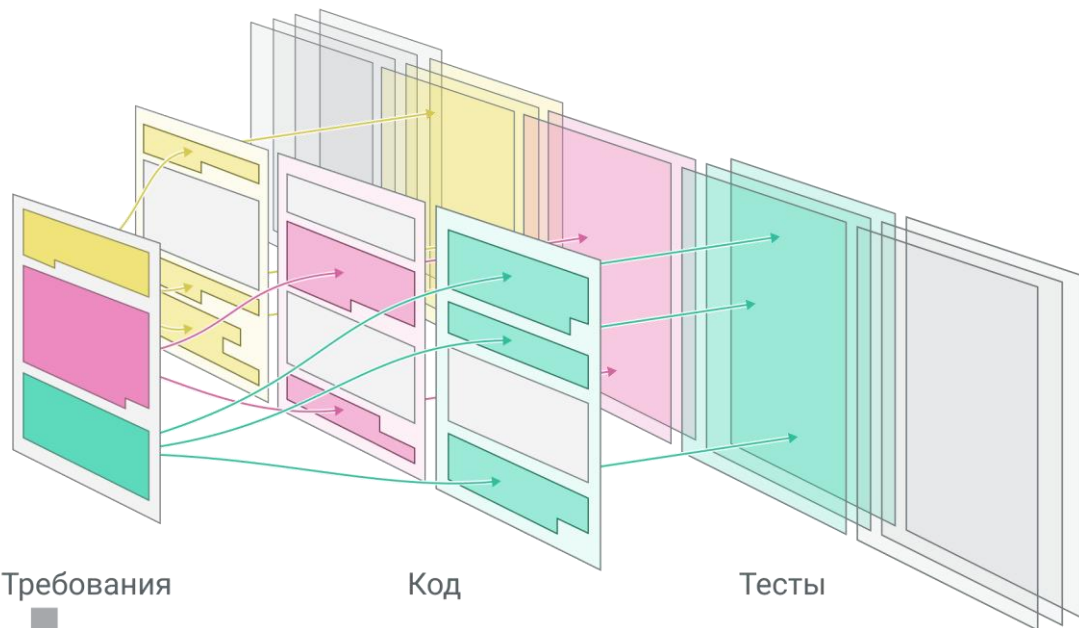
- Отражают отношения между артефактами
- Служат для согласованной обработки артефактов
- Позволяют анализировать группы артефактов

Процессы

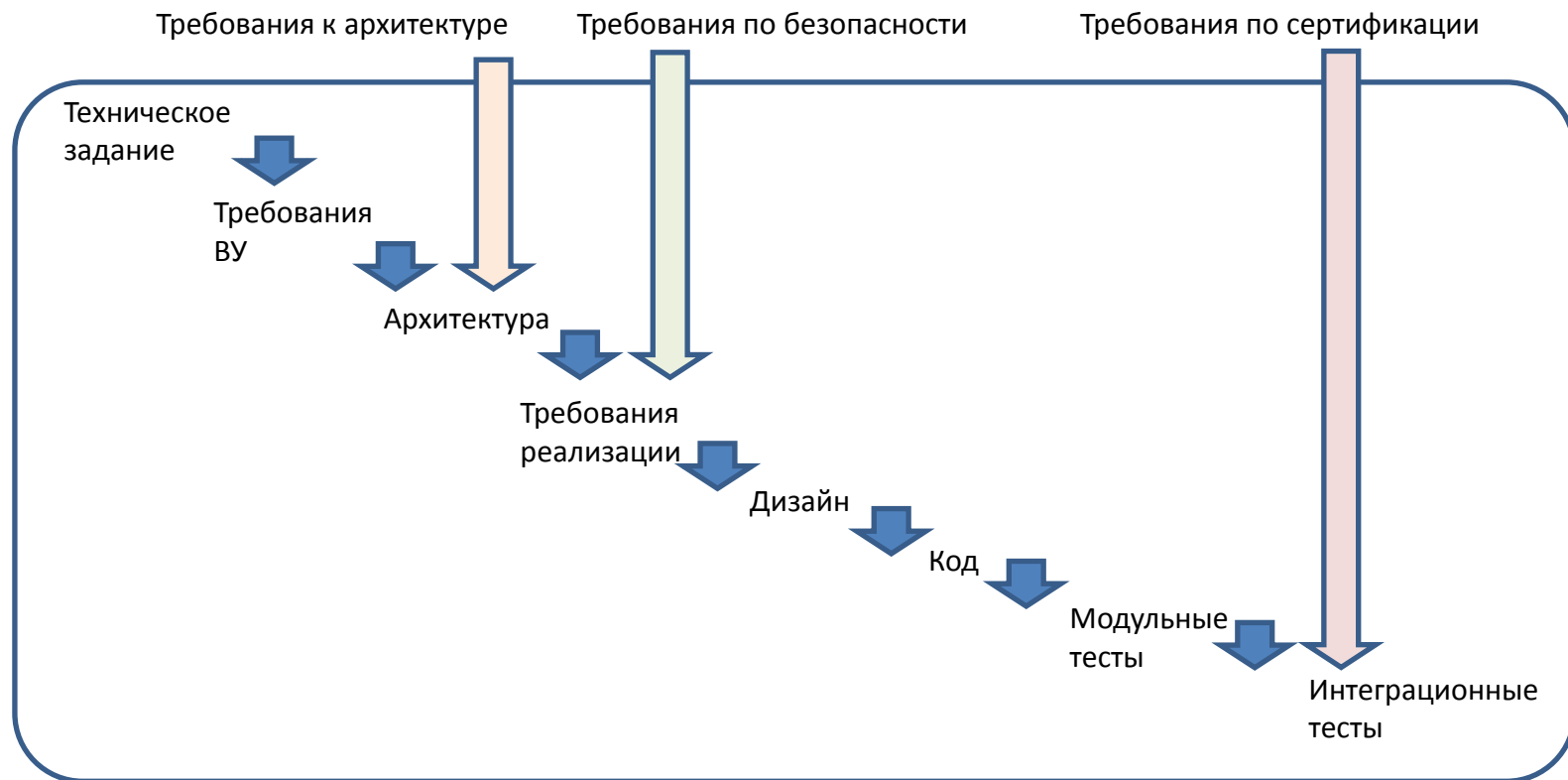
- Регламенты (правила) работы с Артефактами и Связями

Практика

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



Этапы разработки сложного ПО

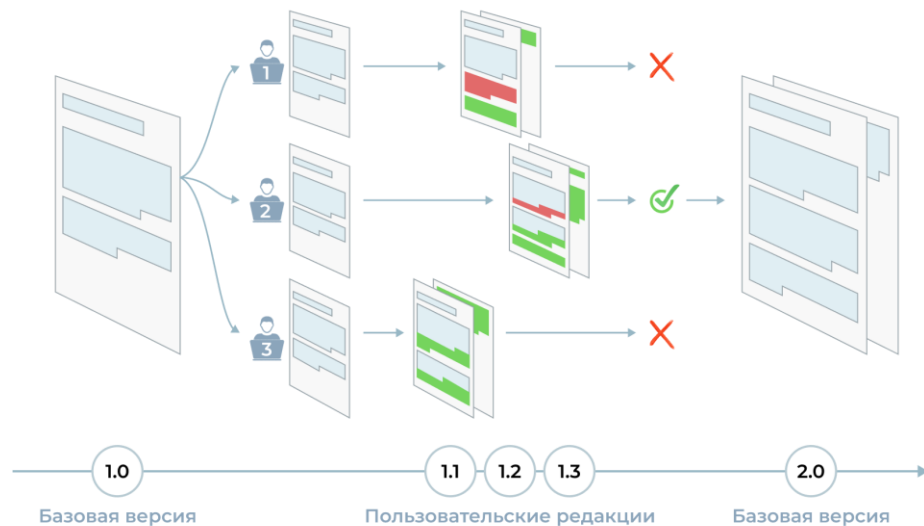


Артефакты отдельных этапов разработки ПО

- **Архитектура**
 - Требования к архитектуре
 - Описание архитектуры на AADL
 - Анализ на отказобезопасность
 - 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 $N \cdot 10$ шагов.
- На каждом шаге свой набор артефактов
- Всего $M \cdot 10^2$ видов артефактов
- $K \cdot 10^6$ экземпляров артефактов
- $L \cdot 10^6$ связей между артефактами
- Артефакты и связи версионятся





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

The screenshot displays the 'Индикация цифрового значения полной температуры воздуха' requirement. It includes a table with the identifier 'MC21.CDS.EWD.SDN.REQ.0173', a functional description, a graphical description with associated diagrams (Rисунк 3.1 and 3.2), an input signals table, and a code snippet.

Идентификатор	MC21.CDS.EWD.SDN.REQ.0173
Версия	03
Этап	1.0

Функциональное описание
Значение полной температуры воздуха.

Графическое описание
Величина полной температуры воздуха индицируется в виде трехзначного числа со знаком «+» в случае положительного значения или со знаком «-» в случае отрицательного значения, без лидирующих нулей, с выравниванием по центру. Диапазон изменения от -60 °C до 512 °C с шагом 1 °C.

Рисунк 3.1 В виде числа белого цвета со знаком «-»
-40 °C

Рисунк 3.2 В виде числа белого цвета со знаком «+»
+150 °C

Название сигнала	Описание сигнала
TOTAL_AIR_TEMPERATURE	Полная температура воздуха

```
if TOTAL_AIR_TEMPERATURE is valid then
  if TOTAL_AIR_TEMPERATURE < 0 then
    <Рисунк 3.1> в соответствии с TOTAL_AIR_TEMPERATURE
  else <Рисунк 3.2> в соответствии с TOTAL_AIR_TEMPERATURE
```



Артефакт АИС УЖЦ

АИС УЖЦ: Связи

Схемотехника

Схемотехника аналоговых и аналогово-цифровых зл... / пользовательская редакция / § ... Связей: 9

5.2.1 Упрощенная схема стабилизатора

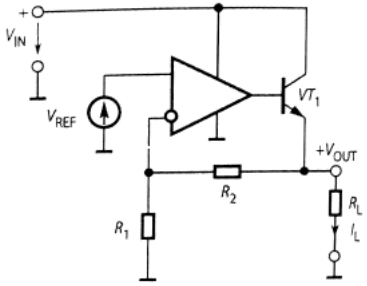


Рисунок 5.1 Схема линейного стабилизатора напряжения

В упрощенном виде схема линейного стабилизатора напряжения приведена на Рис.5.1 Схема состоит из ОУ, включенного по схеме неинвертирующего усилителя с отрицательной обратной связью по напряжению, источника опорного напряжения V_{REF} и регулирующего транзистора VT_1 , включенного последовательно с нагрузкой.

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

The screenshot displays a web-based code repository interface. At the top, there is a navigation bar with icons for home, search, and other functions. Below the navigation bar, the repository name "Репозитории" is visible. The main content area is divided into two parts: a file tree on the left and a code editor on the right.

The file tree on the left shows a directory structure for a project named "dosbox". The files and folders listed are:

- branches
- tags
- trunk (selected)
- docs
- include
 - Makefile.am
 - bios.h
 - bios_disk.h
 - callback.h
 - control.h
 - cpu.h
 - cross.h
 - debug.h
 - dma.h
 - dos_inc.h
 - dos_system.h
 - dosbox.h
 - fpu.h
 - hardware.h
 - inout.h
 - ipx.h
 - ipxserver.h

Each file entry in the tree includes the author's name, a commit hash, and a brief description of the change. For example, the "trunk" folder is associated with commit 4471 by user ripsaw8080, with the description "Improve BIOS FDD motor timeout counter, most notably for earlier PCs. Fixes a Chinese variant of Space Harrier."

The code editor on the right shows the content of the file "mem.h". The code is a C header file with the following content:

```
1 /*
2  * Copyright (C) 2002-2021 The DOSBox Team
3  *
4  * This program is free software; you can redistribute it and/or
5  * modify it under the terms of the GNU General Public License as
6  * published by the Free Software Foundation; either version 2 of
7  * the License, or (at your option) any later version.
8  *
9  * This program is distributed in the hope that it will be useful,
10 * but WITHOUT ANY WARRANTY; without even the implied warranty of
11 * MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
12 * GNU General Public License for more details.
13 *
14 * You should have received a copy of the GNU General Public License
15 * along with this program; if not, write to the Free Software
16 * Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA
17 * 02110-1301 USA
18 */
19 #ifndef DOSBOX_MEM_H
20 #define DOSBOX_MEM_H
21
22 #ifndef DOSBOX_DOSBOX_H
23 #include "dosbox.h"
24 #endif
25
26 typedef Bit22u RhwPt;
```

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

The screenshot displays a web application interface for analyzing relationships in a code repository. The interface is divided into several sections:

- Top Section:** A navigation bar with tabs for "Требования нижнего уровня" (Lower-level requirements) and "Репозитории" (Repositories).
- Left Panel:** A list of requirements. Requirement 1.2, "Требование к программной реализации регулирования усилия" (Requirement for software implementation of force regulation), is highlighted with a red circle. Below it, requirement 1.3 is also visible.
- Right Panel:** A file repository view showing a tree structure of files and folders. The file "dosbox.ico" is highlighted with a red circle. The repository view includes columns for file name, author, revision number, and commit message.
- Bottom Panel:** A table titled "Отслеживание связей" (Relationship tracking) for the selected requirement. The table has columns for "Тип связи" (Type of relationship), "Смежный объект" (Adjacent object), and "Роль смежного объекта" (Role of adjacent object). The first row shows "Трассировка" (Tracing) for "dosbox.ico" with the role "Является родителем" (Is parent). The second row shows "Трассировка" for "dosbox.cpp" with the role "Является родителем". The third row shows "Трассировка" for "Требование к управляемости" (Requirement for controllability) with the role "Является потомком" (Is child). A red circle highlights the first row, and a tooltip "Перейти к объекту" (Go to object) is visible over the "dosbox.ico" cell.

Тип связи	Смежный объект	Роль смежного объекта
Трассировка	dosbox.ico	Является родителем
Трассировка	dosbox.cpp	Является родителем
Трассировка	Требование к управляемости	Является потомком

АИС УЖЦ: GAP анализ трассировочных связей

ID ошибки	MC21_Требования_Ве...	MC21_Требования_Ве...	→	MC21_Функциональнь...	→	Код
GAP.001			▶	MC21.CDS.SSDD.REQ.0135		Landing Module Steering Module
GAP.002	MC21.CDS.SRS.REQ.0011		→	MC21.CDS.SSDD.REQ.0111	▶	
GAP.003					■	Payment Module
GAP.004	MC21.CDS.SRS.REQ.0032		→	MC21.CDS.SSDD.REQ.0144		■
	MC21.CDS.SRS.REQ.0055		→			Air Condition Module
GAP.005			▶	MC21.CDS.SSDD.REQ.0162	▶	
GAP.006	MC21.CDS.SRS.REQ.0053		→			Autopilot Module
GAP.007		MC21.CDS.SRS.REQ.0024	←	MC21.CDS.SSDD.REQ.0086		

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

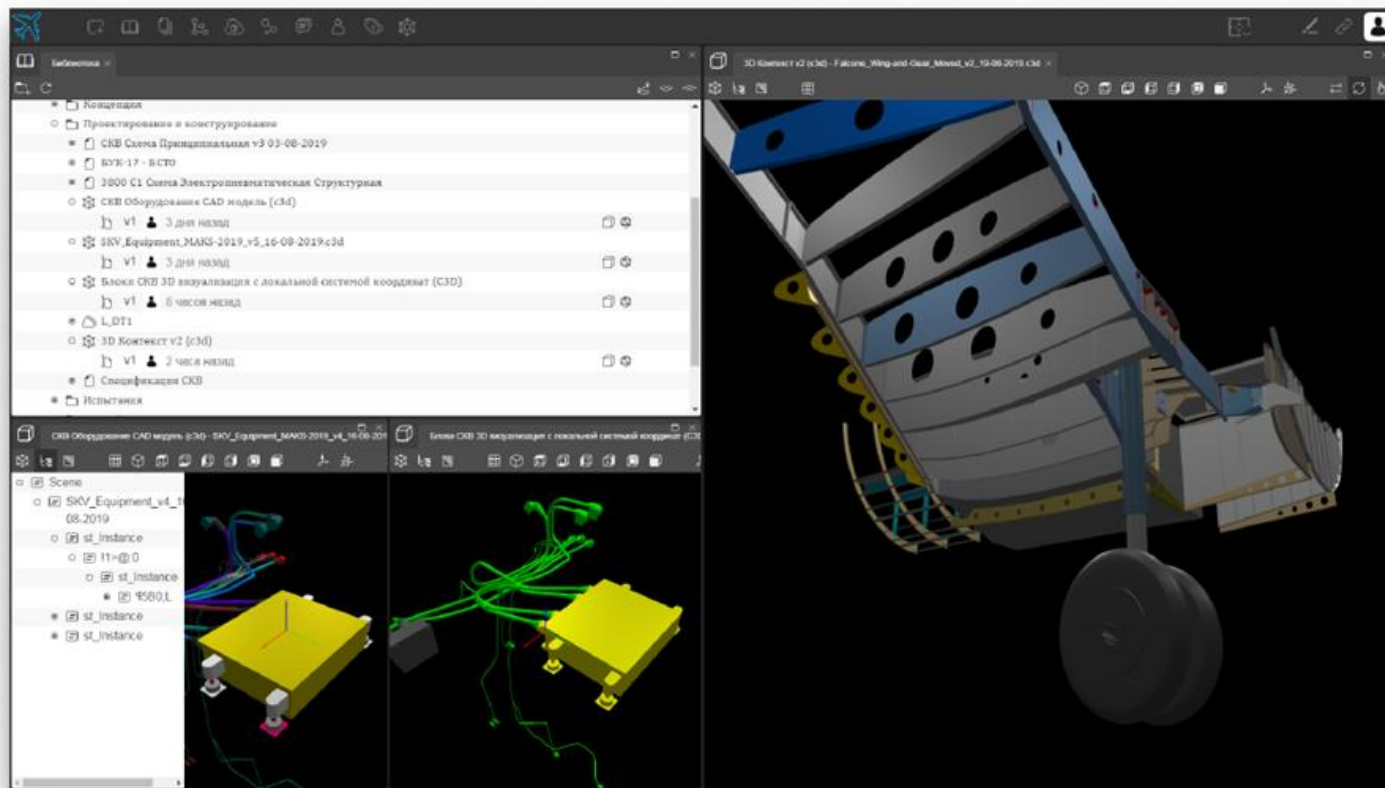
АИС УЖЦ: охват всего ЖЦ

The screenshot displays the АИС УЖЦ (AIS UJC) software interface, which is used for aircraft maintenance and operations. The interface is divided into several panels:

- Top Left Panel:** A navigation menu with a tree structure under the heading "Эксплуатация" (Operation). It includes items like "Настройка параметров СКВ" (SKV parameter settings), "Работа с электронным бортовым журналом" (Work with the electronic flight log), and "Данные инженерно-конструкторского ЭД (СКД)" (Engineering design data).
- Top Middle Panel:** A table titled "Эксплуатация ЭЖК 2.jpg" showing flight data. The table has columns for "Полет" (Flight), "Авиационный номер" (Aircraft number), "Дата" (Date), and "Полетное задание" (Flight task).

Полет	Авиационный номер	Дата	Полетное задание
8	090	06.11.2015	ЗАПЛАНОВАНО ПО ПОСЛЕДОВАТЕЛЬНОСТИ
10	090	06.11.2015	РЕДЕРЖИВАНИЕ В ВОЗДУШНОМ ПРОСТРАНСТВЕ
15	090	06.08.2016	ПРОВЕРКА ПОСЛЕДОВАТЕЛЬНОСТИ
21	700	14.08.2016	ПРОВЕРКА ПОСЛЕДОВАТЕЛЬНОСТИ
- Top Right Panel:** A detailed table titled "БОРТОВОЙ" (Crew/Flight Log) with multiple columns for flight parameters and crew information.
- Bottom Left Panel:** A configuration screen for "Функции ЛА" (Aircraft Functions). It shows a list of functions and their settings, including "Автоматическое регулирование абсолютного давления в кабине" (Automatic cabin absolute pressure regulation).
- Bottom Middle Panel:** A schematic diagram of the cabin pressure control system. It shows a pressure gauge set to "OFF" and a range of "160-212". Below it, a diagram shows air flow from "AVNCS EXTRACT" and "RAM AIR" through "L PACK 100%" and "RECIRC" to the cabin. Cabin temperature is indicated as "18°C".
- Bottom Right Panel:** A diagnostic screen for "Инцидент_Отказ_в_Кабине_2.jpg" (Cabin Failure Incident). It displays "Fault Message Details" for a "Cabin Temperature below minimal value" fault, including the date and time (AUG 7 2019 12:17), flight phase (Cruise), and fault type (Hard).

АИС УЖЦ: совместная работа с САПР



Спасибо за внимание!



ГосНИИАС

ГОСУДАРСТВЕННЫЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ АВИАЦИОННЫХ СИСТЕМ