



**Современные технологии и средства разработки
программного обеспечения
критичных по безопасности систем,
сертифицируемых по требованиям DO-178B**

**Демьянов А.В.
AVD Systems
www.avdsys.ru**





Структура встраиваемого ПО

Прикладное ПО

(наиболее сложная, объемная и часто изменяемая часть)

Подсистема ввода/вывода и драйверы

Операционная система и планировщик

Аппаратура

Затраты на разработку ПО критичных и сертифицируемых по безопасности систем в 4 раза выше, чем ПО обычных встраиваемых систем



Пути снижения стоимости разработки

Прикладное ПО

Автоматизация разработки с помощью квалифицированных (по стандарту безопасности) инструментальных средств

Системное ПО

Применение готовых коммерческих (COTS) сертифицируемых компонент (ОС, сетевой стек, BSP, драйверы)

Прикладное ПО



SCADE

Safety Critical Application Development Environment

Система разработки прикладного ПО критичных и сертифицируемых по безопасности систем управления (SCADE Suite) и систем отображения (SCADE Display)

Системное ПО

WIND RIVER

VxWorks 653

Операционная система для Интегрированной Модульной Авионики (ИМА), удовлетворяющая стандарту ARINC 653 и сертифицируемая по DO-178B



Что такое DO-178B

Это инструктивные материалы (guidelines) по созданию программного обеспечения, выполняющего предписанные ему функции с уровнем доверия к безопасности, удовлетворяющим требованиям летной годности

Эти инструктивные материалы определяют:

- Цели процессов жизненного цикла ПО
- Описание мероприятий и конструктивных соображений для достижения этих целей
- Описание доказательных материалов, подтверждающих, что цели достигнуты

Эти инструктивные материалы изложены в документах:

DO-178B/EUROCAE ED-12B

“Software Considerations in Airborne Systems and Equipment Certification”

МАК КТ-178В

“Требования к программному обеспечению бортовой аппаратуры и систем при сертификации авиационной техники”



DO-178B

Три группы процессов жизненного цикла ПО



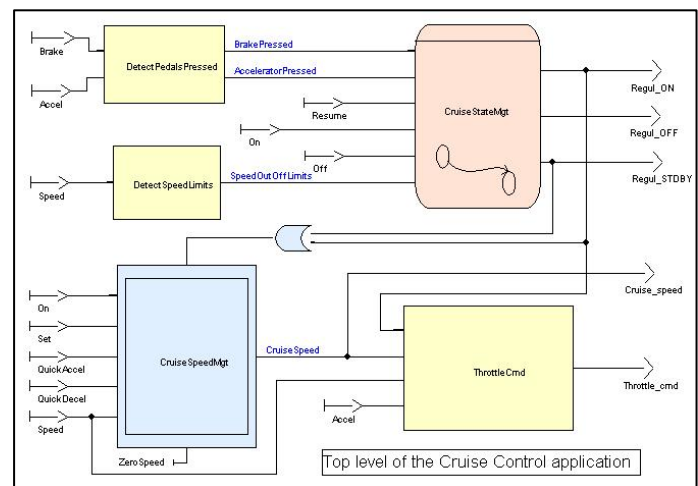
Система разработки/производства **SCADE** фирмы Esterel Technologies предназначена для автоматизации процессов **проектирования, кодирования, интеграции и верификации** ПО встраиваемых компьютерных систем с критичными требованиями к безопасности, сертифицируемых по DO-178B



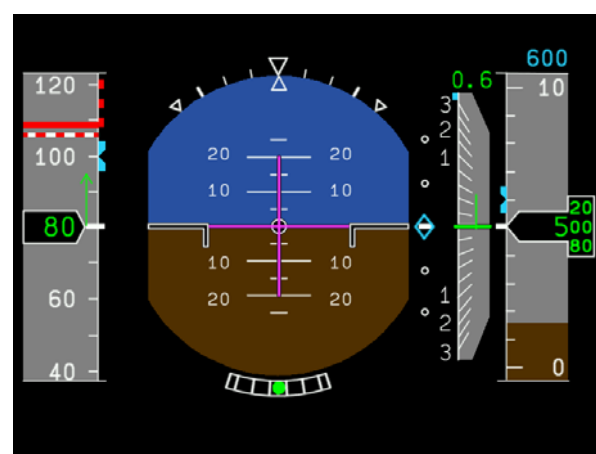
SCADE

Safety Critical Application Development Environment

Для систем управления



Для систем отображения



SCADE Suite KCG
 Квалифицированный по DO-178B
 генератор С-кода

SCADE Display KCG
 Квалифицированный по DO-178B
 генератор вызовов графических функций



SCADE в авиации



55%



25%



20%

Aircraft Braking
Systems

Airbus

AVIC1

Avionika

BAE SYSTEMS

Bundeswehr

CASC

CETC

CS-SI

Dassault Aviation

Diehl Aerospace

EADS Military

EADS Space

Transport

EADS SD&E

Edisoft

Elbit Systems

ELV

ELTA

ESA

Eurocopter

Flight Dynamics

General Electric

Goodrich

GosNIIAS

Hispano-Suiza

Honeywell CRL

Intertechnique

Liebherr-Aerospace

Lockheed Martin

MBDA

NASA

Messier-Bugatti

ONERA

Pratt & Whitney

Rockwell Collins

Rovsing

Saab Avionics

Safran

Sagem

Snecma

Sukhoi (SCAC)

Teuchos

Thales Airborne Systems

Thales Avionics

Turbomeca

Silver Arrow

Silver Software

Smiths Aerospace

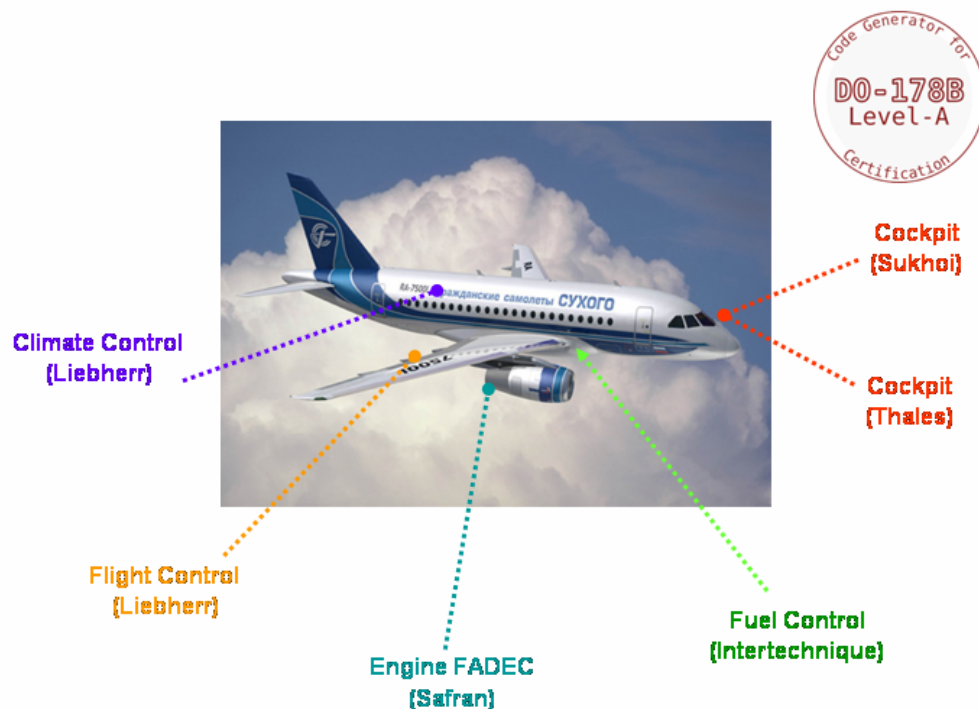
United Arab Emirates Air Force

US Air Force

Ultra Electronics



SCADE Suite и SCADE Display в Superjet 100



Подсистемы разработки ГСС/Thales:

CDS (Cockpit Display System)

Система кабинной индикации

FWS (Flight Warning System)

Система предупреждения экипажа и аварийной сигнализации

DCF (Data Concentration Function)

Система ввода/вывода и концентрации данных

С помощью SCADE сгенерировано в

CDS – 80% (общий объем приложения 240000 строк кода)

FWS – 70% (60000 строк кода)

DCF – 85% (100000 строк кода)

Другие подсистемы SJ100, при разработке которых применялась SCADE:

Система управления полетом (Liebherr)

Система жизнеобеспечения (Liebherr)

Топливная система (Intertechnique)

Система управления FADEC двигателя SaM146 (Snecma)



Структура встраиваемого ПО

Прикладное ПО,
сгенерированное в SCADA
(70-95% всего объема ПО)

«Ручной»
код

Подсистема ввода/вывода и драйверы

VxWorks 653

Операционная система и планировщик

Аппаратура

Wind River VxWorks 653

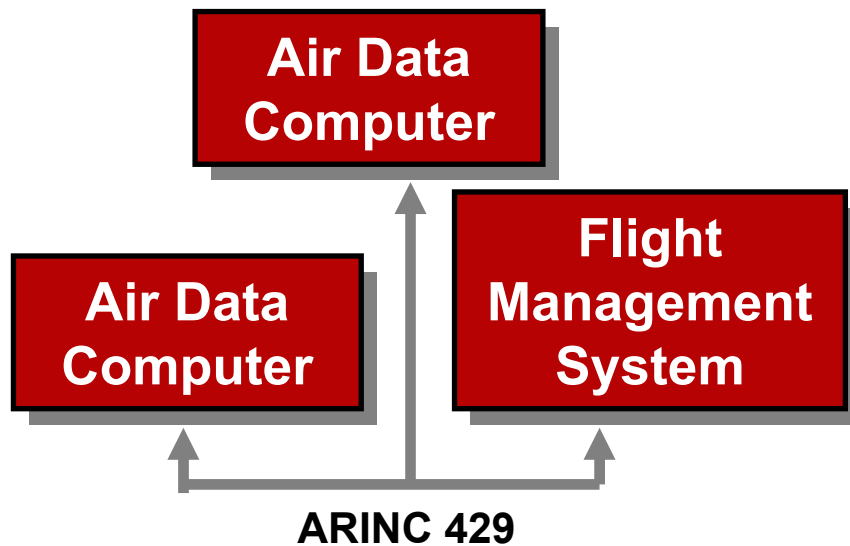
Операционная система для Интегрированной Модульной Авионики (ИМА), удовлетворяющая стандарту ARINC 653 и сертифицируемая по DO-178B



ИМА и ARINC 653

**Федерированная (federated)
Авионика**

**Интегрированная (integrated)
Модульная Авионика**



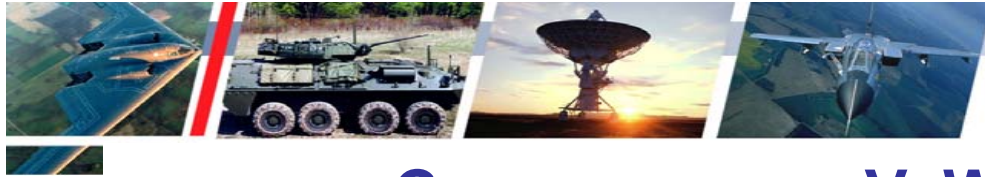
Стандарт ARINC 653 «Avionics Application Software Standard Interface» определяет интерфейс между приложениями и операционной системой, обеспечивающей пространственную и временную изоляцию приложений



WIND RIVER

Архитектура VxWorks 653





WIND RIVER

Состав пакета VxWorks 653 Platform

- Сперационная система **VxWorks 653** в исходных текстах;
- Среда разработки **Workbench for VxWorks 653**, основанная на архитектуре Eclipse;
- Симулятор **VxWorks 653 Simulator**;
- Визуализатор системных событий **System Viewer for VxWorks 653**;
- Пакет для портирования **BSP Porting Kit**;
- **Компилятор конфигурационных XML-описаний** Квалифицирован по DO-178B как средство разработки
- **Средства мониторинга целевой системы** Квалифицированы по DO-178B как средство верификации)
- Техническая поддержка и апгрейд

Дополнительные компоненты:

- Сертификационный пакет **Certification Evidence**, в который входят все артефакты (материалы) по операционной системе VxWorks 653, требуемые для предоставления в органы по сертификации.
- Сертифицируемый по DO-178B Level A сетевой стек **UDP/IPv4** и его сертификационный пакет

Wind River Workbench

Integrated Partner Software

VxWorks 653

Hardware Support (PowerPC)

Support, Training, Professional Services



ARINC653/DO-178B проекты на VxWorks



Boeing 787



Boeing KC-767A



Eurocopter EC-225/EC-725



Boeing C130 AMP



Boeing P-8A MMA



Airbus A400M



Northrop Grumman X47B



Airbus A330 MRTT

**Более 30 проектов с сертификацией
по различным Уровням DO-178B**



Boeing 787 Common Core System (CCS)



- Разработчики CCS: Smiths Aerospace и еще 11 поставщиков
- Около 60 приложений, включая flight management, breaks, cabin pressure, displays, fuel management, health management, landing gear, steering, thrust reversers
- ARINC 653 и различные Уровни DO-178B



WIND RIVER

VxWorks 653

Поддерживаемые микропроцессоры PowerPC

Семейство PowerPC	Микропроцессоры
7xx	750GX, 750FX, 755
74xx	7410, 7447, 7455, 7457
82xx	8245, 8260, 8270
83xx	8349E
85xx	8541E, 8560
86xx	8641 (single core)



Резюме

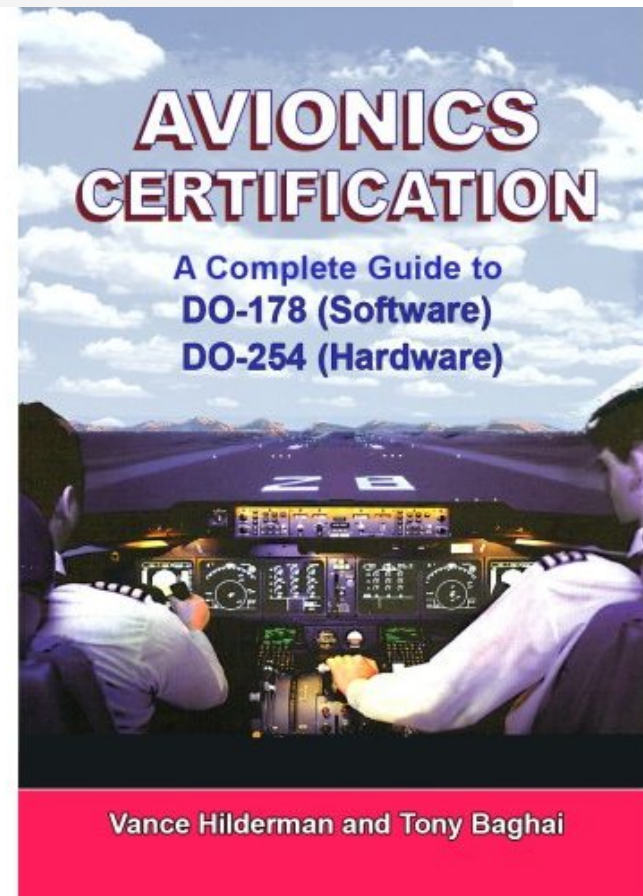
Применение готовых коммерческих (COTS) сертифицируемых по DO-178В программных компонент и квалифицированных по требованиям DO-178В средств разработки значительно сокращает сроки и снижает стоимость разработки и сертификации проектов с критичными требованиями к безопасности и снижает степень риска



**Сертификация авионики
Полное руководство по
DO-178В (программное обеспечение)
DO-254 (аппаратура)**

www.bolero.ru (www.amazon.com)

**Тренинги по DO-178В и DO-254
Ближайший тренинг в Европе:
28-29 апреля, Лондон**





Дополнительная информация

AVD Systems

www.avdsys.ru

Esterel Technologies

www.esterel-technologies.com

Wind River

www.windriver.com

