

А.В. Демьянов, АВД Системс

## Технологии разработки авиационных систем с критичными требованиями к безопасности

### Часть 2. Средства автоматической генерации сертифицированного программного кода

*В статье представлены современные тенденции в архитектуре авиационной электроники (авионики) и рассмотрен вопрос влияния стандартов интегрированной модульной авионики (ИМА) на развитие коммерческих операционных систем реального времени и средств разработки программного обеспечения с критичными требованиями к безопасности (часть 1). Автор анализирует современные средства автоматической генерации ПО сертифицируемых авиационных систем (часть 2), а также приводит примеры применения нового модульного стандарта VPX для построения ИМА (часть 3).*

#### Вступление

В условиях всё возрастающих требований к безопасности авиационных (и не только) систем, всё более важную роль играют и всё более широкое применение находят средства автоматической генерации программного кода, исключаяющие ошибки кодирования и значительно сокращающие сроки разработки и сертификации. В настоящее время наиболее распространенным средством разработки/производства ПО критичных по безопасности систем является комплекс SCADE (Safety Critical Application Development Environment) фирмы Esterel Technologies (Франция). Он применяется в авиации более чем 60 пользователями, в том числе и в России: в ГосНИИАС для исследовательского проекта по архитектуре ИМА, МНПК «Авионика» для Бе-200 и ГСС (Гражданские Самолёты Сухого) для SuperJet 100.

В индустрии разработки ПО авиационных встроенных компьютерных систем (управление полётом, торможением, дисплеями кабины и т.д.) традиционно сложилась следующая технологическая цепочка: функции и архитектура определяются системными инженерами, соответствующие законы управления формируются инженерами по системам управления с использованием нотаций на базе блок-схем или конечных автоматов, а программное обеспечение разрабатывается инженерами-программистами уже в текстовом виде и кодируется вручную на языках C или Ada.

В этой ситуации автоматическая генерация кода из формальных моделей является технологией, которая может оптимизировать процесс разработки и обеспечить при этом необходимую степень безопасности приложения. Идея состоит в том, чтобы описать приложение и его законы управления программной моделью и автоматически сгенерировать из этой модели программный код (на

пример, на языке C), используя квалифицированный – в смысле стандарта DO-178B – кодогенератор и внести, таким образом, в жизненный цикл разработки программного изделия значительные усовершенствования.

#### DO-178B и процессы жизненного цикла программного продукта

Прежде чем какой-либо программный продукт будет допущен к работе на борту гражданского самолёта, он должен пройти процедуру сертификации – подтверждения соответствия требованиям обеспечения безопасности, изложенных в руководстве DO-178B «Software Considerations in Airborne Systems and Equipment Certification». Руководство DO-178B используется производителями авиационного оборудования при разработке ПО и контролирующими органами при его сертификации. Органами по сертификации являются FAA (Federal Aviation Administration) в США, EASA (European Aviation Safety Agency) в Европе и МАК (Межгосударственный Авиационный Комитет) в России и СНГ. Документ DO-178B подготовлен и опубликован в 1992 году организацией RTCA (Radio Technical Commission for Aeronautics). В Европе этот документ имеет аналог под названием ED-12B, подготовленный организацией EUROCAE, а в России – КТ-178B, подготовленный в НИИ Авиационного Оборудования.

В руководстве DO-178B определены три группы процессов жизненного цикла программного продукта (рис. 1):

- процессы планирования (planning);
- процессы разработки (development);
- процессы интегральные (integral).

Группа процессов разработки включает в себя процесс определения требований (requirements), процесс проектирования (design), процесс кодирования (coding)



Рис. 1. Процессы жизненного цикла по DO-178B

Рис. 2. Область применения SCADE – прикладная часть ПО

и процесс интеграции (integration). В группу интегральных процессов попадают процесс верификации (verification), процесс управления конфигурацией (configuration management), процесс гарантии качества (quality assurance) и процесс взаимодействия с сертифицирующим органом (certification liaison).

Система разработки/производства сертифицированного ПО SCADE (Safety Critical Application Development Environment) фирмы Esterel Technologies предназначена для автоматизации процессов проектирования, кодирования, интеграции и верификации ПО встраиваемых компь-

ютерных систем с критичными требованиями к безопасности.

### SCADE – система разработки/производства сертифицированного ПО

Система SCADE предназначена для разработки прикладной части встроенного ПО, которая составляет от 70% до 95% всего ПО (рис. 2).

Система SCADE представляет собой систему модельно-ориентированного проектирования, использующую формальные нотации в виде блок-схем алгоритмов и конечных автоматов для описания поведения (рис. 3). После отладки управляющей

системы на уровне моделей применяется генератор С-кода, квалифицированный по DO-178B. Автоматическая генерация сертифицированного кода позволяет значительно сократить затраты на этапе сертификации, а отсутствие ручного кодирования позволяет избежать ошибок и сократить время разработки и верификации программного продукта.

Система SCADE включает в себя два комплекта средств разработки:

- **SCADE Suite** – комплект средств для разработки систем управления;
- **SCADE Display** – комплект средств разработки систем отображения.

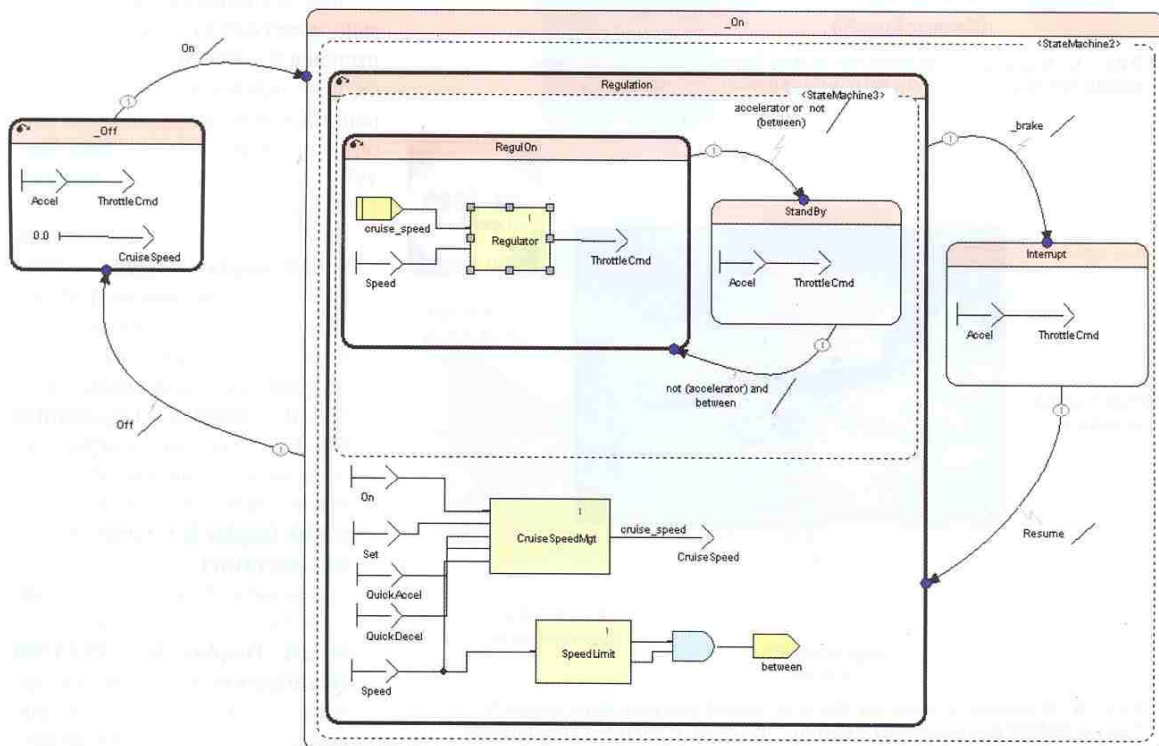


Рис. 3. Модельно-ориентированное проектирование в SCADE

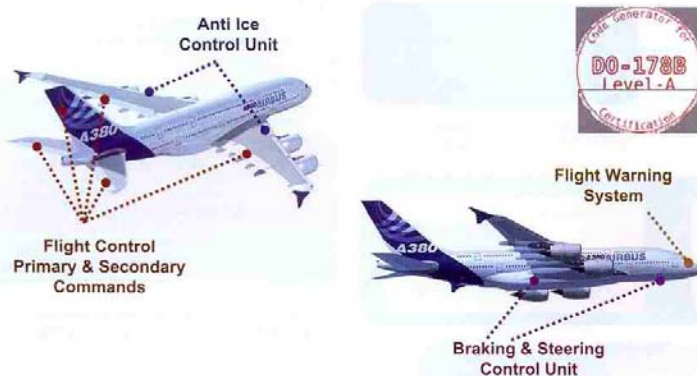


Рис. 4. В самолёте A380 SCADE применяется в системе управления полётом, в системе предупреждения экипажа, в системе рулевого управления и торможения, в системе антиобледенения и др.



Рис. 5. В самолёте Boeing 787 SCADE используется в системе управления шасси и в системе управления торможением

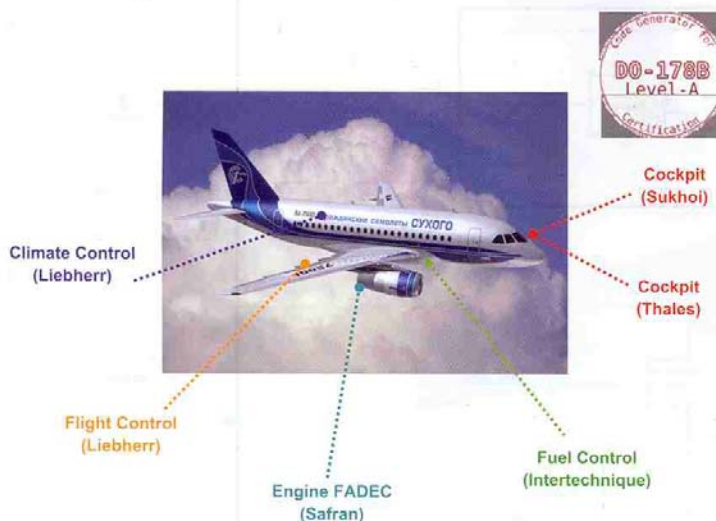


Рис. 6. В самолёте SuperJet 100 компании Гражданские Самолёты Сухого SCADE применяется в кабине экипажа, в системе управления полётом, в топливной системе, в системе управления двигателями и в системе климат-контроля

В комплект SCADE Suite входят следующие основные компоненты:

- SCADE Advanced Modeler – система ввода из библиотеки графических моделей, средства проектирования системы управления и её моделирования;
- SCADE Design Verifier – верификатор дизайна;
- SCADE Model Test Coverage – анализатор полноты покрытия при тестировании на уровне моделей;
- SCADE Configuration Management Gateway – шлюз к системам управления конфигурацией;
- SCADE Suite Requirement Management Gateway – шлюз к системам управления требованиями;
- SCADE Suite KCG (Qualified Code Generator) – генератор С-кода, квалифицированный по стандарту DO-178B до Уровня А;
- SCADE Suite KCG DO-178B Qualification Kit – комплект артефактов (материалов), предъявляемых при прохождении процесса сертификации по DO-178B;
- SCADE Suite Compiler Verification Kit – система тестирования выбранного компилятора.

Код, сгенерированный в SCADE Suite, может работать как в среде операционной системы, так и на «без-ОСовой» целевой машине. Кодогенератор SCADE Suite KCG поддерживает операционные системы Wind River VxWorks 653, Green Hills Integrity-178B и др.

В комплект SCADE Display вошли:

- SCADE Display Modeler – система ввода из библиотеки графических объектов, компоновки графического пользовательского интерфейса и его моделирования;
- SCADE Display Ergonomics Checker – система проверки требований эргономики и учёта влияния человеческого фактора;
- SCADE Display KCG (Qualified Code Generator) – генератор С-кода, квалифицированный по стандарту DO-178B до Уровня А;
- SCADE Display KCG DO-178B Qualification Kit – комплект артефактов (материалов), предъявляемых при прохождении процесса сертификации по DO-178B.

Кодогенератор SCADe Suite KCG поддерживает графическую библиотеку SGL фирмы Thales и открытый стандарт OpenGL SC (Safety Critical), а также может быть настроен на нестандартную графическую библиотеку, разработанную самими пользователями.

### Примеры применения SCADe Suite и SCADe Display

#### Airbus A380

Система SCADe является де-факто стандартом в компании Airbus. Она применяется для разработки систем самолётов A340, A380 и A400M. Например, в самолёте A380 SCADe применяется в системе управления полётом, в системе предупреждения экипажа, в системе рулевого управления и торможения, в системе антиобледенения и др. В более чем десяти различных системах A380 с помощью SCADe сгенерировано 8 млн строк исходного кода (рис. 4).

#### Boeing 787

В самолёте Boeing 787 SCADe применяется в системе управления шасси (разработчик Smiths Aerospace) и в системе управления торможением (разработчик Messier Bugati) (рис. 5).

#### Сухой SuperJet 100

В самолёте SuperJet 100 компании Гражданские Самолёты Сухого SCADe применяется в кабине экипажа (Сухой и Thales), в системе управления полётом (Liebherr), в топливной системе (Intertechnique), в системе управления двигателями (Safran) и в системе климат-контроля (Liebherr) (рис. 6).

**Затраты, приходящиеся на различные этапы разработки программного обеспечения авиационных систем, и их сокращение при использовании SCADe**

Этап разработки проекта	Доля затрат (по данным AGARD)	Экономия при применении SCADe (по данным пользователей SCADe)
Определение концепций	5%	0%
Системное проектирование	12%	0%
Разработка системных требования к ПО	14%	50%
Проектирование ПО (детализация спецификаций)	15%	50%
Кодирование	10%	70%
Модульное тестирование	12%	70%
Интеграционное тестирование	7%	30%
Системное тестирование	10%	30%
Документирование	15%	70%
Суммарная экономия от применения SCADe		46%

### Экономический эффект от применения SCADe

В таблице приведены данные американской организации AGARD (Advisory Group for Aerospace R&D) по затратам, приходящимся на различные этапы разработки программного обеспечения авиационных систем. Рядом с ними приведены данные пользователей SCADe о степени сокращения их затрат на этих этапах разработки проекта. Суммарное сокращение затрат на проект составляет 46%.

## Новости рынка встраиваемых систем

*Продолжение. Начало на стр. 31*

визуализации, игровое оборудование, кассовые аппараты и информационные терминалы, а также разнообразная компьютерная техника, которая устанавливается на улицах, в общественных зданиях и жилых домах.

### Спецификация

Впервые стандарт UGM был анонсирован на выставке Embedded World в Нюрнберге (Германия) в феврале 2007 года.

Модули UGM имеют размеры 84 x 95 мм и способны поддерживать самые передовые на сегодняшний день средства визуализации. Они устанавливаются на базовую плату параллельно ей, что выгодно отличает их от видеокарт, вставляющихся в слоты расширения перпендикулярно. Такой монтаж экономит свободное пространство, позволяя создавать гибкие низкопрофильные решения. При этом модули UGM имеют гарантии доступности на

рынке не менее трёх-пяти лет. Изделия стандарта UGM комплектуются необходимыми драйверами, и их очень легко интегрировать в разрабатываемые системы.

Шина PCI Express и видеоинтерфейсы у UGM выведены в 220-контактный разъём того же типа, что используется на одноплатных компьютерах-модулях COM Express/ETExpress. Через этот разъём идёт двусторонняя передача данных PCI Express x1/4/8/16 (PCI Express Graphics) и видеосигналов. Графический процессор модуля UGM поддерживает видеопамять объёмом до 1 Гбайт. Спецификация UGM 1.0 позволяет осуществлять вывод видео и графики через двоянные порты LVDS, выходы DVI и порты VGA.

Модули UGM могут питаться от напряжения 12... 22 В и иметь энергопотребление до 72 Вт. Этого вполне достаточно для обеспечения быстрой работы самых передовых графических алгоритмов и адекватной поддержки самых современных игр.

*Окончание на стр. 83*