А.В. Демьянов, АВД Системс

Технологии разработки авиационных систем с критичными требованиями к безопасности. Часть 1

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 приводит примеры применения нового модульного стандарта VPX для построения ИМА (часть 2), а также анализирует современные средства автоматической генерации ПО авиационных систем с критичными требованиями к безопасности (часть 3).

Вступление

Многие системы авионики были успешно созданы с использованием специально разработанного аппаратного и программного обеспечения. Но в последние годы стоимость полного жизненного цикла таких разработок перестала удовлетворять производителей авионики, в связи с чем наметилась тенденция к построению систем из коммерческих (COTS – Commercial Of The Shelf) аппаратных и программных компонентов. В то же самое время начался процесс отхода от традиционной технологии построения систем авионики, в соответствии с которой каждая подсистема выполняла отдельную функцию и была реализована как отдельных аппаратный блок. В зарубежной литературе такая авионика называется «федерированная» (от слова federated – отдельные самостоятельные, объединённые между собой), и хотя такого русского авиационного термина, судя по всему, нет, всё-таки будем его использовать, поскольку он помогает глубже понять смысл термина «интегрированная».

Новый подход, получивший название Интегрированная Модульная Авионика (ИМА), предлагает строить функциональные подсистемы из набора модулей стандартных форматов: не разрабатывать каждый раз специализированную аппаратную платформу, а конфигурировать систему под выполнение данной функции. Концепция ИМА предусматривает также выполнение на одной аппаратной платформе нескольких прикладных функций, что значительно снижает параметр SWaP (Space, Weight and Power) – габариты, вес и потребляемую мощность бортовых авиационных систем. О том, почему новый модульный стандарт VPX наиболее подходит для построения систем интегрированной модульной авионики (по сравнению с традиционными форматами VME и CompactPCI), мы поговорим во второй части этой статьи.

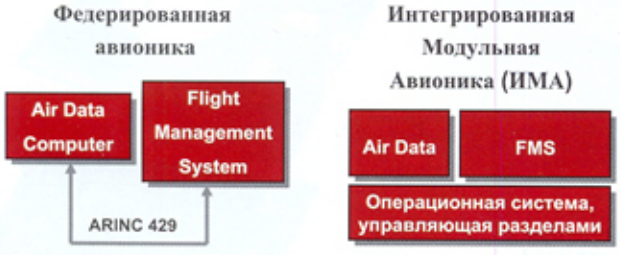

Рис. 1. Федерированная авионика и интегрированная авионика

Для того чтобы на одной аппаратной платформе могли выполняться несколько функциональных приложений, концепция ИМА определяет уровень абстракции, изолирующий приложение от конкретной аппаратной платформы и приложения друг от друга. Этот уровень абстракции определён стандартом ARINC 653 и обеспечивается операционной системой, удовлетворяющей этому стандарту, например, операционной системой VxWorks 653 фирмы Wind River или LynxOS-178 фирмы LynuxWorks. Операционные системы для ИМА должны также удовлетворять и быть сертифицируемыми по стандарту безопасности RTCA DO-178B. В настоящее время VxWorks 653 применяется, например, в самолётах Airbus A400M и MRTT, Boeing 787 Dreamliner, KC767A и C-130 AMP и Saab Grippen, вертолётах Eurocopter EC-225/EC-725 и беспилотнике Northrop Grumman X-47B, а LynxOS-178 – в самолёах Bombardier Challenger, KC-135 Stratotanker, KC-767 и F-35 JSF (по информации на сайтах фирм). Объём продаж Wind River на рынке аэрокосмических/оборонных систем составляет, по данным годового финансового отчёта фирмы, 25% от общего объёма продаж (285 млн долларов). Финансовые показатели фирмы LynuxWorks на сайте не опубликованы.

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, исключающие ошибки кодирования и значительно сокращающие сроки разработки и сертификации. В настоящее время наиболее распространённой системой 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 ГосНИИ-

АС для исследовательского проекта по архитектуре ИМА, МНПК «Авионика» для Бе-200 и ГСС (Гражданские Самолёты Сухого) для SuperJet 100. О комплексе SCADE мы поговорим в третьей части этой статьи.

Стандарт ARINC 653 и ОС VxWorks 653

Спецификация стандарта ARINC 653 была опубликована в середине 90-х годов. Первой реализацией концепций ИМА и стандарта ARINC 653 была система AIMS (Airplane Information Management System), разработанная фирмой Honeywell для Boeing 777 и сертифицированная в 1995 году. Система AIMS работает под управлением собственной ОС фирмы Honeywell, которая реализует временное и пространственное разделение приложений по стандарту ARINC 653.

Рассмотрим современную коммерческую реализацию стандарта ARINC 653 на примере операционной системы VxWorks 653 и её применения в центральной компьютерной системе CCS (Common Core System) Boeing 787, созданной фирмой Smith Aerospace. Всего в разработке участвовало 11 фирм-субподрядчиков Smith. На CCS исполняется более 60 различных функциональных приложений.

Пространственное Разделение (Spatial Partitioning)

Пространственное разделение необходимо для изоляции друг от друга приложений, реализованных на одной и той же аппаратной платформе: приложение, исполняющееся в одном разделе (partition), не должно иметь доступа к ресурсам приложений, исполняющихся в другом разделе. Для реализации разделов обычно используются различные виртуальные адресные пространства. Их защита обеспечивается процессорным устройством управления памятью MMU (Memory Management Unit). Приложение состоит из Процессов, исполняющихся в одном Разделе. Планирование их исполнения управляется операционной системой Раздела (Partition OS). Разделы исполняются на аппаратной платформе – Модуле. И планирование исполнения разделов и коммуникация между разделами управляются операционной системой Модуля (Module OS).

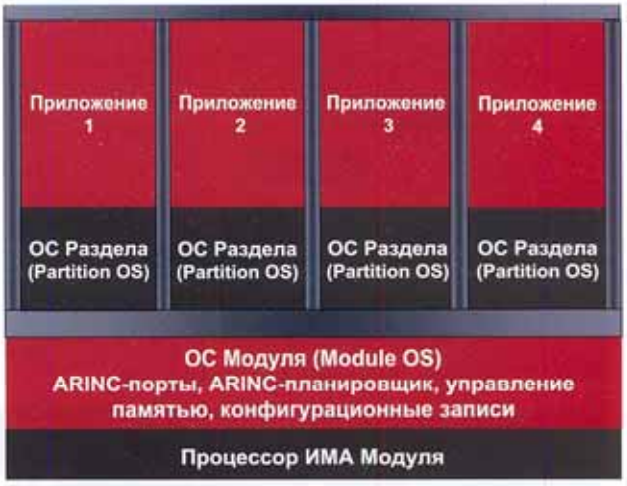

Рис. 2. ОС Раздела и ОС Модуля

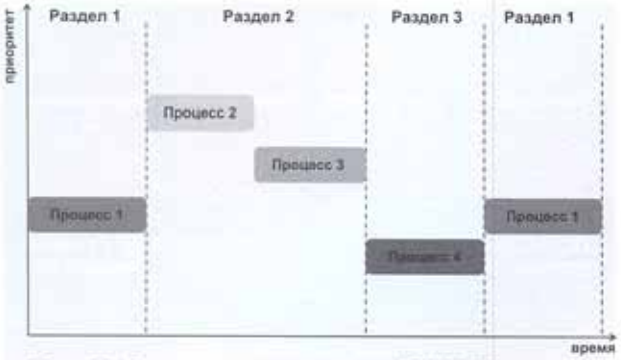

Рис. 3. Временное разделение в ARINC 653

Временное Разделение (Temporal Partitioning)

Одного пространственного разделения недостаточно, чтобы обеспечить полную изоляцию приложений. Для того чтобы одно приложение не могло «узурпировать» процессор и, таким образом, повлиять на выполнение другого приложения, применяется временное разделение. Каждому Разделу отводится промежуток времени (одинаковой или различной длительности) для исполнения, по истечении которого планировщик передаёт исполнение другому Разделу. Планировщик Разделов находится в ОС Модуля, планировщик Процессов внутри раздела – в ОС Раздела. Внутри Разделов применяется планирование по приоритету (priority-based scheduling).

Расширения планировщика VxWorks 653

Планировщик VxWorks 653 полностью совместим с ARINC 653 Supplement 1 (653-1). Он также поддерживает планирование по режиму (mode-based scheduling), алгоритм которого был предложен совместно Wind River и Smith Aerospace для включения в будущую спецификацию ARINC 653 Supplement 2. Планирование по режиму допускает смену алгоритма планирования в зависимости от режима полёта. Всего может быть 16 различных алгоритмов планирования по режиму.

При временном разделении в ARINC 653 возможны ситуации, когда все процессы Раздела выполнились, а временной интервал, выделенный данному Разделу, ещё не истёк. При этом образуются простои (slacks) – свободное время в неактивном Разделе. Планировщик VxWorks позволяет предоставлять назначенным Разделам возможность захвата простоев (slack stealing) других Разделов.

Средства разработки для VxWorks 653

Операционная система VxWorks 653 поставляется в составе интегрированного пакета Wind River Platform for Safety Critical ARINC 653, в который входят следующие компоненты:

- операционная система VxWorks 653 в исходных текстах;
- Workbench for VxWorks 653 – интегрированная среда разработки, основанная на архитектуре Eclipse;
- Симулятор VxWorks 653;
- Визуализатор системных событий System Viewer for VxWorks 653;
- Пакет для портирования VxWorks 653 BSP Porting Kit.

Интегрированные пакет Platform SC ARINC 653 поставляется по модели лицензирования «годовая подписка». Она позволяет снизить стартовые затраты на разработку и распределить их на несколько лет, в течении которых ведётся проект.

Для этапа сертификации Wind River поставляет пакет DO-178B Level A/B/C/D Certification Evidence. В него входят все артефакты (материалы) по операционной системе VxWorks 653, необходимые для предоставления в органы по сертификации.

Поддерживаемые аппаратные платформы

Операционная система VxWorks 653 поддерживается для семейств архитектуры PowerPC IBM PPC750GX, Freescale MPC7xx, 74xxx, 82xx, 85xx. Она портирована на платы Aitech, Curtiss-Wright, CES, Lockheed Martin, Motorola, Radstone, а также на отладочные платы Wind River: SBC7447 (MPC7447), SBC7457 (MPC7457), PPMC7xx (MPC750/755), PPMC74xx (MPC74xx), SBC750GX (PPC750GX), PPMC8245 (MPC8245), SBC PowerQUICCII for MPC8270 (MPC8270) и SBC PowerQUICCII for 8260 (PPC 8260).

(Продолжение в следующем номере)