

Аспекты изоляции приложений в ARINC 653

Земкин Валерий Александрович, vazemkin@gosniias.ru
ФАУ ГосНИИАС,
125319, г. Москва, ул. Викторенко, 7, к. 2.

В рамках проекта ГосНИИАС при участии ИСП РАН им. В.П. Иванникова и ИПМ им. М.В. Келдыша РАН ведется работа по созданию операционной системы реального времени JetOS для применения в бортовых системах гражданской авиации, в частности, в системе индикации импортозамещенных воздушных судов MC-21 и SJ-100. Основным программным интерфейсом JetOS является интерфейс ARINC 653, который будет далее рассмотрен более подробно.

Основной целью ARINC 653 [1] является определение универсального интерфейса (API) APEX (APplication/EXEcutive) между операционной системой (ОС) и прикладным программным обеспечением (ПО) – в частности, в рамках интегрированной модульной авионики (integrated modular avionics, IMA). ARINC 653 также включает в себя требования к интерфейсу между ПО и ОС, и список сервисов, которые позволяют прикладному программному обеспечению управлять расписанием, взаимодействием и информацией о состоянии его внутренних элементов (объектов). Интерфейс APEX обеспечивает общую логическую среду для ПО, которая позволяет независимо созданным приложениям выполняться вместе на одном и том же оборудовании. Это достигается с помощью разделения приложений авионики для сдерживания ошибок и сбоев системы. Единица разделения называется разделом. Раздел по сути то же самое, что и программа в среде одного приложения: он включает в себя данные, собственный контекст выполнения, атрибуты конфигурации и т.д.

Основной вопрос, который необходимо решить при разработке ОСРВ, заключается в построении системы по концепции изоляции, а именно надежного разделения ресурсов и времени. В ARINC 653 представлена реализация такой концепции согласно DO-248C [2] и CAST-32A [3]. Для надежного разделения ресурсов необходимо, чтобы:

- Программные разделы не могли повреждать области хранения для кода, ввода-вывода или данных других разделов.
- Программные разделы не могли потреблять больше, чем им выделено от общих ресурсов.
- Сбои оборудования, уникальные для программного раздела, не могли оказывать негативного воздействия на другие программные разделы.

Надежное разделение по времени достигается, когда:

- На одноядерном процессоре ни одному разделу программного обеспечения не разрешено использовать больше отведенного ему времени выполнения.
- На многоядерном процессоре, в результате уменьшения интерференции времени между разделами, размещенными на разных ядрах, ни одному разделу программного обеспечения не разрешено использовать больше отведенного ему времени выполнения на ядре, на котором он выполняется.

Тем самым интерфейс APEX обеспечивает временное и пространственное разделение ресурсов. Единицей планирования ресурсов является раздел. Каждый раздел получает как временные ресурсы (процессорное время), так и «пространственные» (часть ёмкости ОЗУ). В рамках раздела возможно организовать выполнение нескольких процессов / потоков.

Спецификация ARINC 653 предоставляет ряд сервисов, обеспечивающих работу с разделами и процессами; данные сервисы можно разделить по следующим направлениям:

- Управление разделами (partition management), временем (time management) и процессами (process management).
- Взаимодействие между разделами (interpartition communication) и между процессами внутри одного раздела (intrapartition communication).
- Планирование разделов (partition scheduling) и процессов (process scheduling).

- Монитор состояния и обработка ошибок на разных уровнях (процесс, раздел, модуль).

Следует отметить, что хотя ARINC 653 был разработан для использования в системах авионики, он в равной степени подходит для любой системы, которой требуются API-сервисы и механизмы разделения, позволяющие нескольким приложениям (с одинаковыми или разными уровнями безопасности) работать на аппаратном обеспечении целевой платформы.

Список литературы:

- [1] ARINC Specification 653P0-3. Avionics Application Software Standard Interface Part 0. Overview of ARINC 653. — AEEC : SAE-ITC, 2021. — 51 стр.
- [2] DO-248C. Supporting Information for DO-178C and DO-278A.— RTCA : SC-205, 2011. — 166 стр.
- [3] CAST-32A. Multi-core Processors. — The Federal Aviation Administration : Certification Authorities Software Team, 2016. — 23 стр.