Обеспечение надёжной пространственной изоляции процессов посредством системы статического распределения памяти

В. Ю. Чепцов cheptsov@ispras.ru, С. А. Зеленова sophia@ispras.ru, М.В.Доледёнок doledenok@ispras.ru

Институт системного программирования им. В.П. Иванникова РАН, Москва

В работе рассматриваются вопросы статического распределения памяти в целях надёжной пространственной изоляции процессов.

В настоящее время стандартом становится использование архитектур систем реального времени, в которых различные приложения могут выполняться на одном и том же оборудовании, что способствует снижению требований к энергопотреблению, веса, других технических характеристик, а также затрат на техническое обслуживание.

Одним из стандартов, регулирующих системы подобного рода, является ARINC 653, описывающий компоненты интерфейса между приложениями интегрированной модульной авионики (IMA) и операционной системой. Надёжность системы в ARINC 653 обеспечивается, в частности, за счёт пространственной изоляции. Понятия ARINC 653 являются достаточно общими и могут быть применены не только в модульной авионике, но и в гораздо более широком классе встроенных систем.

Авторами в ходе создания ОСРВ семейства КЛОС на базе ARINC 653 разработана система изоляции, отвечающая требованиям стандарта ARINC 653, имеющая следующие особенности:

- учитываются как требования на память со стороны операционной системы, так и требования на память со стороны разработчика ПО, в промышленном применении учёт таких деталей необходим;
- понятия, используемые для описания особенностей архитектуры и требований операционной системы на память, являются общими, что позволяет упростить разработку для новых платформ;
- требования на память формулируются разработчиком ПО в терминах, не зависящих от аппаратного обеспечения, что даёт высокую переносимость программного обеспечения;
- описание требований на память обладает широкими возможностями, есть поддержка виртуальной памяти, разделяемой памяти, инструментации кода, выравнивания адресов, ограничения на области физической памяти и др.;
- техническая поддержка системы изоляции включает инструмент автоматической генерации статической раскладки памяти по конфигурации памяти и заданным требованиям на память;
- дополнительный контроль использует инструменты обеспечения корректности системных требований на память, проверки корректности и согласованности требований на память и проверки соответствия статической раскладки памяти описанным требованиям.