

Система программирования GNAT: поддержка сертификации программных продуктов на основе стандарта DO-178B

С.И. Рыбин
консультант компании AdaCore,
ст.н.с, к.ф-м.н, НИВЦ МГУ, Москва,
rybin@adacore.com

Ада (ISO/IEC 8652) - язык программирования, специально созданный в начале 80-х годов прошлого века для применения в области больших встроенных систем реального времени с повышенными требованиями к надежности (с момента своего создания Ада претерпела две серьезные ревизии и является в настоящее время мощным универсальным индустриальным языком - <http://www.adaic.com>). Современные применения основанных на Аде технологий разработки программного обеспечения (ПО) включают значительное количество проектов в аэрокосмической области. Требования к надежности и безопасности ПО, применяемого в аэрокосмических системах, как правило, включают обязательную сертификацию программных систем. Часто в качестве основы для программ и процедур сертификации используется стандарт DO-178B. Этот стандарт содержит процедуры и требования к сертификации, которые имеют много общего с применяемыми в других системах сертификации ПО, требования к надежности которого являются критичными.

Сертификация ПО на базе DO-178B (или аналогичных стандартов) предполагает демонстрацию и обоснование того, что сертифицируемая система обладает рядом заявленных свойств. Сертификация - это длительная, трудоемкая и, следовательно, дорогостоящая процедура, требующая высококвалифицированного персонала. Значительные усилия тратятся на таких этапах сертификации, как:

- тестирование: для тестирования, проводимого в рамках сертификации ПО, во-первых, требуется выбор конкретного критерия полноты (обычно это тот или иной критерий структурного тестирования), а во-вторых, требуется доказать, что проведенная процедура тестирования обеспечивает выполнение выбранного критерия для тестируемого ПО;
- проверка соответствия кода ПО определенному стандарту кодирования, как правило, стандарт кодирования призван обеспечить отсутствие в тексте ПО нежелательных по тем или иным причинам языковых конструкций и их сочетаний (например, стандарт кодирования может запрещать конструкции, снижающие ясность и структурированность кода, ведущие к неконтролируемому росту динамической памяти и т.п.);

Система программирования GNAT (<http://www.adacore.com>) в настоящее время является одной из основных индустриальных систем программирования на базе языка Ада. Система поддерживает все ревизии стандарта ISO/IEC 8652. Среди пользователей системы GNAT такие компании, как Raytheon, Boeing, BAE Systems, EADS, Eurocontrol, Indra, Lockheed Martin, MBDA, Thales. GNAT-технология реализована на всех современных индустриальных платформах, имеется возможность кросс- компиляции для встроенных архитектур на базе Embedded Linux, PikeOS, Nucleus OS, LynxOS, VxWorks. Среди проектов, разрабатываемых на основе GNAT-технологии, немало таких, для которых сертификация на основе стандарта DO-178B (или аналогов) является актуальной. На сайте компании AdaCore, разработчика GNAT-технологии, содержится обзор некоторых проектов, выполняемых клиентами компании, среди них:

- модернизация транспортного самолета C-130J (Lockheed Martin);
- система определения положения в пространстве для Airbus A350 (Thales);
- Thales – встроенное ПО для перископов подводных лодок;
- система предупреждения конфликтов при управлении воздушным движением (Lockheed Martin);
- боевое корабельное ПО (Raytheon);
- Boeing - 787 Dreamliner
- BAE Systems – бортовое ПО для европейского истребителя (Eurofighter Typhoon)
- MBDA – встроенное ПО для компонент международной космической станции.

В рамках каждого из этих проектов практически наверняка потребуются сертификация тех или иных программных компонент.

Стандарт DO-178B разрешает на определенных условиях использование программных инструментов для выполнения тех или иных действий, связанных с сертификацией ПО. Автоматизация наиболее ресурсоемких шагов процесса сертификации позволяет на порядки сократить требуемые временные, человеческие и финансовые ресурсы.

В ответ на пожелания клиентов предоставить решения и инструменты, облегчающие и автоматизирующие действия по стандартизации ПО, AdaCore специально разработала в рамках GNAT-технологии следующие решения:

- **Конфигурируемая библиотека периода исполнения** (Run-Time Library – RTL). При сертификации программного продукта возникает проблема сертификации используемым этим продуктом библиотек, в число которых, как правило, входит стандартная библиотека компилятора. Для решения этой проблемы, помимо версии RTL, определяемой стандартом Ады, GNAT предлагает несколько уровней RTL, отвечающих разным требованиям к сертификации кода. Так, минимальная версия библиотеки периода исполнения ZFP (Zero Foot Print) предоставляет минимальный набор возможностей, позволяющих создавать встроенные приложения, при этом затраты на сертификацию самой ZFP RTL минимальны, так как она практически не содержит исполняемого кода. Версия RTL, называемая Certified Profile, является сертифицированным расширением ZFP RTL, позволяющим разрабатывать практически любые

встроенные приложения, не использующие асинхронные процессы. Версия RTL, удовлетворяющая профайлу Ravenscar, позволяет создавать приложения с асинхронными процессами, для которых может быть обосновано, что поведение системы всегда остается предсказуемым и детерминированным.

- **Статический анализ максимальной глубины стека.** Инструмент gnatstack, входящий в состав системы программирования GNAT, позволяет на основе статического анализа текста программы для каждого вызова подпрограммы определять максимально возможную глубину стека, а также найти вызовы, которые могут привести к неограниченному росту стека.
- **Traceability Analysis Package:** методика и набор инструментов, позволяющих определять для конкретной платформы набор языковых конструкций и параметров компиляции, для которых выполнение критериев структурного тестирования для исходного кода гарантирует выполнение тех же критериев для объектного кода.
- **Couverture:** методика и набор инструментов, позволяющие в процессе тестирования автоматически проверять выполнение критериев структурного тестирования без модификации тестируемого кода. Более того, для встроенного приложения анализ полноты тестирования полностью проводится на инструментальной машине (за счет эмуляции выполнения программы в целевой среде).
- **Контроль стиля кодирования:** набор инструментов, входящих в состав системы программирования GNAT, содержит инструмент gnatcheck, который проверяет выполнение для анализируемого кода различных правил, выходящих за требования стандарта языка и относящихся к стилям и стандартам кодирования. Набор правил постоянно расширяется, инструмент позволяет определять различные стили кодирования, комбинируя правила и их параметры.

Стандарт DO-178B, разрешая применение программных инструментов и технологий в процессе сертификации программного кода, требует, чтобы для самих этих инструментов и технологий были представлены материалы, демонстрирующие, что данный инструмент или технология работает корректно (qualification materials в терминах DO-178B). Для всех перечисленных выше компонент GNAT-технологии в случае их использования в процессе сертификации пользовательского ПО могут быть представлены материалы, демонстрирующие их корректное функционирование для конкретной платформы и целевой среды.

В настоящее время отсутствуют какие-либо ограничения, которые могли бы воспрепятствовать использованию GNAT-технологии в странах СНГ. Есть опыт успешного использования профессиональной версии GNAT-технологии в Российской Федерации. Версии GNAT для популярных платформ Windows (NT, Vista, 7) и Linux свободно доступны под лицензией GPL на сайте <http://libre.adacore.com>. Эти версии позволяют познакомиться с технологией и содержат часть из описанных выше решений, поддерживающих сертификацию ПО в рамках стандарта DO-178B. Полностью эти решения доступны в профессиональной версии GNAT-технологии, для получения которой требуется заключение контракта на техническую поддержку с компанией AdaCore. Стоимость годового контракта сопоставима с годовой зарплатой квалифицированного разработчика, что вполне себя оправдывает для проектов, предполагающих сертификацию разрабатываемых программ. Вся информация, необходимая для заключения договора на техническую поддержку, доступна на сайте www.adacore.com.