

Свободные программные инструменты для разработки ответственных программных систем

А.К.Петренко¹

¹Институт системного программирования РАН, petrenko@ispras.ru

Аннотация — к инструментам разработки ответственных программных систем предъявляются повышенные требования по надежности и требования по поддержке процесса сертификации разработанных продуктов. Дается обзор видов инструментов, поддерживающих жизненный цикл разработки ответственных систем, показано место свободных инструментов, рассмотрены проблемы расширения доли свободных инструментов в данной области и последние инициативы, направленные на решение этих проблем.

Ключевые слова — инструменты разработки, инструменты поддержки жизненного цикла, СПО, сертификация, квалификация инструментов.

I. Введение

Разработка программного обеспечения (ПО), входящего в состав ответственных систем, отказы и некорректное функционирование которых приводят к серьезным последствиям, предъявляет особые требования как ко всему процессу разработки и сопровождения этих систем и к инструментам разработки, используемым в этих процессах. Требования к процессам разработки ответственного ПО определяются рядом международных, национальных и отраслевых стандартов. Наиболее известным стандартом является DO-178B (на смену ему идет DO-178C). Этот стандарт изначально позиционировался как стандарт разработки ПО в авионике. Сейчас он и его модификации широко используются на транспорте вообще, в энергетике и других отраслях, где высоки риски, связанные с отказами ПО. Идеология стандартов обеспечения качества опирается на принцип систематического и тотального анализа требований к системам и доказательной демонстрации того, что заданные требования, последовательно были выполнены на всех фазах жизненного цикла и, соответственно, обеспечиваются конечным продуктом.

II. Виды инструментальных средств и требования к ним

В соответствии с фазами жизненного цикла можно провести условную классификацию инструментов поддержки разработки, это инструменты для:

- Анализа и спецификации требований
- Моделирования и проектирования
- Разработки, компиляции и отладки исполнимого кода
- Верификации, разработки и исполнения тестов.

Каркасом для объединения инструментов служат среды разработки и другие системные средства для интеграции и исполнения инструментов и компонентов целевых систем: средства конфигурационного управления, операционные системы и другие системные средства.

Необходимым условием сертификации ответственного ПО является предоставление данных о высоком качестве инструментов, которые использовались при его разработке. Данные, подтверждающие качество инструмента, называются квалификационным набором (qualification kit). Помимо формальных требований существуют и другие требования, которые адресуются не только к собственно инструменту, но и к его поставщику. К этим требованиям относится, в частности, деловая репутация поставщика и наличие налаженного механизма сопровождения инструментов.

III. Новые позиции СПО в разработке ответственных систем

Высокие требования к программным продуктам и к процессу их разработки, естественно, препятствуют выходу многих СПО-инструментов на рынок разработки ответственных систем. За рубежом и, в особенности, в Европе развора-

чиваются инициативы, направленные на изучение проблемы развития СПО в этом секторе информационных технологий и способам их преодоления. Одной из инициатив является проект SHARE-Project, поддержанный 7-й Рамочной программой. Его девиз – «Развитие европейской индустрии встроенных систем за счет опоры на открытое ПО» [1]. В задачи проекта входит сбор и систематизация данных об опыте использования СПО в ответственных проектах, о способах и метриках, оценки зрелости и качества СПО программных продуктов, распространение этих данных в среде европейских фирм-разработчиков ответственных систем.

Другой важной инициативой является создание открытого и хорошо интегрированного набора инструментов поддержки жизненного цикла ответственных систем OSEE (Open System Engineering Environment). Роль лидера в этой работе играет компания Boeing. Каркасом интеграции служит Eclipse. В базовый комплект инструментов входят средства управления проектом (Action Tracking System), средства для поддержки определения требований, тестирования и отслеживания требований и изменений. Все эти базовые средства нацелены на решение задач обеспечения надежности и упрощения сертификации.

Тенденции расширения масштабов применения СПО-инструментов в секторе разработки встроенных систем можно проследить на основе анализа работ, представленных на одной из крупнейших европейских конференций ERTS2 2010 – Встроенное ПО и системы реального времени [2]. В рамках данной конференции прошел Индустриальный Форум Открытого ПО [3].

IV. Заключение

Можно отметить следующие характеристики процесса расширения использования СПО в области ответственных систем:

- СПО инструменты покрывают практически все фазы жизненного цикла и предоставляют возможности для разработки многих видов ответственных систем. Коллекцию наиболее известных инструментов, использующихся в телекоммуникации, здравоохранении и критических приложениях, можно найти, например, в [2].
- Пожалуй, самые устойчивые позиции среди свободных средств разработки ответвен-

ных систем занимают операционные системы, в том числе, ОС реального времени (MobilIn Real-Time, Altreonic).

- Многие разработчики, предлагающие полно-профильные наборы инструментов (tool-chains), включая и СПО-наборы, настаивают на необходимости обеспечения гетерогенности таких наборов, так как в реальных проектах всегда нужно собирать набор из инструментов от различных разработчиков, построенных на разных технологиях.
- Идет процесс овладения искусством сертификации, см [4], есть прецеденты предоставления СПО-разработчиком квалификационного набора для прохождения сертификации.
- СПО является лидером в овладении формальными методами для обеспечения повышенных требований надежности и требований сертификации новых поколений стандартов (например, DO-178C).

Литература

- [1] www.share-project.eu
- [2] www.erts2010.org
- [3] www.ossif.org
- [4] www.certification-together.com