Rodin — платформа для разработки и верификации моделей на Event-B

Илья Щепетков
Москва
Институт Системного Программирования РАН
Rodin
http://www.event-b.org

Аннотация

При проектировании и анализе сложных систем часто возникает потребность в описании моделей этих систем. Одним из подходов для решения этой задачи является использование формального метода Event-B. В докладе рассказывается о свободной платформе Rodin, которая предоставляет среду для разработки, анализа и верификации моделей на Event-B.

Критичные по безопасности системы, ошибки в которых могут привести к гибели или травмам людей, крупным финансовым потерям и ущербу окружающей среды, имеют повышенные требования к своей корректности. Один из способов повышения уверенности в корректности заключается в моделировании системы и требований к ней и доказательстве их непротиворечия с использованием формальных методов.

Существуют различные формальные методы, многие из которых были использованы в большом количестве проектов индустриального уровня. Одним из наиболее активно развивающихся и используемых является Event-B. Средства для разработки, анализа и верификации моделей на Event-B предоставляются свободной платформой Rodin — она содержит текстовый редактор моделей, набор систем автоматического доказательства, поддержку интерактивного доказательства. Функционал платформы может быть расширен за счет использования плагинов. Доступны плагины, позволяющие писать собственные расширения формального метода Event-B, дополнительные системы автоматического доказательства, инструменты для анимации и model checking, и т. д.

Наш опыт использования Rodin состоит в формализации и доказательстве корректности модели управления правами доступа и информационным потоками операционной системы специального назначения Astra Linux Special Edition. Модель была полностью формализована и верифицирована, что позволило обнаружить и исправить ряд неточностей в её изначальном текстовом описании.

В результате мы можем сказать, что применение формальных методов даёт следующие преимущества: нахождение ошибок, которые иначе не были бы найдены; повышение уверенности в корректности системы; решение задачи сопровождения системы при последующих правках и расширениях в её описании. Однако, при использовании Rodin мы столкнулись и с трудностями. Следует отметить высокий уровень трудозатрат на проведение формальной верификации; ограниченную поддержку Rodin командной разработки; отсутствие поддержки выделения часто используемых выражений в отдельные сущности с последующим доступом к ним по ссылке.

Платформа Rodin это совместный проект различных команд. Наибольший вклад в разработку вносят Саутгемптонский университет, компания Systerel и Дюссельдорфский университет. В результате мы имеем свободный инструмент, не уступающий коммерческим аналогам, а также успешно используемый для повышения качества критичных по безопасности систем.