Разработка программного обеспечения для производства

Специалисты компании Esterel Technologies, Inc.

В статье на примере комплекта средств разработки программного обеспечения SCADE CSF компании Esterel Technologies рассматривается метод модельно-ориентированного проектирования, который является следующим эволюционным шагом в разработке ПО. Публикация представляет собой авторизованный перевод [1].

Одной из наиболее удивительных вещей в программном обеспечении (ПО) является то, что, вообще говоря, ошибки в конечном продукте не вызывают бурного отторжения. Ни в какой другой продукции пользователи не мирятся с дефектами, принимая за данность то, что система часто перезагружается или зависает без видимой на то причины, либо такие периферийные устройства как принтеры не всегда работают. Даже на случайное срабатывание автоматической тормозной системы автомобиля из-за ошибки ПО смотрят скорее как на милую шалость, а не как на серьезное происшествие.

Разумеется, поначалу каждая новая технология грешит определенными недостатками и недоработками, но спустя некоторое время она приобретает завершенный вид. Индустрии встраиваемого ПО еще предстоит достичь следующего уровня — в настоящее время все еще используются языки и методы программирования 30-летней давности. Возникла настоятельная необходимость в более современном подходе, позволяющем избежать ошибок программирования, которые приводят к необходимости длительного поиска и устранения неисправностей.

Модельно-ориентированное проектирование является тем самым подходом, однако до тех пор, пока имеется возможность прогнозируемо генерировать 100% приложения на основе модели. Инструменты CASE с функцией генерации кода появились около 20 лет назад, но с их помощью было невозможно произвести полный код прикладной программы. В большинстве случаев получали только структуры данных и заглушки. Современные UML- и SysML-средства столь же ограничены — большую часть графической спецификации нельзя использовать для генерации кода, т.к. по-прежнему требуется вручную произвести трансляцию.

УНИФИЦИРОВАННАЯ МЕТОДОЛОГИЯ МОДЕЛИРОВАНИЯ

Современное модельно-ориентированное проектирование не требует кодирования вручную, поэтому любые ошибки, которые обычно появляются при ручной транскрипции абстрактной модели в код программирования, исключаются. Такие ошибки как доступ через неинициализированный указатель или запись данных вне границ массива, не возникают.

Модельно-ориентированное проектирование с генерацией полного кода позволяет увеличить производительность и снизить стоимость приложения в той же мере, что и переход от программирования на ассемблере к использованию языков высокого уровня, особенно в тех случаях, когда моделирование на хосте эквивалентно конечному встроенному коду.

Для модельно-ориентированного проектирования требуются современные и надежные инструменты, но только их недостаточно. Необходимо также правильно сформулировать требования к процессу проектирования, т.к. только в этом случае указанные средства заработают полнофункционально. В системах безопасности уже используются такие методы, и через некоторое время опробованные концепции найдут применение в других встраиваемых системах.

Таким образом, для эффективного проектирования встраиваемого ПО требуется соответствующий комплект разработки. Сертифицированный пакет проектирования программного обеспечения SCADE Certified Software Factory (см. рис. 1) поддерживает полный цикл разработки в соответствии с установленными требованиями с помощью унифицированной методологии моделирования. Она в равной мере позволяет осуществлять разработку сложных алгоритмов и сложного управляющего ПО. Унифицированная методология моделирования SCADE сочетает методы потока данных и конечного автомата на любом уровне иерархии проектирования. Оба метода можно комбинировать в соответствии с задачей моделирования, поддерживая модульный принцип проектирования. Схема потоков данных может содержать конечные автоматы, и наоборот.

Унифицированная методология моделирования SCADE обеспечивает разработчика стратегией «писать все единожды», подразумевающей ввод требований без избыточности и создание более совершенных моделей программного обеспечения, которое легче поддерживать, проверять и повторно использовать. Стандартная система управления полетом состоит примерно из 3000 подсистем. Используя унифицированную методологию моделирования SCADE и генератор кода SCADE KCG, разработчики получают гарантию того, что в случае любого изменения в каком-либо элементе оно не окажет скрытого побочного эффекта на остальные 2999 элементов.

Унифицированная методология моделирования SCADE является циклической и имеет строгий контроль типов. Эти два качества позволяют с начального этапа разработки создавать безопасные приложения. Методология позволяет осуществлять квалификацию с помощью автоматического генератора C-кода SCADE KCG в соответствии со стандартом DO-178B до уровня A и сертификацию в соответствии с IEC 61508 и EN 50128 до SIL 3/4. Сгенерированный код оптимизируется как по размеру, так и по скорости и, что важнее, не уступает, по отзывам пользователей, наиболее совершенному коду, записанному вручную.

Для лайнера Airbus A380 было разработано более 10 систем с использованием метода SCADE. Совокупный объем сертифицированного C-кода составил более 8 млн строк. В настоящее время, таким образом, создаются системы управления полетом, блоки управления электрической нагрузкой, система рулевого управления и система тормоза, а также системы бортового индикатора.

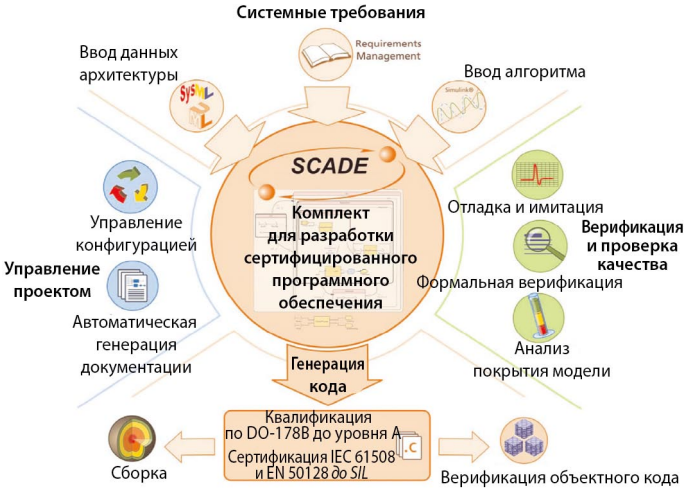

рис. 1. **Сертифицированный комплект средств разработки программного обеспечения SCADE**

РАЗРАБОТКА ПО ДЛЯ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ

В настоящее время SCADE используется в нескольких больших производственных проектах как часть разработки сложных централизованных систем управления движением поездов. С помощью SCADE была создана и верифицирована базовая модель сигнализации SIL 4, включающая свыше 150 функций. Каждая из них, определяемая как конечный автомат, воплощает базовое поведение системы, которое, в свою очередь, реализуется на очень высоком уровне сложности с несколькими тысячами входов и выходов, определяя программное обеспечение для заданной зоны станции.

Метод модельно-ориентированного SCADE-проектирования технологических процессов позволяет:

- собирать системные требования для программного обеспечения;
- разрабатывать архитектуру ПО, точно и однозначно описывать поведение системы (алгоритмы, конечные автоматы и т.д.);
- осуществлять синхронизацию, классификацию данных и внутренние соединения в проекте;
- формировать C-код с помощью генератора SCADE KCG;
- управлять звеньями в цепи трассируемости между требованиями, моделью и кодом.

Этот технологический процесс поддерживается сертифицированным комплектом средств разработки программного обеспечения SCADE CSF (Certified Software Factory). Комплект SCADE CSF позволяет работать со многими необработанными и промежуточными продуктами. Определения требований, описания архитектуры SysML/UML2 и фрагменты алгоритма легко комбинируются с самостоятельно разработанными и отредактированными спецификациями. Импорт из таких программных сред общего назначения как Simulink и StateFlow осуществляется в строгом соответствии с нормативами моделирования для безопасных и надежных систем, обеспечиваемыми с помощью унифицированной методологии моделирования SCADE. Комплект разработки SCADE CSF оснащен набором инструментов, выполняющих верификацию и оценку качества продукции во всей технологической цепи.

Сценарии тестов для имитационного моделирования создаются независимо исходя из системных требований, выполняются на модели, записываются и повторно просматриваются. Параллельно с помощью анализа MTC (Model Test Coverage — тестовое покрытие модели) оценивается, насколько полно модель была изучена при имитации. Метод SCADE MTC позволяет быстро обнаружить недостатки тестовых процедур и все несоответствия требованиям, а также обнаружить непреднамеренные функциональные возможности, которые не были прослежены по спецификации. Как только анализ MTC подтверждает, что все элементы модели проверены на соответствие требованиям, функциональная верификация заканчивается. Методы формальной верификации очень хорошо дополняют возможности тестирования программистом. Средство SCADE Design Verifier очень эффективно позволяет проверить безопасность требований, а также обнаружить ошибки, которые ускользают при стандартном тестировании, но проявляются в производственных системах.

Системные требования, SCADE-модель, тестовый план и вся проектная документация всегда синхронизированы благодаря SCADE-шлюзу, ведущему к системам управления требованиями (Requirements Management — RM). Шлюз SCADE RM создает отчеты, упрощающие процесс сертификации, матрицу трассируемости, анализ покрытия и анализ последствий. Полученный код можно интегрировать в различное оборудование или сертифицированные ОСРВ, используя тот или иной кросс-компилятор C-кода. Комплект кодового генератора SCADE KCG был рекомендован промышленными сертификационными организациями для использовании в большинстве критичных к безопасности приложениях.

Благодаря этому квалификационному комплекту у разработчика исчезла необходимость затрачивать большую часть усилий на низкоуровневое тестирование сгенерированного кода и его верификацию, проверять сгенерированный код на соответствие спецификации, выполнять контроль кода или структурный анализ его покрытия. Благодаря архитектуре комплекта SCADE CSF, специально предназначенной для проектирования критичных к безопасности приложений, автоматизируются многие задачи. В результате первоочередное внимание при тестировании обращается на то, чтобы обеспечить функциональное соответствие модели спецификации, а не на поиск ошибок в реализации проекта.

Если на этапе создания модели часто приходится вносить те или иные изменения, то при конструктивном подходе требуется известное терпение, чтобы реализовать на практике исходное технические задание. Комплект SCADE CSF помогает не только быстро пройти этап получения прототипа, но и подготовить ПО для сертификации. Шлюз SCADE RM позволяет ввести высокоуровневые требования, увязать их при проектировании с моделью SCADE и обеспечивает естественную прослеживаемость между всеми артефактами, требованиями, элементами проекта и тестами на всех этапах разработки ПО.

Модельно-ориентированное проектирование — эффективный метод производства промышленного программного обеспечения, т.к. он является не только основой всего процесса, но и обладает гибкостью. Гибкость обеспечивает соответствие модели требованиям, а также возможность быстро внести изменения на этапе ее создания и разработки сертифицируемого программного обеспечения. Благодаря комплекту SCADE CSF такие центральные аспекты процесса как требования, трассируемость и обеспечение качества учитываются совместно с принципами конструктивного и творческого проектирования, позволяющими воплотить идею в готовый промышленный продукт для конечного пользователя.

ЛИТЕРАТУРА

1. www.esterel-technologies.com.