Модельно-ориентированное проектирование по стандарту DO-254 с помощью инструментов компаний MathWorks и Mentor Graphics

Стандарт RTCA/DO-254 (далее обозначаемый «DO-254») предоставляет руководства для разработки авиационной электронной аппаратуры. Федеральное управление гражданской авиации США (FAA), Европейское агентство по авиационной безопасности (EASA) и другие международные органы по безопасности в авиации требуют использования этого стандарта, чтобы обеспечить надлежащее функционирование сложной электронной аппаратуры авиационных систем в любых прогнозируемых ситуациях, исключить неполадки в работе и возможность авиакатастроф.

Соответствие стандарту DO-254 все чаще становится обычным требованием при реализации коммерческих и военных авиационных проектов. Компании часто испытывают трудности при реализации требований стандарта DO-254 и трудности с затратами, связанными с этими требованиями. При создании авиационной электронной аппаратуры, удовлетворяющей стандарту DO-254, разработчики могут применять модельно-ориентированное проектирование для анализа требований, проектирования, автоматической генерации HDL-кода и верификации. Модельно-ориентированное проектирование по стандарту DO-254 осуществляется совместным использованием инструментов компаний MathWorks и Mentor Graphics при проектировании и верификации, что обеспечивает сквозной процесс разработки — от концептуального замысла до реализации. Такой подход упрощает процесс разработки и сокращает издержки.

Отправной точкой модельно-ориентированного проектирования является применение инструмента Simulink® компании MathWorks, с помощью которого на стадии концептуального проектирования создаются модели всей системы, включающие алгоритмы и внешнюю среду. Эти модели можно симулировать и анализировать на протяжении всего процесса проектирования для обеспечения соответствия алгоритмов и спецификаций, на основании которых разрабатываются алгоритмы. Такой подход дает два преимущества:

- обнаружение и исправление ошибок на ранних стадиях проектирования обходится гораздо дешевле по сравнению с выявлением ошибок во время реализации и тестирования;
- результаты проектирования, тесты и анализ можно повторно использовать в течение всего процесса разработки.

Компания Mentor Graphics предлагает инструменты, охватывающие рабочий процесс проектирования и являющиеся наиболее передовыми в своей отрасли. Рассматриваемые в данной статье инструментальные средства ориентированы на проектирование и верификацию оформленных на языке HDL аппаратных решений на уровне кристалла. Такие средства также предусматривают управление связностью и трассируемостью требований от концептуального замысла до стадии реализации.

Модельно-ориентированное проектирование способствует представлению проекта на основании требований, а также улучшенной степени интеграции и повторному использованию на этапах концептуального и детализированного моделирования и проектирования[1].

[1] В версии стандарта DO-254, принятого в России(КТ-254), этап концептуального проектирования называется эскизным проектированием, а этап детализированного проектирования называется техническим проектированием

В данной статье на высоком уровне рассматривается рабочий процесс модельно-ориентированного проектирования, объясняются типы мероприятий на всех этапах разработки и выдвигаются на первый план такие способы применения инструментальных средств, при которых обеспечивается максимальная эффективность и степень повторного использования.

Обзор стандарта DO-254

FAA начало проводить в жизнь стандарт DO-254 в 2005 году, когда был выпущен рекомендательный циркуляр AC 20-152. Стандарт DO-254 определяет набор целей, которые должны быть достигнуты заявителями и интеграторами, претендующими на сертификацию создаваемой ими аппаратуры для использования в бортовых авиационных системах. Стандарт DO-254 создан по аналогии с DO-178B — эквивалентным стандартом для сертификации программного обеспечения, который был опубликован как DO-178 более 25 лет назад. Хотя первоначально DO-254 возник как стандарт для гражданской авиации, постепенно он все чаще используется при создании систем военной авиации и в других применениях, требующих высокой степени надежности, например, в таких отраслях, как медицина, атомная энергетика и транспорт.

Соответствие стандарту DO-254 и жизненный цикл

DO-254 задает как жизненный цикл процесса проектирования, так и поддерживающие процессы, выполнение которых обязательно на протяжении всего процесса разработки. Как показано на рис. 1, эти два аспекта проекта DO-254 поддерживаются интенсивным процессом планирования, который определяет и детализирует методологию проекта.

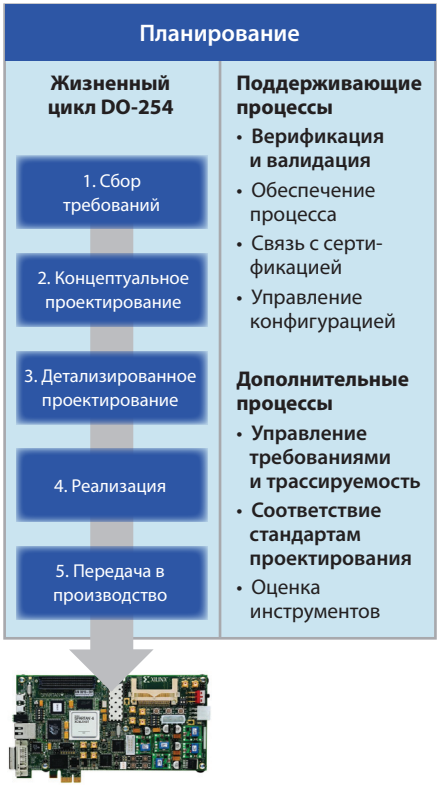

Рисунок 1. *Жизненный цикл по стандарту DO-254 и связанные процессы. В данной статье рассматриваются этапы жизненного цикла по стандарту DO-254 и связанные процессы, выделенные полужирным шрифтом.*

На рисунке 1 показан жизненный цикл DO-254 и перечислены процессы, которые должны выполняться и документироваться по мере продвижения проекта по этапам жизненного цикла. В этой статье рассматриваются следующие процессы, выделенные на рис. 1 полужирным шрифтом:

- Управление требованиями и трассируемость требований — стандарт DO-254 требует, чтобы элементы проекта и артефакты верификации имели обратную связь с требованиями, на основании которых они были разработаны. Трассируемость требований подтверждает, что в проекте реализована намеченная функция и что она была тщательно верифицирована с целью доказательства работоспособности функции в любых прогнозируемых ситуациях.
- Соответствие стандартам проектирования — для процесса разработки, осуществляемого согласно стандартам, каждому этапу разработки должны соответствовать применимые стандарты. По мере продвижения проекта по этапам жизненного цикла необходимо показывать соблюдение таких стандартов.
- Верификация и валидация — На каждом этапе проекта разработчик должен гарантировать, что текущая версия проекта (концептуальная модель, описание на языке HDL, список соединений (netlist), разработанная аппаратура) удовлетворяет требованиям и соответствует предыдущей версии. Для верификации проекта на разных этапах могут использоваться самые разные методы и средства, от симуляции до расширенного анализа (например, анализа с помощью формальных методов). В данной статье рассматриваются методы верификации на высоком уровне, и особое внимание уделяется вопросу повторного использования проектных работ и результатов на протяжении всего процесса.

Обзор рабочего процесса по стандарту DO-254 при использовании модельно-ориентированного проектирования

На рисунке 2 показан рабочий процесс по стандарту DO-254 при использовании модельно-ориентированного проектирования. Пять расположенных по центру прямоугольников представляют этапы проекта. Вертикальные стрелки, соединяющие этапы проекта, представляют видоизменения проекта, такие, как переход от выраженных на естественном языке требований к концептуальному проекту с использованием Simulink.

Дуговые стрелки, соединяющие этапы проекта, представляют поддерживающие процессы, в том числе трассируемость требований, проверку соответствия и верификацию. Применяемые продукты и возможности инструментов, обеспечивающие переходы между этапами проекта и поддерживающие процессы, показаны в виде элементов списка.

В этом рабочем процессе разработчики осуществляют сбор требований и управление ими с помощью средства Mentor Graphics® ReqTracer™. На основании требований создается исполняемая модель Simulink, предназначенная для исследования концептуального проекта и непосредственно связанная с требованиями в ReqTracer.

Применяя инструменты компании MathWorks для верификации и валидации, инженеры могут затем осуществлять функциональное тестирование и формальный анализ на уровне концептуальной модели, а также добавлять к модели специфические детали проекта и атрибуты реализации, такие как влияние разрядности чисел с фиксированной точкой. Такие проработанные модели позволяют специалистам проверять полноту тестирования проекта и соблюдение всех необходимых требований. На основании этой полностью протестированной модели можно автоматически сгенерировать детализированное описание проекта на языке HDL, применяя инструмент HDL Coder™.

Начиная с этой стадии, средство Mentor Graphics HDL Designer обеспечивает основную среду для дополнительной разработки на языке HDL, проверки кода, его визуализации и рассмотрения. Дальнейшая верификация детализированного проекта на языке HDL может осуществляться в среде верификации компании Mentor Graphics при помощи средств ModelSim® и Questa®, с повторным использованием тестовых векторов, созданных на уровне концептуальной модели. Формальный анализ поддерживается средством 0-In® Formal Verification для проверки модели, а для проверки логической эквивалентности — средством FormalPro™. Анализ пересечения сигналом области тактовой частоты выполняется с помощью средства 0-In® CDC. Синтез ПЛИС (FPGA), а также интеграция с инструментами размещения и трассировки (place and route) от производителя ПЛИС осуществляется при помощи средства Precision RTL®.

Рабочий процесс с совместным использованием инструментальных средств компаний MathWorks и Mentor Graphics

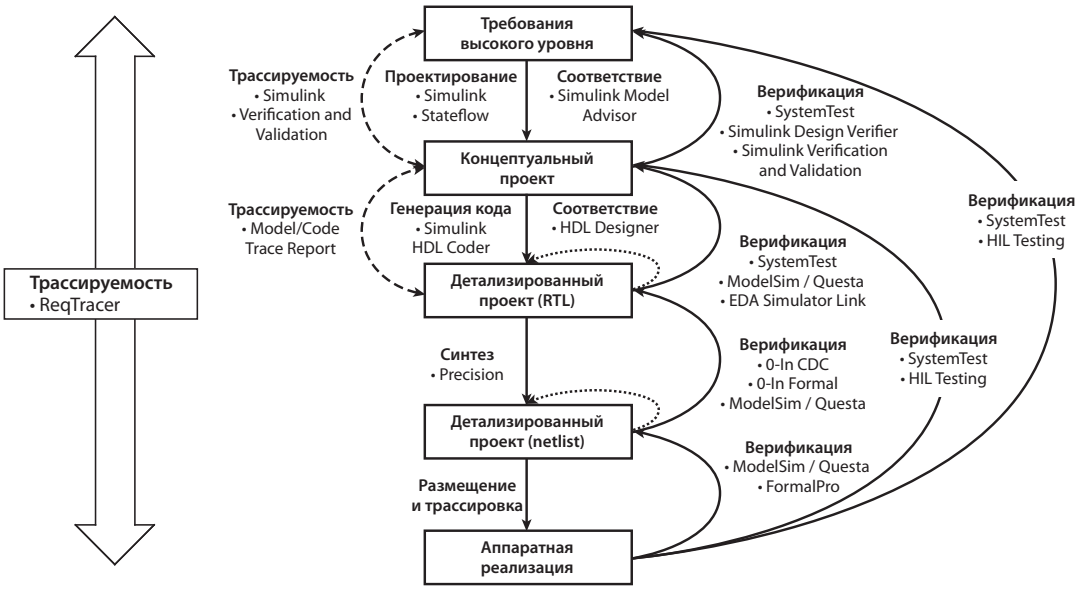

Рис. 2. Рабочий процесс модельно-ориентированного проектирования согласно стандарту DO-254.

1. Сбор требований

Проекты в соответствии с DO-254 разрабатываются на основании требований. Требования задают намеченную функцию разрабатываемого устройства, а процесс разработки в рамках DO-254 гарантирует, что это устройство выполняет предназначенную для него функцию. Системные требования, назначенные к аппаратному компоненту, должны рассматриваться, формулироваться, управляться и трассироваться к соответствующим мероприятиям проектирования. Аналогично, для производных требований, возникающих на базе проектных решений, принимаемых в ходе этих процессов, также должны применяться те же самые процессы.

Таким образом, в проекте по стандарту DO-254 должны применяться механизмы для осуществления следующих мероприятий:

- сбор требований — первая стадия жизненного цикла по стандарту DO-254;
- управление изменениями требований на всех этапах проекта;
- трассирование требований к проектным работам и мероприятиям по верификации на всех этапах проекта.

Многие компании, работающие в аэрокосмической отрасли, применяют системы управления требованиями корпоративного уровня, такие как база данных DOORS® разработки фирмы IBM. DOORS предоставляет механизм базы данных для хранения и управления требованиями и рассчитан на поддержку крупномасштабных и сложных систем. Другие компании, например, субподрядчики по разработке отдельных компонентов большой системы, могут для сбора требований на уровне компонентов пользоваться такими средствами офисной автоматизации, как Microsoft® Word или Excel®. В любом случае важно, чтобы, независимо от типа исходной среды по работе с требованиями, обеспечивалась обратная связь с этими требованиями в результате работ по проектированию и верификации. По стандарту DO-254 такая обратная связь называется трассируемостью требований.

Сбор статического набора требований осуществляется относительно просто. Однако построение проектного процесса, зависящего от требований, и управление требованиями по ходу их развития вместе с проектом представляют собой гораздо более серьезную проблему. Процесс проектирования, управляемый требованиями, подразумевает ввод этих требований, отслеживание их изменений, а также связь с артефактами проектирования и верификации.

Компания Mentor Graphics, обладающая опытом по созданию средств автоматизации проектирования, разработала систему автоматизации управления требованиями и трассируемости требований. Система ReqTracer принимает требования в исходном формате (например, из таких средств, как DOORS или Word) и связывает их с элементами проекта и артефактами верификации. Это также помогает осуществлять валидацию требований, предлагая возможности рассмотрения требований, проведения верификационных работ в зависимости от состояния требований и предоставления артефактов для сертификации.

ReqTracer интегрируется со средами компании Mentor Graphics, в которых осуществляется разработка на языке HDL, верификация и синтез. ReqTracer обладает достаточной гибкостью для адаптации почти к любым другим инструментальным средствам, которые могут использоваться в процессе разработки в соответствии со стандартом DO-254. Для поддержки рабочих процессов, использующих модельно-ориентированное проектирование, ReqTracer имеет специальные средства интеграции с системой Simulink. Проектировщики могут добавлять информацию о требованиях к конкретным блокам, подсистемам и моделям в качестве свойств блоков. Такая информация о требованиях затем автоматически проходит до стадии генерации кода на языке HDL с помощью средства HDL Coder. Этот процесс подробно рассматривается в разделе 3 «Детализированное проектирование».

Кроме поддержки трассируемости и валидации, ReqTracer помогает управлять проектом, создавая визуальное отображение состояния проекта, в котором показываются требования, и отмечается, было ли выполнено их проектирование и верификация. ReqTracer также может генерировать матрицы трассируемости, необходимые для достижения целей трассируемости, предусмотренных стандартом DO-254.

По сути, ReqTracer обеспечивает ориентированную на требования среду управления проектом на этапах от концептуального проектирования до реализации, а также поддерживает функции трассируемости в соответствии со стандартом DO-254. На рисунке 3 показан рабочий процесс, управляемый требованиями, выстроенный при помощи ReqTracer.

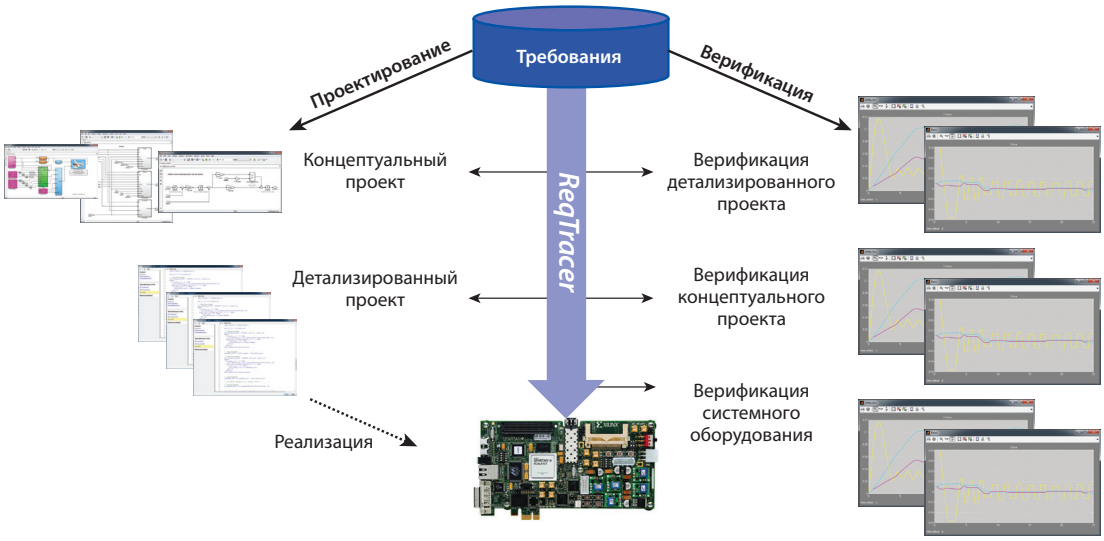

Рисунок 3. Рабочий процесс, управляемый требованиями, выстроенный при помощи ReqTracer.

2. Концептуальное проектирование

Когда требования четко сформулированы, следующий шаг процесса для инженера-проектировщика заключается в разработке концептуальной модели, которая соответствует требованиям высокого уровня, полученным на предыдущей стадии, и позволяет выполнить эти требования. В этом разделе описывается, как Simulink и другие инструменты можно использовать при разработке и верификации концептуальной модели.

Проектирование концептуальной модели

Simulink представляет собой отраслевой стандарт инструментальных средств для проектирования, реализации и тестирования аэрокосмических проектов. Это средство служит платформой для модельно-ориентированного проектирования. По ранее собранным требованиям инженер-проектировщик конструирует исполняемую версию проекта. Simulink дает возможность инженерам создавать эти алгоритмические модели в интуитивно понятной графической среде. Дополнением к системе Simulink является инструмент Stateflow®, который используется для разработки конечных автоматов и логики. Дополнительные наборы блоков обеспечивают функционал более высокого уровня для специфических прикладных задач.

Симуляция работы крупной системы и среды, в которой функционирует аппаратура, позволяет инженерам выполнять полное тестирование системы до начала ее реализации. Например, рассмотрим проект алгоритма прерывания взлета. Этот алгоритм можно разрабатывать независимо в среде Simulink или как часть более высокоуровневой модели самолета. Такая модель самолета системного уровня может включать в себя алгоритм логики, модель динамики летательного аппарата с шестью степенями свободы и учетом воздействия внешних факторов, моделями датчиков и моделями исполнительных механизмов.

Наличие системной модели позволяет специалистам тестировать свои проекты на более ранней стадии и оперативно оценивать сценарии по принципу «что, если». В рассматриваемом примере системная модель позволяет инженеру тестировать алгоритм прерывания взлета, варьируя значения скорости взлета, имитируя различные отказы датчиков и управляющие воздействия пилота.

По мере возрастания уверенности в проектных решениях происходит детализация моделей с целью задания архитектуры изделия и включения эффектов реализации. Средство Fixed Point Designer™ обеспечивает возможности моделирования и анализа проекта, помогающие разработчикам подобрать оптимальную длину слова с фиксированной точкой. Simulink предоставляет возможность симуляции этих эффектов и сравнения их с базовым проектом в плавающей точке, чтобы удостовериться в соблюдении заданных требований.

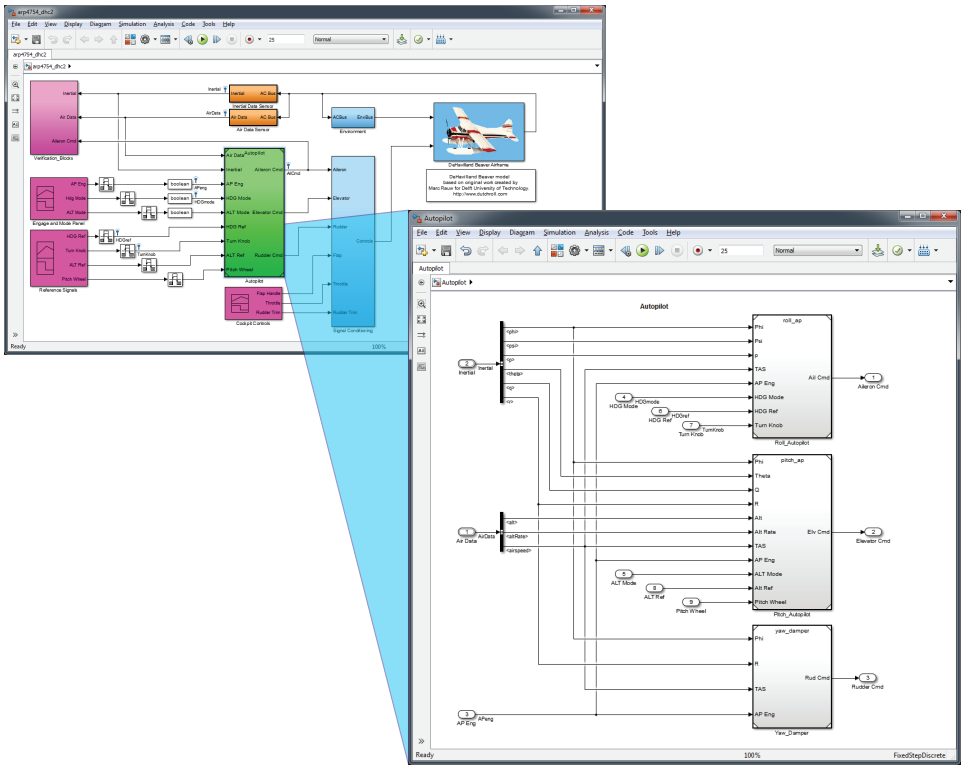

Рисунок 4. Системная модель самолета с алгоритмом автопилота.

Трассируемость требований в концептуальной модели

В рабочем процессе при использовании модельно-ориентированного проектирования все элементы концептуального проекта должны трассироваться к требованиям, которые они удовлетворяют. MathWorks обеспечивает базовую поддержку трассируемости при помощи средства Simulink Verification and Validation™.

ReqTracer также обеспечивает поддержку трассируемости. В этом рабочем процессе ReqTracer используется для организации трассируемости на уровне модели Simulink. Трассируемость поддерживается в сгенерированном коде на языке HDL и действует также на этапах анализа и тестирования HDL-кода.

Верификация концептуальной модели

Концептуальный проект должен анализироваться для верификации выполнения заданных требований. В этой задаче могут оказать помощь несколько продуктов компании MathWorks. Например, система MATLAB® может применяться для выполнения скриптов, подбора значений параметров и выполнения анализа выходных результатов симуляции. Эти задачи могут запускаться параллельно на многоядерных компьютерах или кластерах с использованием возможностей параллельных и распределенных вычислений.

Компания MathWorks разработала также специальные инструменты, ориентированные на верификацию систем. Средство SystemTest™ представляет собой платформу для тестирования, которую можно применять для создания и выполнения тестов для моделей в среде Simulink. Тесты можно создавать для демонстрации выполнения конкретных функциональных требований. SystemTest автоматически генерирует отчеты, которые можно рассматривать как артефакты верификации. Ниже будет отмечено, что эти тесты могут в дальнейшем использоваться повторно в ходе проектирования.

Симуляция помогает убедиться, что заданные требования выполняются, для чего проект подвергается испытаниям при различных условиях. Хотя проведение симуляции имеет важное значение, существенной проблемой в данном случае является вопрос полноты испытаний модели проекта при всех возможных условиях. Для обеспечения полного покрытия при функциональном тестировании можно использовать формальный анализ в сочетании с симуляцией для генерации тестовых векторов. Такие методики основываются на математически строгих процедурах для упрощения и поиска возможных путей выполнения модели, позволяя создавать тестовые вектора и контрпримеры. Этот систематический анализ обеспечивает более глубокое понимание поведения проектируемой системы.

Например, снова рассмотрим описанный выше алгоритм прерывания взлета. Обычно такой тип логики в программном или аппаратном обеспечении задействует несколько входных сигналов, таких как скорость по прибору, значение ускорения и управляющее воздействие от пилота. Применяя технику доказательства свойств, инженер может использовать инструмент формальной верификации с целью верификации конкретного поведения системы: «Доказать, что эта логика никогда не активируется, если скорость по прибору и значение ускорения находятся в указанных пределах». Инструмент Simulink Design Verifier™ позволяет разработчику задавать подобные критически важные свойства и доказывать, что определенные сценарии на уровне модели не могут происходить ни при каких условиях.

Во время тестирования покрытие модели тестами может служить полезной метрикой, позволяющей оценить, насколько полно тесты охватывают модель. Инструмент Simulink Verification and Validation может анализировать покрытие модели и формировать соответствующие отчеты. Метрики по покрытию должны сначала собираться с помощью функциональных тестов, выполняемых на модели. Хотя функциональные тесты используются для подтверждения выполнения проектных требований, они зачастую не позволяют проверить проект на 100%. Инструмент Simulink Design Verifier использует формальные методы для автоматической генерации тестовых векторов для дополнения функциональных тестов и достижения 100% модифицированного покрытия условий/решений (MC/DC) на уровне модели.

Даже при отсутствии требования сертификации такой анализ покрытия на уровне модели может быть полезным при валидации и верификации проекта. Если при использовании тестовых векторов не получается достигнуть уровня покрытия 100%, это может свидетельствовать о необходимости задания дополнительных требований, о наличии ненужных элементов проекта или же о том, что данный проект трудно поддается тестированию. Подобная информация представляет ценность при уточнении требований, разработке концептуального проекта и при создании тестов. Выявление таких ошибок на ранней стадии концептуального проектирования способствует значительной экономии средств.

Следует отметить, что тестирование необходимо также выполнять на уровне кода HDL и на более поздних этапах проекта. Вместе с тем, как отмечается далее, набор тестовых векторов, сгенерированных для концептуальной модели, может быть повторно использован при тестировании на уровне HDL-кода.

Соответствие стандартам проектирования концептуальной модели

Как отмечалось ранее, согласно стандарту DO-254 необходимо разработать и использовать стандарты проектирования и кодирования. Можно разработать стандарты концептуального проектирования и применить их к модели Simulink. Стандарты моделирования тождественны стандартам кодирования и способны определять эстетические и функциональные аспекты модели. Стандартной функцией системы Simulink является инструмент Model Advisor, который может выполнять заранее подготовленные наборы проверок над моделью. Инструмент Simulink Verification and Validation обеспечивает возможность настройки и применения таких проверок на уровне организации.

Такие проверки носят статический характер, и это означает, что инженеры-проектировщики не выполняют запуск модели, а рассматривают ее статически и анализируют ее характеристики. Типичными характеристиками являются параметры, типы данных, настройки генератора кода и настройки HDL. Статический процесс анализа может выявить простые ошибки, такие как отсутствие соединения для входа или выхода блока. Также можно при этом обнаружить более сложные и серьезные проблемы, такие, как настройки блока, при которых возможна ситуация переполнения при выполнении операции над числами с фиксированной точкой. Детализированный проект на уровне языка HDL также должен соответствовать стандартам. В следующем разделе рассматривается проверка соответствия кода HDL применяемым стандартам.

3. Детализированное проектирование

Обычно принято считать, что процесс детализированного проектирования начинается на этапе разработки кода на языке HDL. Такая разработка может вестись вручную или с помощью средства автоматической генерации кода HDL Coder. Автоматическая генерация HDL-кода может повысить эффективность за счет снижения требуемого объема ручного кодирования и ускорения итераций проектного процесса. Рабочий процесс, рассматриваемый далее, включает автоматическую генерацию HDL-кода.

Следует отметить, что мероприятия верификации, упоминаемые в процессе работы по стандарту DO-254, могут выполняться как для ручного кодирования, так и для автоматической генерации HDL-кода.

Генерация HDL-кода из концептуальной модели

В рабочем процессе при использовании модельно-ориентированного проектирования сгенерированное описание на языке HDL можно загрузить в средство HDL Designer компании Mentor Graphics для независимой оценки и интеграции либо с существующим HDL-кодом, либо с частями проекта, менее подходящими для концептуального моделирования в среде MathWorks.

В среде HDL Designer код на языке HDL исследуется при помощи рассмотрений кода, автоматизированной проверки относительно стандартов кодирования HDL и визуализируется для облегчения понимания.

Трассируемость на стадии детализированного проекта

Когда из концептуальных моделей Simulink генерируется HDL-код для этапа детализированного проектирования, вся информация, содержащаяся в концептуальной модели, сохраняется и в данных детализированного проекта. Например, информация по трассируемости собирается в модели Simulink и сохраняется в HDL-коде.

Инструмент HDL Coder обеспечивает вставку всей информации о требованиях в сгенерированный код на языке HDL. Эту информацию по трассируемости можно затем просматривать и использовать на протяжении дальнейших шагов процесса с помощью ReqTracer. Тем самым обеспечивается трассируемость от этапа детализированного проектирования обратно к этапам концептуального проектирования и сбора требований.

Проверка стандартов кодирования HDL

Подобно тому, как на уровне модели Simulink продемонстрировано соответствие концептуальной модели стандартам проектирования, необходимо продемонстрировать соответствие детализированного проекта стандартам кодирования языка HDL. HDL Designer обладает встроенным механизмом проверки проектных правил, иногда называемым «линтингом» (linting). Эта возможность предполагает использование нескольких наборов различных правил, которые можно применять как есть или настраивать. Один из таких наборов называется «DO-254 rule set» (Набор правил для DO-254). Этот набор правил содержит определенное число правил кодирования, которые можно использовать для выполнения целей стандарта DO-254 по заданию стандарта кодирования на языке HDL (как указано в Order 8110-105). HDL Designer может автоматически проверять код на языке HDL для обеспечения его соответствия данному набору правил.

Рассмотрение кода

Код на языке HDL необходимо подвергнуть независимому рассмотрению на соответствие стандартам кодирования HDL и правильность реализации требуемой функциональности. Использование механизма HDL Designer для обеспечения соответствия стандартам языка HDL было рассмотрено ранее.

Как HDL Coder, так и HDL Designer могут помочь при рассмотрении кода HDL для обеспечения реализации требуемой функциональности. HTML-отчет по генерации кода, формируемый инструментом HDL Coder, облегчает переход от HDL-кода обратно к блокам концептуальной модели в среде Simulink, а также к требованиям. Такие переходы являются двусторонними. Использование графической концептуальной модели вместе со сгенерированным HDL-кодом может помочь быстрее понять и проанализировать проект во время рассмотрения. Кроме того, формируется отчет о трассируемости, помогающий в процессе рассмотрения.

HDL Designer также облегчает рассмотрение кода за счет возможности визуализации HDL-кода. Такая визуализация, результаты проверки правил, контроль связей с требованиями и функциональная верификация (описанная в следующем разделе) должны обеспечивать независимую выходную оценку любого сгенерированного кода.

Верификация модели на языке HDL

Верификация должна выполняться и на уровне детализированного проекта. Эту задачу необходимо решать как для кода, написанного вручную, так и для автоматически сгенерированного кода. Как и в случае концептуальной модели, для выполнения верификации могут использоваться различные методы. Эти методы варьируются от базовой симуляции до продвинутых формальных методик.

Мероприятия по верификации могут осуществляться с высокой степенью гибкости. В некоторых случаях продукты компании MathWorks предоставляют доступ к возможностям симуляции компании Mentor Graphics непосредственно из инструментов MathWorks. Другие мероприятия будут выполняться только в пределах инструментов Mentor Graphics. Организация должна решить, какие инструментальные средства и методы планируется использовать, и обсудить это с контактными лицами по их сертификации. Следующие разделы посвящены тому, как повторно использовать данные тестирования и результаты, полученные ранее на этапе концептуального проектирования.

Симуляция модели на языке HDL

В разделе под названием «Концептуальное проектирование» отмечено, что симуляция является важным элементом верификации концептуального проекта. Кроме того, симуляция — необходимое инструментальное средство для верификации детализированного проекта на уровне языка HDL. ModelSim — это наиболее передовой симулятор в военной и аэрокосмической отраслях. ModelSim симулирует работу проектов на языке HDL, предоставляя развитые возможности по их отладке. Этот симулятор также обеспечивает встроенный режим анализа покрытия кода, предназначенного для поддержки метода элементного анализа для проектов уровней A/B согласно стандарту DO-254. ModelSim поддерживает проекты любой сложности, но чаще всего применяется для малых или средних ПЛИС.

Система Questa объединяет в себе механизм симуляции ModelSim с продвинутыми возможностями верификации от таких языков, как SystemVerilog, PSL и SystemC. Эти возможности включают в себя:

- моделирование на уровне транзакций;
- случайное тестирование с ограничениями;
- технологию объектно-ориентированного программирования (ООП) для создания тестовой обвязки;
- автоматизированные тестовые воздействия;
- динамическая верификация на основе утверждений, включая отладчик утверждений;
- унифицированная база данных покрытия (UCDB), предоставленная и принятая в качестве стандарта Accellera (организация, разрабатывающая стандарты в сфере автоматизации проектирования электронных приборов и разработки интегральных схем);
- среда управления верификацией для упрощения работ по управлению мероприятиями верификации проекта и формированию отчетов.

Эта система также тесно интегрирована со средством ReqTracer для обеспечения дополнительного уровня автоматизации от UCDB до источника требований (например, DOORS). Эти продвинутые методы верификации помогают осуществлять верификацию устройств значительной сложности с параллельно выполняющимися задачами. Таким образом, система Questa обычно используется для сложных устройств, содержащих заказные интегральные схемы (ASIC) и большие ПЛИС (FPGA).

Верификация модели на языке HDL — повторное использование тестовых векторов концептуального проекта

На этапе концептуального проектирования механизмом симуляции является система Simulink. На этапе детализированного проектирования механизмом симуляции являются системы ModelSim или Questa. Хотя тип применяемого средства симуляции меняется, существует несколько способов повторного использования мероприятий верификации, выполненных на этапе концептуального проектирования, для этапа детализированного проектирования. Два основных инструмента для этого — косимуляция и генерация тестовой обвязки.

Инструмент HDL Verifier™ (ранее известный как EDA Simulator Link) компании MathWorks позволяет выполнять тесты, созданные в среде MATLAB, Simulink и SystemTest, над кодом HDL, симуляция которого осуществляется в системах ModelSim и Questa. Косимуляция позволяет инженерам с легкостью осуществлять повторное использование тестовых векторов и процедур анализа, разработанных при концептуальном проектировании, для подтверждения их функциональной эквивалентности на этапе детализированного проектирования.

Рассмотренный ранее алгоритм прерывания взлета разрабатывался и симулировался как часть большей системной модели самолета. Из этой концептуальной модели Simulink при помощи HDL Coder был автоматически сгенерирован детализированный проект данного алгоритма на языке HDL. Инструмент HDL Verifier позволяет разработчику исполнять системную модель и тесты, полученные на этапе концептуального проектирования, применительно к сгенерированному коду HDL, выполняемому в системах ModelSim или Questa.

HDL Coder также предоставляет возможность генерировать файлы тестовой обвязки на языке HDL, основываясь на тестах, которые выполнялись на этапе концептуального проектирования. Пользуясь возможностями генерации кода HDL, разработчик может указать, что файлы тестовой обвязки с данными должны генерироваться наряду с кодом HDL, реализующим основные алгоритмы. Таким способом тесты, выполненные при концептуальном проектировании в среде Simulink, можно повторно использовать даже когда разработчики аппаратуры не имеют доступа к Simulink.

Косимуляция и генерация тестовой обвязки способствуют повторному использованию тестовых векторов и позволяют инженерам быстро тестировать детализированный проект (HDL-код). Такая возможность может заметно сократить время итераций и снизить соответствующие затраты. Это также позволяет инженерам воспользоваться возможностями анализа, имеющимися в обеих средах. Функциональное тестирование высокого уровня можно быстро выполнять и анализировать в среде проектирования Simulink. Анализ на уровне детализированного проекта можно проводить в средах ModelSim и Questa.

Верификация модели на языке HDL — продвинутый анализ

Рабочий процесс по стандарту DO-254, использующий модельно-ориентированное проектирование, способствует применению принципа повторного использования для проектирования и верификации. Повторное использование, реализуемое посредством косимуляции и генерации тестовой обвязки, хорошо подходит для функционального тестирования. Однако есть дополнительные средства анализа, доступные для разработчиков в средах проектирования компании Mentor Graphics. Эти продвинутые методы анализа рассматриваются далее.

Анализ пересечения сигналом области тактовой частоты (CDC)

Сегодня широко распространено размещение на одном кристалле нескольких различных функций. Обычно такая интеграция реализуется на одном устройстве с несколькими асинхронными генераторами тактовых частот. Передачи сигналов между регистрами, имеющими разные тактовые частоты, могут привести к возникновению условия, называемого метастабильностью и являющегося основной причиной сбоев в работе устройств. Проблемы, связанные с передачей сигналов между регистрами, имеющими разные тактовые частоты, являются исключительно сложными, их отладка и исправление приводят к значительным затратам, поскольку такие проблемы чаще всего не удается обнаружить, пока не происходит сбой в лабораторных условиях или на объекте. Система 0-In CDC служит средством анализа ситуаций пересечения сигналом областей тактовых частот и построена на формальных методах. В проектах с двумя или более асинхронными тактовыми частотами необходимо применять средство 0-In CDC в процессе проектирования, чтобы уменьшить вероятность возникновения метастабильности.

Формальная верификация (проверка модели на языке HDL)

Проверка модели представляет собой основанный на формальных методах способ анализа проекта относительно предъявляемых к нему требований, записанных в виде утверждений. Проверка модели рассматривалась выше в разделе «Верификация концептуальной модели». На рассматриваемом здесь уровне проекта также применима концепция тщательного доказательства свойств, критически важных для безопасности. В данном случае проверке подлежит модель в виде детализированного проекта, оформленного на языке HDL. Проверка модели может исчерпывающе доказать, что проект выполняет намеченную функцию. Проверка модели упоминается в Приложении B к стандарту DO-254, как приемлемый метод продвинутой верификации для устройств уровня A/B. Система 0-In Formal Verification является инструментальным средством проверки моделей, разработанным компанией Mentor Graphics.

Синтез кода на языке HDL

Синтез, который является частью процесса детализированного проектирования, представляет собой преобразование кода на языке HDL в список соединений (netlist). Синтез проекта лежит в основе всех современных процессов проектирования программируемых логических устройств (PLD), ПЛИС и ASIC. Разработчики и применяемые ими инструментальные средства синтеза традиционно уделяли особое внимание достижению трех основных целей проектирования: временны́е характеристики, площадь на кристалле и время работы инструмента. Однако, в военных и аэрокосмических приложениях, для которых критически важной является гарантия проектирования, инструментальное средство синтеза должно учитывать дополнительные факторы.

В системе Precision Synthesis, разработанной компанией Mentor Graphics для синтеза HDL в независимости от производителя ПЛИС, сочетаются принципы надежного синтеза и выполнение целей производительности, оптимизации и временны́х характеристик. В этой системе гарантируется, что электронные схемы, предназначенные для надежного функционирования, такие как специализированные схемы сброса и схемы специального кодирования конечных автоматов, будут сохранены при выполнении синтеза. Система также поддерживает присущий стандарту DO-254 принцип повторяемости, обеспечивая средство генерации детерминированного и повторяемого списка соединений при согласованном окружении и условиях. Кроме того, эта система интегрируется с инструментом Mentor Graphics FormalPro, предназначенным для проверки логической эквивалентности, что позволяет предоставить дополнительную гарантию при генерации списка соединений. Дополнительная информация о FormalPro представлена в следующем разделе.

Размещение и трассировка (place and route) списка соединений в физическом устройстве требует специальных знаний о целевом устройстве ПЛИС. Этот процесс нуждается в инструментарии, предоставляемом производителем ПЛИС. Система Precision Synthesis интегрируется с программным обеспечением производителя ПЛИС и может непосредственно вызывать такой инструментарий из среды Precision.

Верификация на уровне списка соединений

Как было сказано во введении, верификация необходима на каждом этапе жизненного цикла в соответствии со стандартом DO-254 для обеспечения того, что проект удовлетворяет требованиям и соответствует предыдущей версии. Такая гарантия проектирования первостепенно важна, в особенности для проектов уровня A/B согласно стандарту DO-254.

В Приложении B стандарта DO-254 говорится: «При повышении уровня обеспечения безопасности проекта подход, используемый для верификации выполнения требований безопасности проекта, может потребовать использования перекрывающихся, многослойных сочетаний нескольких методов обеспечения безопасности проекта».

Есть несколько способов выполнить эту верификацию на уровне вентилей после этапа синтеза и убедиться, что список соединений соответствуют детализированному проекту на языке HDL.

Статический анализ временны́х характеристик

Система Precision Synthesis осуществляет статический анализ временны́х характеристик во время процесса синтеза. При этом такой анализ выполняется лишь приблизительно, поскольку еще неизвестно физическое размещение электронных схем. Во время выполнения процесса размещения и трассировки инструментальное средство производителя ПЛИС проведет окончательный анализ временны́х характеристик, когда физическое размещение на целевом устройстве будет определено.

Симуляция на уровне вентилей с учетом временны́х характеристик

Системы ModelSim и Questa поддерживают верификацию списка соединений на уровне вентилей. Верификацию можно выполнять по окончании процесса синтеза с оценками временны́х характеристик или можно включать окончательную информацию о временны́х характеристиках с обратными ссылками из процедуры размещения и трассировки. В любом случае можно применять одну и ту же тестовую обвязку, которая также использовалась при верификации HDL-кода. Инструмент HDL Verifier также поддерживает косимуляцию на этом уровне проекта.

Проверка логической эквивалентности

В рабочем процессе по стандарту DO-254 повторение функциональной верификации на уровне вентилей обычно принимается в качестве способа валидации результатов синтеза и верификации результатов симуляции HDL-кода. Однако для больших и сложных проектов такие повторения могут требовать слишком много времени. Более быстрый подход к верификации результатов синтеза заключается в использовании метода формальной верификации, известного как проверка логической эквивалентности или LEC. Компания Mentor Graphics в качестве средства LEC предлагает систему FormalPro.

FormalPro сравнивает одну модель с другой и определяет, являются ли они функционально эквивалентными. Это сравнение обычно осуществляется на входе и выходе процесса. Например, FormalPro может сравнивать HDL-код, подаваемый на вход синтеза, и сгенерированный список соединений, проверяя их функциональную эквивалентность. Такой же процесс может выполняться для сравнения входа процесса размещения и трассировки (т.е. синтезированного списка соединений) с выходом этого же процесса. Подход на основе формальных методов обеспечивает более быструю верификацию, чем симуляция на уровне вентилей.

Реализация и передача в производство

Рассмотренный в данной статье рабочий процесс по стандарту DO-254 при использовании модельно-ориентированного проектирования ставит во главу угла такие этапы разработки, как сбор требований, концептуальное проектирование и детализированное проектирование. Соответствие стандарту DO-254 подразумевает более широкий диапазон мероприятий, включая реализацию — например, программирование устройства ПЛИС — и передачу в производство (перенос информации и артефактов, необходимых для изготовления работоспособного и воспроизводимого конечного экземпляра проектируемого аппаратного устройства).

На этих этапах могут повторно использоваться рассмотренные выше артефакты проектирования и верификации. Подробное описание этих этапов выходит за рамки этой статьи.

Выводы и заключение

Возрастающее значение соответствия требованиям стандарта DO-254 и связанные с этим затраты на проектирование вынуждают компании проводить оценку способов повышения эффективности процессов разработки и поддержки соответствия требованиям стандарта DO-254.

Заказчики, осуществляющие разработку сложных электронных изделий для авиации, в настоящее время применяют широкий набор инструментальных средств проектирования, тестирования и реализации. Инструменты компании MathWorks широко используются для задач проектирования алгоритмов, симуляции, реализации и анализа. Компания Mentor Graphics предлагает стандартные для отрасли возможности по проектированию аппаратуры, симуляции, анализу и реализации.

Рабочий процесс в соответствии со стандартом DO-254, использующий модельно-ориентированное проектирование, поддерживает основанное на требованиях представление проекта и увеличивает степень повторного использования результатов проектирования и верификации на всех этапах жизненного цикла согласно DO-254. В этой статье описаны способы совместного использования инструментов компаний MathWorks и Mentor Graphics для такого рабочего процесса.

Для заметок

Дополнительная информация и контакты

Информация о продуктах
matlab.ru/products

Пробная версия
matlab.ru/trial

Запрос цены
matlab.ru/price

Техническая поддержка
matlab.ru/support

Тренинги
matlab.ru/training

Контакты
matlab.ru
E-mail: **matlab@sl-matlab.ru**
Тел.: +7 (495) 232-00-23, доб. 0609
Адрес: 115114 Москва,
Дербеневская наб., д. 7, стр. 8

MathWorks®
Accelerating the pace of engineering and science