Переход к DO-178C и ARP4754A при разработке ПО повышенной надежности для БПЛА с использованием модельно-ориентированного проектирования

По мере того, как организации FAA и EASA принимают новые авиационные стандарты, такие, как DO-178C и ARP4754A, разработчикам ПО для БПЛА требуется ознакомиться с этими стандартами, особенно при переходе к модельно-ориентированному проектированию.

Очень небольшое число систем придают большее значение верификации или требуют более строгое следование процессам разработки, чем в авиастроении. Такие организации как FAA или её европейский эквивалент, EASA, предоставляют руководства по процессам разработки с использованием стандартов ARP 4754 для авиационных систем и DO-178B для бортового ПО. Эти стандарты часто используются за пределами гражданской авиации – полностью или частично – для применений, включающих военную авиацию и наземные транспортные средства.

Применение этих стандартов для БПЛА быстро увеличивается из-за недавнего решения FAA (FAA Order 8130.34A) требовать сертификации UAS (Unmanned Aircraft System – прим. перев.) и OPA (Optionally Piloted Aircraft – прим. перев.). Системы БПЛА являются смешанными, и не ограничены одним лишь бортовым ПО. Поэтому также используются другие стандарты – такие, как DO-254 для аппаратного обеспечения и DO-278 для наземного и космического ПО.

Однако этим стандартам уже более десяти лет и их возраст дает о себе знать. Например, в них отсутствует руководство по современным парадигмам разработки и верификации – таким, как модельно-ориентированное проектирование, объектно-ориентированные методы и формальные методы. Так было до момента разработки стандарта DO-178C.

Документ	Дата выхода	Предыдущий релиз	Фокус
SAE ARP4754A	12/01/2010	11/01/1996	Aircraft Systems
RTCA DO-178C	12/13/2011	12/01/1992	Airborne Software
RTCA DO-254	04/19/2000	нет	Airborne Electronic Hardware
RTCA DO-278A	12/13/2011	03/05/2002	Ground and Space Software
RTCA DO-330	12/13/2011	нет	Software Tool Qualification Supplement
RTCA DO-331	12/13/2011	нет	Model-Based Design Supplement
RTCA DO-332	12/13/2011	нет	Object-Oriented Supplement
RTCA DO-333	12/13/2011	нет	Formal Methods Supplement

Таблица 1: Документы со стандартами и недавние обновления.

FAA и EASA работали с производителями самолетов, поставщиками и разработчиками инструментов - включая MathWorks, для того, чтобы обновить стандарты с учетом современных технологий. Вместо того чтобы существенно изменять стандарты, были созданы технологические дополнения – документы, расширяющие стандарт.

Особенно сильное влияние новые стандарты оказали на разработчиков БПЛА, использующих модельно-ориентированное проектирование. Прежде, чем перейти к описанию нововведений, сделаем небольшое введение в модельно-ориентированное проектирование.

Введение в модельно-ориентированное проектирование

С использованием модельно-ориентированного проектирования, инженеры разрабатывают БПЛА и запускают симуляции моделей, описывающих аппаратные и программные составляющие системы. Графически модель выглядит как диаграмма, состоящая из блоков, как показано на рисунках 1 и 2. Затем инженеры автоматически генерируют, развёртывают и проводят верификацию кода на своих встраиваемых системах.

Используя языки более высокого уровня и инструменты моделирования блочных диаграмм, можно сгенерировать код на языках C, C++, Verilog и VHDL – позволяя получить реализации на микроконтроллерах, ЦСП, ПЛИС и заказных ИС. Это позволяет системным инженерам, программистам и аппаратным инженерам работать совместно, используя одни и те же инструменты и окружение для разработки, реализации и верификации систем.

Учитывая автономную природу БПЛА, в этих системах широко используются системы управления с обратной связью. Это приводит к тому, что системное моделирование и симуляция систем с обратной связью (показанных на рисунках 1 и 2) идеально подходят для создания таких систем.

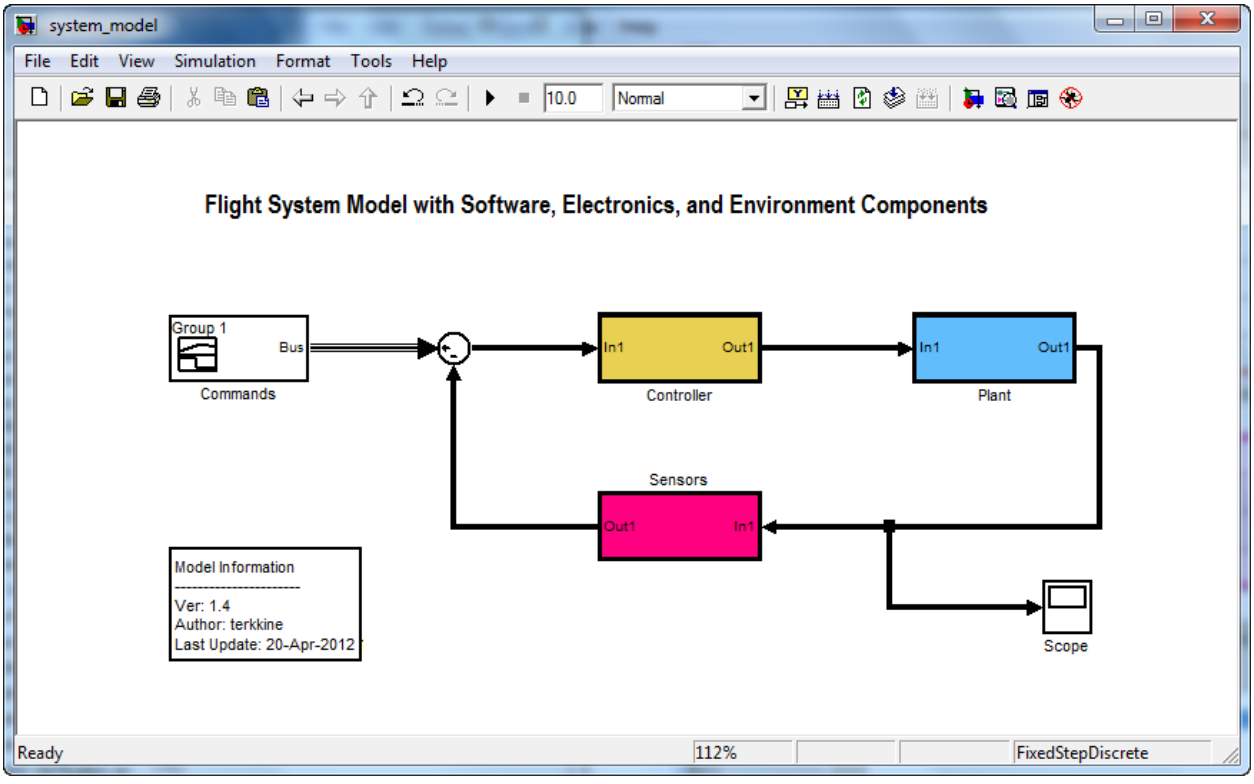

Рис. 1: Пример системной модели БПЛА с регулятором и объектом управления.

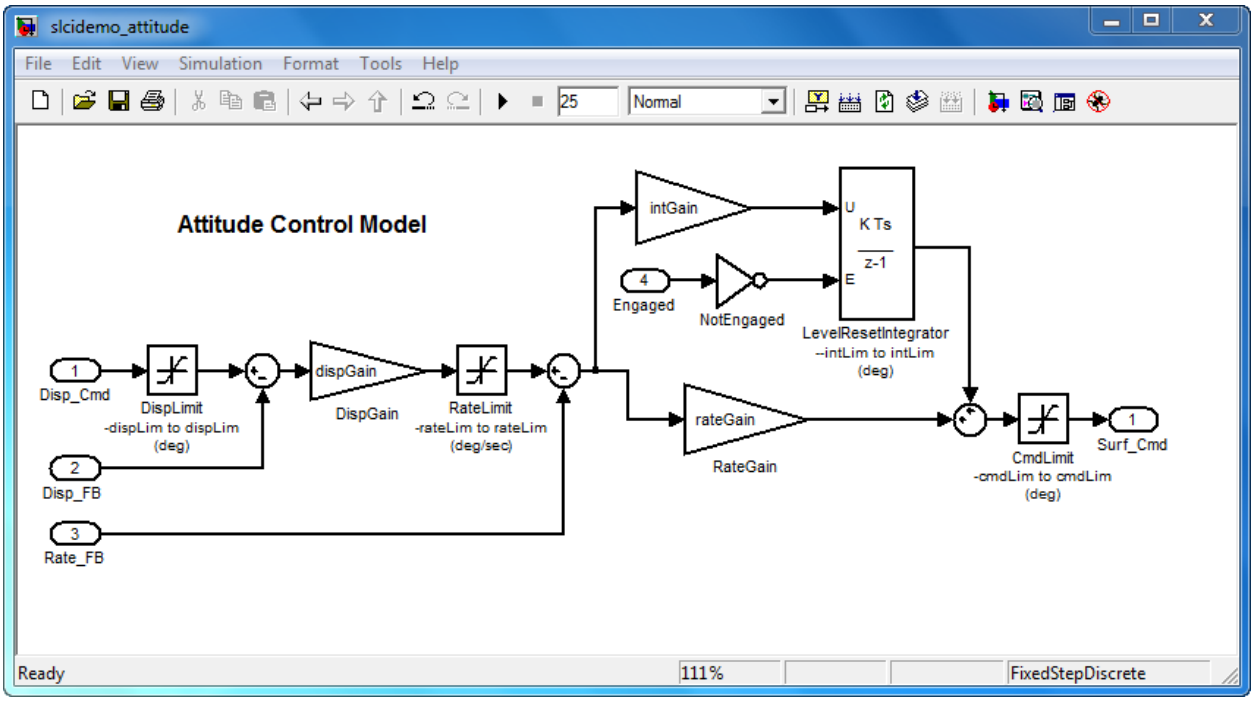

Рис. 2: Пример модели ПО, реализующей законы управления БПЛА

Тестирование БПЛА посредством настоящих тестовых полетов с управлением с земли требует существенных денежных расходов. Гораздо лучше начать тестирование на ранних стадиях процесса разработки с использованием симуляции на рабочих станциях и лабораторных стендах.

С использованием модельно-ориентированного проектирования, верификация начинается в тот самый момент, когда модель создается и впервые запускается для симуляции. Тестовые вектора, созданные на основании требований высокого уровня, формализуют тестирование во время симуляции. Распространённый подход к верификации – это повторное использование тестов в течение всего процесса модельно-ориентированного проектирования, когда модель превращается из системной модели в модель ПО, а далее в исходный код и объектный код с использованием генераторов кода и кросс-компиляторов.

Часто используются техники тестирования "в контуре", как описано ниже и обобщено в таблице 2:

1. Создаются тестовые вектора для симуляции и запускаются над моделью в режиме модель-в-контуре (model-in-the-loop, MIL).
2. Осуществляется верификация исходного кода посредством компиляции и выполнения его на хост-компьютере в режиме код-в-контуре (software-in-the-loop, SIL).
3. Осуществляется верификация исполняемого объектного кода посредством кросс-компиляции и выполнения его на встраиваемом процессоре или симуляторе процессора в режиме процессор-в-контуре (processor-in-the-loop, PIL).
4. Осуществляется верификация аппаратной реализации посредством синтеза HDL и выполнения его на ПЛИС в режиме ПЛИС-в-контуре (FPGA-in-the-loop, FIL).
5. Осуществляется верификация и валидация встраиваемой системы с использованием исходной модели объекта управления в режиме программно-аппаратного тестирования (hardware-in-the-loop testing, HIL).

Тест	Что тестируется	Где тестируется	Фокус
MIL	Модель проекта	Simulink	Верификация проекта
SIL	Исходный код	Хост-компьютер	Верификация исходного кода
PIL	Исполняемый код	Встраиваемый процессор или симулятор процессора	Верификация объектного кода
FIL	Аппаратная реализация	ПЛИС или симулятор HDL	Верификация аппаратной реализации
HIL	Встраиваемая система (ЭБУ)	Встраиваемая система, подключенная к системе (симулятору) реального времени	Верификация системы

Таблица 2: Возможности тестирования посредством симуляции.

Подход к тестированию на основании требований с повторным использованием тестов для моделей и кода описывается в явном виде в ARP 4754A, DO-178C и DO-331 (дополнение, описывающее модельно-ориентированное проектирование и верификацию).

Переход к новым стандартам ARP4754A и DO-178C

ARP4754A

ARP4754A относится ко всему циклу разработки воздушного судна - от требований до интеграции через верификацию - и описывает три уровня абстракции: воздушное судно, система и компонент. Компонент определяется как *аппаратный или программный элемент, который ограничен и имеет строго определенные интерфейсы.* В соответствии со стандартом, требования к воздушному судну назначаются к системным требованиям, которые в свою очередь назначаются к требованиям к компоненту.

Тот факт, что ARP4754A адресует назначение и выделение системных требований к аппаратным и программным компонентам, является важным для разработчиков БПЛА, особенно для поставщиков. Некоторые поставщики ранее могли говорить о том, что разработка подсистем для БПЛА находится за пределами описания оригинального ARP4754 - даже для сложных подсистем, содержащих аппаратное и программное обеспечение. Но теперь становится очевидным, что поставщики тоже должны этим руководствоваться, поскольку ARP4754A явно ссылается на DO-178 и DO-254 для создания компонентов. В действительности, в предисловии к ARP4754A говорится, что его рабочие группы находились в тесной координации со специальными комитетами RTCA *для обеспечения того, чтобы используемые терминология и подходы соответствовали тем, которые разрабатываются при обновлении DO-178B [DO-178C].*

Учитывая высокую взаимосвязь между системами, аппаратным обеспечением и ПО для БПЛА, очень полезным является тот факт, что регулирующие стандарты теперь проясняют взаимосвязь между системами и аппаратными/программными подсистемами.

DO-178C

Неудивительно, что одним из первых нововведений в DO-178C является явное упоминание ARP4754A в Разделе 2: *System Aspects Relating to Software Development (Системные аспекты, имеющие отношение к разработке ПО)* для того, чтобы еще больше синхронизировать стандарты:

Процессы жизненного цикла системы описываются в других документах (например, SAE ARP4754A).

За исключением пояснений – таких, как приведенное выше - DO-178C не отличается существенно от DO-178B, по крайней мере, на первый взгляд. В действительности, обычный читатель может не заметить замечание, приведенное в Разделе 1.4: *How to Use this Document (Как использовать этот документ)*:

Существует одно или несколько дополнений к этому документу, которые расширяют руководства в этом документе для определенных методик … если существует дополнение для определенной методики, это дополнение должно применяться …

Другими словами, самые большие изменения в стандарте отражены в дополнениях, таких, как RTCA DO-331, *Model-Based Development and Verification Supplement to DO-178C and DO-278A (Дополнение по модельно-ориентированному проектированию и верификации для DO-178C и DO-278A).*

Переход к новым стандартам с использованием модельно-ориентированного проектирования

ARP4754A

ARP4754A рекомендует использовать моделирование и симуляцию для нескольких мероприятий в течение процесса разработки – включая привязку требований и валидацию требований.

Таблица 6 из ARP4754A рекомендует (обозначение "R" – прим. перев.) анализ, моделирование и симуляцию (тестирование) для валидации требований при работе по самым высоким уровням ПО (в терминологии ARP4754A - Development Assurance Level – прим. перев.) - A и B. Для уровня C, моделирование указано как одно из нескольких рекомендаций. Хотя в ARP4754 тоже были подобные рекомендации, ARP4754A дает больше описания и утверждает, что репрезентативная модель окружения – например, такая, как модель объекта управления на рисунке 1, является существенной частью системной модели.

При применении моделирования для валидации требований, обычно используется модель окружения разрабатываемой системы, которая сообщается с прототипом проекта ПО для этих требований. Модель окружения, которая является репрезентативным представлением окружения разрабатываемой системы, предоставляет высокую степень функционального покрытия как во время симуляции, так и во время работы реальной системы.

В ARP4754A также упомянуто то, что графическое представление модели может быть использовано для привязки системных требований. Стандарт теперь утверждает, что модель может быть повторно использована для разработки ПО и аппаратного обеспечения.

Модели, используемые для привязки требований и затем напрямую используемые для производства встраиваемого кода (программного или HDL), находятся в рамках DO-178B/ED-128 и DO-254/ED-80, начиная с момента, когда требуется получить кредиты для сертификации, и до момента, когда ПО или аппаратное обеспечение возвращается обратно в системные процессы для верификации системы.

Если вы используете модели для привязки требований, ARP4754A рекомендует следующие мероприятия:

1. *Идентифицировать использование моделей/моделирования*
2. *Идентифицировать предполагаемые инструменты и их использование в процессе разработки*
3. *Определить стандарты моделирования и библиотеки*

Модельно-ориентированное проектирование предоставляет дополнительные возможности для верификации, помимо приведенных в таблице 2. Эти возможности включают в себя трассировку требований, проверку на стандарты моделирования по DO-178C, проверку структурной эквивалентности модели и кода, а также анализ робастности с использованием формальных методов. Учитывая автономную природу и сложность БПЛА, тщательная верификация, включающая несколько технологий для верификации, является высшим приоритетом для таких систем.

DO-178C и DO-331

Проблема с DO-178B, которая долгое время не оставляла в покое практиков модельно-ориентированного проектирования, заключается в неясности привязки целей DO-178B к артефактам модельно-ориентированного проектирования. Основная цель рабочей группы DO-178C SG-4, которая фокусировалась на модельно-ориентированном проектировании, заключалась в том, чтобы создать такую привязку. Оказалось, что одна привязка не может адресовать все возможные аспекты использования, поэтому в DO-331 приведено несколько привязок. Некоторые привязки содержат концепцию "модели спецификации", которая является отдельной моделью относительно модели, которая используется для разработки и генерации кода. Другая привязка содержит концепцию "модели дизайна", которая служит в качестве детализированных требований, использующихся при генерации кода.

Суть "модели дизайна" заключается в следующем:

1. Модель может быть использована для разработки (системы и/или ПО) и должна быть разработана с использованием требований, которые являются внешними относительно модели (например, текстовые требования или база данных с требованиями).
2. Исходный код может быть сгенерирован непосредственно из "модели дизайна" (вручную или автоматически).

Конечно, будучи документом на 125 страницах, DO-331 может предложить гораздо больше, чем описано выше. Один из подходов, упомянутых в стандарте, заключается в том, что модель, используемая первоначально для разработки системы, может быть расширена и повторно использована для разработки ПО и генерации кода. Это связывает ARP 4754A и DO-178C вместе и отлично подходит для систем БПЛА и разработчиков ПО, использующих модельно-ориентированное проектирование.

Например, регулятор, показанный как часть системной модели на рисунке 1, и как отдельный компонент на рисунке 2, используется во время разработки системы; повторно используется как отправная точка для разработки ПО, и расширяется во время детализированного дизайна ПО (например, путем дискретизации непрерывных блоков и изменения арифметики в плавающей точке с двойной точностью на единичную или на арифметику с фиксированной точкой), а затем используется как вход для генерации встраиваемого кода. Тестовые вектора для валидации системных требований похожим образом повторно используются для модели, исходного кода и исполняемого объектного кода для осуществления функционального тестирования и сбора метрик по покрытию тестами.

Хотя и без определенной привязки, использование и повторное использование моделей для разработки систем и ПО, в связке с генерацией кода при помощи инструментов MathWorks - MATLAB®, Simulink® и Embedded Coder™ - уже давно упрощает процессы разработки для инженеров, занимающихся БПЛА. Отрадно видеть, что тот же самый подход теперь является принятым и признанным при сертификации по руководящим стандартам.

MathWorks предоставляет наборы для квалификации инструментов верификации и руководства по рабочему процессу с использованием модельно-ориентированного проектирования для DO-178. Больше информации вы можете получить на странице:

www.mathworks.com/aerospace-defense/standards/do-178c.html

Об авторе:

Том Эрккинен (Tom Erkkinen) является руководителем направления встраиваемых приложений и сертификации в MathWorks. Он возглавляет корпоративную инициативу по содействию принятию технологий генерации встраиваемого кода в промышленности. Его команда участвовала в рабочей группе DO-178C SG-4, которая фокусировалась на модельно-ориентированном проектировании.

Вы можете связаться с ним по адресу tom.erkkinen@mathworks.com