**Валидация и верификация**

Процесс создания комплекса оборудования состоит из взаимодополняющих этапов планирования — проектирования — интеграции, а также верификации и валидации — сертификации. Каждый этап разработки — это составная часть всего процесса создания комплекса бортового оборудования (КБО), результатом выполнения которого является некоторый промежуточный продукт (техническая документация, программно-аппаратные комплектующие КБО и т.п.). Эти продукты являются входной информацией для соответствующего им этапа верификации и последующих этапов разработки/доработки на соответствующих уровнях создания КБО.

Процесс валидации КБО — это процесс определения полноты соответствия разработанного комплекса его функциональному назначению. Валидация требований и принятых допущений представляет собой процесс, гарантирующий, что они являются достаточно правильными/корректными (correctness) и полными (completeness), обеспечивая соответствие требованиям Норм летной годности. Процесс валидации поддерживает разработку требований, вытекающих из необходимости выполнения функциональных задач и обеспечения безопасности.

Вследствие сложности процесса разработки КБО валидация обычно представляет собой многоступенчатый процесс, выполняемый на всех этапах жизненного цикла, включая этап эксплуатации. На каждом этапе мероприятия по валидации обеспечивают нарастающую уверенность в правильности и в полноте требований.

Целями процесса валидации являются проверка правильности и полноты требований.

Также задача валидации заключается в предотвращении появления избыточных функций как в разрабатываемой, так и во взаимодействующих системах.

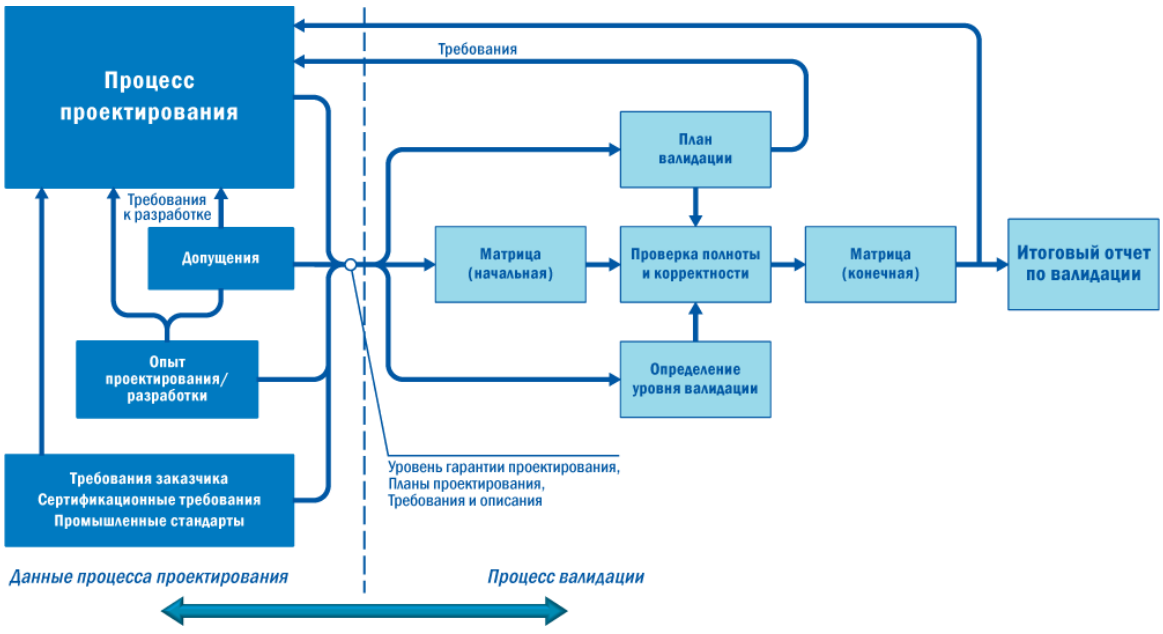


***Рис. 3.8. Модель процесса валидации.***

Взаимосвязь валидации и процесса проектирования системы показана на рис. 3.8. Входная информация процесса валидации может включать в себя описание системы (включая ожидаемые условия эксплуатации), требования к системе, описание архитектуры системы и уровень гарантии проектирования. В плане валидации должны быть указаны методы, применяемые при валидации требований к системе и допущений.

Необходимый уровень валидации определяется уровнем гарантии проектирования функции, к которой относится требование.

Проверки полноты и корректности требований могут потребовать инженерной оценки, проведения анализа или испытания. В большинстве программ проектирования имеются допущения, правильность которых нельзя напрямую доказать в момент их использования. В процессе валидации принятых допущений доказывается, что допущения точно изложены, соответствующим образом распределены и оценены с использованием представленных данных. Допущения должны быть идентифицированы, а их обоснованность должна быть показана применительно к конкретной системе и ее уровню гарантии проектирования.

Для контроля хода процесса валидации рекомендуется использовать матрицу валидации. Для ее подготовки используются требования и результаты валидации, в том числе характеристики аппаратной части, программного обеспечения, производные требования, рассмотрения окружающих и эксплуатационных условий, а также допущения и подтверждающие данные. Должен быть указан источник каждого требования. В процессе разработки матрица должна регулярно обновляться и в окончательном виде включаться в сводный отчет по валидации.

Сводный отчет (заключение) по валидации должен гарантировать, что валидация была проведена надлежащим образом.

Для поддержки процесса валидации используются следующие методы: трассировка требований, анализ, моделирование, испытания, анализ сходства и инженерные оценки. Методы валидации и данные выбираются в зависимости от установленного уровня гарантии проектирования A — E. При валидации некоторых требований для проверки правильности могут использоваться одни методы, а для проверки полноты — другие.

План проведения валидации требований должен иметь место на протяжении всего процесса проектирования.

Под верификацией комплекса бортового оборудования понимается совокупность мероприятий (анализ, демонстрации, моделирования и испытания), направленных на оценку и демонстрацию соответствия КБО функциональным, эксплуатационным и сертификационными требованиям.

В процессе верификации КБО:

- подтверждается, что предусмотренные функции комплекса бортового оборудования самолета правильно реализованы комплектующими изделиями (системами, оборудованием);

•гарантируется, что требования по безопасности к КБО в целом и к его комплектующим изделиям выполняются.

Объем работ по верификации систем и оборудования самолета зависит от назначенного уровня гарантии проектирования на основе проведенной оценки отказобезопасности (FHA, PASA, PSSA).

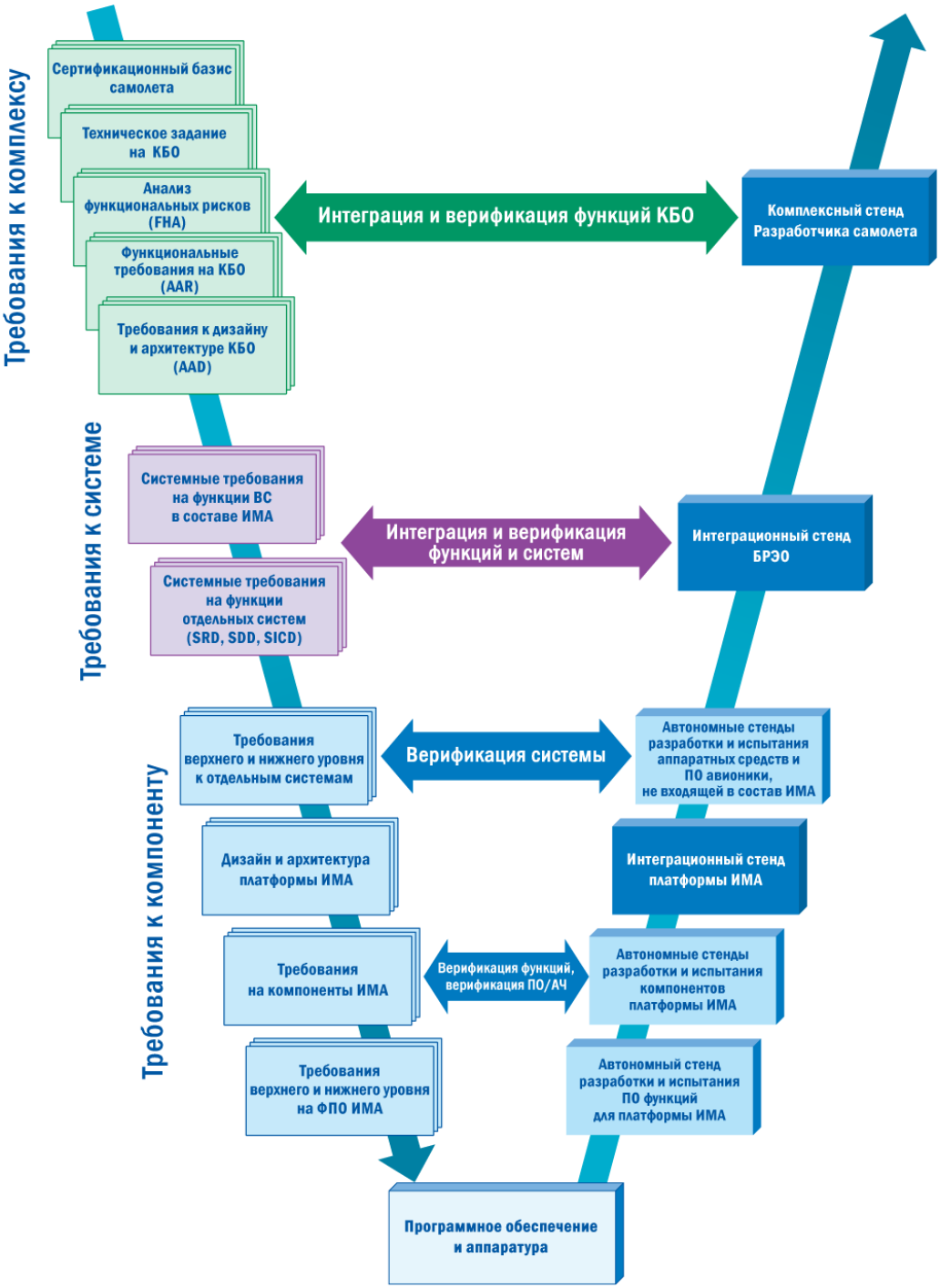


***Рис. 3.9. Взаимосвязь спецификаций КБО и стендового оборудования.***

Процесс верификации комплекса бортового оборудования реализуется мероприятиями трех уровней (рис. 3.9):

- Уровень разработчика самолета/Интегратора КБО — оценивается реализация требований к комплексу в целом. Испытания проводятся на самолете и на комплексном стенде Разработчика самолета под руководством Разработчика.
- Уровень разработчика (поставщика) системы КБО — оценивается реализация системных требований. Испытания проводятся на автономных стендах разработки и испытаний систем Поставщика системы и на интеграционном стенде КБО (под руководством Интегратора КБО).
- Уровень разработчика компонента — оценивается реализация каждого из требований к компонентам. Испытания проводятся на автономных стендах разработки и испытаний компонентов платформы ИМА, на автономных стендах разработки и испытаний ПО приложений (функций для платформы ИМА), а также на автономных стендах разработки и испытаний аппаратных средств и ПО, не входящих в состав ИМА, под руководством Разработчиков компонентов.

На каждом уровне ответственности должны выполняться мероприятия планирования, верификации реализаций требований (соответствующего уровня) и подготовки выходных данных, а также разрабатываться Программы сертификационных, квалификационных испытаний систем и оборудования (Планы верификации).

Задачи процесса верификации комплекса оборудования — продемонстрировать соответствие комплекса оборудования техническим требованиям проекта.

Количество технических проверок и критерии их прохождения определяются Разработчиком самолета совместно с Поставщиками компонентов (комплектующих изделий) в рамках конкретного проекта.

Разработчик самолета планирует мероприятия по верификации интегрированного КБО. Верификация осуществляется на различных уровнях.

За верификацию системы отвечает Разработчик системы. В соответствующем Плане верификации системы должно быть указано, кто отвечает за выполнение соответствующих работ. За проверку компоновки системы на борту самолета отвечает Разработчик системы.

Верификация оборудования относится к зоне ответственности Поставщика оборудования. Для доказательства достоверности работ по верификации Поставщик оборудования должен представить соответствующие доказательства для аттестации и проверки своей продукции.

Процесс верификации ПО должен выполняться в соответствии с требованиями КТ-178С (раздел 6). Он включает подготовку входных данных для процесса верификации (требования к системе, требования к ПО высокого и низкого уровней, данные по трассируемости, Исходный код, Исполняемый объектный код и План верификации ПО), мероприятия по выполнению верификации, а также разработку выходных данных

(тестовые варианты, тестовые процедуры, анализ покрытия требований, анализ структурного покрытия, результаты тестирования ПО).

Процесс верификации аппаратуры выполняется в соответствии с требованиями КТ-254 (раздел 6.2). Мероприятия процесса верификации должны осуществляться в соответствии с планом верификации аппаратуры.

Верификация системы ИМА выполняется в рамках процесса сертификации системы и в соответствии с «Планом валидации и верификации системы ИМА». Структура и содержание должны отвечать требованиям АР МАК Р-297. Процесс верификации системы ИМА состоит в проверке соответствия реализации назначенных требований к системе ИМА. Основной целью процесса верификации системы ИМА является проверка того, что все уровни требований реализованы корректно и полностью, и что методы верификации, используемые для этой цели, также корректны.

Доказательство соответствия интегрированного комплекса оборудования самолета требованиям достигается посредством сочетания следующих методов верификации:

- осмотр и экспертная оценка;
- анализ;
- моделирование;
- анализ охвата требованиями;
- испытания;
- опыт эксплуатации.

На каждом уровне верификации выполняется анализ покрытия требований, чтобы определить степень охваченности требований в испытаниях. При выполнении анализа используются матрица верификации и результаты верификации соответствующих уровней.

На рис. 3.10 показана связь технических требований на КБО и тестовых процедур для проверки правильности реализации этих требований.

Указанные ниже данные формируются на каждом уровне верификации:

- план верификации системы и оборудования КБО (разрабатывается в соответствии с Р-4754А, Р-297, КТ-254 и КТ-178С);
- процедуры и результаты верификации;
- матрица верификации;
- итоговое заключение по верификации.

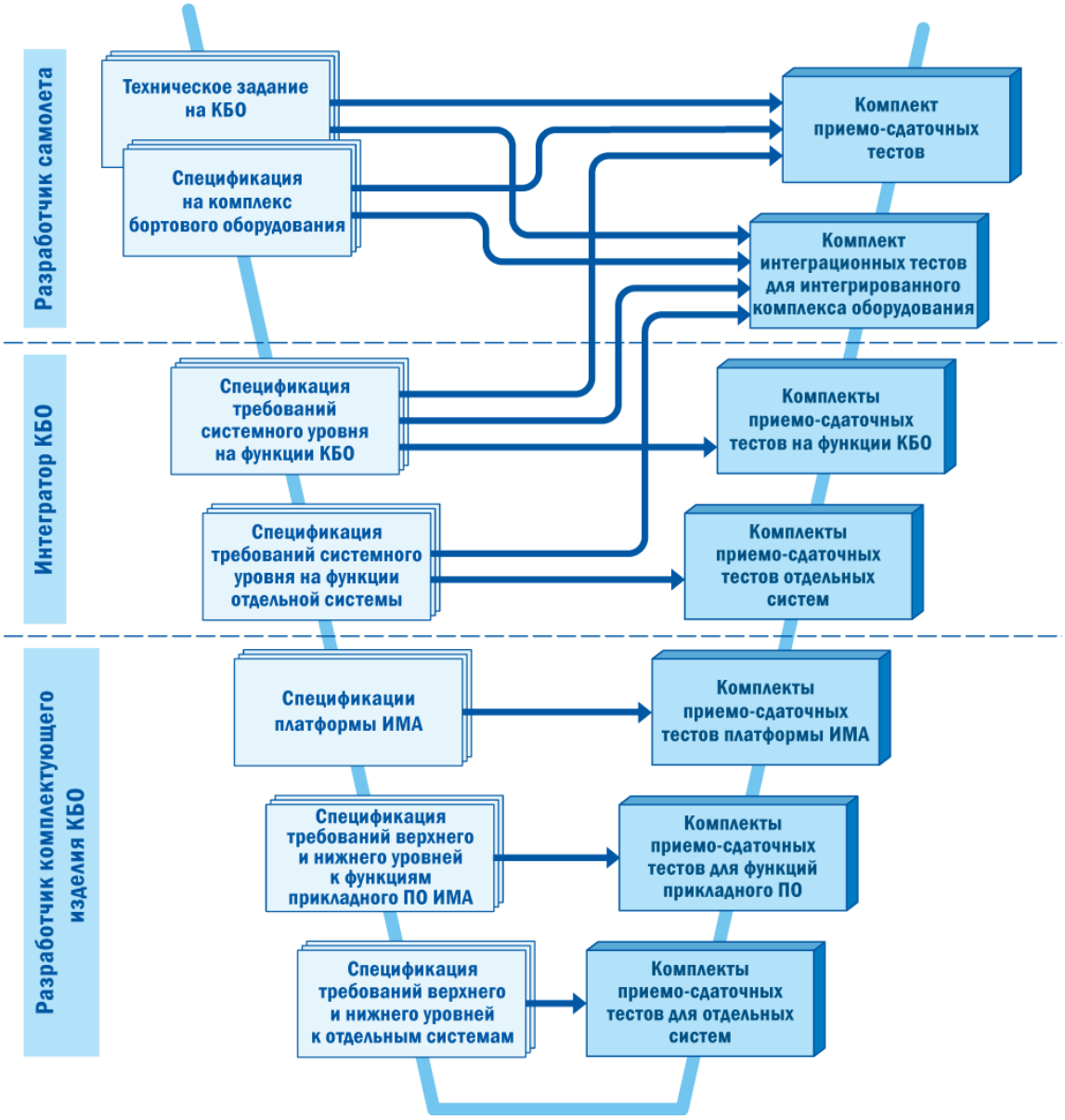


***Рис. 3.10. Взаимосвязь спецификаций КБО и процедур испытаний.***

Стендовая база КБО должна представлять собой систему стендов с единой аппаратно-программной платформой и открытой архитектурой на базе уникальных общепромышленных COTS-компонентов.

Состав стендов должен соответствовать технологии разработки, валидации и верификации программного обеспечения и аппаратуры КБО. Типовой состав приведен на рис. 3.11.


***Рис. 3.11. Типовой состав стендовой базы КБО.***

В основе построения экспериментальной базы стендов должны быть заложены следующие принципы:

- открытость архитектуры;
- модульность программно-аппаратных средств;
- унификация используемых программно-аппаратных средств;
- обеспечение технологической и конструктивной совместимости элементов стендов всех уровней;
- обеспечение информационной совместимости протоколов и интерфейсов стендов;
- применение однотипной элементной базы компонентов стендов;

- использование широко распространенных и апробированных операционных систем, языков и систем программирования;
- применение стандартных, хорошо проработанных интерфейсов, принятых в качестве международных стандартов при реализации соединения устройств авионики.