МЕЖГОСУДАРСТВЕННЫЙ АВИАЦИОННЫЙ КОМИТЕТ
АВИАЦИОННЫЙ РЕГИСТР

РУКОВОДСТВО

по гарантии конструирования бортовой электронной аппаратуры КТ-254

2011

ОГЛАВЛЕНИЕ

ПРИЛОЖЕНИЯ

1. ВВЕДЕНИЕ

Применение усложняющейся электронной аппаратуры для обеспечения многих самолетных функций, критичных для безопасности полета, выдвигает новые проблемы сертификации и безопасности. Эти проблемы возникают из-за того, что многие самолетные функции все больше подвергаются неблагоприятному влиянию ошибок в конструкции аппаратуры, которые достаточно трудно устранить из-за возрастающей сложности оборудования. Чтобы противостоять этой осознаваемой эскалации риска, стало необходимым обеспечить возможность устранения конструктивных ошибок аппаратуры более регулярным и контролируемым образом во время процессов конструирования и сертификации.

По мере усложнения бортового электронного оборудования, развития технологии и накопления опыта в использовании процедур, описанных в данном документе, этот документ будет пересматриваться.

1.1. Назначение документа

Данный документ был подготовлен с целью оказания помощи организациям, обеспечивая руководство для конструирования бортового электронного оборудования, которое безопасно выполняет предназначенные функции в специально установленных условиях эксплуатации. Это руководство должно быть равно применимо к существующим, новым и перспективным технологиям. Назначение данного документа состоит в следующем:

1. Определить цели гарантии конструирования аппаратуры.
2. Описать основу для этих целей – для гарантии правильной интерпретации руководства.
3. Обеспечить описание задач – для того чтобы разработать средства оценки соответствия данному и другим руководствам.
4. Предоставить руководство по действиям в обеспечение качества конструирования – для достижения целей гарантии конструирования.
5. Обеспечить гибкость в выборе процессов, необходимых для достижения целей данного документа, включая усовершенствования процессов по мере появления новых технологий.

Данный документ в большей степени рекомендует действия, которые должны быть выполнены для достижения целей гарантии конструирования, чем дает детальное описание того, как следует выполнять конструирование.

Философия, используемая при создании данного документа – это некоторый нисходящий подход, основанный на функциях системы, выполняемых электронной аппаратурой, а не восходящий подход и не концепция, основанные единственно на специфических компонентах аппаратуры, применяемых для реализации функции. Нисходящий подход более эффективен при рассмотрении ошибок конструирования, влияющих на безопасность, он облегчает конструктивные решения для системы и аппаратных средств и эффективен на этапе верификации. Например, верификация должна выполняться на самом высоком иерархическом уровне системы, устройства и подустройства, компонента или блока аппаратуры, для которого обеспечивается соответствие аппаратного изделия требованиям к нему и выполняются задачи верификации.

1.2. Область применения

Данный документ представляет собой руководство по конструированию бортовой электронной аппаратуры, начиная от концепции, далее через сертификацию и последующие послесертификационные усовершенствования изделия в обеспечение поддержания летной годности. Он разработан для демонстрации соответствия сертификационным требованиям к самолетам транспортной категории и их оборудованию, но некоторые разделы данного документа могут быть применимы и к другому оборудованию. В нем описывается взаимосвязь между жизненным циклом системы и жизненным циклом конструирования аппаратуры, чтобы облегчить понимание взаимоотношений между процессами гарантии конструирования системы и аппаратуры. Он не предназначен для полного описания жизненного цикла системы, включая оценку безопасности системы и обоснования, а также процесса сертификации самолета.

Аспекты сертификации обсуждаются только в отношении жизненного цикла конструирования аппаратуры. Аспекты, связанные с возможностью создания, испытания и технического обслуживания аппаратуры, рассматриваются только в контексте летной годности конструкции аппаратуры.

Руководство в данном документе применимо к следующим, но не только, компонентам аппаратуры:

1. Быстросменные блоки.
2. Монтажные платы.
3. Микропрограммируемые пользователем компоненты, такие, как заказные специализированные интегральные схемы и программируемые логические интегральные схемы, включая любые связанные макрофункции.
4. Интегрированные технологические компоненты, такие, как гибридные и многокристальные модули.
5. Покупные компоненты.

Дополнительные рассмотрения, относящиеся специально к COTS-компонентам, включены в раздел 11, поскольку поставщики компонентов COTS не обязаны следовать процессу конструирования, описанному в данном документе, или обеспечивать необходимые данные жизненного цикла конструирования аппаратуры.

В данном документе не делается попытка определить программно-аппаратные средства. Программно-аппаратные средства должны быть классифицированы как аппаратные средства или как программное обеспечение и рассматриваться в соответствующих процессах. Данный документ предполагает, что во время определения системы ее функции распределятся между аппаратными средствами и программным обеспечением. Документ КТ-178В обеспечивает руководство для функций, которые назначены для реализации в программном обеспечении. Настоящий документ обеспечивает руководство для функций, которые назначены аппаратным средствам.

Примечание. *Такой подход позволяет определить эффективный метод реализации и гарантии конструирования в момент спецификации системы и распределения функций. Все части должны быть согласованы с данным системным решением в момент, когда сделано распределение функций.*

Оценка и квалификация инструментов, используемых при конструировании и верификации компонента аппаратуры, описаны в подразделе 11.4.

Данный документ не обеспечивает руководство, касающееся организационных структур или распределения ответственности между этими структурами.

Критерии квалификации в условиях эксплуатации также выходят за рамки содержания данного документа.

1.3. Связь с другими документами

Помимо требований летной годности, имеются различные национальные и международные стандарты на аппаратные средства. В некоторых случаях может потребоваться демонстрация соответствия этим стандартам. Однако в рамках данного документа не предполагается рассматривать специальные национальные и международные стандарты или предлагать средства, с помощью которых эти стандарты могут использоваться как альтернативные или дополнительные к данному документу.

Когда в данном документе используется термин «стандарты», это означает, что применяются стандарты, принятые обязательными для конкретного проекта бортовой системы, бортового оборудования, двигателей, или стандарты разработчика воздушного судна. Подобные стандарты могут быть получены из общих стандартов, созданных или принятых фирмой-изготовителем. Описание стандартов дано в подразделе 10.2.

1.4. Документы, относящиеся к рассматриваемому вопросу

Документ Р-4754 «Руководство по процессам сертификации высокоинтегрированных или сложных бортовых систем воздушных судов гражданской авиации» – как основа для конструирования высокоинтегрированных или сложных авиационных систем.

Документ Р-4761 «Руководство по методам оценки безопасности систем и бортового оборудования воздушных судов гражданской авиации» – как основа методов оценки безопасности, которые должны использоваться в процессе гарантии конструирования аппаратуры.

Документ «Требования к программному обеспечению бортовой аппаратуры и систем при сертификации авиационной техники КТ-178В» – как дополнительный документ по гарантии разработки ПО.

Документ «Условия эксплуатации и окружающей среды для бортового авиационного оборудования КТ-160()» может быть использован разработчиками оборудования как основной стандарт испытаний элементов квалификации аппаратуры на внешние воздействия.

1.5. Как применять данный документ

Данный документ предназначен для применения международным авиационным сообществом. Чтобы облегчить его применение, ссылки на специальные национальные правила и процедуры сведены к минимуму. Вместо этого используются общие термины. Например, термин «сертифицирующий орган» означает организацию или персону, которому предоставлено право одобрения от имени страны, ответственной за сертификацию. Когда вторая страна или группа стран проводит или участвует в данной сертификации, настоящий документ может использоваться в рамках двухстороннего соглашения или меморандума взаимопонимания между участвующими странами.

Руководящие положения в данном документе представляют собой консенсус авиационного сообщества и являются собранием наилучших практических промышленных данных по гарантии конструирования бортовой электронной аппаратуры. Принимая во внимание процесс, разработанный в данном документе, было намерение создать руководство, которое могло бы быть применимым к совершенно новым разработкам аппаратных средств и последующим изменениям. Руководящие указания для аппаратных средств, ранее разработанные по другим процессам, рассматриваются в подразделе 11.1. Понятно, что средства, отличные от тех, что описаны здесь, могут существовать и могут быть использованы заявителем.

В тех случаях, когда для того чтобы показать, как могут быть применены руководящие указания, примеры используются либо графически, либо повествовательно, они не должны интерпретироваться как предпочтительный метод.

В разделе 11 обсуждаются дополнительные указания для особых известных случаев, для которых задачи разделов с 2 по 9 не могут быть выполнены. К ним относятся описание ранее разработанных аппаратных средств, использование компонентов COTS, опыт эксплуатации изделия, оценка и квалификация инструментальных средств.

В Приложении А представлено руководство по необходимым данным жизненного цикла конструирования аппаратуры, основанным на реализуемом уровне гарантии конструирования.

В Приложении В даны руководящие указания по методам гарантии конструирования для аппаратных средств, используемых для реализации функций уровней А и В, которые должны применяться дополнительно к указаниям разделов с 2 по11. Приложение В можно применять к аппаратуре уровней С и D гарантии конструирования на усмотрение заявителя.

Словарь терминов содержится в Приложении С.

Приложение D содержит перечень сокращений, которые используются в документе, и их полное название. Перечень не предполагает, что дается полное описание или что все элементы значимы для конкретного изделия.

Примечания используются в данном документе для того, чтобы дать объяснения, выделить пункт или привлечь внимание к соответствующим предметам, которые не полно описаны в контексте. Примечания не содержат руководящие указания.

Слово «должен» используется, когда есть намерение обеспечить руководство. Слово «может» относится к необязательной информации.

В данном документе используется термин «элемент аппаратуры» для описания электронной аппаратуры, которая является предметом данного документа.

Определитель «аппаратный» принят в рамках всего документа, если не оговорено особо. Применение термина «требования» означает «требования к аппаратным средствам». Определители «системный» или «программное обеспечение» всегда будет применяться специализировано, например «требование к системе».

Примечание. *Различные промышленные рекомендательные документы и авиационные требования не всегда используют адекватную терминологию. Читателю следует знать об этом при использовании того или иного термина. Определения терминов, используемых в документе, даны в Словаре терминов.*

1.6. Определение сложности

Хотя в различных классификациях термин «сложность» используется для описания электроники, как простой, сложной и очень сложной, разница между этими классификациями четко не определена. Определение различий в сложности в данном документе основано на осуществимости и уровне трудности, необходимом для выполнения допустимого покрытия верификации детерминистскими средствами.

Проверка аппаратуры должна проводиться иерархически на уровнях интегральных схем, плат и быстросменных блоков по степени интеграции, включая соответствующие функции, которые не могут быть проверены, такие, как неиспользуемые режимы в устройствах многократного применения и потенциально скрытые состояния в последовательных машинах.

Элемент аппаратуры определяется как простой, только если обширная комбинация детерминистских испытаний и анализов, соответствующих уровню гарантии конструирования, сможет гарантировать правильность функциональной характеристики во всех предполагаемых условиях эксплуатации без аномалий в поведении.

Когда элемент не может быть классифицирован как простой, он должен быть классифицирован как сложный. Элемент, созданный из простых элементов, сам может быть сложным. Элементы, которые содержит схема, такие, как ASIC и PLD, могут считаться простыми, если они соответствуют критерию простоты, описанному в этом подразделе.

Чтобы снизить риск проекта, предлагаемые средства обеспечения гарантии конструирования для сложных элементов должны быть согласованы с сертифицирующим органом на раннем этапе жизненного цикла конструирования аппаратуры.

Для простого элемента аппаратуры нет необходимости в обширной документации на процесс конструирования. Поддерживающие процессы верификации и управления конфигурацией должны выполняться и документироваться и для простого элемента аппаратуры, но обширная документация не требуется. Следовательно, существуют незначительные издержки при конструировании простого элемента аппаратуры, соответствующего данному документу. Основное влияние данного документа должно быть направлено на конструирование сложных элементов аппаратуры.

1.7. Альтернативные методы или процессы

Для гарантии конструирования аппаратуры могут использоваться методы или процессы, отличные о тех, которые описаны в настоящем документе. Эти методы и процессы должны быть оценены на основе их способности удовлетворять применяемым правилам. Альтернативные методы или процессы должны быть одобрены сертифицирующим органом до их внедрения. Вместо прямого сравнения с применяемыми правилами для уменьшения риска проекта при оценке альтернативных методов или процессов путем сравнения с данным документом заявитель может использовать следующее инструкции.

Внимание при оценке альтернативных методов и процессов может быть обращено на следующее:

1. Когда вместо процессов, предписанных данным документом, используются иные процессы, то следует показать, что они обеспечивают эквивалентный уровень гарантии конструирования в отношении одной или более целей, указанных в разделах с 2 по 9 данного документа.
2. Следует оценить влияние предложенных альтернативных методов или процессов на удовлетворение целей гарантии конструирования аппаратуры.
3. Следует оценить влияние предложенных альтернативных методов или процессов на данные жизненного цикла.
4. Логическое обоснование использования предложенных альтернативных методов или процессов следует подтвердить доказательствами того, что методы или процессы дадут ожидаемые результаты.

1.8. Обзор документа

На рисунке 1-1 дан графический обзор разделов данного документа и некоторые их связи с другими разделами или с другими соответствующими процессами. Цель состоит не в том, чтобы показать поток данных, а в том, чтобы показать, как соотносятся разделы и внешние процессы.

1.9. Отличия данного документа от DO-254/ED-80

Настоящий документ следует рассматривать как технический перевод документа RTCA DO-254/EUROCAE ED-80 «Design Assurance Guidance for Airborne Electronic Hardware».

В документе сохранены все разделы и подразделы документа DO-254/ED-80.

Раздел 1 дополнен настоящим подразделом.

Подраздел 1.4 содержит ссылки на документы, аналогичные указанным в DO-254/ED-80

В раздел 5 добавлено Примечание 3 о рекомендуемом сопоставлении стадий конструирования и документов по Единой системе конструкторской документации с процессами и данными в настоящем документе.

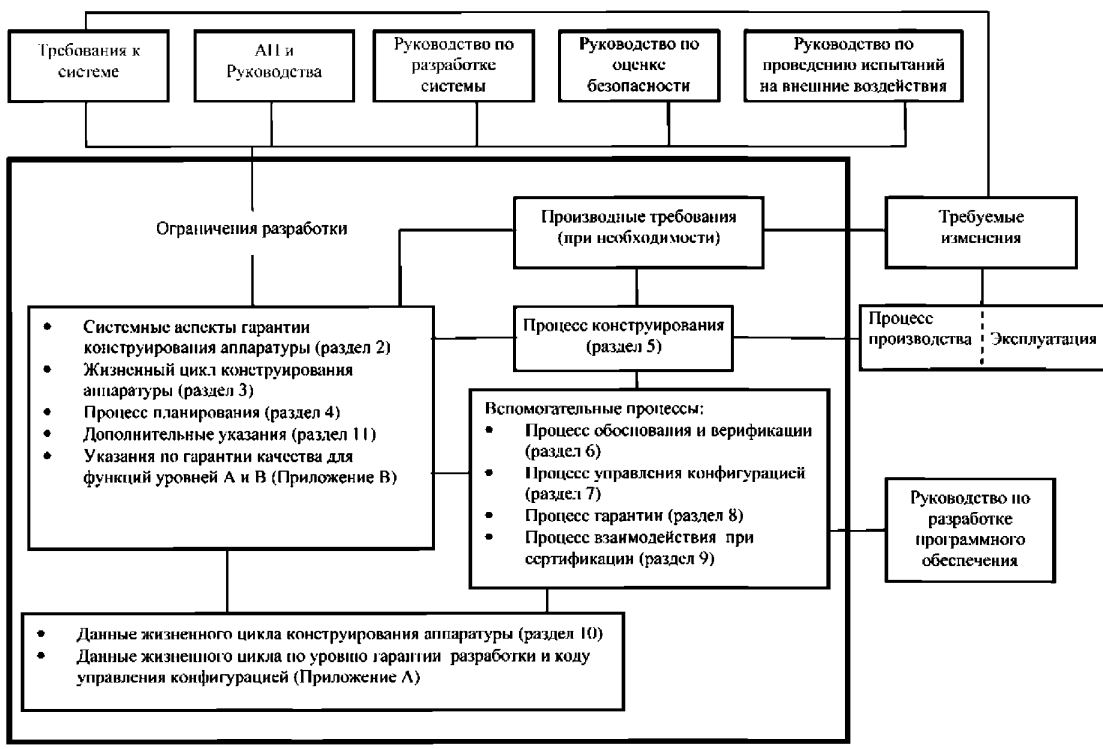

Рисунок 1-1. Обзор документа

2. СИСТЕМНЫЕ АСПЕКТЫ ГАРАНТИИ КОНСТРУИРОВАНИЯ АППАРАТУРЫ

Гарантия конструирования аппаратуры начинается на уровне системы с распределения функций системы аппаратным средствам и с назначения им соответствующих системе уровней гарантии конструирования.

Отдельная функция системы может быть назначена компоненту аппаратуры, компоненту программного обеспечения или комбинации аппаратуры и ПО. Требования по безопасности, связанные с функцией, рассматриваются с точки зрения системы, с точки зрения ПО и с точки зрения аппаратуры для определения уровня надежности и уровня гарантии, необходимых для удовлетворения этим требованиям.

На рисунке 2-1 показано взаимоотношение процесса разработки системы для бортовых систем и оборудования с оценкой безопасности, конструированием аппаратуры и процессом разработки ПО.

Рисунок 2-1. Взаимоотношение между бортовыми системами, оценкой безопасности и процессами аппаратных средств и ПО

На рисунке 2-1 представлены четыре области совмещения: Безопасность/Аппаратура, Безопасность/ПО, Аппаратура/ПО и Безопасность/Аппаратура/ПО. Эти совмещения иллюстрируют взаимоотношения и взаимодействия между данными процессами, когда требования к системе могут выражаться в относящихся требованиях и указаниях по гарантии конструирования многих процессов. Например, функция аппаратуры, которая содержит требования по безопасности, будет входить как процесс оценки безопасности, так и процесс жизненного цикла конструирования аппаратуры.

Совмещения показывают необходимость в координированном взаимодействии между процессами с целью обеспечения удовлетворения требований к функции системы. Обсуждение процессов обеспечения ПО или системы выходит за рамки данного документа. Однако при координации конструирования для функции аппаратуры заявитель может пожелать воспользоваться преимуществом гарантии, обеспечиваемой деятельностью в процессах системы или программного обеспечения.

Эти взаимоотношения и взаимосвязи описываются в подразделах с 2.1.1 по 2.1.3 ниже.

2.1. Информационный поток

Поток информации между процессами жизненного цикла представлен на рисунке 2-2. В следующих подразделах описывается поток информации от процесса разработки системы к процессу жизненного цикла конструирования аппаратуры, от процесса жизненного цикла конструирования аппаратуры к процессу разработки системы и между процессом жизненного цикла конструирования аппаратуры и процессом жизненного цикла программного обеспечения.

Примечание. *Считается, что эти процессы итеративные, а изменения могут наблюдаться в пределах всего жизненного цикла конструирования аппаратуры.*

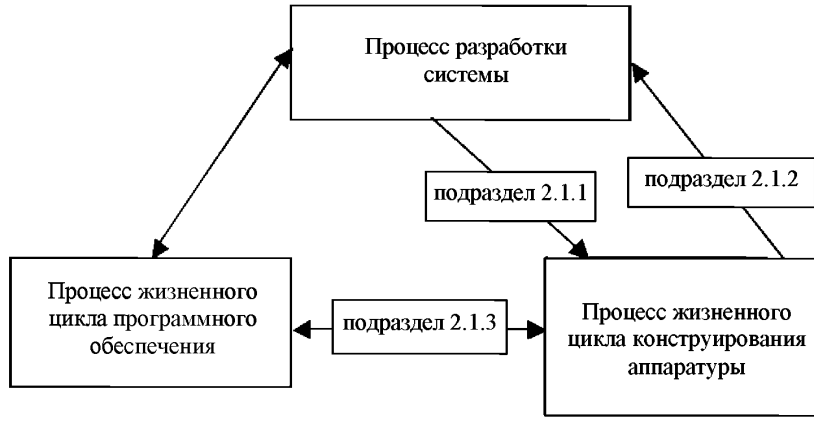

Рисунок 2-2. Процессы разработки системы

2.1.1. Информационный поток от процесса разработки системы к процессу жизненного цикла конструирования аппаратуры

Эта информация может включать:

1. Требования к конструкции и по безопасности, предъявляемые к аппаратуре.
2. Уровень гарантии разработки для каждой функции вместе с соответствующими требованиями и условиями отказа, если применимо.
3. Распределенные вероятности и время подверженности риску для функциональных отказов аппаратуры.
4. Описание интерфейса аппаратура/программное обеспечение.
5. Требования к стратегии безопасности и конструктивные ограничения, такие, как контролепригодность, методы конструирования и архитектура аппаратуры.
6. Требования по верификации системы, которые должны выполняться на уровне верификации аппаратуры.
7. Требования к размещению, к эргономике и окружающим условиям, относящиеся к аппаратуре.
8. Отчеты о проблемах интеграции, которые могут оказать влияние на требования. Они могут возникнуть в результате таких видов деятельности, как верификация системы, формирование требований к системе и оценка безопасности системы.

2.1.2. Информационный поток от процесса жизненного цикла конструирования аппаратуры к процессу разработки системы

Этот информационный поток может включать:

1. Реализацию требований в виде чертежей, схем и перечней деталей.
2. Производные требования к аппаратуре, которые могут оказать влияние на любое предписанное требование.

3. Архитектура реализации, включая пределы парирования неисправностей.
4. Подтверждающие материалы по любому требуемому мероприятию верификации и обоснования, выполненному во время жизненного цикла конструирования аппаратуры.
5. Данные анализа безопасности изделия, такие, как:
   a. Вероятности и интенсивности отказов для обозначенных функциональных отказов, относящихся к процессу SSA.
   b. Анализ отказов общего режима.
   c. Границы локализации и общие стратегии ослабления последствий отказов.
   d. Данные анализа скрытых состояний, относящиеся к системным требованиям. Примерами являются аппаратные средства контроля отказов, интервалов обнаружения отказов и необнаруживаемые отказы.
6. Требования к действиям по верификации аппаратуры, которые должны выполняться при верификации на уровне системы.
7. Допущения и методы анализа требований по установке и окружающим условиям, необходимым для достоверности результатов исследований.
8. Отчеты о проблемах или изменениях, которые могут повлиять на требования к системе, к программному обеспечению или к аппаратуре.

2.1.3. Информационный поток между процессом жизненного цикла конструирования аппаратуры и процессом жизненного цикла программного обеспечения

Эта информационный поток может содержать:

1. Производные требования, необходимые для интеграции аппаратуры/ПО, такие, как определение протоколов, временных ограничений и схем адресации интерфейса аппаратуры и ПО.
2. Ситуации, при которых верификация аппаратуры и ПО требует координации.
3. Выявленные несовместимости между аппаратурой и ПО, которые могут входить в систему регистрации внесения изменений.
4. Данные оценки безопасности, которые также должны быть доступны для системных процессов.

2.2. Процессы оценки безопасности системы

Существует три процесса оценки безопасности системы: оценка функциональной опасности, предварительная оценка безопасности системы и собственно оценка безопасности системы. Эти процессы используются для установления целей безопасности системы, применимых к процессу гарантии разработки системы и определения того, что функции системы достигают целей безопасности.

Процесс SSA должен преобразовывать цели безопасности в требования по безопасности к системе и аппаратуре. Эти требования должны включать основные цели безопасности и характеристики безопасности для функций и архитектуры системы и аппаратуры. Процесс SSA и процесс разработки системы распределяет эти требования безопасности к аппаратуре.

Существует пять уровней гарантии разработки системы, с уровня A до уровня E, соответствующие пяти категориям отказных состояний: катастрофическое, аварийное, сложное, усложнение условий полета и без последствий. В таблице 2-1 установлено соотношение уровней гарантии конструирования аппаратуры с пятью категориями отказных состояний, даны определения отказных состояний аппаратуры и соответствующих им уровней гарантии конструирования. Первоначально уровень гарантии конструирования аппаратуры для каждой функции аппаратуры определяется процессом SSA путем использования FHA для определения потенциальных опасностей, а затем в процессе PSSA распределяются требования по безопасности и соответствующие отказные состояния по функциям, реализуемым в аппаратуре.

В течение жизненного цикла конструирования аппаратуры может существовать итеративная обратная связь между процессами оценки безопасности, разработки системы и конструирования аппаратуры для гарантии того, что сконструированная и изготовленная аппаратура удовлетворяет требованиям по безопасности, функциональным требованиям и требованиям к рабочим характеристикам системы, предназначенным аппаратуре.

Таблица 2-1. Определения уровня гарантии конструирования аппаратуры и их взаимоотношения с уровнем гарантии разработки системы

Уровень гарантии разработки системы	Классификация отказного состояния	Описание отказного состояния	Определение уровня гарантии конструирования аппаратуры
Уровень A	Катастрофическое	Отказное состояние, для которого принимается, что при его возникновении предотвращение гибели людей оказывается практически невозможным	A: Аппаратура, ненормальное выполнение функций которой, согласно оценке, полученной в процессе анализа безопасности аппаратуры, может вызвать или способствовать отказу функции системы, приводящему к катастрофическому отказному состоянию для воздушного судна
Уровень B	Аварийное	Отказное состояние, которое может привести к значительному ухудшению характеристик воздушного судна и/или физическому утомлению, или такой рабочей нагрузке экипажа, что уже нельзя полагаться на то, что он выполнит свои задачи точно и полностью	B: Аппаратура, ненормальное выполнение функций которой, согласно оценке, полученной в процессе анализа безопасности аппаратуры, может вызвать или способствовать отказу функции системы, приводящему к аварийному отказному состоянию для воздушного судна
Уровень C	Сложное	Отказное состояние, которое может привести к заметному ухудшению характеристик воздушного судна и/или выходу одного или нескольких параметров за эксплуатационные ограничения, но без достижения предельных ограничений, и/или уменьшению способности экипажа справиться с неблагоприятными условиями, как из-за увеличения рабочей нагрузки, так и из-за условий, понижающих эффективность действий экипажа	C: Аппаратура, ненормальное выполнение функций которой, согласно оценке, полученной в процессе анализа безопасности аппаратуры, может вызвать или способствовать отказу функции системы, приводящему к сложному отказному состоянию для воздушного судна
Уровень D	Усложнение условий полета	Отказное состояние, которое может привести к незначительному ухудшению характеристик воздушного судна, и/или незначительному увеличению рабочей нагрузки на экипаж	D: Аппаратура, ненормальное выполнение функций которой, согласно оценке, полученной в процессе анализа безопасности аппаратуры, может вызвать или способствовать

Уровень гарантии разработки системы	Классификация отказного состояния	Описание отказного состояния	Определение уровня гарантии конструирования аппаратуры
			отказу функции системы, приводящему к отказному состоянию для воздушного судна типа усложнение условий полета
Уровень E	Без последствий	Отказное состояние, которое не влияет на характеристики воздушного судна и не увеличивает рабочую нагрузку на экипаж	E: Аппаратура, ненормальное выполнение функций которой, согласно оценке, полученной в процессе анализа безопасности аппаратуры, может вызвать или способствовать отказу функции системы без влияния на эксплуатационные возможности воздушного судна или загрузку экипажа. К функциям уровня E не требуется применение каких-либо положений данного документа, однако они могут использоваться как ориентиры

2.3. Оценка безопасности аппаратуры

Оценка безопасности аппаратуры производится в соответствии и в обеспечение процесса SSA. Назначение этого процесса безопасности заключается в демонстрации того, что применяемые системы и оборудование, включая аппаратуру, удовлетворяют требованиям по безопасности применимых правил сертификации воздушного судна.

Используя требования по безопасности, функциональные требования и требования к характеристикам, которые предъявлены к аппаратуре, оценка безопасности аппаратуры определяет уровень гарантии конструирования аппаратуры для каждой функции и содействует определению используемой стратегии обеспечения гарантии конструирования.

2.3.1. Обсуждение оценки безопасности аппаратуры

Разработчик компонента аппаратуры может показать соответствие требованиям по безопасности, предъявляемым к аппаратуре, и уровню гарантии конструирования аппаратуры по соответствующей стратегии гарантии конструирования.

Один уровень гарантии конструирования и одна стратегия могут быть применимы ко всему элементу аппаратуры, или элемент аппаратуры может быть оценен как имеющий отдельные тракты функционального отказа – для того чтобы включить несколько уровней гарантии конструирования или стратегий гарантии конструирования. Анализ тракта функционального отказа может использоваться для того, чтобы оправдать более низкий уровень гарантии конструирования для части элемента аппаратуры или для реализации различных функций, применяемых с различными технологиями или различным характером эксплуатации изделия.

Примечание. *Описание FFPA приведено в разделе 2 Приложения B. Хотя он адресован конкретному предмету Приложения B, этот метод анализа может быть применен к любому уровню гарантии конструирования.*

Если элемент аппаратуры содержит функции, которые сами имеют различные уровни гарантии конструирования, то в подобных ситуациях можно применять любой из следующих методов:

Весь элемент может отвечать самому высокому уровню гарантии конструирования.

Отдельные функции (реализующие их функциональные компоненты) могут отвечать раздельно их соответствующим уровням гарантии конструирования, как это определяется оценкой безопасности аппаратуры, если их функционирование, интерфейсы и разделяемые ресурсы могут быть защищены от неблагоприятных влияний функциональных компонентов с более низкими уровнями гарантии конструирования. Гарантией конструирования разделяемых ресурсов будет служить уровень гарантии конструирования функции с наивысшим уровнем.

Руководство по оценке безопасности аппаратуры включает следующие положения:

1. Итеративная оценка безопасности аппаратуры и конструирование должны определять производные требования по безопасности аппаратуры и гарантировать выполнение предписанных аппаратуре требований по безопасности и производных требований.
2. Эти производные требования должны содержать требования по безопасности к архитектуре аппаратуры, схемам и компонентам и защите от аномального поведения, включая применение специальных характерных свойств архитектурной и функциональной безопасности аппаратуры, таких, как:
   a. Резервирование компонентов и схем;
   b. Разделение или электрическая изоляция между схемами и компонентами;
   c. Разнородность схем или компонентов;
   d. Контроль схем или компонентов;
   e. Механизмы защиты или реконфигурации;
   f. Допустимые интенсивности отказов и вероятности случайных отказов и скрытых отказов для схем и компонентов;
   g. Ограничения по применению или установке;
   h. Предупреждение и контроль срывов в работе и восстановление после срывов.
3. Процесс гарантии конструирования аппаратуры и оценка безопасности аппаратуры должны вместе определять специальные методы обеспечения соответствия и уровень гарантии конструирования для каждой функции и должны определять, что приемлемый уровень гарантии конструирования достигнут.

Примечание. *Аномальное поведение аппаратуры может быть вызвано случайными неисправностями или ошибками конструирования элемента аппаратуры или срывами в работе аппаратуры.*

Конструктор аппаратуры может выбрать более высокий уровень гарантии конструирования аппаратуры для реализующего функцию компонента аппаратуры. Примером может служить возможность повторного использования этого компонента аппаратуры в установке, требующей более высокого уровня гарантии конструирования.

В оценке безопасности аппаратуры могут использоваться различные методы количественной и качественной оценки. К ним относятся анализ дерева неисправности, анализ общего режима, анализ видов и последствий отказов, методы статистической оценки надежности для прикладной количественной оценки случайных отказов.

2.3.2. Количественная оценка случайных отказов аппаратуры

Методы прогнозирования и статистической оценки отказов, которые основаны на интенсивностях отказов аппаратуры, резервировании, разделении и изоляции, статистических данных о видах отказов, анализе вероятности, контроле процесса конструирования подтвердили свою пригодность как средства оценки количественных факторов риска для случайных отказов аппаратуры.

2.3.3. Качественная оценка ошибок конструирования аппаратуры и срывов

В отличие от случайных отказов аппаратуры ни ошибки конструирования, ни некоторые типы срывов статистически непрогнозируемы, и могут пересекать границы резервирования в форме отказов общего режима. Методы, которые должны использоваться для управления резервом, и методы количественной оценки нужно выбирать так, чтобы потенциальные отказы общего режима и влияние срывов могли быть, когда это необходимо, предотвращены или уменьшены.

Несмотря на трудности количественной оценки, угроза безопасности от ошибок конструирования и срывов может быть на практике эффективно оценена методами качественной оценки безопасности. Такие методы анализа, как анализ дерева неисправности, анализ общего режима и функциональный анализ видов и последствий отказа, являются основными качественными методами и могут использоваться для оценки ошибок конструирования и срывов. В частности, эти методы могут определять потенциальные влияния ошибок конструирования и срывов и могут помочь в определении средств, с помощью которых ошибки и срывы могут быть предотвращены или ослаблено их влияние. Применение данных методов позволит включить оценку безопасности аппаратуры в определение стратегий гарантии конструирования аппаратуры, которые используются и могут использоваться итеративно в течение всего процесса конструирования аппаратуры для качественного определения гарантии конструирования, достигнутого с помощью выбранных стратегий.

2.3.4. Обсуждение гарантии конструирования для классификации отказных состояний аппаратуры

По мере возрастания степени опасности отказного состояния системы увеличивается значимость гарантии конструирования – в обеспечение того, что относящиеся отказные состояния ослаблены. Для всех уровней гарантии конструирования должен быть разработан соответствующий подход или стратегия. На рисунке 2-3 представлен процесс принятия решения для разработки соответствующей стратегии гарантии конструирования.

Устанавливается следующее:

1. Для реализуемых в аппаратуре функций уровня А или В при определении гарантии конструирования следует рассматривать потенциальные аномальные поведения или потенциальные ошибки при конструировании функций аппаратуры.
2. При разработке стратегий гарантии конструирования каждой реализуемой функции следует использовать процесс принятия решения, представленный на рисунке 2-3.
3. В дополнении к правилам, данным в разделах с 3 по11, для функций уровней А и В следует применять стратегии, описанные в Приложении В.
4. Стратегию гарантии конструирования следует выбрать в зависимости от архитектуры аппаратуры и выбранной технологии реализации аппаратуры.

Разные технологии, отличия в подборе компонентов и их использовании дают отличающуюся информацию жизненного цикла конструирования аппаратуры и различные степени внутренней защиты от ошибок конструирования и их последствий. Наиболее подходящий метод гарантии конструирования может варьироваться для различных функций внутри одного и того же элемента аппаратуры.

Цифры в блоках принятия решения и действий на рисунке 2-3 относятся к сопровождающим рисунок пронумерованным примечаниям, которые поясняют решение или действие.

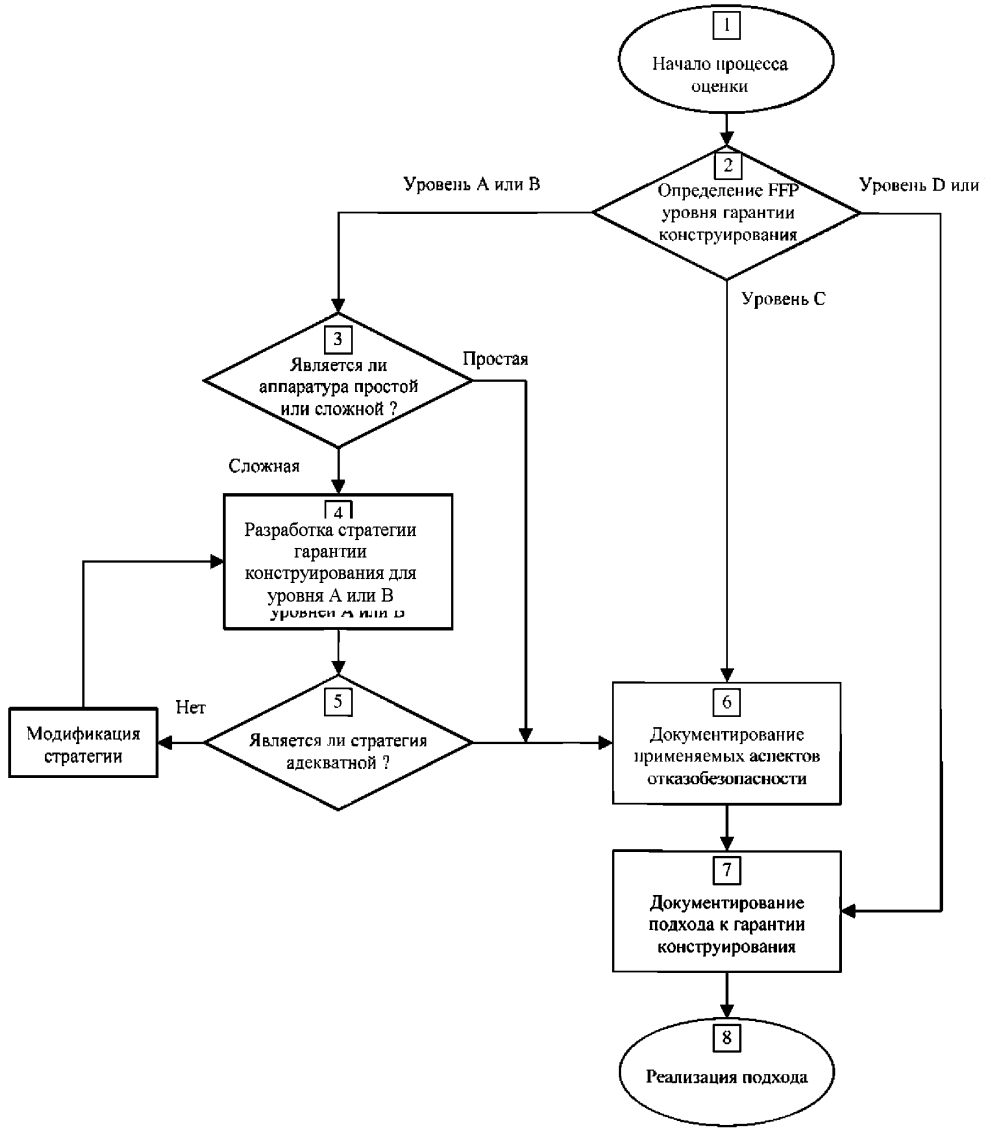

Рисунок 2-3. Процесс принятия решения для выбора стратегии гарантии конструирования аппаратуры

1. Начало процесса оценки. Для всех уровней гарантии конструирования должен быть разработан подход или стратегия обеспечения соответствующего уровня гарантии конструирования.

2. Определение FFP уровня гарантии конструирования. Для каждого определенного элемента аппаратуры определите и документируйте тракты функционального отказа, связанные с элементом, и уровень гарантии конструирования. Следует использовать общепринятые методы оценки безопасности для определения того, какие аппаратные схемы есть, а каких нет в идентифицированных трактах функционального отказа уровня A или B.

3. Является ли аппаратура простой или сложной? Для трактов функционального отказа уровня A или B гарантии конструирования аппаратуры определите, является ли аппаратура простой или сложной, как описано в подразделе 1.6.

4. Разработка стратегии гарантии конструирования сложных FFPs уровня A или B. Если тракт функционального отказа сложный, а уровень A или B, используйте дополнительные стратегии, описанные в Приложении B, для определения стратегии гарантии конструирования, соответствующей концепции применения и методам ослабления влияния ошибок. Для каждого тракта функционального отказа уровня A или B должна быть определена стратегия гарантии конструирования, используя эффективный анализ, опыт эксплуатации изделия или архитектурное ослабление влияния.

   При реализации трактов функционального отказа уровня A может потребоваться более одного метода, если выбранный метод не обеспечивает полного снижения потенциальных отказов и аномальных поведений.

5. Является ли стратегия адекватной? Определите, существуют ли недостатки в стратегиях гарантии конструирования и, если недостатки в стратегии существуют или будут существовать в предлагаемых данных, модифицируйте стратегию, с тем чтобы скорректировать недостатки, предлагая дополнительную гарантию конструирования, реализации или архитектурную стратегию. Когда стратегия гарантии конструирования является приемлемой, документируйте процессы гарантии конструирования для каждого тракта функционального отказа. Стратегия должна быть связана с аспектами участия сертифицирующего органа, такими, как планы, рассмотрение программ и контроль деятельности.

6. Документирование применяемых аспектов отказобезопасности. Определите соответствующую отказобезопасную архитектуру и характеристики элемента аппаратуры и выполните анализ с целью удовлетворения требований к готовности и целостности системы. Документируйте аспекты отказобезопасной конструкции и соответствующий анализ общего режима, анализ вероятности, архитектурные и другие особенности.

7. Документирование подхода к гарантии конструирования. Документируйте и получите одобрение сертифицирующего органа для соответствующих стратегии и метода в плане сертификации системы или в плане сертификации аппаратуры.

8. Реализация подхода. Реализуйте конструкцию аппаратуры в соответствии с подходом к обеспечению гарантии конструирования, как определено в одобренном плане, и документируйте материалы, подтверждающие соответствие одобренным планам и стратегии.

3. ЖИЗНЕННЫЙ ЦИКЛ КОНСТРУИРОВАНИЯ АППАРАТУРЫ

В этом разделе описывается жизненный цикл конструирования аппаратуры, обсуждаемый в разделах с 4 по 9. В данном документе не обсуждается ни наиболее предпочтительная модель жизненного цикла, ни подразумеваемая структура реализующей проект организации. Жизненный цикл конструирования аппаратуры равно применим как к разработке новых систем или оборудования, так и к модификациям существующих систем и оборудования. Жизненный цикл для каждого проекта должен основываться на выборе и распределении процессов и действий, определяемых атрибутами проекта, такими, как стабильность требований, применение ранее разработанной аппаратуры и уровни гарантии конструирования аппаратуры. Процессы жизненного цикла конструирования аппаратуры могут быть итеративными, т.е. первично выполненными, повторно выполненными и модифицированными вследствие расширяющегося конструирования и обратной связи между процессами.

3.1. Процессы жизненного цикла конструирования аппаратуры

Процессами жизненного цикла конструирования аппаратуры являются:

1. Процесс планирования аппаратуры, описываемый в разделе 4, определяет и координирует действия конструирования аппаратуры и процессы поддержки проекта.
2. Процессы конструирования аппаратуры, описываемые в разделе 5, формируют данные конструирования и результирующее аппаратное изделие. Эти процессы охватывают формирование требований, эскизное проектирование, детальное проектирование, реализацию и переход к производству.
3. Процессы поддержки, описываемые в разделах с 6 по 9, формируют данные жизненного цикла конструирования аппаратуры, которые обеспечивают правильность и управление жизненным циклом конструирования аппаратуры и его выходными данными, включая планирование, конструирование, оценку безопасности аппаратуры и процессы поддержки. Эти процессы, как правило, выполняются одновременно с процессами планирования и конструирования. К этим процессам относятся обоснование, верификация, управление конфигурацией, процесс гарантии и взаимодействие при сертификации.

3.2. Критерии перехода

Проблемы разработки изделия с различными элементами на различных этапах разработки требуют методов для обеспечения целесообразного управления процессом конструирования, чтобы справляться с риском запуска следующего процесса до того, как будут завершены все части предыдущего процесса. Критерии перехода, определенные как минимальные данные, используемые для оценки передвижения от одного процесса к другому, могут использоваться в ключевых точках процесса. Анализ, выполняемый в процессе планирования, должен определять применение критериев перехода. Нет необходимости устанавливать критерии перехода между каждой парой этапов процессов, определенных в планах. Выбор критерия перехода должен быть связан с влиянием на безопасность. Например, перед выполнением верификации функции для получения сертификационного зачета требования к этой функции должны быть документированы и ее реализация должна находиться под управлением конфигурацией.

Критерии перехода должны быть документированы в планах аппаратуры. Использование критериев перехода не предполагает никакую конкретную модель жизненного цикла и не препятствует таким стратегиям конструирования, как быстрая разработка прототипа и параллельное конструирование.

4. ПРОЦЕСС ПЛАНИРОВАНИЯ

В данном разделе описывается процесс планирования аппаратуры, используемый для управления конструированием элемента аппаратуры. В рамках данного процесса формируются планы аппаратуры, которые могут содержаться в одном или более документах. Если используется множество документов, главный план должен содержать соответствующие ссылки на необходимые документы. Стандартные документы, обеспечивающие реализацию специфических процессов жизненного цикла конструирования аппаратуры, таких, как процесс управления конфигурацией или процесс гарантии, допускаются при условии, что они отвечают задачам планирования для соответствующего процесса.

4.1. Цели процесса планирования

Назначение процесса планирования состоит в определении средств, с помощью которых функциональные требования и требования к летной годности преобразуются в элемент аппаратуры и сопровождаются приемлемым количеством доказательств, гарантирующих, что он будет безопасно выполнять предназначенные ему функции. Цели процесса планирования следующие:

1. Определение процессов жизненного цикла конструирования аппаратуры.

Примечание. *В планы могут быть включены действия, контрольные точки, входные и выходные данные, организационная ответственность.*

2. Определение и выбор стандартов.
3. Определение или выбор среды конструирования и верификации.
4. Представление сертифицирующему органу средств подтверждения соответствия целям гарантии конструирования аппаратуры, включая стратегии, определенные на основе положений пункта 2.3.4.

Примечание. *Новые и развивающиеся технологии, средства и процессы могут потребовать изменение деталей процесса планирования. Следовательно, ключевым элементом процесса планирования является гибкость.*

4.2. Мероприятия процесса планирования

Рекомендации по процессу планирования:

1. Следует определить процесс жизненного цикла конструирования аппаратуры, включая критерии перехода, если они применяются, и взаимосвязи между отдельными процессами, такие, как очередность и механизмы обратной связи.
2. Следует определить и объяснить предлагаемые методы конструирования. Сюда относится рассмотрение предполагаемой конфигурации аппаратуры и предлагаемых методов верификации.
3. Следует определить стандарты на конструирование аппаратуры, если предполагается их использование в проекте, включая допустимые отклонения от стандартов. Стандарты могут находиться в диапазоне от базовых стандартов качества до специальных стандартов компании или относиться только к конкретной программе.

Примечание. *Стандарты помогают уменьшить вероятность необнаруженных ошибок конструирования через применение проверенных технологических методов, определенных в ходе предыдущих разработок.*

Пользователь и разработчик аппаратуры должны знать, применяя стандарты к новым конструкциям и технологиям, что такое применение может быть ошибочным. Отклонения от этих стандартов могут быть обусловлены ограничениями конструирования, конфликтами с требованиями системы или несовместимостью с новыми технологиями. Процесс планирования – это возможность рассмотрения приемлемых отклонений при использовании стандартов.

4. Следует определить средства достижения координации процесса конструирования аппаратуры и процессы поддержки при особом внимании к деятельности, связанной с сертификацией систем, ПО и самолета.

Примечание. *Координация может быть выполнена в форме графика, показывающего контрольные точки для событий при выполнении задач процессов, описанных в данном документе.*

5. Следует определить мероприятия для каждого процесса конструирования аппаратуры и соответствующих процессов поддержки. Определение должно быть выполнено на уровне, который позволяет контролировать процесс конструирования аппаратуры и соответствующие процессы поддержки.

6. Следует выбрать среду конструирования, включая инструменты, процедуры, программное и аппаратное обеспечение, которые используются в конструировании, верификации и управлении изделием и данными жизненного цикла.

   a. Если при сертификации предусматривается использование инструментов в их комбинации, то последовательность работы инструментов должна быть специально определена в соответствующем плане.

   b. Среда конструирования может влиять на конструкцию изделия. В подразделе 11.4 дано руководство по оценке инструментов и определена необходимость их классификации.

7. Следует определить процесс отклонения от установленных планов, если отклонения становятся необходимыми и влияют на сертификацию.

8. Следует определить правила, процедуры, стандарты и методы, которые необходимо использовать с целью определения, управления и контроля аппаратуры, соответствующих базовых версий и данных жизненного цикла конструирования аппаратуры.

9. Когда заявитель намеревается использовать субподрядчиков для всего или части жизненного цикла конструирования аппаратуры, в планах аппаратуры следует определить метод для обеспечения соответствия целям гарантии конструирования .

10. Следует описать правила и процедуры для реализации гарантии процессов конструирования аппаратуры.

11. В «Плане сертификации аппаратуры» следует отразить независимость процесса верификации, независимость процесса гарантии и полномочия соответствующих организаций.

12. Средства достижения целей данного руководства следует зарегистрировать и передать сертифицирующему органу в начале процесса. Эти средства следует записать в «Плане сертификации аппаратуры».

Примечание. *Своевременная координация любых изменений, вносимых в эти средства, максимально способствует принятию окончательных данных сертификации как подтверждение соответствия качества конструирования установленным требованиям.*

5. ПРОЦЕССЫ КОНСТРУИРОВАНИЯ АППАРАТУРЫ

В процессах конструирования аппаратуры создается изделие, которое выполняет требования, назначенные аппаратуре на основе требований к системе. В данном разделе описывается пять основных процессов, показанных на рисунке 5-1. К ним относятся: определение требований, эскизное проектирование, техническое проектирование, реализация и переход к производству. Эти процессы конструирования могут применяться на любом иерархическом уровне элемента аппаратуры, таком, как LRU, печатные платы и схемы ASIC/PLD. В последующих разделах описывается каждый процесс, его цели и соответствующие мероприятия, которые необходимо выполнять, чтобы уменьшить вероятность ошибок конструирования и реализации, которые влияют на безопасность. Важно, чтобы каждый из этих процессов планировался, а его детали регистрировались в плане конструирования аппаратуры.

Каждый процесс и взаимодействие между процессами может быть итеративным. Для каждой итерации влияние изменения на каждый из процессов следует рассмотреть и оценить влияние изменения на результаты предыдущих итераций.

Примечание 1. *Считается хорошим практическим подходом документировать в течение всего процесса конструирования заметки по процессу, такие, как примечания к проектированию, примечания к рассмотрению проекта и сообщения о проблемах.*

Существующая практика предлагает много различных средств, графических, математических, баз данных или текстов для представления требований и реализаций конструирования. Примерами таких представлений являются схемы, языки описания аппаратуры HDL, диаграммы состояний, булевы представления и графические методы.

Примечание 2. *Некоторые средства адаптированы к особому процессу или комбинации процессов, таким, как описание требований, эскизное проектирование или техническое проектирование, а некоторые адаптированы для более эффективного применения специальных технологий реализации. Независимо от используемого представления проекта необходимо обеспечивать подтверждающие данные для поддержки уровня гарантии конструирования.*

Для любого используемого представления конструкции необходимо учитывать следующие аспекты:

1. Рекомендациям данного документа необходимо следовать независимо от представления или комбинации используемых представлений.
2. Представление конструкции должно позволить постоянно тиражировать элемент аппаратуры.
3. Небольшие изменения в представлении конструкции могут иметь большое влияние на реализацию конструкции. Влияние этих изменений на гарантию конструирования следует учитывать.
4. Среда представления конструкции или метод могут изменяться, после того как будут установлены базовая версия конструкции. Если это произойдет, необходимо учесть влияние изменения на тиражирование результата.

Представления конструкции на языке HDL основаны на методах текстового кодирования, которые аналогичны по виду тем, что использовались для представления ПО. Эта похожесть по внешним признакам может неправильно привести к попытке использовать методы проверки ПО непосредственно к представлению конструкции на языке HDL или на других эквивалентных языках описания аппаратуры. Правила данного документа применимы для гарантии конструирования конструкций, в которых используется представление на языке HDL.

Примечание. *Структурные процессы, описанные в данном документе, применимы к сложным конструкциям аппаратуры, включая схемы ASIC и PLD. Как пример, приведенная ниже таблица 5-1 показывает отображение типичных процессов для ACIC/PLD с представленными на рисунке 5-1 этого документа.*

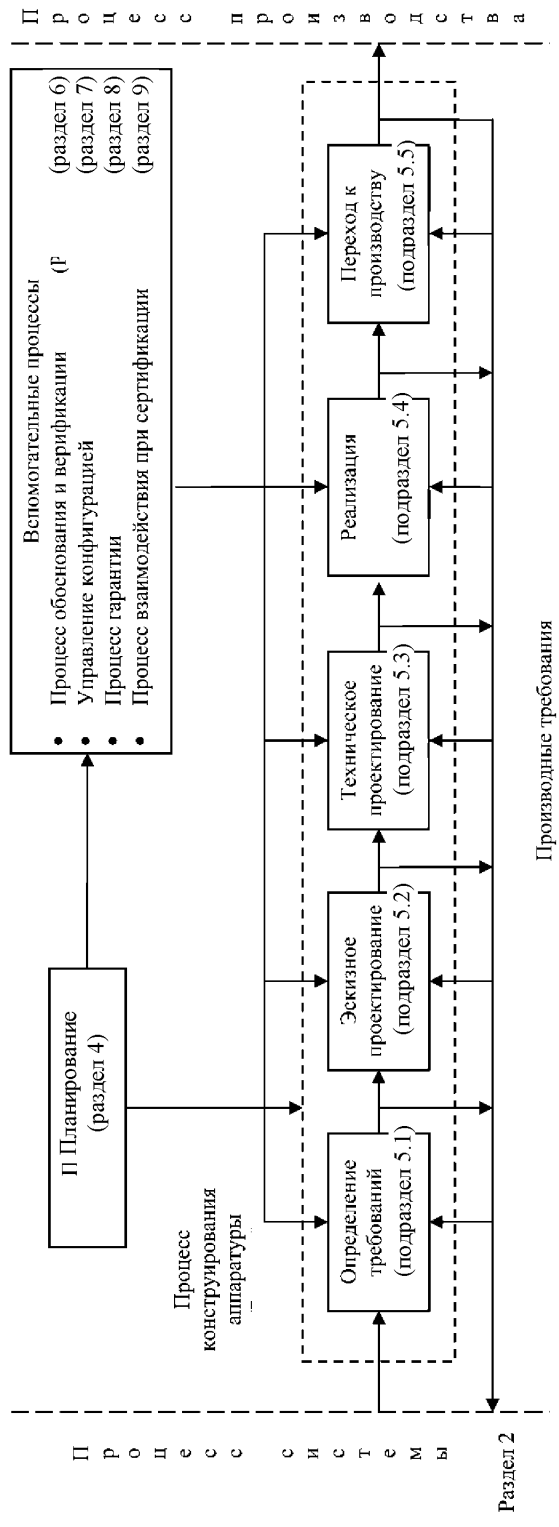

Рис 5-1. Жизненный цикл конструирования аппаратуры

Таблица 5.1. Типичное отображение процесса для ASIC/PLD

Типичный процесс ASIC/PLD	Процесс
Часть планирования высокого уровня	Планирование (раздел 4)
Архитектурные решения ASIC/PLD	Оценка безопасности (подраздел 2.3)
Определение требований ASIC/PLD	Определение требований (подраздел 5.1)
Предварительное проектирование ASIC/PLD, включая поведенческое	Эскизное проектирование (подраздел 5.2)
Детальное проектирование ASIC/PLD, включая синтез, создание маски и файла	Техническое проектирование (подраздел 5.3)
Изготовление ASIC/PLD, включая внешнее производство и испытания, а также программирование программных компонентов	Реализация (подраздел 5.4)
Переход к производству ASIC/PLD	Переход к производству (подраздел 5.5)
Верификация и обоснование ASIC/PLD, включая временной анализ, поведенческое моделирование, моделирование на уровне вентилей и всей конструкции	Процесс обоснования и верификации (раздел 6)
Управление конфигурацией ASIC/PLD, включая инструментальные средства и базу данных	Процесс управления конфигурацией (раздел 7)

Примечание 3. *Стадии конструирования конструкторской документации изделий, установленные ГОСТ 2.1003-68* , следует сопоставлять с процессами конструирования аппаратуры, описываемыми в этом документе, следующим образом:*

*Стадии по ГОСТ 2.1003-68**	*Процессы в этом документе*
Техническое предложение *Эскизный проект*	*Процесс эскизного проектирования*
Технический проект *Рабочая конструкторская документация*	*Процесс технического проектирования*

Виды конструкторских документов в зависимости от стадии конструирования, следует сопоставлять аналогично.

5.1. Процесс определения требований

В процессе определения требований идентифицируются и регистрируются технические требования к изделию. Сюда входят те производные требования, которые определяются предложенной архитектурой изделия, выбором технологии, базовыми и выбираемыми функциями, окружающими условиями, требованиями к эффективности, а также требованиями, выдвигаемыми при оценке безопасности системы. Этот процесс может быть итеративным, поскольку в процессе конструирования могут возникнуть дополнительные требования.

5.1.1. Цели определения требований

Целями процесса определения требований являются:

1. Требования идентифицируются, определяются и документируются. Сюда входят требования, полученные из анализа PSSA и производные требования из оценки безопасности аппаратуры.

Примечание. *Трассируемость результатов верификации относительно требований к аппаратуре обсуждается в разделе 6. Желательно, чтобы этот метод был установлен во время процесса определения требований.*

2. Производные требования передаются обратно в соответствующий процесс.

3. Ошибки и пропуски требований передается для решения в соответствующий процесс.

5.1.2. Мероприятия по определению требований

Мероприятия по определению требований образует итеративный процесс, который помогает обеспечить соответствие требований задачам реализации проекта, требованиям системы и требованиям ПО.

Рекомендации по мероприятиям определения требований включают:

1. Следует документировать системные требования, предъявляемые к изделию. Сюда относится идентификация требований, таких, как функциональность и технические характеристики; архитектурные аспекты, такие, как разделение, встроенный контроль, контролепригодность, внешние интерфейсы, окружающие условия, контроль и техобслуживание, электропитание и физические характеристики.

2. Следует, на основе PSSA, определить требования к безопасности, относящиеся к изделию, а именно:

   a. Уровни гарантии конструирования, назначаемые функциям, которые реализуются в аппаратуре.

   b. Вероятностные требования к неправильному выполнению или потери функции.

   c. Характеристики архитектурной и функциональной безопасности, такие, как приведенные в подразделе 2.3.1, которые выбраны для удовлетворения требованиям функционального распределения.

3. Следует определить ограничения проекта в зависимости от процесса производства, стандартов, процедур, технологии, окружающих условий и руководств по конструированию.

4. Следует определить необходимые для реализации производные требования. Требования, полученные на основе оценки безопасности аппаратуры, которые имеют отношение к безопасности, следует определить отдельно.

Примечание. *Производные требования могут быть связаны со следующим:*

   a. Особые ограничения для гарантии того, что функции более высокого уровня могут противостоять аномалиям функций более низкого уровня гарантии конструирования.

   b. Диапазон входных данных, учитывающих типичные полномасштабные значения данных, а также высокие и низкие состояния битов в информационных словах или в управляющих регистрах.

   c. Повторное включение электропитания или другие состояния повторной установки.

   d. Требования к напряжению питания и току.

   e. Характеристики временных функций, таких, как фильтры, интеграторы и задержки.

   f. Переходы машинных состояний, которые возможны независимо от того, ожидаются они или нет.

   g. Соотношения синхронизации сигналов или электрических условий в нормальных и неблагоприятных условиях.

   h. Сигнальная помеха и перекрестная помеха.

   i. Кратковременные импульсные сигнальные помехи в асинхронных логических схемах.

   j. Особые ограничения для управления неиспользуемыми функциями.

5. Производные требования следует возвратить обратно в процесс SSA, чтобы можно было оценить влияние требований на систему.

6. Информацию о требованиях следует документировать в количественном виде с допусками, там, где это применимо. Сюда не входит описание конструкции или решения по верификации.

7. Процессы или ошибки в требованиях, обнаруженные в течение данного процесса, следует направить в процесс разработки системы.

8. Требования, включая те, которые должны быть подготовлены для соответствия требованием PSSA, необходимо прослеживать до следующего более высокого иерархического уровня требований. Производные требования следует идентифицировать и прослеживать как можно дальше по иерархическим уровням.

Примечание. *Подтверждение приемлемости на уровне системы предписанных аппаратуре требований по безопасности может проводиться во время процесса определения требований. Подтверждение приемлемости производных требований к аппаратуре описано в подразделе 6.1.*

5.2. Процесс эскизного проектирования

В процессе эскизного проектирования формируется концепция проектирования высокого уровня, которую можно оценить, для того чтобы определить возможности реализации конструкции в соответствии с требованиями. Этот процесс может быть выполнен, используя такие элементы, как функциональные блок-схемы, описания конструкции, архитектуры, схемы печатных плат и корпусов.

5.2.1. Цели эскизного проектирования

Целями эскизного проектирования являются:

1. Эскизный проект изделия разрабатывается в соответствии с требованиями к нему.

2. Производные требования поступают обратно в процесс определения требований или в другие процессы.

3. Пропуски и ошибки в требованиях передаются в соответствующие процессы для разрешения.

5.2.2. Мероприятия эскизного проектирования

Рекомендации по мероприятиям эскизного проектирования включает:

1. Для элемента аппаратуры следует подготовить описание высокого уровня. Оно может включать:

   a. Архитектурные ограничения, связанные с безопасностью, включая те, которые необходимы для рассмотрения ошибок проектирования, функциональных сверхнагрузок компонентов, надежности и дефектов устойчивости к желательным воздействиям.

   b. Идентификацию любых ограничений на реализацию ПО или других компонентов системы.

2. Следует определить главные компоненты. Следует определить направление их влияния на требования к безопасности аппаратуры, включая воздействие в неиспользуемых функциях.

3. Производные требования, включая определение интерфейсов, следует направить обратно в процесс определения требований.

4. Пропуски или ошибки в требованиях следует направить обратно в соответствующий процесс для решения.

5. Необходимо определить характеристики надежности, техобслуживания и контроля.

Примечание. *Рекомендуется провести согласование между заинтересованными сторонами достигнутых целей эскизного проектирования. Обычно для этого используется рассмотрение проекта.*

5.3. Процесс технического проектирования

В процессе детального проектирования формируются детальные данные о проекте, при использовании требований к изделию и данных эскизного проектирования как основы для технического проектирования.

5.3.1. Цели технического проектирования

Целями технического проектирования являются:

1. Технический проект разрабатывается на основе требований к изделию и данных эскизного проектирования.
2. Производные требования поступают обратно в процесс эскизного проектирования или другие соответствующие процессы.
3. Пропуски и ошибки в требованиях передаются в соответствующие процессы для решения.

5.3.2. Мероприятия процесса технического проектирования

Рекомендации по мероприятиям технического проектирования включает:

1. Данные технического проектирования для изделия следует разрабатывать на основе требований и данных эскизного проектирования. Они могут включать данные сборки и межсоединений, данные о компонентах, описания на языке HDL, методы испытаний и данные интерфейса аппаратуры и ПО.

Примечание. *Во время процесса технического проектирования неформально применяются методы верификации – для облегчения принятия технических решений, сделанных в течение данного процесса. Например, анализ параметров конструкции, таких, как логическая синхронизация или допуски параметров, может дать информацию для принятия решения о конструкции.*

2. Если это необходимо, следует применять технические приемы архитектурного проектирования. К ним относятся введение в обеспечение безопасности средств контроля правильности функционирования, разнородность средства обеспечения функции назначения и средств контроля безопасности, предотвращение влияния ошибок конструирования на безопасность и применение отказоустойчивых конструкций.
3. Следует ввести в конструкцию свойство самопроверки в обеспечение верификации требований безопасности, когда это необходимо.

Примечание. *Важно разработать конструкцию так, чтобы определенные характеристики безопасности можно было проверять не только в течение жизненного цикла конструирования аппаратуры, но также в приемочных испытаниях и в испытаниях при возврате в эксплуатацию после восстановительных работ.*

4. Следует выполнить оценку неиспользуемых функций с целью определения их потенциального влияния на безопасность. Следует рассмотреть неблагоприятные влияния.
5. Следует определить ограничения на конструкцию, установку или функционирование изделия, которые, если их не учитывать, могут повлиять на безопасность изделия.
6. Производные требования, полученные в процессе технического проектирования, следует направить обратно в процесс эскизного проектирования или другой подходящий процесс.
7. Пропуски и ошибки в требованиях, обнаруженные во время процесса технического проектирования, следует направить в соответствующий процесс для решения.

5.4. Процесс реализации

В процессе реализации используются данные технического проектирования – для создания изделия, которое затем подвергается испытаниям.

5.4.1. Цели реализации

Целями процесса реализации являются:

1. Создается изделие, в котором реализуется технический проект изделия с использованием установленного процесс изготовления.
2. Завершается реализация изделия, сборка и установка.
3. Производные требования поступают обратно в процесс технического проектирования или другие соответствующие процессы.
4. Пропуски и ошибки в требованиях направляются в соответствующий процесс для решения.

5.4.2. Мероприятия реализации

Рекомендации по мероприятиям реализации включают:

1. Изделие следует создавать, используя данные проектирования и, где возможно, ресурсы, предназначенные для производства изделия. Сюда относятся закупка, комплектация, производство, проверка и испытания.
2. Производные требования, полученные в процессе реализации, следует направить обратно в процесс технического проектирования или другие соответствующие процессы.
3. Пропуски и ошибки, обнаруженные во время процесса реализации, следует направить в соответствующий процесс для решения.

5.5. Процесс перехода к производству

В данном процессе необходимо проверить данные изготовления, испытательные установки и общие ресурсы для гарантии готовности и пригодности к производству. В процессе перехода к производству используются выходные данные процессов реализации и верификации с целью передачи изделия в производство.

5.5.1. Цели перехода к производству

Задачами данного процесса являются:

1. Устанавливается базовая версия документации, которая включает все данные конструирования и изготовления, необходимые для точного воспроизведения изделия.
2. Определяются и документируются требования к изготовлению, связанные с безопасностью, и устанавливаются средства контроля производства.
3. Производные требования направляются обратно в процесс реализации или другие соответствующие процессы.
4. Ошибки и пропуски направляются в соответствующий процесс для решения.

5.5.2. Мероприятия перехода к производству

Рекомендации по мероприятиям перехода к производству включают:

1. На основе сформированных проектных данных следует подготовить данные для производства.
2. Данные производства (изготовления) следует проверить на полноту и соответствие данным конструкции.

Примечание. *Определение любых положений о характере документации на изготовление выходит за рамки данного документа.*

3. Любые изменения или улучшения, произведенные в течение процесса перехода к производству, следует оценить, для того чтобы показать, что они соответствуют всем требованиям к изделию, особенно требованиям по безопасности. Любые изменения, не соответствующие требованиям заказчика или требованиям сертификации должны быть одобрены заинтересованными сторонами.
4. Требования к производству, связанные с безопасностью, следует четко определить, чтобы их можно было контролировать в процессе производства.

5. Следует определить данные, необходимые для разработки критериев приемочных испытаний.

6. Пропуски и ошибки, которые были определены, следует направить в соответствующий процесс для решения.

5.6. Приемочные испытания

Приемочные испытания демонстрируют, что изготовленное, модифицированное или отремонтированное изделие работает в соответствии с основными параметрами блока, на которых основана сертификация. Эти основные параметры выбираются с использованием технического решения и показывают способность изделия отвечать требованиям, для выполнения которых изделие было разработано.

Примечание 1. *Контроль конфигурации «изготовленного» изделия не является функцией, которая должна быть выполнена в процессе приемочного испытания. План управления конфигурацией, как описано в разделе 7 данного документа, должен описывать, как заявитель планирует выполнить эту деятельность.*

В содержание данного документа не включено определение критерия приемочных испытаний, включая условия прошел/отказал. Мероприятия производства, включая приемочные испытания, считается выходящей за рамки данного документа.

Примечание 2. *Приемочные испытания не предназначены для проверки всех требований по каждому выпускаемому изделию.*

Испытания части изделия могут использоваться, как часть приемочных испытаний.

Критерии приемочных испытаний должны гарантировать, что:

1. Определены испытания изделия как приемника электроэнергии.

2. Определены испытания на защиту от внешних воздействий, когда требуется.

3. Приемочные испытания обеспечивают охват тех свойств конструкции, которые необходимы для выполнения требований безопасности. Изделие или часть изделия, связанное с безопасностью, которые не охвачены испытаниями, следует определить и обеспечить другими средствами гарантии. К этим средствам могут относиться анализ, контроль проекта, статистический контроль процесса или другие подходящие средства.

5.7. Серийное производство

Этот процесс выходит за рамки содержания данного документа, однако элементы, влияющие на гарантию конструирования, кратко описаны с целью полноты описания жизненного цикла.

В данном процессе изделие воспроизводится на стандартной основе, которая соответствует данным и требованиям производства.

Учитывается следующее:

1. Управление изменением в процессах производства или конструкции обеспечивает гарантию того, что изменение не оказывает неблагоприятного влияния на достигнутую безопасность или на сертификацию, или на соответствие требованиям.

Примечание. *В дополнение к руководству, предложенному данным документом, подраздел 11.1.1 охватывает модификации предварительно разработанной аппаратуры. При рассмотрении выходящего из употребления компонента следует обратиться к подразделу 11.2.*

2. Корректировка всей документации, связанной с изменениями, выполняется в соответствии с одобренными планами управления конфигурацией.

6. ПРОЦЕСС ОБОСНОВАНИЯ И ВЕРИФИКАЦИИ

В данном разделе описываются процесс обоснования и процесс верификации. Процесс обоснования обеспечивает гарантию того, что производные требования к изделию являются верными и полными по отношению к требованиям системы отнесенным к изделию. Процесс верификации обеспечивает гарантию того, что реализация изделия соответствует всем требованиям к аппаратуре, включая производные требования.

6.1. Процесс обоснования

Обсуждаемый здесь процесс обоснования предназначен обеспечить правильность и полноту производных требований по отношению к требованиям системы, отнесенных к аппаратному изделию, путем использования комбинации объективных и субъективных процессов. Обоснование может быть проведено до или после того, как будет готово аппаратное изделие, однако обычно обоснование производится в течение жизненного цикла конструирования.

Примечание 1. *Опыт показывает, что внимание к разработке и обоснованию требований может выявить ошибки и пропуски на раннем этапе конструирования и уменьшить вероятность повторного конструирования и неадекватных характеристик аппаратуры.*

Процесс обоснования, обсуждаемый здесь, не предназначен для оценки требований, полученных на основе требований к системе, поскольку обоснование этих требований обеспечивается как часть системного процесса. Кроме того, не все производные требования к изделию требуют оценки.

Конструкторские решения, которые влияют на безопасность системы или на функциональные требования, назначенные другим частям системы, должны быть классифицированы как производные требования и должны быть оценены. Кроме того, решения и допущения по конструкции, которые ограничивают последующие задачи конструирования, должны обосновываться как производные требования.

Производные требования, которые необходимо обосновать, должны обосновываться с учетом требований к системе, назначенным изделию. Производные требования, которые нельзя проследить до более высокого уровня требований, должны оцениваться по конструкторскому решению, на основе которого они были получены.

Примечание 2. *Конструкторское решение по включению отдельного источника электропитания для схемы, выполняющей особую функцию, может привести к производным требованиям проведения конструирования этого источника питания. Эти производные требования должны содержать требования безопасности, основанные на условии отказа в результате отказа или ошибки в функции, обеспечиваемой схемой, которая получает питание от источника электропитания. Эти требования должны быть обоснованы.*

Другим примером конструкторского решения, которое становится производным требованием, является присвоение адреса памяти для периферийных устройств. Зачастую не существует никаких базовых требований для присваивания, однако если они сделаны, то они ограничивают последующие задачи конструирования, обеспечивая правильность функционирования конструкции. Это производное требование может и не требовать обоснования.

6.1.1. Цели процесса обоснования

Целями процесса обоснования для производных требований к аппаратуре являются:

1. Производные требования к аппаратуре, по которым должно верифицироваться изделие, являются правильными и полными.
2. Производные требования оцениваются по их влиянию на безопасность.
3. Пропуски и ошибки направляются обратно в соответствующие процессы для решения.

6.1.2. Мероприятия процесса обоснования

Цель обоснования аппаратуры может быть достигнута комбинацией мероприятий, таких, как рассмотрения, моделирование, макетирование, анализ, опыт эксплуатации, техническая оценка или разработка и проведение испытаний.

Рекомендации по мероприятиям процесса обоснования включают:

1. Следует определить производные требования к аппаратуре, которые необходимо обосновать.
2. Для каждого требования, определенного по п. 1 выше, должны быть определены и удовлетворены следующие критерии обоснования:
   a. Каждое требование обосновывается на некотором иерархическом уровне с помощью рассмотрения, анализа или испытания.
   b. Рассмотрение, анализ или испытание каждого требования пригодны для обоснования требования, особенно относительно безопасности.
   c. Результаты рассмотрения, анализа или испытания результатов, связанных с обоснованием каждого требования, являются правильными, а расхождения между реальными и прогнозируемыми результатами объяснимыми. Когда ожидаемые результаты заранее не определены, как в случае рассмотрений или анализов, результаты обоснования должны быть совместимы с требованием, особенно относительно требований по безопасности.

Примечание. *Критерий завершения обоснования может основываться на требованиях, соображениях безопасности, режиме эксплуатации или реализации.*

3. Производные требования должны оцениваться по их влиянию на безопасность.
4. Производные требования к аппаратуре должны оцениваться на полноту относительно требований к системе, назначенных изделию. Для целей данного процесса ряд требований являются завершенными, если все параметры, которые были определены, необходимы, а все необходимые параметры были определены.
5. Производные требования к аппаратуре должны оцениваться на правильность относительно требований к системе, назначенных изделию. В контексте данного документа, требование считается правильным, когда требование определено без неоднозначности и нет ошибок в определениях параметров.
6. Следует установить трассируемость между производными требованиями к аппаратуре, мероприятиями обоснования и результатами.
7. Пропуски и ошибки в требованиях следует направить обратно в соответствующие процессы для решения.

6.2. Процесс верификации

Процесс верификации обеспечивает гарантию того, что реализация изделия соответствует требованиям. Верификация состоит из рассмотрений, анализов и испытаний, применяемых на основе плана верификации. Процесс верификации должен включать оценку результатов.

Примечание 1. *Аспекты безопасности конструирования аппаратуры принимают форму требований по безопасности, которые должны удовлетворяться при реализации аппаратуры.*

В данном разделе даются инструкции для процесса верификации, которые применяется к конструированию аппаратуры. Процесс верификации может применяться на любом уровне иерархии конструирования, в соответствии с планом верификации аппаратуры. Для требований безопасности целесообразно применять процесс верификации на различных этапах процесса конструирования с целью повышения вероятности того, что ошибки конструирования исключены. Некоторые уровни гарантии конструирования требуют, чтобы цели процесса верификации выполнялись с независимостью, как отмечено в Приложении А.

Процессы верификации ПО, верификации интеграции ПО/аппаратуры и верификации интеграции систем в данном документе не рассматриваются. Однако верификация требований к аппаратуре в этих процессах считается обоснованным методом верификации аппаратуры.

Изменения в верифицированной конструкции могут быть повторно проверены с помощью аналогий, анализа, заново разработанных испытаний или путем повторения части первоначальной верификации.

Примечание 2. *Рекомендуется вне документированного процесса верификации применять неформальное тестирование. Процедуры и результаты, однако, не обязательно поддерживать контролем управления конфигурации, но они очень эффективны при обнаружении и исключении ошибок конструирования в начале процесса конструирования. Верификационный зачет для такого тестирования возможен только, если оно формализовано.*

6.2.1. Цели процесса верификации

Целями процесса верификации являются:

1. Обеспечена очевидность того, что реализация аппаратуры соответствует требованиям.
2. Установлена трассируемость между требованиями к аппаратуре, реализацией, процедурами верификации и результатами.
3. Критерии приемочных испытаний определены, могут быть реализованы и соответствуют уровням гарантии конструирования аппаратуры для функций аппаратуры.
4. Пропуски и ошибки направляются обратно в соответствующие процессы для решения.

6.2.2. Мероприятия процесса верификации

Цели процесса верификации могут быть выполнены за счет комбинации методов, таких, как рассмотрения, анализы, разработка и выполнение тестов. Мероприятия верификации, которые должны применяться для того, чтобы продемонстрировать соответствие требованиям, документируются в плане верификации

Мероприятия верификации следующие:

1. Следует определить требования, для которых необходимо верификационное мероприятие. Это не означает, что требования должны верифицироваться на каждом иерархическом уровне. Требования могут быть проверены на более высоком иерархическом уровне.
2. Следует выбрать методы верификации, такие, как испытания, моделирование, макетирование, анализы и рассмотрения, и выполнить верификацию.
3. Следует установить трассируемость требований, реализации, процедур и результатов верификации. Трасссируемость должна быть совместима с уровнем гарантии конструирования функции, выполняемой аппаратурой. Не обязательно требовать трассируемости для отдельных компонентов, таких, как резисторы, емкости или вентили, если это не требуют условия безопасности.
4. Следует выполнить анализ полноты верификации, чтобы определить, что процесс верификации завершен, включая следующее:
   a. Каждое требование верифицировано на некотором иерархическом уровне с помощью рассмотрения, анализа или испытания.
   b. Рассмотрение, анализ или испытание каждого требования адекватны требованию верификации, особенно относительно требований по безопасности.
   c. Результаты рассмотрения, анализа или испытания, связанные с проверкой каждого требования правильные, а расхождения между реальными и ожидаемыми результатами объяснимы. Когда ожидаемые результаты предварительно не определены, как в случае обзоров и анализов, результаты проверки должны быть совместимы с требованием, особенно относительно требований по безопасности.

5. Результаты мероприятий верификации следует документировать.

6. Пропуски и ошибки должны следует направить обратно в соответствующий процесс для решения.

6.3. Методы обоснования и верификации

В данном подразделе описываются некоторые методы, которые могут применяться и для обоснования и верификации.

6.3.1. Испытание

Испытание – это метод, который подтверждает, что изделие правильно реагирует на стимул или серию стимулов. Примерами испытаний служат функциональные испытания изделия, стендовые испытания системы, заводские испытания для оценки системы и испытания на борту самолета.

Испытания можно проводить, используя ручное, автоматизированное или специальное испытательное оборудование. В процессе верификации испытания могут использовать преимущества внутренних испытательных средств изделия, таких, как встроенный контроль.

Когда невозможно проверить особые требования, испытывая изделие в предназначенных ему внешних условиях эксплуатации, следует обеспечить и обосновать применение других средства верификации.

Испытания могут выполняться в течение различных процессов конструирования аппаратуры. Испытания, выполняемые для сертификационного зачета, требуют сконфигурированного изделия. Результаты интеграции системы или результаты испытания интеграции ПО/аппаратуры также можно использовать для зачетных испытаний.

Рекомендации по испытаниям следующие:

1. Любое требование, которое необходимо подтвердить или верифицировать в испытании, следует определить. Частью этих требований являются требования к испытаниям на воздействие окружающей среды.

2. Испытательные воздействия, последовательность и условия испытания, такие, как окружающая изделие температура и применяемое напряжение, следует определить для каждого испытания.

3. Критерий «прошел/отказал» и метод регистрации результатов следует определить до проведения испытания.

4. Полную идентификацию испытательного оборудования и данные калибровки для каждого изделия следует зарегистрировать.

5. Следует зарегистрировать идентичность конфигурации испытуемого изделия.

6. Результаты испытания следует регистрировать и сохранять.

7. Данные неудачных испытаний следует направить обратно в соответствующий процесс для решения.

6.3.2. Анализ

Анализ – это детальный повторяемый аналитический метод для оценки специальных характеристик изделия с целью демонстрации соответствия специальным требованиям. Примером анализа является анализ нагрузок, анализ запасов конструкции, анализ отказов общего режима, анализ самого неблагоприятного варианта и анализ полноты испытаний. Опыт эксплуатации может обеспечить данные для различных видов анализа.

Примечание. *По мере возрастания сложности конструирования аппаратуры рекомендуется использовать компьютерные средства, такие, как моделирование, с целью проверки требований и реализации конструкции.*

Анализ может содержать детальное исследование функциональности, характеристик, трассируемости и значения для безопасности функции элемента аппаратуры и ее взаимосвязь с

другими функциями в пределах бортовой системы или оборудования. Анализ сам по себе или в комбинации с другими методами проверки обеспечивает очевидность того, что требование правильно реализовано. Анализ должен быть основан на данных, полученных в процессе конструирования, из опыта эксплуатации или других доступных баз данных.

Моделирование является важным средством анализа проекта, как для визуализации работы схемы, так и для функционирования на более высоком уровне. Моделирование может использоваться для анализа влияния изменений параметров аппаратуры, который трудно выполнить, используя другие средства проверки, и тем самым добиться достоверности в уменьшении ошибок конструирования, влияющих на безопасность, как результат этих изменений. Поскольку результаты зависят от применяемых моделей и сценариев, сами по себе результаты моделирования не могут быть использованы для сертификации без обеспечения очевидности их правильности.

Примерами анализа являются:

1. Термический анализ. При термическом анализе обеспечивается проверка соответствия реализации проекта установленным требованиям при воздействии тепловой среды.
2. Анализ нагрузок. При анализе нагрузок осуществляется проверка того, что компоненты соответствуют критериям снижения номинальных показателей вне требуемого диапазона работы.
3. Анализ надежности. Анализ надежности устанавливает, удовлетворяет ли реализация конструкции требованиям к надежности изделия.
4. Анализ запасов конструкции. Анализ запасов конструкции проверяет соответствие реализации конструкции установленным функциональным требованиям с учетом изменяемости компонентов.
5. Анализ подобия. При анализе подобия характеристики и применение сравниваются с теми характеристиками систем, которые уже были ранее сертифицированы.
6. Анализ моделирования. При анализе моделирования результаты моделирования сравниваются с прогнозируемыми результатами.

6.3.3. Рассмотрения

Рассмотрение – это качественный метод оценки планов, требований, данных конструирования, технического проектирования и реализации конструкции.

Рассмотрения следует проводить в течение всего жизненного цикла конструирования аппаратуры, как это определено в соответствующем плане. Все рассмотрения, используемые при сертификации, должны быть определены в плане обоснования и верификации.

Рекомендации по рассмотрениям могут содержать следующее:

1. Участники должны иметь знания, необходимые для выполнения рассмотрений.
2. Результаты рассмотрения аппаратуры могут использоваться для того, чтобы принять или отклонить переходы между мероприятиями жизненного цикла конструирования аппаратуры.
3. Результаты рассмотрения следует документировать, включая принятые решения и распределение предпринятых действий.

6.3.3.1. Рассмотрение требований

Рассмотрение требований – это метод для обеспечения приемлемости требований. Рассмотрение требований может обращаться к целям процессов обоснования и верификации одновременно.

Изменение требований, которые происходят после первичного рассмотрения требований, следует сделать предметом того же самого процесса рассмотрения, использованного первоначально, или же эквивалентного процесса рассмотрения. В рассмотрении не предусматривается оценка требований к системе, назначенных изделию.

Рекомендации по рассмотрению требований следующие:

1. Каждое требование должно быть четким, проверяемым и описанным достаточно полно для его иерархического уровня и не должно входить в противоречие с другими требованиями.
2. Производные требования должны быть совместимы с требованиями к системе или требованиями, на основе которых они получены.
3. Требования должны быть совместимы с SSA.
4. Производные требования безопасности должны быть определены и направлены обратно в SSA.
5. Требования должны быть совместимы с соответствующими стандартами на конструирование аппаратуры.
6. Требования должны быть совместимы с возможностями и ограничениями современной технологии.
7. Требования к компонентам, такие, как характеристики, температурный диапазон, снижение номинальных показателей и экранирование, должны соответствовать требованиям по безопасности и надежности.
8. Следует рассмотреть способность к испытанию, обслуживанию и изготовлению изделия.
9. Следует определить требования к интерфейсу ПО/аппаратура.
10. Требования должны быть трассируемы снизу-вверх до следующего иерархического уровня, в соответствии с критериями, определенными в плане.
11. Производные требования должны отражать ограничения реализации, которые нельзя проверить на более высоком иерархическом уровне.
12. Пропуски и ошибки следует направить обратно в соответствующий процесс для решения.

Примечания: 1. *Следующие вопросы могут помочь оценить полноту требований:*

- *a. Все ли требования верхнего уровня рассмотрены?*
- *b. Все ли применяемые стандарты и руководства рассмотрены?*
- *c. Учтены ли все функции и связи аппаратуры?*
- *d. Полностью ли описана архитектура?*
- *e. Правильно ли описана вся требующая верификацию реализация аппаратуры?*
- *f. Учтены ли все характеристики поведения, запрещенные при оценке безопасности?*
- *g. Правильно ли установлена рабочая среда?*
- *h. Рассмотрены ли допуски и ограничения?*
- *i. Позволит ли данная реализация избежать любых известных проблем использования существующей или аналогичной аппаратуры?*

2. *Следующие вопросы помогут оценить правильность требований:*

- *a. Соответствуют ли требования требованиям более высокого уровня?*
- *b. Распределены ли к изделию соответствующие требования к системе?*
- *c. Утверждают ли требования «что», а не «как»?*
- *d. Являются ли требования однозначными?*
- *e. Могут ли быть реализованы требования?*
- *f. Можно ли верифицировать требования?*
- *g. Определены ли режимы функционирования?*
- *h. Соответствуют ли требования оценке безопасности?*
- *i. Правильно ли определены допуски и ограничения как производные требования?*

6.3.3.2. Рассмотрение конструкции

Рассмотрение конструкции – это метод, позволяющий определить, что данные конструкции и реализация удовлетворяют требованиям безопасности. Рассмотрения конструкции должны выполняться, как определено в плане, много раз во время жизненного цикла конструирования аппаратуры. Примерами являются рассмотрения эскизного проектирования, технического проектирования и реализации. Для иерархических конструкций, которые охватывают несколько уровней изделия, такие, как схемы ASIC и печатные платы, рассмотрения конструкции должны проводиться там, где существует наивысший потенциал для гарантии правильной конструкции.

Рекомендации по рассмотрению конструкции следующие:

1. Все требования должны быть рассмотрены, а производные требования и данные конструкции должны быть правильно определены.
2. Необходимо рассмотреть требования к окружающей среде.
3. Необходимо рассмотреть требования по надежности и безопасности.
4. Должны быть точно определены аспекты безопасности данных конструкции.
5. Конструкция должна быть готова к реализации, испытанию и техобслуживанию.
6. Должны быть оценены новые способы производства.
7. Должны удовлетворяться критерии выбора компонентов, определенные в планах.
8. Конструкция должна быть трассируема к требованиям.
9. Пропуски и ошибки следует направить обратно в соответствующий процесс для решения.

7. ПРОЦЕСС УПРАВЛЕНИЯ КОНФИГУРАЦИЕЙ

Процесс управления конфигурацией предназначен обеспечить постоянное тиражирование единицы конфигурации, восстановление информации, если это необходимо, и способность модифицировать единицу конфигурации управляемым способом, если модификация необходима. В данном разделе описываются цели управления конфигурацией и мероприятия, которые обеспечивают достижение этих целей.

7.1. Цели управления конфигурацией

Целями процесса управления конфигурацией являются:

1. Единицы конфигурации уникально идентифицированы и документированы.
2. Обеспечивается постоянное и точное тиражирование элементов конфигурации.
3. Обеспечивается контролируемый метод определения и прослеживания модификации единиц конфигурации.

7.2. Мероприятия управления конфигурацией

Рекомендации по мероприятиям управления конфигурацией следующие:

1. Единицы конфигурации следует уникально идентифицировать, документировать и контролировать. Сюда может входить, но этим не ограничиваться, аппаратура, проектные представления аппаратуры, инструменты и другие единицы данных, используемых для сертификационного зачета и базовых версий.
2. Следует установить базовые версии.
3. Проблемы следует уникально идентифицировать, прослеживать и регистрировать.
4. Следует обеспечивать контроль изменений и трассируемость изменений. Для этого требуется, чтобы данные жизненного цикла, определенные в планах, были защищены и воспроизводимы.
5. Архивирование, воспроизведение и выпуск единиц конфигурации следует контролировать.

Для удовлетворения целей и выполнения мероприятий по управлению конфигурацией можно использовать различные методы. В следующих параграфах даны руководящие указания по мероприятиям, которые можно использовать в качестве приемлемых методов.

7.2.1. Идентификация конфигурации

Целью мероприятия по определению конфигурации является однозначное определение элемента конфигурации, чтобы установить основу для контроля и исходные данные элементов конфигурации.

Руководство содержит следующие рекомендации :

1. Следует ввести идентификацию конфигурации для элементов.
2. Идентификацию конфигурации следует ввести для каждой единицы конфигурации, для каждой отдельно контролируемой компоненты единицы конфигурации и для комбинаций единиц конфигурации, которые образуют изделие, в соответствии с планом, согласованным с сертифицирующим органом.

Примечание. *Детали, до которых проводится идентификация таких компонентов, как схемы ASICS, конфигурируемые PLD, печатные платы и «черные ящики», определяются планом управления конфигурацией.*

3. Единицы конфигурации следует идентифицировать для компонентов COTS и предварительно разработанных изделий до того, как они будут использоваться в базовой версии.
4. Идентификацию конфигурации следует ввести для каждого элемента конфигурации до того, как он будет использоваться в новой базовой версии, использоваться в качестве исходного другими элементами данных или использоваться при изготовлении изделия.

7.2.2. Установление базовой версии

Целью установления базовой версии является определение основы для дальнейшей деятельности и обеспечение контроля и прослеживания единиц конфигурации.

Рекомендации следующие:

1. Базовые версии следует устанавливать для элементов конфигурации, используемых для сертификационного зачета.

Примечание. *Промежуточные базовые версии могут помочь в контроле мероприятий по аппаратуре.*

2. После установления базовой версии ее следует сделать объектом процедуры контроля изменений.

3. При разработке производной базовой версии на основе установленной базовой версии следует использовать рекомендации по контролю изменений.

4. Если при разработке новой базовой версии предусматривается сертификационный зачет данных, связанных с конструированием предыдущей версии, эту новую базовая версию следует трассировать до той версии, от которой она является производной.

Примечание. *Базовая версия может быть элементом конфигурации, предварительно сертифицированным элементом аппаратуры или компонентом COTS.*

7.2.3. Регистрация проблем, отслеживание и корректирующие действия

Целью регистрации проблем, отслеживания и корректирующих действий является запись проблем и гарантия правильной локализации и решения. К проблемам могут относиться несоответствие планам и стандартам, недостатки выходных данных жизненного цикла, аномалии в поведении изделий и неадекватность или недостаток средств и технологических процессов. Регистрация проблем должна вводиться не позднее, чем установлена базовая версия, на основе которой проводится сертификация.

Рекомендации следующие:

1. Каждую отмеченную проблему следует записать в сообщении о проблеме.

2. В сообщении о проблеме следует определить версии затронутых единиц конфигурации.

3. Сообщения о проблеме, которые требуют исправления, должны инициировать действия по контролю изменения.

4. Во все закрытые отчеты о проблеме следует внести описание действия, предпринятого, чтобы закрыть сообщение о проблеме, включая комплект измененных единиц данных, которые были для затронуты мероприятием коррекции.

5. Не все сообщения о проблеме должны быть закрытыми, для того чтобы получить сертификационный зачет. Однако все сообщения о проблеме должны оцениваться, и те, которые могут повлиять на безопасность или сертификацию, должны быть закрытыми.

6. Система сообщений о проблеме должна отслеживать состояние сообщений о проблемах, включая их одобрение и размещение.

7.2.4. Управление изменениями

Целью мероприятия управления изменениями является обеспечение регистрации, оценки, принятия решения и одобрения изменений. Управление изменениями должно быть реализовано в соответствии с планом управления конфигурацией и должно начинаться не позднее, чем установлена базовая версия, на основе которой может быть получен сертификационный зачет.

Рекомендации следующие:

1. При управлении изменениями следует сохранять целостность единиц конфигурации путем защиты от несанкционированного изменения.

2. Управление изменениями должно гарантировать, что изменение оценено для определения, требуется ли корректировка единицы конфигурации или нет.

3. Изменения единиц конфигурации под управлением изменениями следует регистрировать, одобрять и отслеживать. Одобряющий орган определяется в плане управления конфигурацией.

Примечания: 1. *Сообщение о проблеме связано с управлением изменениями, поскольку решение отмеченной проблемы может привести к изменениям единиц конфигурации.*

2. *Общепризнанно, что раннее введение управления изменениями улучшает контроль и управление мероприятиями процессов.*

4. Управление изменениями должно обеспечить трассируемость изменений для определения причины изменения.

5. Управление изменениями должно гарантировать, что изменение оценено для определения его влияния на изменение выходных данных процессов и что выходные данные обновлены.

Примечания: 1. *Все или некоторые мероприятия могут быть повторены до того момента, когда было оказано влияние на выходные данные.*

2. *Необходимо признать, что изменение в средствах производства, технологических процессах и внешних компонентах может повлиять на конструкцию.*

6. Управление изменениями должно гарантировать, что установлена обратная связь с затронутыми процессами.

7.2.5. Выпуск, архивирование и воспроизведение

Целью мероприятия выпуска является введение элементов данных под контроль управления конфигурацией так, чтобы обеспечить в других мероприятиях использование только санкционированных данных. Целью архивирования и воспроизведения является гарантия того, что элементы данных, связанные с изделием, могли быть воспроизведены в случае необходимости дублирования, восстановления, повторных испытаний или модификации изделия.

Рекомендации следующие:

1. Единицы конфигурации должны быть идентифицированы и выпущены до их использования при изготовлении и должны быть установлены полномочия на их выпуск.

2. Элементы данных, связанные с изделием, должны поступать из одобренного источника, например разрабатывающей организации или компании.

Примечание. *Данные контроля изменения и данные сообщения о проблеме являются частью элементов данных.*

3. Процедуры хранения данных должны удовлетворять требованиям летной годности и позволять провести модификации.

4. Необходимо установить процедуры для обеспечения целостности хранящихся данных в течение времени, требуемого сертифицирующим органом, посредством:

   a. Гарантии, чтобы не были выполнены несанкционированные изменения.

   b. Выбора среды хранения данных.

   c. Обеспечения поддержки сохраненных данных. Например, используя или обновляя архивные данные с частотой, совместимой со сроком хранения и средой.

   d. Гарантии, что отдельное событие, которое может вызвать потерю архивированных данных, было маловероятным. Например, с помощью хранения дублированных копий в физически отдельных архивах.

7.3. Категории контроля данных

Определяются две категории контроля данных, связанные с управлением конфигурацией элементов данных: категория 1 контроля аппаратуры и категория 2 контроля аппаратуры.

Определение двух категорий допускает менее жесткий контроль конфигурации определенных элементов данных. Категория НС1 предусматривается, если мероприятия по управлению конфигурацией не выполняются по менее жесткой НС2. Элементы данных, классифицированные как НС2, изменяются не дополнением, а заменой новыми данными.

В таблице 7-1 определены мероприятия управления конфигурацией, которые должны выполняться при НС1 и НС2. Например, в таблице 7-1 показано, что элементы данных, идентифицированные в Приложении А (таблица А-1) как НС2, необходимо воспроизводить, но не нужно выпускать. Кроме того, в таблице 7-1 показано, что любой элемент данных НС1 будет иметь базовую версию.

Приложение А определяет категорию контроля для каждого элемента данных как функцию уровня гарантии конструирования. Например, в таблице А-1 НС1 применяется к требованиям аппаратуры для всех уровней гарантии, а НС2 применяется для всех уровней гарантии к рассмотрению аппаратуры и анализу результатов.

Таблица 7-1. Мероприятия управления конфигурацией для категорий НС1 и НС2

Пункт	Мероприятие управления конфигурацией	НС1	НС2
7.2.1	Идентификация конфигурации	x	x
7.2.2(1), (2), (3)	Базовые версии	x	
7.2.2(4) ([1])	Трассируемость базовой версии	x	x
7.2.3	Сообщение о проблеме	x	
7.2.4(1),(2)	Управление изменениями – целостность и идентификация	x	x
7.2.4(3), (4), (5), (6)	Управление изменениями – регистрация, одобрение и тассируемость	x	
7.2.5(1)	Выпуск	x	
7.2.5(2)	Воспроизведение	x	x
7.2.5(3)	Архивирование данных	x	x
7.2.5(4a)	Защита от несанкционированных изменений	x	x
7.2.5(4b), (4c), (4d)	Выбор среды, обновление, дублирование	x	

([1]) Идентификация данных НС2 для использования с новой базовой версией не означает повторной классификации данных по НС1.

8. ПРОЦЕСС ГАРАНТИИ

Процесс гарантии обеспечивает выполнение целей процесса жизненного цикла и завершение мероприятий в соответствии с указанным в планах и обеспечивает рассмотрение отклонений от планов. В данном разделе описываются цели процесса гарантии и мероприятия в обеспечение достижения этих целей. Это не предполагает формирование специальных организационных структур.

Мероприятия процесса гарантии следует проводить с независимостью, для того чтобы объективно оценить процесс жизненного цикла, определить отклонения и обеспечить исправление.

8.1. Цели процесса гарантии

Цели процесса гарантии состоят в обеспечении того, что:

1. Процессы жизненного цикла соответствуют одобренным планам.
2. Данные жизненного цикла конструирования аппаратуры создаются в соответствии с одобренными планами.
3. Изделие, используемое для оценки соответствия, сделано по соответствующим данным жизненного цикла.

8.2. Мероприятия процесса гарантии

Рекомендации по мероприятиям процесса гарантии следующие:

1. Должна быть обеспечена доступность планов аппаратуры, как определено в разделе 4 «Процесс планирования» данного документа и как согласовано в «Плане сертификации аппаратуры».
2. Должно быть обеспечено сохранение рассмотрений в соответствии с одобренными планами и отслеживание пунктов корректирующих действий до их закрытия.
3. Должно быть обеспечено обнаружение, регистрация, оценка, одобрение, сопровождение и разрешение отклонений от планов и стандартов на аппаратуру.
4. Должно быть обеспечено удовлетворение критериям перехода процессов жизненного цикла аппаратуры в соответствии с одобренными планами.

Примечание. *Аудиты являются эффективным методом для выполнения действий по пунктам 1–4 выше.*

5. Для гарантии того, что изделие было выполнено в соответствии с проектными данными, должна быть выполнена инспекционная проверка.

Примечание. *Примером этого мероприятия является проверка FAI.*

6. Должны быть сделаны записи о мероприятиях процесса гарантии, включая доказательства оценки завершения мероприятий конструирования.
7. Там где это применимо, заявитель должен обеспечить, чтобы процессы, используемые субподрядчиком, были совместимы с планами аппаратуры.

9. ПРОЦЕСС ВЗАИМОДЕЙСТВИЯ ПРИ СЕРТИФИКАЦИИ

Цель процесса взаимодействия при сертификации состоит в том, чтобы установить связь и взаимопонимание между Заявителем и сертифицирующим органом в течение всего жизненного цикла конструирования аппаратуры, для содействия процессу сертификации. Процесс взаимодействия при сертификации должен выполняться, как указано в разделе 4 о процессе планирования аппаратуры, и в подразделе 10.1.1 «План сертификации аппаратуры». Таблица А-1 Приложения А дает краткий обзор выходных данных этого процесса. Кроме того, мероприятия взаимодействия могут включать совещания для своевременного одобрения подхода к конструированию, переговоры, касающиеся методов соответствия сертификационному базису, одобрение подхода к конструированию, средства одобрения данных и любые требуемые сертифицирующим органом рассмотрения и совместные испытания.

При завершении проекта в «Итоговом заключении по аппаратуре», описанном в подразделе 10.9, должно содержаться краткое описание используемых процессов конструирования, полученных выходных данных и состояния аппаратуры.

9.1. Средства соответствия и планирование

Заявитель предлагает средства соответствия для аппаратуры. Предложенные средства соответствия определяются в «Плане сертификации аппаратуры». Рекомендации следующие:

1. «План сертификации аппаратуры», «План верификации аппаратуры» и другие запрашиваемые данные должны быть представлены сертифицирующему органу для рассмотрения в тот момент времени, когда влияния изменений проекта на программу минимальны.
2. Вопросы, поставленные сертифицирующим органом по аспектам планирования сертификации аппаратуры, должны быть решены.
3. Соглашение с сертифицирующим органом по «Плану сертификации аппаратуры» должно быть достигнуто.
4. Связь с сертифицирующим органом во время цикла разработки и сертификации должно продолжаться, как отмечено в плане, а вопросы, поднятые сертифицирующим органом, должны своевременно разрешаться.

В некоторых программах сертификационное взаимодействие было установлено не изготовителем оборудования, а изготовителем самолета или другим заказчиком с изготовителем оборудования во вспомогательной роли. Такое взаимодействие должно быть определено в «Плане сертификации аппаратуры» и контакт с сертифицирующим органом должен осуществляться через заявителя. Заявитель несет ответственность за обеспечение сертифицирующего органа необходимыми данными.

Когда некоторые элементы аппаратуры, встроенные в оборудование, закупаются у субподрядчика, в плане сертификации должно быть определено какие данные предполагается получить у субподрядчика и какие должен дать заявитель.

Для заявителя считается приемлемым включить «План сертификации аппаратуры» и план верификации вместе с другими подходящими планами в план сертификации высокого уровня.

9.2. Доказательство соответствия

Заявитель обеспечивает подтверждение того, что процессы жизненного цикла конструирования аппаратуры удовлетворяют планам аппаратуры. Экспертизы сертифицирующего органа могут проводиться в производственных помещениях заявителя или в производственных помещениях поставщика заявителя. Заявитель организует эти экспертизы и представляет, если требуется, данные жизненного цикла конструирования аппаратуры.

Заявитель должен:

1. Разрешать вопросы, поднятые сертифицирующим органам по результатам его экспертиз.
2. Представлять сертифицирующему органу «Итоговое заключение об аппаратуре» по подразделу 10.9 и «Чертеж общего вида» по подразделу 10.3.2.2.1.
3. Предоставлять или делать доступными другие данные или сведения о соответствии, запрашиваемые сертифицирующим органом.

10. ДАННЫЕ ЖИЗНЕННОГО ЦИКЛА КОНСТРУИРОВАНИЯ АППАРАТУРЫ

В данном разделе описываются элементы данных жизненного цикла конструирования аппаратуры, которые могут быть получены во время жизненного цикла конструирования аппаратуры для обеспечения доказательств гарантии конструирования и соответствия требованиям сертификации. Содержание, качество и подробности данных жизненного цикла, требуемые сертифицирующим органом как доказательства гарантии конструирования будут изменяться в зависимости от ряда факторов. Эти факторы включают прикладные требования сертифицирующего органа для бортовых систем, назначенные уровни гарантии конструирования, сложность и опыт эксплуатации аппаратуры. Детали доказательства гарантии конструирования следует определить и зарегистрировать в «Плане сертификации аппаратуры» и согласовать с сертифицирующими органами.

Дополнительные указания в разделе 11 и указания по гарантии конструирования для функций уровня А и В в Приложении В могут привести к формированию дополнительных данных жизненного цикла.

В Приложении А указано, какие данные жизненного цикла конструирования аппаратуры должны быть разработаны, степень независимости проверки и применяемая категория контроля данных, определенная в разделе 7 исходя из уровня гарантии конструирования аппаратуры.

1. Характеристиками данных жизненного цикла конструирования аппаратуры должны быть:
   a. Однозначность. Информация должна быть записана так, чтобы она имела единственную интерпретацию.
   b. Полнота. Информация/данные должны содержать необходимые и существенные требования и описательный материал, рисунки, определение терминов и единиц измерения.
   c. Верифицируемость. Правильность информации/данных может проверить человек или инструмент.
   d. Совместимость. Информация/данные не содержат противоречий.
   e. Модифицируемость. Информация/данные структурированы, и изменения могут осуществляться полно, постепенно и правильно при сохранении структуры.
   f. Трассируемость. Источник информации/данных может быть определен.

Описания в данном разделе не предполагают представить конкретный метод компоновки данных, форму или организацию данных жизненного цикла аппаратуры в рамках комплекта данных. Например, все планы, стандарты и процедуры могут быть описаны в одном документе или в нескольких документах.

2. Метод компоновки данных, форма и организация должны быть предложены в плане PHAC, а соглашение с сертифицирующим органом получено в начале программы.

3. Согласованные данные и информация должны быть восстанавливаемыми и доступными в течение всего срока эксплуатации бортовой системы или оборудования.

10.1. Планы аппаратуры

В планах аппаратуры описываются процессы, процедуры и стандарты, которые должны использоваться при разработке, сертификации, оценке, проверке, обеспечении качества процесса и управлении конфигурацией.

10.1.1. План сертификации аппаратуры

В Плане сертификации аппаратуры определяются процессы, методы, процедуры и стандарты, которые должны использоваться для достижения целей данного документа и получения одобрения на сертификацию системы, содержащей элементы аппаратуры. «План сертификации аппаратуры», после одобрения, представляет сбой соглашение между заявителем и сертифицирующим органом по процессам и мероприятиям, которые должны быть проведены, и итоговым доказательствам, которые следует получить для удовлетворения вопросов сертификации аппаратуры. «План сертификации аппаратуры» может быть частью другого плана, например плана сертификации бортовой системы.

«План сертификации аппаратуры» должен включать:

1. Обзор системы. В данном разделе приводится обзор бортовой системы, в которой должны использоваться элементы аппаратуры, включая функциональное описание системы, отказные состояния системы, архитектуру системы, описание распределения функций для элементов аппаратуры и ПО, а также ссылки на существующую системную документацию.
2. Обзор аппаратуры. В данном разделе описываются функции аппаратуры, элементы аппаратуры, архитектуры, новые технологии и любые методы отказобезопасности, отказоустойчивости, резервирования и обособления, которые предполагается использовать.
3. Сертификационные соображения. В данном разделе описывается сертификационный базис, предлагаемые методы оценки соответствия и уровень гарантии конструирования каждой функции элемента аппаратуры. В нем также приводится подтверждение правильности выбранного уровня гарантии конструирования на основе оценки безопасности аппаратуры и ее использования в бортовой системе, включая описание потенциальных условий отказа аппаратуры, как описано в пункте 2.3.4. Там где применимо, могут быть также включены либо краткое изложение FFPA, либо план для выполнения и применения результатов FFPA.
4. Жизненный цикл конструирования аппаратуры. В данном разделе описываются процедуры, методы и стандарты, которые должны применяться, а также процессы и мероприятия, которые должны выполняться для удовлетворения целей гарантии конструирования аппаратуры. Также описываются действия, комбинации и последовательность действий, взаимоотношения между процессами и действиями, критерии перехода, ответственность, использование инструментов и средств для обеспечения обратной связи и взаимодействия внутри процессов аппаратуры и между процессами аппаратуры и процессами системы и ПО. Данный раздел может обращаться к приемлемым планам, стратегиям, стандартам, процедурам и к отклонениям от этих планов и стандартов для данной программы.
5. Данные жизненного цикла конструирования аппаратуры. В данном разделе описываются или делается ссылка на данные, которые должны быть разработаны или должны представляться или иметься в наличии для свидетельствования соответствия целям данного документа и плану.
6. Дополнительные соображения. В данном разделе описываются дополнительные соображения. К ним относятся применение ранее разработанной аппаратуры, включая ссылки на применяемые данные, которые должны повторно использоваться, использование COTS, опыт эксплуатации изделия, оценка и квалификация инструмента, как описано в разделе 11, или указания по гарантии конструирования для функций уровня A или B, как описано в Приложении B.
7. Альтернативные методы. В разделе описываются альтернативные методы, предлагаемые к использованию в программе, которые либо не описаны в данном документе, либо должны применяться способом, отличным от того, который описан в данном документе. Должно быть представлено обоснование необходимости применения альтернативного метода.
8. График сертификации. В данном разделе описываются основные вехи программы и сроки представления данных жизненного цикла конструирования аппаратуры сертифицирующему органу.

10.1.2. План конструирования аппаратуры

В «Плане конструирования аппаратуры» описываются процедуры, методы и стандарты, которые необходимо применять, и процессы и действия, которые должны быть выполнены при конструировании элемента аппаратуры. Этот план может быть включен в «План сертификации аппаратуры» и может излагать исходную стратегию конструирования и применяемые стандарты.

«План конструирования аппаратуры» должен включать:

1. Жизненный цикл конструирования аппаратуры. Ссылки на стратегию конструирования и стандарты, которые должны применяться, и описание процессов и мероприятий жизненного цикла конструирования аппаратуры, которые будут использоваться для достижения целей конструирования на уровне гарантии конструирования аппаратуры.
2. Описание аппаратного изделия. Идентификация спецификаций аппаратуры, которые должны быть получены, альтернативные применения, запланированный срок службы и соображения модификации.
3. Методы конструирования аппаратуры. Описание содержания требований и методов спецификации, методов эскизного проектирования, методов технического проектирования, синтетических методов, методов реализации и методов перехода к производству, которые должны использоваться для элемента аппаратуры. Когда архитектурное смягчение для функций уровней A и B, как описано в подразделе 3.1 Приложения B, было рассмотрено, но не реализовано в момент написания данного плана, следует установить как в процессе конструирования будет принято такое решение.
4. Среда конструирования аппаратуры. Описание инструментов конструирования, которые предполагается использовать.
5. Данные элемента аппаратуры. Определение данных конструирования элемента аппаратуры, которые необходимо сформировать, или ссылки на ранее разработанные спецификации элемента аппаратуры, номера документа или чертежа, шифр компонента.
6. Другие соображения. Описание вариантов запланированных технологических процессов, вариантов применения, компоновки изделия и вариантов монтажа аппаратуры.

10.1.3. План обоснования аппаратуры

«План обоснования аппаратуры» описывает процедуры, методы и стандарты, которые должны быть применимы, процессы и мероприятия, которые должны быть выполнены для обоснования производных требований к изделию с целью достижения целей обоснования, представленных в данном документе. Этот план может быть включен в «План сертификации аппаратуры» и может иметь ссылки на стандарты оценки качества, которые должны использоваться.

«План обоснования аппаратуры» должен включать:

1. Методы обоснования. Описание и ссылки на процедуры обоснования, стандарты и методы, которые должны использоваться. Методы могут включать анализ, рассмотрения и испытания.
2. Данные обоснования. Идентификация и описание получаемых доказательств по результатам процесса обоснования аппаратуры.
3. Среда обоснования. Идентификация и описание анализа и испытательного оборудования, а также инструментов обоснования, которые должны использоваться с целью реализации процесса обоснования и мероприятий с ним связанных.

10.1.4. План верификации аппаратуры

«План верификации аппаратуры» описывает процедуры, методы и стандарты, которые должны применяться и процессы и действия, которые должны быть выполнены для проверки элементов аппаратуры с целью достижения задач проверки данного документа. Этот план может быть включен в «План сертификации аппаратуры» и может содержать ссылки на стратегию и стандарты, которые должны использоваться.

«План верификации аппаратуры» должен включать:

1. Методы верификации. Описание и ссылки на стратегию проведения верификации, процедуры, стандарты и методы, которые должны применяться с целью доказательства целостности элементов аппаратуры, включая COTS и используемые функции. Методы могут включать анализы, рассмотрения и испытания. Когда применяются перспективные методы анализа из подраздел 3.3 Приложения B, следует включить детальное описание методов для применяемых FFP и критерии полноты проведенной верификации.

2. Данные верификации. Определение и описание получаемых доказательств по процессу верификации аппаратуры.

3. Независимость верификации. Описание средств, которые необходимо использовать, чтобы гарантировать независимость верификации для целей, требующих независимость.

4. Среда верификации. Определение и описание оборудования для анализа и испытаний, инструментов верификации, которые должны применяться с целью реализации процесса верификации и мероприятий.

5. Организационная ответственность. Определение организаций, ответственных за реализацию процесса верификации.

10.1.5. План управления конфигурацией аппаратуры

В «Плане управления конфигурацией аппаратуры» описываются стратегии, процедуры, стандарты и методы, которые должны использоваться с целью удовлетворения целей управления конфигурацией, изложенных в данном документе.

«План управления конфигурацией аппаратуры» должен включать:

1. Методы управления конфигурацией аппаратуры. Описание и ссылка на стратегию, процедуры, стандарты и методы, которые должны использоваться для идентификации, организации и управления аппаратурой и данными ее жизненного цикла.

2. Базовые версии аппаратуры. Описание методов и процедур, используемых для установления базовых версий изделия и проекта и обеспечения прослеживаемости базовой версии.

3. Регистрация проблем и решение. Описание методов и процедур, которые должны использоваться для регистрации, сопровождения и решения по сообщениям о проблеме.

4. Контроль изменения. Описание методов, процедур и процессов для идентификации, управления и сопровождения изменений контролируемых элементов данных.

5. Хранение и воспроизведение. Описание процедур для выпуска, архивирования и воспроизведения данных жизненного цикла конструирования аппаратуры. Описание должно включать содержание архива, формат и стандарты на среду, правила, методы и критерии.

6. Контроль среды. Описание процедур и методов для идентификации и контроля инструментов, используемых для конструирования и верификации аппаратуры.

7. Инструменты управления конфигурацией. Описание инструментов и ресурсов, используемых в процессе управления конфигурацией и мероприятиях.

10.1.6. План процесса гарантии аппаратуры

«План процесса гарантии аппаратуры» описывает процедуры, методы и стандарты, которые должны применяться, и процессы и действия, которые должны выполняться для достижения целей процесса гарантии данного документа.

«План процесса гарантии аппаратуры» должен включать:

1. Управление процессом. Описание стратегии и процедур для реализации процесса гарантии процессов конструирования аппаратуры.

2. Организационная ответственность. Описание организаций, ответственных за реализацию процесса гарантии.

3. Соответствие. Описание политики, процедур и критериев для определения соответствия процесса и изделия.

4. Мероприятия процесса гарантии. Описание рассмотрений и аудитов процесса гарантии проводимых с целью демонстрации соответствия процессов планам и стандартам.

5. Отклонения. Описание методов для обнаружения, регистрации, оценки, решения и одобрения отклонений от планов и стандартов.

10.2. Стандарты и руководства по конструированию аппаратуры

Стандарты и руководства по конструированию аппаратуры могут определять правила, процедуры, методы и критерии для процессов конструирования, обоснования, верификации, гарантии и контроля аппаратуры и используются для оценки приемлемости и качества результатов конструирования аппаратуры. Стандарты могут не потребоваться, но если заявитель считает необходимым использовать их в проекте, они становятся частью сертификационного базиса и планов по проекту. Как и в случае планов, такие стандарты и руководства могут быть представлены как отдельный документ или как множество документов. Для проведения в жизнь стандартов можно использовать инструменты.

10.2.1. Стандарты на требования

«Стандарты на требования» могут использоваться во время процесса определения требований с целью установления правил, процедур, методов, руководств и критериев для разработки требований. «Стандарты на требования» могут включать методы и критерии для разработки и описания требований, методы и критерии для обоснования требований, используемые для выражения требований формы представления, руководства по использованию инструментов спецификации требований и средств, используемых для направления производных требований в процесс конструирования системы.

10.2.2. Стандарты на конструирование аппаратуры

«Стандарты на конструирование аппаратуры» могут использоваться в процессе эскизного проектирования и в процессе технического проектирования с целью определения правил, процедур, методов, руководств и критериев для разработки и спецификации конструкции аппаратуры.

«Стандарты на конструирование аппаратуры» могут включать:

1. Методы и способы представления конструкции аппаратуры.
2. Соглашение по определению наименований и спецификации конструкции.
3. Руководство по методам конструирования.
4. Руководство по использованию инструментов конструирования.
5. Руководство по выбору электронных компонентов.
6. Руководство по оценке альтернативных вариантов конструирования.
7. Руководство по оценке отказобезопасных и отказоустойчивых конструкций.
8. Описание средств для обеспечения обратной связи с процессом определения требований и для уточнения требований.

10.2.3. Стандарты на обоснование и верификацию аппаратуры

«Стандарты на обоснование и верификацию аппаратуры» могут применяться в процессах обоснования и верификации с целью определения правил, процедур, методов, руководств и критериев для обоснования и верификации проекта аппаратуры и ее реализации.

10.2.4. Стандарты на архивирование аппаратуры

«Стандарты на архивирование аппаратуры» могут применяться с целью определения процедур, методов и критериев, используемых для сохранения и архивирования данных по изделию и для разработки и поддержки архивов программы и проекта. Стандарты на архивирование аппаратуры могут включать содержание архива, формат, стандарты на среду, правила, методы и критерии.

10.3. Данные конструирования аппаратуры

Данными конструирования аппаратуры являются спецификации, документы и чертежи, которые определяют элементы аппаратуры.

10.3.1. Требования к аппаратуре

Требования определяют функциональные требования, требования к характеристикам, безопасности, качеству, ремонтопригодности и надежности для разрабатываемого элемента аппаратуры.

«Требования к аппаратуре» должны включать:

1. Требования к конструкции и безопасности системы, назначенные аппаратуре.
2. Определение применяемых стандартов для аппаратуры.
3. Функциональные и технические требования к аппаратуре, включая производные требования и пределы нагрузок для нормального применения.
4. Требования к надежности и качеству аппаратуры, включая требования, связанные с частотой отказов, времени воздействия и конструктивными ограничениями.
5. Требования к техобслуживанию и ремонту аппаратуры в течение срока эксплуатации элемента аппаратуры.
6. Требования к изготовлению и сборке аппаратуры.
7. Требования к контролепригодности аппаратуры.
8. Требования к транспортировке и хранению аппаратуры.
9. Требование к монтажу.

10.3.2. Конструкторские документы аппаратуры

Конструкторские документы аппаратуры обеспечивают определение элемента аппаратуры и состоят из комплекта чертежей, документов и спецификаций, используемых для создания элемента аппаратуры. В следующих параграфах определяются некоторые типичные конструкторские документы и их содержание. Тип данных, чертежи и документы, подготовленные для заданного проекта аппаратуры, будут изменяться в зависимости от размера, сложности и количества компонентов, которые содержит изделие.

10.3.2.1. Данные эскизного проектирования

«Данные эскизного проектирования» – это данные (пояснительная записка, чертеж общего вида, схемы и др.), которые описывают архитектуру элемента аппаратуры и функциональную схему и могут содержать:

1. Описание высокого уровня, такое как блок-схема или определение на языке HDL, которое выделяет основные функции и показывает поток информации между этими функциями.
2. Габаритный чертеж, которая описывает компоновку элемента аппаратуры, например, чертежи или рисунки, показывающие внешнюю компоновку, размещение печатной платы, выбор и размещение соединителей и главную электромонтажную схему.
3. Другие архитектурные особенности и обособление, важные с точки зрения летной годности. К ним могут относиться такие аспекты, как защита от электромагнитной помехи, молнии, удара и вибрации, неиспользуемые функции в главных компонентах, а также человеко-машинные интерфейсы, такие, как эргономические факторы, характеристики освещенности и разрешающая способность индикаторов.
4. Функциональное описание элемента аппаратуры высокого уровня.
5. Функциональная архитектура элемента аппаратуры.
6. Данные предварительной оценки безопасности аппаратуры.

10.3.2.2. Данные технического проектирования

«Данные технического проектирования» описывают данные, необходимые для реализации элемента аппаратуры в соответствии с требованиями. В зависимости от иерархического уровня

элемента аппаратуры, эти данные могут содержать чертежи высокого уровня, сборочные чертежи, данные взаимодействия, данные о деталях, описания аппаратуры на языке HDL, данные надежности, данные по методологии испытаний, перечень неиспользуемых функций в выбранных компонентах и действия, предпринятые с целью обеспечения того, чтобы они не влияли на безопасность элемента аппаратуры, данные контроля установки и данные интерфейса аппаратура/ПО. Некоторые специфические данные описаны ниже.

Примечание. *В дополнение к данным технического проектирования, которые требуются в других применяемых требованиях сертификации, таких, как технические стандартные заказы, содержание и наличие других элементов данных технического проектирования предлагается заявителем для сертифицирующего органа в плане PHAC.*

10.3.2.2.1. Чертеж общего вида

«Чертеж общего вида» определяет элемент аппаратуры и все устройства, подустройства, компоненты и соответствующую документацию для элемента аппаратуры.

10.3.2.2.2. Сборочные чертежи

«Сборочные чертежи» включают дополнительную детальную информацию, необходимую для сборки элемента аппаратуры, устройства или подустройства.

«Сборочный чертеж» может включать:

1. Размещение и ориентацию элементов аппаратуры в аппаратном устройстве.
2. Определение последовательностей инструкций по сборке или методов обеспечения правильного и отказоустойчивого устройства.
3. Размещение идентификационных меток, адресов, наглядных обозначений, используемых в последующих операциях.

10.3.2.2.3. Монтажные чертежи

Чертежи обеспечивают правильность установки элемента аппаратуры в системе или правильную установку элемента аппаратуры в другом элементе аппаратуры. Для элемента аппаратуры более низкого уровня сборочные чертежи для элемента аппаратуры следующего более высокого уровня или устройства могут действовать как монтажные чертежи.

«Монтажный чертеж» может включать:

1. Габаритные размеры.
2. Требование по допускам.
3. Информацию по монтажу и охлаждению.
4. Информацию о массе, центре тяжести и других параметрах, необходимых для обеспечения безопасной и правильной установки.

10.3.2.2.4. Данные интерфейса аппаратура/ПО

Технические характеристики аппаратуры, как определено в спецификации требований, могут зависеть от конфигурации аппаратуры, определяемой ПО, калибровки аппаратуры с помощью ПО или необходимого взаимодействия между аппаратурой и ПО.

«Данные интерфейса аппаратура/ПО» могут включать:

1. Адреса памяти.
2. Распределение адресных полей памяти, в которые могут загружаться данные.
3. Информацию о последовательности и синхронизации.
4. Другую информацию, необходимую для функционирования интерфейса аппаратура/ПО.

10.4. Данные обоснования и верификации

«Данные обоснования и верификации» являются свидетельством полноты и правильности результатов конструирования аппаратуры и самого элемента аппаратуры. Они обеспечивают гарантию того, что аппаратура была разработана в соответствии с требованиями и проектом, правильно изготовлена и что цели конструирования были достигнуты. Данные включают процедуры и результаты рассмотрений, анализов и испытаний аппаратуры. Дополнительные данные, помимо тех, что описаны в данном разделе, могут потребоваться для функций уровней А и В, как описано в Приложении В.

10.4.1. Данные трассируемости

Трассируемость аппаратуры устанавливает соответствие между требованиями, техническим проектированием, реализацией и данными проверки, что облегчает управление конфигурацией, модификацию и верификацию компонента аппаратуры.

«Данные трассируемости аппаратуры» должны включать:

1. Соотношение требований к системе, назначаемых аппаратуре, с требованиями к аппаратуре.
2. Соотношение между требованиями и данными технического проектирования аппаратуры.
3. Соотношение между данными технического проектирования аппаратуры и созданного компонента аппаратуры или сборки.
4. Соотношение между требованиями, включая производные требования к аппаратуре, и данными технического проектирования и процедурами и результатами верификации.
5. Результаты анализа трассируемости.

10.4.2. Процедуры рассмотрений и анализов

«Процедуры рассмотрений и анализов аппаратуры» определяют процесс и критерии для проведения рассмотрений и анализов.

«Процедуры рассмотрений и анализов аппаратуры» должны включать:

1. Назначение рассмотрения и анализа.
2. Организации, участвующие в рассмотрении.
3. Критерии рассмотрения или анализа.
4. Детальные инструкции для проведения рассмотрения или анализа.
5. Приемлемость рассмотрения или анализа и критерии завершения.

10.4.3. Результаты рассмотрений и анализов

«Результаты рассмотрений и анализов аппаратуры» подтверждают, что рассмотрения и анализы были выполнены в соответствии с одобренными процедурами и критериями.

«Результаты рассмотрений и анализов аппаратуры» должны включать:

1. Идентификацию процедуры рассмотрения или анализа.
2. Идентификацию рассмотренных и проанализированных элементов данных.
3. Участие персонала в рассмотрении или анализе.
4. Результаты рассмотрения или анализа.
5. Корректирующие действия, сформированные в результате рассмотрения или анализа, такие, как перечень отчетов по проблеме и действий.
6. Выводы по результатам рассмотрения или анализа с включением: для рассмотрений – качественной оценки проверенного элемента, для анализа – количественной оценки проанализированного элемента и данных анализа.

10.4.4. Процедуры испытаний

«Процедуры испытаний аппаратуры» определяют методы, окружающие условия и инструкции для проведения функциональных и квалификационных испытаний, используемых для верификации элемента аппаратуры.

«Процедуры испытаний аппаратуры» включают:

1. Назначение испытаний.
2. Определение испытательных установок, ПО и инструкций по испытательному оборудованию, требуемых для каждого испытания аппаратуры.
3. Детальные инструкции для проведения процедур испытаний.
4. Входные данные испытаний.
5. Предполагаемые результаты, такие, как критерии «прошел/отказал», и требования, проверяемые в процессе испытаний.

10.4.5. Результаты испытаний

«Результаты испытаний аппаратуры» подтверждают, что испытания выполнены в соответствии с одобренными процедурами проведения верификации элемента аппаратуры.

«Результаты испытания аппаратуры» должны включать:

1. Определение процедуры испытаний.
2. Определение испытуемого элемента.
3. Реальные результаты проведения испытаний.
4. Определение персонала, проводящего испытания и даты, когда испытания были проведены.
5. Трактовку результатов с помощью анализа или рассмотрения и реально достигнутый в испытаний охват требований.

10.5. Критерии приемочных испытаний аппаратуры

Эти данные обеспечивают критерии и данные оценки того, что испытание и результаты соответствующих испытаний способны обеспечить правильность изготовления или ремонта блока.

Критерии должны включать:

1. Основные параметры для испытаний.
2. Критерий «прошел/отказал» для каждого основного параметра.
3. Любые ограничения испытаний.
4. Обоснование основных параметров и критериев «прошел/отказал».
5. Покрытие характеристик конструирования, необходимых для выполнения требований безопасности.
6. Данные оценки, которые показывают, что критерии испытания были правильно применены и основаны на реальных процедурах испытаний и соответствующих результатах испытаний.

10.6. Сообщения о проблемах

«Сообщения о проблемах» являются средством определения и записи разрешения проблем конструирования аппаратуры, несоответствия процесса планам аппаратуры и стандартам или расхождений в данных жизненного цикла аппаратуры.

«Сообщения о проблемах» должны включать:

1. Определение элемента конфигурации и процесса, при которых наблюдалась проблема.
2. Определение элемента конфигурации, который должен быть модифицирован, или описание процесса, который должен быть изменен.

3. Описание проблемы, которое позволяет понять проблему и решить ее.

4. Описание корректирующего мероприятия, предпринятого для решения выявленной проблемы.

10.7. Протоколы управления конфигурацией аппаратуры

Результаты мероприятий процесса управления конфигурацией регистрируется в «Протоколах управления конфигурацией аппаратуры». Они могут включать перечни определения конфигурации, базовые версии или электронные записи, отчеты об изменениях, краткое содержание сообщений о проблеме, данные определения инструментов, архивные записи и записи выпусков.

10.8. Протоколы процесса гарантии аппаратуры

Результаты мероприятий процесса гарантии аппаратуры регистрируются в «Протоколах процесса гарантии аппаратуры». Они могут содержать отчеты о рассмотрениях и аудитах, протоколы совещаний, записи разрешенных отклонений процесса или отчеты по оценке соответствия.

10.9. Итоговое заключение об аппаратуре

«Итоговое заключение об аппаратуре» – это первичный элемент данных для демонстрации соответствия «Плану сертификации аппаратуры» и демонстрации сертифицирующему органу того, что задачи данного документа для элементов аппаратуры достигнуты. Это заключение может быть объединено с итоговым заключением по системе.

«Итоговое заключение об аппаратуре» должно включать следующую информацию, как изложено в «Плане сертификации аппаратуры»:

1. Обзор системы.

2. Обзор аппаратуры.

3. Сертификационные соображения.

4. Жизненный цикл конструирования аппаратуры.

5. Данные жизненного цикла конструирования аппаратуры.

6. Ранее разработанная аппаратура.

7. Дополнительные соображения.

8. Альтернативные методы.

Должны быть определены отличия конструирования от одобренного «Плана сертификации аппаратуры». Кроме того, должны быть рассмотрены следующие четыре пункта:

1. Идентификация аппаратуры. В этом пункте с помощью номера изделия и версии определяются конфигурация аппаратуры и элементы аппаратуры.

2. История изменений. Если применимо, данный пункт включает краткое описание изменений аппаратуры с учетом изменений, сделанных вследствие отказов, влияющим на безопасность, и определяет изменения процессов жизненного цикла конструирования аппаратуры с момента прошлой сертификации.

3. Состояние аппаратуры. Пункт содержит краткое описание отчетов по проблеме, нерешенных к моменту сертификации, включая определение функциональных ограничений.

4. Уведомление о соответствия. Этот пункт включает уведомление о соответствии данному документу и краткое описание методов, использованных для демонстрации соответствия критериям, определенным в планах аппаратуры. В этом пункте также рассматриваются дополнительные правила и отклонения от планов аппаратуры, процедур и данного документа.

Примечание. *Данные, включенные в «План сертификации аппаратуры», не обязательно должны повторяться в Итоговом заключение об аппаратуре, однако выполнение этого может помочь в процессе сертификации.*

11. ДОПОЛНИТЕЛЬНЫЕ УКАЗАНИЯ

В данном разделе даны дополнительные указания по вопросам гарантии конструирования, которые не были отражены в предыдущих разделах. Эти дополнительные указания могут использоваться на усмотрение заявителя для выполнения задач разделов с 2 по 9. Любое использование дополнительных указаний должно быть согласовано с сертифицирующим органом.

11.1. Применение ранее разработанной аппаратуры

В данном подразделе обсуждаются вопросы, связанные с использованием ранее разработанной аппаратуры. Указания включают оценку модификаций аппаратуры, установки на самолете, условий применения или условий конструирования и модернизацию базовых конфигураций проекта. Руководство по использованию компонентов COTS, особый случай ранее разработанной аппаратуры, изложено в подразделе 11.2. Указания по управлению конфигурацией и процессу гарантии должны рассматриваться для каждого применения ранее разработанной аппаратуры.

Намерение использовать ранее разработанную аппаратуру должно быть изложено в «Плане сертификации аппаратуры».

11.1.1. Модификации ранее разработанной аппаратуры

В данном подразделе обсуждаются модификации ранее разработанной аппаратуры. Модификация может быть вызвана изменением требований, обнаруженными ошибками, совершенствованием технологии и аппаратуры или трудностями закупки.

Анализ мероприятий для предложенных модификаций включает:

1. Рассмотрение выходных данных процесса оценки безопасности системы.
2. Применение указаний подраздела 11.1.4, если увеличен уровень гарантии конструирования аппаратуры.
3. Должно быть проанализировано влияние изменений, включая последствия изменений, которые могут привести к необходимости повторной верификации – большей, чем непосредственно связанная с изменяемой областью. Эта область может быть определена с помощью анализа потоков сигналов, функционального анализа, анализа синхронизации, анализа трассируемости или других подходящих средств.

11.1.2. Изменение установки на самолете

В данном подразделе обсуждается использование установке на новом самолете аппаратуры, которая была ранее сертифицирована на определенном уровне гарантии конструирования аппаратуры и со специальным сертификационным базисом. При использовании ранее разработанной аппаратуры на новых самолетах должны применяться следующие инструкции:

1. В процессе оценки безопасности системы оценивается установка на новом самолете, определяется уровень гарантии конструирования аппаратуры и сертификационный базис. Никаких дополнительных усилий не требуется, если для новой установки они те же самые или менее жесткие, чем были в предыдущей установке.
2. Если в новой установке требуются функциональные модификации, то должно удовлетворяться руководство подраздела 11.1.1 по модернизации ранее разработанной аппаратуры.
3. Если в результате ранней деятельности по конструированию не были получены данные, требуемые для выполнения задач безопасности новой установки, должно выполняться руководство подраздела 11.1.4 «Модернизация базовой версии».

11.1.3. Изменение среды применения или конструирования

Использование ранее разработанной аппаратуры может предусматривать новую среду конструирования или интеграцию с другими ПО и аппаратурой относительно применявшихся в первоначальном варианте.

Новая среда конструирования может увеличить или уменьшить некоторые мероприятия в пределах процессов жизненного цикла конструирования аппаратуры. Инструкции следующие:

1. Если в новых условиях конструирования применяются инструментальные средства, то могут быть применимы положения подраздела 11.4 «Оценка и квалификация инструмента».
2. Должна производиться верификация интерфейсов аппаратуры там, где ранее разработанная аппаратура использовалась с другой взаимодействующей аппаратурой.
3. Должна учитываться необходимость повторной верификации интерфейсов ПО/аппаратура, когда в ранее разработанной аппаратуре используется другое ПО.

11.1.4. Модернизация базовой версии

Следующее руководство предназначено для элементов аппаратуры, данные жизненного цикла которых с предыдущего применения оказались недостаточными для задач безопасности, связанных с новым применением. Данное руководство предназначено помочь заявителю в получении одобрения с сертифицирующим органом аппаратуры, ранее разработанной при более низком уровне гарантии конструирования аппаратуры. Руководство по модернизации базовой версии проекта включает:

1. Цели данного документа должны быть выполнены с преимущественным использованием данных жизненного цикла ранее выполненного конструирования.
2. Аспекты сертификации аппаратуры должны быть основаны на отказных состояниях и уровнях гарантии конструирования аппаратуры, как определено процессом оценки безопасности системы. Должно быть проанализировано влияние изменений на предыдущее применение с целью определения областей с недостаточными данными.
3. Данные жизненного цикла ранее выполненного конструирования должны быть оценены для гарантии того, что цели процесса верификации удовлетворяются для аппаратуры, в которой планируется реализация измененной функции на требуемом уровне гарантии конструирования аппаратуры.
4. Может использоваться обратное конструирование для восстановления данных жизненного цикла аппаратуры, которые для удовлетворения целей данного документа недостаточны или отсутствуют.
5. Если для удовлетворения целей гарантии конструирования данного документа планируется использование опыта эксплуатации изделия, то при модернизации базовой версии проекта, должны быть рассмотрены указания подраздела 11.3 «Опыт эксплуатации изделия».
6. Заявитель должен определить стратегию обеспечения соответствия с данным документом в «Плане сертификации аппаратуры».

11.1.5. Дополнительные указания по управлению конфигурацией

Процесс управления конфигурацией для нового применения ранее разработанной аппаратуры должен, в дополнение к положениям раздела 7, включать следующее:

1. Трассируемость изделия аппаратуры и данных жизненного цикла предшествующего применения к новому применению.
2. Процессы управления изменениями, для организации запросов на изменение от различных применений общего элемента.

11.2. Применение коммерческих готовых компонентов

Компоненты COTS интенсивно используются в проектах аппаратуры и обычно данные конструирования компонентов COTS не представляются для рассмотрения. В процессе сертификации не рассматриваются отдельные компоненты, модули или подсистемы, если они являются частью специальной сертифицируемой самолетной функции. При этом применение компонентов COTS будет проверено в общем процессе конструирования, включая вспомогательные процессы, как описано в данном документе. Использование процесса управления электронными компонентами вместе с процессом конструирования обеспечивает основу для применения компонентов COTS.

11.2.1. Управление электронными компонентами для коммерческих готовых компонентов

Управление электронными компонентами для COTS-компонентов является важным вспомогательным процессом, связанным с конструированием и разработкой аппаратуры. Процесс управления электронными компонентами применяется к электронным компонентам COTS. Хотя существуют деловые и технические аспекты данного процесса, в этом разделе описываются только технические аспекты, т.к. они влияют на сертификацию.

Сертификационный зачет может быть получен при установлении того, что:

1. Изготовитель компонента может продемонстрировать доказательства производства высококачественных компонентов.
2. Изготовителем компонентов установлены процедуры контроля качества.
3. Существует опыт эксплуатации, подтверждающий успешную работу компонента.
4. Компонент был квалифицирован изготовителем или с помощью дополнительных испытаний, которые устанавливает надежность компонента.
5. Изготовитель компонента контролирует уровень качества компонента или же он гарантируется с помощью дополнительных испытаний компонента.
6. Компоненты выбираются на основе технической пригодности к назначенному применению, например учитывается температурный диапазон, мощность или номинальное напряжение, или для установления этого используются дополнительные испытания или другие средства.
7. Характеристики компонента и надежность контролируются на постоянной основе с обратной связью с изготовителями компонентов относительно требующих улучшения областей.

11.2.2. Закупка коммерческих готовых компонентов

Руководство по закупке компонентов COTS не является целью данного документа, но обратная связь с аспектами закупки должна быть организована и разрешена заявителем, когда они имеют существенное влияние на гарантию конструирования аппаратуры.

Основные аспекты включают:

1. Реальное наличие данных гарантии конструирования компонентов COTS, как требуется в данном документе.
2. Изменения параметров компонента, которые зависят от производственных объемов, не могут быть определены даже испытаниями на отказоустойчивость.
3. Выделение аспектов технологии электронных компонентов.
4. Компоненты COTS, которые становятся незакупаемыми.

11.3. Опыт эксплуатации изделия

Опыт эксплуатации может использоваться для доказательства гарантии конструирования ранее разработанной аппаратуры и компонентов COTS. Опыт эксплуатации относится к данным, собранным на основе любого предыдущего или настоящего использования компонентов. Данные небортовых применений не исключаются.

Примечание. *Широкое и успешное использование изделия может обеспечить уверенность в том, что конструирование изделия является зрелым и свободным от ошибок и что качество изготовления изделия продемонстрировано.*

11.3.1. Критерии приемлемости данных опыта эксплуатации изделия

Когда данные опыта эксплуатации используются для гарантии конструирования, соответствие и приемлемость данных опыта эксплуатации зависит от одного или более следующих положений:

1. Схожести использования элемента аппаратуры по отношению к применению, функции, среде эксплуатации и уровню гарантии конструирования.

2. Предела, до которого данные гарантии конструирования базируются на предложенной конфигурации элемента аппаратуры.

3. Предела, до которого ошибки конструирования, обнаруженные во время оцениваемого периода эксплуатации, были ограничены, уменьшены или проанализированы и определены, как не имеющие влияния на безопасность в используемой конфигурации.

4. Реальная интенсивность отказов в эксплуатации.

Примечание. *В «Плане сертификации аппаратуры» должны быть специально рассмотрены те аспекты, при которых гарантия конструирования применяемых изделий основывается на данных опыта эксплуатации.*

11.3.2. Оценка данных опыта эксплуатации изделия

Для удовлетворения выше приведенным критериям заявитель должен:

1. Оценить на основании технического анализа соответствие предыдущих применений, установок и окружающих условий целевому применению.

Примечание. *Данные, используемые для определения соответствия применения и ограничений применения, могут быть приведены в технических условиях, картах данных, примечаниях по использованию, сервисных бюллетенях, переписке пользователя и записях об опечатках. Эти источники информации могут также описывать функции, связанные с элементом аппаратуры, так что бортовое применение может быть скоординировано с предшествующими применениями.*

2. Оценить предназначенное применение с точки зрения влияния на процесс оценки безопасности, включая возможное ослабление влияния ошибок конструирования, идентифицированных с помощью данных.

3. Оценить любые доступные статистические данные по ошибкам конструирования и их влиянию на процесс оценки безопасности. Качественная оценка может использоваться тогда, когда нет статистических данных.

4. Оценить имеющиеся сообщения о проблеме. Сообщения о проблеме могут показать, что опыт эксплуатации привел к улучшениям в существующей конфигурации. Выявленные, но не зафиксированные проблемы, могут быть ослаблены архитектурными средствами или путем выполнения дополнительной верификации. Установить или оценить взаимоотношения между сообщениями о проблеме и изменением требований к изделию или элементу аппаратуры.

Примечание. *Для электронных компонентов надлежащая эксплуатация может увеличить уверенность в том, что ошибки обнаружены и устранены или что имеются временные «трудности».*

11.3.3. Данные оценки опыта эксплуатации изделия

Данные оценки опыта эксплуатации изделия, используемые для доказательства гарантии конструирования для предлагаемого применения, должны включать:

1. Определение компонента и его функции в бортовой системе. Определение уровня гарантии конструирования или, для компонентов, используемых в уровнях А и В, – описание дополнительных средств гарантии компонента, таких, как архитектурные средства и дополнительные или перспективные стратегии проверки, которые необходимо применять.

2. Описание процесса сбора и оценки данных опыта эксплуатации, включая критерии для определения адекватности и достоверности данных.

3. Данные опыта эксплуатации, включая учитываемую детальную эксплуатационную информацию, историю изменения, используемые для анализа данных опыта эксплуатации допущения, и краткое описание результатов анализа.

4. Доказательство адекватности данных опыта эксплуатации относительно предназначенного применения и требуемого уровня гарантии конструирования.

11.4. Оценка и квалификация инструмента

Во время конструирования и верификации аппаратуры будут использоваться как аппаратные, так и программные инструменты. Когда инструменты конструирования используются для создания элемента аппаратуры или проекта аппаратуры, ошибка в средстве может вызвать ошибку в элементе аппаратуры. Когда инструменты верификации используются для проверки элемента аппаратуры, ошибка в инструменте может вызвать отказ в обнаружении ошибки в элементе аппаратуры или проекте аппаратуры. Прежде чем использовать инструмент, необходимо выполнить его оценку. Результаты этой оценки и, если необходимо, квалификация инструмента, должны быть документированы.

Целью квалификации и оценки инструмента является обеспечение того, чтобы инструмент был способен выполнять конкретные действия конструирования или верификации с требуемым уровнем доверия, для которого инструмент будет использоваться.

11.4.1. Процесс оценки и квалификации инструмента

При оценке инструмента оценивается роль инструмента в процессе жизненного цикла конструирования, и в зависимости от роли средства и уровня гарантии конструирования функции аппаратуры может предусматриваться выполнение квалификационных мероприятий. Руководство по оценке представлено как блок-схема и применяется как к инструментам конструирования, так и к инструментам верификации, когда они используется для достижения целей или генерирования элементов данных для достижения этих целей.

Блок-схема приведет заявителя к ограниченной оценке некоторых категорий инструментов или к квалификации инструментов других категорий.

Процесс квалификации и оценки инструментов может быть применен или к отдельному инструменту или к совокупности инструментов. Инструменты часто обладают возможностями за пределами тех, которые требуются для конкретного мероприятия конструирования или верификации любого специального проекта. Поэтому необходимо только оценить те функции инструмента, которые используются для жизненного цикла конкретной аппаратуры, а не весь инструмент.

Признается, что инструменты часто используются совместно и раздельно на разных этапах жизненного цикла. Если один и то же инструмент используется и на этапе конструирования и на этапе верификации, тогда инструмент необходимо оценивать как инструмент конструирования, пока не будут установлены различие и защита между двумя функциями.

Примечания: ***1.*** *Если оценка конкретного инструмента показывает, что некоторые из функций используются для конструирования, а другие функции для проверки, целесообразно рассмотреть функции отдельно и выполнить оценку для каждой группы оцениваемых функций инструмента.*

2. *Оценка фокусируется скорее на применении инструмента, чем на нем самом.*

Блок-схема рисунка 11-1, показывает соображения относительно оценки инструмента и обеспечивает руководство для определения того, когда может быть необходима квалификация инструмента. Номера в блоках решений и действий относятся к номерам пунктов, сопровождающих рисунок, которые дают дальнейшее разъяснение решения или действия.

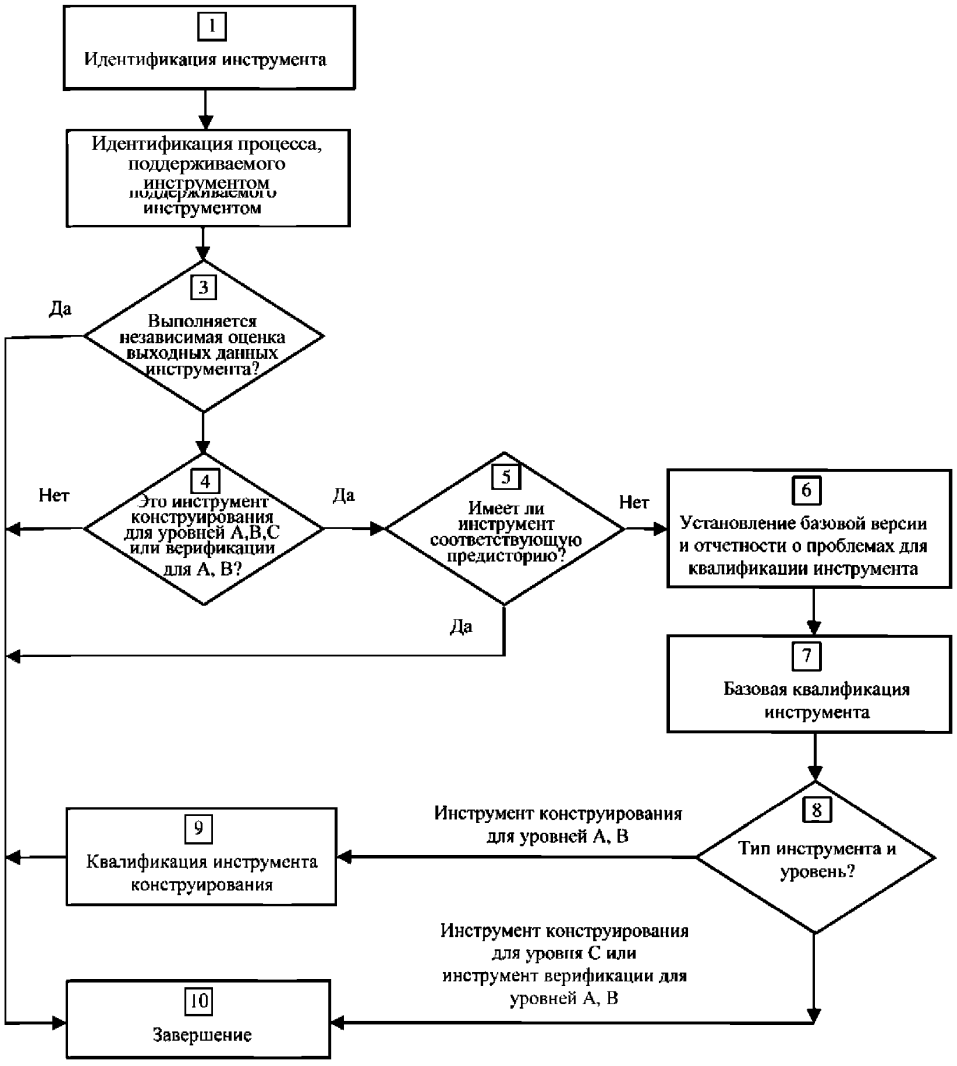

Рисунок 11-1. Квалификация и оценка инструмента конструирования и верификации

1. Идентификация инструмента. Включает название, источник, номер версии и необходимую для его работы операционную среду. Модернизация инструмента должна быть документирована и отслежена.

Примечание. *При модернизации инструмента оцените потенциальное влияние модернизации на существующие результаты и на оставшийся жизненный цикл аппаратуры.*

2. Идентификация процесса, поддерживаемого инструментом. Определение процесса конструирования или верификации, который поддерживается инструментом, любых соответствующих ограничений инструмента и его выходных данных для использования в жизненном цикле конструирования аппаратуры. Если известно, что с инструментом существуют определенные проблемы, то излагается приемлемость использования инструмента и обоснование.

3. Выполняется независимая оценка выходных данных инструмента? Независимая оценка проверяет правильность выходных данных инструмента, используя независимые средства. Если выходные данные инструмента оценены независимо, то оценки инструмента не требуется.

Примечание. *Независимая оценка выходных данных инструмента конструирования, которые формируются целиком или по частям, может устанавливаться в результате верификации, выполненной на элементе, таком, как компонент, сборка или устройство. В этом случае целостность конечного элемента не зависит от правильности только самих выходных данных инструмента конструирования.*

Независимая оценка выходных данных инструмента верификации может включать рассмотрение вручную выходных данных инструмента или может включать сравнение выходных данных другого средства, способного выполнять то же самое мероприятие верификации, что и оцениваемое средство.

Заявитель может также предлагать другие методы независимой оценки.

4. Это инструмент конструирования уровней A, B или C или верификации уровня A или B? Если инструмент используется для функций уровня D, или используется для верификации функций уровня C, или используется для оценки завершения верификационных испытаний, как в элементном анализе, описанном в подразделе 3.3.1.1.2 Приложения B, то никакой другой оценки не требуется. Если инструмент используется как инструмент конструирования аппаратуры, реализующей функции на уровне A, B или C или используется как инструмент верификации аппаратуры, реализующей функции уровня A или B, тогда дальнейшая оценка необходима.

5. Имеет ли инструмент соответствующую предысторию? Когда можно показать, что инструмент был предварительно использован и дал положительные результаты, тогда дальнейшая оценка не требуется. Обсуждение соответствия предыдущего применения средства относительно предлагаемого применения средства должно быть включено в обоснование.

Примечание. *Предыстория инструмента может быть основана или на бортовом или на небортовом применении, при условии, что данные показывают соответствие и пригодность предыстории инструмента.*

6. Установление базовой версии и отчетности о проблемах для квалификации инструмента. Установление базовой версии для управления конфигурацией инструмента и отчета о проблемах инструмента, чтобы подготовить инструмент к квалификации.

7. Базовая квалификация инструмента. Установление и выполнение плана для подтверждения того, что инструмент создает правильные выходные данные для предназначенного применения, используя анализ или испытания. Для составления требований может использоваться Руководство пользователя инструмента или другое описание функций и применения инструмента.

8. Тип инструмента и уровень? Является ли рассматриваемый инструмент инструментом конструирования аппаратуры уровня A или B, или инструментом конструирования аппаратуры уровня C или инструментом верификации аппаратуры уровня A или B?

9. Квалификация инструмента конструирования. Квалифицируйте инструмент конструирования уровня A или B, используя стратегии, описанные в Приложении B данного документа, руководство по квалификации инструмента в КТ-178B для средств разработки ПО или другие методы, приемлемые для сертифицирующего органа. Должна быть установлена независимость этого мероприятия от разработки инструмента.

Примечание. *Специальное руководство для квалификации инструмента конструирования уровня A и B здесь не приводится из-за разных обстоятельств применения инструмента, используемой технологии, очевидности реализации инструментов и данных жизненного цикла и других факторов. Использование подобного инструмента конструирования без независимой оценки выходных данных инструмента или установления соответствующей предыстории не рекомендуется, т.к. это может оказаться задачей такой же сложности, как и конструирование аппаратуры, для которой предназначено использование данного инструмента.*

10. Завершение. Документируйте оценку инструмента, обоснование решений по оценке и, если применяется, данные квалификации инструмента. Обеспечьте специальные указания об инструкциях по установке, руководствах пользователя и данных квалификации инструмента, необходимых для обеспечения квалификации и оценки инструмента.

11.4.2. Данные квалификации и оценки инструмента

Данные квалификации и оценки инструмента должны включать:

1. Определение инструмента, процесса, который он обеспечивает, а также, если применимо, следующих пунктов:
   a. Обоснование и результаты независимой оценки по п. 3 рисунка 11-1.
   b. Обозначение инструмента по п. 4 рисунка11-1.
   c. Предысторию инструмента для выполнения п. 5 рисунка 11-1. Обсуждение соответствия предыдущего использования инструмента предлагаемому применению инструмента должно быть включено в обоснование.
2. Однозначное определение конфигурации, которая используется в квалификации инструмента, в соответствии с п. 6 рисунка 11-1 и обоснование применимости испытанной конфигурации, если она отличается от той, что реально используется для конструирования или проверки конечного элемента аппаратуры.
3. Детали квалификации инструмента, включая требования, используемые при испытаниях, процедуры испытаний, предполагаемые результаты, процедуры анализа, используемые для интерпретации и представления результатов испытаний, и того, как устанавливается независимость.
4. План для квалификации инструмента конструирования, включая применяемые процедуры и результаты любых мероприятий, идентифицированные в плане.
5. Определение известных ошибок инструмента, включая метод компенсации ошибок, и, когда приемлемо, сообщений о проблеме как результат квалификации инструмента.

ПРИЛОЖЕНИЯ

ПРИЛОЖЕНИЕ А

Изменение данных жизненного цикла аппаратуры в зависимости от уровня гарантии конструирования аппаратуры

Данное приложение обеспечивает руководство по изменению данных жизненного цикла конструирования аппаратуры в зависимости от уровня гарантии конструирования аппаратуры. Оно также обеспечивает руководство, связанное с требованиями к независимости во время процесса верификации.

В таблице А-1 определена классификация представленных данных и категории контроля аппаратуры в процессе управления конфигурацией для каждого элемента данных со ссылкой на таблицу 7-1.

По признаку представления определены два типа данных:

1. Представляемые. Данные должны быть представлены сертифицирующему органу.
2. Непредставляемые. Данные не требуются.

Вся верификация функций уровня А и В должна быть независимой. Функции уровня С и ниже не требуют независимой верификации. Независимость необходима только на уровне иерархии конструирования, на котором проект верифицируется на соответствие требованиям. Должны быть доступны эквивалентные средства независимости, которые учитывают отказ общего режима.

Независимость – это способ рассмотрения ошибок общего режима, которые могут наблюдаться, когда разработчик проверяет, что разрабатываемый элемент аппаратуры действует как сконструировано, а не как требуется. В этой связи ответственность за обеспечение процесса верификации совместима с демонстрацией того, что требования к проекту были выполнены индивидуально, с помощью независимого от разработчика инструмента или процесса. Существует много средств установления независимости, и план верификации должен описывать специальные средства, которые следует использовать для конкретного мероприятия верификации.

Некоторыми приемлемыми методами являются:

1. Требования или проекты рассматриваются другим лицом.
2. Контрольные примеры и процедуры разрабатываются другим лицом.
3. Контрольные примеры и процедуры, разработанные проектировщиком, рассматриваются другим лицом.
4. Анализ, выполненный разработчиком, рассматривается другим лицом или группой лиц.
5. Различные испытания, которые подтверждают результаты испытаний, выполненных разработчиком. Например, испытания во время летных испытаний подтверждают испытания элемента аппаратуры или испытания верификации ПО, разработанные независимо и выполненные на определенном элементе аппаратуры.
6. Испытания или результаты анализа проверяются с помощью инструмента.

Примечания: 1. *Часто проверочные испытания автоматизируются и требуют только «нажатия клавиши» для их выполнения. Целью независимости не является требование того, чтобы кто-нибудь другой, кроме разработчика, выполнял испытания, поскольку они оценены или разработаны независимо. Может потребоваться независимое рассмотрение для подтверждения использования правильных процедур и проверки соответствия поставленным требованиям.*

2. *Для достижения независимости не требуется создание отдельной организационной структуры.*

Номера в скобках в таблице А-1 соответствуют примечаниям за таблицей.

Таблица А-1. Данные жизненного цикла аппаратуры по уровню гарантии конструирования аппаратуры и категориям контроля аппаратуры

Подраздел	Данные жизненного цикла аппаратуры ([1])	Цели ([2])	Поставка	Уровень A	Уровень B	Уровень C	Уровень D
10.1	Планы аппаратуры						
10.1.1	План сертификации аппаратуры	4.1(1, 2, 3, 4)	S	HC1	HC1	HC1	HC1
10.1.2	План конструирования аппаратуры	4.1(1, 2, 3, 4)		HC2	HC2	HC2	NA
10.1.3	План обоснования аппаратуры ([3]) ([4])	4.1(1, 2, 3, 4); 6.1.1(1)		HC2	HC2	HC2	NA
10.1.4	План верификации аппаратуры	4.1(1, 2, 3, 4); 6.2.1(1)	S	HC2	HC2	HC2	HC2
10.1.5	План управления конфигурацией аппаратуры	4.1(1, 2, 3, 4); 7.1(3)		HC1	HC1	HC2	HC2
10.1.6	План процесса гарантии аппаратуры	4.1(1, 2, 4); 8.1(1, 2, 3)		HC2	HC2	NA	NA
10.2	Стандарты и руководства по конструированию аппаратуры						
10.2.1	Стандарты на требования ([3])	4.1(2)		HC2	HC2	NA	NA
10.2.2	Стандарты на конструирование аппаратуры ([3])	4.1(2)		HC2	HC2	NA	NA
10.2.3	Стандарты на обоснование и верификацию аппаратуры ([3])	4.1(2)		HC2	HC2	NA	NA
10.2.4	Стандарты на архивирование аппаратуры ([3])	4.1(2)		HC2	HC2	NA	NA
10.3	Данные конструирования аппаратуры						
10.3.1	Требования к аппаратуре	5.1.1(1, 2); 5.2.1(2); 5.3.1(2); 5.4.1(3); 5.5.1(1, 2, 3); 6.1.1(1, 2); 6.2.1(1)		HC1	HC1	HC1	HC1
10.3.2	Конструкторские документы аппаратуры						
10.3.2.1	Данные эскизного проектирования ([3])	5.2.1(1)		HC2	HC2	NA	NA
10.3.2.2	Данные технического проектирования	5.3.1(1); 5.4.1(2)		([5])	([5])	([5])	([5])
10.3.2.2.1	Чертеж общего вида	5.3.1(1); 5.4.1(2); 5.5.1(1)	S	HC1	HC1	HC1	HC1
10.3.2.2.2	Сборочные чертежи	5.3.1(1); 5.4.1(2); 5.5.1(1)		HC1	HC1	HC1	HC1
10.3.2.2.3	Монтажные чертежи	5.4.1(2); 5.5.1(1)		HC1	HC1	HC1	HC1
10.3.2.2.4	Данные интерфейса аппаратура/ПО ([3])	5.3.1(1); 5.5.1(1)		HC1	HC1	HC1	HC1
10.4	Данные обоснования и верификации						
10.4.1	Данные трассируемости аппаратуры	6.1.1(1); 6.2.1(1, 2)		HC2	HC2	HC2 ([6])	HC2 ([6])
10.4.2	Процедуры рассмотрений и анализов аппаратуры ([3])	6.1.1(1, 2); 6.2.1(1)		HC1	HC1	NA	NA
10.4.3	Результаты рассмотрений и анализов аппаратуры ([3])	6.1.1(1, 2); 6.2.1(1)		HC2	HC2	HC2	HC2
10.4.4	Процедуры испытаний аппаратуры ([3])	6.1.1(1, 2); 6.2.1(1)		HC1	HC1	HC2	HC2 ([7])
10.4.5	Результаты испытаний аппаратуры ([3])	6.1.1(1, 2); 6.2.1(1)		HC2	HC2	HC2	HC2 ([7])
10.5	Критерии приемочных испытаний аппаратуры	5.5.1(3); 6.2.1(3)		HC2	HC2	HC2	HC2
10.6	Сообщения о проблемах	5.1.1(3); 5.2.1(3); 5.3.1(3); 5.4.1(4); 5.5.1(4); 6.1.1(3); 6.2.1(4); 7.1(3)		HC2	HC2	HC2	HC2
10.7	Протоколы управления конфигурацией аппаратуры	5.5.1(1); 7.1(1, 2, 3)		HC2	HC2	HC2	HC2
10.8	Протоколы процесса гарантии аппаратуры	7.1(2); 8.1(1, 2, 3)		HC2	HC2	HC2	NA
10.9	Итоговое заключение об аппаратуре	8.1(1, 2, 3)	S	HC1	HC1	HC1	HC1

NA – не применяется.

([1]). Данные должны быть представлены, если в графе «Поставка» указана буква S. Данные HC1 и HC2, используемые для сертификации, которые не требует представления, должны быть доступны. См. подраздел 7.3.

([2]). Цели, перечисленные здесь, используются только для ссылки. Не все цели могут применяться ко всем уровням гарантии.

([3]). Если эти данные используются для сертификации, тогда их наличие показано в таблице. Эти данные не всегда используются для сертификации и могут не потребоваться.

([4]). Это может быть выполнено неформально через процесс сертификационного взаимодействия для уровней C и D. Документация может быть в форме протоколов совещания и/или материалов представления.

([5]). Если заявитель соглашается на эти данные как на представляемые данные, они должны быть доступны.

([6]). Необходимы только данные трассируемости требований к испытаниям.

([7]). Испытания покрытия производных требований или требований более низкого иерархического уровня не требуется.

ПРИЛОЖЕНИЕ В

Указания по гарантии конструирования для функций уровней А и В

1. Введение

Разработчик аппаратуры, реализующий функции уровней А и В, принимает решения, которые могут сказаться на безопасности. По мере возрастания уровня гарантии конструирования, для проверки того, что данный проект соответствует его требованиям безопасности, могут потребоваться перекрестные, многослойные комбинации методов гарантии конструирования аппаратуры. Заявителю следует выбрать один или более из таких методов или предложить другой.

Данное приложение обеспечивает разработчика руководством как выполнить и применить FFPA для создания стратегии гарантии конструирования, а также по некоторым специальным методам, которые можно применять для гарантии конструирования.

2. Анализ тракта функционального отказа

Анализ тракта функционального отказа – это структурированный итеративный анализ сверху вниз. Он определяет специфические части конструкции, которые реализуют функцию, т.е. устройство, компоненты и элементы, связанные с каждым трактом, и далее анализируются соответствующие отказные состояния и последствия для определения того, насколько архитектура аппаратуры и ее реализация соответствуют требованиям безопасности. FFPA определяет также те устройства, компоненты и элементы конструкции, которые реализуют функции уровней А и В.

FFPA начинается с предварительной оценки безопасности системы, используемой для определения трактов функциональных отказов на уровне системы, которые могут быть разложены на и распределены по трактам функциональных отказов аппаратуры.

Целью FFPA является определение отдельных трактов функциональных отказов, так что:

1. Аппаратура, реализующая функции уровней А и В, может быть рассмотрена в соответствующем методе гарантии конструирования, описанном в данном Приложении или в другом приемлемом для сертифицирующего органа перспективном методе.
2. Положения данного Приложения являются необязательными для реализации функций аппаратуры уровня С или более низких уровней, а именно тех функций, которые будут гарантированы при использовании только инструкций разделов с 3 по 11 данного документа.

Примечание. *Идентификация отдельных трактов функционального отказа для функций, реализованных в различных технологиях или предлагающих различные степени прозрачности проекта, часто очень полезна, т.к. общая гарантия конструирования элемента аппаратуры может быть достигнута при использовании многочисленных методов гарантии конструирования. Уровень декомпозиции может изменяться для каждого тракта функционального отказа.*

Декомпозиция выполняется, при использовании методов оценки безопасности сверху вниз, таких, как Анализ дерева неисправности. Декомпозиция может быть выполнена, используя Анализ видов и последствий отказа, Анализ логической схемы и Анализ общего режима для каждого последующего уровня декомпозиции. Уровень декомпозиции может изменяться для каждого тракта функционального отказа уровня системы в зависимости от стратегии гарантии конструирования, соответствующей концепции реализации и методов ослабления влияния ошибок, которые предлагаются для разрабатываемой аппаратуры. Декомпозиция проводится:

- из FFPs на уровне системы в FFPs на уровне аппаратуры;
- из FFPs на уровне аппаратуры в FFPs на уровне схемы (контура, цепи);
- из FFPs на уровне схемы в FFPs на уровне компонента;
- из FFPs на уровне компонента в FFPs элементного уровня

2.1. Метод анализа тракта функционального отказа

FFPA должен выполняться следующим образом:

1. Для каждой функции уровней A и B выполняется идентификация функции и ее уровня гарантии конструирования, основываясь на требованиях к аппаратуре и FHA системы для этой функции. Функция может быть образована как совокупность подфункций, каждая из которых имеет соответствующий набор производных требований и соответствующий уровень гарантии конструирования. Эти подфункции могут быть разложены и дальше, если необходимо.
2. Для каждой функции уровней A и B определяются средства реализации функции или подфункций и анализируются варианты гарантии конструирования. Данные гарантии, имеющиеся в наличии, или которые будут получены для исполнения функции или подфункции, должны быть полными и приемлемыми для выбранных стратегии или стратегий гарантии конструирования. Если данные гарантии полные, правильные и приемлемые, тогда дальнейшая декомпозиция не требуется.
3. Для трактов функционального отказа других уровней должны быть оценены их взаимосвязи с трактами функционального отказа уровней A или B, используя Анализ видов и последствий отказа, Анализ общего режима или Анализ логической схемы – для гарантии того, чтобы на тракты функционального отказа уровней A и B не могли неблагоприятно влиять тракты функционального отказа не уровня A или B.

Этот процесс оценки является итеративным. Если не существует приемлемого метода гарантии конструирования для тракта функционального отказа, процесс оценки и декомпозиции повторяется или архитектура и реализация функции аппаратуры изменяются, пока не будет определен подходящий метод гарантии конструирования и получены, или могут быть получены, подходящие данные гарантии для каждого тракта функционального отказа уровней A и B.

Результаты FFPA и выбранные методы, используемые для гарантии конструирования аппаратуры, связываются с процессами систем самолета, как описано в подразделе 2.1 данного документа. Эти результаты используются для проверки того, что допущения на уровне самолета, особенно те, которые связаны с многократным перекрестным использованием системы и аналогичных элементов аппаратуры, все еще достоверны.

2.2. Данные анализа тракта функционального отказа

Данные FFPA должны:

1. Определять аномалии поведения и функциональные отказы, которые были делегированы элементу аппаратуры с системного уровня.
2. Определять тракты функциональных отказов, последствия их аномального поведения или функционального отказа, уровень декомпозиции в иерархии проекта, до которого был выполнен анализ, тип и местонахождение приемлемых данных гарантии, которые должны быть доступны.
3. Описывать взаимосвязи между трактами функциональных отказов для определения их независимости от других трактов функциональных отказов и компонентов. Такие взаимосвязи могут быть описаны с использованием качественного FHA или других нисходящих анализов, таких, как Анализ общего режима, Анализ видов и последствий отказа или Анализ логических схем. Описание взаимосвязей должно определять такие взаимовлияющие тракты, компоненты и их зависимости.
4. Показывать трассировку трактов функциональных отказов к требованиям к аппаратуре и производным требованиям.

3. Методы гарантии конструирования для функций уровней A и B

Задачей данного приложения не является ограничение реализации гарантии конструирования только применением любого существующего или будущего метода. Обсуждаемые в данном приложении методы могут использоваться для удовлетворения одной или более целей процессов, описанных в данном документе в разделах с 4 по 6.

3.1. Архитектурное ослабление

Архитектурные особенности конструирования, такие, как разнородная реализация, резервирование, контроль, изоляция, обособление и ограничение команд/влияния могут быть специально использованы для ослабления или сдерживания неблагоприятных эффектов от ошибок конструирования и реализации аппаратуры. Как часть Предварительной оценки безопасности системы такие мероприятия, как количественный Анализ дерева неисправности и Анализ общего режима, могут обеспечить гарантию при определении сферы архитектурных параметров, необходимых для ослабления или сдерживания воздействия отказов аппаратуры, неисправностей и ошибок конструирования и реализации. Более специфически, данный подход должен применяться совместно с подходом FFPA для аппаратуры, как описано в разделе 2 выше, и должен использовать процесс Анализа общего режима для определения применимости конкретных стратегий ослабления для покрытия ошибок конструирования и реализации аппаратуры. Например, резервирование обычно помогает в области случайных ошибок и неисправностей, но резервирование также может быть эффективно использовано для ослабления ошибок конструирования и реализации, если рассмотрены аспекты общего режима для таких ошибок.

3.1.1. Метод архитектурного ослабления

Архитектурное ослабление выполняется путем определения трактов функционального отказа, связанных с предложенной реализацией аппаратуры, с последующим анализом вариантов конструкции и предложением характеристик аппаратуры и стратегий, которые ослабляют воздействия в этих трактах функционального отказа. Должны быть рассмотрены и оценены суммарные эффекты от предложенной архитектуры в отношении ослабления всех соответствующих воздействий трактов функционального отказа. Введение стратегии архитектурного ослабления также вводит некоторые производные требования, на соответствие которым должна быть проверена реализация этих требований. В частности, архитектурные особенности должны защищать от некоторых или от всех неблагоприятных воздействий идентифицированных трактов функционального отказа и должны быть оценены на предмет внесения дополнительных трактов отказов, к которым следует применить иные архитектурные ослабления или другие стратегии гарантии конструирования, описанные в данном Приложении.

3.1.2. Разрешение вопросов архитектурного ослабления

В процессе оценки безопасности определяется допустимость архитектурного ослабления. FFPA должен в первую очередь определить все тракты функционального отказа аппаратуры уровней A и B, где архитектурное ослабление может быть полезным, и должен определить используемые методы и рациональность ослабления. Адекватность определяется с помощью оценки каждой функции, поддерживающей ослабление в контексте общего архитектурного подхода, который может быть включен в более или менее сложные составляющие стратегий архитектурного ослабления.

Анализ общего режима должен рассматривать потенциальные ошибки для общего режима в требованиях, реализации, изготовлении и техобслуживании, которые могут аннулировать архитектурное ослабление. Разработчик должен также рассмотреть потенциальные случайные отказы аппаратуры, формирующей функции архитектурного ослабления, которые могут вызвать потерю ослабления. Вероятностная доступность функций, поддерживающих ослабление, должна быть соизмерима с последствиями потери ослабления, что может привести к сужению границ безопасности.

Общий подход должен гарантировать, что были достигнуты и поддерживаются правильность работы и допустимая независимость между необходимыми функциями. Любые специальные защитные средства, необходимые для ограничения, локализации или связывания остаточных последствий в общем режиме, должны быть выявлены и внедрены либо в форме дополнительного архитектурного ослабления, либо с другими стратегиями гарантии, изложенными в этом Приложении.

Когда архитектурное определение завершено, тракты функционального отказа функций аппаратуры уровней A и B, определенные как неослабленные или неадекватно ослабленные, должны быть пересмотрены с использованием других методов гарантии конструирования из данного Приложения. Например, частичное архитектурное ослабление отдельных схем и ком-

понентов может использоваться вместе со специальным методом анализа безопасности, когда анализ применяется для определения и обеспечения проверки для неослабляемых частей применяемых схем и компонентов.

3.1.3. Данные архитектурного ослабления

Документация на средства архитектурного ослабления, применяемые для защиты трактов функционального отказа уровней А и В в аппаратуре, должна быть представлена в форме данных оценки безопасности, данных по требованиям безопасности и данных трассирования. Данные оценки безопасности должны основываться на оценке трактов функционального отказа аппаратуры и анализе общего режима, специально относящихся к аспектам архитектурного ослабления конструкции аппаратуры.

Данные архитектурного ослабления должны включать:

1. Определение трактов функционального отказа аппаратуры уровней А и В, которые должны быть защищены с помощью архитектурных средств.
2. Описание архитектурного подхода и обоснование покрытия, обеспечиваемого данным подходом.
3. Целесообразность границ общего режима и аспектов конструирования общего режима, применимых к аппаратуре.
4. Определение неослабленных или неадекватно ослабленных трактов функционального отказа уровней А и В, которые должны быть адресованы к другими методам гарантии конструирования.
5. Требования к функциональной работе и необходимые проектные параметры механизмов архитектурного ослабления.
6. Механизмы ослабления, используемые для выполнения требований безопасности аппаратуры, которые содержат ПО, такие, как обособление ПО, контроль безопасности и несхожее ПО. Эти механизмы и требования к безопасности ПО должны быть предоставлены для системного процесса и для процесса разработки ПО.
7. Традиционные данные об интенсивности отказов и данные времени воздействия скрытого отказа для любой аппаратуры, которая выполняет прикладное архитектурное ослабление.
8. Данные трассирования, связанные с требованиями безопасности, применяемыми к данным оценки безопасности и данным верификации проекта.

3.2. Опыт эксплуатации изделия

В подразделе 11.3 дано основное руководство по оценке данных опыта эксплуатации системы для применения в бортовой аппаратуре. Для функций уровней А и В, которые используют ранее разработанную аппаратуру как часть конструкции, необходима дополнительная гарантия конструирования. Эта гарантия может быть обеспечена следующим образом.

3.2.1. Метод опыта эксплуатации изделия

После завершения оценки по подразделу 11.3 тракты функционального отказа, которые реализуются рассматриваемой аппаратурой, должны быть проанализированы относительно любого применимого опыта эксплуатации. Заявитель или разработчик должен определить данные опыта эксплуатации и установить, что эти данные демонстрируют, что повторно используемая функциональность аппаратуры имела удовлетворительный опыт во время предыдущего использования аппаратуры.

3.2.2. Разрешение вопросов опыта эксплуатации изделия

Когда анализ данных опыта эксплуатации изделия завершен, тракты функционального отказа функций аппаратуры уровней А и В, которые определены как неосуществленные, неадекватно осуществленные или для которых нет опыта обслуживания при эксплуатации, должны

быть рассмотрены с использованием другого метода гарантии конструирования или с помощью определения дополнительной верификации, которая может быть применена для проверки функций.

3.2.3. Данные опыта эксплуатации изделия

Данные опыта эксплуатации изделия, применяемые для защиты трактов функционального отказа уровней А и В аппаратуры должны включать:

1. Данные оценки опыта эксплуатации изделия из подраздела 11.3.2.
2. Определение трактов функционального отказа, для которых гарантия конструирования достигнута с помощью опыта эксплуатации и подтверждением обоснованности данных опыта эксплуатации.
3. Определение трактов функционального отказа, для которых данные опыта эксплуатации являются неудовлетворительными, и определение условий испытаний, процедур испытаний, анализов и результатов, используемых для полноты гарантии конструирования трактов функционального отказа.
4. Определение трактов функционального отказа и условий эксплуатации, не продемонстрированных опытом эксплуатации, которые потребуют дополнительного архитектурного ослабления или перспективного метода верификации.
5. Данные трассировки из подраздела 10.4.1, показывающие точную взаимосвязь данных опыта эксплуатации и верификации, которые обеспечивают покрытие гарантии конструирования каждого тракта функционального отказа.

3.3. Перспективные методы верификации

Дополнительное подтверждение гарантии конструирования может быть достигнуто, и очевидность этого доказана такими методами проверки, как Элементный анализ, Формальные методы, Специальный анализ безопасности для верификации, или другими предлагаемыми заявителем и принятыми сертифицирующим органом методами.

Перспективные методы верификации гарантии конструирования используют и расширяют метод FFPA, представленный в разделе 2 настоящего Приложения. Метод FFPA применяется на уровне оборудования, на уровне схемы, на уровне компонента для определения реализации в аппаратуре трактов функционального отказа уровней А и В. Данные анализа FFPA затем используются для определения предлагаемых средств гарантии конструирования, применяемых к схемам аппаратуры, компонентам и элементам, содержащимся в этих трактах функционального отказа уровней А и В.

Эти три метода кратко изложены ниже и описаны в следующих разделах:

1. Элементный анализ. Элементный анализ обеспечивает измерение полноты проверки аппаратуры с перспективой снизу вверх. Каждый функциональный элемент в тракте функционального отказа определяется и верифицируется с использованием контрольных примеров, которые соответствуют целям верификации подраздела 6.1. Анализ может также определить проблемные области, которые необходимо рассмотреть с помощью других соответствующих средств.
2. Специальный анализ безопасности. Стратегия фокусируется на выявлении и исправлении ошибок конструирования, которые могут неблагоприятно повлиять на выходные данные аппаратуры с точки зрения безопасности системы. Аналитически определяются чувствительные к безопасности части входного пространства и выходного пространства аппаратуры. Чувствительные части входного пространства аппаратуры моделируются, а выходное пространство наблюдается не только с точки зрения верификации требований, чувствительных по безопасности функций, но также аномалий поведения. Методы наблюдения выходного пространства определяются заранее с помощью анализа, который выполняется с использованием традиционных методов анализа безопасности.
3. Формальные методы. В формальных методах применяются методы формальной логики и дискретной математики для спецификации, конструирования и проверки компьютерных систем. Эти методы могут использоваться в различных процессах жизненного цикла конструирования аппаратуры для доказательства обоснованности применения.

Заявителем могут быть предложены другие перспективные методы верификации, отличные от тех, которые описаны в данном подразделе.

3.3.1. Элементный анализ

Элементный анализ может использоваться для демонстрации того, что тракты функционального отказа верифицированы с помощью соответствующих контрольных примеров. Элементный анализ обеспечивает достоверность и очевидность того, что ошибки конструирования устранены путем разделения сложной реализации тракта функционального отказа на элементы на том уровне, на котором они были созданы разработчиком. Данный метод анализа обеспечивает измерение процесса верификации с целью определения полноты и содержания верификации и наиболее подходит для применения тогда, когда технический проект очевиден и находится под управлением конфигурацией. Это может относиться к схемам ASIC и PLD, в которых функции рассматриваются на том же самом уровне гарантии конструирования, или там, где функции различных уровней гарантии конструирования изолированы или сегментированы. Каждый функциональный элемент прикладных схем или компонентов определяется и проверяется на правильность предназначенной функции с использованием процедур верификации, которые обеспечивают выполнение целей верификации подраздела 6.1. Элементный анализ обычно применяется ко всему компоненту или устройству независимо от количества проверенных трактов функционального отказа, которые в нем реализованы, но может быть также применен к части компонента или устройства, если обеспечено обоснование изоляции, независимости или разделения различных трактов функционального отказа.

Примечание. *Когда элементный анализ выполняется на функции, применяемой в устройстве PLD, необходимо рассмотреть программируемое содержание и применение характеристик PLD, а непрограммируемые компоненты могут рассматриваться, используя отдельный метод, например предшествующий опыт эксплуатации.*

В анализе определяются области интереса, к которым необходимо обратиться с помощью соответствующих средств. Процесс верификации без подобного анализа может привести к неадекватному контролю схем. Исторически подобные неадекватности происходили из-за недостатков в процедурах испытаний на основе требований, неточных или неполных требований к аппаратуре, неиспользуемых схем, инициализации схем или библиотечных функций. Данный анализ обеспечивает верификацию элементов в представляющих интерес трактах функционального отказа и определяет полноту верификации каждого элемента. Определение того, что верификация для элементов неполная, указывает на необходимость дополнительных верификации проверки или соответствующих мероприятий.

Заявитель должен определить уровни в иерархии проекта, на которых определены элементы, и как они должны быть проанализированы для полноты верификации.

3.3.1.1. Метод элементного анализа

Метод элементного анализа начинается с определения набора критериев, которые должны использоваться при анализе, с учетом уровня гарантии конструирования аппаратуры, технологий аппаратуры и доступности деталей реализованной аппаратуры.

Критерии должны включать:

1. Выявление и определение элементов на соответствующем уровне конструкции аппаратуры.

2. Верификационное покрытие для каждого элемента, который необходимо проверить.

Эти критерии затем применяются в анализе верификационных мероприятий для определения, смогут ли критерии полноты верификации быть достигнуты при запланированной верификации. Если критерии не будут достигнуты, тогда каждый проверяемый элемент должен быть испытан соответствующим набором стимулов и должен вызвать соответствующие наблюдаемые отклики на контролируемые в процессе испытания сигналы.

Примечание. *Поскольку данный процесс проверяет испытания самой аппаратуры, он может выявить недостатки в испытательных процедурах. Рассматривая*

недостатки испытаний, необходимо обеспечить дополнительную достоверность и очевидность того, что испытания прошли удовлетворительно и что выполнение новых или предлагаемых контрольных примеров может затем выявить ошибки в аппаратуре.

3.3.1.1.1. Выбор критериев элементного анализа

Применяемые критерии элементного анализа должны выбираться на индивидуальной основе, в зависимости от типа и сложности элемента аппаратуры и определяемых функциональных операций элемента. Анализ может продемонстрировать, что либо все примитивные блоки низкого уровня, типа счетчиков, регистраторов, мультиплексоров и фильтров, были адекватно испытаны, либо все группы соединенных между собой примитивных блоков были адекватно испытаны и критерии полноты верификации достигнуты. Критерии анализа процедур испытаний должны быть получены на основе оценки функциональной работы элемента и его интеграции с другими элементами аппаратуры для этого, в обеспечение выполнения функции аппаратуры следующего, более высокого, иерархического уровня.

***Примечание 1**. Например, если элемент – это счетчик по модулю N, используемый как временная задержка, то в процедурах испытаний могут применяться выборки из классов эквивалентности входных данных – для проверки того, что он выполняет счет, когда включен, останавливает счет, когда выключен, считает с нужной частотой, достигает величины N и сбрасывает это значение в установленное время. Нет необходимости показывать, что в процедурах испытаний проверяются отдельные вентили или триггеры, которые вместе образуют счетчик.*

Примером использования соединения примитивных блоков в качестве элемента может служить арифметическое логическое устройство, созданное из таких примитивных блоков, как регистры, сумматоры и логика управления. Это устройство может быть смоделировано – для показа того, что примитивные блоки вместе образуют арифметическое логическое устройство, но процедуры верификации, применяемые в элементном анализе, должны использовать входные данные соответствующего класса эквивалентности, чтобы показать, что это устройство выполняет свои функции.

Не требуется определение элементов на уровне конструкции ниже установленного разработчиком аппаратуры. Анализ на уровне вентиля может быть пригоден, только если конструкция недвусмысленно рассматривается как вентили управления в форме комбинационной логики или конечного автомата.

***Примечание 2.** Анализ реализации более низкого уровня, чем установленный разработчиком, например на уровне вентиля или транзистора, не требуется, так как он будет аналогичен анализу ПО на языке ассемблера или на уровне двоичного кода. Эти более низкие уровни абстракции неявно рассматриваются при выполнении элементного анализа верификационных испытаний, выполняемых на аппаратуре или на послекомпоновочных имитаторах, успешно оцененных и, если необходимо, квалифицированных как инструменты верификации в соответствии с подразделом 11.4.*

Схемы ASIC или устройства PLD могут содержать соответствующие библиотечные функции, которые не обеспечивают видимость их внутренней конструкции и, следовательно, не могут быть пригодны для анализа, выполняемого вручную. Библиотечные функции могут рассматриваться как элементы COTS в элементном анализе с аспектами аппаратуры COTS, определенными в подразделе 11.2 и подразделе 2.2 Приложения В. Верификация применения библиотечной функции должна показать, что она соответствует своей спецификации или своему описанию, которые подготовлены изготовителем библиотеки, и что испытания должны выполняться в окружении, которое позволяет наблюдать результаты испытаний.

***Примечание 3.** Препятствовать применению библиотек конструкций с целью создания новых функций не входит в намерение данного документа. Практическое использование библиотек предназначено для минимизации вероятности внесения ошибок в аппаратуру.*

Для схем ASIC и PLD, синтезированных на основе описания на языке высокого уровня, критерии анализа могут базироваться на представляющем аппаратуру языке описания поведения высокого уровня. Однако, поскольку реализации, синтезированные из описаний языка высокого уровня, могут включать параллельные логические структуры и непоследовательные временные аспекты, то синтезированные выходные данные должны быть включены в анализ определения завершенности. Должен также быть оценен и синтезатор.

3.3.1.1.2. Выполнение элементного анализа

Элементный анализ должен использовать основанные на требованиях верификационные испытания, выполненные в одной (или более) из следующих сред испытаний:

1. Испытания схемы, реализующей функциональный канал, установленной в целевом сборочном узле.
2. Испытания, выполненные на автономном прототипе. Такие испытания типичны для схем ASIC и устройств PLD.
3. Приемочные испытания в процессе производства.

Примечание. *Поскольку испытания в процессе производства часто не основываются на требованиях, приемочные испытания готовых изделий могут быть ограничены по своей применимости в элементном анализе.*

4. Послекомпоновочная имитация, обычно для ASIC и PLD, которая оценивается и, если необходимо, квалифицируется для применения в качестве инструмента верификации, как описано в подразделе 11.4.

Сам элементный анализ может быть выполнен с применением имитации для определения достигнутой полноты, подтверждая, что проанализированные процедуры испытаний могут быть связаны с применяемыми критериями элементного анализа и теми, которые используются для функционального верификационного зачета аппаратуры в соответствии с целями раздела 6. Если проанализированные процедуры испытания получены на основе внутрисхемных испытаний аппаратуры или автономного прототипа и проводятся с использованием имитации, то входные испытательные сигналы возбуждения и предполагаемые результаты могут быть преобразованы для использования имитирующего устройства – при условии, что процесс преобразования проверяется на точность, как часть элементного анализа. Имитатор, используемый для выполнения элементного анализа, должен показать способность правильно определять, соответствует ли критериям анализа каждый тип элемента, введенного в реализацию.

3.3.1.2. Разрешение вопросов в результатах элементного анализа

Элементный анализ может выявить непроверенные элементы аппаратуры, указывая или на необходимость дополнительных мероприятий верификации, или, возможно, на необходимость устранить неиспытанные элементы или ослабить любое аномальное поведение, которое может быть результатом архитектурных особенностей. Неиспытанные элементы аппаратуры могут быть результатом следующего:

1. Недостатки в контрольных примерах или процедурах верификации. Недостатки могут возникнуть, если контрольные примеры просто не испытывают элементы изделия в соответствии с критериями подразделе 3.3.1.1 Приложения В. Они могут также возникнуть, если имеются «неосторожности» в функциональных требованиях, но элемент аппаратуры был соответствующим образом сконструирован для создания повторяемых характеристик. В этих условиях процедуры и контрольные примеры испытаний должны быть дополнены или изменены. Более того, необходимо оценить возможности испытаний проверить соответствующие требования.
2. Неадекватность требований. Требования должны быть уточнены, или дополнительно определены производные требования. Затем должны быть разработаны дополнительные верификационные испытания для новых или пересмотренных требований, выполненных и проанализированных.
3. Неиспользуемые функции. Аппаратное изделие может содержать функции, которые не используются в целевом применении схемы, такие, как неиспользуемые подфункции

в библиотечной функции или контрольные структуры, применяемые только для приемочных испытаний на уровне компонента. Должно быть показано, что такие функции либо изолированы от других используемых функций, либо не имеют потенциального аномального поведения, которое может оказать неблагоприятное влияние на безопасность. Этого можно достичь, показав, что неиспользуемые элементы безусловно дезактивированы либо в рамках аппаратуры, либо при установке. Если неиспользуемые функции должны применяться в будущих приложениях, то недостаток элементного анализа может быть пересмотрен в надлежащее время, при этом – показано, что такие установленные функции не полностью проверены.

4. Элемент без последствий для безопасности. С помощью анализа может быть выявлено и показано, что последствие аномального поведения элемента не влияет на безопасность самолета и его пассажиров. Эти вопросы должны быть решены с помощью регистрации ограничения анализа последствий аномального поведения элемента.

3.3.1.3. Выходные данные жизненного цикла элементного анализа

Выходные данные жизненного цикла элементного анализа должны:

1. Определять тракты функционального отказа, рассматриваемые в элементном анализе, уровни в иерархии конструкции, на которых определяются элементы, и как они проанализированы на верификационную достаточность, что является частями критериев полноты верификационного покрытия. Это должно быть включено в «План сертификации аппаратуры» или в «План верификации аппаратуры».
2. Описывать методы и определять тракты функционального отказа, рассматриваемые в анализе, а также уровни в иерархии конструкции, при которых выполняется анализ.
3. Гарантировать, что данные трассировки, описанные в подразделе 10.4.1, показывали четкое взаимоотношение процедур верификации с элементами в элементном анализе.
4. Определять контрольные примеры верификации и дополнительные или измененные требования как результат элементного анализа.
5. Устанавливать уровень полноты верификации, достигнутый для трактов функционального отказа, рассмотренных в элементном анализе, включая определенные анализом недостатки, не исправленные модификацией верификационных испытаний или требований, и обоснование их приемлемости.

3.3.2. Специальный анализ безопасности

Там где он применяется, метод специального анализа безопасности расширяет концепцию FFPA аппаратуры за счет более глубокого анализа выбранных схем и компонентов. Расширенный FFPA используется как для производных, так и для валидированных требований к безопасности в отношении внутренних операций этих схем и компонентов. Эти производные требования безопасности затем рассматриваются в ходе верификационных испытаний, как описано ниже.

Специальный анализ безопасности основан на концепции того, что потенциально скрытые ошибки конструирования могут повлиять на выход элемента аппаратуры только под воздействием специальных стимулов. Следовательно, для правильного стимулирования и выявления ошибок, влияющих на безопасность, необходимо определить подмножество входных примеров, для которых необходима безопасная работа, а затем в верификационные испытания включаются соответствующие эквивалентные классы из этого подмножества. Во время выполнения этих контрольных примеров выходные данные элемента оцениваются на отсутствие специфических аномалий поведения, которые могут привести к небезопасным выходным условиям. Специальный анализ безопасности используется для ограничения набора входных условий, которые должны быть использованы при верификационных испытаниях, чтобы не рассматривался потенциально бесконечный ряд входных контрольных примеров.

Примечание. *Реализация может также ограничивать входное множество и условия, так что невозможно или в достаточной мере невероятно, что реализация позволит входным данным выйти за испытанные пределы.*

Метод специального анализа безопасности может также использоваться для определения аспектов невыполненного ослабления схем и функций компонентов, в которых применяется частичное архитектурное ослабление. В этом случае дополнительный специальный анализ безопасности может стать полезным и эффективным методом определения того, какая дополнительная гарантия конструирования требуется для завершения покрытия безопасности.

Метод специального анализа безопасности равно применим как к аппаратуре COTS, так и к коммерческим схемам и компонентам, потому что он способен использовать данные руководства пользователя об этих схемах и цепях, вместо детальных данных внутренней конструкции. Объединяя данные пользователя с более детальным применением метода FFPA, специальный анализ безопасности способен успешно определить чувствительные к безопасности аспекты применения схем и компонентов и соответствующие внутренние тракты функционального отказа, в которых требуется уделить большое внимание устранению ошибок конструирования. Эта информация может затем использоваться для успешной подготовки верификационных испытаний схем и компонентов, максимально повышающих вероятность того, что процесс верификации обеспечил обнаружение, исправление, ослабление или обход ошибок конструирования схем и компонентов, которые могут неблагоприятно воздействовать на аппаратуру с точки зрения безопасности.

3.3.2.1. Метод специального анализа безопасности

После выбора схем и компонентов, которые должны быть рассмотрены с использованием метода специального анализа безопасности гарантии конструирования, выполняется дополнительный FFPA, с целью их более детальной проверки. Этот анализ определяет более специфически, какие функции схемы, компонента вносят вклад в уже определенные функции уровней А и В, в реализации которых используются такие схемы, компоненты. Анализ осуществляется проверкой на индивидуальной основе каждой прикладной схемы и компонента, в их функциональных границах, с учетом реального функционального использования этой схемы и компонента – для выполнения функций аппаратуры более высокого уровня, содержащихся в определенных трактах функционального отказа уровней А и В.

Примечание. *Достаточная информация может быть получена из данных руководства пользователя по схемам и компонентам, которые пользователь может успешно использовать для выполнения функций аппаратуры более высокого уровня. Если имеется достаточная информация о внутреннем функционировании схем и компонентов, она должна быть адекватной для проведения этой оценки. Если достаточной информации нет, тогда оценка не может быть выполнена и должен использоваться другой метод вместо этого или вместе с ним.*

После того как уместные чувствительные к безопасности функции схем и компонентов определены на основе реального применения данных схем и компонентов, следующим шагом является более детальный функциональный анализ. Этот анализ должен определить специфические чувствительные к безопасности и неослабленные атрибуты функций тех схем и компонентов, которые должны быть рассмотрены более детально с применением чувствительных к безопасности условий верификации. Эти условия верификации должны быть получены и валидированы с помощью функциональных методов анализа видов и последствий отказа для определения специальных функциональных атрибутов, которые чувствительны к безопасности, а затем определить любые аномалии поведения этих функций, которые составляют тракт функционального отказа уровней А и В в пределах схемы или компонента.

Выведенные условия верификации, полученные с применением вышеописанного специального анализа безопасности, затем используются вместе со следующими инструкциями по подготовке критериев специального анализа безопасности для верификации схемы и компонентов, содержащихся в трактах функционального отказа уровней А и В. Инструкции включают:

1. Идентификацию подходящего входного пространства функций. Определение критериев «прошел/отказал» соответствующего выходного пространства, основанное на определенных чувствительных к безопасности атрибутах и аномалиях поведения, разработка классов эквивалентности, которые обеспечат необходимое покрытие соответствующего входного пространства.

2. Идентификацию подходящих средств обнаружения наблюдением и средств имитации входного пространства для каждой рассматриваемой функции.

Примечание. *Специальные инструменты и особенности реализации могут использоваться для обеспечения наблюдаемости и контролепригодности.*

3. Установление условий испытаний, которые обеспечивают проверку потенциальных источников ошибок и взаимозависимостей.

Примечание. *Функции на уровне компонента должны быть тестированы на более высоком уровне интеграции. Испытание на более высоком уровне интеграции обычно обеспечивает наилучшее покрытие источников ошибок, таких как срывы, взаимозависимости и потенциальные перекрестные взаимодействия.*

Испытания должны разрабатываться с использованием классов эквивалентности. При испытаниях необходимо рассмотреть основные логические решения, арифметику, синхронизацию, переходы состояний и атрибуты в реальном масштабе времени.

3.3.2.2. Разрешение вопросов, выявленных специальным анализом безопасности

Критерии завершения чувствительной к безопасности верификации должны быть установлены с помощью выполнения специального анализа безопасности для всех прикладных схем и компонентов. Любые недостатки, обнаруженные при этом анализе или при самой верификации, должны быть разрешены одним из следующих методов:

1. Изменение конструкции для исправления ошибки.
2. Добавление архитектурного ослабления, которое решает ошибку путем устранения ее из соответствующего тракта функционального отказа.
3. Дополнительные подходящие испытания.

3.3.2.3. Данные специального анализа безопасности

Документация специального анализа безопасности, применяемого к схемам и компонентам в трактах функционального отказа уровней А и В, должна быть представлена в форме данных оценки безопасности, данных о требованиях по безопасности, процедур и результатов верификации и данных трассирования. Процедуры верификации должны быть трассируемы к требованиям безопасности и специальному анализу безопасности. Данные специального анализа безопасности должны включать следующее:

1. Идентификацию схем и компонентов, которые рассматриваются в методе специального анализа безопасности.
2. Идентификацию трактов функционального отказа уровней А и В, в которых размещается каждая из таких схем и компонентов.
3. Идентификацию специального архитектурного ослабления, применяемого к схемам и компонентам, когда гарантия конструирования пополняется применением метода специального анализа безопасности.
4. Идентификацию функций для каждой применяемой схемы и каждого компонента, чувствительных к безопасности.
5. Идентификацию атрибутов и аномалий поведения для каждой идентифицированной чувствительной к безопасности функции.
6. Верификацию условий, относящихся к схемам, компонентам, внутренним функциям, функциональным атрибутам и аномалиям поведения.
7. Верификацию условий, относящихся к проверенным входным зависимостям и поведению выходных данных.
8. Процедуры и результаты верификации.
9. Данные трассируемости процедур верификации к условиям верификации безопасности аппаратуры для специального анализа данных безопасности аппаратуры.

3.3.3. Формальные методы

Термин «формальные методы» относится к использованию методов логической и дискретной математики при спецификации, конструировании и создании компьютерных систем.

Примечание. *Материал для данного раздела получен из справочника "Formal Methods Specification and Analysis Guidebook for the Verification of Software and Computer Systems, Volume II: A Practitioner's Companion," May 1997, NASA-GB-001-97. Более детальное представление формальных методов с иллюстративными примерами дано там.*

Применение формальных методов подразделяется на две категории – описательную и дедуктивную. В описательных методах применяются формальные технические языки, которые даны для ясного понятного описания требований и других артефактов проекта. Дедуктивные методы основаны на дисциплине, которая требует использовать полный перечень всех допущений и этапов обоснования. Кроме этого, каждый этап обоснования должен содержать небольшое количество допускаемых правил, представляющих интерес. Более жесткие формальные методы применяют эти методы для подтверждения обоснования, используемого для доказательства требований или других аспектов конструирования или реализации сложной или критичной системы. Целью формальных методов является уменьшение необходимости полагаться на интуицию человека и его суждения при оценке аргументов. Таким образом, дедуктивные формальные методы уменьшают приемлемость аргумента до уровня вычисления, что может в принципе быть проверено с помощью инструмента, заменяя тем самым внутреннюю субъективность процесса рассмотрения на повторяемое применение.

Существует несколько областей, в которых применение формальных методов дает дополнительную гарантию процесса конструирования. Хотя формальные методы применяются в рамках процесса конструирования, повышение гарантии конструирования может быть достигнуто путем целевого применения. Ниже перечисляются некоторые возможности:

1. Формальные методы могут применяться на разных этапах жизненного цикла конструирования. Обычно применение формальных методов наиболее эффективно на ранних этапах жизненного цикла, особенно во время определения требований и конструирования на высоком уровне.
2. Формальные методы могут быть применимы ко всему проекту или они могут быть предназначены для отдельных компонентов. Анализ FFPA используется для того, чтобы определить, какие тракты функционального отказа необходимо анализировать с помощью формальных методов. С использованием формальных методов могут эффективно анализироваться аппаратная реализация отказоустойчивых функций и протоколов сложных параллельных взаимодействий.
3. Формальные методы могут применяться для верификации функциональности системы или для установления специфических свойств. Хотя формальные методы традиционно связаны с «доказательством правильности», т.е. с гарантией соответствия компонентов функциональным спецификациям, они также могут применяться только к наиболее важным свойствам. Часто более важно подтвердить, что конструкция не проявляет нежелательных свойств, а не доказывать, что она имеет полную функциональность.

Практическое применение формальных методов обычно требует инструментальной поддержки. Используемые инструменты должны быть оценены и, если необходимо, квалифицированы как описано в подразделе 11.4.

3.3.3.1. Методология формальных методов

Применение формальных методов начинается с выражения требований формальным языком. Спецификация требований служит важной описательной функцией. Она обеспечивает базу для документирования, соединения и макетирования поведения и свойств системы, используя однозначные указания. Кроме того, спецификация требований служит основой для вычисления или формального прогнозирования поведения системы. Формальная модель компонента, который должен анализироваться, строится с использованием формального языка. Модель анализируется по отношению к формальному установлению требований согласно правилам выбранной формальной логики. Характеристики модели определяются стилем формального анализа, который должен быть выполнен.

Уровень детализации в модели компонента определяется целью выбранного формального способа анализа. Некоторые подходы приспосабливаются к нахождению ошибок конструирования, которые могут ускользать от испытаний, а другие подходы стараются гарантировать отсутствие ошибок конструирования определенных классов:

1. Обнаружение ошибки. Наиболее общим формальным способом для обнаружения ошибки считается проверка модели. В этом случае требования выражаются как формулы во временной решаемой логике. Модель компонента – это абстрактный механизм состояния, созданный так, чтобы свойства, которые должны испытываться, сохранялись. Процедура доказательства является автоматической. Неудачная попытка доказательства указывает на ошибку конструирования в моделируемом компоненте. Результат неудачного доказательства это последовательность входных стимулов, которые специально демонстрируют, как компонент не удовлетворяет установленному требованию.
2. Предотвращение ошибки. Формальные методы, направленные на предотвращение ошибок, обычно основаны на языке спецификаций и теории обеспечения доказательства. Для увеличения выразительности могут устанавливаться более сложные требования и создаваться более сложные модели компонента. Однако процедура доказательства может быть только частично автоматизированной. Соответствующий уровень детализации для моделей компонента может быть синтезируемым описанием на языке высокого уровня конструирования. В некоторых случаях одна и та же модель может применяться как для моделирования, так и для формального анализа. Полным доказательством является очевидность того, что компонент логически правилен в отношении установленных требований для анализируемого входного пространства.

3.3.3.2. Разрешение вопросов, выявленных формальными методами

Существует три возможных результата дедуктивного формального анализа:

1. Если попытка доказательства успешна, проверка завершена. Уровень гарантии конструирования зависит от правильности применяемых моделей. Например, если модель элемента аппаратуры соответствует техническому проектированию, доказательство обеспечивает гарантию функциональной корректности данных всеобъемлющего испытания.
2. В некоторых случаях неудачное доказательство приводит к точному контрпримеру, т.е. оно определяет сценарий испытания, который ясно показывает, каким образом проект не соответствует установленным требованиям. Оно может указывать либо на недостатки в проекте, либо на недостатки в требованиях. Такие недостатки могут быть решены соответствующим исправлением проекта, пересмотром требований, оказавшихся физически нереализуемыми, или использованием другого метода. Все контрпримеры должны быть идентифицированы, чтобы поднятые в них вопросы можно было разрешить. Изменения в проекте или требованиях должны быть направлены обратно в соответствующий процесс:
   a. После того как проект или требование были изменены, в связи с недостатком, выявленным неудавшейся попыткой доказательства, доказательство должно быть предпринято заново, чтобы подтвердить, что модификация успешно решает выявленную проблему. Этот цикл повторяется до тех пор, пока не будет получено успешное доказательство.
   b. В случаях когда контрпример считается разрешаемым без изменения проекта или требований, но средство определяет только один контрпример, т.е. разрешенный контрпример, процесс должен быть модифицирован, так чтобы он мог идентифицировать другие контрпримеры.
3. Наиболее трудным случаем для решения является случай, когда доказательство не может быть проверено и контрпример не может быть идентифицирован. Одним из возможных вариантов является пересмотр проекта, для того чтобы упростить проверку. В противном случае проверка может быть распределена на составляющие с четким определением примеров, которые рассмотрены методом доказательства, и примеров, когда требования должны быть рассмотрены с помощью других средств. Изменения в проекте и производные требования должны быть возвращены обратно в FFPA.

3.3.3.3. Данные формальных методов

Данные, разработанные при применении формальных методов, включают:

1. Описание подходов к используемым специальным формальным методам, описание компонентов или тракта функционального отказа, к которым будут применены формальные методы.
2. Формальное установление требований.
3. Формальные модели компонента.
4. Доказательство и достаточно детальный сценарий для создания доказательства, относящийся к моделям компонента, и для формального установления требований, включая коррекцию в данных трассируемости.
5. Идентификацию применяемых инструментов и результатов оценки инструментов.
6. Идентификацию верификационных контрольных примеров и требований, дополненных или измененных в результате анализа.
7. Установление уровня полноты верификации для трактов функционального отказа, достигнутого в анализе. Включается перечень выявленных анализом недостатков, не разрешенных при модификации верификационных контрольных примеров или требований, и обоснование приемлемости недостатков.

ПРИЛОЖЕНИЕ С

Словарь терминов

Настоящие определения даны для терминов, используемых в данном документе. Если термин не определен в этом Приложении, он может быть определен в тексте.

Анализ (Analysis) – Процесс математического или любого логического объяснения, который ведет от установления предпосылок к выводу, касающемуся специальных способностей оборудования или элемента аппаратуры и его адекватности для конкретного применения.

Анализ границ конструирования (Design Margin Analysis) – Процесс определяющий, что сумма воздействия различных границ конструирования компонентов аппаратуры обеспечивает изделие, которое соответствует или превосходит требования к его характеристикам, а также требования к технологичности и обслуживанию.

Анализ покрытия (Coverage Analysis) – Процесс определения степени, при которой предложенный процесс проверки аппаратуры удовлетворяет его цели.

Аномальное поведение (Anomalous Behavior) – Поведение, которое несовместимо с установленными требованиями.

Архитектура системы (System Architecture) – Структура аппаратуры и ПО, выбранная для реализации требований к системе.

Базовая версия (Baseline) – Определенная и одобренная конфигурация, которая с этого момента служит основой для дальнейшего конструирования и которая изменяется только при изменении процедур контроля.

Безопасность (Safety) – Состояние, при котором величина риска ниже, чем его предельное значение. Предельное значение – это верхняя граница приемлемого риска. Он характерен для технических процессов или состояний. Риск определяется частотой или вероятностью появления и предполагаемым наносимым вредом.

Верификация (Verification) – Оценка реализации требований для определения того, что эти требования могут быть удовлетворены.

Вид отказа (Failure Mode) – Характер проявления отказа.

Время воздействия (Exposure Time) – Период времени между последним известным моментом правильного функционирования элемента аппаратуры и известным моментом его следующего правильного функционирования.

Выпуск (Release) – Акт официальной передачи данных элемента аппаратуры под контроль конфигурации.

Гарантия (Assuarance) – Результат запланированных или систематических действий, необходимых для обеспечения доказательства и очевидности того, что изделие или процесс удовлетворяет заданным требованиям.

Гарантия конструирования (Design assurance) – Все запланированные и систематические действия, используемые для того, чтобы привести достаточные основания на соответствующем уровне достоверности, что ошибки конструирования были выявлены и устранены, так что аппаратура удовлетворяет действующему сертификационному базису.

Готовность (Availability) – Вероятность того, что элемент или функция находятся в работоспособном состоянии.

Дефект (Defect) – Любое несоответствие характеристик установленным требованиям.

Дефекты надежности (Reliability Defects) – Дефекты, которые вызывают отказ аппаратуры с высокой интенсивностью, когда условия нагрузки не превосходят номинальные расчетные пределы. И дефекты чрезмерной нагрузки, и дефекты надежности могут быть продемонстрированы как проявившие очень высокую интенсивность случайных отказов или чрезмерную степень износа.

Дефекты отказоустойчивости (Robustness Defects) – Дефекты, которые могут вызвать отказ аппаратуры или ее неправильную работу при воздействии нагрузки и сроке эксплуатации, не превышающем конструктивные пределы. Результатом этих дефектов может стать восприимчивость к внешним нагрузкам и нестабильность в течение срока службы.

Дефекты превышения нагрузки (Over-stress defects) – Дефекты, которые вызывают превышение расчетных конструктивных пределов компонента или появляются в результате превышения нагрузки, встречающейся во время жизненного цикла конструирования аппаратуры.

Допущения (Assumptions) – Утверждения или принципы, предложенные без доказательства.

Единица конфигурации (Configuration item) – Один или более компонентов, средств или элементов данных, рассматриваемых как блок, – с целью управления конфигурацией.

Жизненный цикл (Life Cycle) – Период времени между началом проекта или модификации элемента аппаратуры и завершением конструирования или модификации и переходом к производству.

Примечание. *В данном документе, если особо не оговорено, это означает «жизненный цикл конструирования аппаратуры».*

Заказная интегральная микросхема (Application Specific Integrated Circuit) – Интегральная схема, которая разработана для реализации функции и включает (но не ограничивается этим) следующие элементы: вентильные решетки, стандартную ячейку и заказные компоненты, содержащие линейные, цифровые или смешанные технологии.

Заявитель (Applicant) – Лицо или организация, которая пытается получить одобрение от сертифицирующего органа.

Идентификация конфигурации (Configuration Identification) – Процесс определения и обозначения элемента конфигурации.

Изделие (Product) – Аппаратура, ПО, элемент или система, созданные в результате выполнения определенного набора требований.

Инспекция (Inspection) – Проверка и контроль поставок и обслуживания, включая когда требуется, необработанные материалы, компоненты, промежуточные устройства или службы – с целью определения их соответствия установленным требованиям.

Инструмент верификации (Verification Tool) – Средства, используемые для обеспечения характеристик в соответствии с предварительно определенными стандартами или требованиями. Эти средства не вводят ошибок, но могут их не обнаружить. Например, аналоговое или цифровое моделирующее устройство или автоматический тест, который измеряет реальные характеристики сети.

Интегральная схема (Integrated Circuit) – Схема, состоящая из элементов, неотделимо связанных или собранных на одной подложке для выполнения функции электронной схемы.

Интеграция ПО/АС (Hardware/Software Integration) – Объединение аппаратных и программных средств для реализации прикладной системы или функции.

Интенсивность отказов (Failure Rate) – Общее количество отказов в пределах совокупности элементов, деленное на общее количество часов работы элемента в установленных условиях.

Инструменты конструирования (Design Tools) – Средства, результатом применения которых является создание части конструкции аппаратуры, которая может содержать ошибки. Например, маршрутизатор ASIC или средство, которое позволяет создать плату или компоновку чипов, основываясь на схематических или других технических требованиях.

Испытание (Test) – Процедура количественной оценки характеристик с использованием установленных объективных критериев, в результате которой продукт «прошел/отказал»:

- Элемент аппаратуры. Для определения его технических характеристик при эксплуатации в управляемых условиях.
- Электронное цифровое вычисление. Подтвердить состояние или условие элемента, компонента, программы и т.д.

- Иногда используется как общий термин для определения как процедур проверки, так и диагностики.
- Иногда – как проверка.
- Как элемент проверки часто означает определение техническими средствами свойств элементов поставщиков или замечаний к таким элементам, включая функциональную эксплуатацию, и предусматривает применение установленных научных принципов или процедур (методик).

Квалификация инструмента (Tool Qualification) – Процесс, необходимый для получения сертификата на инструмент в контексте конкретной бортовой системы.

Класс эквивалентности (Equivalence Class) – Разделение входного пространства функции так, чтобы контроль представленной величины класса был эквивалентен другим величинам данного класса.

Коммерческий готовый компонент (COTS Component) – Компонент, интегральная схема или подсистема, разработанные поставщиком для многочисленных пользователей, чьи конструкция и конфигурация контролируются техническими условиями поставщиков или промышленности.

Примечание. *Примерами компонентов COTS могут служить резисторы, конденсаторы, микропроцессоры, непрограммируемые полевые вентильные решетки и логические программируемые устройства со стираемой памятью, другие интегральные схемы и их внедряемые модели, печатные платы и целые быстросменные блоки, которые обычно поставляются по каталогу.*

Компонент (Component) – Любая автономная часть, совокупность частей, субблоков или блоков, которая выполняет заданную функцию системы.

Контролепригодность (Testability) – (1) Способность успешно контролировать элемент аппаратуры, для того чтобы гарантировать, что во всех возможных состояниях элемент аппаратуры выполняет предназначенные ему функции. (2) Простота, с которой элемент аппаратуры может контролироваться, для того чтобы обеспечить очевидность его соответствия требованиям.

Контроль (Monitoring) – (1) Безопасность. Функциональность внутри системы, которая разработана с целью обнаружения аномального поведения систем. (2) Обеспечение качества процесса. Акт доказательства или проверки выбранных примеров испытания, проверка или другая деятельность и документирование этой деятельности – с целью обеспечения того, что деятельность находится под контролем и что полученные результаты соответствуют ожидаемым. Контроль обычно ассоциируется с действиями, выполненными в расширенный период времени, когда 100%-ное доказательство не практикуется или не является необходимым. Контроль позволяет устанавливать достоверность того, что утвержденная деятельность была выполнена как планировалось.

Контроль изменений (Change Control) – (1) Процессы документирования, оценки, утверждения или отклонения и координации изменений элементов конфигурации после формального установления идентичности их конфигураций или основы, после ее установления. (2) Систематическая оценка, координация, утверждение или отклонение и внедрение утвержденных изменений в элементе конфигурации после его формального утверждения, а также базовых характеристик после их установления.

Конфигурация (Configuration) – Перечень элементов конфигурации, которые полностью определяют реализацию функции.

Кратковременная импульсная помеха (Glitch) – Входной перепад или всплеск напряжения в течение периода времени, более короткого, чем задержка в результате поврежденной логики, которая может распространиться на выходной сигнал.

Летная годность (Airworthiness) – Состояние изделия (самолета, системы или части самолета), при котором это изделие, обеспечивая безопасность, выполняет предназначенные ему функции.

Методы оценки соответствия (Means of Compliance) – Методы, которые должны использоваться заявителем для удовлетворения требований, установленных в сертификационных документах для самолета или двигателя. Примерами являются утверждения, чертежи, анализ,

вычисления, испытания, моделирование, проверка и классификация внешних условий. Применяется рекомендательный материал, выпущенный сертифицирующим органом, если он имеется.

Надежность (Reliability) – Вероятность того, что элемент будет выполнять предназначенную ему функцию в определенном интервале при установленных условиях.

Независимость (Independence) – Разделение ответственности, которое обеспечивает выполнение объективной оценки. Относится к интеллектуальной независимости, например отдельного автора, а не компании или отдела:

1. Для проверки независимость достигается оценкой технической корректности данных посредством кого-то или чего-то, отличного от того, что использовалось для выполнения процесса.
2. Для обеспечения процесса независимость достигается путем оценки соответствия процесса средствами, отличными от тех, что использовались для выполнения процесса.

Неисправная работа (Malfunction) – Возникновение условий, при которых изделие работает, выходя за установленные пределы.

Неисправность (Fault) – (1) Проявление изъяна в аппаратуре из-за ошибки или случайного события. Неисправность, если она наблюдается, может вызвать отказ. (2) Нежелательная аномалия в элементе.

Обозначение конфигурации (Configuration Identity) – Уникальное имя, данное элементу конфигурации или всей конфигурации в результате идентификации конфигурации.

Обоснование (Validation) – Процесс обоснования того, что требования являются корректными и полными.

Обособление аппаратных средств (Hardware Partitioning) – Метод повышения надежности и безопасности, обеспечиваемый физическим разделением и изоляцией аппаратуры, которая реализует функции, включая резервирование, – с целью предотвращения влияния отказов из-за общих ошибок.

Обратное конструирование (Reverse Engineering) – Повторное применение элемента аппаратуры путем изучения его конструкции, функции и характеристик в заданных окружающих условиях.

Общий режим (Common Mode) – Событие, которое вызывает аномальное поведение двух или более элементов, подэлементов или функций.

Одобрение (Approval) – Акт или постановление, выражающее одобрительное мнение или дающее формальную или официальную санкцию.

Опытный образец (First Article) – Блок, представленный на проверку для контроля промышленных чертежей, инструментальных средств и процедур.

Опыт эксплуатации изделия (Product Service Experience) – Период времени, в течение которого аппаратура функционирует в известных окружающих условиях и в течение которого последовательно регистрируются отказы.

Отказ (Failure) – Неспособность системы или компонента системы выполнять требуемую функцию в установленных пределах. Отказ может быть вызван неисправностью.

Отказное состояние (Failure Condition) – Состояние, оказывающее непосредственное или косвенное влияние на самолет и его пассажиров, вызванное одним или несколькими отказами, соответствующими неблагоприятным эксплуатационным или окружающим условиям.

Отклонение от номинала (Component Derating) – Метод конструирования, который расширяет рабочие границы компонентов путем изменения ограничений на использование компонента, которые являются более жесткими, чем обычные нормы или рабочие нормы изготовителя компонента.

Оценка (Assessment) – Оценка, основанная на инженерном заключении.

Оценка инструмента (Tool Assesment) – Совокупность действий для оценки средств, используемых при конструировании и проверке элемента аппаратуры – с целью подтверждения способности инструментального средства выполнять корректно его функции, совместимые с уровнем гарантии конструирования тех функций, которые выполняются элементом аппаратуры.

Оценка безопасности системы (System Safety Assessment, SSA) – Непрерывная, систематическая обширная оценка предлагаемой системы – с целью демонстрации выполнения специфических требований к безопасности.

Ошибка (Error) – Ошибка в требованиях, проекте или реализации.

Подобие (Similarity) – Относится к системам, которые по своим характеристикам и применению подобны системам, используемым на ранее сертифицированным заявителем самолете. Кроме того, считается, что ни одна из частей конкретной системы не находится в условиях более высокого риска (в связи с окружающими условиями или установкой) и что эксплуатационные нагрузки не более жесткие, чем для аналогичной системы.

Последствие отказа (Failure Effect) – (1) Описание работы элемента как результат отказа. (2) Последствия вида отказа на работу, функцию или состояние системы или элемента.

Предварительная оценка безопасности системы (Preliminary System Safety Assessment) – Систематическая оценка предлагаемой архитектуры системы и ее реализации, основанная на оценке функциональной опасности и классификации условий отказа – с целью определения требований безопасности для всех элементов в архитектуре.

Примечание. *Предварительная оценка безопасности системы применяется к системе при разработке. Она используется для управления дальнейшей деятельностью по анализу безопасности, необходимой для завершения окончательной оценки безопасности системы.*

Признание (Acceptance) – Подтверждение сертифицирующим органом того, что представленные данные, аргументы или доказательства эквивалентного соответствия удовлетворяют применяемым требованиям.

Проверка опытного образца (First article Inspection) – Проверка обеспечения качества процесса, которая подтверждает что «созданная» аппаратура соответствует документации на процесс изготовления. Выполняется на серийных элементах аппаратуры, представляющих первую изготовленную конфигурацию, как предварительное условие для одобрения производства.

Программируемое логическое устройство (Programmable Logic Device, PLD) – Компонент, который предназначен выполнять специальную прикладную функцию. PLD включает (но не ограничивается этим) следующие компоненты: программируемые компоненты логики массива, программируемые компоненты логического массива, общие компоненты логики массива, программируемые пользователем компоненты массива и перепрограммируемые логические устройства.

Программное обеспечение (Software) – Компьютерная программа и, возможно, соответствующая документация, а также данные, имеющие отношение к работе компьютерной системы.

Производное требование (Derived requirement) – Дополнительное требование, полученное в результате процесса конструирования аппаратуры, которое не может быть непосредственно исследовано на более высоком уровне требований.

Производство (Production) – Изготовление изделия путем документированной и управляемой последовательности процессов.

Простой элемент аппаратуры (Simple Hardware Item) – Элемент аппаратуры считается простым, если обширная комбинация детерминистских испытаний и анализов может обеспечить точную функциональную характеристику во всех предлагаемых условиях эксплуатации без аномалий в поведении.

Прототип (Prototype) – Опытный элемент аппаратуры, который полностью отражает конечное изделие, использующее одобренные компоненты, и подходит для полной оценки формы, конструкции и характеристик.

Процедура испытаний (Test Procedure) – Детальные инструкции для контроля условий выполнения заданного набора тестов.

Процесс (Process) – Набор взаимосвязанных действий, выполненных с целью получения заданного результата или изделия.

Процесс гарантии (Process Assurance) – Задача процесса гарантии заключается в следовании планам, выполнении задач жизненного цикла конструирования аппаратуры и завершении действий.

Процесс жизненного цикла конструирования аппаратуры (Hardware Design Life Cycle Process) – Один из процессов конструирования или поддержки, определенный организацией как достаточный для конструирования элемента аппаратуры.

Процесс конструирования (Design Process) – Процесс создания элемента аппаратуры на основе ряда требований с использованием следующих процессов: определение требований, эскизное проектирование, техническое проектирование, реализация и переход к производству.

Процесс поддержки (Supporting Process) – Процесс, используемый для поддержки процесса конструирования, состоящий из одного из следующих процессов: обоснования, верификации, управления конфигурацией, процесса гарантии и взаимодействия при сертификации.

Процесс планирования (Planning Process) – Процесс для определения и координации мероприятий и процессов конструирования аппаратуры и поддержки.

Рассмотрение (Review) – Качественная оценка доступности планов, требований, данных конструирования, эскизного проекта или реализации конструкции – с целью демонстрации высокой степени уверенности в том, что требования удовлетворяются или будут удовлетворяться.

Реализация (Implementation) – Действие по созданию физической реальности на основе данных технического проектирования.

Ремонтопригодность (Maintainability) – Характеристика конструкции и установки, которая выражается как вероятность того, что элемент будет сохранен или восстановлен до соответствующего состояния в заданный период времени, когда техобслуживание выполнено в соответствии с предписанными процедурами и ресурсами.

Риск (Risk) – Комбинация частоты и последовательности возникновения установленного опасного состояния.

Руководство (Guidance) – Совет или консультация по установлению соответствия сертификационным требованиям.

Сборка (Assembly) – Набор компонентов или любая их комбинация, объединенная вместе для выполнения специальной функции.

Сертификационный базис (Certification Basis) – (1) Комплекс требований к летной годности и охране окружающей среды, распространенных на данный образец авиационной техники. (2) Определенные сертифицирующим органом, при консультации с заявителем, конкретные сертификационные требования (вместе с любыми особыми условиями, которые могут дополнять опубликованные нормативы), используемые в качестве основы для сертификации самолета, двигателя или воздушного винта.

Сертификационный зачет (Certification Credit) – Признание сертифицирующим органом того, что процесс, изделие или демонстрация удовлетворяют сертификационному требованию.

Сертификация (Certification) – (1) Установление соответствия авиационной техники и ее производства требованиям действующих авиационных правил. (2) Юридическое признание сертифицирующим органом, что изделие, служба, организация или лицо соответствуют требованиям.

Сертифицирующий орган (Certification Authority) – организация или лицо, ответственное за выдачу сертификата о соответствии требованиями.

Сложный элемент аппаратуры (Complex Hardware item) – Все элементы, которые не являются «простыми», считаются «сложными». См. определение «простой элемент аппаратуры».

Система (System) – Совокупность компонентов аппаратуры и ПО, организованных с целью осуществления специальной функции или ряда функций.

Согласованность (Conformity) – Согласование физической реализации элемента аппаратуры с определяющими документами.

Совместное конструирование (Concurrent Engineering) – Процесс, при котором в конструировании аппаратуры участвуют многие дисциплины – с целью того, чтобы обеспечить рассмотрение уникальных требований каждой дисциплины.

Совпадение (Conformance) – Точное совпадение со стандартом, техническими условиями или чертежом.

Соответствие (Compliance) – Успешное выполнение всех обязательных действий, совпадение предполагаемых или заданных результатов с реальными результатами.

Спецификация (Specification) – Собрание требований, которые создают критерии, определяющие функции и атрибуты элемента.

Срыв (Upset) – Нарушение работы, вызванное внешними событиями, такими, как молния, или другими событиями в среде экспуатации.

Стандарт (Standard) – Правило или основа для сравнения, используемая для обеспечения как руководства, так и оценки заданной деятельности или содержания установленного блока данных.

Структура (Structure) – Системное размещение или взаимодействие элементов для создания целого.

Тестирование (Testing) – Процесс проверки характеристик элемента аппаратуры.

Технологичность (Manufacturability) – Характеристика конструкции изделия, которая упрощает экономичное массовое производство путем оптимизации материалов и средств производства, а также применения методов конструирования, снижающих влияние отклонений характеристик компонента на функциональность.

Тракт функционального отказа (Functional failure path) – Особое множество независимых схем, которые могут вызвать конкретное аномальное поведение в аппаратуре, реализующей функцию, или в аппаратуре, зависящей от функции.

Трассируемость (Traceability) – Характеристика, позволяющая устанавливать связь между элементами аппаратуры или процессами, между требованием и источником требования или между методом проверки и его основным требованием.

Требование (Requirement) – Элемент спецификации, который можно проверить.

Тренажер (Simulator) – Устройство, компьютерная программа или система, используемые во время проверки аппаратуры, которые принимают те же самые входные сигналы и выдают те же выходные сигналы, что и заданная система.

Управление конфигурацией (Configuration management) – (1) Процесс идентификации конфигурации, контроля выпуска документации и внесения изменений в конфигурацию. (2) Порядок применения мер технического или административного управления и надзора – с целью определения и документирования функциональных и физических характеристик элемента конфигурации, управления изменением этих характеристик, а также описание и оповещение об изменениях в управлении и статусе применения.

Функциональные дефекты (Functional Defects) – Дефекты, которые вызывают неправильное функционирование аппаратуры, даже если не наблюдается физический отказ аппаратуры. Неправильное функционирование аппаратуры, в свою очередь, может вызвать неправильное функционирование зависимых функций ПО.

Функциональный тракт (Functional Path) – Особое множество независимых схем, которые реализуют функцию.

Целостность (Integrity) – Признак элемента, указывающий, что на него можно положиться при выполнении предназначенной функции.

Шифр детали (Part Number) – Ряд номеров, букв или других знаков, используемых для определения единицы конфигурации или совокупности конфигураций.

Элемент аппаратуры (Hardware item) – Элемент, который существует физически. Это в общем случае относится к быстросменным блокам, монтажным платам, источникам электропитания и компонентам [переставить с «Элементом»].

Элемент (Item) – Общий термин, используемый для описания компонента аппаратуры, системы и ПО.

Язык описания аппаратуры (Hardware Description Language) – Язык высокого уровня, используемый в данном документе для представления всех языков описания аппаратных средств, включая «Verilog HDL», «Very High Speed Integrated Circuit Hardware», «Description Language» и «Analog Hardware Description Language».

ПРИЛОЖЕНИЕ D

Сокращения

АС	Аппаратные средства
ПО	Программное обеспечение
ASIC	Специализированная заказная интегральная схема
FAI	Испытания первого изделия
HC1	Категория 1 контроля аппаратуры
HC2	Категория 2 контроля аппаратуры
COTS	Готовый коммерческий (продукт)
FFPs	Тракты функционального отказа
FFPA	Анализ тракта функционального отказа
FHA	Оценка функциональной опасности
F-FMEA	Функциональный анализ видов и последствий отказов
FTA	Анализ дерева неисправности
HDL	Язык описания аппаратуры
LRU	Быстросменный блок
PHAC	План сертификации аппаратуры
PLD	Программное логическое устройство
PSSA	Предварительная оценка безопасности системы
RTCA	Радиотехническая комиссия по аэронавтике
SSA	Оценка безопасности системы

РУКОВОДСТВО
по гарантии конструирования бортовой электронной аппаратуры
КТ-254

Зак. 3185
Издание – ОАО «Авиаиздат», 2011