МЕЖГОСУДАРСТВЕННЫЙ АВИАЦИОННЫЙ КОМИТЕТ

АВИАЦИОННЫЙ РЕГИСТР

РУКОВОДСТВО 4761

по методам оценки безопасности систем и бортового оборудования воздушных судов гражданской авиации

2010

Documents
Document Sharing Hub

Full document details: Guidance 4761: Guidelines and...

СОДЕРЖАНИЕ

1. Область применения документа 1
2. Вспомогательные сведения 2
3. Процесс оценки безопасности....6
4. Аналитические методы оценки безопасности 11
5. Задачи и интервалы обслуживания, связанные с безопасностью 15
6. Ограниченная по времени отправки в рейс 16
ПРИЛОЖЕНИЕ A. Оценка функциональной опасности 22
ПРИЛОЖЕНИЕ B. Предварительная оценка безопасности системы 30
ПРИЛОЖЕНИЕ C. Оценка безопасности системы 34
ПРИЛОЖЕНИЕ D. Анализ дерева неисправности 38
ПРИЛОЖЕНИЕ E. Анализ логических схем 76
ПРИЛОЖЕНИЕ F. Марковский анализ 79
ПРИЛОЖЕНИЕ G. Анализ видов и последствий отказа 100
ПРИЛОЖЕНИЕ H. Сводка видов и последствий отказа 109
ПРИЛОЖЕНИЕ I. Зонный анализ безопасности 112
ПРИЛОЖЕНИЕ J. Анализ специфического риска 116
ПРИЛОЖЕНИЕ K. Анализ общего режима 118
ПРИЛОЖЕНИЕ L. Сопровождающий пример процесса оценки безопасности 125

AVA Documents
Document Sharing Hub

Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems...

1 ОБЛАСТЬ ПРИМЕНЕНИЯ ДОКУМЕНТА

В этом документе представлены инструктивные материалы, методы проведения оценки безопасности в обеспечение сертификации гражданского самолета. Методы, изложенные в нем, определяют упорядоченные способы, но не единственные способы, для достижения заданного.

Документ непосредственно относится к демонстрации соответствия требованиям параграфа 25.1309 АП-25. Часть содержащегося материала может применяться и к оборудованию, на которое не распространяются требования параграфа 25.1309. В документе также вводится понятие оценки безопасности на уровне самолета, и рассматриваются средства выполнения этой работы с учетом ожидаемых условий эксплуатации самолета.

Когда проводятся дополнительные сертификационные работы, связанные с внесением изменений в конструкцию самолета или в оборудование, то рассмотренные здесь процессы в большинстве случаев применимы только к новым изделиям или к ранее установленным изделиям, на которые оказывают влияние изменения. В случае применения в новых конструкциях самолетов изделий ранее установленных на других самолетах могут использоваться альтернативные методы определения соответствия, например, опыт эксплуатации.

1.1 Назначение документа

Документ содержит инструктивные материалы по проведению принятой в авиационной отрасли оценке безопасности, которая включает этапы Оценки функциональной опасности, Предварительной оценки безопасности системы и Оценки безопасности системы.

В документе приводится информация по методам анализа безопасности, обеспечивающим проведение оценки безопасности. В состав этих методов включены Анализ дерева неисправности, Анализ логической схемы, Анализ видов и последствий отказов, Сводка анализа видов и последствий отказов, а также Анализ общих причин, состоящий из Анализа зонной безопасности, Анализа специфического риска и Анализа общего режима.

1.2 Ожидаемая аудитория

К ожидаемым пользователям относятся все те специалисты, действия которых затрагивают оценку безопасности самолета и связанные с такой оценкой системы и оборудование, в том числе: конструкторы самолета, системные интеграторы, поставщики оборудования, специалисты по сертификации.

1.3 Как применять этот документ

Инструктивные материалы и методы документа предназначены для использования с другими руководящими документами, к которым относятся Р-4754, КТ-178В, РМ-25.1309 (для изделий применяемых в двигателях и винтах следует обращаться к соответствующим Рекомендательным Материалам).

Документ определяет типовые действия, методы и документацию, которые могут использоваться для характеристики оценок безопасности гражданского самолета и связанных с ним систем и оборудования. Поэтому конкретную реализацию таких действий следует разработать организации, проводящей оценку безопасности и организации получающей эту оценку.

Этот документ содержит общие инструктивные материалы по аспектам оценки безопасности проекта. Основные аналитические методы, реализующие их средства и взаимосвязи, описываются обзорно. Читатели, которым нужна более полная информация по конкретному методу, могут найти ее в Приложениях с А по К. Эти приложения содержат информацию по Оценке функциональной опасности, Предварительной оценке безопасности системы, Оценке безопасности системы, по Анализу дерева неисправности, Анализу логической схемы, Марковскому анализу, Анализу видов и последствий отказов, по Сводке анализа видов, по Анализу зонной безопасности, Анализу специфического риска и Анализу общего режима.

Примечание: *Приложения не являются отдельными документами. Они предназначены для использования вместе с основной частью документа. Читателям не рекомендуется использовать приложения независимо от основной части документа. Более того,*

AVA Documents
Document Sharing Hub

Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Syst...

примеры в приложении L «Сопровождающий пример...» не следует использовать без обращения к соответствующим приложениям и основной части этого документа.

Примеры, приведенные в этом документе, включая примеры документации, должны использоваться только как инструктивные материалы. Эти примеры не следует воспринимать как усиление или дополнения какого-либо требования.

В этом документе и в приложениях в иллюстративных целях применяется Анализ дерева неисправности. Читателям следует понимать, что для достижения той же цели, в зависимости от обстоятельств и желаемого вида данных, можно применять Анализ логической схемы или Марковский анализ.

1.4 Отличия данного документа от ARP 4761

Настоящий документ следует рассматривать как технический перевод документа SAE ARP 4761 "Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment".

В документе сохранены все разделы и подразделы документа ARP 4761.

Раздел 1 дополнен настоящим подразделом.

Подраздел 2.1 содержит ссылки на документы, аналогичные указанным в ARP 4761.

Подраздел 2.2 содержит ряд определений гармонизированных с применяемыми в Руководстве 4754 и Руководстве 254.

Подраздел 2.3 сохранил оригинальную аббревиатуру ряда терминов.

В таблице 1 основной части документа указаны термины и определения АР МАК.

2 ВСПОМОГАТЕЛЬНЫЕ СВЕДЕНИЯ

2.1 Применимые документы

Следующие документы расширяют здесь изложенное:

Руководство 4754 (рабочее название документа).

Руководство 254 (рабочее название документа).

Рекомендательный материал 25.1309 (рабочее название документа).

Квалификационные требования КТ-178В.

2.2 Определения

Примечание: *Приведенные ниже определения распространяются на термины, используемые в этом документе.*

Авиарегистр (Certification authority) – Компетентный орган Межгосударственного авиационного комитета.

Анализ (Analysis) – Оценка, основанная на разложении на простые элементы.

Анализ общих причин (Common cause analysis) – Родовой термин, охватывающий Анализ безопасности зон, Анализ специфического риска и Анализ общего режима.

Аппаратное обеспечение (Hardware) – Физически существующий объект. Применяется, в основном, в отношении блоков, плат, источников питания и т.д.

Валидация (Validation) – Определение того, что требования к продукту достаточно полны и точны.

Верификация (Verification) – Оценка реализации для определения соответствия предъявленным требованиям.

Вид отказа (Failure mode) – Признак проявления отказа объекта.

Documents
Document Sharing Hub
Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Syst...

Власть (Authority) – Организация или лицо уполномоченное Государством для проведения сертификации на соответствие применяемым требованиям.

Время воздействия (Exposure time) – Интервал времени между наиболее поздним моментом, когда было известно о правильном функционировании и моментом, когда снова будет известно о правильном функционировании.

Гарантия (Assurance) – Планируемые и систематические действия, необходимые для обеспечения достаточной степени доверия к тому, что продукт или процесс удовлетворяет данным требованиям.

Гарантия разработки (Development assurance) – Все те планируемые и систематические действия, которые используются для доказательства адекватного уровня доверия к тому, что ошибки разработки выявлены и исправлены так, что система удовлетворяет применимому сертификационному базису.

Доступность (Availability) – Вероятность того, что объект находится в работоспособном состоянии в данном месте в данное время.

Демонстрация (Demonstration) – Метод доказательства соответствия характеристик через наблюдение.

Интервал риска ("At risk" time) – Период времени, в течение которого объект может отказать с возникновением интересующих последствий отказа. Это обычно связано с конечной неисправностью в последовательности неисправностей, ведущей к конкретному отказному состоянию.

Интенсивность отказов (Failure rate) – Производная функции распределения вероятности отказа деленная на функцию распределения надежности к моменту времени t. $\lambda(t)=F'(t)/(1-F(t))$. Если функция распределения вероятности отказа является экспоненциальной, то интенсивность отказов является константой и интенсивность отказов может быть приблизительно определена как отношение числа отказов в рассматриваемом множестве аппаратных объектов на общее число часов эксплуатации. Отметим, что интенсивность отказов может также выражаться в таких единицах, как вероятность на час полета или вероятность на цикл.

Инструктивные материалы (Guidelines) – Рекомендуемые процедуры для достижения соответствия нормативам.

Инспекция (Inspection) – Проверка объекта на соответствие определенному стандарту.

Интеграция (Integration) – (1) Действие, позволяющее элементам объекта работать вместе. (2) Действие по объединению нескольких отдельных функций в одну реализацию.

Компонент (Component) – Любая законченная часть, комбинация частей, модулей или блоков, которые выполняют определенную функцию, необходимую для работы системы.

Критичность (Criticality) – Показатель уровня опасности связанного с функцией, аппаратурой, программным обеспечением и т.д., определяемый при рассмотрении ненормальной работы (этих функций, аппаратуры, программного обеспечения и т.д.) в отдельности, в комбинации или в комбинации с внешними событиями.

Летная годность (Airworthiness) – (1) Характеристика образца авиационной техники, которая обеспечивается реализацией норм летной годности в его конструкции, параметрах и летных качествах. (2) Состояние объекта (самолета, системы самолета или его компонента) в котором он безопасно работает, выполняя назначенные функции.

Надежность (Reliability) – Вероятность того, что объект будет выполнять требуемую функцию в указанных условиях, в установленный период времени без отказа.

Неисправность (Fault) – Нежелаемая аномалия объекта или системы.

Независимость (Independence) – (1) Подход к проектированию, который гарантирует, что отказ одного объекта не вызовет отказ другого объекта. (2) Разделение ответственности, которое гарантирует надлежащую объективность оценки.

Неправильное выполнение функции (Malfunction) – Возникновение условий, когда действия выполняются за установленными пределами.

AVA Documents
Document Sharing Hub

Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Syst...

Новизна (Novelty) – Применяется к системам, использующим новые технологии или к системам, в которых используется общепринятая технология ранее не использованная в отношении решения конкретного вопроса.

Оценка функциональной опасности (Functional hazard assessment) – Систематическая всесторонняя проверка функций для определения и классификации отказных состояний.

Опасность (Hazard) – Возможное небезопасное состояние, возникающее вследствие отказов, неисправностей, внешних событий, ошибок или их комбинаций.

Ошибка разработки (Development error) – Ошибка в определении требований или в проекте.

Ошибка (Error) – (1) Происшествие, возникающее вследствие неправильных действий или решений персонала эксплуатирующего или обслуживающего систему. (2) Ошибка в требованиях, проектировании или реализации.

Общая причина (Common cause) – Событие или отказ, которые обходят или делают недейственными резервирование или независимость.

Отказ общего режима (Common mode failure) – Событие, которое воздействует на несколько элементов, которые в других отношениях рассматриваются независимыми.

Одобрение (Approval) – Акт формального разрешения применения, который выполняется Авиарегистром.

Одобрено (Approved) – Принято Авиарегистром как годное для конкретного использования.

Отказ (Failure) – Событие, заключающееся в переходе к прекращению или неправильному выполнению функции системой или ее частью.

Отказное состояние (Failure condition) – Состояние, возникающее вследствие прямого или косвенного воздействия на самолет или пассажиров в результате одного или более отказов, неправильной эксплуатации или воздействия окружающей среды. Отказное состояние приводит к возникновению особой ситуации, классифицируемой по серьезности ее последствий в соответствии с КТ-178В.

Объект (Item) – Один или несколько аппаратных или программных элементов рассматриваемых как целое.

Оценка (Assessment) – Определение характеристик, основанное на техническом здравом смысле.

Отделение (Segregation) – Обеспечение независимости средствами физического барьера между двумя аппаратными компонентами.

Оценка безопасности системы (System safety assessment) Систематическая, всесторонняя проверка реализованной системы для установления удовлетворения относящихся требований по безопасности.

Предположения (Assumption) – Выражения, принципы и/или предпосылки, предлагаемые без доказательства.

Повреждение (Defect) – Состояние объекта, в котором имеется невыполнение заданных требований к характеристикам объекта. Повреждение может, но не обязательно, приводить к отказу.

Производные требования (Derived requirements) – Дополнительные требования, возникающие при проектировании или реализации решений во время процесса разработки. Производные требования не являются прямо трассируемыми к требованиям более высокого уровня. Несмотря на это, производные требования могут воздействовать на требования более высокого уровня.

Проект (Design) – Результат процесса проектирования.

Процесс проектирования (Design process) – Процесс создания системы или объекта из набора требований.

Последствие отказа (Failure effect) – Описание работы системы или блока после возникновения отказа, то есть указание последствий вида отказа на режим, функцию или состояние системы или объекта.

Documents
Document Sharing Hub
Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Syst...

Предварительная оценка безопасности системы (Preliminary system safety assessment) – Систематическая оценка предполагаемой архитектуры и реализации системы, основанная на Оценке функциональной опасности и классификации отказных состояний, для определения требований по безопасности ко всем объектам.

Продукт (Product) – Объект, создаваемый на основе определенного набора требований.

Подобие (Similarity) – Применяется к системам подобным по характеристикам и использованию относительно систем используемых на ранее сертифицированных самолетах. В принципе, это означает, что в рассматриваемой системе нет составляющих с более высоким риском (в отношении окружающих условий или реализации), и что эксплуатационные нагрузки не больше чем у ранее сертифицированной системы.

Программное обеспечение (Software) – Программы компьютера, процедуры, правила и любая связанная документация, относящаяся к работе компьютерной системы.

Процесс оценки безопасности системы (System safety assessment process) – Полный процесс, применяемый при проектировании системы для установления целей безопасности и демонстрации соответствия требованиям параграфа 25.1309 и другим связанным с безопасностью требованиям.

Реализация (Implementation) – Действия по созданию физической сущности на основе спецификации.

Разделение (Separation) – Обеспечение независимости средствами физического удаления двух аппаратных компонентов.

Резервирование (Redundancy) – Множество независимых средств объединенных для выполнения данной функции.

Риск (Risk) – вероятность возникновения и связанный уровень опасности.

Сертификация (Certification) – (1) Установление соответствия авиационной техники требованиям летной годности и охраны окружающей среды. (2) Официальное признание того, что продукт, услуга, организация или лицо соответствуют применяемым требованиям. Такая сертификация включает в себя действия по техническим проверкам продукта, услуги, организации или лица и формальное признание соответствия применяемым требованиям с оформлением сертификата, лицензии, одобрения или других документов, как это требуется национальными законами и процедурами.

Сложность (Complexity) – Атрибут систем или объектов, который делает трудным понимание их работы. Увеличение сложности системы часто вызвано такими объектами, как нечетко определенные компоненты и множественные взаимосвязи.

Соответствие (Compliance) – Успешное выполнение всех обязательных действий, согласованность между ожидаемым или заданным результатом и действительным результатом.

Согласованность (Conformity) – Взаимное согласие физической реализации объекта и определяющим реализацию документом.

Событие (Event) – Происшествие, которое имеет свою исходную причину вне самолета, такую как атмосферные условия (например, порывы ветра, изменение температуры, обледенение, удары молнии), состояние ВПП, пожар в салоне или в багажном отсеке. Это определение, как оно дано здесь, описывает «внешнее событие». Имеются другие использования термина «событие», которые рассматривают другие аспекты.

Скрытый отказ (Latent failure) – Отказ, который при возникновении не обнаруживается и/или не сигнализируется.

Спецификация (Specification) – Набор требований, когда берутся вместе, то устанавливают критерии, определяющие функции и атрибуты системы или объекта.

Система (System) – Набор взаимодействующих объектов, предназначенный для выполнения конкретных функций.

Требование (Requirement) – Отдельный элемент спецификации, который может быть подтвержден и на соответствие которому может быть проверена реализация.

AVA Documents
Document Sharing Hub

Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Syst...

Уполномоченный орган (Authority) – Организация или лицо уполномоченной Государством для проведения сертификации на соответствие применяемым требованиям.

Функция (Function) – Внешнее проявление свойств какого-либо объекта в данной системе отношений.

Функция обмена (Exchanged function) – Взаимозависимость между функциями.

Примечание: *Термины и определения в области надежности приведены в ГОСТ 27.002-89.*

2.3 Сокращения

FHA	Оценка функциональной опасности
PSSA	Предварительная оценка безопасности системы
SSA	Оценка безопасности системы
FTA	Анализ дерева неисправности
DD	Анализ логической схемы
FMEA	Анализ видов и последствий отказа
FMES	Сводка видов и последствий отказов
CCA	Анализ общих причин
ZSA	Анализ зонной безопасности
PRA	Анализ специфического риска
CMA	Анализ общего режима
PM	Рекомендательный материал
MA	Марковский анализ
CMR	Сертификационные требования по обслуживанию
FADEC	Полностью цифровая система управления двигателем
TLD	Ограниченная по времени отправка в рейс

3 ПРОЦЕСС ОЦЕНКИ БЕЗОПАСНОСТИ

3.1 Обзор оценки безопасности

Процесс оценки безопасности включает определение и проверку требований, что сопровождает действия разработки воздушного судна. Этот процесс обеспечивает методы оценки функций самолета и конструкцию систем, выполняющих эти функции, для определения того, что связанные с ними опасности точно установлены. Процесс оценки безопасности является качественным и может быть количественным.

Процесс оценки безопасности следует планировать и контролировать для получения необходимой гарантии, что все относящиеся особые ситуации были определены, и что все значащие комбинации отказов, которые могут вызвать эти особые ситуации, рассмотрены.

Процесс оценки безопасности для интегрированных систем должен принимать во внимание любые дополнительные усложнения и взаимозависимости, которые возникают вследствие интеграции. Во всех случаях введения интегрированных систем, процесс оценки безопасности является основным действием в установлении приемлемых целей безопасности для систем и определении того, что реализация удовлетворяет этим целям.

Рис. 1 представляет видение сверху процесса оценки безопасности (Оценку функциональной опасности, Предварительную оценку безопасности системы, Оценку безопасности системы) и как методы оценки безопасности применяются в этом процессе. Процесс разработки является интегрированным по своей природе. Процесс оценки безопасности является составной частью процесса разработки. Процесс оценки безопасности начинается на эскизном проекте, для которого формирует требования по безопасности. По мере развития проекта, в него вносятся изменения, и уточненный проект должен быть оценен повторно. Эта повторная оценка может вызвать новые производные требования к проекту. Эти новые требования могут потребовать дальнейших изменений проекта. Процесс оценки безопасности завершается с проверкой того, что проект

AVA Documents
Document Sharing Hub
Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Syst...

соответствует требованиям по безопасности. В верхней части рисунка приведено типовое прохождение цикла разработки для показа хронологической связи процесса оценки безопасности и процесса разработки. Составляющие процесса оценки безопасности, связанные с этапами процесса разработки, показаны в прямоугольниках, чтобы подчеркнуть их взаимосвязь.

Оценка функциональной опасности проводиться в начале цикла разработки самолета/системы. Она позволяет определить и классифицировать отказные состояния, связанные с функциями самолета и комбинациями этих функций. Такая классификация отказных состояний устанавливает цели по безопасности. Такие цели показаны в таблице 1.

Задачей проведения FHA является четкое определение каждого отказного состояния с проверенным обоснованием его классификации. После того как функции уровня самолета в процессе проектирования будут распределены между системами, каждая система, которая будет применяться для выполнения нескольких таких функций, должна быть дополнительно рассмотрена с применением процесса FHA. FHA повторяется рассмотрением единичных отказов или комбинаций отказов функций уровня самолета, которые будет выполнять такая система. Результаты FHA используются как исходное положение для проведения Предварительной оценки безопасности системы.

PSSA является упорядоченной проверкой предполагаемой архитектуры системы для определения того, как отказы системы могут приводить к функциональным опасностям, определенным в FHA. Целью PSSA является установление требований по безопасности системы и определение того, что при реализации предполагаемой архитектуры разумно ожидать выполнение целей безопасности определенных в FHA.

PSSA является итерационным процессом, связанным с развитием проекта. PSSA проводится на многих этапах разработки системы, включая определение характеристик системы, составляющих программного обеспечения и аппаратного обеспечения. PSSA обычно принимает форму Анализа дерева неисправности (может быть использован DD или MA) и включает анализ общих причин.

Оценка безопасности системы является упорядоченной, подробной оценкой реализованной системы для демонстрации того, что цели безопасности определенные в FHA и производные требования по безопасности определенные в PSSA удовлетворяются. SSA обычно основана на FTA, рассматриваемом при выполнении PSSA (может быть использован DD или MA) и использует численные значения, полученные из FMES. В SSA следует проверить, что все значимые проявления отказов, содержащиеся в FMES, рассмотрены на предмет включения в качестве первичных событий в FTA. FMES обобщает отказы, выявленные в FMEA, группируя отказы с учетом их последствий. SSA должна включать относящиеся результаты Анализа общих причин.

Архитектура любой системы устанавливает ее структуру и ограничения, в пределах которых реализуется конкретный проект системы. Анализ общих причин помогает разработать архитектуру конкретной системы и архитектуру сопряженных систем с использованием оценки чувствительности всех архитектур к событиям общей причины. Такие события общей причины оцениваются при выполнении следующих видов анализа: Анализа специфического риска, Анализа зонной безопасности и Анализа общего режима. Результаты Анализа общей причины выполняемого на уровне самолета, рассматриваются в PSSA и SSA каждой системы.

При выполнении FTA как в ходе PSSA, так и ходе SSA, используемые в анализе средства обнаружения отказов, обеспечивающие задачи обслуживания и время воздействия, должны быть согласованы с задачами и интервалами программы наземного обслуживания, применяемой к самолету. Во многих случаях средствами обнаружения отказов будет наблюдение их последствий в кабине экипажа или встроенные средства системы (например, средства тест-контроля, контроля при включении питания и т.д.).

Анализ логических схем принципиально эквивалентен FTA и выбор одного из них определяется предпочтением выполняющего анализ специалиста. Методы Марковского анализа часто применяются при рассмотрении различных сценариев обслуживания. В Приложениях D, E и F перечисляются преимущества использования FTA, DD и MA соответственно.

В процессе оценки безопасности используются не только количественные показатели. В нем рассматриваются такие качественные вопросы как уровни гарантии качества разработки,

AVA Documents
Document Sharing Hub

Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Syst...

поля радиопомех высокой энергии, удары молний и т.п. Многое из этого включено в Анализ общих причин (Приложения I, J и K).

Процесс анализа безопасности завершается, когда результаты SSA верифицированы с материалами FHA уровня системы и самолета.

3.2 Оценка функциональной опасности

Оценка функциональной опасности определяется как упорядоченное всестороннее исследование функций для выявления и классификации их отказных состояний в соответствии со степенью опасности. FHA обычно выполняется на двух уровнях. Эти два уровня анализа известны как FHA уровня самолета и FHA уровня системы.

FHA уровня самолета является качественной оценкой уровня основных функций самолета определенных на начальной стадии его создания. FHA уровня самолета будет выявлять и классифицировать отказные состояния, связанные с функциями уровня самолета. Однако если в отдельных системах используются подобные архитектурные решения или одинаковые, сложные компоненты, а также если вводятся дополнительные отказные состояния уровня самолета рассматривающие несколько функций, то FHA следует видоизменить для выявления и классификации новых отказных состояний. Классификация рассмотренных отказных состояний устанавливает требования по безопасности, которым должен удовлетворять самолет. Задачей проведения такой FHA является четкое определение каждого отказного состояния с последующим логическим обоснованием классификации степени опасности.

FHA уровня системы также является качественной оценкой, которая выполняется итерационно и становится более точной и основательной с развитием системы. В ней рассматриваются отказы и комбинации отказов системы, которые влияют на функции уровня самолета. Оценка любого конкретного объекта программного или аппаратного обеспечения не является задачей FHA уровня системы. Однако если в отдельных системах используются подобные архитектурные решения или одинаковые сложные компоненты, а также если вводятся дополнительные отказные состояния уровня системы, то FHA следует видоизменить для выявления и классификации таких новых отказных состояний. Уровень гарантии разработки функций уровня самолета зависит от степени опасности видов отказов или ошибок разработки этих функций для самолета, экипажа или пассажиров. Уровень гарантии разработки каждого объекта зависит как от архитектуры системы, так и от конечных отказных воздействий объекта на выполняемые системой функции.

После того как функции уровня самолета распределены по системе в процессе проектирования, каждая система, которая объединяет несколько функций самолета, должна быть повторно исследована с использованием процесса FHA уровня системы.

Результаты FHA уровня самолета и/или уровня системы являются отправной точкой для создания и распределения требований по безопасности. Средством создания требований более низкого уровня может служить FTA (DD или MA) на основании материалов FHA (дерево неисправности уровня самолета на основе FHA уровня самолета и дерево неисправности PSSA на основе FHA системы). Эти производные требования следует взять в качестве требований в спецификации самолета и систем. Рис. 2 показывает общую взаимосвязь между FHA/FTA/FMEA. На рисунке показан пример того, как FHA создает события верхнего уровня для FTA. Рисунок поясняет как количественные результаты из FMEA и FTA возвращаются в FTA уровня системы и уровня самолета для демонстрации соответствия численным значениям требований по безопасности из FHA.

Детали выполнения FHA приведены в Приложении A.

3.3 Предварительная оценка безопасности системы

PSSA используется для пополнения перечня отказных состояний и соответствующих требований по безопасности. Эта оценка используется также для демонстрации соответствия системы качественным и количественным требованиям, связанным с различными выявленными опасностями. Процесс PSSA определяет стратегии защиты, учитывает концепции отказобезопасности и архитектурные решения, которые могут потребоваться для соответствия целям безопасности. Процесс должен определить и включить в рассмотрение все предъявляемые

AVA Documents
Document Sharing Hub
Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and...

к системе производные требования по безопасности (например, такие стратегии защиты, как обособление, встроенные проверки, различие конструкции, оперативный контроль, связанные с безопасностью задачи обслуживания и интервалы и т.д.). Результаты PSSA будут использоваться в качестве исходных данных в SSA и в других документах, включая, но не ограничиваясь указанными, требования к системе, требования к аппаратному обеспечению и требования к программному обеспечению.

PSSA является итерационным анализом, входящим во все этапы разработки системы. Процесс PSSA начинается на ранних фазах проекта, когда функции уровня самолета и требования к ним распределяются на уровень систем. Требования уровня системы затем распределяются на составляющие ее объекты и, наконец, требования к объектам распределяются между аппаратным обеспечением и программным обеспечением. Распределение риска между объектами будет формировать требования к надежности аппаратного обеспечения и требования к гарантии разработки для аппаратных средств и программного обеспечения (смотри Руководство 4754). Эти требования и уровни гарантии вносятся в спецификации блоков.

PSSA должна выявлять отказы, приводящие к отказным состояниям определенным в FHA системы. Возможные содействующие факторы, приводящие к отказным состояниям, могут определяться применением FTA, DD, MA или других аналитических методов. Отказы аппаратных средств и возможные ошибки в аппаратных средствах/программном обеспечении, также как и отказы вызываемые общими причинами, должны быть включены в PSSA для выяснения их последствий и определения необходимых требований по безопасности к системе или объекту. Следует обратить внимание на возможные скрытые отказы и связанные с ними времена их воздействия.

Введение в качественной форме в анализ ошибок в аппаратных средствах и программном обеспечении показывает их участие в различных отказных состояниях и может дать ценную информацию для определения Уровней гарантии разработки (смотри Руководство 4754). PSSA также может определить конкретные требования по безопасности для программного обеспечения такие как определение защищаемой области, стратегии обособления и конкретные стратегии верификации. Появление таких требований в анализе должно привести к их введению в требования к системе.

В левой части Схемы оценки безопасности, приведенной на рис. 3 показана рекомендуемая последовательность этапов в процессе PSSA. Не все показанные этапы обязательны в каждой оценке, но необходимость каждого из них должна быть рассмотрена. Ниже описывается левая часть рис. 3. Отметим, что там, где указан FTA, его можно заменить эквивалентным анализом, таким как DD или MA.

У PSSA имеется две основные части исходных данных: данные FHA системы и данные FTA самолета. FHA системы раскрывает отказные состояния и их классификацию, необходимые для последующих этапов. FTA самолета определяет функциональные отказы, приводящие к этим состояниям. FTA самолета дополняется Анализом общих причин для разработки необходимых для FHA системы последствий отказов верхнего уровня. CCA также устанавливает требования к системе, которые необходимо реализовать в ее конструкции, такие как надежность, разделение и независимость функций.

CCA на уровне системы дополняет результаты FTA системы по формированию последствий отказа верхнего уровня для выполнения FTA на уровне блока системы. CCA блока аналогично дополняет FTA блока для дальнейшего установления требований к конструкции, уровню гарантии разработки, к аппаратным средствам и программному обеспечению. Полученные таким образом требования используются для описания проектных требований к аппаратным средствам, программному обеспечению отдельных объектов системы. Результаты PSSA будут определять последствия отказов аппаратных средств, последствия ошибок разработки аппаратных средств и программного обеспечения, показатели надежности и уровни гарантии разработки. В PSSA следует сформировать стратегии защиты и архитектуры, особенности необходимые для соответствия требованиям по безопасности.

Требования по безопасности, полученные из основных событий дерева неисправности PSSA, следует направить специалисту, выполняющему FMEA. Эта информация может быть в форме последствий отказов и допустимых интенсивностей отказов и предназначена для

AVA Documents
Document Sharing Hub
Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Syst...

гарантии рассмотрения в FMEA таких специфических последствий отказов. Эта информация поможет специалистам по FMEA определить направленность и глубину этого анализа.

Более подробно выполнение PSSA описано в Приложении B.

3.4 Оценка безопасности системы

Оценка безопасности системы является методической, всесторонней оценкой созданной системы для демонстрации соответствия относящимся к ней требованиям по безопасности. Процесс анализа системы подобен действиям PSSA, но отличается по назначению. Отличия между PSSA и SSA в том, что PSSA является методом оценки предполагаемых архитектур и разработки требований по безопасности к системе/объекту, тогда как SSA является верификацией того, что реализованный проект соответствует как качественным, так и количественным требованиям по безопасности, определенным в FHA и PSSA.

SSA объединяет результаты различных анализов для проверки безопасности системы в целом и охвата всех конкретных особенностей обеспечения безопасности определенных в PSSA. Процесс документирования SSA включает, при необходимости, доказательства и результаты уместных анализов. Выходной документ SSA может содержать следующую информацию:

a. Перечень одобренных ранее вероятностей внешних событий.

b. Описание системы.

c. Перечень отказных состояний (FHA, PSSA).

d. Классификацию отказных состояний (FHA, PSSA).

e. Качественный анализ отказных состояний (FTA, DD, FMES).

f. Количественный анализ отказных состояний (FTA, DD, MA, FMES).

g. Анализ общих причин.

h. Связанные с обеспечением безопасности задачи и интервалы времени (FTA, DD, MA, FMES).

i. Уровни гарантии разработки для аппаратных средств и программного обеспечения (PSSA).

j. Верификацию того, что требования по безопасности из PSSA учтены в конструкции и/или в процессе испытаний.

k. Результаты не аналитических составляющих процесса верификации (т.е. испытания, демонстрации, инспекционные действия).

В правой части Схемы процесса оценки безопасности (см. рис. 3) показана рекомендуемая последовательность этапов процесса SSA. Не все этапы могут потребоваться для каждой оценки, но каждый из них должен быть рассмотрен на применимость. Далее описывается показанное в правой части рис. 3. Отметим, что там, где показан FTA, он может быть заменен на эквивалентный аналитический метод оценки безопасности, такой как DD или MA.

Движение процесса SSA представлено последовательными уровнями верификации. Поднимаясь по этим иерархическим уровням верификации на соответствие требованиям по безопасности определенным в процессе выполнения PSSA, проверяются надежность элементов аппаратных средств, архитектурные требования, уровни гарантии разработки аппаратных средств и программного обеспечения. Нижний уровень конструкции оценивается также на соответствие производным требованиям. Для проверки соответствия реализации программного обеспечения требуемым, для определения того, что реализация программного обеспечения отвечает требуемым уровням гарантии разработки, следует использовать процедуры, изложенные в КТ-178. Заявителю следует установить соответствующие процедуры гарантии разработки аппаратных средств и согласовать их с Авиарегистром. Уровень гарантии разработки аппаратных средств проверяется на соответствие процедурам, изложенным в Руководстве 254.

Для расчета интенсивности отказов, видов отказов рассматриваемых в FTA/CCA уровня блока, выполняется FMEA уровня блока, результаты которого излагаются в FMES. Результаты FMEA уровня системы суммируются в FMES системы для подтверждения интенсивностей отказов видов отказов, которые рассмотрены в FTA системы. Система оценивается с использованием FTA/CCA

AVA Documents
Document Sharing Hub
Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Syst...

для выявления видов отказов и вероятностей, использованных в FTA уровня самолета. FTA/CCA уровня самолета применяется для установления соответствия отказным состояниям и вероятностям уровня самолета сравнением с результатами FHA уровня самолета. Как только объект введен в систему, а система внесена в конструкцию самолета, последствия отказов сравниваются с отказными состояниями, определенными в FHA. Это сравнение называется «перекрестная проверка интеграции».

Подробности выполнения SSA приведены в Приложении C.

3.5 Методы верификации, применяемые при сертификации самолетов

Для каждого отказного состояния следует определить, каким образом самолет/системы будут удовлетворять цели безопасности. Схема на рис. 4 показывает пути подготовки плана верификации отказных состояний конкретной системы. Категория отказов, приводящих к сложной ситуации, является наиболее трудной категорией для определения порядка оценки. Схема дает некоторые рекомендации по планированию верификации отказов этой категории.

4 АНАЛИТИЧЕСКИЕ МЕТОДЫ ОЦЕНКИ БЕЗОПАСНОСТИ

4.1 Анализ дерева неисправности/Анализ логической схемы/Марковский анализ

Анализ дерева неисправности, Анализ логической схемы и Марковский анализ являются методами анализа сверху-вниз. Эти анализы последовательно рассматривают все более детальные (т.е. более нижние) уровни конструкции.

После определения отказных состояний в FHA, FTA/DD/MA могут использоваться как часть PSSA для определения тех единичных отказов или комбинаций отказов (если имеются) на нижних уровнях, которые могут вызывать каждое конкретное отказное состояние. При проведении FTA/DD/MA следует выполнять проверки, для гарантии того, что все отказные состояния со значащими последствиями рассматриваются в качестве базовых событий в FTA/DD/MA. Базовые события FTA/DD/MA получают их интенсивности отказов из FMEA и/или FMES.

Подробности выполнения FTA приведены в Приложении D. Подробности выполнения DD приведены в Приложении E. Подробности выполнения MA приведены в Приложении F.

4.1.1 Применение FTA/DD/MA

Завершенности FTA/DD/MA содействуют технические и организационные оценки и рассмотрения, потому что в них определены только отказы, которые могут в отдельности или совместно приводить к возникновению нежелательного события верхнего уровня. В противоположность этому FMEA рассматривает только единичные отказы, включая даже те, которые могут не иметь отношение к рассматриваемому состоянию.

FTA/DD/MA содействуют распределению событий уровня системы на события нижнего уровня для упрощения анализа.

FTA/DD/MA могут использоваться для:

a. Назначения величины вероятности для события верхнего уровня.

b. Оценки предполагаемых атрибутов архитектуры системы для установления бюджетов надежности аппаратных средств и уровней гарантии разработки для аппаратных средств и программного обеспечения в процессе PSSA.

c. Рассмотрения влияния изменений конструкции.

d. Определения необходимости изменения конструкции и/или определения особых состояний, которые требуют специального внимания.

e. Доказательства соответствия качественным и/или количественным целям безопасности при выполнении SSA.

f. Обеспечения графического наглядного представления значения программного обеспечения в отношении классификации отказных состояний для события верхнего уровня.

g. Установления задач летного экипажа и технического персонала и необходимых интервалов обслуживания для соответствия требованиям оценки безопасности.

AVA Documents
Document Sharing Hub

Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Syst...

Анализ дерева неисправности использует булевские логические символы для демонстрации связи последствий отказа с видами отказа. Двумя наиболее общими логическими символами являются И-символы и ИЛИ-символы. И-символ представляет условие, когда требуется одновременное наличие всех входных событий для получения выходного события более высокого уровня. ИЛИ-символ представляет условие, когда для получения выходного события более высокого уровня необходимо одно или более входных событий.

DD для демонстрации связи отказов заменяет на схеме логические символы FTA на трассы. Параллельные трассы эквивалентны И-символу, а последовательные трассы эквивалентны ИЛИ-символу.

MA рассчитывает вероятность нахождения системы в различных состояниях как функцию времени. Состояние в модели представляет статус системы в качестве функции дерева отказа, поврежденных компонент и резервирования систем. Переход из одного состояния в другое происходит с заданной скоростью перехода, которая определяет интенсивности отказов компонент и резервирование. Система изменяет состояние вследствие различных событий таких, как отказ компоненты, реконструкция после обнаружения отказа, завершения восстановления и т.д. Каждое изменение состояния является случайным процессом, который представляется отдельным функциональным уровнем. Дифференциальная природа модели ограничивает в ходе анализа вычисления в любой точке до вероятности перехода из одного определенного состояния в другое состояние. Вероятность достижения определенного конечного состояния может быть вычислена по комбинации переходов, необходимых для достижения этого состояния.

4.1.2 Программное обеспечение в FTA/DD/MA

Применяемое в некоторых системах и объектах программное обеспечение может в качественной форме рассмотрено в FTA/DD/MA. В частности FTA/DD/MA может быть необходимым для обеспечения адекватной аналитической видимости проблем безопасности ПО в сложных системах, особенно когда доверие основано на следующих атрибутах безопасности:

a. Системы и объекты, которые обеспечивают необходимую защиту при ошибках ПО (Защита может обеспечиваться как с помощью другого ПО или только аппаратурой).

b. Системы и блоки, в которых ПО обеспечивает необходимую защиту от ошибок в аппаратных средствах и при отказах в аппаратуре.

c. Системы и блоки, в которых ПО обеспечивает защиту от скрытых отказов аппаратуры.

Когда программное обеспечение вводится в дерево неисправности, следует четко указать взаимосвязь между опасными состояниям верхнего уровня и конкретными аномалиями работы ПО. Важно явно определить затрагиваемые функции, и каким образом, и как это осуществляется. Могут быть определены специальные защитные стратегии от различных потенциально воздействующих факторов связанных со специфическим поведением системы при аномалиях ПО. Эти защитные стратегии могут включать архитектурные решения в аппаратных средствах или программном обеспечении и/или специальные действия по верификации, включаемые в ориентируемую на безопасность разработку (смотри Руководство 4754).

Проявление ошибок ПО случайно, но не в том смысле как случайны аппаратурные отказы. В отличие от аппаратурных отказов эти вероятности не могут быть определены. Вследствие этого на дереве неисправности связанные с категориями численные вероятности для ошибок ПО не могут быть указаны. Любой анализ ПО для в FTA должен выражаться в терминах гарантии разработки, обеспечивающей защиту от ошибок ПО. Анализ должен быть оценен на полноту исключительно на качественной основе.

4.1.3 Вероятность среднего времени воздействия

При проведении количественного FTA/DD/MA вероятности оцениваются по интенсивностям отказов и времени воздействия событий. Расчеты вероятности при сертификации гражданских самолетов основываются на средних вероятностях рассчитанных для всех самолетов одного типа. Для цели таких анализов обычно предполагается, что интенсивность отказов постоянная во времени и определяется по достаточно надежным интенсивностям отказов после начальной тренировки до наступления износа. Если рассматриваются интервалы, включающие износ и начальную «тренировку», то следует использовать другие методы, например, ограничение

AVA Documents Document Sharing Hub

Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Syst...

ресурса или улучшение производства. При этом следует применить другие функции распределения (например, Вейбула) или использовать моделирование методом Монте-Карло. Но это остается за пределами целей настоящего документа. В этих анализах (FTA/DD/MA) следует рассчитывать среднюю вероятность возникновения отказного состояния за час полета, при типовой средней продолжительности полета и рассматривая относящие времена воздействия и риски. Более подробное обсуждение точного определения времени воздействия и риска содержится в Приложениях D и F.

При разработке нового самолета, среднее время полета обычно определяется из требований заказчика к самолету. Эта величина является предполагаемой. При модификации существующего самолета можно использовать основанное на данных эксплуатации реальное среднее время полета.

4.2 Анализ видов и последствия отказов

FMEA является систематическим методом анализа снизу-вверх, для определения видов отказов системы, блока или функции и определения воздействия на следующий, более высокий уровень. Он может выполняться на любом уровне в системе (например, на уровне элементов, функций, модуля и т.д.). При использовании функционального подхода в FMEA может качественно анализироваться ПО. Обычно FMEA рассматривает последствия, вызванные единичными отказами.

Назначение FMEA следует координировать с использующим его потребителем. Анализ может быть поэлементным или функциональным. Если интенсивность отказов, полученная при использовании функционального FMEA, обеспечивает соответствие бюджету вероятностей PSSA, то поэлементный FMEA может не потребоваться. Обычно FMEA содержит следующую информацию:

a. Определение компоненты, сигнала и/или функции.

b. Виды отказов и соответствующие интенсивности отказов аппаратных средств (численные или по категориям).

c. Последствия отказа (непосредственные или на следующий более высокий уровень).

d. Обнаруживаемость и методы обнаружения.

FMEA может также содержать следующую информацию:

a. Парирующие действия (т.е. автоматические или ручные).

b. Фазы полета на которых возникает отказ.

c. Серьезность последствий отказа.

FMEA может использоваться совместно с вероятностными методами, такими как FTA и DD, для получения количественного анализа. Кроме того, FMEA может использоваться для дополнения FTA/DD выявлением, при выполнении его снизу-вверх, дополнительного перечня последствий отказов.

Подробности выполнения FMEA приведены в Приложении G.

4.3 Сводка видов и последствий отказов

В FMES группируются единичные виды отказов, которые приводят к одинаковым последствиям (т.е. каждое отдельное последствие отказа является отдельной группой единичных видов отказа). FMES может формироваться из Анализов видов и последствий отказа разработчика самолета, системных интеграторов или поставщиков оборудования.

Кроме того, FMES следует координировать с потребителями для адекватного обращения к необходимым исходным данным для FMES более высокого уровня и/или FTA этапа оценки безопасности системы.

Подробности выполнения FMES приведены в Приложении H.

Documents
Document Sharing Hub
Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and...

4.4 Анализ общих причин

Для удовлетворения требований по безопасности может потребоваться обеспечение независимости между функциями, системами или объектами. Следовательно, требуются гарантии, что такая независимость существует или, что риск, связанный с наличием зависимости, считается приемлемым. Анализ общих причин предлагает методы для проверки такой независимости и /или для выявления конкретных зависимостей.

В частности, CCA определяет отдельные виды отказов или внешние события, которые могут привезти к катастрофическим или аварийным отказным состояниям. Такие события общей причины должны быть предотвращены для катастрофических отказных состояний и должны быть в разработанном бюджете вероятности для аварийных отказных состояний.

Анализ безопасности должен особо уделить внимание изучению неисправностей с общей причиной.

CCA подразделяется на три типа:

a. Анализ зонной безопасности.

b. Анализ специфического риска.

c. Анализ общего режима.

4.4.1 Анализ зонной безопасности

Анализ следует выполнять для каждой зоны самолета. Целью анализа является получение гарантий, что размещение оборудования отвечает требованиям по безопасности в отношении следующего:

a. Основные размещения (размещение следует проверить на применяемые требования к конструкции и размещению).

b. Взаимное нежелательное воздействие систем (последствия отказов оборудования следует рассмотреть с точки зрения их влияния на другие системы и элементы конструкции самолета, которые находятся в их физической области воздействия).

c. Ошибки обслуживания (следует рассмотреть ошибки эксплуатационного размещения и их последствия).

Когда выявлено воздействие, которое может влиять на безопасность, его следует рассмотреть в анализе зонной безопасности. Анализ может привести к перепроектированию или будет показана приемлемость воздействия в ходе соответствующей оценки безопасности.

Подробности выполнения ZSA приводятся в Приложении I.

4.4.2 Анализ специфического риска

Специфические риски определяются как события или воздействия внешние по отношению к рассматриваемой системе (системам), объекту (объектам), которые могут нарушить утверждаемую независимость. Некоторые примеры указанных ниже рисков требуют анализа из-за указаний норм летной годности, другие вызываются по известным экспериментальным воздействиям на самолет или систему.

Типичные риски включают, но не ограничиваются следующим:

a. Пожар.

b. Устройства с высокой энергией.

c. Утечка жидкости.

d. Град, снег, дождь.

e. Столкновение с птицей.

f. Обрыв протектора от шины.

g. Разрыв обода колеса.

Documents
Document Sharing Hub
Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Syst...

h. Удар молнии.

i. Радио поля высоких энергий.

j. Расцепление валов.

После определения соответствующих рисков для рассматриваемой конструкции, каждый риск следует сделать объектом специального изучения для проверки и документирования его одновременных или каскадных эффектов.

Целью анализа является получение гарантии, что любой связанный с безопасностью эффект устраним или его риск (вероятность) приемлем.

Подробности выполнения PRA приведены в Приложении J.

4.4.3 Анализ общего режима

Анализ выполняется для проверки того, что И-события в FTA/DD и MA являются независимыми в существующей реализации. Анализируются воздействия ошибок проектирования, производства, обслуживания и отказы компонент систем, которые разрушают такие независимости. Следует рассматривать независимость функций и их средств контроля. Объекты с одинаковыми аппаратными средствами и/или программным обеспечением могут быть чувствительны к возникновению отказов, которые могут вызывать нарушения функций во многих объектах.

Отказы общего режима могут разделяться на несколько категорий, которые следует проанализировать. Указанные ниже, являются примерами отказов общего режима:

a. Ошибка в аппаратуре.

b. Ошибка в ПО.

c. Отказ в аппаратуре.

d. Брак производства/ремонта.

e. Нагрузки, связанные с ситуацией (т.е. аномальные условия полета или аномальные конструкции системы).

f. Ошибка размещения.

g. Ошибка в требованиях.

h. Факторы внешней среды (т.е. температура, вибрация, влажность и т.д.).

i. Каскадные отказы.

j. Отказы общего внешнего источника.

Подробности выполнения CMA приводятся в Приложении K.

5 ЗАДАЧИ И ИНТЕРВАЛЫ ОБСЛУЖИВАНИЯ, СВЯЗАННЫЕ С БЕЗОПАСНОСТЬЮ

Расчет вероятности события, связанного с отказным состоянием должен учитывать время, в течение которого скрытые отказы могут существовать без их обнаружения.

Во многих случаях отказы обнаруживаются наблюдениями летного экипажа или в ходе периодических тестов включения или самоконтроля. Скрытый период для таких отказов короток. Однако в некоторых случаях время воздействия для скрытых отказов связано с проверками оборудования в мастерской или со специфическими задачами обслуживания самолета. В таких случаях скрытый период может быть величиной, которую следует учитывать.

Интервалы времени и задачи обслуживания, которые определяются в ходе PSSA и SSA с использованием FTA, DD, MA или других подобных анализов, являются предполагаемыми сертификационными требованиями обслуживания. Когда выявление отказов связано с задачей обслуживания самолета, интервалы времени для соответствия цели безопасности должны быть направлены в соответствующее подразделение обслуживания для реализации требуемых процедур и периодов времени. Некоторые проверки обслуживания, связанные с удовлетворением требований по безопасности, могут быть назначенными сертификационными требованиями

AVA Documents
Document Sharing Hub

Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Syst...

по обслуживанию. CMR являются обязательной периодической задачей, требуемой для сохранения безопасности самолета, установленной при сертификации самолета, как эксплуатационное ограничение сертификата типа.

Важно отметить, что CMR разрабатываются для целей обеспечения безопасности, по эксплуатационным и экономическим причинам, включая задачи предупредительного Обслуживания, выполняемые до проявления отказа, и задачи поиска отказа. С другой стороны CMR являются только задачами по обнаружению отказов и существуют только для ограничения воздействия других скрытых отказов.

CMR разрабатываются для проверки того, произошли или нет отдельные отказы, и не несут никакой функции упреждающего Обслуживания.

В процессе разработки CMR могут проверяться пути проявления отказа с использованием критерия «следующий отказ» (т.е., что наиболее серьезное может произойти, если произойдет первый отказ).

После утверждения, CMR являются требуемыми задачами обслуживания и должны выполняться эксплуатантом в назначенные интервалы, определенные из анализа безопасности, для сохранения Сертификата летной годности самолета.

Если методом обнаружения является испытание, то должны быть гарантии, что процедуры испытания на самом деле обнаруживают рассматриваемые скрытые отказы.

Основной целью проектирования любой системы должна быть минимизация числа CMR, с отсутствием в идеальном случае.

6 ОГРАНИЧЕННАЯ ПО ВРЕМЕНИ ОТПРАВКИ В РЕЙС

В этом разделе обсуждается метод, используемый для определения и контроля требований по возможности отправки в рейс для полностью цифровой системы управления двигателем. Здесь это приводится только для прояснения предпосылок концепции.

Концепция TLD делает возможным получение выгод от любого имеющегося резервирования, при планировании действий по обслуживанию на специфических интервалах ранее, чем возможные убытки от задержек и отмен, если будет требоваться, что все неисправности устранены перед следующим полетом. Эксплуатация TLD сохраняет средний уровень безопасности. Рекомендуемый процесс одобрения TLD операции требует дополнительных критериев для уменьшения рисков в конкретной конфигурации отправки в рейс.

Ниже рассмотрен пример применения этой концепции к двигателю. В принципе это может применяться к любой системе, которая проектируется с использованием резервирования.

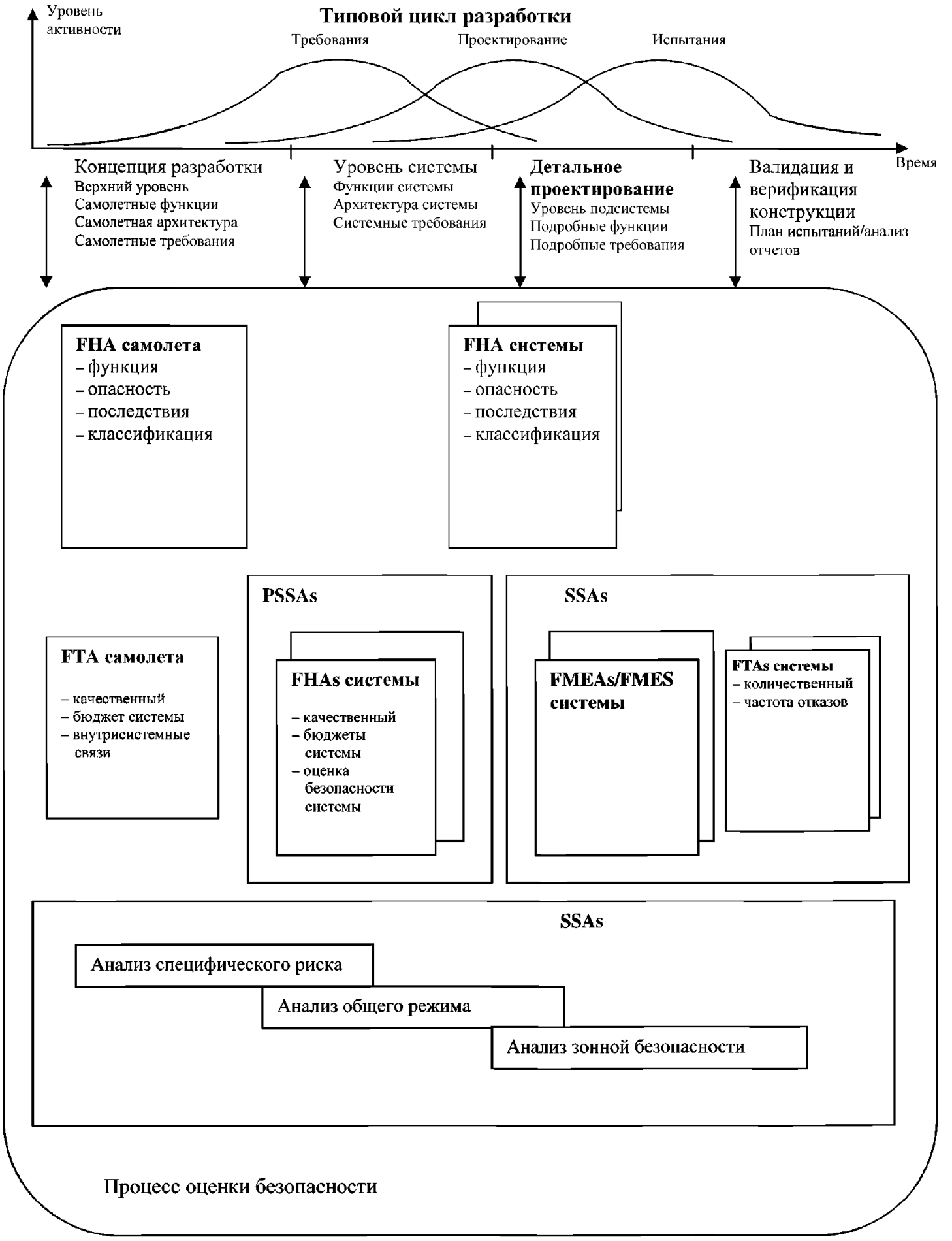
6.1 Применение к FADEC

Концепция применяется в двухканальной системе FADEC с позиций отказного состояния в виде потери тяги одного двигателя.

Эксплуатация по принципу TLD зависит от результата эксплуатации системы и надежности, достаточных для удовлетворения требований по безопасности сертифицирующих авиационных властей. Перечень, показывающий какие отказы появляются в каждой конфигурации отправки и допустимые времена отправления, должен быть одобрен сертифицирующими авиационными властями.

Более подробно о методах для определения интервалов времени, в течение которого самолет может быть отправлен в рейс указано в соответствующем документе SAE. Этот документ будет описывать использование MA и аналитических расчетов для определения периодов времени в течение которых самолет может вылетать с известными неисправными блоками системы управления двигателем. *(Примечание. Методы описаны в документе ARP 5107A от 2005-01).*

Documents
Document Sharing Hub
Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Syst...



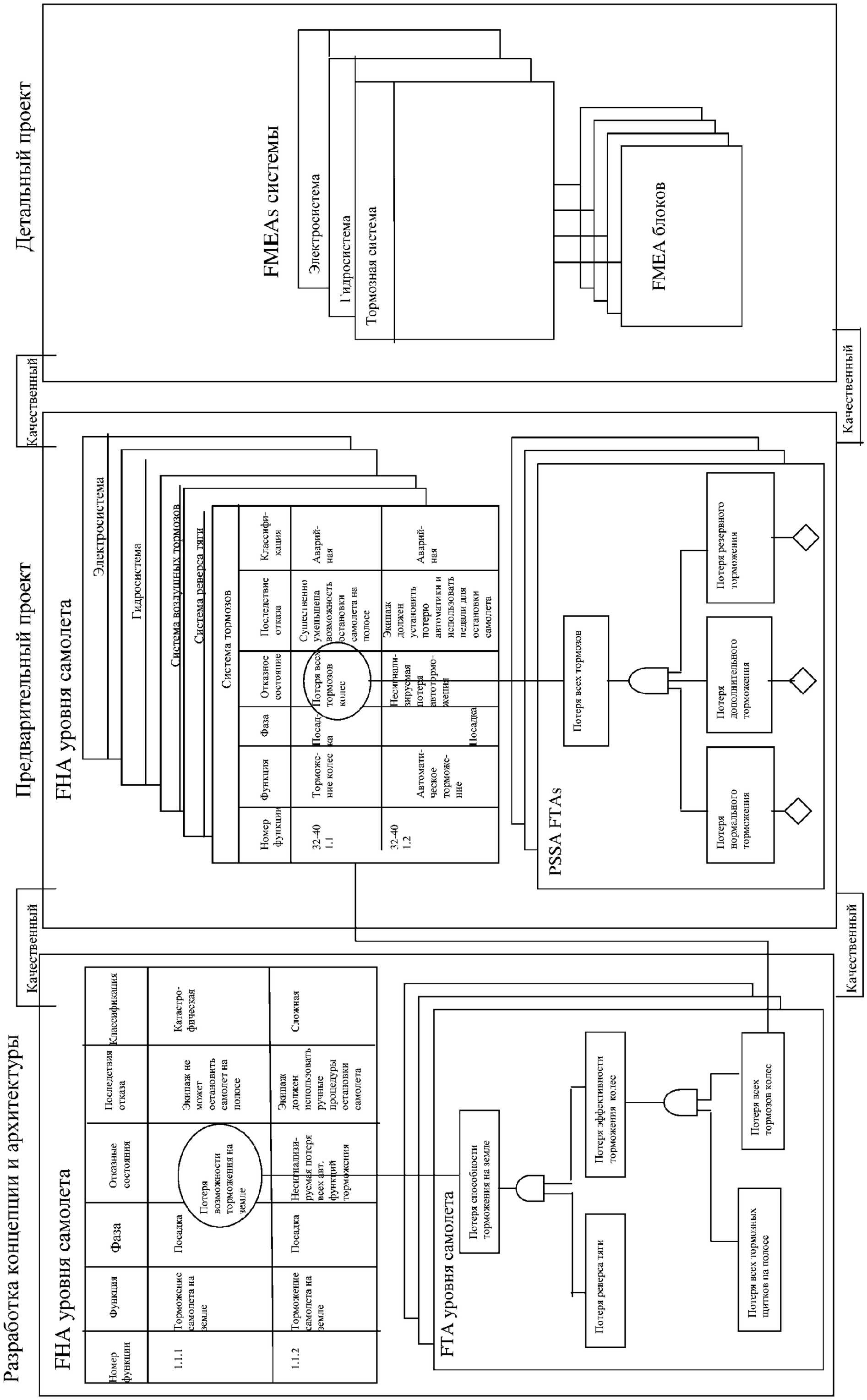
Обзор процесса оценки безопасности
Рис. 1

Documents
Document Sharing Hub
Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment

Таблица 1. Последствия отказных состояний в зависимости от величины вероятности и уровня гарантии качества разработки

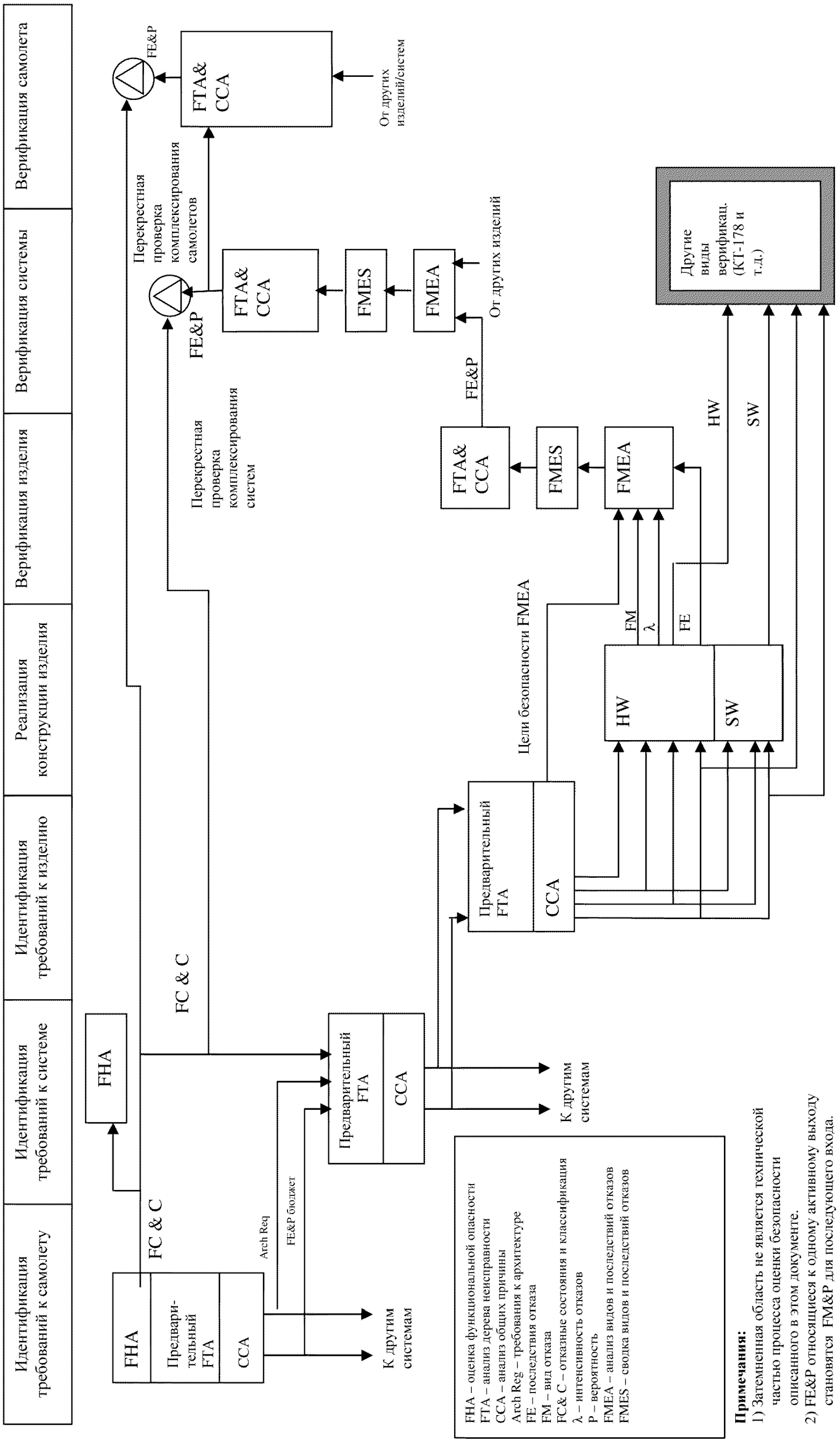
Вероятность (численные значения)	На час полета 1.0	1.0E-3	1.0E-5	1.0E-7	1.0E-9
Вероятность (качественная)	FAA	Вероятный	Маловероятный		Практически невероятный
	APMAK&JAA	Частый / Умеренно вероятный	Маловероятный	Крайне маловероятный	Практически невероятный
Классификация отказных состояний	FAA	Незначительное	Сложное	Опасно сложное	Катастрофическое
	APMAK&JAA	Незначительное	Сложное	Аварийное	Катастрофическое
Последствия отказных состояний	FAA&JAA	– небольшое уменьшение границ безопасности; – небольшое увеличение нагрузки экипажа; – некоторое неудобство для лиц находящихся на борту.	– существенное сокращение запаса безопасности или функциональных возможностей; – значительное увеличение рабочей нагрузки экипажа или условия влияющие на эффективность работы экипажа; – некоторый дискомфорт для лиц находящихся на борту.	– значительное сокращение запаса безопасности или функциональных возможностей; – высокая рабочая нагрузка или такое физическое состояние, которое не дает экипажу выполнять задачи точно или полностью; – существенное влияние на лиц находящихся на борту.	– все отказные состояния, которые препятствуют продолжению безопасного полета и посадки.
	APMAK	– незначительное ухудшение характеристик; – незначительное увеличение рабочей нагрузки на экипаж (например, изменение плана полета).	– заметное ухудшение характеристик и (или) выход одного или нескольких параметров за эксплуатационные ограничения, но без достижения предельных ограничений; – уменьшение способности экипажа справиться с неблагоприятными условиями (возникшей ситуацией) как из-за увеличения рабочей нагрузки, так и из-за условий, понижающих эффективность действий экипажа.	– значительное ухудшение характеристик и (или) достижение (превышением) предельных ограничений; – физическое утомление или такая рабочая нагрузка на экипаж, что уже нельзя полагаться на то, что он выполнит свои задачи точно или полностью.	при возникновении предотвращение гибели людей оказывается практически невозможным.
Уровень гарантии качества разработки	P-4754	Уровень D	Уровень C	Уровень B	Уровень A

Documents
Document Sharing Hub
Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment



Пример взаимосвязи FHA и FTA/FMEA
Рис. 2

Documents
Document Sharing Hub
Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment

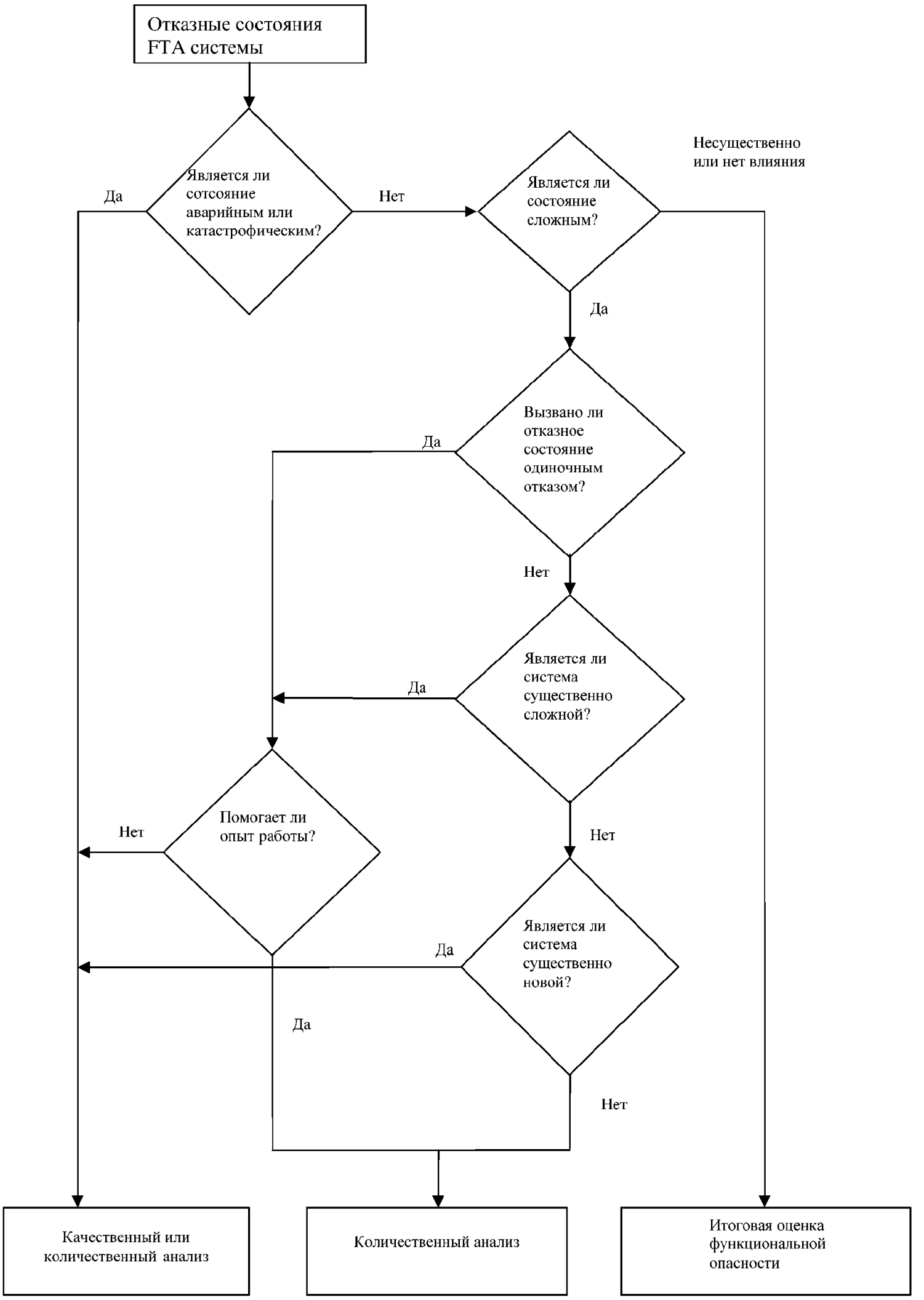


Примечания:

1) Затемненная область не является технической частью процесса оценки безопасности описанного в этом документе.
2) FE&P относящиеся к одному активному выходу становятся FM&P для последующего входа.
3) FTA эквивалентны DD и MA.

Блок схема оценки безопасности
Рис. 3

Documents
Document Sharing Hub
Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment



Пути подготовки плана верификации безопасности
Рис. 4

Documents
Document Sharing Hub
Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment

ПРИЛОЖЕНИЕ А

Оценка функциональной опасности

Примечание: *Основной текст документа дает общее представление об информации, которая содержится в этом приложении. Это приложение следует использовать совместно с основным текстом документа.*

А.1 ВВЕДЕНИЕ

Целью FHA является рассмотрение функций на наиболее приемлемом уровне, выявление и классификация возникающих отказных состояний вследствие как потери функций, так и их неправильного выполнения. FHA должна выявлять отказные состояния для каждого этапа полета, если воздействие отказа и классификация состояния изменяется от одного этапа к другому. FHA устанавливает также производные требования по безопасности, которые необходимы для ограничения воздействия нарушений функций влияющих на классификацию отказных состояний. Эти требования могут выражаться в виде ограничений на проектирование, необходимости сигнализации об отказных состояниях, рекомендуемых действий летному экипажу или техническому персоналу и т.д. Эти требования могут распространяться на одну или несколько систем. Все требования по безопасности должны прослеживаться к каждому уровню их формирования и подтверждаться на нем. Хорошим способом достижения этого может быть подготовка таблицы производных требований, основанных на проектных решениях. Как только определены требования верхнего уровня, они могут использоваться для разработки требований нижнего уровня, как часть процесса PSSA для систем или компонент. Этот процесс продолжается итеративно, пока не будет завершен процесс проектирования.

Оценка функциональной опасности может выполняться на двух уровнях – на уровне самолета и на уровне системы. Выполняемые на этих двух уровнях FHA, используют одни и те же принципы.

Выполнение FHA на высшем приемлемом уровне зависит от полноты знаний и опыта, и может потребовать консультаций с большим числом специалистов. В таблице А1, в качестве примера, содержатся функции высокого уровня и связанные отказные состояния, которые могут рассматриваться при выполнении FHA.

Таблица А1

Функция	Отказное состояние
Управление траекторией полета	Невозможность управления траекторией полета
Управление посадкой и пробегом	Невозможность управления посадкой и пробегом
Управление тягой двигателей	Невозможность управления тягой двигателей
Управление средой в кабине экипажа	Невозможность управления средой в кабине экипажа
Обеспечение пространственной ориентации	Невозможность обеспечения пространственной ориентации
Защита от пожара	Потеря защиты от пожара

Эти отказные состояния могут быть многократно разложены на компоненты с использованием FHA и деревьев неисправности. Например, отказное состояние «невозможность управления траекторией полета» может быть разложено следующим образом:

a. Невозможность управления траекторией полета

(1) Потеря балансировки:

AVA Documents Document Sharing Hub

Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Syst...

(a) Потеря ручной балансировки.

(b) Потеря балансировки топливом.

(c) Другое.

(2) Произвольная балансировка.

(3) Потеря всех гидросистем.

(4) Потеря системы управления полетом.

(5) Неисправная работа системы управления полетом:

(a) Активный отказ в канале руля высоты.

В конечном счете, должны быть определены все влияющие на безопасность отказные состояния совместно с относящимися условиями обеспечения безопасности и предполагаемыми методами оценки соответствия. Для требований по безопасности на уровне самолета методы оценки соответствия следует определить при выполнении FHA на уровне самолета. Для требований по безопасности на уровне системы, методы оценки соответствия следует показать при выполнении PSSA.

FHA на уровне самолета следует использовать для выявления таких возможных отказных состояний одновременно в нескольких системах, которые могут приводить к более опасной классификации результирующего отказного состояния, чем в случае выполнения анализа полагающегося на независимость систем.

Желательно подготовить базовый перечень функциональных опасностей на уровне самолета, который мог бы использоваться в дальнейших проектах для того чтобы не были пропущены известные функциональные опасности. Если такой перечень уже существует, то его следует использовать для перекрестной проверки при разработке FHA на уровне самолета.

A.2 ТРЕБОВАНИЯ К ВЫПОЛНЕНИЮ FHA

FHA является первым шагом в процессе оценки безопасности, который выполняется в проектах создания новых или модифицированных самолетов. FHA устанавливает требования по безопасности для новой или модифицированной конструкции.

A.3 ВЫПОЛНЕНИЕ FHA

Процесс FHA использует подход сверху-вниз для идентификации функциональных отказных состояний и оценки их последствий.

Оценка выполняется в следующем порядке:

a. Идентифицируются все функции, относящиеся к уровню рассмотрения (внутренние функции и функции обмена).

b. Идентифицируются и описываются отказные состояния, связанные с этими функциями, при рассмотрении одиночных и множественных отказов в нормальных и в аварийных/ненормальных условиях эксплуатации.

c. Определяются последствия отказных состояний.

d. Отказные состояния классифицируются в соответствии с последствиями на уровне самолета (катастрофическое, аварийное, сложное, усложнение условий полета и без последствий).

e. Назначаются требования к отказным состояниям, подлежащие рассмотрению на более низком уровне.

f. Определяются вспомогательные материалы, необходимые для подтверждения классификации последствий каждого отказного состояния.

g. Определяются методы проверки соответствия требованиям к отказным состояниям.

На рис. A1 и рис. A2 показаны действия процессов FHA уровня самолета и уровня системы соответственно.

Documents
Document Sharing Hub
Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems...

А.3.1 Идентификация функций

Следует идентифицировать все функции, связанные с уровнем рассмотрения, как внутренние функции, так и функции обмена. Эти функции идентифицируются, в процессе сбора необходимых исходных данных и последующего формирования перечня функций.

А.3.1.1 Сбор необходимых исходных данных

Первый шаг в выполнении FHA - это сбор необходимых исходных данных.

К исходным данным для FHA на уровне самолета можно отнести:

a. Перечень функций самолета верхнего уровня (например, создание подъемной силы, тяги, и т.д.).

b. Цели самолета и требования заказчика (например, число пассажиров, дальность, и т.д.).

c. Начальные (исходные) проектные решения (например, число двигателей, обычный хвост, и т.д.).

К исходным данным для FHA на уровне системы можно отнести:

a. Перечень основных рассматриваемых функций.

b. Функциональную схему, показывающую внешние интерфейсы.

c. Перечень функций, сформированных при выполнении FHA проекта более высокого уровня.

d. Перечень отказных состояний, идентифицированных при выполнении FHA более высокого уровня.

e. Требования, определенные в документах с целями и требованиями к конструкции.

f. Варианты конструкции, выбранные на более высоком уровне, и их обоснование.

А.3.1.2 Формирование перечня функций

Формирование перечня функций в FHA начинается с рассмотрения перечня ожидаемых функций и документов с исходными данными.

После того как на уровне самолета или системы выполнено распределение функций между аппаратными средствами и программным обеспечением, необходимо включить в перечень новые функции, порожденные принятым архитектурным проектным решением. Это выполняется перечислением всех функций аппаратных средств или программного обеспечения и контролем того, что все эти функции включены в перечень функций на уровне самолета или системы. В ходе этого процесса идентифицируются два типа функций:

a. Внутренние на рассматриваемом уровне функции (внутренние функции).

   (1) На уровне самолета к ним относятся основные функции самолетных систем и функции обмена между внутренними системами самолета.

   (2) На уровне системы к ним относятся функции рассматриваемой системы и функции обмена составляющего оборудования системы.

b. Внешние к рассматриваемому уровню функции (функции обмена).

   (1) На уровне самолета – это функции взаимодействия с другим самолетом или с наземными системами.

   (2) На уровне системы, для любой взятой системы, – это функции, которые или выполняются другими системами или выполняются данной системой для других систем (включая другие самолетные системы или наземные системы).

А.3.2 Идентификация и описание отказных состояний

Процесс идентификации отказных состояний начинается с создания перечня вариантов окружающих условий и аварийных конфигураций. Затем, рассматриваются все пункты перечня внутренних функций, перечня функций обмена и перечня вариантов окружающих условий

AVA Documents Document Sharing Hub

Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Syst...

и аварийных/ненормальных конфигураций. Затем создается перечень отказных состояний для самолета или системы рассмотрением единичных и множественных отказов в нормальных и ухудшенных окружающих условиях. Порождая эти отказные состояния и предположения об условиях их возникновения, необходимо учитывать возможные виды каждого отказа. Следует предусмотреть рассмотрение отказных состояний на различных этапах полета, если их критичность меняется с изменение этапов полета.

A.3.2.1 Перечень вариантов окружающих условий и аварийных конфигураций

В дополнение к перечню функций по A.3.1.2, необходимо перечислить условия внешней среды, которые должны рассматриваться при определении последствий отказов. Примерами условий внешней среды, рассматриваемых на уровне самолета являются следующие:

a. Погодные условия.

b. Электромагнитное поле высокой интенсивности.

c. Вулканический пепел.

Необходимо также перечислить конфигурации самолета, которые возникают при аварийных/ненормальных условиях и должны быть рассмотрены при определении последствий отказа. Примерами аварийных/ненормальных условий на уровне самолета/системы являются следующие:

a. Вынужденная посадка.

b. Отказ двигателя.

c. Потеря связи.

d. Разгерметизация.

Для FHA уровня системы этот перечень получается из соответствующего перечня, исходящего из FHA уровня самолета или FHA предшествующего уровня с учетом архитектурных решений проекта, сделанных в течение начальной фазы разработки.

Примерами аварийных/ненормальных условий, которые на уровне системы добавляются к вышеуказанному перечню, являются следующие:

a. Потеря гидросистемы.

b. Потеря системы электроснабжения.

c. Потеря системы охлаждения.

A.3.2.2 Определение отказного состояния при рассмотрении одиночных и множественных отказов

Формирование перечня одиночных отказов включает исследование первоначального перечня, полученного на предыдущем шаге, дополненное анализом конструкции созданной на начальном этапе разработки. Формирование перечня множественных отказов является более трудоемкой работой и требует понимания интеграции компонентов системы и взаимодействия анализируемой системы с другими системами самолета. Этому процессу помогает понимание архитектуры самолета и системы. Множественные отказы рассматриваются в тех случаях, когда последствие некоторого отказа зависит от работоспособности другой системы.

Типичными одиночными отказными состояниями являются следующие:

a. Потеря функции.

b. Несигнализируемая потеря функции.

c. Неисправное выполнение функции.

Типичными множественными отказными состояниями являются следующие:

a. Потеря двух гидросистем, при наличии на самолете трех гидросистем.

b. Потеря связи и потеря навигации.

Documents
Document Sharing Hub

Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems...

А.3.3 Определение последствий отказных состояний

Необходимо определить последствия отказного состояния для самолета, экипажа и пассажиров. При классификации последствий отказных состояний следует консультироваться с персоналом, обладающим эксплуатационным опытом. Непосредственно это может быть выполнено при выполнении FHA на уровне самолета. В случае выполнения FHA уровня системы, последствия на уровне самолета могут быть такими же, как и на уровне системы, или для определения последствия отказного состояния системы могут рассматриваться комбинированные воздействия других систем, которые выполняют такие же самолетные функции.

А.3.4 Классификация последствий отказных состояний

Классификация выполняется на основе анализа эксплуатационных данных об авиационных происшествиях, рассмотрения нормативных руководящих материалов, использования предыдущего опыта разработок, и консультаций с летными экипажами, если это необходимо. Последствия классифицируются как катастрофическое, аварийное, сложное, усложнение условий полета и без последствий (см. таблицу 1 основной части документа).

Следует сохранять документы со вспомогательными данными (анализы, исследования, испытания, и т.д.), которые использовались при выявлении и классификации отказных состояний, чтобы гарантировать трассируемость полученных результатов в будущих работах.

А.3.5 Назначение требований к вероятности отказных состояний, подлежащих рассмотрению на более низком уровне

Для каждого отказного состояния необходимо назначить требования к вероятности возникновения и соответствующие требования к гарантии качества разработки. Эти требования принимают вид записанных в спецификациях требований (требования к самолету, требования к системе, требования к объекту).

А.3.6 Определение вспомогательных материалов, необходимых для подтверждения классификации последствий отказного состояния

Для тех последствий отказных состояний, которые не очевидны, следует определить вспомогательные материалы, обеспечивающие подтверждение сделанной классификации (например: моделирование, исследования, летные испытания).

А.3.7 Определение методов верификации соответствия требованиям к отказным состояниям

Для каждого отказного состояния следует определить, каким образом будет показано, что самолет/система удовлетворяют цели безопасности. Блок-схема, приведенная на рис. 3 основной части документа, дает руководящие указания для определения необходимого подхода к верификации цели безопасности исследуемого отказного состояния.

А.3.8 Предыдущий опыт

После разработки перечня отказных состояний и их классификации, сделанное целесообразно сопоставить с перечнями предыдущих подобных проектов. Это может служить дополнительной защитой от пропуска некоторых редковстречаемых отказных состояний. Кроме того, может быть полезным разработка и сопровождение универсального перечня, как контрольного перечня, используемого при проверках в процессе FHA.

А.4 ВЫХОДНЫЕ ДАННЫЕ

А.4.1 Документация

Результаты процесса FHA следует задокументировать таким образом, чтобы обеспечивалась трассируемость отчета с этапами выполнения FHA. В процессе FHA следует задокументировать следующую информацию:

a. Перечень исходных функций для выполнения FHA.

b. Перечень вариантов окружающих условий и аварийных конфигураций.

AVA Documents Document Sharing Hub

Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Syst...

c. Производные требования по безопасности для каждого уровня проекта.

d. Отчет по FHA содержащий:

(1) Описание функции.

(2) Отказные состояния.

(3) Фазы эксплуатации.

(4) Воздействие отказного состояния на самолет, экипаж и пассажиров.

(5) Классификацию отказного состояния.

(6) Перечисление вспомогательных материалов.

(7) Метод верификации (для проектных решений, которые выбраны для удовлетворения требований по безопасности).

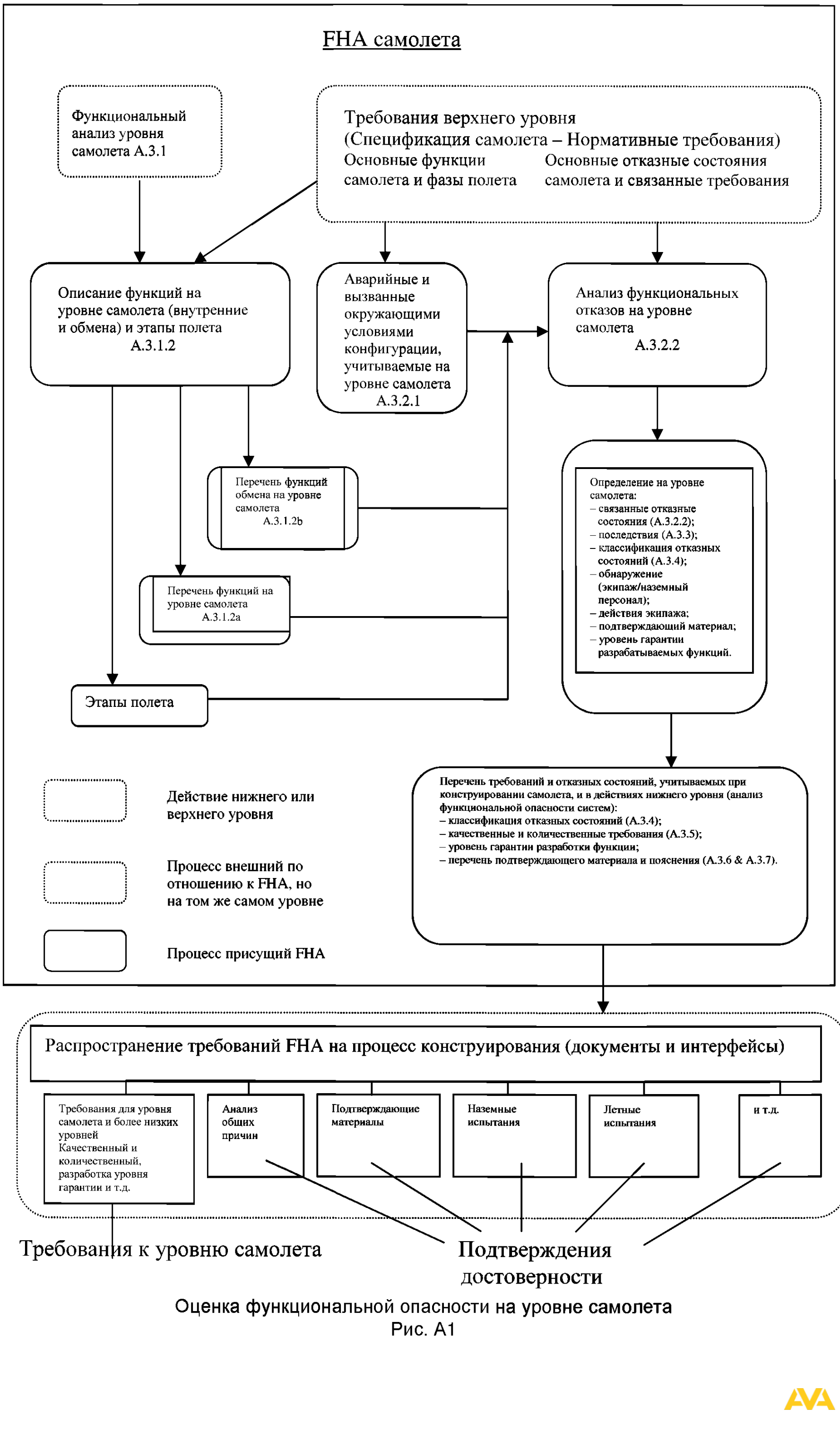
A.4.2 Связь FHA с PSSA

Результаты FHA уровня самолета и соответствующие самолетные деревья неисправности являются исходными данными для FHA уровня системы.

Глубина процесса PSSA может быть различной в зависимости от конструкции, сложности и классификации отказных состояний анализируемой системы.

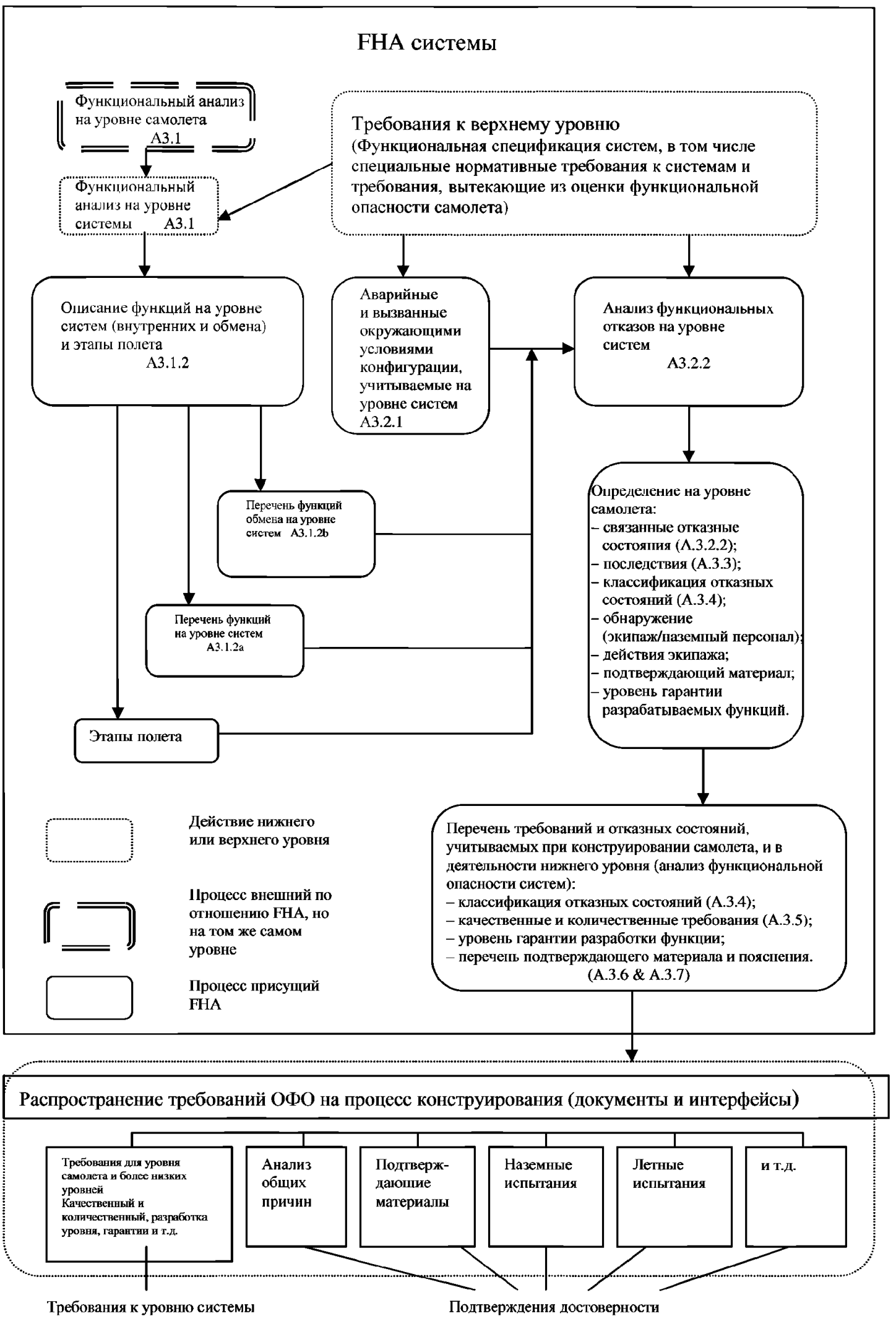
Глубина этапа PSSA определяется FHA уровня системы (т.е. классификацией отказных состояний) и предполагаемым проектным решением (сложностью, новизной и интеграцией). С увеличением критичности и/или сложности конструкции увеличивается глубина оценки/анализа.

Documents
Document Sharing Hub
Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Syst...



Оценка функциональной опасности на уровне самолета
Рис. A1

Documents
Document Sharing Hub
Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment



Оценка функциональной опасности на уровне систем
Рис. А2

Documents
Document Sharing Hub
Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment

ПРИЛОЖЕНИЕ B

Предварительная оценка безопасности системы

Примечание: *Основной текст документа дает общее представление об информации, которая содержится в этом приложении. Это приложение следует использовать совместно с основным текстом документа.*

B.1 ВВЕДЕНИЕ

Процесс предварительной оценки безопасности системы является систематическим исследованием предполагаемой архитектуры системы для определения того, каким образом отказы могут приводить к полученным в ходе FHA функциональным опасностям и как могут удовлетворяться соответствующие требования по безопасности. Процесс PSSA связан с разработкой конструкции системы и является итерационным, поскольку итерационным является процесс проектирования. Процесс PSSA проходит через весь цикл проектирования.

Для каждой анализируемой системы PSSA обращается ко всем значительным отказным состояниям, идентифицированным при проведении FHA. Методы анализа могут быть как качественные, так и количественные.

PSSA может выполняться более чем на одном уровне. Самый высокий уровень PSSA разрабатывается на основе FHA уровня самолета и/или уровня системы. Более низкий уровень PSSA разрабатывается исходя из выходных данных PSSA более высокого уровня.

В этом приложении используется Анализ дерева неисправности. Читателям должно быть понятно, что для достижения той же цели, в зависимости от обстоятельств и исходных данных, может использоваться Анализ логической схемы или Марковский анализ.

B.2 ТРЕБОВАНИЕ ПО ВЫПОЛНЕНИЮ PSSA

Решение о проведении PSSA зависит от архитектуры системы, сложности, серьезности отказных состояний и их последствий, а также от типа функций, которые выполняет анализируемая система. Требование по выполнению PSSA должно быть установлено на основе результатов FHA уровня самолета или уровня системы в соответствии с подходом к верификации описанном на рис. 4 основного текста документа.

B.3 ПРОЦЕСС PSSA

Предварительная оценка безопасности системы использует нисходящий подход для того, чтобы определить, каким образом отказы могут приводить к функциональным опасностям, идентифицированным в FHA и как могут быть удовлетворены требования FHA. Эта оценка делается выполнением следующих процессов:

a. Формирование полного перечня требований по безопасности уровня самолета и уровня системы.

b. Определение приемлемости ожидания соответствия целям и требованиям по безопасности при имеющейся архитектуре и планируемом подходе к проектированию.

c. Формирование требований по безопасности для конструкции объектов более низкого уровня (аппаратных средств и программного обеспечения), для размещения на самолете самой системы и других систем и для эксплуатации (задачи полета и обслуживания).

На рис. B1 показано прохождение PSSA.

B.3.1 Формирование полного перечня требований по безопасности уровня самолета и уровня системы

Процессы FHA/CCA уровня самолета создают начальный набор требований по безопасности для конструкции самолета. Точно так же процессы FHA/CCA уровня системы создают начальный набор требований по безопасности для системы. Формирование полного перечня требований к системе выполняется объединением в ходе PSSA этих начальных наборов требований по безопасности и рассмотрением принятых конструктивных/архитектурных решений.

AVA Documents
Document Sharing Hub
Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Syst...

B.3.1.1 Получение необходимых исходных данных

Входными данными PSSA являются результаты FHA уровня самолета и/или системы, результаты предварительного CCA и описание каждого варианта архитектуры рассматриваемой системы. Для каждого варианта архитектуры эти данные могут включать:

a. Отказные состояния и требования, идентифицированные в FHA уровня самолета и/или системы.

b. Описание архитектуры системы и объяснение ее выбора.

c. Перечень и функции оборудования системы.

d. Интерфейсы системы и связи с другими системами.

e. Результаты предварительного CCA:

(1) Результаты ZA.

(2) Внешние угрозы из PRA.

(3) Результаты CMA.

Для каждого рассматриваемого в PSSA варианта архитектуры следует подтвердить применимость предположений, которые сделаны при выполнении FHA уровня самолета/системы.

B.3.1.2 Комплектация требований по безопасности системы

Реализация функций в архитектуре системы и в отдельных частях (аппаратные средства или программное обеспечение) или интеграция функций может привести к появлению новых функций, которые должны рассматриваться в FHA для выявления новых отказных состояний. Реализация может также привести к новым требованиям (например, требования по разделению и эксплуатационные требования). Эти новые требования и новые отказные состояния могут потребовать определения дополнительного доказательного материала в PSSA или FHA.

B.3.2 Оценка конструктивных/архитектурных решений на соответствие полученным требованиям по безопасности и целям

После завершения формирования требований к системе в FHA, каждое идентифицированное аварийное и катастрофическое отказное состояние должно быть оценено, как показано на рис. 4 основной части документа. Оценка должна:

a. Показать, используя Анализ дерева неисправности или подобный метод, как комбинации отказов отдельных объектов приводят к рассматриваемому отказному состоянию.

b. Идентифицировать все требования связанные с утверждениями о независимости сделанными в Анализе дерева неисправности посредством определения:

(1) всех требований по разделению/отделению и связанных требований по верификации из материалов Анализа общих причин;

(2) испытаний (наземных или летных) для проверки независимости;

(3) отказов с общей причиной (Анализ зонной безопасности, Анализ специфического риска, Анализ общего режима).

c. Показать, используя Анализ дерева неисправности или подобный метод, что качественные и количественные требования и цели, связанные с отказными состояниями, могут быть удовлетворены предложенной архитектурой системы и предусматриваемыми бюджетом вероятностями отказов.

d. Определить «непревышаемый» интервал для эксплуатационных задач, необходимость которых определяется скрытыми отказами из Анализа дерева неисправности. (Рассматриваемые скрытые отказы, которые могут существовать для проектируемой эксплуатации самолета или системы/объекта без превышения численных допущений из FHA, не будут приводить к появлению «непревышаемых» интервалов обслуживания).

e. Определить уровень гарантии разработки объектов, рассматриваемых в Анализе дерева неисправности.

AVA Documents
Document Sharing Hub

Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Syst...

(Примечание: Отказные состояния, классифицированные как сложные или усложнение условий полета, могут оцениваться, при необходимости, с использованием приведенных выше методов).

Эта оценка делается в той точке процесса разработки, когда результаты детальных исследований при уровне объектов системы полностью еще недоступны. Следовательно, оценка отказного состояния в PSSA должна полагаться частью на техническое суждение и на эксплуатационный опыт с подобными конструкциями. Этот процесс является итерационным и становится более завершенным в ходе развития проекта.

B.3.3 Получение требований безопасности для проектирования объектов более низкого уровня

Каждое проектное требование по безопасности, полученное на уровне системы, должно быть распределено на составляющие систему объекты. При этом распределяются:

a. Откорректированный перечень отказных состояний, который включает пояснение того, как требования по безопасности (качественные и количественные) могут выполняться в выбранной архитектуре.

b. Требования по безопасности (качественные и количественные), распределенные на объекты (аппаратные средства и программное обеспечение).

c. Требования для конструирования размещения (разделение, отделение, защита и т.д.).

d. Уровни гарантии разработки аппаратных средств и программного обеспечения.

e. Эксплуатационные задачи сохранения безопасности и соответствующие времена «непревышения».

Виды отказов и значения их вероятностей, идентифицированные в Анализе дерева неисправности PSSA, следует использовать как требования при проведении детальных исследований более низкого уровня.

B.4 ВЫХОДНЫЕ ДАННЫЕ

B.4.1 Документация

Результаты процесса PSSA должны быть задокументированы так, чтобы имелась трассируемость отчета с этапами выполнения PSSA. Часть информации, которая может представлять ценность для дальнейшего процесса и должна сохраняться, включает следующее:

a. Предполагаемые методы подтверждения соответствия требованиям из FHA.

b. Уточненные FHAs.

c. Перечень использованных при классификации материалов.

d. Перечень отказных состояний.

e. Требования по безопасности нижнего уровня (включая уровни гарантии разработки).

f. Материалы качественных FTAs.

g. Материалы предварительных CCAs.

h. Эксплуатационные требования (для полета и обслуживания).

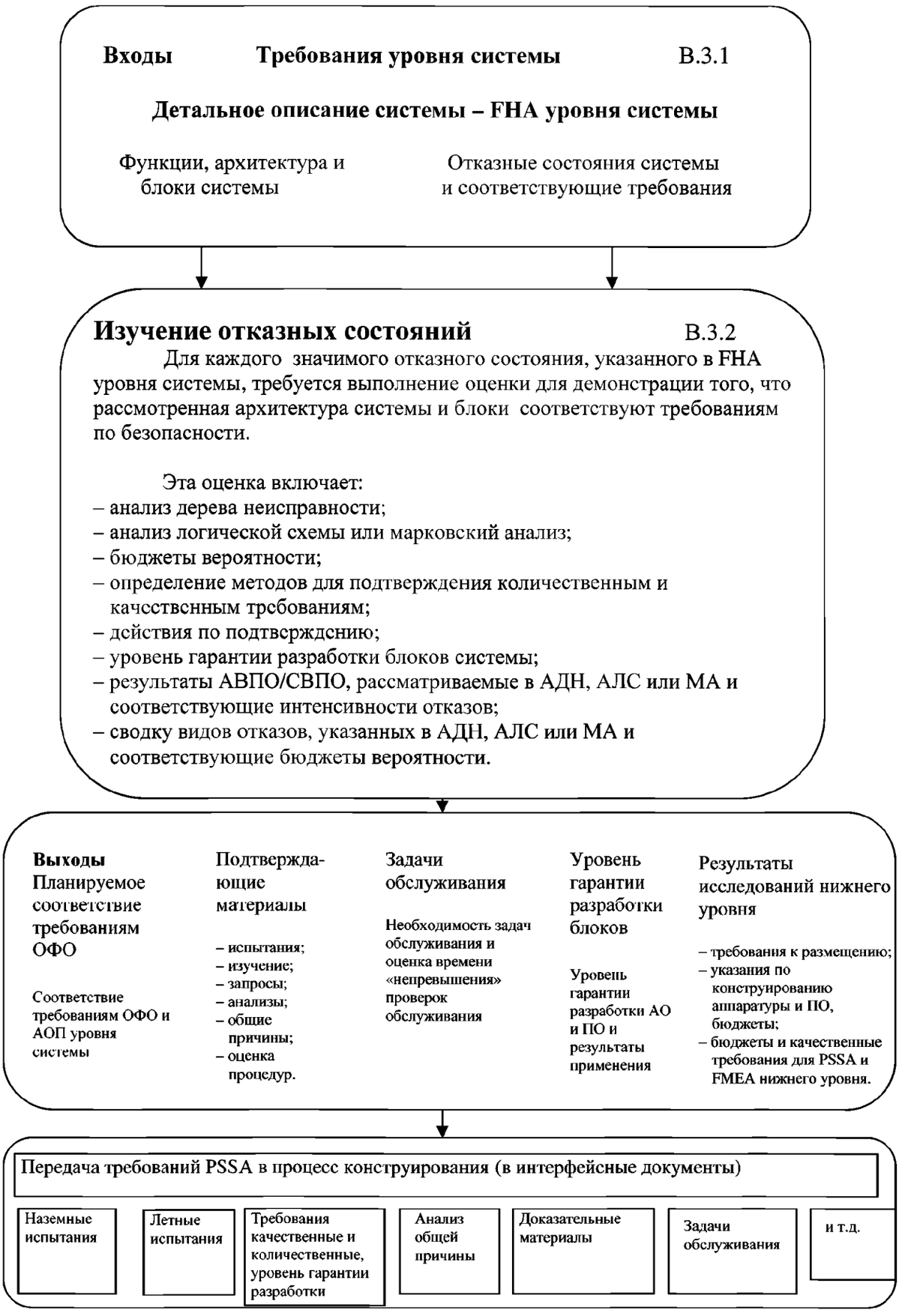
B.4.2 Выходные данные PSSA нижнего уровня

PSSA может выполняться на уровнях ниже уровня системы. Исходными данными для PSSA нижнего уровня служат значимые последствия отказов, качественные требования, бюджетные вероятности и уровни гарантии разработки, идентифицированные при проведении FHA/PSSA более высокого уровня. После получения входных данных, процесс PSSA нижнего уровня эквивалентен описанному выше.

B.4.3 Связь PSSA и SSA

Выходные данные PSSA являются исходными данными для процесса SSA.

Documents
Document Sharing Hub
Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Syst...



Процесс PSSA уровня системы
Рис. B1

Documents
Document Sharing Hub
Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment

ПРИЛОЖЕНИЕ C

Оценка безопасности системы

Примечание: *Основной текст документа дает общее представление об информации, которая содержится в этом приложении. Это приложение следует использовать совместно с основным текстом документа.*

C.1 ВВЕДЕНИЕ

Оценка безопасности системы является систематическим исследованием системы, ее архитектуры и размещения, для демонстрации соответствия требованиями по безопасности. Для каждой PSSA, выполненной на различном уровне, должна иметься соответствующая SSA. Самым высоким уровнем SSA является SSA уровня системы. Для каждой анализируемой системы SSA кратко излагает все значимые отказные состояния и их последствия для самолета. Методы анализа, используемые для показа соответствия, могут быть качественные или количественные.

В этом приложении используется Анализ дерева неисправности. Читателям должно быть понятно, что для достижения той же цели, в зависимости от обстоятельств и исходных данных, может использоваться Анализ логической схемы или Марковский анализ.

C.2 ТРЕБОВАНИЕ ПО ВЫПОЛНЕНИЮ ОЦЕНКИ

Требования к выполнению анализа могут изменяться в зависимости от конструкции, сложности и типа функции, выполняемой анализируемой системой. Они должны быть установлены в соответствующей PSSA.

C.3 ПРОЦЕСС SSA

Процесс SSA использует восходящий подход для верификации соответствия целям и требованиям по безопасности конструкции. На рис. C1 показана последовательность действий для SSA уровня системы. Такая оценка включает следующее:

a. Верификацию того, что требования к конструкции, установленные FHA уровня системы, удовлетворены.

b. Подтверждение того, что классификация, установленная для последствий на уровне самолета оправдана.

c. Верификацию того, что требования безопасности, приведенные в документах с целями и требованиями к самолету или выведенные из них, удовлетворены.

d. Верификацию того, что требования к конструкции, определенные при выполнении CCA, удовлетворены.

e. Согласование SSA уровня системы с FHA уровня самолета.

C.3.1 Верификация требований к конструкции FHA

C.3.1.1 Получение необходимых исходных данных

Входными данными SSA являются следующие материалы:

a. Описание архитектуры системы и связанное обоснование конструкции.

b. Системные интерфейсы и их применение к объектам смежных систем.

c. Требования и отказные состояния, идентифицированные в FHA/PSSA уровня системы.

d. Перечень функций и связанное обоснование из FHA уровня системы.

e. Результаты Анализа общих причин:

(1) Результаты ZA.

(2) Внешние угрозы PRA.

(3) Результаты CMA.

Documents
Document Sharing Hub
Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Syst...

f. Результаты всех исследований более низкого уровня и вспомогательные материалы, требуемые FHA/PSSA (FMEA/FMES от поставщиков отдельных объектов, результаты летних испытаний, исследований, и т.д.).

C.3.2 Оценка отказного состояния

Каждое отказное состояние, идентифицированное в FHA, должно быть оценено в соответствии с указанным на рис. 4 основного текста документа. Используя выбранные методы следует:

a. Показать, используя Анализ дерева неисправности, как объединяются отказы объектов для того, чтобы привести к рассматриваемому отказному состоянию.

b. Показать, используя Анализ дерева неисправности, что удовлетворяются качественные и количественные требования и цели, связанные с отказным состоянием.

c. Рассмотреть эксплуатационную документацию для проверки того, что «непревышаемый» интервал для эксплуатационных задач, определенный при рассмотрении и скрытых отказов в Анализе дерева неисправности, внесен в соответствующие документы. (Не все скрытые отказы вызывают необходимость «непревышаемых» интервалов обслуживания).

d. Проверить, что обеспечивается уровень гарантии разработки объектов, полученный из Анализа дерева неисправности.

e. Оценить условия испытаний, гарантирующих соответствие требованиям.

f. Продемонстрировать, что воздействие на самолет данного отказного состояния соответствует ожидаемому.

C.3.2.1 Валидация классификации отказного состояния

Следует продемонстрировать трассируемость между установленными в FHA/PSSA требованиями и документами, в которых эти требования определены. К таким документам относятся:

a. Документы с целями и требования к самолету.

b. Документы с требованиями к системам.

c. Программы испытаний (наземные и летные испытания и т.д.).

d. Руководство по технической эксплуатации.

e. Документы Анализов общих причин.

Одним из методов решения этой задачи является подготовка матрицы, показывающей требования и документы об их подтверждении.

C.3.2.2 Верификация соответствия требованиям по безопасности выведенных из документов с требованиями к самолету

Документы с требованиями к самолету содержат все требования необходимые для разработки самолета. Они включают все требования Норм летной годности и все требования компании. Верификация этих требований выполняется одним или несколькими стандартными методами (то есть, рассмотрением конструкции, анализом, моделированием и испытаниями).

C.3.2.3 Верификация соответствия требованиям к конструкции из CCA

Документация Анализа общих причин содержит требования к системе и ее компонентам по отделению и разделению (из Анализа зонной безопасности), по внешним угрозам (из Анализа специфического риска) и по отказам общего режима (из Анализа общего режима). Эти требования должны быть верифицированы с использованием одного или нескольких стандартных методов (то есть, рассмотрением конструкции, анализом, моделированием и испытаниями).

AVA Documents
Document Sharing Hub

Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Syst...

C.4 ВЫХОДНЫЕ ДАННЫЕ SSA

C.4.1 Документация

Результаты процесса SSA должны быть зарегистрированы так, чтобы имелась трассируемость отчета с этапами выполнения SSA. Часть информации, которая может представлять ценность для дальнейшего процесса и должна сохраняться, включает следующее:

a. Откорректированный перечень отказных состояний или отчет FHA, который содержит объяснение показанного соответствия требованиям по безопасности (качественных и количественных).

b. Документация, показывающая, как требования к проектированию размещения объектов системы (разделение, отделение и т.д.), были учтены.

c. Материалы, используемые для валидации классификации отказных состояний.

d. Задачи обслуживания и связанное время «непревышения».

e. Документация, показывающая как система и объекты (включая аппаратные средства и программное обеспечение) были разработаны в соответствии с назначенными уровнями гарантии разработки.

C.4.2 Связь SSA уровня системы и FHA уровня самолета

Для того чтобы завершить процесс оценки безопасности, каждый отчет SSA должен быть рассмотрен на соответствие основным требованиям как FHA уровня системы, так и уровня самолета. Последствия и вероятность возникновения отказов на уровне самолета в отчете следует проверить на соответствие указанным отказным состояниям и их классификациям в отчете FHA уровня самолета.

Documents
Document Sharing Hub
Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Syst...



Процесс SSA уровня системы
Рис. C1

Documents
Document Sharing Hub
Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment

ПРИЛОЖЕНИЕ D

Анализ дерева неисправности

Примечание: *Основной текст документа дает общее представление об информации, которая содержится в этом приложении. Это приложение следует использовать совместно с основным текстом документа.*

D.1 ВВЕДЕНИЕ

Анализ дерева неисправности – дедуктивный анализ нарушения, который сосредотачивается на одном специфическом нежелательном событии и предоставляет метод для определения причин этого события. Другими словами, Анализ дерева неисправности – «нисходящая» процедура оценки системы, в которой сформирована и затем оценена качественная модель для специфического нежелательного события. Выполняющий анализ начинает с нежелательного события верхнего уровня и систематически определяет все вероятные одиночные отказы и комбинации отказов функциональных блоков системы на следующем нижнем уровне, которые могут вызывать это событие. Анализ развивается вниз, последовательно через более детальные (то есть нижние) уровни конструкции объекта, до достижения первичного нераскрываемого события или до получения подтверждения, что требования к нежелательному событию верхнего уровня удовлетворяются. Первичное событие определяется как событие, которое по той или другой причине далее не разрабатывается (то есть событие не нуждается в разбиении на более точные уровни детализации для показа соответствия применяемым к анализируемой системе требованиям по безопасности). Основное событие может быть внутренним или внешним по отношению к анализируемой системе и может быть отнесено к отказам/ошибкам аппаратных средств или к ошибкам программного обеспечения.

Выполняющего анализ следует поощрять к продолжению FTA для определения достаточной детализации удовлетворения требований к нежелаемому событию.

Графическое представление дерева неисправности иерархично и получило наименование из-за показываемых ветвлений. Это формат, который делает результаты анализа наглядными и для разработчиков, и для авиационной власти. Как один из семейства методов оценки безопасности, используемых для гарантии выполнения системой/оборудованием установленных функции безопасности, Анализ дерева неисправности связан с гарантией того, что аспекты безопасности конструкции идентифицированы и контролируемы.

Применение Анализа дерева неисправности обеспечивает:

a. Помощь при выполнении оценок и рассмотрений техническими и сертифицирующими органами. (Завершенное дерево неисправности показывает только отказные события, которые могли в отдельности или в комбинации привести к установленному нежелательному событию верхнего уровня).

b. Оценку влияния модификации конструкции на безопасность.

c. Определение значения вероятности встречаемости события верхнего уровня.

d. Распределение бюджетов вероятности по событиям нижних уровней.

e. Наблюдаемость вклада ошибок конструкции посредством обеспечения формата для смешанных количественной и качественной оценок.

f. Оценку последствий одиночных и множественных отказов.

g. Оценку интервалов воздействия, скрытого состояния и интервалов «риска» в отношении их общего влияния на систему.

h. Наблюдаемость потенциальных границ событий с общей причиной.

i. Оценку источников отказов с общей причиной.

j. Оценку свойств «отказобезопасности» конструкции (устойчивая к отказам и устойчивая к ошибкам).

AVA Documents Document Sharing Hub

Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Syst...

D.2 Это приложение содержит информационные и процедурные инструктивные материалы для выполнения опытным инженером Анализа дерева неисправности на начальном этапе разработки. Здесь приводится основная информация в отношении FTA, подробные сведения имеются в других опубликованных материалах (таких как «NUREG-0492»).

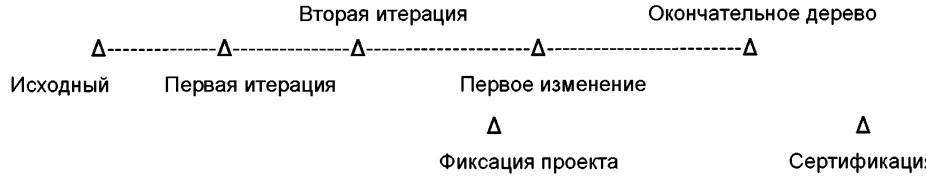
D.3 РОЛЬ FTA В ОЦЕНКЕ БЕЗОПАСНОСТИ

Анализ дерева неисправности следует выполнять при определении концепции системы (часть процесса PSSA, о чем указывается в разделе 3.3 основного текста) или после того, как концепция системы сформирована (часть процесса SSA по разделу 3.4). «Нисходящий» анализ, подобный FTA можно применять на различных уровнях детализации для рассмотрения соответственно предполагаемой и имеющейся компоненты конструкции.

Изменения FTA после «фиксации» конструкции диктуются уровнем изменения проекта. Это происходит из-за того, что интенсивности отказов основных событий в FTA основаны на данных Сводки видов и последствий отказа и FTA подлежит уточнению, если при изменении проекта аппаратных средств изменяются интенсивности отказов, которые были приведены в FMES. Анализ дерева неисправности следует пересматривать и на последующих стадиях программы летных испытаний. Материалы FTA, которые включают любые изменения конструкции, вызванные выполнением программы летных испытаний самолета, обычно необходимы как часть вспомогательных данных квалификации оборудования.

На рис. D1 показан пример типичного развития FTA по ходу проекта. Отметим, что на рисунке показан только пример. Все участники разработки бортовой системы должны принять решение о конкретном временном графике создания FTA в начале процесса оценки безопасности.

FHA	PSSA	SSA	
Эскизный проект	Технический проект	Рабочий проект	Производство и испытания



Пример типичного развития FTA
Рис. D1

В приведенном примере:

a. «Исходный» FTA выполняется как часть процесса FHA для того, чтобы определить комбинацию отказов системы и распределить бюджеты вероятностей по элементам системы.

b. «Первая итерация», может включать изменения дерева неисправности, обусловленные пересмотром или прояснением некоторых исходных предположений выполняющего анализ при подтверждении предъявленных требований к системе. Этот FTA выполняется как часть процесса выбора архитектуры системы. На этом этапе осуществляется распределение риска и бюджета вероятности для событий нижнего уровня.

c. «Вторая итерация (прототип)» включает изменения дерева неисправности вследствие лучшего понимания системы при детальном проектировании аппаратуры и программного обеспечения. На этом этапе программы изменяют следующее:

   1) В первичные события дерева неисправности вводится информация по интенсивности отказов, полученная из Сводки видов и последствий отказа.

AVA Documents
Document Sharing Hub
Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Syst...

2) Рассчитывается и указывается вероятность события верхнего уровня.

3) Эта вероятность отказа сравнивается с соответствующим требованием безопасности, как часть процесса верификации.

Эта версия дерева неисправности становится частью вспомогательной документации необходимой для полного завершения этапа программы, называемого «Фиксацией проекта».

d. «Первое (производственное) изменение» включает изменения дерева неисправности, основанные на изменениях аппаратных средств или программного обеспечения, следующих из разрешения проблем при испытаниях прототипа.

e. Затем выполняющий анализ создаст «Окончательное дерево», включением всех изменений аппаратуры и программного обеспечения, выполненных по результатам летных испытаний самолета. Эта версия дерева неисправности затем становится частью документации оценки безопасности системы, необходимой для завершения этапа «Сертификация».

D.4 СИМВОЛЫ ДЕРЕВА НЕИСПРАВНОСТИ И ОПРЕДЕЛЕНИЯ

Все деревья неисправности составлены из двух видов символов: символы логики и символы события. Общим правилом относительно символов является сохранение простоты; если использовано меньше различных типов символов, то для специалиста, делающего обзор дерева неисправности, будет проще понять его. Логические символы используются, чтобы связать вместе различные ветви дерева неисправности. Логические символы дерева неисправности не следует соединять непосредственно. Их входами и выходами следует всегда делать символы событий.

Два основных используемых логических символа – булевы логические «И» и «ИЛИ». Выполняющий анализ выбирает символ «И», когда нежелательное событие верхнего уровня может происходить только, когда все входные нижние условия истинны. Символ «ИЛИ» используется, когда нежелательное событие может происходить, если истинно одно из входных нижних условий. Можно также использовать другие логические символы, если структура системы гарантирует использование этих типов символов.

Наиболее часто используемые символы событий включают: прямоугольник, треугольник, овал, круг, дом, и ромб (смотри рис. D2).

Прямоугольник содержит описание выхода логического символа или события.

Треугольник показывает перемещение информации и бывает двух типов. Треугольник с вертикальной линией из верхней точки показывает, что в данное место дерева неисправности «включаются» другие данные (события и их соответствующие вероятности возникновения). Треугольник с горизонтальной линией сбоку указывает, что событие, к которому треугольник привязан, «перемещается» к другой ветви дерева.

Овал представляет условное событие, которое определено как условие, которое является необходимым для возникающего вида отказа (обычно используется вместе с символом «Приоритетное И» и символом «Блокировка»). Например, «сначала отказывает контроль» является условным событием, потому что оно необходимо для необнаруживаемого распространения недостоверных данных в системе.

Круг, Дом и Ромб представляют типы первичных событий. Круг обозначает основное событие. Основное событие определено, как событие, которое является внутренним в анализируемой системе и не требует никакой дальнейшей разработки (то есть, может быть причиной возникновения неисправности). При этом только для элементов аппаратных средств может быть назначена необходимая для количественной оценки бюджетная интенсивность отказов или фактическая интенсивность отказов по результатам FMES или другого источника.

Событие Дом – событие, которое, как ожидается, произойдет. Это событие имеет два возможных состояния:

– событие произошло;

– событие не произойдет в течение периода исследования.

Documents
Document Sharing Hub
Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Syst...

Функция Дом подобна ключу и используется для того, чтобы включать или исключать части дерева неисправности, которые могут или не могут рассматриваться в некоторых ситуациях.

Ромб выражает неразрабатываемое событие. Неразрабатываемое событие определено как событие, которое далее не раскрывается, потому что оно имеет незначительное влияние на события верхнего уровня или потому что подробности, необходимые для дальнейшего раскрытия события, трудно доступны. Часто эти типы событий добавляются к дереву неисправности для того, чтобы сделать дерево неисправности «полным» с качественной точки зрения. Первичные события, касающиеся программного обеспечения, обычно имеют форму неразрабатываемого события.

Многие пакеты программного обеспечения для выполнения FTA имеют дополнительные символы, которые являются обычно уникальными особенно для конкретного пакета программ. Выполняющий анализ может использовать другие символы, которые не показаны на рис. D2, если эти символы правильно определены.

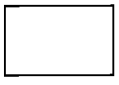
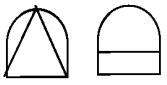
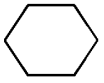
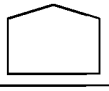
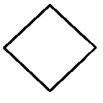
Математические символы, применяемые в тексте приложения, включают:

λ – интенсивность отказов на час (обычно на час полета, но может быть на час работы);

T – интервал проверки;

t – время воздействия или «время риска» связанное с конкретным исходным событием;

P или P_t – вероятность события или отказа за время t.

Символ	Наименование	Описание
	Прямоугольник	Описание выхода логического символа или события
	Символ И	Событие может произойти, когда все условия нижнего уровня истинны
	Приоритетное И	Событие может произойти, когда все условия нижнего уровня возникают в специфической последовательности (обычно последовательность показывается условным событием)
	Символ ИЛИ	Событие может произойти, если истинно любое одно условие нижнего уровня
	Блокировка	Выходная неисправность возникает, если (одна) входная неисправность возникает при наличии условного события
	Перемещение	Показывает перемещение информации
	Основное событие	Внутреннее в анализируемой системе событие, не требующее дальнейшей разработки
	Дом	Внешнее к анализируемой системе событие, которое может или не может произойти
	Неразрабатываемое событие	Событие, которое далее не раскрывается, потому что оно имеет незначительное влияние на события верхнего уровня или потому что подробности, необходимые для дальнейшего раскрытия события, труднодоступны
	Условное событие	Условие, которое является необходимым для возникающего вида отказа

Символы дерева неисправности
Рис. D2

Documents
Document Sharing Hub
Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equi...

D.5 ОБЗОР ДЕЙСТВИЙ АНАЛИЗА ДЕРЕВА НЕИСПРАВНОСТИ

Выполнение Анализа дерева неисправности требует шести основных шагов.

1. Определение цели и глубины анализа

Будет ли цель специфической? Будет ли дерево неисправности использоваться для определения бюджетов отказных событий (часть процесса PSSA)? Будет ли анализ использоваться для проверки соответствия конструкции системы установленным требованиям по безопасности (часть процесса SSA)? Будет ли дерево неисправности оцениваться качественно, количественно или совместно? Определение цели FTA поможет выполняющему анализ определить пределы FTA.

2. Определение требуемого уровня анализа.

Как глубоко в систему (т.е. до какого уровня) будет входить выполняющий анализ в своей работе? Будет ли система «разделяться», чтобы выполнить многоуровневый FTA? Знание глубины анализа важно для определения области FTA и для определения того, как результаты FTA будут записаны (т.е. связь с шагом 5). Раздел D.6 содержит дополнительную информацию по определению анализа.

3. Определение Нежелательного события

Это Нежелательное событие может быть связано или непосредственно с FHA, или оно может быть связано с первичным событием в другом дереве неисправности, если система разделялась на несколько уровней (то есть, выравнивание границ в многоуровневом FTA). Если нежелательное событие является подразделом большего события, тогда следует принять меры предосторожности при объединении поддеревьев. Все объединяемые поддеревья должны быть проверены на независимость до включения их в новое дерево неисправности. На этом шаге также устанавливается бюджет вероятности нежелательного события (бюджет имеет численное значение, даже если анализ качественный). Раздел D.7 содержит дополнительную информацию по определению нежелательных событий.

4. Сбор наиболее полных данных по системе, доступных началу работы, и анализ их на предмет определения возможных отказов, неисправностей и их комбинаций, которые приводят к событию верхнего уровня.

Раздел D.8 содержит дополнительную информацию по этому шагу.

5. Конструирование дерева неисправности с нежелательным событием из шага 3.

Раздел D.9 содержит дополнительную информацию по конструированию дерева неисправности.

6. Анализ и обобщение результатов FTA

Разделы с D.10 по D.13 содержат дополнительную информацию по рассмотрению деревьев неисправности и обобщению их результатов.

D.6. ОПРЕДЕЛЕНИЕ ГРАНИЦ АНАЛИЗА

Дерево неисправности может использоваться для достижения указанных ниже основных целей:

1. В процессе PSSA:

   a. Распределение вероятности отказа P_f, когда ведется работа с количественными целями по P_f. Бюджетные вероятности отказа в дереве неисправности PSSA могут быть более жесткие (то есть, меньшая вероятность), по сравнению с величиной вероятности, требуемой по математическим расчетам дерева.

   b. Установление требований к структуре системы, когда ведется работа с качественными целями по отказобезопасности.

2. В процессе SSA

   a. Проверка соответствия целям, установленным в FTA процесса PSSA.

Documents
Document Sharing Hub
Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Syst...

Выполняющий анализ может работать над любой целью на любом уровне в пределах системы. Допустимым уровнем является любой уровень в пределах многоуровневого FTA. Выполняющему анализ потребуется определить необходимые границы FTA. Эти границы будут субъективно основываться на том, что он хочет или что необходимо для выполнения анализа. В таблице D1 перечисляется несколько возможных допустимых уровней и их потенциальные границы. Отметим, что информация, представленная в колонке «Граница FTA», указывает одну потенциальную границу анализа (т.е. самый нижний уровень детальности конструкции, который будет рассматриваться при выполнении нисходящего анализа). Выполняющему анализ следует выбрать границы основываясь на назначении анализа. При этом могут рассматриваться следующие положения: чем являются входы и выходы системы, какие дополнительные подробности по системе следует рассмотреть, следует ли включить в рассмотрение ошибки людей, следует ли включить ошибки программного обеспечения и т.д.

Выбранные границы FTA тесно связаны с представлением результатов оценки дерева неисправности.

Таблица D1. Примеры границ FTA

Необходимый уровень FTA	Граница FTA	Характеристика FTA на этом уровне
Самолет	Блок-схема самолета	FHA/PSSA: Бюджеты P_f различных значимых систем, объединенных функцией уровня самолета FHA/PSSA: Определение последствий отказов, вызывающих или содействующих отказным состояниям уровня самолета
Система	Блок-схема системы	FHA/PSSA: Бюджеты P_f для блоков системы SSA: Использование интенсивностей отказов блока (взятых непосредственно из расчета надежности блока) для оценки Первичного события
Блок	Функциональная блок-схема блока	PSSA: Бюджеты P_f для различных функциональных модулей блока (т.е. распределение по функциям аппаратуры и программного обеспечения) SSA: Использование интенсивностей отказов специфических групп элементов (т.е. интенсивность отказов процессора, генераторов, памяти и т.д.) когда при количественной оценке исходная интенсивность отказов блока слишком велика для демонстрации соответствия требованиям по безопасности
Функциональный блок	Схемы блока Функциональные элементы ПО	PSSA: Бюджеты P_f для различных функциональных цепей рассматриваемого блока их средств контроля. Распределение уровня гарантии разработки по функциональным элементам программного обеспечения. SSA: Использование интенсивностей отказов специфических групп элементов (т.е. интенсивность отказов приемника сигналов по ARINC 429) когда при количественной оценке исходная интенсивность отказов групп компонентов слишком велика для демонстрации соответствия требованиям по безопасности

D.7 ОПРЕДЕЛЕНИЕ НЕЖЕЛАТЕЛЬНОГО СОБЫТИЯ ВЕРХНЕГО УРОВНЯ

Выполняющий анализ должен составить перечень нежелательных событий. Каждое нежелательное событие станет в дереве неисправности событием верхнего уровня. В зависимости от необходимого уровня рассмотрения системы, эти события верхнего уровня могут иметь различное происхождение. Таблица D2 описывает некоторые источники событий верхнего уровня, основанные на схеме процесса оценки безопасности, представленной в основной части документа.

AVA Documents
Document Sharing Hub
Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equi...

Таблица D2. Происхождение событий верхнего уровня

Необходимый уровень FTA	Источник событий верхнего уровня
Самолет	FHA функций самолета
Система	FHA системы и/или FHA функций системы и/или FTA функций самолета
Блок	FTA системы
Функциональный модуль блока	FTA блока

D.8 СБОР ИНФОРМАЦИИ О СИСТЕМЕ

Выполняющий анализ должен накапливать наиболее полные текущие данные по системе и анализировать собранный материал, чтобы определить возможные отказы и их комбинации, которые приводят к событиям верхнего уровня. Информация может поступать из двух основных источников:

a. Функциональные блок-схемы системы.

b. Документация описания конструкции или документация по требованиям к конструкции.

Напомним, для того, чтобы FTA был эффективным инструментом установления критериев безопасности системы, анализ следует выполнять при создании конструкции, а не после этого.

D.8.1 Рассмотрение функциональной блок-схемы системы

Выполняющему анализ следует рассмотреть функциональную блок-схему системы. Такая блок-схема обеспечит информацию по критериям успешного полета и связей системы с другим оборудованием. Слово «система» в этом контексте может относиться к любой группе самолетного или вспомогательного оборудования (например, силовая установка, подсистема двигателя или сменный блок автопилота). Выполняющий анализ должен хорошо знать анализируемую «систему» для того, чтобы определить единичные отказы и их комбинации, которые могут вызывать событие верхнего уровня для конкретного конструируемого дерева.

D.8.2 Рассмотрение документации с описанием/требованиями к конструкции

Выполняющий анализ должен собрать все имеющиеся данные о системе и анализировать их, чтобы определить возможные отказы и их комбинации, которые могут привести к событию верхнего уровня для этого конкретного дерева. Возможные источники данных включают документы описания архитектуры системы, различные документы спецификации и описания конструкции системы, аппаратных средств и программного обеспечения, а также собственное хорошее знание рассматриваемой системы.

D.9 КОНСТРУИРОВАНИЕ ДЕРЕВА НЕИСПРАВНОСТИ

Конструирования дерева неисправности выполняется следующими четырьмя шагами:

1. Формулируется нежелательное событие верхнего уровня в ясном, кратком выражении (и его вероятность как заданное значение для отказа или для интенсивности отказа, если они применимы).

2. Разрабатываются верхний и промежуточные ярусы дерева неисправности. Определяются промежуточные отказы и комбинации отказов, которые являются минимальными, непосредственными, необходимыми и достаточными для того, чтобы произошло событие верхнего уровня, и связываются соответствующими стандартными логическими символами дерева неисправности. Расширяется каждый первый уровень события отказа до следующего нижнего уровня.

AVA Documents
Document Sharing Hub
Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Syst...

3. Разрабатывается каждое событие отказа через последовательные более детальные уровни конструкции системы до тех пор, пока не будут установлены исходные причины или дальнейшее проявление будет сочтено ненужным.

4. Устанавливаются бюджеты вероятности отказов или бюджеты интенсивности отказов, оценивается способность системы соответствовать целям безопасности и, в случае необходимости, система переконструируется (в ходе процесса PSSA) или оценивается дерево неисправности качественно и/или количественно (в ходе процесса SSA).

D.9.1 Формулирование нежелательного события верхнего уровня

Этот раздел рассматривает первый шаг конструирования дерева неисправности.

1. Формулируется нежелательное событие верхнего уровня в ясном, кратком выражении (и его вероятность как заданное значение для отказа или для интенсивности отказа, если они применимы).

Выполняющий анализ вводит событие дерева неисправности верхнего уровня в прямоугольный символ события. Это утверждение должно определять, что является Нежелательным событием и когда оно происходит. Для большинства деревьев неисправности это событие верхнего уровня уже установлено в FHA или в другом дереве неисправности верхнего уровня и требуется только его копирование в прямоугольный символ события. В других случаях, будет необходимо разъяснить утверждение Нежелательного события перед его занесением в прямоугольный символ события.

Нежелательное событие верхнего уровня должно быть выражено понятно и кратко, потому что это устанавливает тон для ряда вопросов, которые будут задаваться при конструировании различных уровней дерева неисправности. В таблице D3 приведены некоторые примеры плохо сформулированных и пересмотренных выражений события верхнего уровня для FTA в процессе выполнения SSA. При проведении PSSA тип информации в колонке «Исправленное утверждение» может быть другим.

Таблица D3. Примеры выражений верхнего уровня

Плохо сформулированное утверждение	Проблема в утверждении	Исправленное утверждение
Потеря индикации воздушной скорости	Очень нечетко указано «что» является неисправностью. Это означает потерю основной индикации, резервной или всей?	Потеря всей индикации воздушной скорости в кабине
Индикация ложных данных захода на посадку без сигнализации об отказе	Очень нечетко о том, где возникает неисправность. Это отображается двумя навигационными индикаторами или только одним?	Индикация ложных данных захода на посадку на двух навигационных индикаторах без сигнализации об отказе
Индикация ложного углового положения на одном основном индикаторе пилота без сигнализации об отказе	Выражает «что», но не «когда». Если рассматривать все этапы полета, то событие вызывает отказное состояние, классифицируемое как сложное. На взлете после отрыва оно классифицируется как аварийное. «Когда» определяет интервал времени, используемый для расчета P_f при численном оценивании	Индикация ложного углового положения на одном основном индикаторе пилота без сигнализации об отказе на взлете после отрыва

Documents
Document Sharing Hub
Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Syst...

D.9.2 Конструирование верхнего и промежуточных ярусов дерева неисправности

Этот раздел рассматривает второй шаг конструирования дерева неисправности.

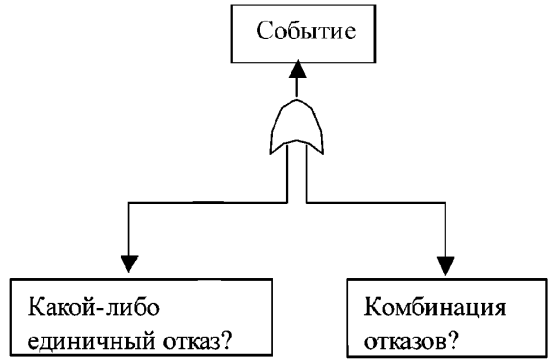
2. Разрабатываются верхний и промежуточные ярусы дерева неисправности. Определяются промежуточные отказы и комбинации отказов, которые являются минимальными, непосредственными, необходимыми и достаточными для того, чтобы произошло событие верхнего уровня, и связываются соответствующими стандартными логическими символами дерева неисправности. Расширяется каждый первый уровень события отказа до следующего нижнего уровня.

Выполняющий анализ должен создать верхние ярусы дерева неисправности (смотри рис. D3). Каждое дерево неисправности будет начинаться событием верхнего уровня, которое является событием определенным в конкретном дереве неисправности предшествующего уровня (см. D.9.1).

Выполняющий анализ расширяет дерево по отношению к первому ярусу, рассматривая следующие вопросы:

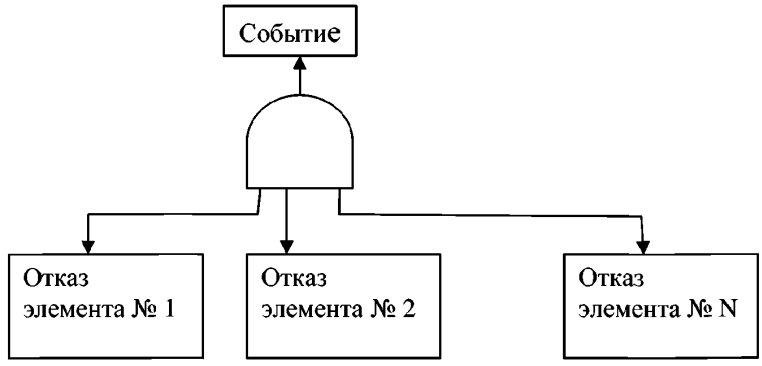
a. Имеются ли там любые одиночные отказы, которые заставят внесенное в перечень событие быть истинными?

b. Имеются ли любые кратные комбинации отказов, которые заставят внесенное в перечень событие быть истинными?



Верхний ярус дерева неисправности на основе первых вопросов
Рис. D3

Если нет никаких одиночных отказов, но имеются кратные комбинации отказов, то первый ярус дерева неисправности может быть показан подобно указанному на рис. D4.

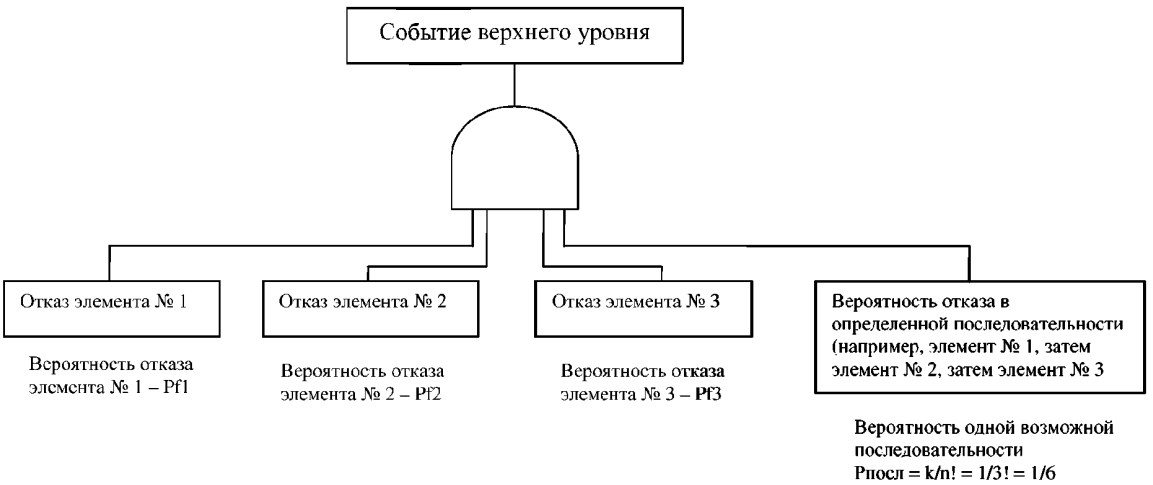


Верхний ярус дерева неисправности без одиночных событий в системе
Рис. D4

Documents
Document Sharing Hub
Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Syst...

Кратные комбинации отказов могут зависеть от специфического порядка, в котором они происходят. Эти события затем определяются, как события зависимые от порядка отказа (известные также как последовательные события). Зависимые от порядка отказа события должны быть выведены как входы в логический элемент «И» слева направо в порядке, в котором они должны происходить. Если в вышеуказанном рис. D4 первый и второй элементы системы должны отказать раньше N-ного элемента для того, чтобы событие произошло, то логический элемент «И» может включить вход от другого неразрабатываемого события, которое представляет вероятность того, что «n» элементов откажут в этом порядке. Другим способом представления порядка зависимых событий является использования логического символа «Приоритетное И». Подробнее это описано в D.11.1.4.

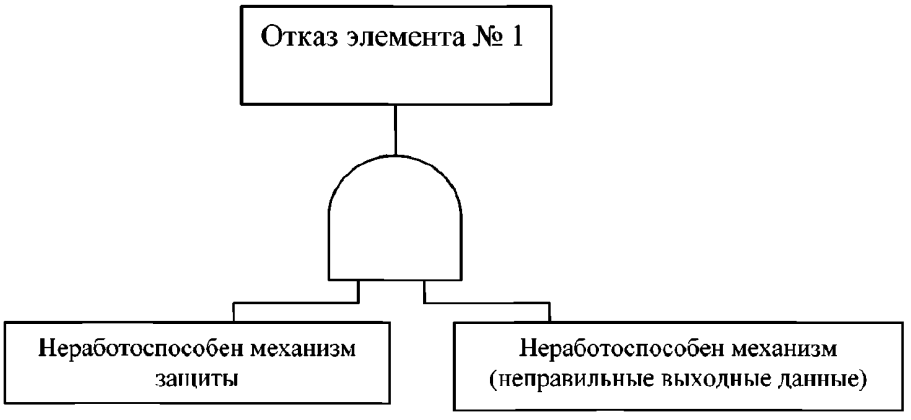
Например, предположим, что в рассмотренной ранее системе имеется три элемента. Первый ярус дерева неисправности будет представлен как на рис. D5.



Верхний ярус дерева неисправности рассматриваемых событий
Рис. D5

Обозначение n! (факториал) представляет число возможных последовательностей событий. Для этого примера возможными последовательностями событий являются P1P2P3, P1P3P2, P2P3P1, P2P1P3, P3P1P2 и P3P2P1.

Затем, выполняющий анализ расширяет дерево, в направлении «сверху-вниз» при рассмотрении вышеупомянутых вопросов для события или последствия отказа, так как это описано, на каждом новом уровне. При рассмотрении отказоустойчивых событий, основанных на кратных отказах, выполняющий анализ должен рассмотреть влияния неправильных выходов и неисправных механизмов защиты и реконфигурации, как показано на рис. D6.



Расширение дерева неисправности для элементов отказобезопасной системы
Рис. D6

Documents
Document Sharing Hub
Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equi...

В ходе конструирования дерева неисправности необходимо удостовериться, что предопределенное соглашение о наименованиях выдерживается так, что каждый работающий над данной системой создает деревья неисправности тем же самым способом. При выборе соглашения о наименованиях, следует иметь в виду три вещи:

a. Соглашение о наименованиях должно предотвращать конфликты между событиями; то есть, никакие два различных события не могут иметь то же самое название, а идентичные события должны иметь то же самое название. Это критично точного сокращения с использованием булевой алгебры.

b. Соглашение о наименованиях не должно быть слишком непонятным или кто-либо рассматривающий дерево не должен постоянно обращаться к некоторому виду таблицы, чтобы декодировать название.

c. Соглашение о наименованиях должно быть сопровождаемым; то есть, уточнение соглашения не должно приводить к переименованию всех событий, потому что существующее не позволяет в последующем добавления нескольких новых событий.

Если для создания деревьев используется пакет программного обеспечения FTA, это предопределенное соглашение о наименованиях должно быть совместимо с этим пакетом. Некоторые пакеты требуют, чтобы именовались логические символы, используемые для определения промежуточных событий.

D.9.3 Расширение ветвей верхнего события до первичных событий

Этот раздел рассматривает третий шаг конструирования дерева неисправности.

3. Разрабатывается каждое событие отказа через последовательные более детальные уровни конструкции системы до тех пор, пока не будут установлены исходные причины или дальнейшее проявление будет сочтено ненужным.

Далее выполняющий анализ должен разработать и завершить дерево неисправности, расширяя ветви дерева неисправности вплоть до первичных событий (то есть до основных событий, внешних событий и неразрабатываемых событий). Эти первичные события являются корневыми причинами отказных событий первого уровня.

Корневая причина, заключающаяся в отказе/ошибке аппаратных средств или ошибке программного обеспечения, будет разделена на уровни детализации, необходимые для поиска соответствия конструкции системы целям безопасности. В этом месте становится очевидным воздействие цели FTA на дальнейшие действия в анализе. Если целью FTA является качественная оценка, накопление дальнейшей информации относительно первичного события не обязательно (до тех пор, пока не будет определено, что далее требуется детальный качественный анализ). Если целью FTA является количественная оценка, то следует собрать более детальную информацию относительно первичного события (интенсивности отказов аппаратных средств и времена воздействия или «риска»).

В этом приложении разрабатываются четыре специальных примера для демонстрации типичного представления дерева неисправности с включением базовых событий при наличии и без скрытых отказов и требуемого порядка факторов. Подробности математических расчетов приведены далее в D.11.1.5.

D.9.3.1 Пример, когда два отказа элементов приводят к потере функции

Дерево неисправности первого примера, приведенное на рис. D7, показывает простой вариант отказа, когда событие верхнего уровня вызывается отказом двух элементов в одном и том же полете. Известно, что оба элемента были работоспособны в начале полета и отсутствовали скрытые отказы. Два отказа могут возникнуть в любом порядке.

AVA Documents Document Sharing Hub

Full document details: Guidance 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Syst...