МЕЖГОСУДАРСТВЕННЫЙ АВИАЦИОННЫЙ КОМИТЕТ
АВИАЦИОННЫЙ РЕГИСТР

РУКОВОДСТВО 4761

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

2010

gost.e-ecolog.ru

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

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,*

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.

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.

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.

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.

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

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,

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

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

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

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.

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

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.

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.

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

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.

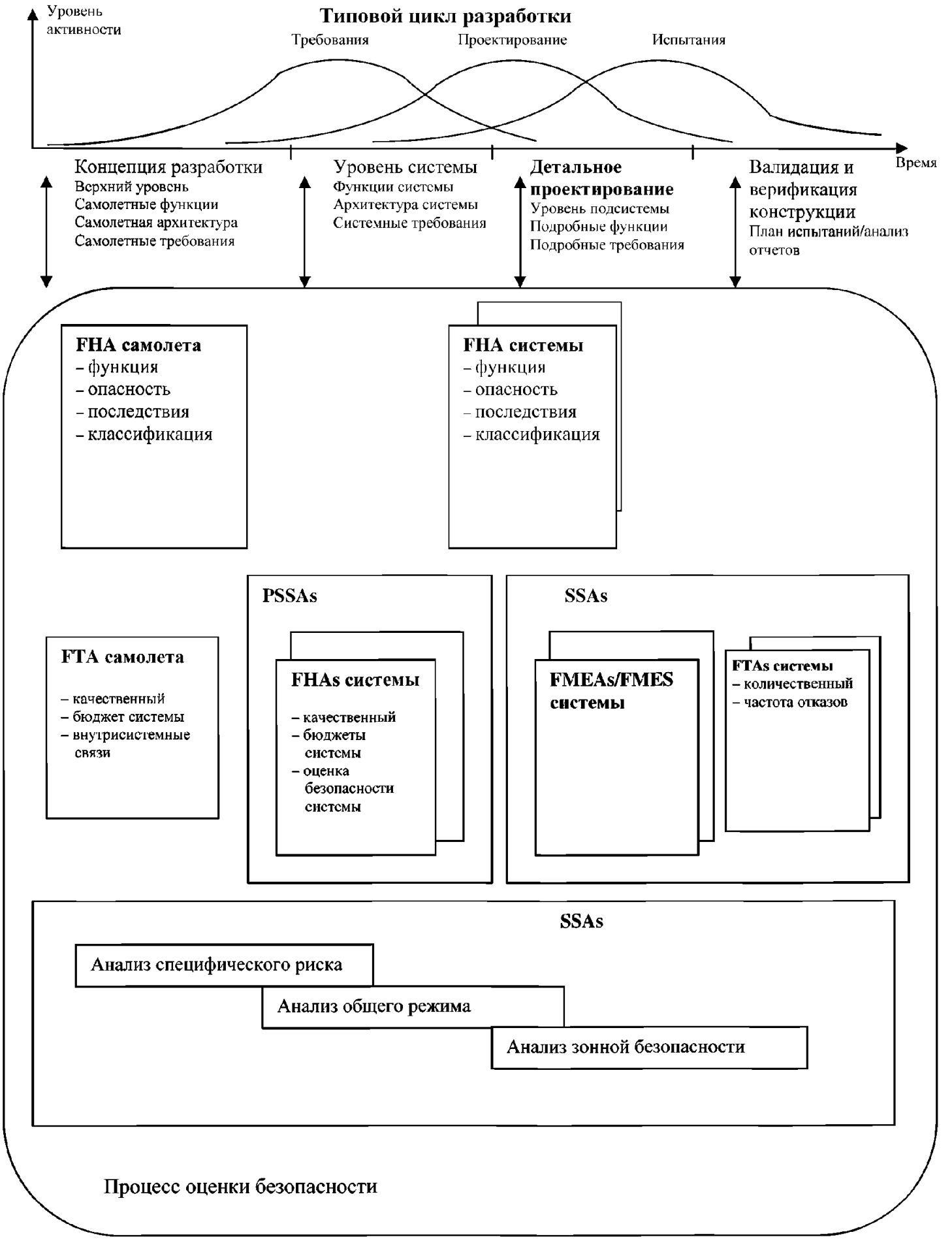
Ниже рассмотрен пример применения этой концепции к двигателю. В принципе это может применяться к любой системе, которая проектируется с использованием резервирования.

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).*

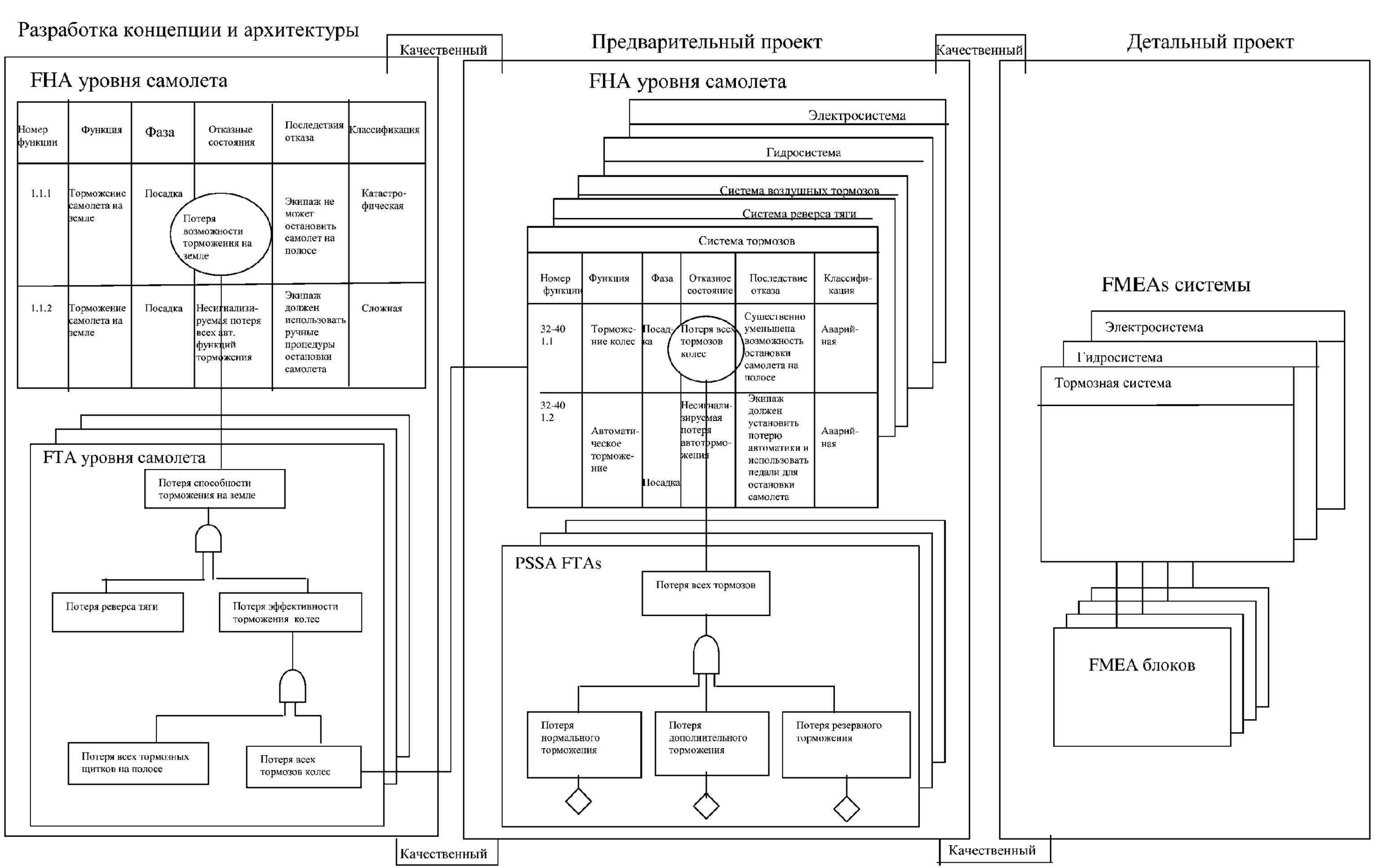


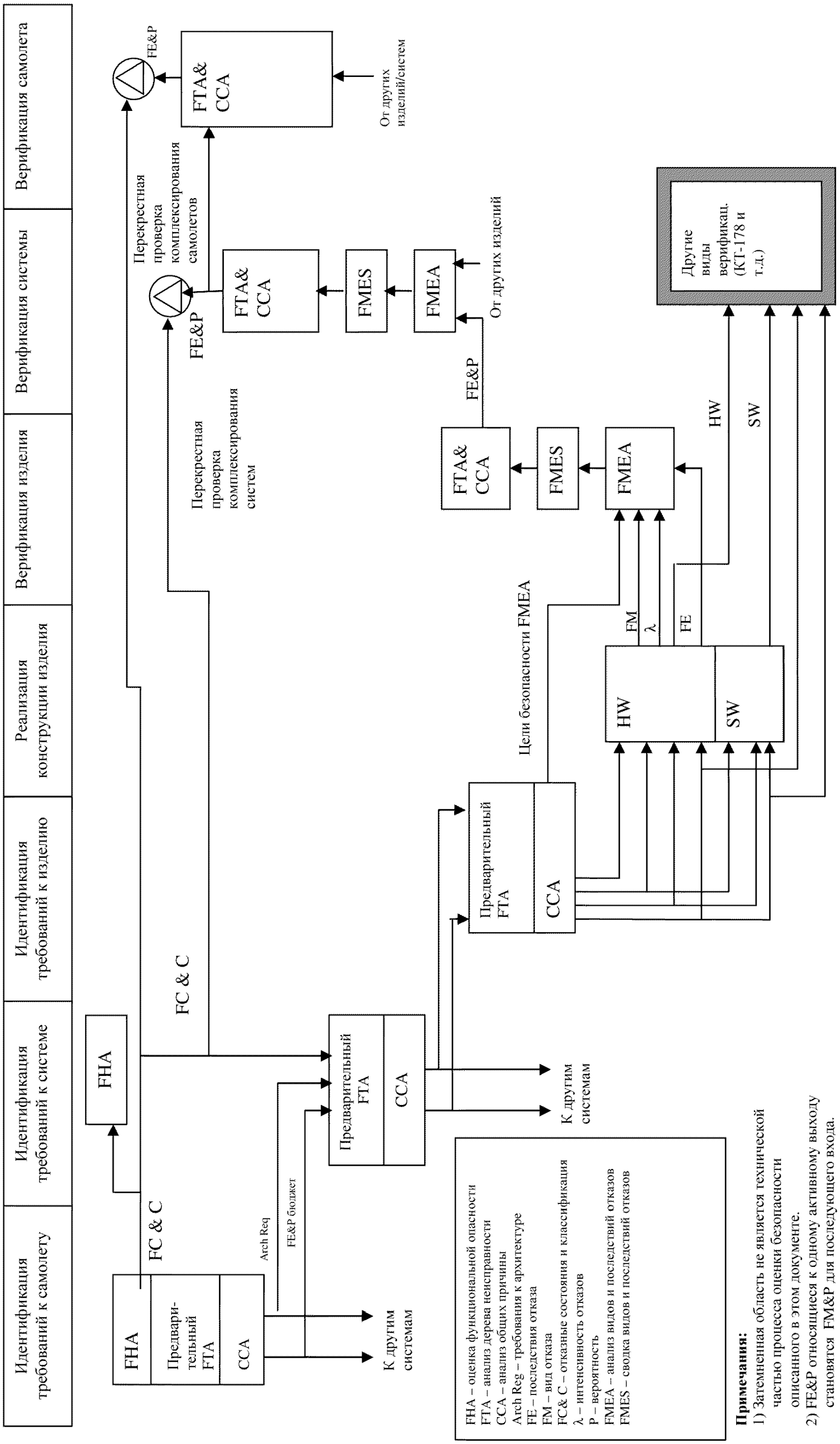
Обзор процесса оценки безопасности
Рис. 1

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
	АРМАК&JAA	Частый	Умеренно вероятный	Маловероятный	Крайне маловероятный	Практически невероятный
Классификация отказных состояний	FAA	Незначительное		Сложное	Опасно сложное	Катастрофическое
	АРМАК&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.
	АРМАК	– 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	Р-4754	Уровень D		Уровень С	Уровень В	Уровень А

Пример взаимосвязи FHA и FTA/FMEA
Рис. 2

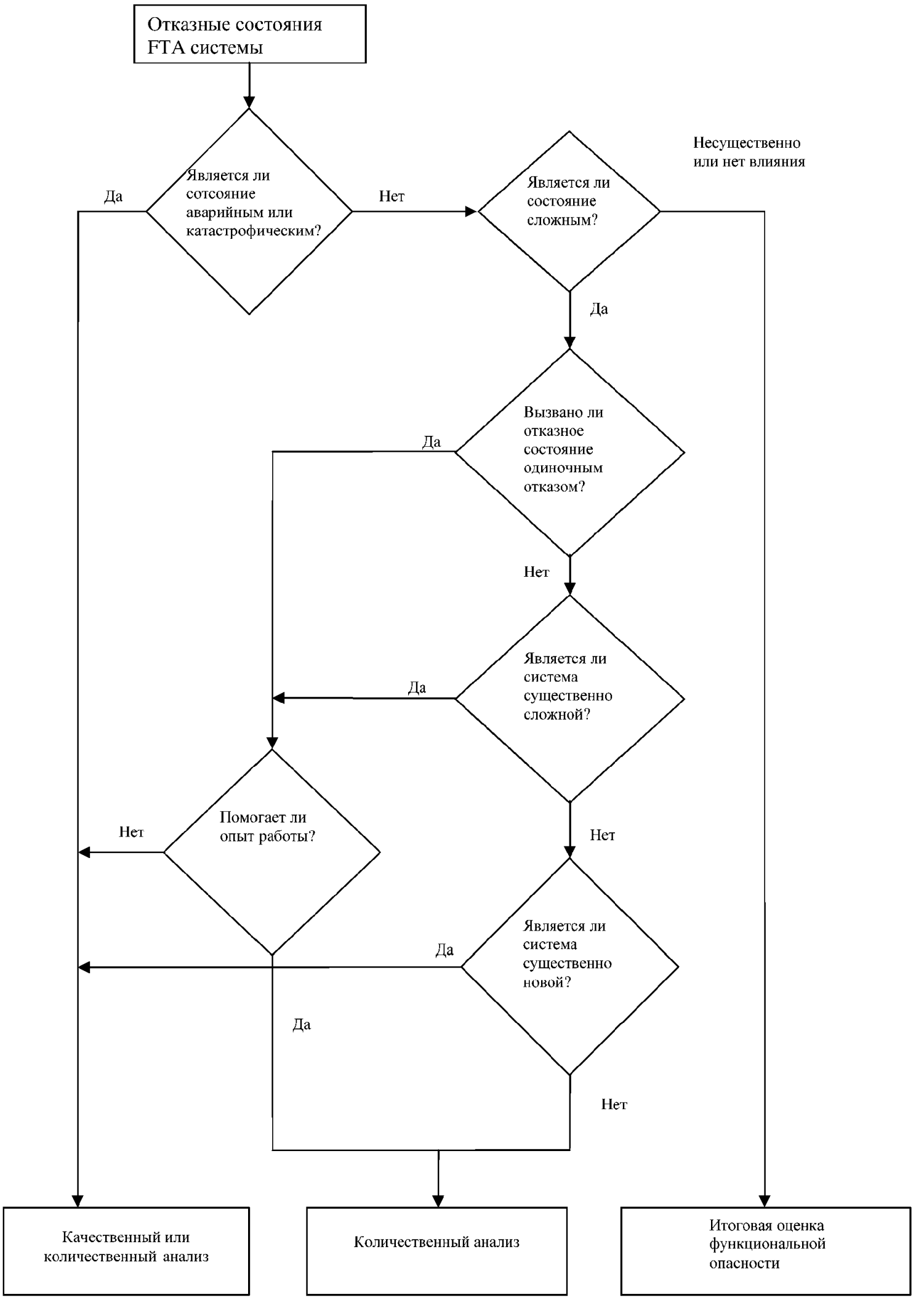




Примечания:

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



Пути подготовки плана верификации безопасности
Рис. 4

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:

(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.

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

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.

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.

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).

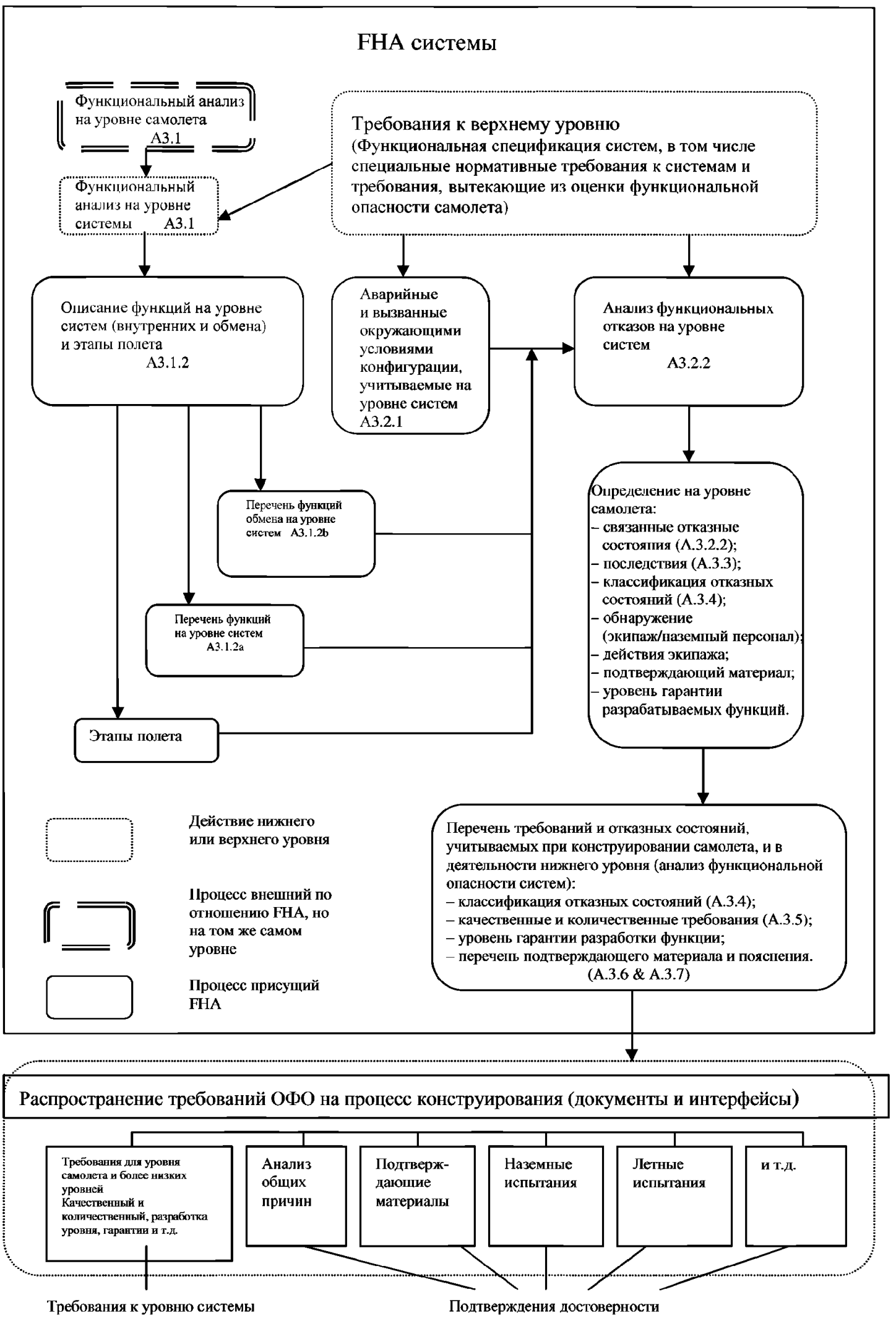
A.4.2 Связь FHA с PSSA

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.

Оценка функциональной опасности на уровне самолета
Рис. A1



Оценка функциональной опасности на уровне систем
Рис. A2

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.

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.

(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.

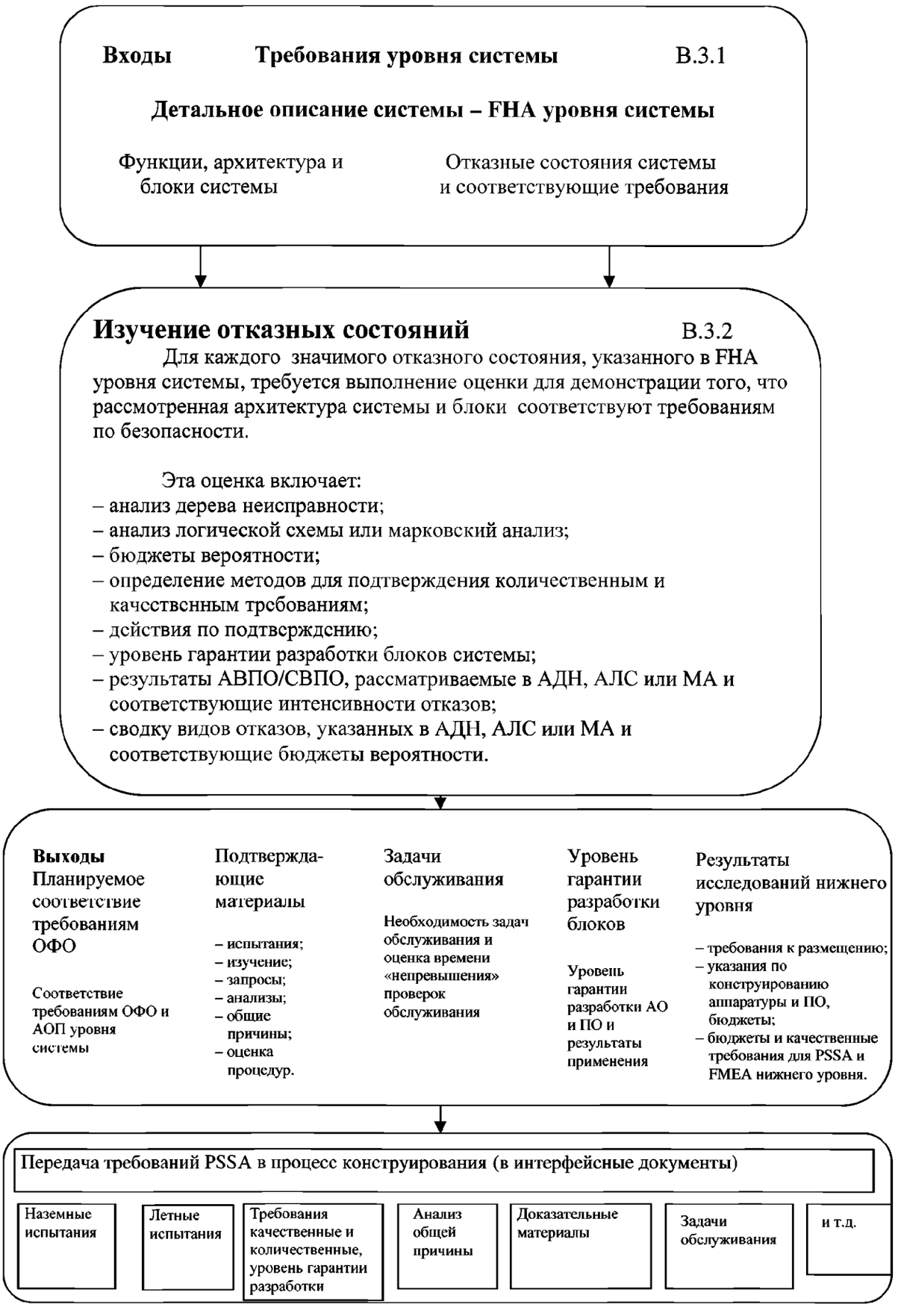
h. Эксплуатационные требования (для полета и обслуживания).

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.



Процесс PSSA уровня системы
Рис. B1

ПРИЛОЖЕНИЕ С

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.*

С.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.

С.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.

С.3 ПРОЦЕСС SSA

Процесс SSA использует восходящий подход для верификации соответствия целям и требованиям по безопасности конструкции. На рис. С1 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.

С.3.1 Верификация требований к конструкции FHA

С.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.

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

С.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.

С.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.

С.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).

С.3.2.3 Верификация соответствия требованиям к конструкции из ССА

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).

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.

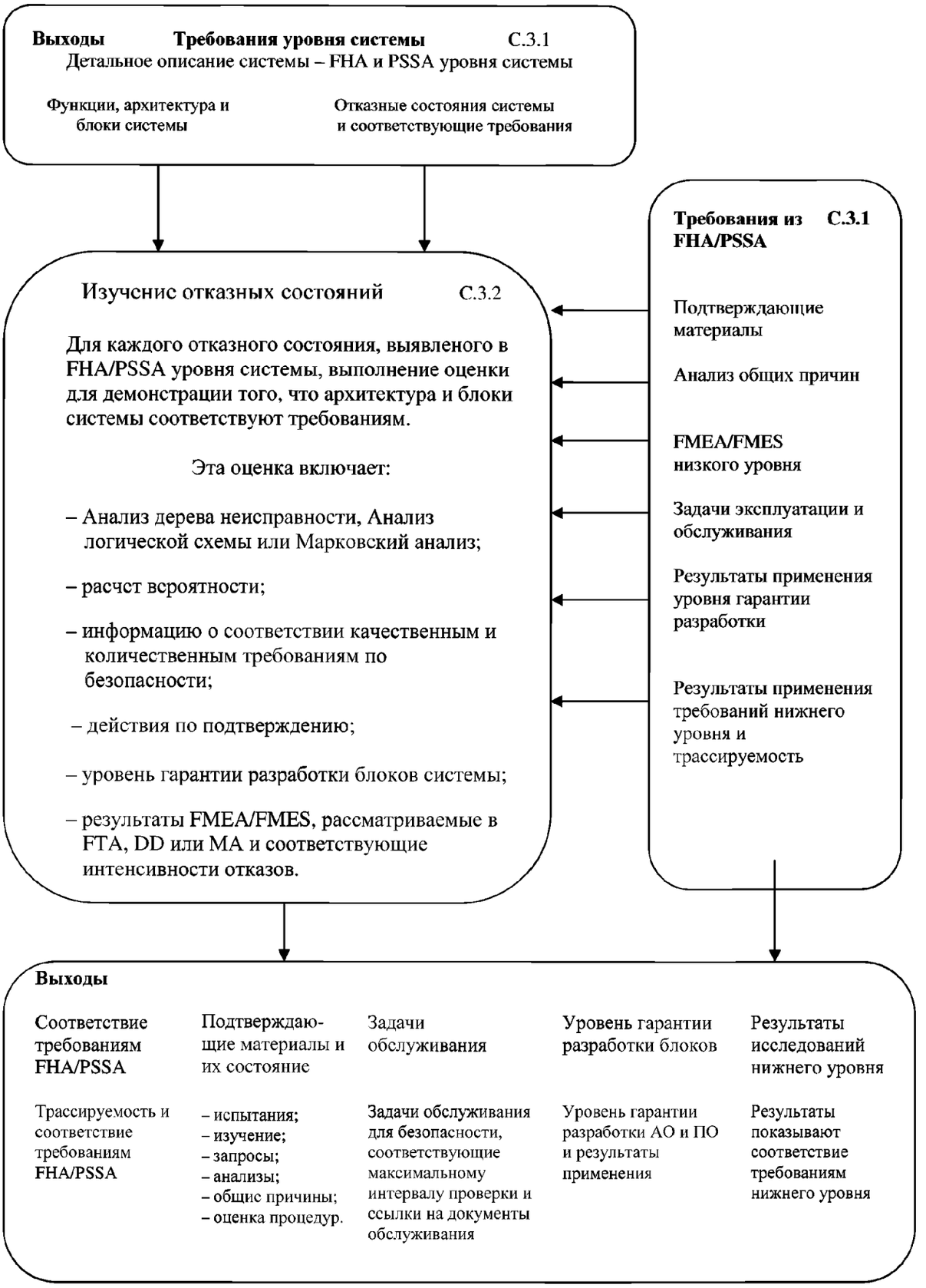
c. Материалы, используемые для валидации классификации отказных состояний.

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.



Процесс SSA уровня системы
Рис. С1

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).

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»).

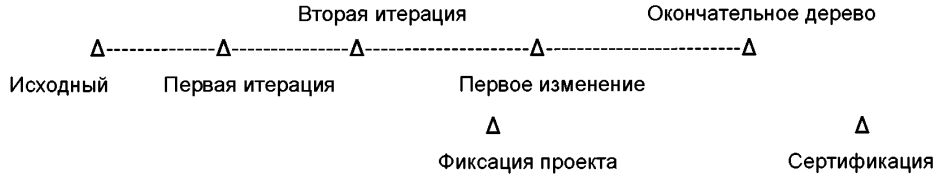
D.3 РОЛЬ FTA В ОЦЕНКЕ БЕЗОПАСНОСТИ

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.

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.

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.

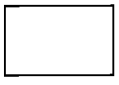
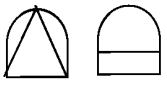
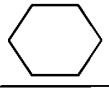
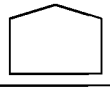
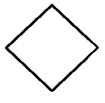
Математические символы, применяемые в тексте приложения, включают:

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

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.

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.

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.

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

D.9.2 Конструирование верхнего и промежуточных ярусов дерева неисправности

Этот раздел рассматривает второй шаг конструирования дерева неисправности.

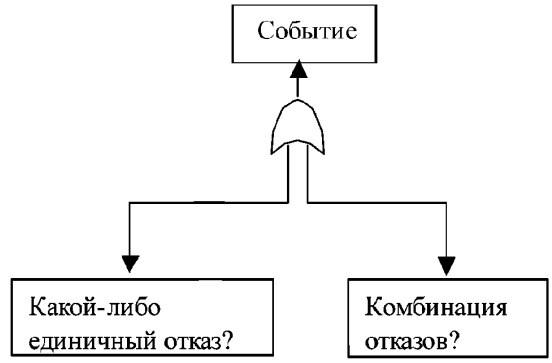
2. Разрабатываются верхний и промежуточные ярусы дерева неисправности. Определяются промежуточные отказы и комбинации отказов, которые являются минимальными, непосредственными, необходимыми и достаточными для того, чтобы произошло событие верхнего уровня, и связываются соответствующими стандартными логическими 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:

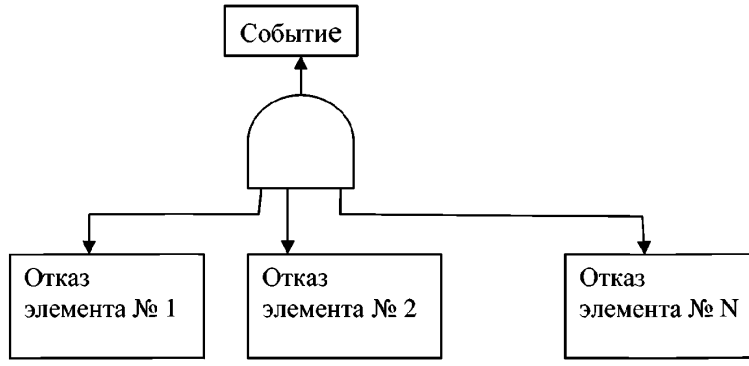
a. Имеются ли там любые одиночные отказы, которые заставят внесенное в перечень событие быть истинными?

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

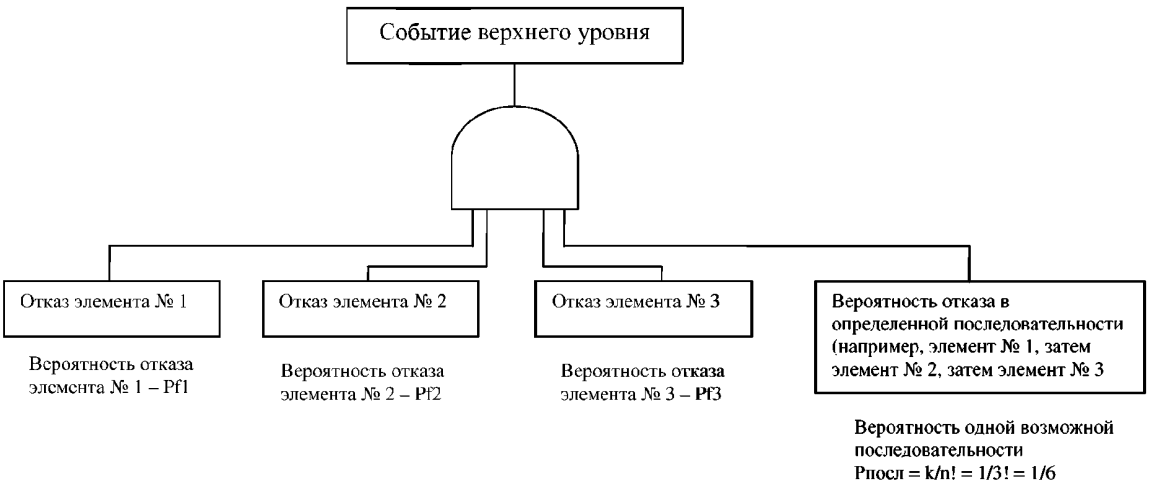
Если нет никаких одиночных отказов, но имеются кратные комбинации отказов, то первый ярус дерева неисправности может быть показан подобно указанному на рис. D4.



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

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.

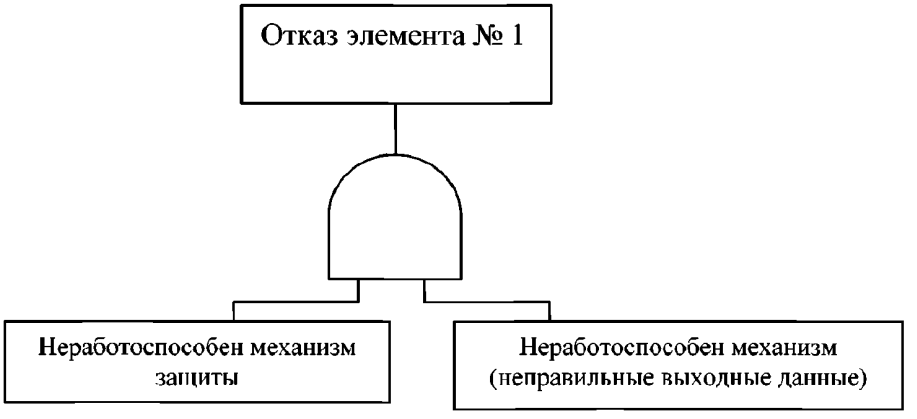
Например, предположим, что в рассмотренной ранее системе имеется три элемента. Первый ярус дерева неисправности будет представлен как на рис. D5.



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

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.

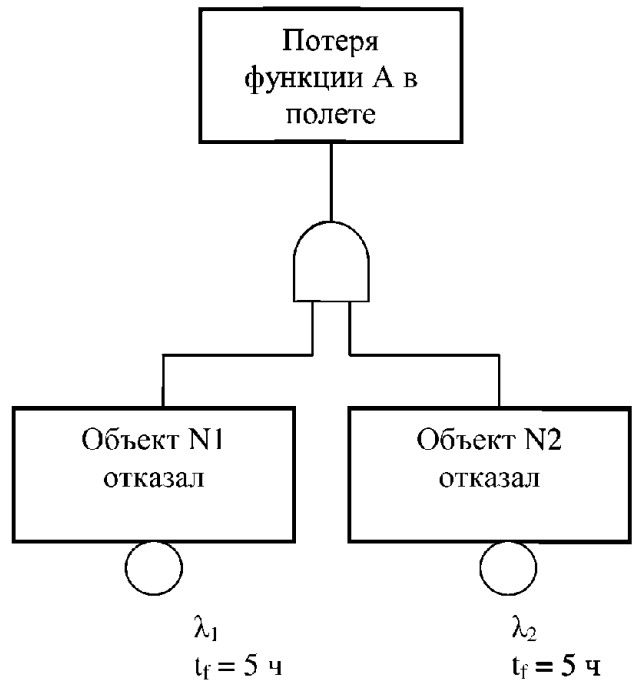
Далее выполняющий анализ должен разработать и завершить дерево неисправности, расширяя ветви дерева неисправности вплоть до первичных событий (то есть до основных событий, внешних событий и неразрабатываемых событий). Эти первичные события являются корневыми причинами отказных событий первого уровня.

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

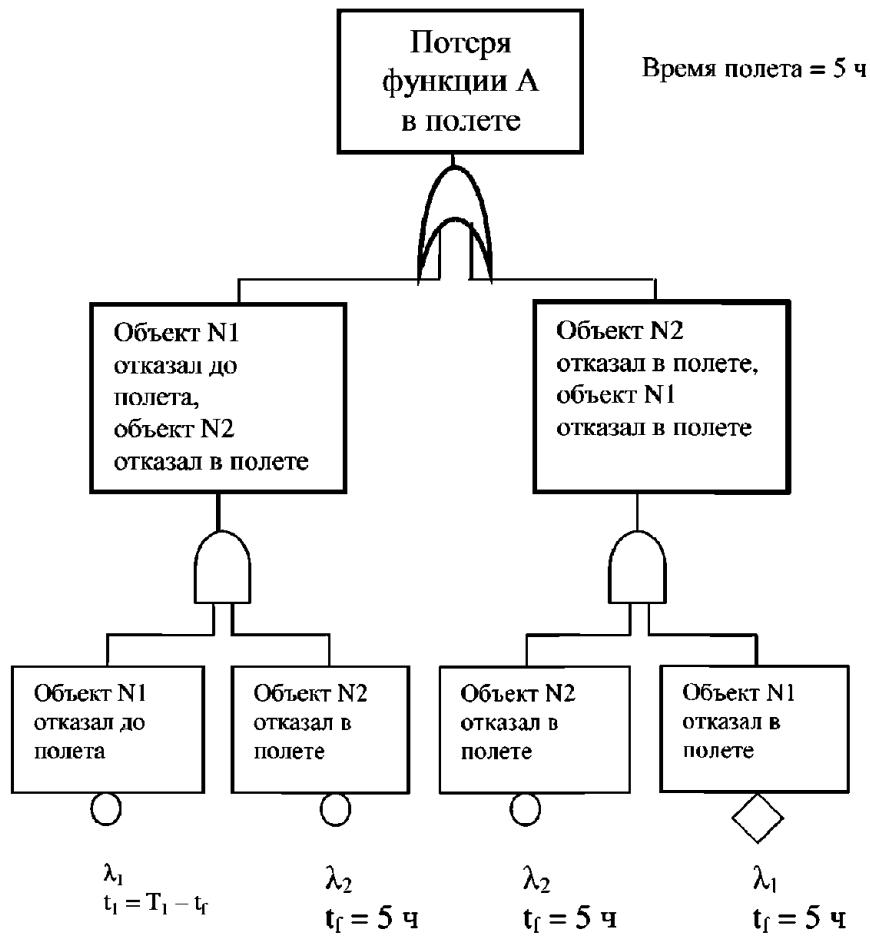
Дерево неисправности первого примера, приведенное на рис. D7, показывает простой вариант отказа, когда событие верхнего уровня вызывается отказом двух элементов в одном и том же полете. Известно, что оба элемента были работоспособны в начале полета и отсутствовали скрытые отказы. Два отказа могут возникнуть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



Пример структуры дерева неисправности, когда отказ двух элементов приводит к потере функции
Рис. D7

D.9.3.2 Пример, когда два отказа элементов вызывают потерю функции при возможном скрытом отказе элемента.

Во втором примере, элемент 1 может отказать в любой момент между временем его проверки (время = ноль) и временем следующей проверки (время = Т). Известно, что элемент 2 был работоспособен в начале каждого полета и никогда не отказывает скрыто. Порядок отказа не имеет значения. Пример дерева неисправности показан на рис. D8.



Пример структуры дерева неисправности, когда отказы двух элементов приводят к отказу функции, при этом один элемент может отказать скрыто
Рис. D8

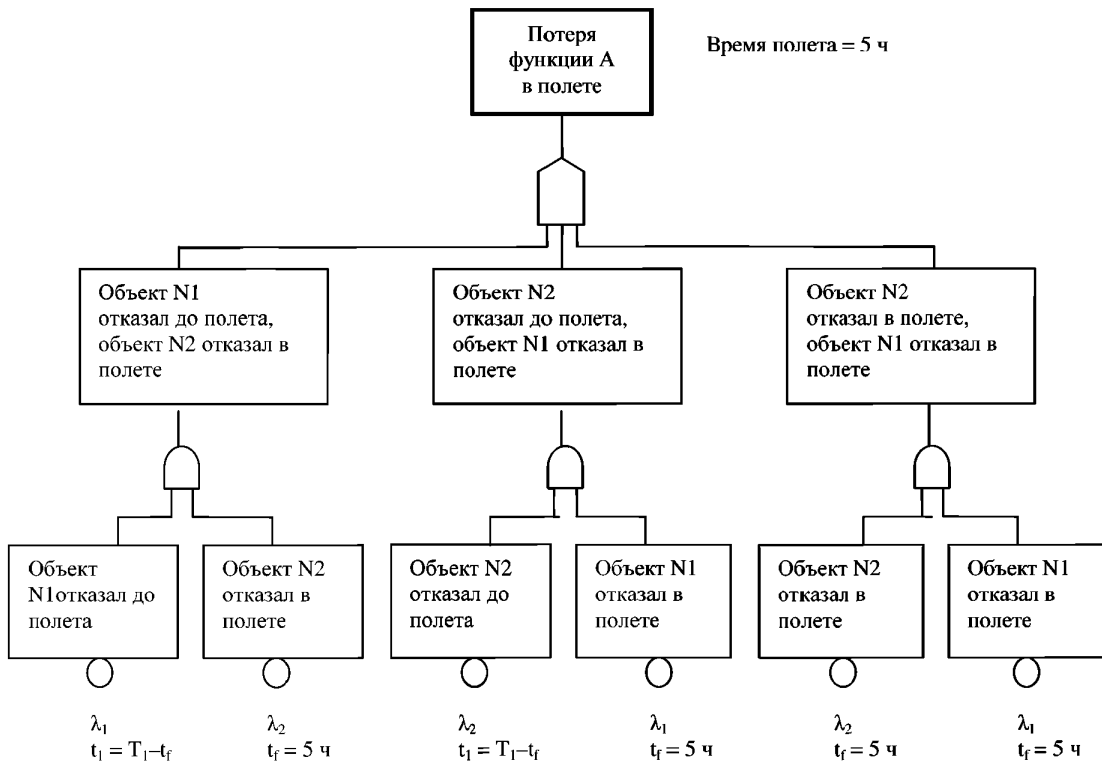
D.9.3.3 Пример потери функции из-за отказа двух элементов, причем каждый элемент может отказать скрыто.

В третьем примере каждый элемент может отказать скрыто, но если оба отказали, это будет обнаружено по их влиянию на возникновение события верхнего уровня. Поэтому, по крайней мере, один элемент должен быть работоспособным в начале полета. Пример дерева неисправности дан на рис. D9. По этому рисунку следует отметить три положения.

1. Неразрабатываемое событие по порядку отказа (т.е. ROF = k / n как показано на рис. D5 и рассматривается в D.11.1.4) не требуется, потому, что зависимость порядка событий встроена в структуру дерева через период скрытости ($t_n = T_n - t_1$). Это представляет отказ до полета в период скрытости.

2. Крайне правый И-символ необходим для описания варианта, когда оба элемента отказывают во время полета вне требуемой последовательности.

3. Крайне правый И-символ часто пропускается и время риска принимается равным интервалу проверки для случая, когда t_1 много меньше интервала проверки.

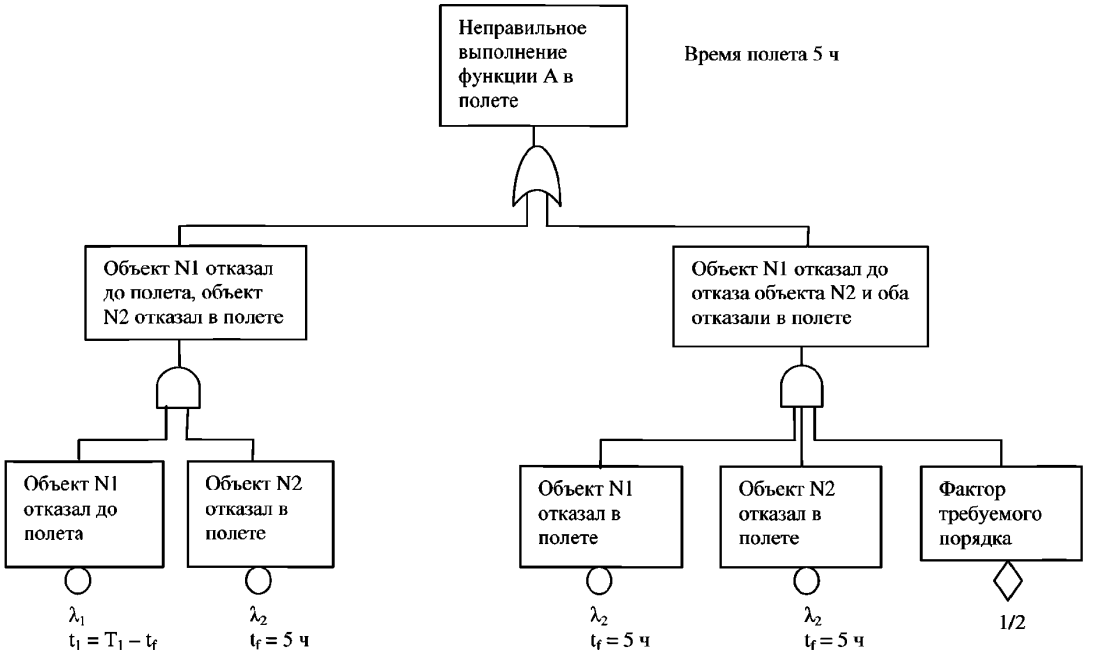


Пример структуры дерева неисправности, когда отказы двух элементов приводят к потере функции и каждый элемент может отказать скрыто
Рис. D9

D.9.3.4 Пример, когда отказы двух элементов приводят к событию верхнего уровня, при этом один элемент может отказать скрыто и последствия зависят от порядка.

В четвертом примере один элемент (со скрытым состоянием) должен отказать до отказа второго. В противном случае события верхнего уровня не будет. Известно, что второй элемент работоспособен в начале полета. Это типично для случая отказа средств контроля, когда событием верхнего уровня является неправильный выходной сигнал, а не потеря функции. Пример включающий передачу неправильных данных приведен на рис. D10.

Фактор необходимого порядка используется по D.11.1.4.



Пример структуры дерева неисправности, когда отказы двух элементов приводят к событию верхнего уровня, при этом один элемент может отказать скрыто и последствия зависят от порядка
Рис. D10

D.9.4 Оценка дерева неисправности на соответствие требованиям по безопасности

Этот раздел рассматривает четвертый шаг конструирования дерева неисправности.

4. Оценивается дерево неисправности качественно и/или количественно.

Деревья неисправности по своей природе являются качественными моделями. В зависимости от цели FTA оценка дерева неисправности будет выполняться качественно или количественно. Если дерево неисправности содержит отказы аппаратуры и ошибки разработки (аппаратуры или программного обеспечения), то даже количественная оценка в действительности будет комбинацией двух методов. В таблице D4 приведены результаты двух методов оценки. Эту таблицу следует использовать при определении цели FTA. В разделах D.10 и D.11 рассматриваются соответственно качественная и количественная оценка.

Таблица D4. Методы и результаты качественной и количественной оценки

Качественная	Количественная
Минимальный установленный набор Комбинация отказов компонент, вызывающая отказ системы	Численные вероятности Вероятности отказов системы и установленного набора
Качественное значение Качественная классификация влияния на отказы системы, влияние на отказобезопасность непосредственных причин и комбинаций	Количественное значение Количественная классификация влияний на отказ системы
Причины общих ошибок Выделение минимальным установленным набором потенциальной восприимчивости к одиночному отказу	Оценки чувствительности Влияние изменений в моделях и данных, определение ошибок

D.10 КАЧЕСТВЕННАЯ ОЦЕНКА ДЕРЕВА НЕИСПРАВНОСТИ

При качественной оценке дерева неисправности формируется минимальный установленный набор. Он может использоваться для определения качественной классификации и оценки причины общих ошибок.

Следующие разделы содержат небольшой объем информации необходимой для понимания предмета рассмотрения. Для более подробного и полного объяснения этих методов следует обратиться к документу "Fault Tree Handbook" (NUREG-0492) или к одной из многих подобных книг по оценке дерева неисправности.

D.10.1 Определение минимального установленного набора дерева неисправности

Минимальный установленный набор дерева неисправности является самым маленьким набором Первичных событий, которые должны произойти для возникновения Нежелательного события верхнего уровня.

Выполняющий анализ должен сознавать возможную потерю независимости двух или более Первичных событий дерева неисправности, чтобы избежать грубых ошибок в качественном и количественном анализе. Эта потеря независимости может происходить всякий раз, когда то же самое событие появляется в более чем одном месте дерева неисправности или когда некоторые одиночные отказы могут приводить к более чем одному отказному событию одновременно. Когда зависимость установлена, она моделируется введением одного и того же события в различные точки дерева неисправности и корректно учитывается применением булевой алгебры для получения установленных наборов. Следует обратить внимание на появление в дереве высокого уровня, когда Первичные события выводятся из событий верхнего уровня в различных анализах дерева неисправности, одинаковых событий в более чем одном из таких деревьев. В этом случае для дерева высокого уровня зависимость не наблюдается, и расчеты будут неправильны. В этом случае для получения точных значений необходимо заменить разработанные Первичные события соответствующими детальными структурами дерева неисправности. Это обеспечит правильное моделирование общих событий в дереве высокого уровня и получение точных перечней установленных наборов и расчетов вероятности.

Выполняющий анализ может использовать «прямой анализ» на дереве неисправности, когда различные Первичные события появляются в данном дереве только один раз. Однако, это не типично для большинства бортовых систем. Более подробно применение метода описано в документе NUREG-0492.

a. Вероятность получения результата A обозначается как P(A), результата B – как P(B), и так же для других результатов.

b. Вероятность возникновения A И B обозначается как P(AB).

c. Вероятность возникновения A ИЛИ B обозначается как P(A+B).

d. Если A и B являются независимыми событиями с вероятностями P(A) и P(B), то вероятность возникновения обоих событий определяется произведением

   P(AB) = P(A) * P(B) – применимо для И-символа с двумя входами.

e. Если A, B и C являются тремя независимыми событиями с вероятностями P(A), P(B) и P(C), то вероятность возникновения трех событий определяется произведением P(AB) = P(A) * P(B) * P(C) – применимо для И-символа с тремя входами.

f. Аналогично рассматриваются четыре и более независимых события.

g. Если два независимых события могут возникнуть одновременно, то вероятность возникновения или A ИЛИ B или A И B есть
   P(A+B) = P(A) + P(B) – [P(A) * P(B)] – применимо для И-символа с двумя входами.

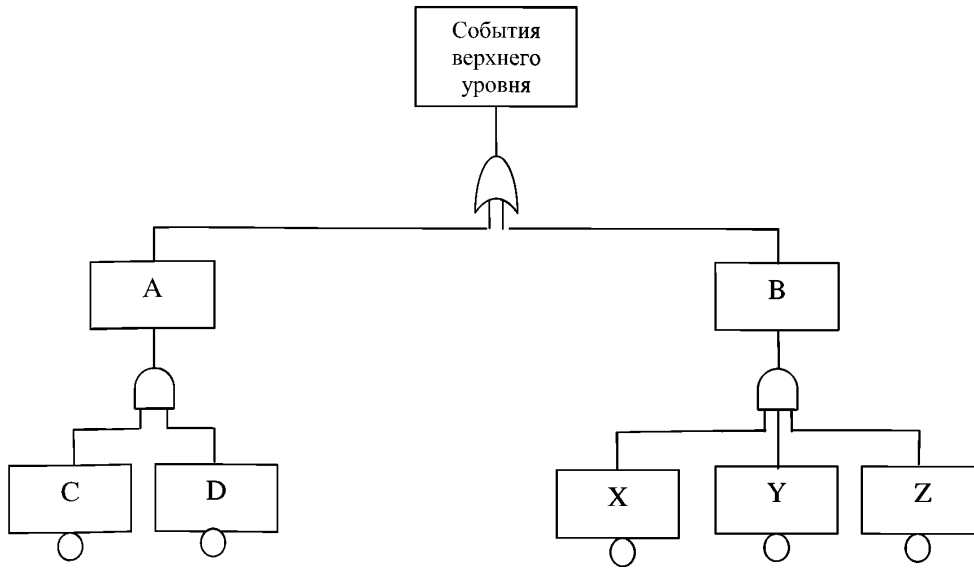
h. Если три независимых события могут возникнуть одновременно, то вероятность возникновения A ИЛИ B ИЛИ C или любой комбинации из этих трех будет
   P(A+B+C) = P(A) + P(B) + P(C) – [P(A) * P(B)] – [P(A) * P(C)] –
   [P(B) * P(C)] + [P(A) * P(B) * P(C)] – применимо для ИЛИ-символа с тремя входами.

Аналогично может быть получено для четырех и более независимых событий.

i. Если два события по существу исключают друг друга, так что при возникновении одного другое не может возникнуть, уравнение для ИЛИ-символа с двумя входами упрощается до P(A + B) = P(A) + P(B), при этом P(AB) равно нулю.

Это уравнение является хорошей аппроксимацией для двух взаимно не исключающих событий с малыми вероятностями (ошибки консервативны).

В качестве примера «прямого анализа» рассмотрим дерево на рис. D11.



Дерево для показа метода прямого анализа
Рис. D11

Из рис. D11 следует:

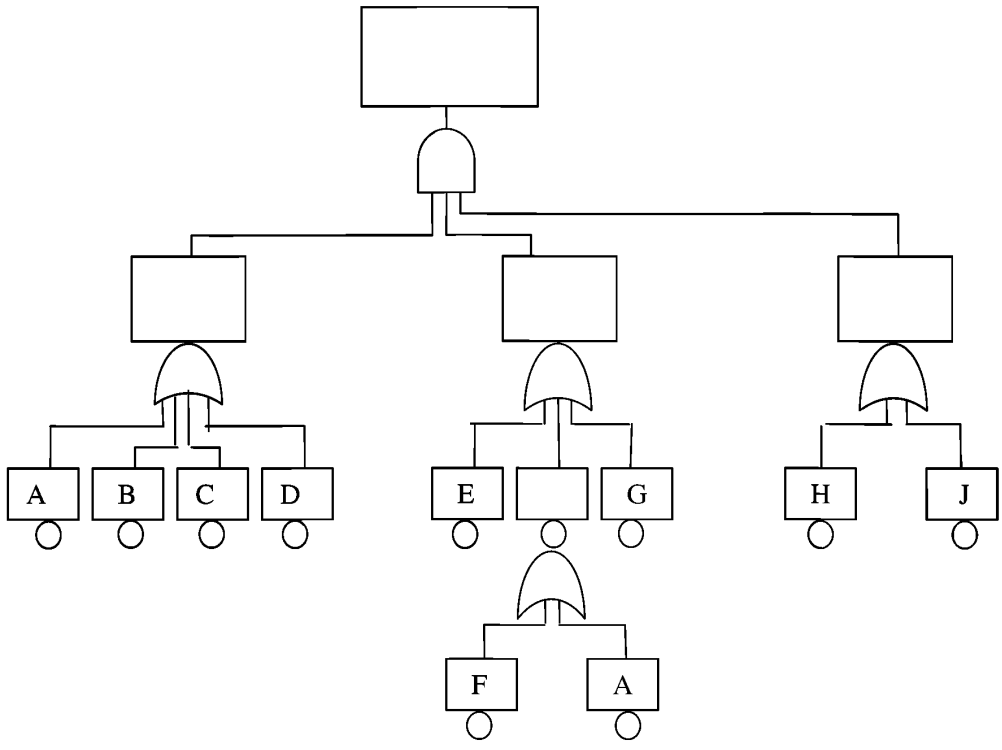
P(A) = P(C) * P(D) [C и D являются независимыми событиями].

P(B) = P(X) + P(Y) + P(Z) [X, Y и Z исключающие друг друга события].

P(СВУ) + P(A) * P(B) = [P(C) * P(D)] * [P(X) + P(Y) + P(Z)].

Выполняющий анализ должен провести Булев анализ по структуре дерева, если Первичное событие входит более одного раза в данное дерево. Основываясь на расположении этих идентичных Первичных событий в дереве, «прямой анализ» без первоначального уменьшения дерева при помощи Булева анализа приведет к вероятности нежелательного события верхнего уровня, которая будет больше или меньше действительной вероятности события.

В качестве примера уменьшения дерева неисправности при помощи Булева анализа, рассмотрим структуру дерева на рис. D12.



Дерево для демонстрации метода Булева уменьшения
Рис. D12

Булево уменьшение выполняется следующими шагами.

a. Используется «прямой анализ» для определения приемлемой «вершины». Термин «приемлемой» используется вследствие того, что событие A находится в двух ветвях дерева неисправности

вершина = (A+B+C+D) * (E+F+A+G) * (H+J)

b. Раскрываем скобки правой части с использованием символов разделенных знаками «+».

вершина = AEH + AFH + AAH + AGH + BEH + BFH + ABH + BGH + CEH +
+ CFH + ACH + CGH + DEH + DFH + ADH + DGH + AEJ +AFJ +
+ AAJ + AGJ + BEJ + BFJ + ABJ + BGJ + CEJ + CFJ + ACJ + CGJ +
+ DEJ + DFJ + ADJ + DGJ

c. Применяем следующие правила логики Буля к этому уравнению FTA

(1) A+A=A, (2) A*A=A, (3) A+AK=A, (4) AAK=AK

При использовании этих правил минимальный установленный набор дерева неисправности определяется сокращением элементов в сочетаниях и сокращением общего числа сочетаний. Преобразуем уравнение из шага b

вершина = ~~AEH~~ + ~~AFH~~ + ~~AAH~~ + ~~AGH~~ + BEH + BFH + ~~ABH~~ + BGH + CEH +
+ CFH + ~~ACH~~ + CGH + DEH + DFH + ~~ADH~~ + DGH + ~~AEJ~~ +~~AFJ~~ +
+ ~~AAJ~~ + ~~AGJ~~ + BEJ + BFJ + ~~ABJ~~ + BGJ + CEJ + CFJ + ~~ACJ~~ + CGJ +
+ DEJ + DFJ + ~~ADJ~~ + DGJ

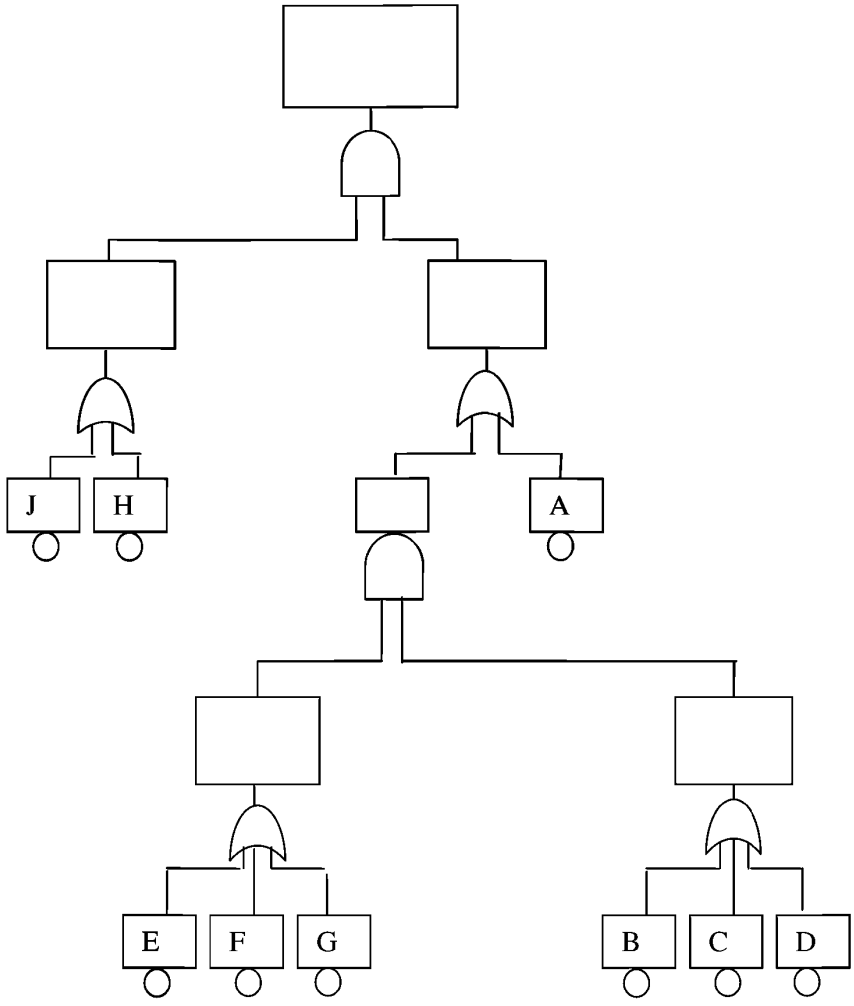
Перепишем полученное уравнение в минимальный установленный набор дерева неисправности. Отметим, что было удалено двенадцать сочетаний и два сочетания из трехэлементных стали двухэлементными.

вершина = AH + BEH + BFH + BGH + CEH + CFH + CGH + DEH + DFH +
+ DGH + AJ + BEJ + BFJ + BGJ + CEJ + CFJ + + CGJ + DEJ + DFJ + DGJ

d. Нарисуем уменьшенное дерево неисправности, объединив прежде сочетания в уравнении минимального установленного набора (не обязательный шаг). Уменьшенное дерево неисправности показано на рис. D13.

вершина = (J + H) * [A + (E + F + G) * (B + C + D)].

Многие коммерчески доступные программные пакеты анализа дерева неисправности будут автоматически создавать минимальный установленный набор при задании соответствующих команд. Как только уменьшенное дерево нарисовано, выполняющий анализ обязан проверить, что все И-символы показывают правильную комбинацию независимых событий. Этот шаг очень важен перед началом численных расчетов FTA.



Уменьшенное дерево неисправности
Рис. D13

D.10.2 Определение качественной значимости

Для того чтобы получить некоторое представление о том, как различные минимальные установленные наборы воздействуют на нежелаемое событие верхнего уровня, выполняющий анализ может оценить дерево неисправности, используя метод известный как Качественная значимость. Качественная значимость является простым упорядочиванием установленных наборов в возрастающем порядке на основе числа Первичных событий в установленном наборе. Метод позволяет выполняющему анализ увидеть относительную важность различных Первичных событий в отношении вызываемого события верхнего уровня, основываясь на числе

вхождений Первичного события в установленный набор и на том в каких комбинациях с другими Первичными событиями оно появляется. Этот метод оценки FTA хорошо работает с аппаратными отказами/ошибками разработки, с ошибками разработки программного обеспечения и с их комбинациями в том же дереве.

Предположим, что аналитик хочет оценить дерево неисправности с использованием качественной важности. Сначала, установленный набор упорядочивается, как описано выше. Это упорядочение дает аналитику знание о том, имеет ли событие верхнего уровня какие-либо единичные отказы и как часто каждое Первичное событие приводит к возникновению верхнего события.

Кроме того, приняв стандартное значение интенсивности отказов (например, 1E-06) и стандартное время риска (например, 100 часов) для всех аппаратных составляющих относящихся базовых событий, аналитик может получить оценку сверху относительной важности установленных наборов. Например, используя приведенные в предыдущем предложении значения, установленный набор с двумя Основными событиями имеет вероятность отказа (P_t) порядка 1E-08, а установленный набор из трех Основных событий имеет P_t порядка 1E-12. Используя этот метод оценки сверху аналитик может быстро заключить, что установленный набор из пяти или более Основных событий имеет очень малое относительное влияние на вероятность появления события отказа верхнего уровня.

Недостатки такого метода оценки следующие:

a. Если аналитик имеет аппаратное Основное событие на уровне идентификации выше чем уровень компонент, то дополнительный анализ надежности следует выполнять в порядке получения представительных значений интенсивностей отказов для оценки P_t.

b. Расчетное время основного события может значительно изменяться от одного Основного события к другому вследствие таких факторов, как время цикла контроля, время риска контроля, интервалы Обслуживания и т.д. Следовательно, полученные вероятности отказов, используемые для взвешивания относительной важности одного установленного набора к другому, не лучше чем оценки сверху. Изменения времени воздействия могут приводить к отличию на два или три порядка в значении оценки вероятности и полученного численным расчетом значения вероятности.

D.10.3 Уязвимость общей причиной

Дерево неисправности может быть качественно оценено с использованием метода известного как Восприимчивость общей причины формирующего перечень Возможных общих причин. Восприимчивость общей причины основывается на том факте, что установленный набор дает конечное перечисление комбинаций Первичных событий, которые приводят к возникновению события верхнего уровня. Аналитик может получить представление о восприимчивости события верхнего уровня к отказам общей причины, проверяя каждый установленный набор. Единичный отказ должен вызвать более чем одно первичное событие в установленном наборе для того, чтобы быть классифицированным как отказ общей причины. Поэтому, установленный набор, содержащий подобные первичные события более вероятно уязвим к отказам общей причины, чем установленный набор имеющий несхожие Первичные события. Например, предположим, что установленный набор № 1 имеет три Первичных события и каждое из них является процессором одного и того же типа в системе из трех несхожих резервируемых частей. Предположим, что установленный набор № 2 также имеет три Первичных события, в каждом из которых есть процессоры различных типов в строенной системе с несхожим резервированием. Проверяя эти два установленных набора, аналитик может легко определить, что установленный набор № 1 имеет больше возможностей для возникновения неисправности общей причины, подобной порождаемой ошибкой микрокода, чем установленный набор № 2.

Каждую возможность для отказа общей причины следует проверить для определения реального существования единичной причины, которая может вызвать такие комбинации отказов и привести к указанному событию. Такие неисправности общей причины анализируются с позиций вероятности и их следует внести в дерево неисправности, если они не могут быть предотвращены в системе.

Анализ общих причин будет обращаться к неисправностям общей причины и порождаемым ошибкам. В приложениях I, J и K содержится подробная информация по выполнению анализа общей причины.

D.10.4 Определение уровня гарантии разработки аппаратуры и программного обеспечения

Минимальный установленный набор дерева неисправности может использоваться для определения надлежащего уровня гарантии разработки для аппаратуры и программного обеспечения при выполнении PSSA.

Описанные в P-4754 правила, следует использовать при рассмотрении архитектуры системы для определения уровня гарантии разработки для аппаратуры и программного обеспечения, для назначения уровня, который отличается от связанного с категорией отказного состояния события верхнего уровня.

Когда аппаратура и/или программное обеспечение в анализе безопасности связаны более чем с одним событием верхнего уровня, следует назначить высший уровень гарантии разработки, который получается из рассмотрения каждого дерева неисправности. Пример дерева неисправности, которое включает рассмотрение аппаратных и программных ошибок приводится в разделе D.12.

D.11 КОЛИЧЕСТВЕННАЯ ОЦЕНКА ДЕРЕВА НЕИСПРАВНОСТИ

Методы количественной оценки дерева неисправности дают результаты трех типов: (1) численные вероятности, (2) количественное значение и (3) оценку чувствительности. Все три результата могут быть получены для минимальных установленных наборов, рассмотренных в разделе D.10. Другие существующие методы могут быть более эффективны для некоторых деревьев неисправности. Следующие разделы дают только минимальную информацию необходимую для понимания предмета рассмотрения и ограничены демонстрацией элементарных примеров, которые основаны на предположении о постоянных интенсивностях отказов и малости λt. Для более подробного и полного пояснения этих методов, следует обратиться к "Fault Tree Handbok" (NUREG-0492) или к другой подобной книге по теме оценки дерева неисправности.

Методы количественного анализа дерева неисправности, отличающиеся от рассматриваемых в этом разделе, логическая и математическая точность которых может быть показана, могут использоваться по усмотрению аналитика.

D.11.1 Численные расчеты вероятности

Количественная методика оценки для определения вероятности отказного события (P_f) дерева неисправности выполняется с использованием пяти основных шагов:

1. Определение минимального установленного набора дерева неисправности.

2. Определение интенсивности отказов Основных событий.

3. Определение времени экспозиции и времени «Риска» для Основных событий.

4. Установление любых факторов требуемого порядка.

5. Выполнение численных расчетов FTA.

Эти пять шагов рассматриваются далее в полседовательных подразделах. Заметим, что аналитик не может выполнять количественный анализ на минимальных установленных наборах содержащих ошибки разработки. Деревья неисправности, содержащие ошибки разработки, следует оценивать с использованием качественных методов оценки, которые рассмотрены в разделе D.10. Для деревьев неисправности, которые содержат первичные события с отказами аппаратуры, а также с ошибками разработки аппаратуры и программного обеспечения, аналитику необходимо выполнить численный анализ только по первичным событиям, относящимся к отказам аппаратуры. Раздел D.12 рассматривает введение ошибок разработки в дерево неисправности более подробно.

D.11.1.1 Определение минимальных установленных наборов дерева неисправности

Процесс определения минимальных установленных наборов для количественного оценивания FTA в точности повторяет процесс, который используется при качественном оценивании. Об этом написано в D.10.1.

D.11.1.2 Определение интенсивностей отказов основных событий

Следует определить интенсивность отказов для каждого относящегося к аппаратуре основного события. Интенсивности отказов необходимо определять насколько возможно по данным об интенсивностях отказов уже используемого подобного оборудования. Имеются широко известные в промышленности справочники по интенсивностям отказов и распределению видов отказов. Хотя эти документы дают основу для интенсивности отказов некоторых типов компонент, может быть много устройств, которые не включены в такие документы. Это в особенности относится к цифровым интегральным микросхемам, которые необходимо рассматривать в некоторых случаях. Определение видов отказа цифровых устройств в основном требует технического подтверждения и маловероятно, что для сложных цифровых интегральных схем могут быть определены все виды отказа. При выполнении FTA как части SSA, интенсивности отказов для основных событий могут быть найдены в имеющихся применимых FMEA/FMES. Обращение к FMES может быть ясно сделано в каждом основном событии для целей трассируемости.

D.11.1.3 Определение времени воздействия и времени риска для основных событий

Аналитик должен определить Время воздействия или интервал риска связанные с каждым основным событием в дереве неисправности. Ниже приведены различные типы основных событий:

Основное событие, связанное с потерей или неправильным выполнением функции объекта используемого в течение полета.

Основные события, связанные с потерей или неправильным выполнением функции объекта только в течение отдельных этапов полета.

Основные события, связанные со скрытым отказом выполняющего функцию объекта.

Основные события, связанные с потерей или неправильным выполнением элементов защиты (например, неисправность средств контроля).

В последующих подразделах описываются способы определения времени воздействия связанных с каждым из этих типов событий.

D.11.1.3.1 Потеря или неправильное выполнение функции объекта используемого в течение полета

В этом случае анализируемый объект используется в течение всего полета. Когда объект отказывает или функционирует неправильно, это приводит к изучаемому отказному последствию. В этом случае интервал риска равен времени полета по типовому профилю.

D.11.1.3.2 Потеря или неправильное выполнение функции объекта используемого только в течение отдельных этапов полета

Имеется два основных подтипа событий связанных с потерей или неправильным выполнением функций объектом, который используется только в течение отдельных этапов полета. В первом подтипе интервал риска равен времени от начала полета до окончания интересующего этапа. Например, предположим, что нас интересует событие «Выпуск шасси» и известно, что объект из состава оборудования, используемый для выпуска шасси, работал правильно при наземной проверке. Интервал риска для оборудования используемого для выпуска шасси определяется как период времени от наземной проверки до конца этапа полета «Выпуск шасси».

Во втором подтипе события, известно, что такой объект сохраняет работоспособность до начала его использования, и также используется только в течение отдельного этапа полета. Для такого подтипа интервал риска равен времени от завершения проверки функции до конца этапа полета. Например, предположим, что интересующим событием является «Автоматическая посадка» и известно, что объект из состава оборудования, используемого при автоматической

посадке самолета, работал правильно в ходе выполненной проверке при включении режима. Интервал риска для такого сценария определяется как время от выполненной проверки до касания самолетом земли.

D.11.1.3.3 Скрытые отказы

Скрытые отказы приводят к неработоспособности механизмов защиты или уменьшают границы безопасности, тем самым увеличивая уровень особых ситуаций из-за последующих условий или отказов. Скрытые отказы, как таковые, не несут опасности (т.е. они сами не оказывают воздействия, которое делает их заметными, в противном случае они не будут скрытыми по определению). Обычно скрытые отказы воздействуют на функции, которые не действуют при нормальной эксплуатации, но они обеспечивают свойство отказобезопасности и/или защиту от аномальных условий.

Скрытые отказы могут существовать на интервале времени, который или больше, или меньше времени полета. Этот интервал известен как время воздействия и определяется как время между наиболее поздним моментом, когда было известно о правильном функционировании и моментом, когда снова будет известно о правильном функционировании. Правильное функционирование может быть проверено приемлемыми испытаниями, проверками обслуживания, периодическим контролем, проверками при включении питания и т.д. Ключевым моментом управления скрытыми отказами является быстрое определение соответствующего отказного состояния и восстановление, что уменьшает время воздействия.

В случае постоянного контроля функции, ее время воздействия связано со временем воздействия средств контроля.

D.11.1.3.4 Полнота контроля и время воздействия

Обнаружение отказов может выполняться специальными аппаратными схемами, кодом программы или различными методами испытаний. Для целей этого раздела эти методы обнаружения отказа называются средствами контроля.

Обычно делаются следующие два трудноуловимые предположения, когда средства контроля вводятся в дерево неисправности:

Средства контроля обеспечивают 100% полноту контроля отказов выполняющего функцию блока.

Проверка средств контроля («зачистка») позволяет подтвердить их полную работоспособность (т.е. операция «зачистка» обеспечивает 100% полноту контроля).

К сожалению, в действительности средства контроля не могут обеспечить 100% полноту контроля. Для учета ограниченной полноты контроля аналитику следует рассмотреть специальные уточнения FTA.

На рис. D14 приведена модель системы, в которой средства контроля обнаруживают только 90% отказов в схемах реализации функции «X» когда средства контроля работают. В этом дереве неисправности достигнута 100% глубина проверки исправности средств контроля. Оставшиеся 10% отказов схемы реализации функции «X» не обнаруживаются до выполнения проверок технического Обслуживания объекта. Это упрощенное дерево дает консервативный результат потому, что в левой ветви дерева не рассматривается требуемый порядок отказов средств контроля и функции в одном полете.

Рис. D15 представляет рассмотренную систему для случая достижения 95% глубины проверок исправности средств контроля.

Для обеспечения эффективности многие методы обнаружения отказов могут требовать проверку надлежащего выполнения функции, тестирования или постоянного контроля. Каждый из этих уровней выявления отказов может иметь свое время воздействия и что должно соответственно учитываться. К числу обычно применяемых методов выявления относятся следующие.

Оперативный самоконтроль.

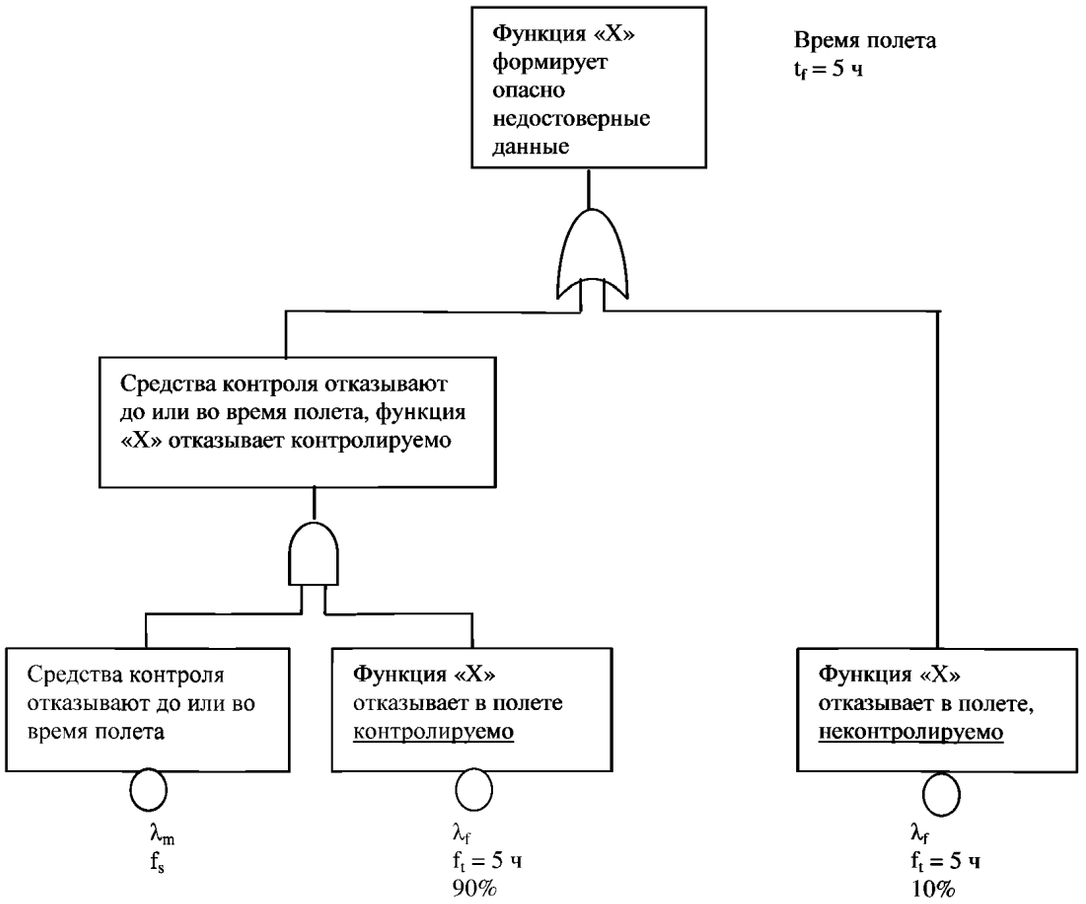
Проверка при включении питания.

Предполетный контроль.

Периодические проверки при техобслуживании.

Приемные испытания.

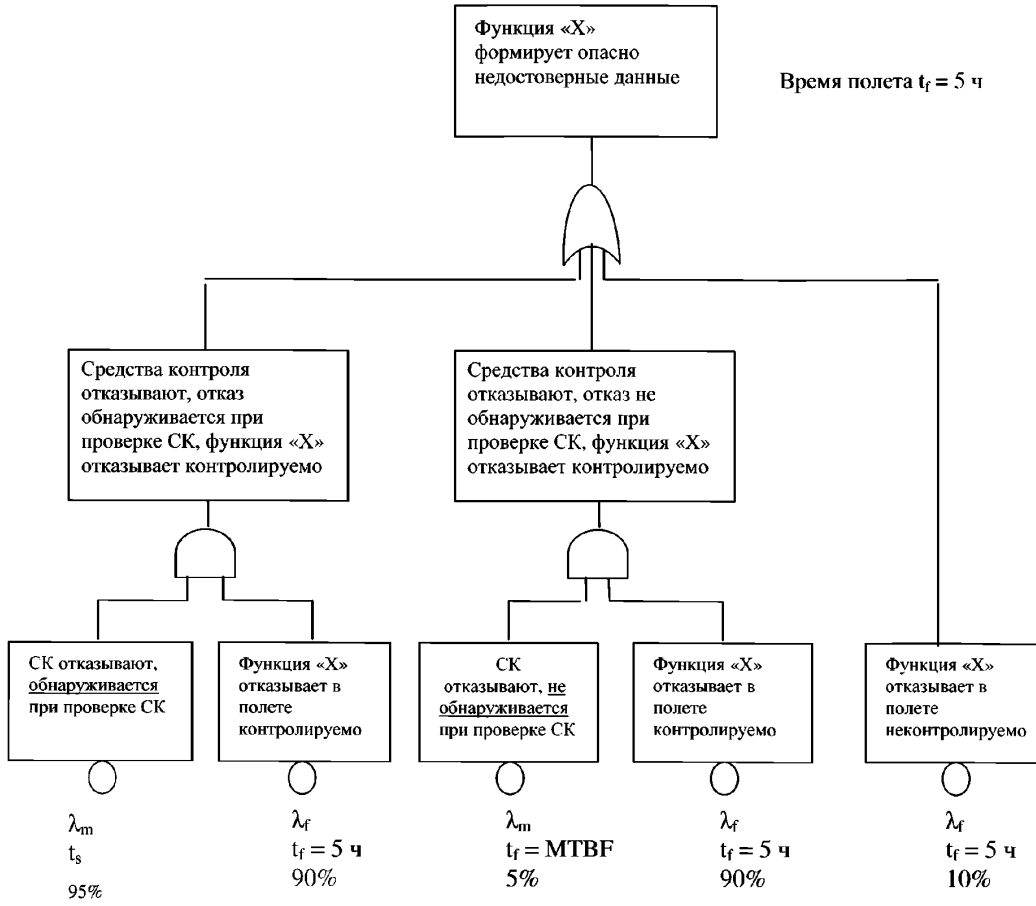
Испытания после установки на борт.



t_s = время проверки средств контроля

$P_t = 0{,}9\lambda_m\lambda_f t_s t_f + 0{,}1\lambda_f t_f$

Пример дерева неисправности для случая 90% глубины контроля отказов функции «X»
Рис. D14



t_s – время проверки средств контроля

$P_t = 0{,}9 \cdot 0{,}95\lambda_m\lambda_f t_s t_f + 0{,}9 \cdot 0{,}05 \cdot \lambda_m\lambda_f t_m t_f + 0{,}1\lambda_f t_f$

Пример дерева неисправности для случая 90% глубины контроля отказов функции «X» и 95% глубины проверок исправности средств контроля
Рис. D15

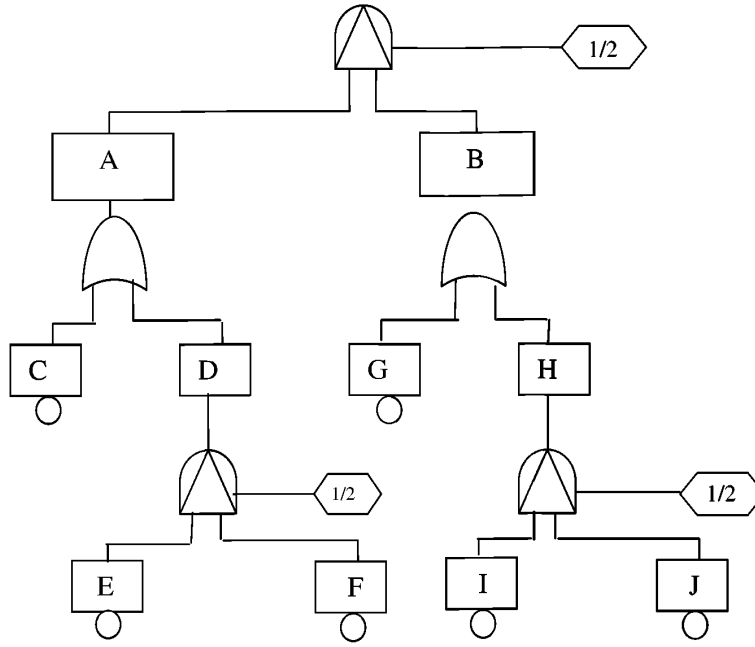
D.11.1.4 Установление уместных факторов требуемого порядка

И-символ дерева неисправности не предполагает специального порядка возникновения отказов. В некоторых случаях это может быть нереалистично. Примером служит комбинация отказов, когда для выявления отказов, которые могут вызвать событие верхнего уровня, используются средства контроля. Если первым отказывает контроль, то отказ может быть скрытым до следующей проверки средств контроля. Если первой отказывает схема функции «X», то событие верхнего уровня не возникает, потому что средства контроля сигнализируют об отказе.

При работе с событиями, зависящими от порядка отказов, в дерево неисправности может быть включен фактор, который делает рассчитанную вероятность менее консервативной. Этот фактор известен как Фактор требуемого порядка (ФТП) или Фактор последовательности. Для малых λt вероятность возникновения двух событий в некотором порядке (принимая, что оба отказали) составляет примерно 1/2 общей вероятности и поэтому ФТП для каждого порядка равняется 1/2. В общем случае, если у И-символа имеется n событий, то имеется n! возможных вариантов их последовательного отказа. Если только k из этих возможных вариантов приводят к событию верхнего уровня, то ФТП = k/n! Это значение действительно только для событий с одинаковым временем воздействия или для событий с различными временами воздействия, когда $(\lambda 1 + \lambda 2)T_{(Max)}$ меньше чем 1/2. В остальных случаях ФТП следует рассчитать. Пример использования ФТП показан на рис. D10.

Когда в дереве неисправности содержится много ФТП, при выполнении вычислений вероятности следует применять ФТП к минимальному установленному набору. Пример показан на рис. D16.

ФТП можно применять только когда все входные события И-символа имеют одинаковые времена воздействия.



Пример дерева неисправности содержащего Приоритетный И-символ и ФТП
Рис. D16

Из рис. D16 следует, что минимальный установленный набор будет
1/2 (P_fC*1/2*P_fE*P_fF) = 1/4* P_fC*P_fE*P_fF.

Это, однако, не совсем верно.

Аналитику следует разработать минимальный установленный набор по рис. D16 пренебрегая ФТП (т.е. P_fC*P_fE*P_fF). Затем, необходимо вычислить k/n!, определяя возможные комбинации, удовлетворяющие требуемому порядку. Их - 3! (т.е. шесть) возможных комбинаций, а именно, CEF, CFE, ECF, EFC, FCE и FEC. Ясно, что комбинация CEF удовлетворяет требуемому порядку, и ECF тоже может этому соответствовать. Для подтверждения этого необходимы дополнительные сведения о существующей системе. Поэтому, k может быть равно 1 или 2 и k/n! может равняться 1/6 или 1/3. Полное и более корректное уравнение для расчета вероятности этого минимального установленного набора будет или 1/6* P_fC*P_fE*P_fF или 1/3* P_fC*P_fE*P_fF. Это показывает, что использование ФТП в анализе установленных наборов может быть как оптимистическим, так и пессимистическим.

D.11.1.5 Выполнение численных расчетов FTA

После завершения указанных выше этапов, с использованием правил Булевой алгебры вычисляется вероятность отказа для события верхнего уровня [P_f(вершины)]. Для определения вероятностей в И-символах и ИЛИ-символах используются методы указанные в D.10.1.

При использовании постоянных интенсивностей отказов (т.е. элементы оборудования работают на горизонтальных частях кривой интенсивности отказов) вероятность безотказности для основного события (также называемая надежностью для основного события) определяется следующим выражением:

$$P_s = R = e^{-\lambda t} \qquad \text{(Ур. D1)}$$

где

P_s – вероятность появления,

R – надежность,

e – основание натурального логарифма,

λ – интенсивность отказа основного события,

t – интервал воздействия или Время риска.

Если использовать термины надежности, то можно сказать, что выживание и отказ компонентов дополняют и исключают друг друга. Для любого взятого периода времени:

$$P_s + P_f = P + Q = 1 \qquad \text{(Ур. D2)}$$

или

$$P_f = Q = 1 - e^{-\lambda t} \qquad \text{(Ур. D3)}$$

где

P_f – вероятность отказа,

Q – ненадежность.

Когда $\lambda t \leq 0{,}1$, уравнение D3 может быть упрощено до $P_f = Q\,\lambda t$.

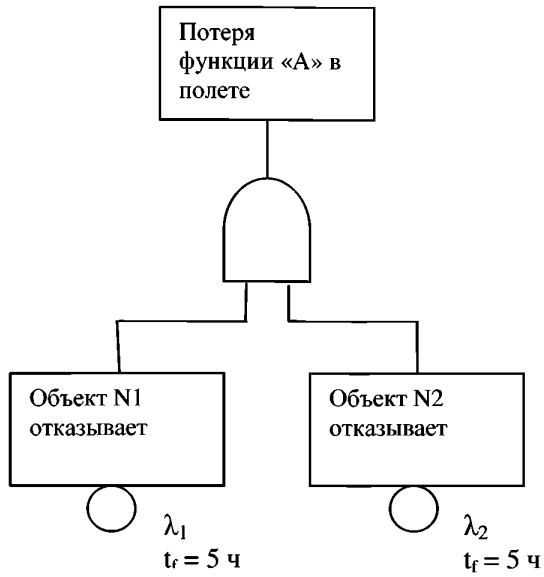
Численные расчеты FTA следует выполнять с использованием P_f, современные электронные системы имеют такую высокую надежность (R = 0,999...), что Q менее чувствительна к ошибкам округления и приводит к более точному значению P_f(вершины). Другими словами, в численных расчетах FTA следует применять значения вероятности отказов вместо значений вероятности безотказного состояния.

В случае если два скрытых отказа вызывают отказ системы, то приемлемым приближением является $n\lambda t_f$ при малых значениях для обоих механизмов отказа, но неправильно будет использовать при больших $n\lambda t_f$. Причиной является то, что если оба компонента в сдвоенной системе отказывают скрыто, то отказ должен быть обнаруживаемым. Поэтому подразумеваемым является предположение, что оба компонента исправны в начале полета. Поскольку этот вариант не включен в расчеты, результат может быть выше, чем необходимо при большом значении $n\lambda t_f$ (n является числом полетов в периоде Обслуживания). Правильный результат может быть получен с использованием Булевских выражений или Марковского анализа.

В разделах с D.11.1.5.1 по D.11.1.5.4 рассматриваются четыре специальных примера, которые поясняют типовые расчеты дерева неисправности с основными событиями, имеющими и не имеющими скрытых отказов и требуемого порядка факторов. Представленная в них методология формирует вероятность при двойных отказах для наиболее тяжелого случая в полете, а также для средней вероятности возникновения за полет события верхнего уровня. Для простых задач могут применяться различные методы расчета средней вероятности за полет. Но в случаях с двумя и более отказами или когда некоторые из рассмотренных выше предположений несправедливы, потребуется разработка точных формульных зависимостей, расчет вероятности за час полета рассматривается в разделе D.13. Для демонстрации соответствия без сложных вычислений средней вероятности может быть представлен консервативный анализ с использованием вероятностей за полет для наиболее тяжелого случая. Необходимо осторожное обращение с программными пакетами для расчетов дерева неисправности, поскольку они могут автоматически выбирать наиболее тяжелый случай или средние вероятности.

D.11.1.5.1 Расчет дерева неисправности, когда отказы двух объектов приводят к потере функции и ни один из них не имеет скрытый отказ.

Это простой случай отказа, когда верхнее событие возникает при потере двух объектов в одном полете. Известно, что оба объекта исправны перед полетом и ни один из них не имеет скрытого отказа. Поскольку скрытые отказы отсутствуют, то вероятности средняя и для наиболее тяжелого случая совпадают. Два отказа могут происходить в любом порядке. Пример показан на рис. D17.



$$P_{f\ худшая} = P_{f\ средняя} = \lambda_1 \lambda_2 t_f^2$$

Пример расчета дерева неисправности, когда отказы двух объектов вызывают потерю функции
Рис. D17

D.11.1.5.2 Расчет дерева неисправности, когда два объекта приводят к потере функции и один из них может отказать скрыто, но другой не может отказать скрыто, без упорядочивания. Здесь объект 1 может отказать в любой точке между его проверкой (время – нуль) и его следующей проверкой (время – T). Известно, что объект 2 работоспособен в начале каждого полета и никогда не отказывает скрыто. Порядок возникновения отказов не имеет значения. В этом случае имеется отличие между средней вероятностью возникновения события верхнего уровня за полет и вероятностью для наиболее тяжелого случая. Предположим, что есть n полетов длительностью t_1 часов каждый, т.е. $T = n*t_1$.

Используя приближенное выражение $P_f = \lambda t$ для малых λt, получим следующие данные, которые приведены в таблице D5:

a. Вероятность возникновения двух отказов в первый полет после проверки равна $\lambda_1 \lambda_2 t_f^2$.

b. Вероятность того, что первый объект откажет в каком-либо из первых двух полетов после проверки, а оба откажут во втором полете равна $2\lambda_1 \lambda_2 t_f^2$.

c. Вероятность того, что первый объект откажет в каком-либо и i полетов после проверки, а оба откажут во i-том полете равна $i\lambda_1 \lambda_2 t_f^2$.

Таблица D5. Демонстрация расчетов средней вероятности для варианта с двумя отказами – один скрытый и один активный

		Проявляющийся в рассматриваемом полете отказ					
Вариант №	Рассматриваемый полет	Скрытый отказ во время 1-го полета	Скрытый отказ во время 2-го полета	Скрытый отказ во время i-го полета	Скрытый отказ предпоследнего полета	Скрытый отказ последнего полета	Полная вероятность для этого варианта
1	1-ый полет скрытого периода	$\lambda_1 t_f \lambda_2 t_f$					$\lambda_1 \lambda_2 t_f^2$
2	2-ой полет скрытого периода	$\lambda_1 t_f \lambda_2 t_f$	$\lambda_1 t_f \lambda_2 t_f$				$2\lambda_1 \lambda_2 t_f^2$

		Проявляющийся в рассматриваемом полете отказ					
Вариант №	Рассматриваемый полет	Скрытый отказ во время 1-го полета	Скрытый отказ во время 2-го полета	Скрытый отказ во время i-го полета	Скрытый отказ предпоследнего полета	Скрытый отказ последнего полета	Полная вероятность для этого варианта
i	i-ый полет скрытого периода	$\lambda_1 t_f \lambda_2 t_f$	$\lambda_1 t_f \lambda_2 t_f$	$\lambda_1 t_f \lambda_2 t_f$			$i\lambda_1 \lambda_2 t_f^2$
n-1	Предпоследний полет скрытого периода	$\lambda_1 t_f \lambda_2 t_f$	$\lambda_1 t_f \lambda_2 t_f$	$\lambda_1 t_f \lambda_2 t_f$	$\lambda_1 t_f \lambda_2 t_f$		$(n-1)*\lambda_1 \lambda_2 t_f^2$
n	Последний полет скрытого периода	$\lambda_1 t_f \lambda_2 t_f$	$\lambda_1 t_f \lambda_2 t_f$	$\lambda_1 t_f \lambda_2 t_f$	$\lambda_1 t_f \lambda_2 t_f$	$\lambda_1 t_f \lambda_2 t_f$	$n \lambda_1 \lambda_2 t_f^2$

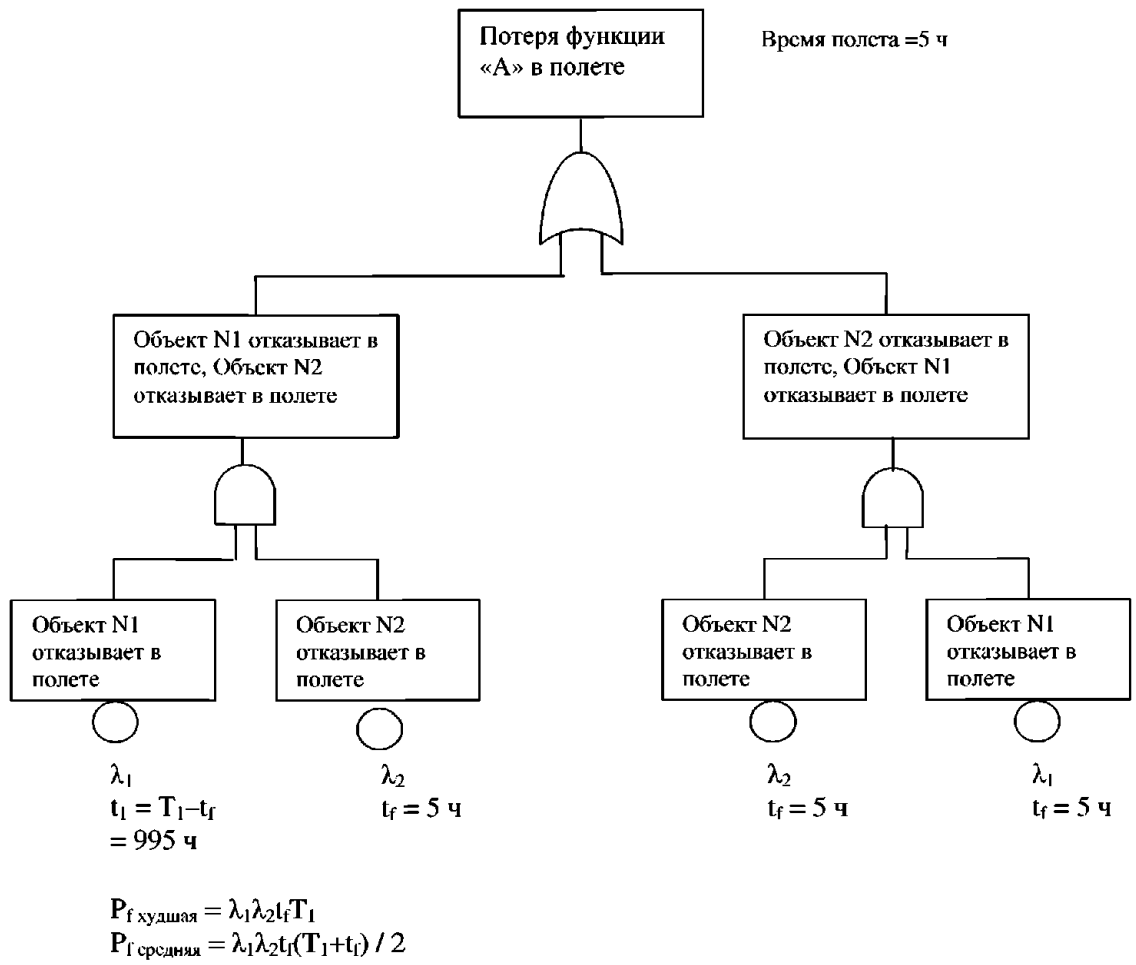
d. Вероятность того, что первый объект откажет в каком-либо и n полетов после проверки, а оба откажут в последнем (n-ном) полете равна $n\lambda_1\lambda_2 t_f^2$ (Эта вероятность для наиболее тяжелого случая).

e. Средняя вероятность за полет равна сумме вероятностей для каждого полета деленной на n, число полетов скрытого периода:

$$P_{f\ средняя} = 1/n * \Sigma\ i\ \lambda_1\lambda_2 t_f^2 \text{ для i от 1 до n}$$
$$= (\lambda_1\lambda_2 t_f^2)/n * \Sigma\ i \text{ для i от 1 до n}$$
$$= (\lambda_1\lambda_2 t_f^2)/n * (n*(n+1))/2$$
$$= 1/2 * \lambda_1\lambda_2 t_f(nt_f + t_f)$$
$$= 1/2 * \lambda_1\lambda_2 t_f(T + t_f)$$

Фактор 1/2 появляется в результате расчета средней вероятности того, что функция откажет в любом одном полете в течение скрытого периода без использования значения времени воздействия T/2.

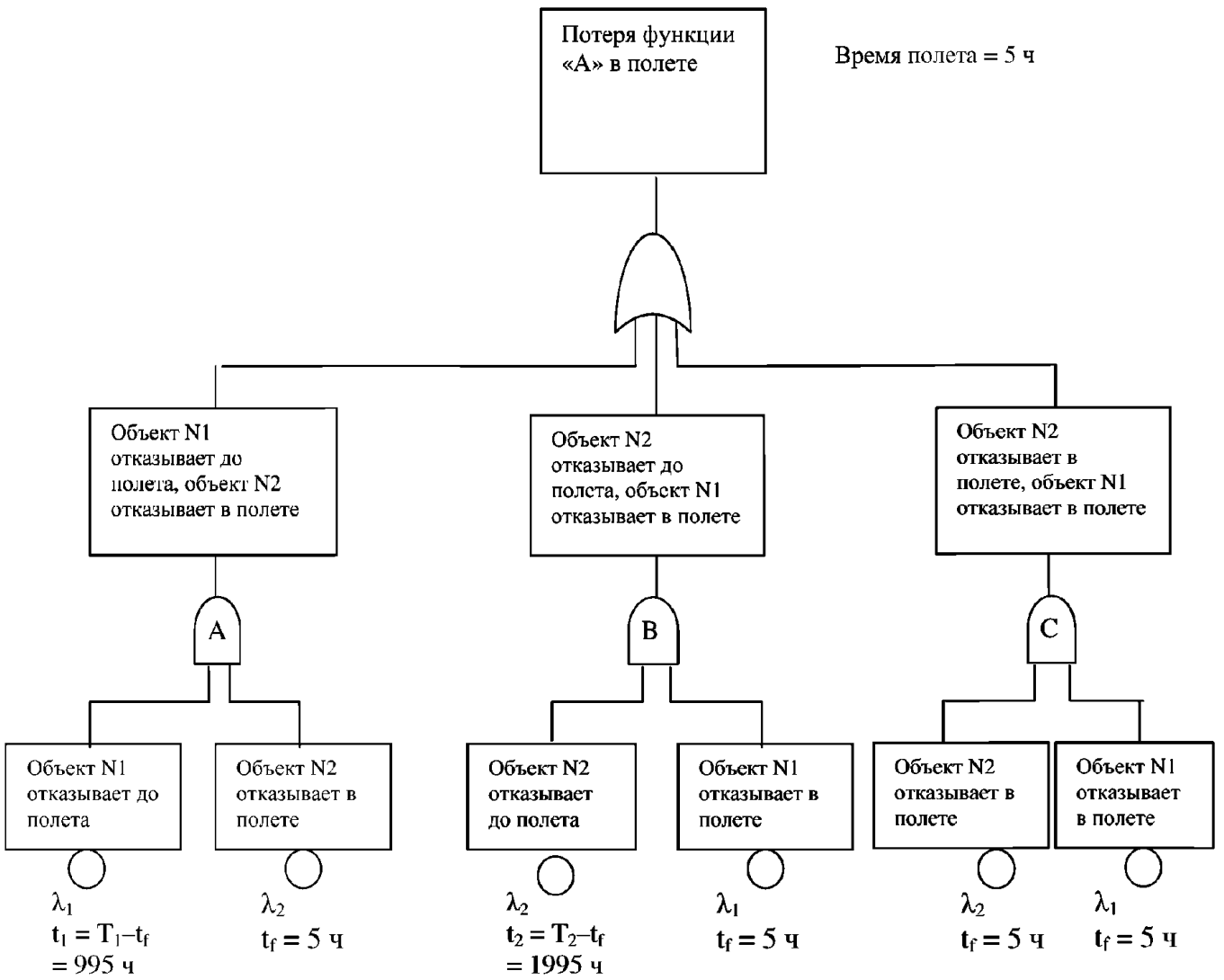
Пример показан на рис. D18.



Пример расчета дерева неисправности, когда отказы двух объектов приводят к потере функции и объект № 1 может отказать скрытно
Рис. D18

D.11.1.5.3 Расчет дерева неисправности, когда два объекта приводят к потере функции и каждый объект может отказать скрытно, без упорядочивания.

Здесь каждый объект может отказать скрыто, но если отказали оба, это может быть обнаружено по появлению события верхнего уровня. Поэтому хотя бы один из объектов должен быть работоспособен в начале каждого полета. Пример показан на рис. D19.



$P_{f\ худшая} = \lambda_1\lambda_2 t_f(T_1+T_2-t_f)$

$P_{f\ средняя} = \lambda_1\lambda_2 t_f(T_1+T_2) / 2$

Пример расчета дерева неисправности, когда отказы двух объектов приводят к потере функции, при этом каждый объект может отказать скрытно
Рис. D19

Относительно рис. D19 следует отметить три особенности. Первая – неразработанное событие для порядка отказов (т.е. ФТП = k / n! как указано в D.11.1.4) не требуется, потому, что зависимость отказа от порядка введена в структуру дерева через период скрытости ($t_n = T_n - t_f$), который представляется для отказа перед полетом. Вторая – наиболее крайний справа И-символ необходим для учета варианта, когда оба объекта отказывают во время полета без требуемого порядка. Третья – крайний справа И-символ часто пропускается и время воздействия принимается равным интервалам проверок, в случае если t_f много меньше чем интервал проверок.

a. Вероятность наиболее тяжелого случая в полете рассчитывается, как показано на рис. D19.

$P_fA = \lambda_1 (T_1 - t_f) \lambda_2 t_f$

$P_fB = \lambda_2 (T_2 - t_f) \lambda_1 t_f$

$P_fC = \lambda_1 t_f \lambda_2 t_f$

$P_{худший} = P_fA + P_fB + P_fC$

$= \lambda_1 \lambda_2 t_f (T_1 - t_f + T_2 - t_f + t_f)$

$= \lambda_1 \lambda_2 t_f (T_1 + T_2 + t_f)$

b. Расчет средней вероятности, как показано в D.11.5.5, дает значение

$P_{среднее} = 1/2 \lambda_1 \lambda_2 t_f (T_1 + T_2)$

D.11.1.5.4 Расчет дерева неисправности, когда отказ двух объектов приводит к верхнему событию, один из них может отказать скрытно и порядок отказов имеет значение.

Здесь объект 1 (со скрытым отказом) должен отказать до отказа объекта 2, иначе верхнее событие не произойдет. Известно, что объект 2 работоспособен в начале полета. Это типичная ситуация с отказом средств контроля, когда верхним событием является недостоверный выход а не потеря функции. Пример, показывающий пропуск недостоверных данных показан на рис. D20.

Фактор требуемого порядка применяется в соответствии с D.11.1.4.

a. Вероятность наиболее тяжелого случая в полете рассчитывается, как указано ниже с учетом приведенного на рис. D20.

$P_fA = \lambda_1 (T_1 - t_f) \lambda_2 t_f$

$P_fB = \lambda_1 \lambda_2 t_f^2$

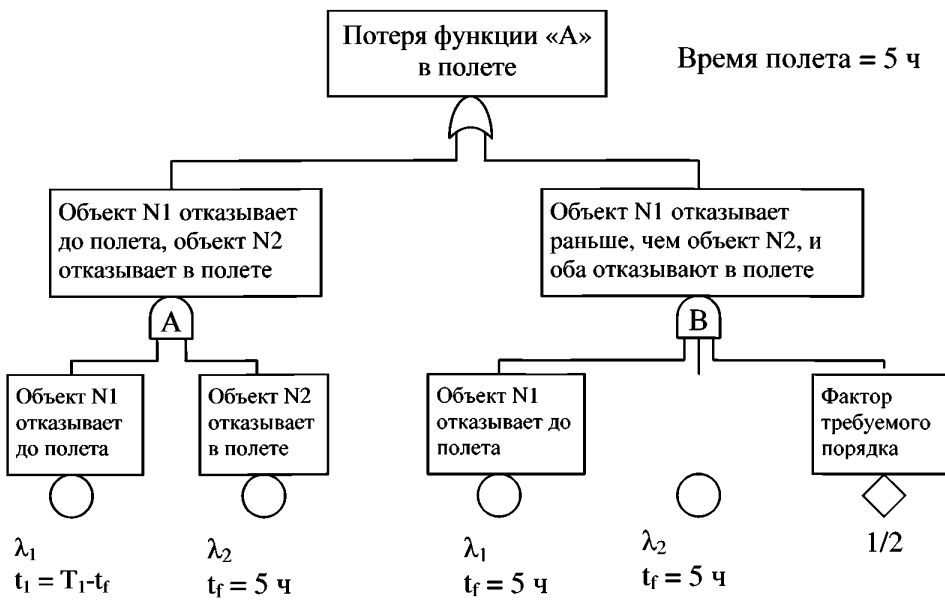
$P_{худший} = P_fA + P_fB$

$= \lambda_1 (T_1 - t_f) \lambda_2 + \lambda_1 \lambda_2 t_f^2/2$

$= \lambda_1 (T_1 - t_f/2) \lambda_2$

b. Расчет средней вероятности, как показано в D.11.5.5, дает значение

$P_{среднее} = 1/2 \lambda_1 \lambda_2 t_f T_1$



$P_{f\ худшая} = \lambda_1 \lambda_2 t_f (T_1 - (t_f/2))$

$P_{f\ средняя} = \lambda_1 \lambda_2 t_f T_1 / 2$

Пример расчета дерева неисправности, когда отказ двух объектов приводит к верхнему событию, один из них может отказать скрытно и порядок отказов имеет значение

Рис. D20

D.11.1.5.5 Примеры расчета средней вероятности возникновения двойного отказа за среднее время полета.

Следующий пример показывает основной вариант двойного отказа F_1 и F_2 с различными интенсивностями отказов λ_1 и λ_2 и двумя периодами скрытости T_1 и T_2 в предположении:

$T_1 \le T_2$, $T_2 = NT_1$ и t_f среднее время полета.

Мы имеем:

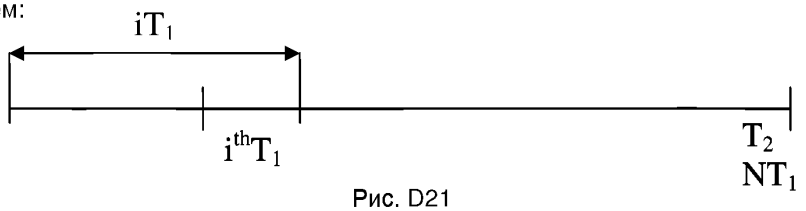


Рис. D21

D.11.1.5.5.1 Вероятность возникновения для i-го T_1

Эта вероятность состоит из двух частей: часть A и часть B.

a. Часть A. F_2 возникает прежде чем F_1.

(1) Эта часть состоит из двух компонентов:

(a) A1: F_2 возникает до i-го T_1, а F_1 возникает во время T_1.

(b) A2: F_2 возникает до i-го F_1 во время i-го T_1

$P_A = P_{A1} + P_{A2} = \lambda_1 (i-1)\, T_1\, \lambda_2 T_1 + (\lambda_1 T_1\, \lambda_2 T_1/2)$
(отметим, что «/2» введена потому, что F_2 возникает до F_1 во время T_1)

$P_A = \lambda_1 \lambda_2 T_1^2 (i - 1 + 1/2) = \lambda_1 \lambda_2 T_1^2 (i - 1/2)$

b. Часть B . F_1 возникает прежде чем F_2

(1) В этом случае скрытый период для F_1 есть T_1, а двойной отказ возникает, если F_1 возникает до F_2 во время T_1

$P_B = (\lambda_1 T_1\, \lambda_2 T_1)/2$
(отметим, что «/2» введена потому, что F_1 возникает до F_2 во время T_1)

Полная вероятность возникновения для i-го T_1 составляет
$P = P_A + P_B = \lambda_1 \lambda_2 T_1^2 (i - 1/2 + 1/2) = \lambda_1 \lambda_2 T_1^2 i$

D.11.1.5.5.2 Вероятность возникновения для периода T_2

Вероятность возникновения за период T_2

Полная вероятность возникновения для периода T_2 определяется как
$P_G = \Sigma (P_A + P_B)$; для i от i=0 до i=N
$P_G = \lambda_1 \lambda_2 T_1^2 [N (N+1)/2 - N/2) + (N/2)]$
$P_G = \lambda_1 \lambda_2 T_1^2 [N^2/2 + N/2 - N/2) + N/2]$
$P_G = \lambda_1 \lambda_2 T_1^2 [N^2/2 + N/2]$

Заменяя NT_1 на T_1 получим
$P_G = 1/2\, \lambda_1 \lambda_2 T_2 (T_1 + T_2)$.

D.11.1.5.5.3 Вероятность возникновения за полет

Величина P_G определяет среднюю вероятность возникновения за период T_2 часов. Для получения средней вероятности возникновения за полет необходимо разделить P_G на T_2 для получения средней вероятности возникновения за час полета и умножить на величину t_F – среднее время полета. В результате получим формулу:

$P_{ft} = P_G * t_F / T_2$

$P_{ft} = 1/2\, \lambda_1 \lambda_2 t_F (T_1 + T_2)$

где P_{ft} есть вероятность двойного отказа за полет.

D.11.1.5.5.4 Вывод для рассматриваемых вариантов

Из формулы для P_{ft}, приведенной в D.11.1.5.5.3, можно вывести формулы для некоторых вариантов двойных отказов.

a. Два скрытых отказа F_1 и F_2, с различными периодами скрытости T_1 и T_2.

Без соблюдения порядка: $P_{ft} = 1/2\ \lambda_1\ \lambda_2\ t_F\ (T_1 + T_2)$

Для порядка – F_2 ранее, чем F_1: $P_{ft} = 1/2\ \lambda_1\ \lambda_2\ t_F\ T_2$

Для порядка – F_1 ранее, чем F_2: $P_{ft} = 1/2\ \lambda_1\ \lambda_2\ t_F\ T_1$

b. Два скрытых отказа F_1 и F_2, с одинаковыми периодами скрытости $T_1 = T_2 = T$

Без соблюдения порядка: $P_{ft} = 1/2\ \lambda_1\ \lambda_2\ t_F\ (T_1 + T_2) = \lambda_1\ \lambda_2\ t_F\ T$

Для порядка - F_2 ранее, чем F_1: $P_{ft} = 1/2\ \lambda_1\ \lambda_2\ t_F\ T$

Для порядка - F_1 ранее, чем F_2: $P_{ft} = 1/2\ \lambda_1\ \lambda_2\ t_F\ T$

c. Один скрытый отказ F_2 и один скрытый отказ F_1 с периодами скрытости

$T_2 = T$ и $T_1 = t_F$

Без соблюдения порядка: $P_{ft} = 1/2\ \lambda_1\ \lambda_2\ t_F\ (T + t_F)$

Для порядка – F_2 ранее, чем F_1: $P_{ft} = 1/2\ \lambda_1\ \lambda_2\ t_F\ T$

(вариант системы управления и контроля)

Для порядка – F_1 ранее, чем F_2: $P_{ft} = 1/2\ \lambda_1\ \lambda_2\ t_F\ t_F = 1/2\ \lambda_1\ \lambda_2\ t_F^2$

d. Два активных отказа F_1 и F_2, $T_1 = T_2 = t_F$

Без соблюдения порядка: $P_{ft} = \lambda_1\ \lambda_2\ t_F\ [(t_F + t_F)\ /2] = \lambda_1\ \lambda_2\ t_F^2$

Для порядка – F_2 ранее, чем F_1: $P_{ft} = 1/2\ \lambda_1\ \lambda_2\ t_F\ t_F = 1/2\ \lambda_1\ \lambda_2\ t_F^2$

Для порядка – F_1 ранее, чем F_2: $P_{ft} = 1/2\ \lambda_1\ \lambda_2\ t_F\ t_F = 1/2\ \lambda_1\ \lambda_2\ t_F^2$

D.11.2 Количественная оценка чувствительности

Оценки чувствительности можно разделить на две категории (обратитесь к NUREG-0492, где это подробно рассматривается):

a. Вариации моделей и данных.

b. Формальный анализ ошибок.

Аналитик может использовать вариации данных или модели дерева неисправности для определения того, насколько чувствительна конструкция системы к специфическому проявлению отдельных первичных событий. Введением различных интенсивностей отказов конкретного первичного события аналитик может принять решение о том, когда повышение надежности объекта/компонента ценнее увеличения стоимости. Рассматривая различные времена воздействия, аналитик получает данные для установления интервалов обслуживания оборудования.

Аналитик может использовать формальный анализ ошибок для определения того, насколько чувствителен вывод FTA к изменению первичного события, т.е. к изменению в интенсивности отказов и интервалов Обслуживания компонента. Метод Монте-Карло является одним из таких способов, который легко приспособить к анализу дерева неисправности. Поскольку анализы ошибок основываются на статистических и вероятностных методах, которые выходят за рамки назначения этого Приложения, читателю следует обратиться к литературе по этой тематике.

Количественная значимость подобна качественной значимости (смотри D.10.2) в том, что оба метода оценки просто располагают по рангу установленные наборы для определения их относительной значимости в отношении к возникновению верхнего события.

Количественная значимость может принимать различные формы. Здесь приводятся некоторые методы. Аналитик получает отличающуюся информацию при использовании разных методов.

Метод № 1. Простое ранжирование установленных наборов в порядке уменьшения получаемой вероятности отказа в каждом из них (т.е. от наибольшего к наименьшему значению P_f). Этот метод тесно связан с качественной значимостью. Аналитик может точно определить ранжирование установленных наборов в противоположность грубой оценке ранжирования установленных наборов при использовании метода качественной значимости.

Метод № 2. Здесь значимость установленного набора определяется долей вероятности отказа установленного набора относительно вероятности отказа верхнего события.

$$\%(i) = \frac{P_f(i)}{P_f(\text{вверхнее})} \qquad \text{(Ур. D24)}$$

Метод № 3. Значимость по Фуселу-Весли (ФВ) – дает риск, который связан с отдельным первичным событием (т.е. дает относительную величину того, насколько велик вклад первичного события в величину P_f верхнего события).

$$\text{ФВ} = \frac{P_f(\text{вверхнее}) \quad P_f(\text{вверхнее}/A = 0)}{P_f(\text{вверхнее})} \qquad \text{(Ур. D25)}$$

где P_f (верхнее/A=0) определяется как вероятность того, что возникает верхнее событие, если не возникает взятое событие A, т.е. $P_f(A) = 0$.

Метод № 4. Значимость по Бирнбауму – дает увеличение риска связанного с первичным событием. Этот метод дает разницу между величинами P_f верхнего события когда возникает первичное событие (т.е. P(A) = 1) и когда первичное событие не возникает (т.е. P(A) = 0).

$$\text{Бирнбаум} = P_f(\text{верхнее}/A=1) - P_f(\text{верхнее}/A=0) \qquad \text{(Ур. D26).}$$

D.12 ИСПОЛЬЗОВАНИЕ ДЕРЕВЬЕВ НЕИСПРАВНОСТИ ДЛЯ ПОКАЗА ВЛИЯНИЯ ОШИБОК

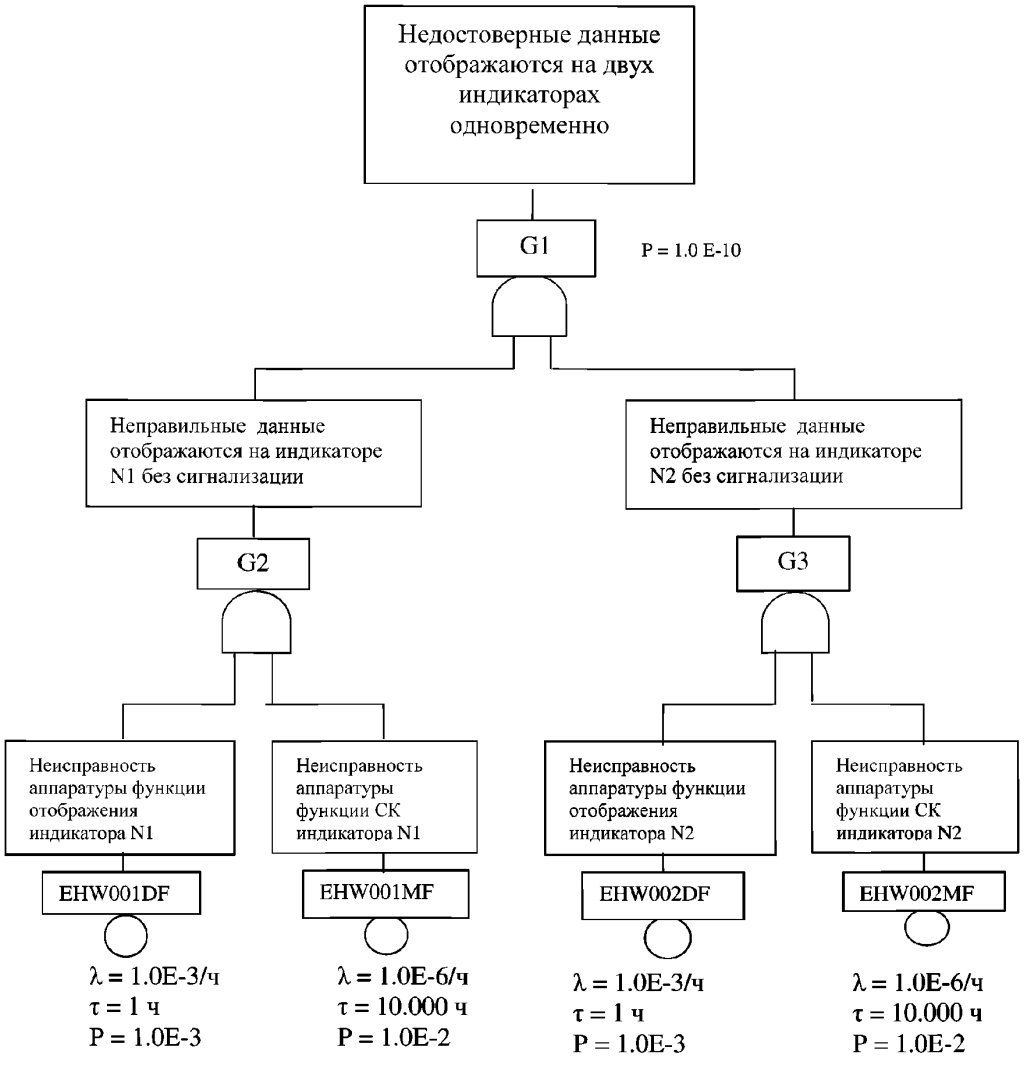
Деревья неисправности могут предоставить средства для иллюстрации влияния ошибок в аппаратуре и программном обеспечении на нежелаемое анализируемое событие. Это достигается введением в дерево неисправности событий о наличии аппаратных и программных ошибок. Такие события вводятся только как качественные. Они не участвуют в вычислениях вероятности события верхнего уровня, определяемой по отказам аппаратуры.

Внесением потенциальных аппаратных и программных ошибок в дерево неисправности аналитик может оценить уровень гарантии разработки, необходимый для того, чтобы ошибки общего режима не могли уменьшить уровень безопасности, который достигнут применением мер защиты от случайных отказов аппаратуры.

Следующий пример, который показывает, как вносятся потенциальные ошибки в аппаратуре и программном обеспечении в дерево неисправности, может помочь аналитику при оценке гарантии разработки, которая должна быть достигнута.

В примере рассмотрены два одинаковых индикатора. Для упрощения источники данных для индикаторов исключены из анализа и предполагается, что в каждом индикаторе имеются средства контроля. Исходное дерево неисправности показано на рис. D22. В этом исходном дереве неисправности предполагается, что все аппаратные отказы независимы. Показано, что соответствие уровню безопасности 1E-9 легко достижимо потому, что должны произойти четыре независимых отказа.

Аналитик может легко определить, что минимальным установленным набором дерева является (EHW0010F)(EHW001MF)(EHW0020F)(EHW002MF). Затем аналитик должен определить, могут ли отказы общей причины влиять на расчеты, выполняемые по этому установленному набору. Деревья неисправности (рис. D23, листы 1-4) на следующих страницах дополнены потенциальными отказами общей причины и наглядно показывают их возможные последствия. Потенциальные отказы общей причины показаны как «внешние отказы общей причины (питание, окружающая среда и т.д.)», «возможность ошибок, если данные и контроль независимы» и «возможность ошибок в аппаратуре и программном обеспечении, если данные и контроль не являются независимыми». Внешние отказы общей причины введены для полноты и далее не рассматриваются.



Пример дерева неисправности, основа для введения ошибок проектирования
Рис. D22

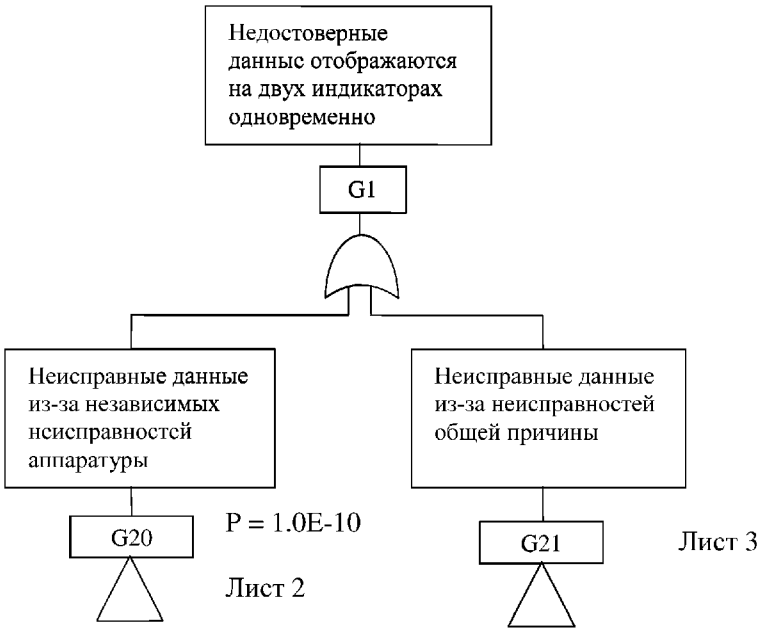
Вследствие идентичности индикаторов, наиболее жестким является предположение, что ошибка в программе или в проектировании аппаратуры будет воздействовать на оба индикатора одновременно. В каждом индикаторе анализируются две функции: функция формирования данных и функция контроля. Если проектирование формирования данных и проектирование контроля выполнены независимо, то ветви дерева неисправности, показанные под событием «возможность ошибок, если данные и контроль независимы» поясняют назначение гарантии разработки для выполняющих эти функции программного обеспечения и аппаратуры. В этом случае события верхнего уровня могут вызывать комбинации ошибок программы, аппаратуры и случайные отказы аппаратуры.

Если функции формирования данных и контроля не проектируются независимо, то ветви дерева неисправности, показанные под событием «возможность ошибок, если данные и контроль не являются независимыми» поясняют назначение гарантии разработки. Если функции не являются независимыми, то ошибки проектирования аппаратуры и программы являются основной причиной возникновения события верхнего уровня.

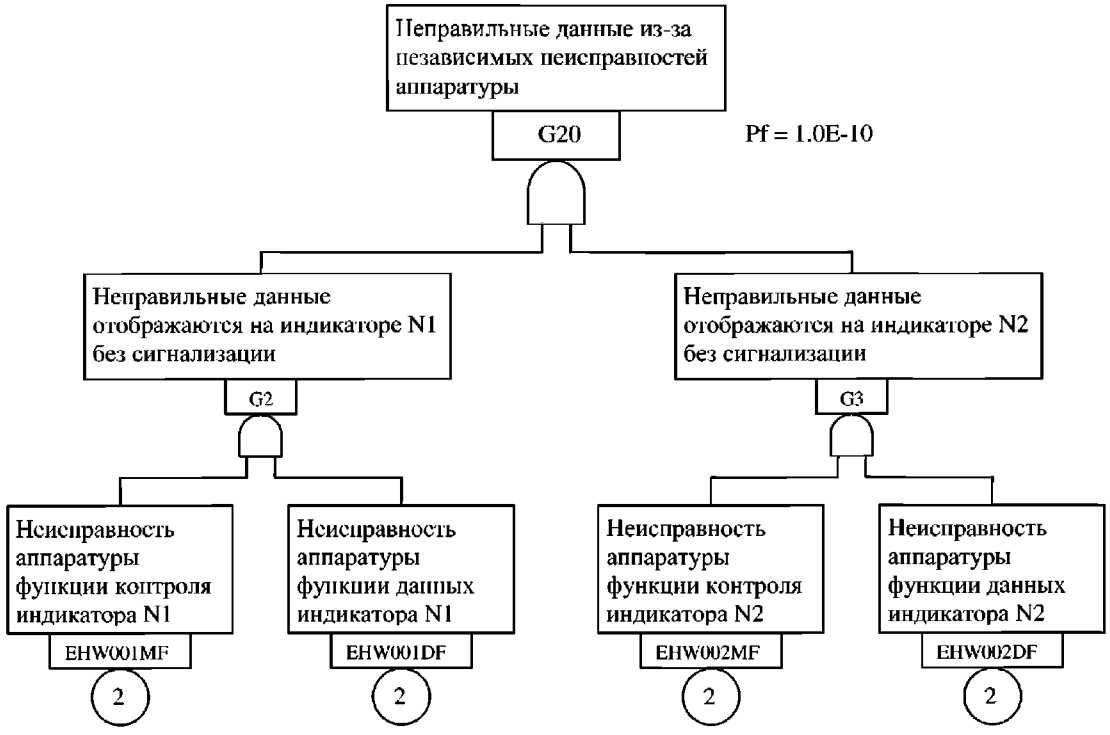
Теперь, аналитик может обратиться к разделу 5.4 Р-4754 для определения Уровня гарантии разработки, который необходимо назначить для таких проектов. Если функции формирования и

контроля не являются независимыми, то аппаратура и программное обеспечение, которые используются для реализации этих обоих функций, должны разрабатываться по уровню А. Если эти функции независимы, становится возможным назначить этот уровень одной или обоим функциям.

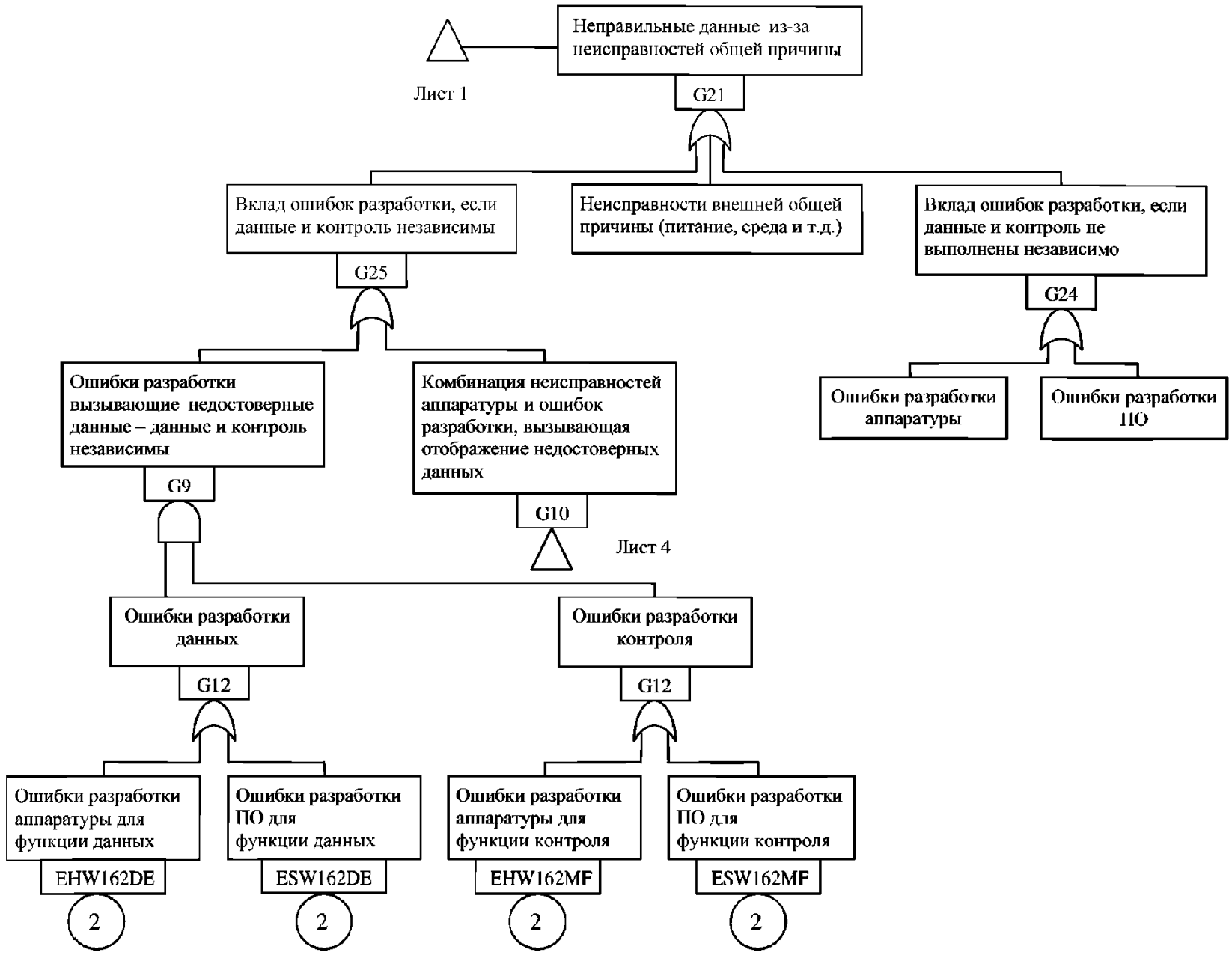
Включение потенциальных ошибок аппаратуры и программного обеспечения в дерево неисправности дает ценное понимание в вопросах, которые необходимо задать относительно независимости и ее предела. Когда будут получены ответы на эти вопросы, появится понимание необходимой гарантии разработки.



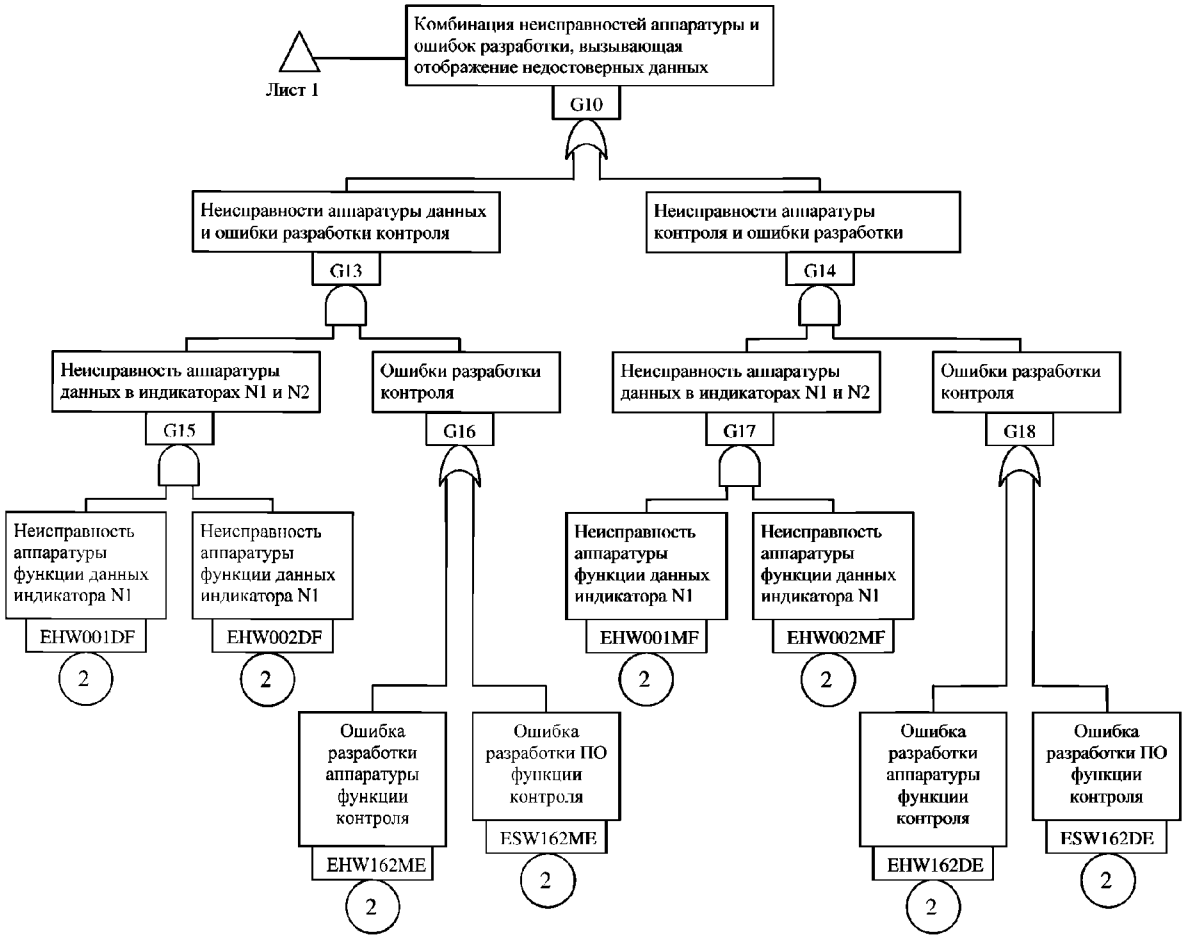
Рассмотрение отказов общей причины (ошибок)
Рис. D23 (лист 1 из 4)



Рассмотрение отказов общей причины (ошибок)
Рис. D23 (лист 2 из 4)



Рассмотрение отказов общей причины (ошибок)
Рис. D23 (лист 3 из 4)



Рассмотрение отказов общей причины (ошибок)
Рис. D23 (лист 4 из 4)

D.13 АНАЛИЗ И ОБОБЩЕНИЕ ИТОГОВ РАБОТЫ

После того как дерево было создано, следует нормализовать и обобщить данные дерева неисправности, а также выпустить документ, который подтвердит, является ли данная структура адекватной для того, чтобы удовлетворить требование к событию верхнего уровня.

D.13.1 Анализ дерева неисправности – Нормализация численных расчетов FTA

Обычно требование безопасности выражается термином «вероятность возникновения отказа на час полета». Если анализируемая система имеет такие требования, то выполняющий анализ должен «нормализовать» вероятность возникновения Нежелательного события.

Когда P_f (вершины) вычисляется на час полета, то аналитик нормализует P_f делением вероятности события верхнего уровня на время полета или другое приемлемое время и получается вероятность возникновения отказа на один час полета.

D.13.2 Обобщение результатов FTA в процессе SSA

Для подведения итогов данных анализа дерева неисправности может быть создана Таблица результатов анализа дерева неисправности. При этом используется формат с колонками, как наиболее удобный для доступа ко всем результатам, как разработчикам, так и экспертам сертифицирующего органа. Далее приводится пример такой заполненной таблицы для анализа уровня системы.

Таблица D6. Пример оформления результатов анализа на уровне системы

Критерии безопасности конструкции	Критерии безопасности конструкции	Критерии безопасности конструкции	Результаты анализа	Результаты анализа	Результаты анализа
Перечень событий верхнего уровня (из FHA)	Перечень событий верхнего уровня (из FHA)	Соответствующие максимально допустимые вероятности	Системные вероятности возникновения	Соответствие	Действия по корректировке
Функция №	Описание				
4A1	Потеря всех индикаторов высоты в кабине	1E-9	5E-9	Нет	Переделка системы воздушных данных или более детальный FTA блоков системы
4A2	Потеря высоты на КПИ обоих пилотов	1E-7	1E-7	Да	Не требуется

Отметим, что значения в колонке «Соответствующие максимально допустимые вероятности» основаны на классификации отказного состояния для данного события верхнего уровня.

Теперь мы можем увидеть связь границ FTA и обобщенных результатов FTA. Таблица D6 показывает, что функция № 4A1 не соответствует требованиям по безопасности к событию верхнего уровня для выполненного анализа на уровне системы. Следует расширить границы анализа переходом на уровень блоков. Предположим, что функция № 4A1B55 уровня блока является первичным событием для функции № 4A1 уровня системы. Тогда таблица D7 может быть примером дальнейшего углубления анализа на уровень блока.

Таблица D7. Оформление анализа на уровне блока

Критерии безопасности конструкции	Критерии безопасности конструкции	Критерии безопасности конструкции	Результаты анализа	Результаты анализа	Результаты анализа
Перечень событий верхнего уровня (из FTA системы)	Перечень событий верхнего уровня (из FTA системы)	Соответствующие максимально допустимые вероятности	Системные вероятности возникновения	Соответствие	Действия по корректировке FTA функционального модуля блока или изменение АС/ПО
Функция №	Описание				
4A1B55		1.0E-9	1.0E-8	Нет	Выполнение FTA функционального модуля блока
4A1B56		1.0E-5	1.0E-7	Да	Не требуется

ПРИЛОЖЕНИЕ E

Анализ логических схем

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

E.1 ВВЕДЕНИЕ

Анализ логических схем может использоваться как альтернативный метод представления данных в Анализе дерева неисправности. Он обеспечивает альтернативное графическое представление комбинаций отказов для проведения вероятностного анализа. Процессы и методы, рассмотренные для FTA в Приложении D также применимы и к DD. Принципиальное отличие между FTA и DD состоит в том, что в DD нет дополнительных логических символов. Схемы показывают логику последовательным и параллельным размещением блоков, и не показывают промежуточные события, которые появляются в FTA в качестве описания выходов логических символов. DD аналитически идентичен FTA и роль DD в процессе оценки безопасности такая же что и роль FTA. В этом приложении рассмотрены уникальные вопросы DD, которые не отражены в описании процесса FTA в Приложении D.

E2 НАЗНАЧЕНИЕ

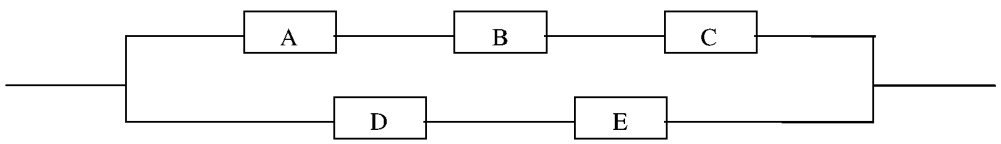
В этом Приложении поясняются основные логические представления, основные процедуры анализа и графические представления отдельных событий различных типов. В обеспечение специфических анализов могут быть применимы изменения и дополнения в представлении событий. Это приложение позволит опытному в выполнении FTA инженеру применять метод DD.

E.3 ОСНОВНОЕ ЛОГИЧЕСКОЕ ПРЕДСТАВЛЕНИЕ

Каждая логическая схема представляет отказное состояние (нежелательное событие верхнего уровня). Она строится с использованием прямоугольных блоков, которые представляют отказные события, которые приводят к состоянию верхнего уровня. Такие прямоугольники располагаются в последовательном или параллельном порядке. Последовательные цепи представляют состояния «ИЛИ», а параллельные цепи показывают состояния «И».

Вероятность конечного отказного состояния P_f логической схемы на рис. E1 приближенно дается выражением

$P_f = (PA + PB + PC) * (PD + PE)$ за полет.



Параллельно-последовательная комбинация
Рис. E1

Показанное логическое представление события упрощено для введения читателя в базовую философию. Логические схемы могут становиться достаточно сложными и могут включать множественное использование единичных отказов в схеме. В таком случае для завершения вероятностных расчетов и создания комплекта минимального сечения будет требоваться применение булевой алгебры.

Все качественные и количественные оценки, использующие комплекты минимального сечения идентичны тем, которые выполняются с комплектами сечений дерева неисправности:

a. Качественная оценка важности (D.10.2).

b. Уязвимость общей причины (D.10.3).

c. Количественная оценка с выполнением вероятностных расчетов и связанные формулы такие же, что и для оценок дерева неисправности, приведенных в разделе D.11.

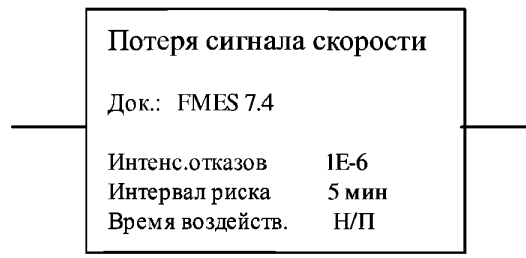
Ошибки могут быть введены в логические схемы таким же путем, как и в дерево неисправности (смотри Приложение D, раздел D.12).

E.4 ГРАФИЧЕСКОЕ ПРЕДСТАВЛЕНИЕ СОБЫТИЙ

Обычно, логические схемы составляются с использованием прямоугольных блоков. Изменения в форме блоков должны использоваться для отражения различных условий, подобно тому, как изменяются используемые в дереве неисправности формы. Примеры этому приводятся в следующих параграфах.

E.4.1 Виды отказов

Ограниченный сплошной линией блок изображает вид отказа, который относится к внутренним для рассматриваемой системы и не нуждается в дальнейшем разложении. Этот блок подобен окружности в дереве неисправности. В PSSA блок следует сопроводить описанием вида отказа и бюджетной интенсивностью отказов совместно с интервалом риска и/или временем воздействия. В SSA бюджетная интенсивность отказов может быть заменена действительной интенсивностью отказов и может дополняться ссылкой на исходный документ FMES. Пример логической схемы из SSA приведен на рис. E.2.

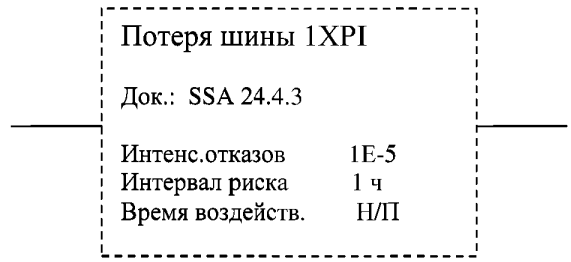


Полностью описанный вид отказа системы
Рис. E2

Пример показывает, что неисправность «Потеря сигнала скорости» ссылается на FMES, имеет интенсивность отказов 1E-6, а интервал риска для этой неисправности составляет 5 мин.

E.4.2 Отказное состояние

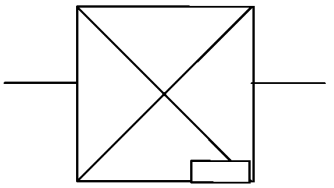
Блок ограниченный пунктирной линией изображает другое отказное состояние исследуемой системы или отказное состояние другой системы. Это можно сравнить с поддеревом в Анализе дерева неисправности.



Неразрабатываемый внутренний или внешний вид отказа
Рис. E3

Пример на рис. E.3 показывает что событие «Потеря шины 1XPI» может быть найдено в соответствующем отчете по SSA.

Блок пересеченный по диагоналям изображает вид отказа, для которого вероятность отказа не может быть прямо получена из его значений λ и t. Этот блок может быть будущей вспомогательной логической схемой справа от него или непосредственно отсылать к определению вероятности отказа. Такой блок показан на рис. E4.



Вероятность из вспомогательной схемы
Рис. E4

Следует быть осторожным при использовании в вероятностных расчетах логических схем таких блоков условных отказных состояний. Они показывают только верхний уровень другой логической схемы, которая может содержать общие с исследуемой логической схемой элементы. Они также могут содержать времена воздействия, отличающиеся от тех, которые рассматриваются в исходной логической схеме.

Расчеты следует всегда проводить по полной структуре логической схемы определяемого отказного состояния, а не простым использованием в расчетах вероятности такого отказного состояния.

E.4.1.3 Внешние события

Блок ограниченный пунктирной линией изображает событие, которое является внешним по отношению к самолету, например, условия обледенения.

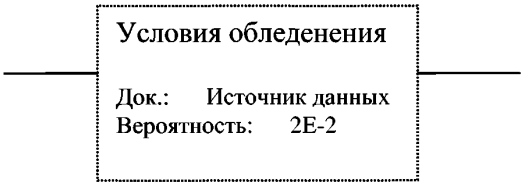


Рис. E5

Пример на рис. E5 показывает, что условия обледенения существуют с вероятностью 2E-2 за полет и дает ссылку для вероятности.

ПРИЛОЖЕНИЕ F

Марковский анализ

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

F.1 ВВЕДЕНИЕ

В этом приложении представлено интуитивное понимание Марковского анализа без сложностей обосновывающей математики. Марковская модель (цепь) представляет различные состояния системы и взаимосвязи между ними. Состояния могут быть как рабочие, так и не рабочие. Скорость перехода из одного состояния в другое является функцией интенсивностей отказов и восстановления. Поскольку некто может знать состояние системы в начальное время, он может инициализировать значение вероятности конкретного состояния системы, величиной 1 и вероятности всех других состояний системы значением 0. Через некоторое время **t** у любого состояния Марковской цепи вероятность станет конечной. Сумма вероятностей всех возможных состояний должна быть равна 1. Вероятности состояния определяются решением системы дифференциальных уравнений, которые выводятся по Марковской цепи. Каждое состояние является взаимоисключающим, поскольку в любое взятое время система может находиться только в одном состоянии. Конечное состояние отказа является основным состоянием, в которое переходят все резервируемые системы или они более не находятся в рабочем состоянии.

F1.1 Предпосылки

Сложность и размер систем быстро увеличивается с новыми успехами в технологии. Системы самолета все более и более выполняются как отказоустойчивые системы. Такие системы очень редко отказывают полностью вследствие постоянного контроля их состояния и немедленной реконфигурации системы. Так происходит до тех пор, пока внешние события не прекратят работу. Взяв этот сценарий устойчивости к неисправности, процесс оценки и расчета безопасности таких систем может быть более предпочтительным с использованием Марковского метода.

Для бортовых систем и оборудования конечные пользователи получают преимущества от имеющегося резервирования при планировании работ по обслуживанию. Такое планирование становится возможным из-за того, что избыточность обеспечивает уровни безопасности оборудования на больших интервалах времени.

FTA и DD широко применяются при оценке безопасности вследствие их концептуальной простоты и легкости понимания. Поэтому FTA и DD следует использовать, где только возможно, понимая следующие ограничения:

a. Они трудны для применения к различным типам, видам отказов и зависимостей, таких как почти совпадающие отказы, перемежающие и повторяющиеся отказы и резервные системы с облегченным режимом.

b. Дерево неисправности конструируется для оценки причины и вероятности единичного верхнего события. Если система имеет много отказных состояний, для каждого из них то, возможно, потребуется разработать раздельные деревья неисправности.

В некоторых случаях может оказаться трудным полностью представить для системы дерево неисправности. Например, для таких как восстанавливаемые системы и системы, в которых скорости отказа/восстановления зависят от состояния.

Марковский анализ не имеет таких ограничений. Последовательно зависимые события вводятся естественным образом и поэтому они могут описать большой диапазон поведения системы.

В Марковском анализе любой может более легко включить сценарии, связанные с условиями эксплуатации пользователя. Например, политику обслуживания авиакомпании, требования отправки и вопросы безопасности. Марковский анализ может поддерживать отдельные фазы полета, интенсивности отказов, зависящие от состояния, отказы общего режима, зависимость

от физических соединений, переходы, зависящие от времени и, для всех указанных выше, полноту покрытия контролем. Неполное покрытие может привести к скрытым отказам и меньшей чем 100% выявляемости отказов. Однако недостатком применения Марковского анализа является то, что размер модели может расти экспоненциально с числом компонентов. Для системы с «**n**» компонентами соответствующая Марковская цепь может иметь до 2^n состояний в простейшем случае, хотя это обычно много меньше, чем при рассмотрении работы системы. Если с одним компонентом связаны более чем два состояния, общее число состояний может быть даже больше. Для решения таких проблем разработаны соответствующие методы.

Определения некоторых терминов, используемых в Марковских моделях, приведены в таблице F1.

Таблица F1. Определения терминов, используемых в Марковском анализе

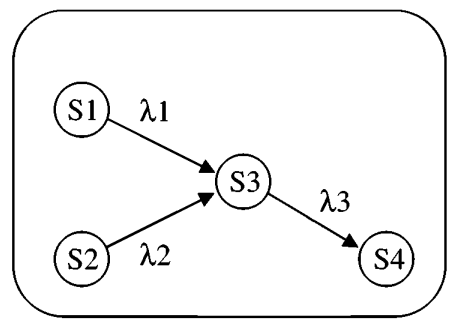
Термины	Определения
Состояние поглощения	Система переходит в состояние и остается в нем, т.е. выхода из этого состояния нет. Если в Марковской цепи имеются состояния поглощения, со временем вероятность нахождения в этом состоянии будет единица
Эргодический процесс	В дополнении к гомогенности, конечное значение вероятности находиться в любом состоянии и не зависит от начального условия
Расширенные стохастические сети Петри (ESPN)	Модель ESPN для подробного анализа восстановления систем из неисправного состояния любого типа
Модели поддержки неисправности и ошибки (FEHM)	Это модели, которые описывают поведение системы при возникновении неисправности. Модель формирует на выходе вероятность обнаружения неисправности, покрытие, вероятность необнаруживаемого и, следовательно, системного отказа, называемого отказом одной точки, вероятность отказа системы вследствие псевдослучайной неисправности, вероятность (N) и вероятность восстановления системы из неисправного состояния (R). Имеется шесть широко используемых FEHM, а именно, Гистограмма, Вероятности и Распределения, средние и стандартные отклонения, CARE III, ARIES и расширенные стохастические сети Петри
Гомогенный процесс	Все вероятности переходов и интенсивности переходов являются постоянными
Гомогенные Марковские процессы	Переходы состояний не имеют памяти, и время нахождения в состоянии распределено экспоненциально. Компоненты не стареют, и переходы состояний возникают с постоянной скоростью переходов
Негомогенный процесс	Ослаблено экспоненциальное выдерживание ограничения времени
Выполняемость	Это измерение является комбинацией надежности и характеристики системы. Характеристика может быть в терминах совершенства системы, среднего времени готовности к работе, среднего расхода топлива и т.д.
Полумарковский процесс	Скорости перехода могут быть функциями времени конкретного состояния, а не общего времени. Время нахождения в состоянии может быть не экспоненциальным и может зависеть от следующего состояния
Пространство состояний	Набор всех возможных состояний, которые может достигнуть система
Состояние	Состояние представляет статус системы
Жесткая Марковская цепь	Постоянные как медленные, так и быстрые переходы, чьи скорости переходов отличаются на порядок величины
Стохастический процесс	Непредсказуемое заранее поведение системы по вероятности различных состояний в конкретное время можно установить

Термины	Определения
Времена перехода	Время, на протяжении которого выполняется переход из одного состояния в другое. Этот переход может происходить на непрерывной или дискретной шкале времени
Переходы	Перемещение от состояния к состоянию с некоторой конечной вероятностью или скоростью перехода. Переход из состояния i в состояние j зависит только от состояния i и состояния j, а не от истории. По этой причине Марковские цепи называют системами без памяти

F.2 ТЕОРИЯ

Марковский анализ любой системы состоит из двух частей. Определение поведения системы записью уравнений связанных с переходами и состояниями в системе и решение этих уравнений с использованием стандартных методов. Для любой системы уравнения состояния могут быть построены на основе экспертизы Марковской цепи. Однако вследствие математической сложности этот ручной метод может привести к ошибкам и пропускам даже для простых систем. Поэтому рекомендуется некоторая форма автоматизации создания модели. Изменения в вероятности состояния, в основном, происходят вследствие наличия у этого состояния входных и выходных потоков. Потоки перехода являются произведением скорости перехода по этому переходу и вероятности состояния в начале такого перехода. Отрицательное значение представляет собой скорость, с которой система покидает это конкретное состояние, тогда как положительное значение подразумевает скорость, с которой система входит в такое новое состояние.

Рассмотрим в качестве иллюстрации следующий сценарий.



Пример переходов и состояний Марковской цепи
Рис. F1

В этой системе состояние S3 имеет вероятность P3(t) зависящую от времени. Состояние имеет две входные дуги из состояний S1 и S2 и одну выходную дугу в состояние S4. Для S1 и S2 зависящие от времени вероятности есть соответственно P1(t) и P2(t). Скорость перехода в состояние S3 из S1 и S2 есть $\lambda 1$ и $\lambda 2$, соответственно. Скорость выхода из состояния есть $\lambda 3$. Скорость изменения вероятности состояния S3 может быть записана с использованием вероятностей P1(t), P2(t) и P3(t) и скоростей перехода $\lambda 1$, $\lambda 2$ и $\lambda 3$ в виде уравнения:

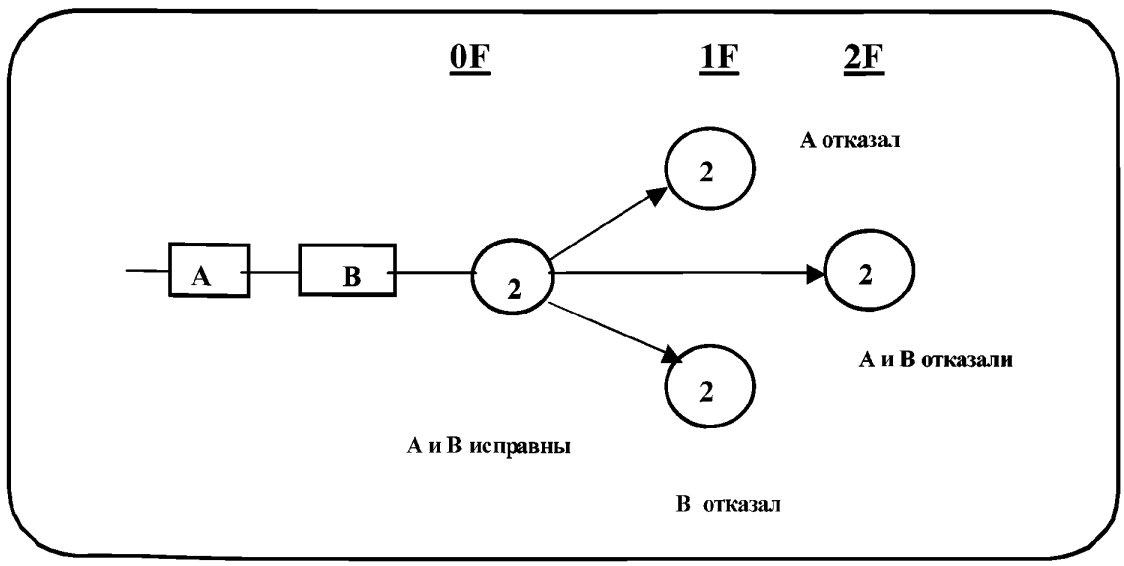
$$\frac{dP3(t)}{dt} = \lambda 1 \times P1(t) + \lambda 2 \times P2(t) - \lambda 3 \times P3(t)$$

Подобно этому могут быть записаны дифференциальные уравнения для любых других состояний этой Марковской цепи. Такой набор дифференциальных уравнений может быть решен с использованием такого математического метода, как преобразование Лапласа. Однако, как только система становится более сложной, увеличивается трудоемкость и время необходимое для ручного решения набора дифференциальных уравнений. Поэтому выполняющему анализ следует использовать один из имеющихся программных пакетов решения Марковских цепей. В следующих подразделах приводятся некоторые примеры.

F.2.1 Последовательные системы

F.2.1.1 Последовательная система не поддающаяся исправлению

В качестве примера можно рассмотреть систему, состоящую из двух последовательных компонентов. Компонент A имеет скорость отказа λ_a отказов в час и компонент B имеет скорость отказа λ_b. Также есть общий вид отказа, на который оба компонента A и B реагируют одновременно и скорость отказа составляет λ_c отказов в час. (Не надо путать с логическим «И» независимых отказов компонентов A и B). Марковская модель для этой системы показана на рис. F2. Модель построена так, что рассматривает все возможные комбинации (состояния) отказов на каждом уровне отказа. Например, на нулевом уровне отказа (0F) есть только одно состояние: A и B исправны, на первом уровне отказа (1F) есть два состояния, одно из них это когда компонент A отказал и другое, где компонент B тоже отказал. На втором уровне отказа (2F) есть общий вид отказа, когда отказывают оба компонента.



Марковская модель простой последовательной системы,
неподдающейся исправлению
Рис. F2

Ниже приведены уравнения состояния для системы, представленной на рис. F2:

$$\frac{dP_1(t)}{dt} = (\lambda_a + \lambda_b + \lambda_c)P_1(t)$$

$$\frac{dP_2(t)}{dt} = \lambda_a P_1(t)$$

$$\frac{dP_3(t)}{dt} = \lambda_b P_1(t)$$

$$\frac{dP_4(t)}{dt} = \lambda_c P_1(t)$$

где $P_i(t)$ – вероятность нахождения в состоянии i в течение времени t. Для постоянной скорости отказа и начального условия $P(0)=[1000]^T$ (T для транспонирования) уравнения состояния могут быть проинтегрированы для получения выражений закрытой формы для всех значений вероятности. Они получаются следующими:

$$P_1(t) = e^{-(\lambda a+\lambda b+\lambda c)t}$$

$$P_2(t) = \frac{\lambda_a}{\lambda_a + \lambda_b + \lambda_c} Ч(1 \quad e^{(\lambda a+\lambda b+\lambda c)t})$$

$$P_3(t) = \frac{\lambda_b}{\lambda_a + \lambda_b + \lambda_c} Ч(1 \quad e^{(\lambda a+\lambda b+\lambda c)t})$$

$$P_4(t) = \frac{\lambda_c}{\lambda_a + \lambda_b + \lambda_c} Ч(1 \quad e^{(\lambda a+\lambda b+\lambda c)t})$$

Для больших значений по времени, $P_1(t)$ стремится к нулю, $P_2(t)$ примерно $\lambda_a / (\lambda_a + \lambda_b + \lambda_c)$, $P_3(t)$ примерно $\lambda_b / (\lambda_a + \lambda_b + \lambda_c)$ и $P_4(t)$ примерно $\lambda_c / (\lambda_a + \lambda_b + \lambda_c)$. Вероятность отказа системы ровна сумме $P_2(t)$, $P_3(t)$ и $P_4(t)$.

Это то же самое решение, которое будет получено путем использования любого комбинированного метода, такого, который представлен ниже:

В течение времени t,

$$P(\text{А-отказал}) = 1 - e^{-\lambda a t};$$

$$P(\text{В-отказал}) = 1 - e^{-\lambda b t};$$

$$P(\text{А и В отказали}) = 1 - e^{-\lambda c t}; \text{ (отказ общего режима)}$$

Теперь из комбинированных методов:

P(А или В отказал) = 1-P (А и В оба не отказали).

Следовательно,

$$P(\text{А или В}) = 1 - e^{-(\lambda a+\lambda b+\lambda c)t}$$

Заметим, что это то же самое, что и $P_2(t) + P_3(t) + P_4(t)$, что вытекает из Марковской цепи.

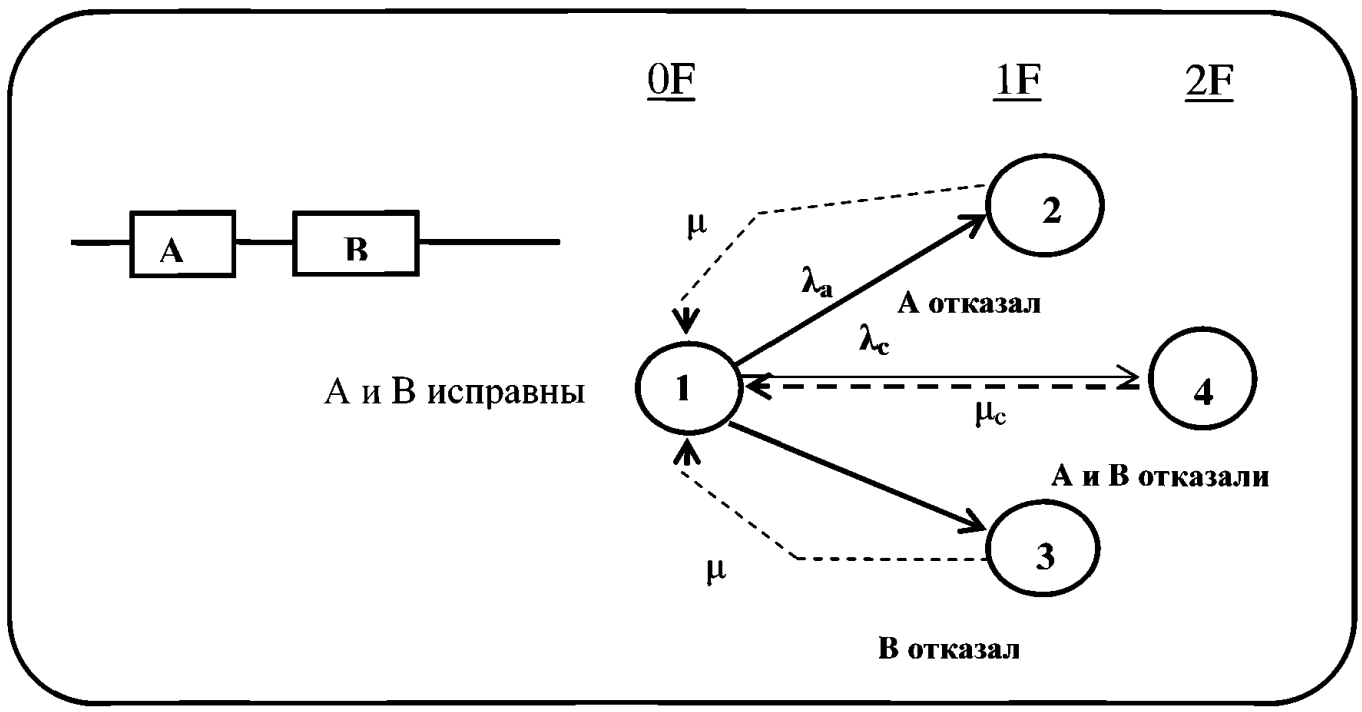
Аналогично,

$$P(\text{А и В не отказали}) = e^{-(\lambda a+\lambda b+\lambda c)t}$$

Заметим, что это уравнение то же самое, что $P_1(t)$, полученное путем использования Марковских методов, описанных выше.

F.2.1.2 Последовательная система с возможностью восстановления

Как пример, еще раз рассмотрим ту же систему, состоящую из двух последовательных компонентов. Компонент А имеет интенсивность отказов λ_a отказов в час и компонент В имеет интенсивность отказов λ_b отказов в час. Также есть общий отказ, на который оба компонента А и В реагируют одновременно и интенсивность отказов составляет λ_c отказов в час. (Не надо путать с логическим «И» независимых отказов компонентов А и В). В дополнение к отказам, оба компонента А и В восстанавливаются с постоянной скоростью μ. В большинстве авиационных случаев восстановление делается в конце интервала проверки и, следовательно, является дискретным процессом восстановления. Однако моделирование в F.2.2.1 и F.2.2.2 приближает дискретное восстановление к непрерывному по времени Марковскому процессу. Это приближение действительно, когда $\lambda << \mu$. В случае, если восстановление является стохастическим процессом, эта модель представляет корректное решение. Примеры моделирования дискретного восстановления даны F.5.1 и F.5.2. Когда отказали оба компонента, скорость восстановления принята как μ_c. Выбрав различные значения μ_c, можно моделировать либо с одиночным восстановлением, либо с многократным восстановлением и т.д. Марковская модель для этой системы показана на рис. F3. Все восстановления на рисунке показаны пунктирами.



Марковская модель простого восстановления последовательной системы
Рис. F3

Уравнения состояния для системы, представленной на рис. F.3:

$$\frac{dP_1(t)}{dt} = (\lambda_a + \lambda_b + \lambda_c)P_1(t) + \mu(P_2(t) + P_3(t) + \mu_c P_4(t)$$

$$\frac{dP_2(t)}{dt} = \lambda_a P_1(t) - \mu P_2(t)$$

$$\frac{dP_3(t)}{dt} = \lambda_b P_1(t) - \mu P_3(t)$$

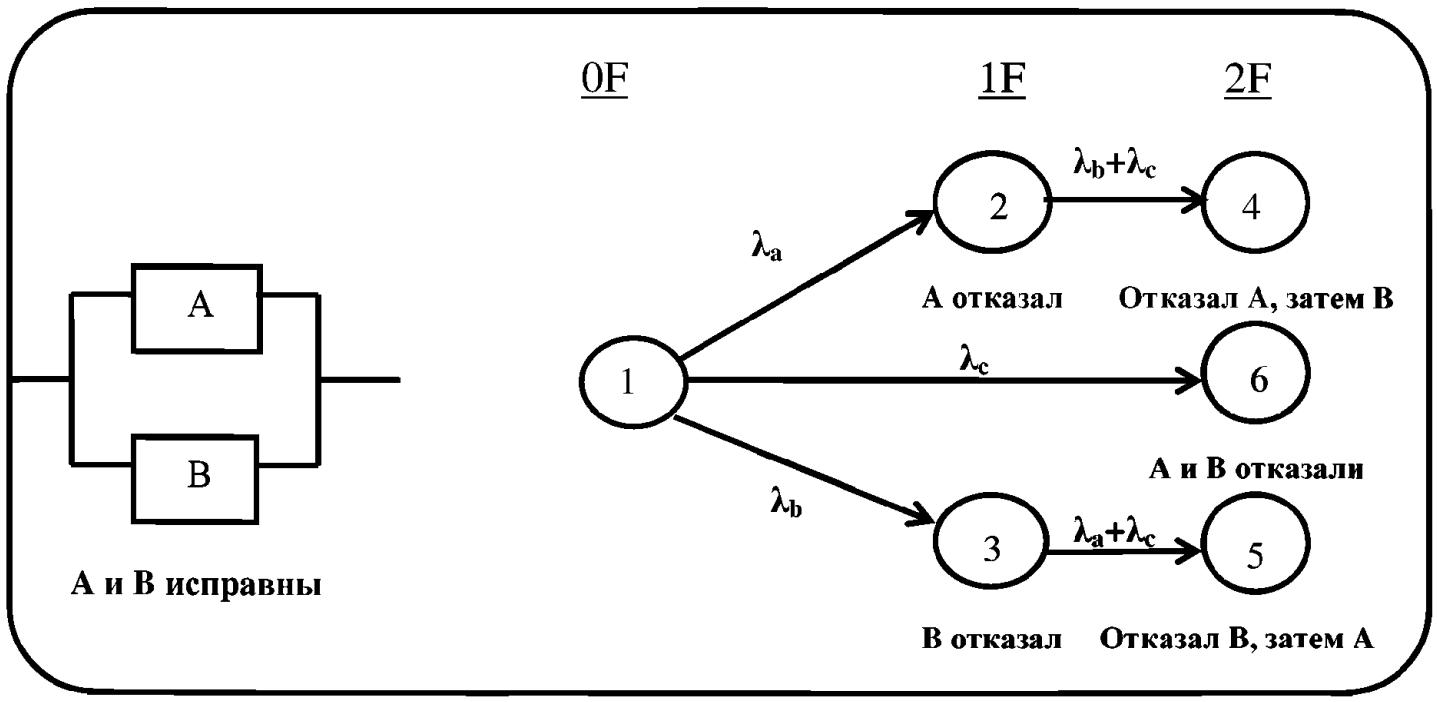
$$\frac{dP_4(t)}{dt} = \lambda_c P_1(t) - \mu_c P_4(t)$$

где $P_i(t)$ – вероятность нахождения в состоянии i в течение времени t. Для постоянных интенсивности отказов и скорости восстановления и при начальном условии $P(0) = [1\ 0\ 0\ 0]^T$ (T означает транспонирование) уравнения состояния могут быть проинтегрированы (подобно процедуре, показанной в F.2.1.1) для получения выражений закрытой формы для всех значений вероятности. Для простоты, они не показаны.

F.2.2 Параллельные системы

F.2.2.1 Невосстанавливаемые параллельные системы

Марковская модель параллельной системы дана на рис. F4, на котором отказ системы обозначен как отказ компонентов A и B. Из-за свойства Марковского метода, последовательность зависимостей может быть легко включена в Марковскую цепь, т.е. состояния 4 и 5. Состояния 4 и 5 в Марковской цепи отличают две возможные последовательности отказа компонента, ведущего к потере системы.



Марковская модель простой параллельной системы
Рис. F4

Принимая интенсивности отказов компонентов A и B как λ_a и λ_b соответственно, скорость отказа общего режима есть λ_c и что Pi(t) есть вероятность нахождения системы в состоянии «i» в течение времени «t», уравнения состояния для этой системы будут иметь следующий вид:

$$\frac{dP_1(t)}{dt} = (\lambda_a + \lambda_b + \lambda_c)P_1(t)$$

$$\frac{dP_2(t)}{dt} = \lambda_a P_1(t) - (\lambda_b + \lambda_c)P_2(t)$$

$$\frac{dP_3(t)}{dt} = \lambda_b P_1(t) - (\lambda_a + \lambda_c)P_3(t)$$

$$\frac{dP_4(t)}{dt} = (\lambda_b + \lambda_c)P_2(t)$$

$$\frac{dP_5(t)}{dt} = (\lambda_a + \lambda_c)P_3(t)$$

$$\frac{dP_6(t)}{dt} = \lambda_c P_1(t)$$

Для постоянной интенсивности отказов и начального условия $P(0) = [1\ 0\ 0\ 0\ 0\ 0]^T$ вероятности состояния есть:

$$P_1(t) = e^{-(\lambda a+\lambda b+\lambda c)t}$$

$$P_2(t) = e^{-(\lambda b+\lambda c)t}(1 - e^{-\lambda at})$$

$$P_3(t) = e^{-(\lambda a+\lambda c)t}(1 - e^{-\lambda bt})$$

$$P_4(t) = \frac{\lambda a}{\lambda a + \lambda b + \lambda c} - e^{-(\lambda b+\lambda c)t} + \frac{\lambda b + \lambda c}{\lambda a + \lambda b + \lambda c} e^{-(\lambda a+\lambda b+\lambda c)t}$$

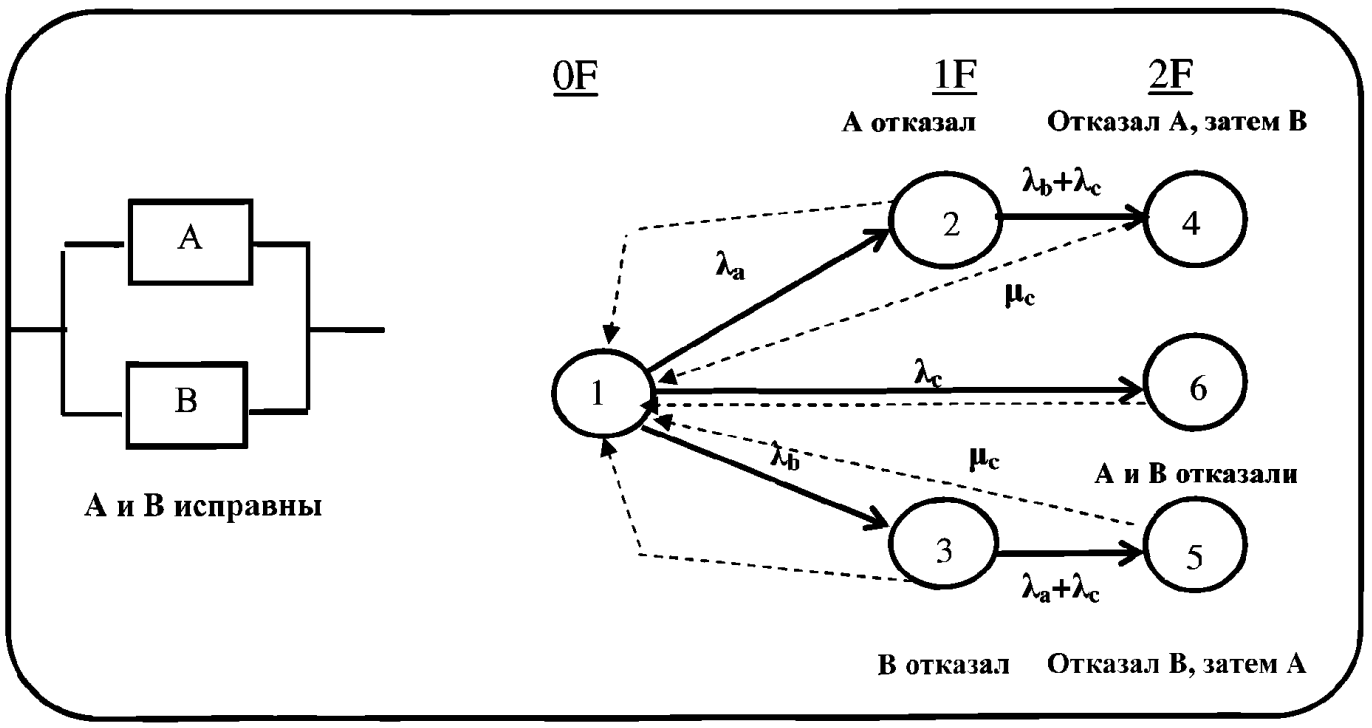
$$P_5(t) = \frac{\lambda_b}{\lambda_a + \lambda_b + \lambda_c} - e^{-(\lambda_a+\lambda_c)t} + \frac{\lambda_a + \lambda_c}{\lambda_a + \lambda_b + \lambda_c} e^{-(\lambda_a+\lambda_b+\lambda_c)t}$$

$$P_6(t) = \frac{\lambda_c}{\lambda_a + \lambda_b + \lambda_c}(1 - e^{-(\lambda_a+\lambda_b+\lambda_c)t})$$

$P_2(t)$ и $P_3(t)$ дают вероятность нахождения системы в деградированном режиме, т.е. А отказал, а В находится в рабочем состоянии и наоборот. Вероятность отказа системы равна сумме $P_4(t)$, $P_5(t)$ и $P_6(t)$. В этом случае может быть показано также, что уравнения вероятности могут быть получены комбинационными методами, подобными вышеуказанным, которые получены использованием подхода, который дается в предыдущем разделе.

F.2.2.2 Параллельная система с возможностью восстановления

Марковская модель для параллельной системы с возможностью восстановления дана на рис. F5.



Марковская модель параллельной системы с простым восстановлением
Рис. F5

Скорости восстановления приняты, как μ и μ_c из состояний, где только один компонент отказал и два компонента отказали, соответственно. Они показаны пунктирными линиями на рис. F5. Принимая интенсивности отказов компонентов А и В как λ_a и λ_b соответственно, интенсивность отказов общего режима как λ_c и что $P_i(t)$ есть вероятность нахождения системы в состоянии «i» в течение времени «t» уравнения состояния для этой системы будут иметь следующий вид:

$$\frac{dP_1(t)}{dt} = -(\lambda_a + \lambda_b + \lambda_c)P_1(t) + \mu(P_2(t) + P_3(t)) + \mu_c(P_4(t) + P_5(t) + P_6(t))$$

$$\frac{dP_2(t)}{dt} = \lambda_a P_1(t) - (\lambda_b + \lambda_c - \mu)P_2(t)$$

$$\frac{dP_3(t)}{dt} = \lambda_b P_1(t) - (\lambda_a + \lambda_c - \mu)P_3(t)$$

$$\frac{dP_4(t)}{dt} = (\lambda_b + \lambda_c)P_2(t) - \mu_c P_4(t)$$

$$\frac{dP_5(t)}{dt} = (\lambda a + \lambda c)P_3(t) - \mu c P_5(t)$$

$$\frac{dP_6(t)}{dt} = \lambda c P_1(t) - \mu c P_6(t)$$

Точные вероятности состояния можно получить, проинтегрировав эти уравнения, как было сделано в предыдущем разделе.

F2.3 Модели учета неисправности и ошибок в Марковском анализе

Обычно отказы в системе происходят на очень низкой скорости. Время обнаружения и обработки отказа будет очень коротким, обычно порядка секунды и меньше. Эти многие порядки различия величин во временах возникновении отказа и обнаружения, делают Марковскую цепь очень жесткой и время решения модели надежности может быть очень большим. Чтобы уменьшить это время, метод решения может быть разбит на две части. Первая часть связана с условиями для системы отказа и включает в себя стратегию восстановления и называется модель возникновения отказа и восстановления (FORM). Поведение системы описывается посредством деревьев неисправности или Марковских цепей. Вторая часть определяет поведение системы после возникновения неисправности. Эта модель, модель поддержки неисправности и ошибки (FEHM), вычисляет четыре вероятности, которые определены ниже:

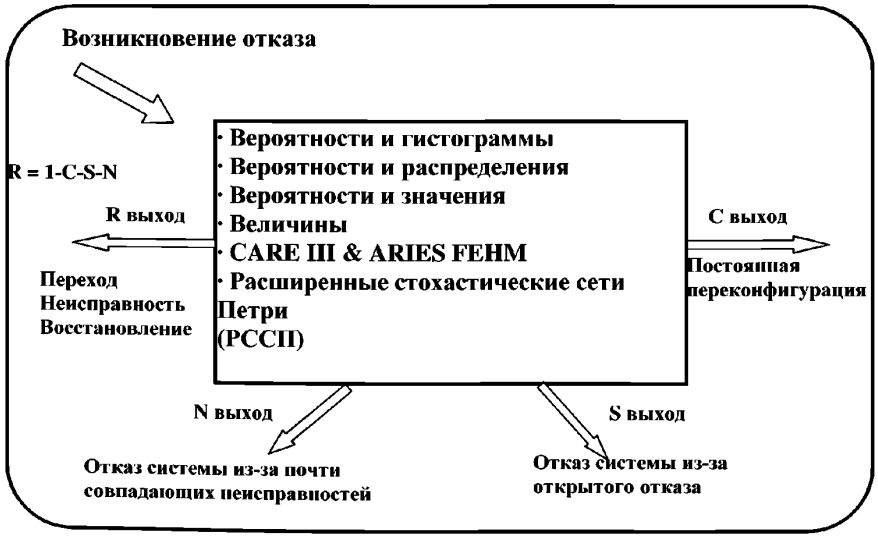
R – вероятность того, что система воспринимает возникшую неисправность как перемежающуюся и восстанавливается из этой перемежающейся неисправности.

C – вероятность того, что система воспринимает возникшую неисправность как постоянную неисправность и успешно выполняет постоянную реконфигурацию с последующей потерей резервирования модуля.

S – вероятность того, что система откажет из-за ее неспособности обнаружить, выделить и/или восстановиться от возникшей неисправности.

N – вероятность того, что система откажет из-за возникновения второй (почти несовпадающей) неисправности пока парируется первая неисправность.

На рис. F6 показаны несколько режимов рассматриваемых моделей, которые могут быть использованы для определения этих комплексных действий и взаимодействий в системе при возникновении неисправности.

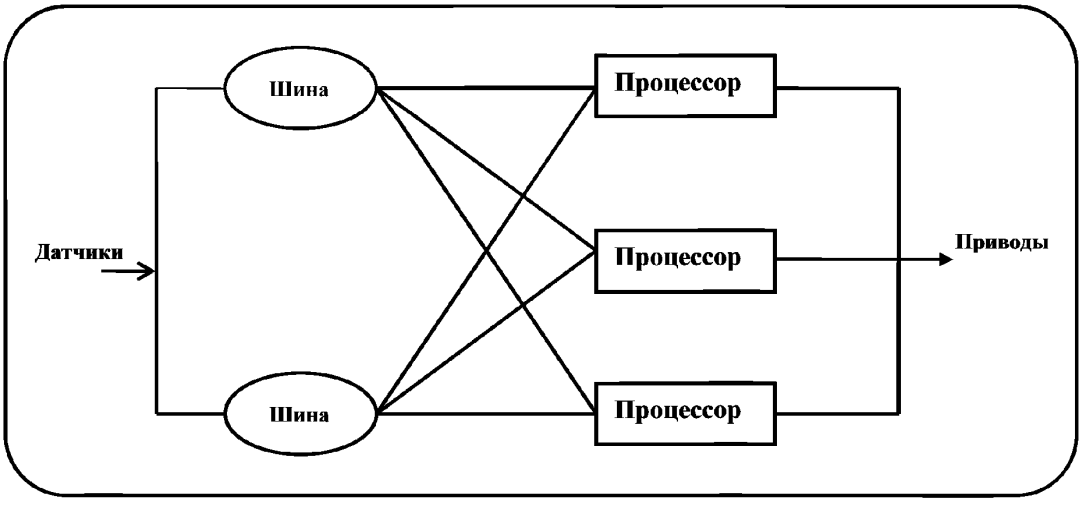


Перечень генерируемых моделей поддержки неисправности и ошибки
Рис. F6

Выход «C» используется, если неисправность в системе обнаружена, и система успешно реконфигурируется в резервный режим. Выход «R» используется, если система способна обнаружить отказы и способна локализовать отказ и выполнить восстановление. В этом случае система поведет себя так, как если бы возникшей ранее неисправности не было. Выход «S» выбирается в случае, если система не в состоянии распознать неисправность и эта неисправность ведет к отказу системы. Выход «N» применяется, если в системе возникает вторая неисправность, в то время, пока система пытается реконфигурироваться при предшествующей неисправности. В такой ситуации всегда принимается, что система переходит в отказное состояние. Эти модели, являются «фиксированными» моделями, которые имеют дело с разнообразием сценариев восстановления ошибки в реальной жизни. Например, модель ARIES FEHM имеет дело с восстановлением системы от неисправности в стадиях, которые могли бы отразить различные повторения на мягкой/переходной неисправности в системе. Точно также модель CARE III FEHM определяет восстановление ошибки в терминах скоростей обнаружения и изоляции и является идеальной для моделирования процедур восстановления ошибки в устойчивой к неисправности памяти. Всегда возможно определить новую модель, которая могла бы отразить процесс восстановления при ошибке более точно. Это возможно путем прямого ввода восстанавливаемой Марковской цепи. Дальнейшие детали моделей даются в руководстве HARP. Должно быть понятно, что такое моделирование является только одним из методов и не является единственным доступным методом решения. Аналитик может использовать любой метод, пока правильность методологии объясняется и понимается должным образом.

F.2.3.1 Использование моделей

В простой системе из 3 процессоров и 2 шин, показанной на рис. F7, система отказывает, когда отказали все три процессора или когда отказали обе шины. Интенсивности отказов каждого процессора и каждой шины приняты как λ_1 и λ_2 соответственно.



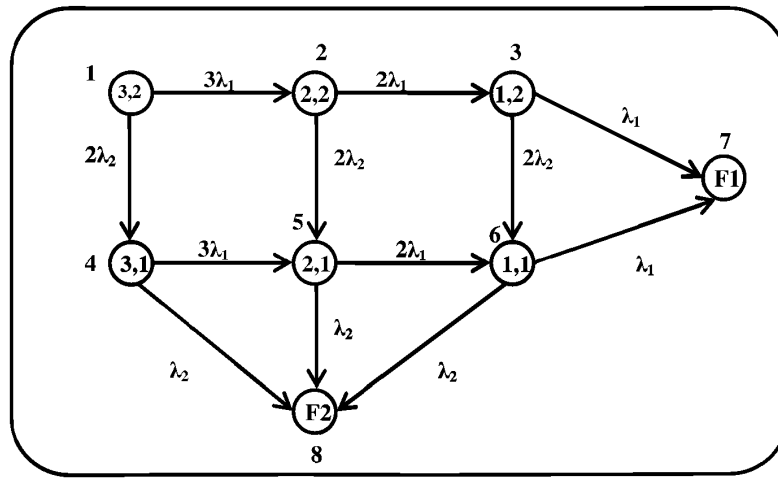
Представление потока сигналов системы, имеющей 3 процессора и 2 шины
Рис. F7

Моделирование для вышеупомянутого примера может показать следующее. В первом случае можно решить систему без включения любой рассмотренной модели. В этом случае, предполагается, что система может всегда обнаружить любую ошибку своевременно и может реконфигурироваться в резервный режим мгновенно. Во втором случае, принята не идеальная полнота контроля. В этом случае, после отказа, возможны варианты решения, такие как неисправность обнаружена, неисправность изолирована, система реконфигурирована, система восстановлена и отказ системы из-за почти совпадающей неисправности. Все эти сценарии могут быть смоделированы, используя описанные модели.

F2.3.2 Моделирование системы с полнотой контроля равной 1

Марковская цепь этой системы показана на рис. F8. Состояния задаются двумя переменными (X,Y), где X – число функционирующих процессоров в системе, а Y – число функционирующих шин в системе.

В случае полного контроля, можно предположить, что когда процессор или шина отказали, система всегда успешно переходит к следующему резервному уровню (т.е. из состояния (3,2) к состоянию (2,2) или из (3,2) к (3,1) при отказе процессора или шины соответственно (см. рис. F8)).



Марковская цепь системы, имеющей 3 процессора и 2 шины
Рис. F8

Предположим, что $P_i(t)$ есть вероятность нахождения системы в состоянии «i» в течение времени «t», тогда уравнения состояния, построенные на основе рассмотрения описанной ранее Марковской цепи, будут следующими:

$$\frac{dP_1(t)}{dt} = (-3\lambda_1 - 2\lambda_2)P_1(t)$$

$$\frac{dP_2(t)}{dt} = 3\lambda_1 P_1(t) - (2\lambda_1 + 2\lambda_2)P_2(t)$$

$$\frac{dP_3(t)}{dt} = 2\lambda_1 P_2(t) - (\lambda_1 + 2\lambda_2)P_3(t)$$

$$\frac{dP_4(t)}{dt} = 2\lambda_2 P_1(t) - (3\lambda_1 + \lambda_2)P_4(t)$$

$$\frac{dP_5(t)}{dt} = 2\lambda_2 P_2(t) + 3\lambda_1 P_4(t) - (2\lambda_1 + \lambda_2)P_5(t)$$

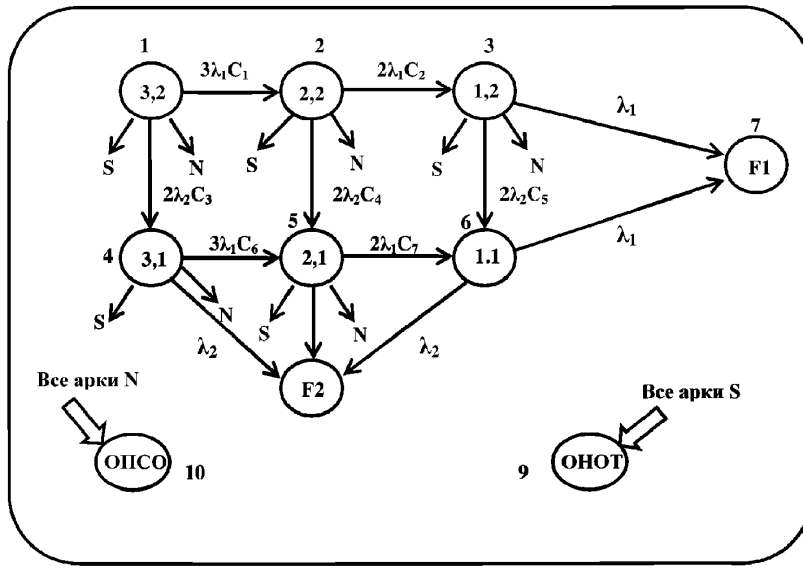
$$\frac{dP_6(t)}{dt} = 2\lambda_2 P_3(t) + 2\lambda_1 P_5(t) - (\lambda_1 + \lambda_2)P_6(t)$$

$$\frac{dP_7(t)}{dt} = \lambda_1 P_3(t) + \lambda_1 P_6(t)$$

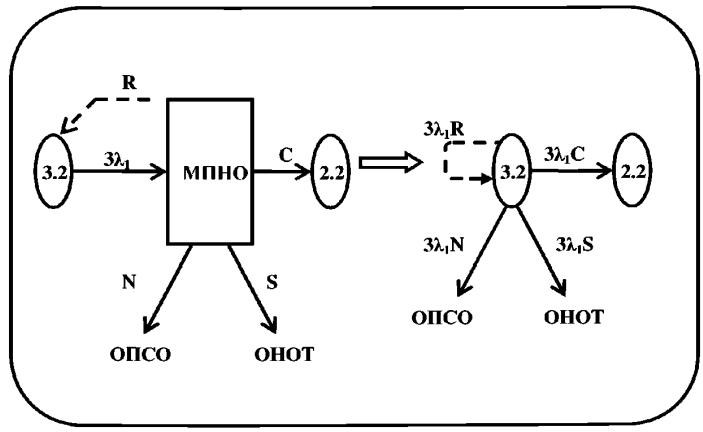
$$\frac{dP_8(t)}{dt} = \lambda_2 P_4(t) + \lambda_2 P_5(t) + \lambda_2 P_6(t)$$

F2.3.3 Моделирование системы с полнотой контроля меньше 1

Если система, имеющая 3 процессора и 2 шины, содержит неполный контроль (т.е. возможны скрытые отказы и способность обнаружить неисправность меньше, чем 100%) или может иметь повторяющиеся, перемежающиеся или совпадающие отказы, то можно моделировать эти сценарии, используя некоторый тип модели учета неисправности и ошибок. Когда возникает неисправность, система может восстановиться без сообщения о наличии неисправности. Рис. F6 показывает шесть исходных моделей, которые являются доступными в среде моделирования HARP. Рис. F9 показывает Марковскую цепь с охватом, используемым для выявления неисправности системы. Когда возникает неисправность, то есть некоторая вероятность C меньше 1, система будет реконфигурирована на следующий более низкий резервный уровень. Неисправность также может быть не обнаружена и это может вызвать полный отказ системы. Вероятность такого отказа обозначена как отказ из-за неисправности одной точки (ОНОТ). Другой вид отказа, который рассмотрен в этой Марковской цепи такой, что когда происходит восстановление от неисправности, вторая неисправность возникает почти в то же самое время или перед реконфигурацией, что может вызвать отказ из-за почти совпадающего отказа (ОПСО).



Представление Марковской цепи, имеющей 3 Процессора и 2 шины, с неполным охватом
Рис. F9



Эффект использования моделей в представлении Марковской цепи
Рис. F10

Здесь, из состояния (3,2) система переходит к состоянию со скоростью отказа $3\lambda_1$. Из этого состояния система может выйти в четыре направления (каждое из которых соответствует поведению системы в состоянии неисправности).

a. Она может перейти в состояние (2,2) с конечной вероятностью, определяемой величиной неполного охвата C.

b. Система устанавливает неисправность и возвращается назад к состоянию (3,2) с вероятностью, данной фактором восстановления R.

c. Неисправность может быть необнаруженной и приводит к отказу системы с вероятностью S.

d. Перед тем, как система может реконфигурироваться от первой неисправности, в системе может произойти вторая неисправность с вероятностью N и эта двойная неисправность в системе приводит к почти совпадающему отказу.

Как показано на рис. F10, каждое состояние в Марковской цепи модифицировано путем C, R, S и N величин и затем решающих Марковскую цепь. Эти величины напрямую обеспечены пользователем или вычислены от распределений для этих выходов, данных пользователем. Инструмент HARP имеет способность модифицировать Марковскую цепь таким образом, что пользователь обеспечивает FEHM.

В инструменте SURE концепция FEHM включена в форме функций. Всякий раз, когда компоненты отказывают, используется функция, определяющая значение времени реконфигурации системы в пониженное состояние с уменьшением резервирования. Точно также другие функции используются для распределения почти совпадающих отказов. Преимущество программы SURE в том, что эти функции могут быть любыми функциями распределения и не ограничены никакими экспоненциальными функциями.

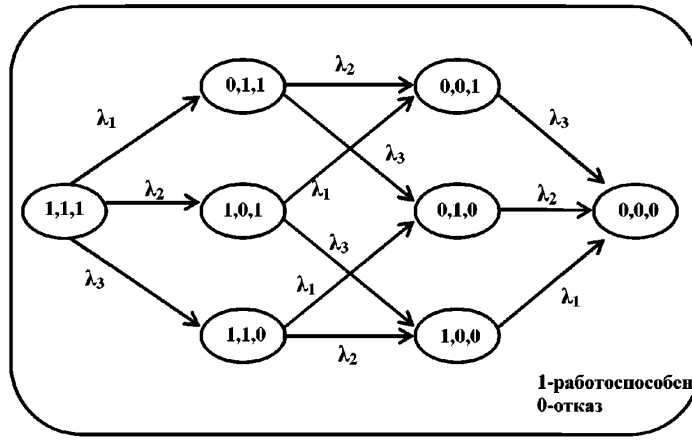
F3 МЕТОДЫ УМЕНЬШЕНИЯ ПРОСТРАНСТВА СОСТОЯНИЯ ДЛЯ МАРКОВСКИХ МОДЕЛЕЙ

Марковские модели могут стать очень большими и комплексными. По этой причине, может быть, необходимо исследовать методы для уменьшения размера моделей.

F.3.1 Агрегированное состояние

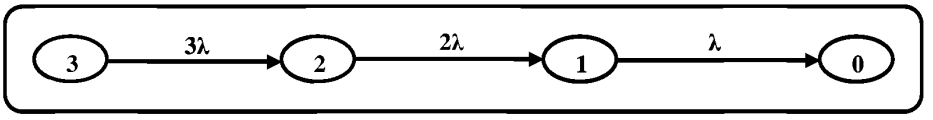
Агрегированное состояние является одним из методов по уменьшению размера Марковской цепи. Этот метод рассматривает в совокупности два состояния с идентификацией скоростей отказа в одном состоянии. Пример, приведенный ниже, показывает концепцию агрегированного состояния.

Система содержит 3 процессора со скоростями отказа λ_1, λ_2 и λ_3. Принято, что система отказала, если отказали все процессоры. Рис. F11 показывает Марковскую цепь системы.



Представление Марковской цепи системы, имеющей три процессора
Рис. F11

Чтобы проиллюстрировать состояние агрегации, принимают, что все процессоры идентичны. Следовательно, скорости отказа всех компонентов задаются, как λ. Эквивалент Марковской цепи в этом случае может быть уменьшен путем комбинирования всех состояний, которые находятся в пределах некоторого столбца на рис. F11. Уменьшение было возможным за счет того, что любая пара переходов между двумя столбцами является идентичной и это уменьшает Марковскую цепь, как показано на рис. F12.



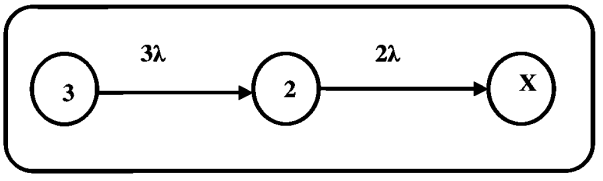
Уменьшенное состояние трехпроцессорной системы за счет использования
Агрегационного состояния
Рис. F12

Любой может заметить, что в одном столбце на рис. F11 три состояния могут быть собраны в одно состояние на рис. F12. Это уменьшает общее число состояний с 8 на рис. F11 до 4 на рис. F12.

Эти состояния являются эквивалентом аппаратных средств, т.к. неисправности, которые определяют эти состояния, равны. Они являются также эквивалентом перехода, так как надежность продолжающейся системы, когда возникают последующие неисправности, тоже идентична. Состояния, эквивалентные аппаратным средствам, не являются эквивалентом необходимого перехода и наоборот. Это только переходная эквивалентность, которая является правильной для уменьшения модели.

F.3.2 Модель усечения

Модель усечения уменьшает Марковскую цепь путем завершения процесса генерации Марковской цепи в направлении, в котором вероятности состояния будут очень малы. Другая форма усечения – это завершение генерации Марковской цепи, после того как в системе возникнет определенное количество отказов. Это предполагает, что вероятность нахождения системы с количеством отказов больше, чем предел усечения очень мала. Используя тот же самый пример, показанный на рис. F12, можно предположить, что модель усечена после двух отказов. Тогда Марковская цепь является уменьшенной и это показано ниже.

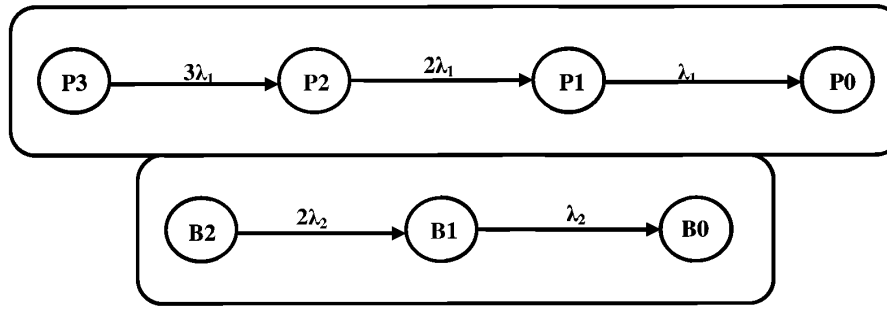


Уменьшенное состояние трехпроцессорной системы
в результате Модели усечения
Рис. F13

Путем решения этих моделей любой может определить/проверить, что точная ненадежность полной системы находится между верхними и более низкими границами, полученными от усеченной модели. Аналитик должен решить какой требуется уровень усечения путем оценки распространения между верхними и более низкими границами. Верхние границы надежности системы получены, предполагая, что все усеченные состояния являются рабочими состояниями. Точно также, более низкие границы надежности системы получены, предполагая, что все усеченные состояния – отказные состояния. Эти вычисления сделаны с применением многих инструментов, таких как HARP, SURE и других, которые рассмотрены ниже.

F.3.3 Иерархическое моделирование

Один метод уменьшения размера Марковской цепи – это разбить большую модель на много независимых подмоделей. Это может быть достигнуто, если каждая подмодель является независимой. Чтобы проиллюстрировать на примере этот сценарий, рассмотрим ранее определенную систему, состоящую из трех процессоров (скорость отказа: λ_1) и двух шин (скорость отказа: λ_2). Принято, что система отказала, если все три процессора отказали или обе шины отказали. Любой может развивать подмодели для системы процессора и системы шины и затем решить их отдельно перед объединением их результатов. Рис. F14 показывает подцепи для системы процессора и шины. В качестве предупреждения можно сказать, что независимость подмоделей, в таких случаях, должна быть оценена очень тщательно; в системах устойчивых к текущей неисправности, где включены зависимости компонента и восстановления, разбивающие модель на независимые подмодели не всегда может быть возможна.



Раздельные порции для системы с процессором и шиной
Рис. F14

Вероятность отказа системы от простых комбинированных методов задана как:

P (отказ всех процессоров или всех шин)

= вероятность отказа всех процессоров (prob.(P0))

+ вероятность отказа всех шин (prob.(B0))

- prob.(P0)* prob.(B0)*

Это уравнение следует из предположения о независимости между подмоделями шины и процессора.

F.4 ДОСТУПНЫЕ ИНСТРУМЕНТЫ

Доступны многочисленные средства решения Марковских моделей. Следующие три компьютерных инструмента (SURE, SHARPE и HARP) можно успешно применить ко многим большим и сложным Марковским задачам. Другие инструменты (SPNP, REST, SURF, ASSURE), которые имеют дело с проблемами надежности и пригодности могут быть отнесены к одному из этих трех инструментов. SURE был разработан в НАСА Ленгли, тогда как HARP был разработан в университетах Дюка и Клемсона при поддержке НАСА. Оба этих инструмента доступны в НАСА Ленгли. SHARPE был разработан в университете Дюка.

F.4.1 SURE – полумарковский оценщик диапазона ненадежности и ASSIST

Программа SURE использует две теоремы ограничения, чтобы вычислить верхние и нижние границы надежности системы. Преимущество метода SURE состоит в том, что границы представлены в алгебраической форме и, следовательно, являются эффективными в отношении вычислений. Программа SURE делит переходы на быстрые и медленные траектории, где быстрые траектории определяют восстановление системы от неисправности, а медленные траектории относятся к отказам системы. Как только траектории определены, программа SURE составляет список траекторий, ведущих от начального состояния к конечному нежелательному состоянию и вычисляет вероятность пересечения этой траектории данного значения и распределение функции перехода для каждой ветви в траектории. Эта программа позволяет решать большие и сложные Марковские модели.

Так как программа SURE может поддерживать общее распределение времени восстановления, полная обработка процесса поддержки неисправности может быть захвачена в отдельном переходе. Выход содержит следующую информацию.

a. Верхние и нижние границы вероятности отказа полной системы.

b. Границы вероятности для каждого нежелательного случая в модели.

c. Список каждой траектории в модели и ее вероятность пересечения.

Связанная программа названа «ASSIST» и может производить Марковские модели в формате, совместимом с SURE. Однако чтобы ввести данные нужно изучить язык ASSIST. Из-за ограничений алгоритмов ограничения, устойчивое решение состояния или быстрые средние вероятности не могут быть вычислены с помощью SURE.

F.4.2 SHARPE – символический иерархический автоматизированный оценщик надежности/работоспособности

SHARPE позволяет пользователю строить гибридные и иерархические модели системы. Гибридное моделирование объединяет гибкость Марковских моделей и эффективность комбинированных методов. Типы встроенной модели: блок-диаграмма надежности, дерево неисправности, грифы надежности, Марковские цепи, нециклические и несократимые полумарковские цепи, сети, организующие очередь формы – изделия отдельной и многократной цепи, (которые являются каскадом Марковских цепей), обобщенные стохастические сети Петри (описание конечного состояния машины системы), и графы последовательно-параллельной задачи. Иерархическое моделирование соединяет предопределенные модели, таким образом избегая проблем жесткости и большого состояния.

Непринужденность использования и эффективность SHARPE делают его очень полезным инструментом для предварительного проекта.

F.4.3 HARP – гибридный автоматический предсказатель надежности

Главный подход для уменьшения размера в HARP – поведенческое разложение. Модель надежности разделена на два типа моделей: медленные и быстрые. Модели восстановления возникшей неисправности проанализированы отдельно. Модели содержат информацию о структуре процедур восстановления резервирования аппаратных средств ЭВМ и может быть представлена либо в виде дерева неисправности либо как Марковская цепь. Модель охвата (FEHM) позволяет моделировать процедуры восстановления, необходимые для трех типов неисправностей: постоянные, промежуточные и переходные неисправности. Пользователю доступны семь различных типов FEHM. HARP принимает номинальное значение и разность всех входных параметров. Дополнительно HARP поддерживает моделирование скоростей отказа, зависимых от времени, связанных с распределением отказов Вейбулла. Эта способность применима только к невосстанавливаемым системам. Выходной файл содержит информацию о вероятности состояний, определенных пользователем. HARP обеспечивает автоматическую генерацию Марковских цепей для невосстанавливаемых систем, если вход является деревом неисправности.

С системами, устойчивыми к неисправности, компоненты могут находиться как в рабочем, так и в нерабочем состоянии к началу полета. Компоненты обслуживаются в различные конкретные периоды времена с учетом планов обслуживания авиакомпаний. Следовательно, возможно, что один или более зарезервированных компонентов могут иметь отказ (скрытый или не скрытый) перед началом полета. Другой сценарий имеет дело с различными режимами полета, где компоненты могут иметь различные скорости отказа или различный набор компонентов, находящихся в рабочем состоянии.

F.5 ПРИМЕРЫ

Некоторые из примеров Марковского моделирования, которые имеют большое значение для авиационных систем приведены ниже. Любой инструмент может быть использован для составления и решения уравнений. Для краткости, уравнения здесь не показаны.

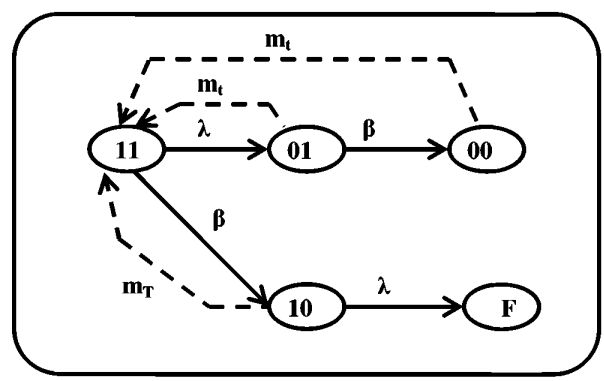
Марковские модели, показанные ниже, представляют методологию для моделирования скрытых неисправностей. Результаты могут быть обработаны для получения вероятностей наихудшего случая отказа и вероятностей среднего отказа. Модели формируют вектор вероятностей отказов, где каждая компонента вектора соответствует вероятности отказа системы на полет. Используя эти величины, вычислена оценка наихудшего случая вероятности отказа, при этом берется вероятность отказа последнего полета. Чтобы вычислить среднее значение вероятности отказа сверх продолжительности интервала проверки обслуживания, можно суммировать все значения вероятности отказа в конце каждого полета и поделить на количество полетов.

F.5.1 Моделирование скрытого отказа с использованием дискретного процесса восстановления

Если известен компонент, работающий в начале полета, то вычисление надежности основывается на времени задержки, равном длительности полета. Некоторые системы самолета включают компоненты, которые не проверяются в каждом полете. Отказы такого типа компонента называются скрытыми, потому что они не обнаруживаются, если не возникает другого отказа или не выполнена намеченная проверка. Есть несколько возможных вариантов, так или иначе зависящих от активных и резервных систем, которые являются скрытыми или наблюдаемыми событиями и последующий отказ является важным или нет. Разделенные дуги восстановления на рисунках с F15 по F18 представляют дискретные восстановления в установленных интервалах. Восстановления из отказных состояний системы F не показаны, потому что они зависят от политики обслуживания (т.е. восстановления могут быть частичные или полные). Некоторые из важных сценариев по Марковскому представлению для этих сценариев, даны ниже.

a. Сценарий I. Система, включающая компонент и контроль.

Компонент проверен перед каждым полетом, чтобы подтвердить его работоспособность или восстановлен, если это необходимо. Контроль не проверен перед каждым полетом, но регулярно проверен в период обслуживания. Таким образом, отказ контроля может быть скрытым. В анализе надежности мы должны различать контролируемый отказ и неконтролируемый отказ компонента, потому что последствия неконтролируемого отказа, вероятно, будут более серьезными. Здесь мы исследуем только вычисление вероятности неконтролируемого отказа. Неконтролируемый отказ возникает только, если контроль отказывает перед компонентом. Марковское представление этого сценария показано на рис. F15. Конец проверок полета и ремонта, если требуется, представлены как пунктиры с параметром m_t на рис. F15. Намеченная проверка и восстановления, если требуется, показаны как пунктиры с параметрами m_T на рис. F15. Это верно во всех последующих Марковских моделях, показанных на рисунках F16 – F18. На рис. F15, λ является скоростью отказа компонента, а β – контроля.



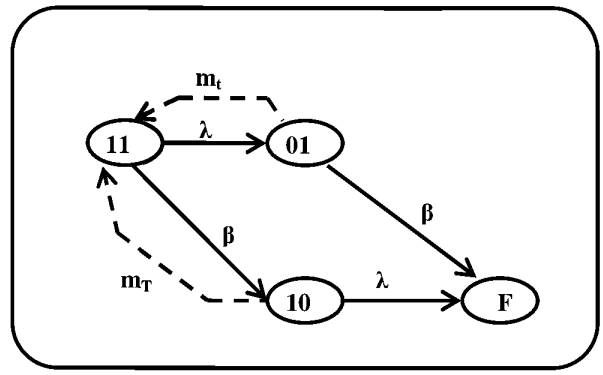
Марковская цепь для компонента и системы контроля со скрытым отказом
Рис. F15

b. Сценарий II. Система, включающая компонент и резервный компонент.

Компонент проверен в каждом полете и восстановлен, если найдены дефекты. Резервный компонент проверен только в период обслуживания. Отказ системы возникает в случае, если резервный компонент отказывает в то же время, когда отказывает компонент или если резервный компонент отказывает в том же самом полете, что и компонент. Это отличается от сценария I тем,

что отказ контроля после отказа компонента, но в том же самом полете, не будет включать неконтролируемый отказ. Марковское представление этого сценария показано на рис. F16.

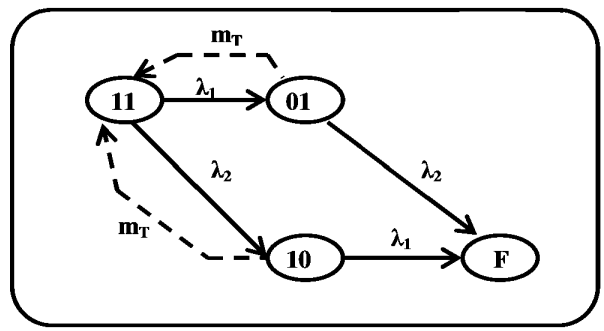
На рис. F16 λ – скорость отказа компонента, а β – резервного компонента.



Марковская цепь для компонента и резервной системы со скрытым отказом
Рис. F16

c. Сценарий III: Система, включающая два компонента.

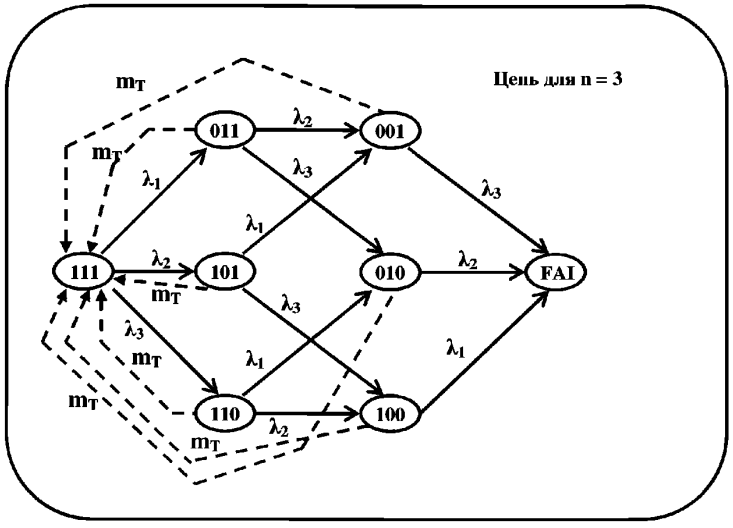
Когда отказывает один компонент системы, состоящей из двух компонентов, в работу включается резервный, но никак не отображается то, что это случилось. Система проверена в каждом полете чтобы гарантировать, что система является работоспособной. Эта проверка гарантирует, что, по крайней мере, один из двух компонентов работает. Индивидуальные компоненты проверены в установленный период Обслуживания. Марковская модель представления для этого сценария показана на рис. F17. Оба компонента восстановлены в конце намеченной проверки, как показано пунктирами в модели. Вероятность состояния «F» в конце каждого полета сведена к нулю, чтобы принять во внимание тот факт, что система работоспособна в начале любого полета, по крайней мере, с одним функциональным компонентом.



Марковская цепь для системы с двумя компонентами,
в обоих случаях скрытый отказ
Рис. F17

d. Сценарий IV. Система, включающая «n» компонентов.

Когда отказывает один компонент системы, включающей «n» – компонентов, в работу включается резервный, но никак не отображается, то что это случилось. Система проверена в каждом полете чтобы гарантировать, что система является работоспособной. Эта проверка гарантирует, что, по крайней мере, один и «n» – компонентов работает. Индивидуальные компоненты все проверены в установленный период Обслуживания T. Марковская цепь представления для системы, состоящей из трех компонентов, показана на рис. F18. Все периоды восстановления в модели являются намеченным периодом проверки всех компонентов. В конце каждого полета вероятность отказного состояния сведена к нулю, чтобы принять во внимание тот факт, что система работоспособна в начале любого полета, по крайней мере, с одним функциональным компонентом.



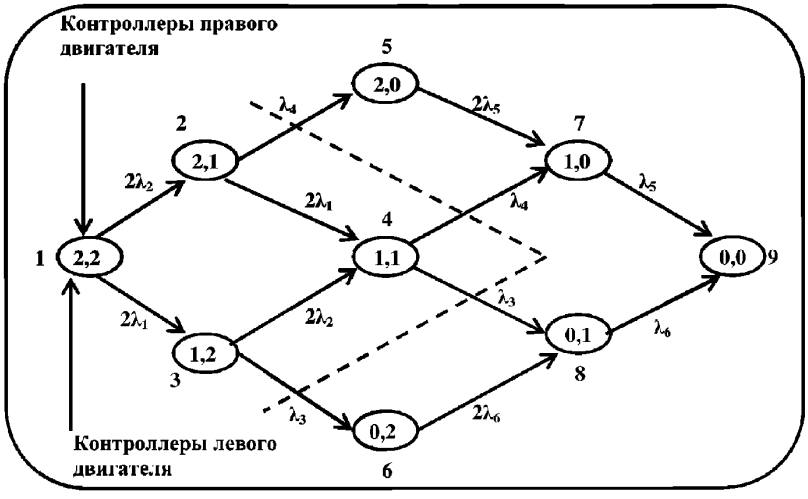
Марковская цепь для системы с темя компонентами, все со скрытым отказом
Рис. F18

F.5.2 Пример намеченного обслуживания

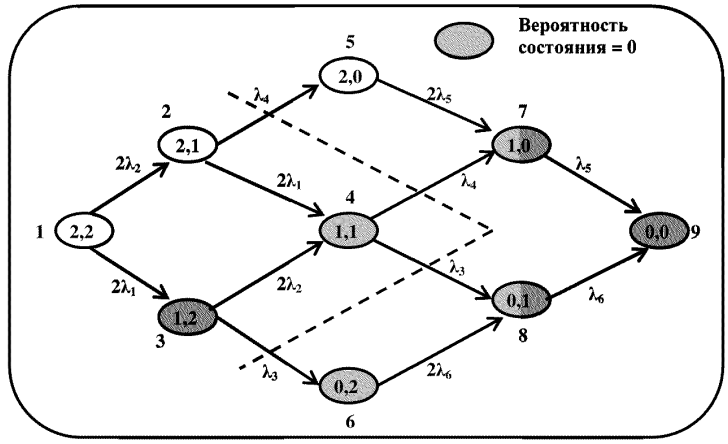
В качестве примера рассматривается система с двумя двигателями, левым и правым, где каждый двигатель имеет два контроллера, как проиллюстрировано на рис. F19. Система отказывает тогда, когда все 4 контроллера теряют возможность функционировать (состояние 9 в Марковской цепи). Функциональность системы ухудшена, когда один или более контроллеров не работают. Рассматривается, что невозможность вылета согласно инструкциям имеет место, когда не работают оба контроллера для одного двигателя. На рис. F19 все состояния, показанные слева от пунктира, являются состояниями, при которых возможен вылет. Однако, определения отказа (сценарии) могут быть изменены, чтобы учитывать минимальный состав оборудования. В примере предполагается, что система имеет различную скорость отказа из каждого состояния.

Если левый двигатель восстановлен к концу полета, то можно знать наверняка, что оба контроллера для этого двигателя будут работоспособны к началу следующего полета. Другими словами, в Марковской цепи к началу следующего полета, вероятность отказа контроллера для левого двигателя должна быть нулевой. Эти результаты в вероятностях состояний 3, 4, 6, 7, 8, 9 (заштрихованы на рис. F20) инициализированы к нулю в начале следующего полета. Пользователь должен знать, что это перераспределени4е вероятностей состояния может быть вычислено в модифицированной версии HARP.

Пользователь должен определить, что левый двигатель доведен до полностью работоспособного состояния, а остальное делает программа.



Марковская цепь для примера с двумя двигателями
Рис. F19

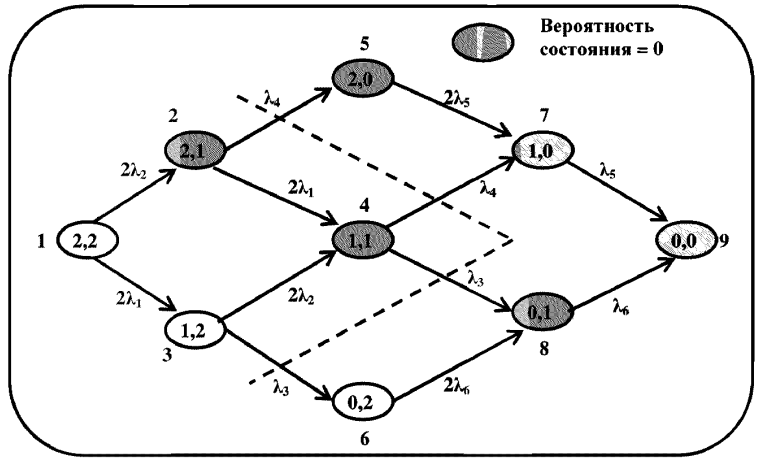


Модификация Марковской цепи, когда левый двигатель приведен в полностью работоспособное состояние к началу следующего полета

Рис. F20

Точно также, когда правый двигатель восстановлен к концу полета, то можно знать наверняка, что оба контроллера для этого двигателя будут полностью работоспособны к началу следующего полета. Другими словами, в Марковской цепи к началу следующего полета вероятность отказа контроллера для правого двигателя должна быть нулевой. Эти результаты в вероятностях состояний 2, 4, 5, 7, 8, 9 (легко заштрихованы на рис. F21) инициированы к нулю в начале следующего полета.

Этот пример показывает полезность Марковского моделирования, поскольку это позволяет пользователю определять различные сценарии обслуживания.



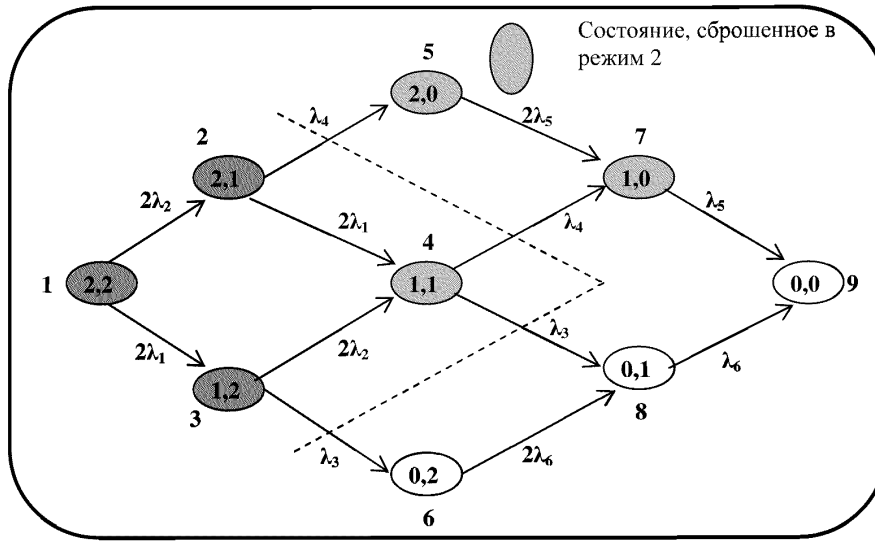
Модификация Марковской цепи, когда правый двигатель приведен в полностью работоспособное состояние к началу следующего полета

Рис. F21

F.5.3 Многорежимный пример

Рассматривается тот же самый пример с двумя двигателями, данный в предыдущем подразделе. Принято, что система имеет два режима. В первом режиме система находится в начале в состоянии, когда два контроллера на обоих двигателях работают исправно. Теперь предположите это во втором режиме, зная, что два контроллера на левом двигателе отказали, требуется оценить определенный риск системы. Здесь определенный риск – это последующий риск в полете, дающем известное сообщение о неработоспособном состоянии (т.е. оба контроллера на левом двигателе отказали). Зная это, требуется узнать, как долго система может работать безопасно пока самолет приземляется в ближайшем аэропорту в пределах указанной продолжительности.

Марковская цепь для режима 1 та же самая, что показана на рис. F19. В режиме 2, поскольку принято что левый двигатель отказал, что в системе есть только три состояния: в правом двигателе либо два, один или ноль контроллеров исправны. Конечная Марковская цепь для режима 2 показана на рис. F22. Принято, что система является работоспособной до тех пор, пока исправен, по крайней мере, один контроллер на правом двигателе. Поскольку каждый предполагает, что левый двигатель отказал в начале второго режима, состояния 1, 2, 3, 4, 5 и 7 обнулены в начале режима 2. Результаты в конце режима 2 дают определенный риск системы, дающей тот факт, что режим запущен в ухудшенной конфигурации.



Модификация Марковской цепи для конфигурации режима 2 в режиме 2, теневые состояния, пониженные от Марковской цепи
Рис. F22

Программные инструменты HARP и SURE могут быть модифицированы, чтобы включать многорежимные анализы и намеченные сценарии обслуживания.

ПРИЛОЖЕНИЕ G

Анализ видов и последствий отказа

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

G.1 ВВЕДЕНИЕ

Анализ видов и последствий отказа является систематическим исследованием видов отказа системы, блока, функции или компонента и определения последствий на следующем более высоком уровне конструкции. Одновременно он может быть определен как метод нахождения всех видов отказа. FMEA может быть количественным или качественным анализом и может выполняться для систем любого типа (т.е. электрических, электронных или механических систем). Если выполняется количественный FMEA, то для каждого вида отказа определяется интенсивность отказов. Результаты FMEA могут использоваться для подготовки сводки видов и последствий отказа и обычно применяются для поддержки других методов анализа в процессе SSA, таких как FTA, DD или MA. Комбинации отказов обычно не рассматриваются как часть FMEA.

G.2 НАЗНАЧЕНИЕ

FMEA выполняется на выбранном уровне (система, блок и т.д.) постулированием возможных проявлений отказа элемента на выбранном уровне. Последствия каждого вида отказа определяются для каждого режима эксплуатации оборудования на выбранном уровне и обычно на следующем более высоком уровне. FMEA может быть сосредоточен на конкретном сценарии эксплуатации, если это требуется для поддержки нисходящих FTA, DD или MA.

FMEA должен рассмотреть все связанные с безопасностью последствия и любые другие последствия, указанные в требованиях к нему. В случаях, когда оказывается невозможным установить конкретное проявление вида отказа, должно быть принято наиболее худшее проявление. Если наиболее худшее неприемлемо для дерева неисправности, то виды отказа должны быть рассмотрены на следующем более низком рассматриваемом уровне (т.е. если FMEA проводится на функциональном уровне, то следует перейти на компонентный уровень и исключить компоненты, которые не влияют на рассматриваемое событие, а если анализ проводится на уровне компонентов, то перейти к рассмотрению конкретных механизмов отказа в компоненте; другим путем может быть изменение конструкции усовершенствованием резервирования или введением контроля).

Независимо от уровня выполнения FMEA основными его этапами являются подготовка, собственно анализ и документирование.

G.3 ПРОЦЕСС FMEA

G.3.1 Подготовка к анализу

Подготовка включает в себя определение требований заказчика, получение действующей документации и изучение выполнения функций.

До начала анализа важно знать требования и ожидания заказчика. Если требования к FMEA неизвестны, то результаты могут не соответствовать нуждам заказчика и может потребоваться переработка.

Требования к FMEA обычно исходят из действий PSSA, таких как FTA, DD или MA. Выполняющему анализ необходимо знать уровень анализа (функциональный или компонентный), связанный с безопасностью последствия и интересующие эксплуатационные режимы. FMEA используется для поддержки процесса оценки безопасности системы, определяя интенсивности отказов для количественных значений основных событий в FTA, DD или MA. FMEA может также использоваться для поддержки верификации FTA сравнением видов отказов FMEA с основными событиями дерева неисправности.

Завершением подготовки к анализу является получение следующей информации, которая может потребоваться для окончания анализа или может упростить выполнение работы:

a. Требования к FMEA, включая связанные с безопасностью, запрашиваемые последствия отказа и интересующие специфические режимы эксплуатации.

b. Спецификации.

c. Действующие чертежи и схемы.

d. Перечень элементов каждой системы или объекта.

e. Функциональные блок-схемы.

f. Пояснительный материал, включая принципы работы.

g. Перечень применимых интенсивностей отказов.

h. FMEA предыдущей разработки или для подобной функции.

i. Любые изменения и уточнения конструкции, которые пока не нашли отражения в схемах. (*Примечание: Конструкция может изменяться достаточно часто, и обработка уточняющих материалов может задерживать обновление данных FMEA.*)

j. Предварительный перечень видов отказов компонент из предыдущих FMEA, если применимо.

Примечание: *Для FMEA, которые выполняются на раннем этапе проекта, некоторые из указанных материалов могут отсутствовать, и могут быть сделаны только оценки и предположения. Подробная документация о таких предположениях должна сохраняться для упрощения будущих корректировок.*

G.3.2 Выполнение анализа

Выполняющему анализ необходимо проверить и разобраться в информации, которая получена на описанном ранее подготовительном этапе. Для выполняющего анализ будет полезным понимание функций, которые анализируемая конструкция выполняет на следующем более высоком уровне. После приобретения выполняющим анализ необходимых знаний определяются виды отказа. Каждый возможный вид отказа аппаратных средств постулируется на анализируемом уровне конструкции. Рассматриваются виды отказов компонент или функций, которые составляют данный уровень. В разделах G.3.2.1 и G.3.2.2 приведена информация, которая поможет в определении видов отказа функции или компоненты.

Каждый установленный вид отказа анализируется для определения его последствий на данном уровне и, кроме того, обычно, на более высоких уровнях. Категории последствий отказа назначаются для каждого отличающегося типа последствий. Каждая категория может получить свое кодовое обозначение. Применение таких кодов упрощает рабочую таблицу FMEA за счет перенесения описания каждого последствия из этой таблицы в текст документа. Рабочая таблица FMEA содержит перечень видов, последствий и интенсивностей отказов. Примеры рабочих таблиц FMEA приводятся в следующих разделах. Каждая категория последствий должна иметь только одно последствие верхнего уровня, в противном случае должно быть сделано более подробное определение категорий последствий. Например, если категория последствий вначале определена как «вызывает выход сигнала xyz за установленные пределы», но выход за пределы при увеличении и при уменьшении имеет отличающиеся последствия, то категорию последствий следует разделить на «... за установленные пределы вверх» и «... за установленные пределы вниз». Аналогично, если найдено, что вид отказа вызывает на более высоком уровне два вида последствий (например, «потеря сигнала A» и «потеря сигнала B»), то они оба должны быть объединены для формирования новой категории последствий «потеря сигнала A и сигнала B».

Обычно в рабочей таблице указываются найденные методы обнаружения отказа. Примерами методов обнаружения служат: обнаружение аппаратными или программными схемами контроля, обнаружение летным экипажем, тест при включении питания и проверки при наземном обслуживании.

В количественном FMEA каждому виду отказа приписывается значение интенсивности отказов. Когда это возможно, такие интенсивности следует определять на основе данных эксплуатации подобного оборудования. Можно также использовать общепринятые справочные

данные по интенсивностям отказов. Общая интенсивность отказов для каждой категории последствий отказа может быть уточнена в обобщающей рабочей таблице или просуммирована в FMEAS, описанной в Приложении H.

Имеется два основных типа FMEA – функциональный и компонентный. Обычно для поддержки анализа безопасности выполняется функциональный FMEA, а компонентные анализы выполняются при необходимости дальнейшего уточнения интенсивности отказов. Компонентный анализ обычно выполняется в том случае, когда более консервативные интенсивности отказов из функционального анализа не обеспечивают соответствия системы или объекта установленному в FTA бюджету вероятности. Компонентный анализ может оказаться полезным для систем, в которых используется резервирование. Функциональный анализ может не обнаружить единичные отказы компонент воздействующих более чем на один резервируемый элемент. Компонентный анализ также может быть полезным при анализе безопасности механических систем и сборок.

G.3.2.1 Функциональный FMEA

Функциональный анализ может проводиться на любом желаемом уровне. Адекватный уровень разбиения определяется сложностью системы и целями анализа. Если требуется проведение анализа для части схемы или механических устройств выполняющих не только конкретную функцию, то схемы или устройства следует разделить на функциональные блоки. На уровне самолета или системы это может означать выделение каждого съемного блока или объекта в функциональный блок. На уровне системы и нижних уровнях разделение может привести к делению съемного блока на много блоков. Задача анализа упрощается, если каждый блок имеет минимально возможное число выходов. Как только определены функциональные блоки, следует сделать функциональную блок-схему и пометить каждый блок в соответствии с наименованием его функции. Для каждого функционального блока следует проанализировать в отношении к операциям системы внутренние и интерфейсные функции.

Следующим шагом является постулирование видов отказа каждого функционального блока. Виды отказа определяются на основе размышлений о назначении функционального блока и попыток определить, независимо от конкретного применения блоков, как эта функция может отказать. Выполняющий анализ должен хорошо знать работу функционального бока, чтобы быть уверенным, что не пропущены значимые виды отказа. Часто многие виды отказа становятся очевидными после ясного описания функции блока.

Указанное ниже является простым примером функциональных видов отказа.

Схемы источника питания, формирующие 5V могут быть названы функциональным блоком. К функциональным видам отказа такого блока можно отнести следующие:

a. Потеря 5V.

b. Напряжение меньше чем 5V.

c. Напряжение больше чем 5V.

d. Шум в напряжении 5V.

e. Короткое замыкание на землю или иное напряжение.

Основываясь на реализации схемы можно выявить другие виды отказа.

Последствия каждого вида отказа определяется рассмотрением того, как функция блока применяется в общей конструкции. Категории последствий отказа обычно находятся для каждого типа последствий. Им присваиваются коды категории последствий отказа. Все виды отказа, которые приводят к одинаковым последствиям, относят к одной категории последствий. Код категории последствий может быть указан в рабочем листе анализа для каждого отказа, как это показано в таблице G1. При определении последствий отказа должны рассматриваться программное обеспечение и средства обнаружения отказа. Выполняющий анализ должен в ходе работы проверить, что средства контроля могут действительно обнаружить отказы такого вида. Для четкого проведения анализа у выполняющего анализ должно иметься детальное представление о требованиях к системе и реализации программного обеспечения, включая внутренние методы контроля исправности, если применимо.

Если выполняется количественный анализ, то каждому виду отказа назначается интенсивность отказов. Один из методов определения прогнозируемой интенсивности отказов для каждого блока и распределения интенсивности по различным видам отказов основывается на имеющемся опыте работы с подобными функциями или другими источниками, которые позволяют определить необходимые вероятности. Рекомендации по разделению отказа на составляющие приведены в разделе G.3.2.2.1.

Результаты функционального анализа записываются в рабочую таблицу подобную приведенной на рис. G1. В зависимости от требований к анализу форма таблицы может быть изменена добавлением или удалением некоторой информации. Выполняющему анализ следует в самом начале убедиться, что форма и содержание рабочей таблицы анализа соответствует нуждам заказчика.

В обеспечение будущего уточнения результатов и разрешения возникающих вопросов следует в ходе проведения анализа неформально зафиксировать следующую информацию:

a. Обоснование каждого вида отказа.

b. Объяснение назначенной интенсивности отказов.

c. Объяснение отнесения конкретного отказа к той или иной категории последствий отказа.

d. Документация по любому сделанному предположению.

Эти сведения обычно не включаются в отчет по FMEA, но сохраняются для ссылок.

G.3.2.2 Компонентный анализ

Компонентный анализ подобен функциональному, за исключением того, что вместо анализа на уровне функций или блок-схем анализируются виды отказов каждой отдельной компоненты объекта или функции. Компонентный анализ может использоваться для определения последствий отказов для возможных электрических, электронных или механических отказов. Например, последствия отказов сопротивления или оси двигателя могут быть рассмотрены в компонентном анализе. Компонентный анализ для электронного оборудования обычно выполняется при необходимости, когда более консервативные результаты функционального анализа не обеспечивают для объекта соответствия вероятностному бюджету FHA. Это происходит, в частности, из-за сложности определения видов отказа для комплексных компонентов.

Первым шагом в проведении компонентного анализа является подготовка перечня всех рассматриваемых в анализе компонентов. Следующий шаг – это определение видов отказа для каждого типа компонента. Это наиболее трудная часть анализа. Определение всех видов отказа любого компонента, исключая простейшие, для которых доступны достоверные данные, чрезвычайно сложно иногда невозможно. В сомнительных случаях о видах отказов компонента должны делаться наиболее неблагоприятные предположения. Информация о методах определения видов отказов приведена в разделе G.3.2.2.1

Как только определены виды отказов компонентов, они вносятся в рабочую таблицу анализа, как показано на рис. G2. Этот образец рабочей таблицы может изменяться для удовлетворения индивидуальных требований, которые могут приводить к добавлению или удалению некоторой информации из таблицы. Выполняющему анализ следует в самом начале убедиться, что форма и содержание рабочей таблицы анализа соответствует нуждам заказчика.

Следующим шагом является определение последствий отказа на следующем более высоком уровне сборки и назначение категории последствий отказа. Для упрощения таблицы могут вводиться коды категорий последствий отказа. Подробное описание каждой категории последствий отказа может быть включено в текст отчета. Все виды отказа, которые приводят к одинаковым последствиям, относят к одной категории последствий. Код категории последствий может быть указан в рабочем листе анализа для каждого отказа, как это показано в таблице G2. При определении последствий отказа должны рассматриваться программное обеспечение и средства обнаружения отказа. Выполняющий анализ должен в ходе работы проверить, что средства контроля могут действительно обнаружить отказа такого вида. Для четкого проведения работы у выполняющего анализ должно иметься детальное представление о требованиях к системе и реализации программного обеспечения, включая внутренние методы контроля исправности, если применимо.

Если выполняется количественный анализ, то каждому виду отказа назначается интенсивность отказов. Рекомендации по разделению отказа на составляющие приведены в разделе G.3.2.2.1.

В обеспечение будущего уточнения результатов и разрешения возникающих вопросов следует в ходе проведения анализа неформально зафиксировать следующую информацию:

a. Обоснование каждого вида отказа.

b. Объяснение назначенной интенсивности отказов.

c. Объяснение отнесения конкретного отказа к той или иной категории последствий отказа.

d. Документация по любому сделанному предположению.

Эти сведения обычно не включаются в отчет по FMEA, но сохраняются для ссылок.

G.3.2.2.1 Определение видов отказов и функций интенсивности отказов компонентов

При проведении компонентного анализа может потребоваться дальнейшее разбиение интенсивности отказов компонента, для того, чтобы определить применимый к специфическому виду отказа процент интенсивности отказов. В нормативных документах промышленности можно найти необходимые данные для многих типов компонентов.

Неполный перечень типовых видов отказа, обычно рассматриваемых в анализе, включают в себя следующее:

a. Обрыв.

b. Короткое замыкание.

c. Смещение параметра.

d. Вне пределов настройки.

e. Пробой диэлектрика.

f. Неустойчивая работа.

g. Прекращение работы.

h. Ложное выполнение.

i. Износ.

j. Механический отказ.

k. Залипание.

l. Расцепление.

m. Разрушение.

В общем случае, должна быть рассмотрена функция компонента, рассмотрены все возможные пути нарушения выполнения компонентом этой функции, затем подготовлен перечень видов отказа компонента. При этом должно быть также рассмотрено ненужное выполнение функции компонента. Технический здравый смысл является необходимой составляющей процесса определения видов отказа.

Хотя существующие нормативные документы дают основу для определения интенсивности и видов отказов многих типов компонентов, могут встретиться типы приборов, которые не включены в эти документы. Это особенно применимо к сложным цифровым интегральным схемам, которые необходимо по-особому рассматривать в каждом отдельном случае. Определение видов отказа цифровых приборов обычно требует инженерного здравого смысла и невероятно, что для сложных цифровых интегральных схем можно определить все виды отказов.

Методом оценивания видов отказов сложных цифровых приборов является моделирование рассматриваемых цифровых приборов с составляющими функциональными блоками, для которых может существовать лучшее определение видов отказа. Если возможно, то виды отказа

прибора идентифицируются при возможных отказах функциональных блоков по последствиям на уровне его штырьков. Особое внимание должно уделяться возможным видам отказов компонента, которые могу привести к основным событиям из FTA.

Не рекомендуется определять для интегральных схем действительные механизмы отказа и связанные последствия с использованием подхода к физике отказа, поскольку это требует выполнения «FMEA» для каждой интегральной схемы. Такой «FMEA» может быть более сложным, чем анализ на верхнем уровне, и может быть даже невозможен для сложных интегральных схем. В дополнение к этому, несообщаемые разработчиком улучшения конструкции кристалла могут полностью обесценить предпринятые усилия. Виды отказа сложной интегральной схемы могут включать промежуточные отказы и различные комбинации отказов, которые возможно воздействуют на множество штырьков.

Виды отказа компонентов других типов более доступны, чем виды отказа интегральных схем. Однако в различных источниках могут приводиться различные распределения видов отказа, а для некоторых типов компонентов даже различные виды отказа. Из этого следует, что даже для простых компонентов трудно определить возможные и невозможные виды отказов.

G.3.2.3 Обоснование

Если для вида отказа трудно определить последствия отказа аналитическим методом, то следует, при наличии возможности, провести лабораторную верификацию. Желательно, чтобы была проведена проверка в испытаниях всех значимых последствий отказа. Для электрических и электронных систем отказы могут вводиться разрывом линий соединения, их закороткой или заземлением. Если выходные сигналы прибора могут принимать три значения, то можно рассмотреть логические комбинации. К сожалению, наиболее трудные для анализа виды отказа часто также трудны и для проверки в испытаниях. Например, невозможно ввести все отказы в большинство интегральных схем. Для моделирования отказов может также использоваться программное обеспечение компьютерного проектирования. Такие программы обеспечивают эквивалентное введение отказа в моделируемые цепи и определение последствий отказа.

Для обоснования результатов FMEA можно также использовать анализ отказов в ходе испытаний и реального использования. Эти данные могут использоваться при разработке библиотеки видов отказа для будущих FMEA.

G.4 ДОКУМЕНТАЦИЯ

G.4.1 Отчет по FMEA

В отчет по FMEA нужно включить следующую информацию:

a. Номер документа для последующих ссылок в FMES, FTA и подобных анализах.

b. Введение, содержащее краткую формулировку назначения и цели работы.

c. Краткий обзор блок-схемы и работы устройств.

d. Раздел с описанием выбранного подхода к анализу. (В раздел следует включить описание того, как был выполнен анализ, определение используемых уровней анализа и перечень принятых допущений).

e. Все результаты анализа (могут использоваться таблицы подобные приведенным в разделах G.3.2.1 и G.3.2.2).

f. Идентификационные номера и варианты исполнения анализируемых аппаратных средств, программного обеспечения и прошитых алгоритмов.

g. В Приложения к отчету следует включить следующие данные:

   (1) Чертежи и схематические диаграммы.

   (2) Распределения по каждому виду отказа компонентов нижнего уровня, которые введены в анализе или получены из других документов (включая обоснование всех рассмотренных видов).

   (3) Перечень использованных в анализе интенсивностей видов отказов и источники этих сведений.

G.4.2 Контрольный перечень FMEA

Следующий контрольный перечень будет гарантировать, что для выполнения эффективного по стоимости и точного анализа сделаны правильные шаги в правильном порядке.

1. Получено записанное техническое задание от заказчика или заинтересованного лица, если возможно, в котором определены:
   (a) интересующие последствия отказа;
   (b) рассматриваемые выходные параметры;
   (c) применяемые методы обнаружения отказа;
   (d) форма заключительного отчета;
   (e) график работы.
2. Подготовка к анализу выполнена:
   (a) найдена и проработана документация;
   (b) разработан перечень компонентов;
   (c) оборудование разделено на подуровни и разделение задокументировано;
   (d) если требуется компонентный анализ, то выполнен сбор видов отказов компонент.
3. Выполнен детальный анализ:
   (a) определены виды отказа и назначены коды последствий отказа;
   (b) удалены плохо определенные виды отказа, так чтобы не возникало путаницы при переходе с текущего уровня на верхние уровни;
   (c) для каждой категории последствий отказа определены средства обнаружения, если требуется;
   (d) сделаны подробные записи, показывающие причины назначения категории отказа.
4. Верифицированы выводы анализа по любому сомнительному случаю (если возможно, то лабораторными или летными данными).
5. Написан заключительный отчет.

G.5 АНАЛИЗ ПОЛНОТЫ ОБНАРУЖЕНИЯ ПРИ ИСПЫТАНИЯХ И КОНТРОЛЕ

Этот тип анализа применяется для определения эффективности различных испытаний по определению скрытых отказов.

Для достижения этого вводятся контрольные применимые виды отказа и определяется, будут ли обнаружены их последствия, и на основании этого определяется процент обнаруживаемой интенсивности отказов. Возможность того, что сами средства обнаружения могут иметь скрытые отказы, считается ограничивающим фактором такого анализа полноты контроля (т.е. покрытие контролем не может быть более достоверным, чем готовность самих средств обнаружения).

Включение полноты контроля в FMEA может привести к тому, что каждый отдельный отказ, имеющий одну категорию последствий, будет, в зависимости от возможной полноты контроля, рассматриваться как имеющий разные категории последствий. Другим способом учета полноты контроля является пессимистическое предположение в FTA о том, что вероятность не обнаружения вследствие скрытых отказов средств контроля добавляется во все отказы, которые отнесены к рассматриваемой категории последствий отказа. В тех случаях, когда такое пессимистическое предположение не будет приемлемо при оценке вероятности события верхнего уровня применяемым требованиям, будет сделано уточнение с необходимым изменением FMEA.

Таблица G1. Рабочий лист функционального FMEA

Анализ видов и последствий отказа		
Система:	Описание FMEA:	Дата:
Подсистема:		Лист из
Объект ATA	Исходный FTA:	Файл
	Автор:	Версия:

Наименование функции	Код функции	Вид отказа	Интенсивность вида отказа	Этап полета	Последствия отказа	Метод обнаружения	Коммен-тарии

Примечание: *Может уточняться для целей и нужд уровня анализа и программы.*

Рис. G1

Таблица G2. Рабочий лист компонентного FMEA

Анализ видов и последствий отказа		
Система:	Описание FMEA:	Дата:
Подсистема:		Лист из
Объект ATA	Исходный FTA:	Файл
Функция:	Автор:	Версия:

Номер компонента	Тип компонента	Вид отказа	Интенсивность вида отказа	Этап полета	Последствия отказа	Метод обнаружения	Коммен-тарии

Примечание: *Может уточняться для целей и нужд уровня анализа и программы.*

Рис. G2

ПРИЛОЖЕНИЕ H

Сводка видов и последствий отказа

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

H.1 ВВЕДЕНИЕ

Сводка видов и последствий отказа является кратким изложением результатов нескольких Анализов видов и последствий отказа. В ней объединяются виды отказа низкого уровня с одинаковыми последствиями, которые в дальнейшем используются в качестве исходных данных в FTA или в других анализах. Последствия отказа из FMEA рассматриваются в FMES как виды отказа. Последствия на более высоком уровне и вносятся столбец последствий FMES. Одинаковые последствия из FMEA категоризируются как один вид в FMES.

Интенсивность отказов для каждого вида отказа в FMES представляет собой сумму интенсивностей отказов, которые получены для вида отказа в отдельных FMEA. FMES не обязательно должен быть отдельным анализом. Это может быть частью FMEA. FMES помогает упростить FTA (уменьшается число ИЛИ элементов на нижнем уровне) и объединить в одно событие отказы компонентов и отказы оборудования имеющих одинаковые последствия. При вычислении интенсивности отказов следует помнить, что в FMEA рассматриваются единичные отказы, тогда как в FTA рассматриваются и единичные отказы, и комбинации отказов.

Взаимосвязь FMEA и FMES показана на рис. H1.

H.2 НАЗНАЧЕНИЕ

В этом приложении о FMES приводится вспомогательная информация и процедурные инструкции выполняющему анализ для осуществления FMES и демонстрируется полезность составления FMES.

H.3 ПРОЦЕСС FMES

H.3.1 Подготовка к FMES

Подготовка к анализу включает определение требований заказчика, получение требуемых данных FMEA и изучения работы анализируемых системы или объекта. Требования заказчика к FMES важно знать и понимать. Кроме того, должны быть доступны все первичные FMEA и связанные с ними вспомогательные материалы (чертежи, перечни компонентов и т.д.).

H3.2 Выполнение FMES

Выполняющему анализ следует рассмотреть все существующие первичные FMEA и проверить в них согласованность последствий всех отказов (т.е. всегда ли одинаковые последствия отказа описаны одинаковыми формулировками, и различные формулировки последствий отказа всегда применены к различным отказам?). Эта проверку следует выполнить с особой осторожностью, когда выполняется FMES уровня системы (т.е. суммируются последствия видов отказа объекта и видов отказа окружения). Последствия отказа из первичных FMEA вносятся в столбец «Вид отказа» таблицы FMES подобной показанной в качестве примера на рис. H1. Отметим, что форма таблицы FMES может меняться для добавления или исключения специфических исходных данных, если это необходимо для выполнения специфических требований заказчика к FMES, и используемых специфических форм результатов FMEA.

Определяются все виды отказов, имеющие одинаковые последствия отказа и суммируются их индивидуальные интенсивности отказов. Вычисленная интенсивность отказов заносится в столбец «Интенсивность отказов» таблицы FMES. Ссылки на индивидуальные виды отказа в FMEA могут заноситься в столбец «Причина отказа» таблицы FMES. Информация о последствии вида отказа на следующем более высоком уровне, о системах с таким отказом и уместных фазах полета может вноситься в соответствующие столбцы таблицы FMES.

H.4 ДОКУМЕНТАЦИЯ

В каждый отчет FMES необходимо включить следующую информацию:

a. Краткое описание анализируемой системы или объекта, принятый подход к проектированию, включая средства контроля и особые свойства конструкции. (Это следует сопроводить уместными диаграммами, схемными решениями и блок-схемами).

b. Перечень первичных и вторичных функций системы или объекта.

c. Перечень использованных материалов, децимальных номеров и версий анализируемых аппаратных средств и программного обеспечения.

d. Раздел с кратким описанием результатов анализа.

e. Перечень источников данных по интенсивностям отказов.

f. Ссылки на первичные FMEA, использованные для разработки FMES.

Результаты оформляются в виде таблиц FMES при внимательном рассмотрении результатов FMEA. Пример рабочего листа FMES приведен в таблице H1. В отчете следует указать последствия отказа на верхнем уровне и средства обнаружения. Также помещается информация по этапам полета и метод обнаружения.

FMEA схемы X

Вид отказа	Интенсивность отказа	Последствия отказа
Обрыв R5	A	Потеря 5V
КЗ R5	B	Вместо 5V Земля

FMEA схемы Y

Вид отказа	Интенсивность отказа	Последствия отказа
КЗ C5	C	Вместо %V Земля
Обрыв C5	D	



FMES блока

Вид отказа	Интенсивность отказа	Последствия отказа	Возможные причины отказа
Вместо 5V Земля	B+C	Нет командных сигналов	Схема X – КЗ R5
			Схема Y – КЗ C5

Пример связи двух FMEA и FMES
Рис. H1

Таблица H1. Рабочий лист FMES

Сводка видов и последствий отказа		
Самолет	FMES №	Дата:
ATA	Поставщик	Лист из
Система	Номер поставщика	Версия:
Подсистема	Чертеж поставщика	Подготовил:

№	Вид отказа	Интенсивн. отказа	Этап	Последствия для системы	Признаки 1. Пилотам 2. Техникам	Ссылка	1. Причина отказа 2. Замечания	№ Проверки	№ Отказн. сост.

Примечание: *Может уточняться для целей и нужд уровня анализа и программы.*

ПРИЛОЖЕНИЕ I

Зонный анализ безопасности

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

I.1 ВВЕДЕНИЕ

Исторически анализ безопасности системы проводился только на основе системных схемных решений. Такой подход не достаточен для распознавания влияния физического размещения аппаратных средств системы, которое может существенно ослабить независимость объектов. Поэтому был разработан анализ, который позволяет рассмотреть аспекты размещения отдельных систем/объектов и взаимного влияния различных систем/объектов, которые установлены на самолете близко друг к другу. Этот анализ называется Зонным анализом безопасности.

ZSA следует проводить для каждой зоны самолета. Разделение самолета на зоны является задачей, которая выполняется в обеспечение выполнения ЗАБ, а также для оценки операций наземного обслуживания. На рис. I1 приведен пример такого разделения на зоны.

ZSA следует проводить в ходе всего процесса разработки нового самолета или при любом главном изменении существующего самолета. На начальном этапе анализируются чертежи и разрабатываются основные инструктивные материалы для конструирования и размещения. По мере развития проекта в анализе используется информация по макету и затем по самолету. Анализ обычно выполняется разработчиком самолета. Заключения ZSA следует использовать как исходные данные для соответствующих SSA самолета и для дополнения анализов нижнего уровня в SSA. Раздел ZSA в приложении L содержит примеры и контрольные перечни.

Анализ общего режима, Зонный анализ безопасности и Анализ специфического риска составляют Анализ общих причин.

I.2 НАЗНАЧЕНИЕ

Это Приложение содержит информационные и процедурные инструктивные материалы для разработки опытным инженером адекватного состава инструктивных материалов по конструированию и размещению систем и для выполнения ZSA.

I.3 ПРОЦЕСС ZSA

Целью Зонного анализа безопасности является гарантия того, что конструкция и размещение системы отвечают требованиям по безопасности в отношении следующего:

a. Основных стандартов конструирования и размещения.

b. Последствий отказов для самолета.

c. Значения ошибок обслуживания.

d. Проверке того, что конструкция отвечает требованиям по независимости событий из FTA.

В анализе можно использовать выделенные для целей обслуживания зоны самолета. Рис. I2 показывает задачи, которые выполняются в анализе.

Зонный анализ безопасности является, в основном, качественным анализом, включающим в себя три отдельные задачи.

I.3.1 Подготовка инструктивных материалов по конструированию и размещению

Первой задачей, которая не зависит от зон самих по себе, является подготовка инструктивных материалов по конструированию и установке для каждого нового проекта самолета. При последующих модификациях самолета необходимо, насколько возможно, использовать разработанные инструктивные материалы для базовой версии самолета.

Инструктивные материалы будут рассматривать требования уровня самолета и соображения из PSSA. Следует также рассмотреть ошибки обслуживания. Инструктивные материалы могут быть сгруппированы в общие материалы, материалы по конструированию и размещению для отдельных систем, а также специфические материалы по конструированию и размещению для отдельных зон. Все эти типы материалов необходимо подготовить соответствующими ответственными конструкторскими группами и одобрить всеми участвующими организациями.

I.3.2 Изучение размещения в зоне

Второй задачей является изучение каждой зоны самолета для оценки соответствия созданного инструктивным материалам. Результаты оценки следует сохранить для последующих ссылок в этой работе и как пример для будущих работ.

I.3.3 Изучение интерфейса систем/объектов

Третья задача начинается с подготовки перечня систем/объектов в каждой зоне самолета. Этот перечень может основываться, в зависимости от этапа проекта, на данных чертежей, макета и самолета. Для этих систем/объектов следует подготовить перечень видов отказов, которые могут воздействовать на другие близко установленные системы/объекты (виды отказа системы объекта с внешним воздействием). Этот перечень видов отказов может основываться на FMEA и FMES систем/объектов и знаниях об опасностях свойственных системам/объектам.

Далее следует рассмотреть, применяя анализ типа FMEA, виды отказов систем/объектов, внешние последствия отказов и конечные последствия для самолета. Последствия видов отказов с внешними воздействиями следует подтвердить, основываясь на описании системы, PSSA или эквивалентных данных. Описание последствий для самолета следует согласовать с данными относящейся SSA. Следует рассмотреть в SSA последствия отказов системы/объекта с внешним воздействием, как отказы общей причины в различных системах. Одним из методов для выполнения этой задачи является FTA.

Результаты изучения зон на соответствие инструктивным материалам по конструированию и размещению, а также результирующие последствия для самолета отказов систем/объектов с внешним воздействием следует зафиксировать в отчете по ZSA. Любые результаты анализа следует использовать в соответствующих SSA. Любые отклонения от инструктивных материалов следует представить как ожидаемое изменение конструкции. Отклонения должны приводить к изменению конструкции или обоснованию отклонения.

I.4 ДОКУМЕНТАЦИЯ

Следует делать ежедневные записи о выполнении анализа. В дополнение к результатам систематической работы с контрольными перечнями в отчет следует включить следующие данные:

a. Как, когда и кем была сделана оценка (т.е. по макету, по самолету и т.п.).

b. Точное определение любого оборудования, которое указывается как потенциально проблемное.

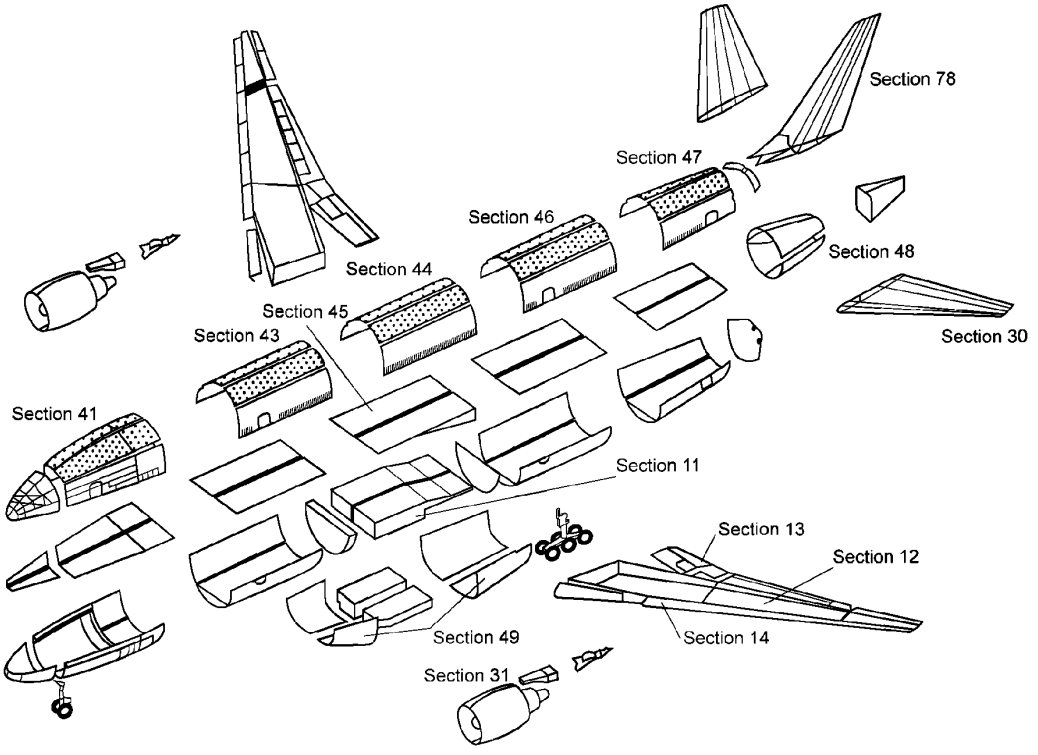
c. Любые отклонения от инструктивных материалов или любые значимые отказы, которые возникают при последующем взаимодействии систем или из-за ошибок обслуживания.

d. Способы разрешения выявленных при анализе проблем (дается ссылка на соответствующие документы).

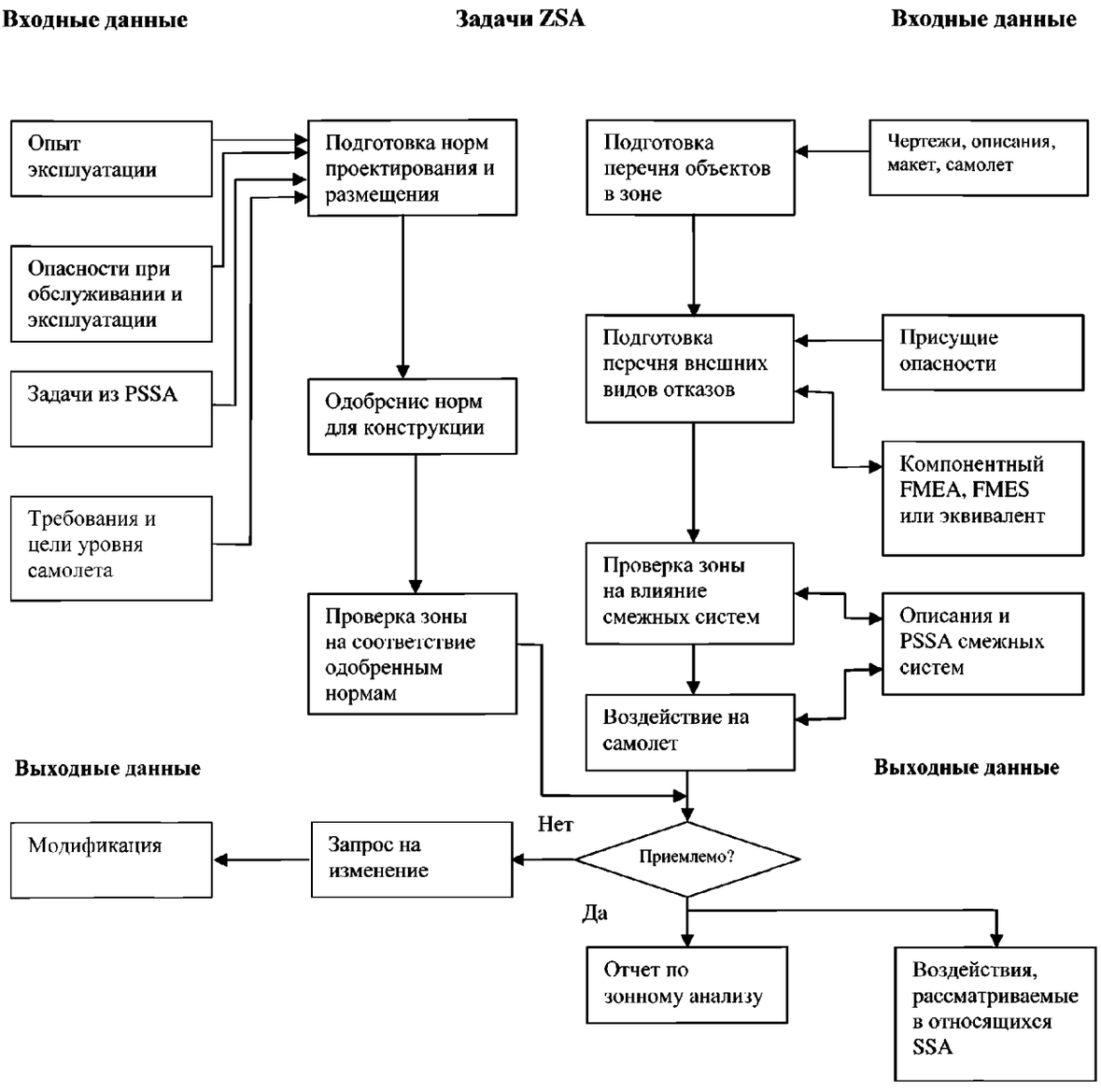
Следует перечислить и проанализировать отказы систем/объектов с внешним воздействием и их последствия. Следует дать ссылки на используемые источники по видам отказов, на обоснования последствий отказов для смежных систем и на соответствующую SSA, в которой рассматривается воздействие на самолет.

Следует обратить внимание ответственных проектных организаций на любые проблемы и отклонения и рассмотреть изменения конструкции.

Предварительные результаты каждого раздела анализа следует направить в соответствующие подразделения проектной организации. Отчет по ZSA следует готовить по ежедневным записям и обобщить приведенные данные. Поскольку этот документ постоянно уточняется и формирует исходные данные для самолетных SSA, его следует в течение цикла проектирования периодически перевыпускать.



Пример зон самолета
Рис. I1



Процесс зонного анализа безопасности
Рис. I2

ПРИЛОЖЕНИЕ J

Анализ специфического риска

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

J1 ВВЕДЕНИЕ

Специфические риски являются событиями или воздействиями, которые находятся вне рассматриваемой системы (систем), но могут нарушать требования к независимости событий. Такие специфические риски могут воздействовать одновременно на несколько зон, тогда как Зонный анализ безопасности ограничивается рассмотрением каждой отдельной зоны. Некоторые из этих рисков могут быть субъектами отдельных требований летной годности (например, нелокализованные разрушения ротора двигателя, разрыв шины и т.д.).

Обычно в состав рисков включают, но не следует этим ограничиваться, следующее:

a. Пожар.

b. Устройства с высокой кинетической энергией:

(1) Двигатель.

(2) ВСУ.

(3) Вентиляторы.

c. Баллоны высокого давления.

d. Разрыв воздухопроводов высокого давления.

e. Утечка из высокотемпературного воздухопровода.

f. Утечка жидкостей (обычно рассматривается как часть Зонного анализа безопасности, но иногда может потребоваться определенная дополнительная оценка).

(1) Топливо.

(2) Гидравлика.

(3) Аккумуляторная кислота.

(4) Вода.

g. Град, лед, снег.

h. Столкновение с птицей.

i. Разрыв шины, отрыв протектора.

j. Поворот колеса.

k. Удар молнии.

l. Электромагнитное поле высокой энергии.

m. Расцепление трансмиссий.

n. Разрушение переборок.

После определения применимых к рассматриваемой конструкции рисков, каждый риск следует рассмотреть отдельно, основываясь на материалах этого приложения. Целью такого анализа является гарантия, что любое влияние на безопасность или конструктивно исключено или показано как приемлемое.

Анализ специфического риска следует выполнять в процессе разработки нового самолета и при любом значительном изменении существующего. В начале анализ может проводиться только по чертежам, но на последующих этапах разработки следует основываться на данных макета, а затем на данных самолета. Обычно анализ выполняет разработчик самолета.

Анализ общего режима, Зонный анализ безопасности и Анализ специфического риска составляют Анализ общих причин.

J.2 НАЗНАЧЕНИЕ

Это приложение содержит информационные и процедурные инструктивные материалы для разработки опытным инженером адекватной модели отказа исследуемого специфического риска, выявления подверженных воздействию зон и проверки последствий этого специфического риска.

J.3 ПРОЦЕСС PRA

Обычно PRA выполняют по каждому отдельному риску. В своей основе анализ является качественным и выполняется следующими действиями:

a. Определяются подробности анализируемого специфического риска (например, разрыв покрышки/колеса).

b. Определяется используемая в анализе модель отказа (например, модель разрыва покрышки и модель разрыва колеса).

c. Перечисляются предъявляемые требования (например, 25.729(f)).

d. Определяются затрагиваемые зоны/области (например, ниша шасси).

e. Определяются затрагиваемые системы/блоки (сопоставление с данными ZSA).

f. Определяются принятые меры предосторожности в конструкции и при размещении (сопоставление с инструкциями конструирования и установки, использованными в ZSA).

g. Проводится проверка последствий специфического риска на затрагиваемые блоки (сопоставление с данными соответствующих FMEA/PSSA).

h. Проводится проверка воздействия специфического риска на самолет вследствие возникновения видов отказов блоков и их комбинаций (сопоставление с соответствующими SSA).

i. Определяются по оценке приемлемости последствий:

   (1) Если приемлемы, то готовятся подтверждающие материалы для сертификации и использования в SSA или другом сертификационном документе.

   (2) Если не приемлемы, то инициируется изменение конструкции.

J.4 ДОКУМЕНТАЦИЯ

Проверка последствий каждого специфического риска документируется в формате, который содержит следующую информацию:

a. Описание анализируемого специфического риска.

b. Блоки, которые затрагиваются специфическим риском.

c. Зоны, в которых размещены блоки.

d. Виды отказа, вызываемые исследуемым специфическим риском.

e. Конечные последствия для самолета и классификация последствий.

Последствия для самолета следует сопоставить с относящимися PSSA/SSA. Более того, следует гарантировать согласованность в PRA и PSSA/SSA данных в столбцах «Влияние на самолет» и «Классификация». Результаты PRA следует включить в относящиеся анализы систем (PSSA/SSA)

В дополнение к указанному выше следует описать в отчете:

a. Любые отклонения от начальных предположений.

b. Способ разрешения выявленных анализом проблем.

Следует привести ссылки на документы с описанием последствий для самолета воздействия внешних угроз.

Любые проблемы, которые открываются в ходе процесса PRA, следует довести до сведения уполномоченной конструкторской организации.

ПРИЛОЖЕНИЕ K

Анализ общего режима

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

K.1 ВВЕДЕНИЕ

Анализ общего режима выполняется в процессе оценки безопасности. CMA является качественным, аналитическим инструментом, который используется для гарантии «хорошего качества» конструкции. При рассмотрении интеграции компонентов в логической последовательности используется опыт проектирования. Эта практика применима на всех уровнях конструкции от уровня объекта до уровня самолета. Анализ включает оценку компонент объекта (CMA уровня компонент/объекта) и того, как они приспособлены к работе в большой системе (CMA уровня системы/самолета).

Этот документ описывает CMA выполняемый на основе исходных данных из FHA и PSSA для обоснования результатов SSA. Учитывая эти предварительные условия, CMA выполняется для проверки того, что И-события в Анализе дерева неисправности, в Анализе логической схемы или в Марковском анализе действительно независимы. Для этого анализируются влияние реализации конструкции, ошибки производства и обслуживания, а также отказы компонентов системы, которые могут обесценить применяемые принципы избыточного проектирования. В общем, CMA способствует проверке того, что принципы независимости применяются, когда это необходимо. Например, следует рассмотреть независимость функций и соответствующих им средств контроля. Точно как же объекты с одинаковыми аппаратными средствами и/или программным обеспечением могут содействовать порождению отказов, которые вызывают неисправную работу многих объектов.

Анализ общего режима, Зонный анализ безопасности и Анализ специфического риска составляют Анализ общих причин.

K.2 НАЗНАЧЕНИЕ

В этом Приложении содержится инструктивный материал по выполнению CMA. Описываемый процесс может быть использован на уровнях объекта, системы или самолета.

K.3 ПРОЦЕСС CMA

Следующие четыре шага суммируют процесс CMA и показаны на рис. K1.

1. Подготовка специфических контрольных перечней (специфические контрольные перечни типов, источников и отказов/ошибок общего режима рассматриваются в разделе K.3.1).
2. Определение требований к CMA (смотри K.3.2).
3. Анализ конструкции для подтверждения соответствия требованиям, определенным на вышеуказанном шаге 2 (смотри K.3.3).
4. Запись результатов первых трех шагов процесса CMA (смотри K.4).

На рис. K1 показаны основные части процесса выполнения CMA на уровне системы/самолета. Процесс может быть приспособлен в обеспечение инструктивного материала для CMA на уровне компонента/объекта.

K.3.1 Контрольный перечень

Основу процесса CMA составляет анализ конструкции и реализации элементов, которые могут обесценить резервирование или независимость функций в изделии. Этот анализ выполняется с использованием контрольных перечней. Как только устанавливается нарушение требуемых резервирования или независимости, необходимо обоснование приемлемости или исключение нарушения.

Следующие общие режимы могут быть примером рассматриваемых в анализе:

a. Ошибки разработки программного обеспечения.
b. Ошибки разработки аппаратных средств.
c. Отказы аппаратных средств.
d. Дефекты производства/ремонта.
e. Стрессовые условия (например, аномальные условия полета, аномальная конфигурация системы).
f. Ошибки размещения.
g. Ошибки в требованиях.
h. Факторы окружающей среды (например, температура, вибрация, влажность).
i. Каскадные отказы.
j. Отказы с общей внешней причиной.

K.3.1.1 Контрольный перечень основных типов, источников и отказов/ошибок общего режима

Имеется много элементов, которые могут быть рассмотрены при выполнении анализа. В таблице K1 приведены примеры основных типов общего режима, примеры источников и отказов/ошибок которые следует рассмотреть. Контрольные перечни для конкретного проекта следует составлять на основе представленных примеров и предшествующего опыта (общих знаний или опыта работ с подобным самолетом). Уровень детализации контрольных перечней зависит от степени сложности или новизны технологии или изучаемой системы.

K.3.2 Определение требований к CMA

Для проведения CMA выполняющему анализ необходимо знать и понимать характеристики рассматриваемой системы в отношении ее работы и размещения. Эти характеристики могут содержаться в следующих документах:

a. План разработки и размещения конструкции.
b. Характеристики оборудования и компонентов.
c. Задачи обслуживания и проверки.
d. Процедуры экипажа.
e. Спецификации систем, оборудования и программного обеспечения.

Кроме этого выполняющему анализ необходимо знать характеристики системы в отношении используемых средств защиты для исключения или минимизации последствий общего режима. К таким средствам относятся следующие:

a. Разнообразие (несхожесть, резервирование и т.д.) и барьеры.
b. Программы испытаний и предупреждающего обслуживания.
c. Уровень контроля и качества проекта.
d. Рассмотрения процедур или спецификаций.
e. Подготовка персонала.
f. Контроль качества.

С указанными выше сведениями о системе выполняющий анализ должен затем определить для исследуемого продукта специфические требования к анализу. Для разработки требований к CMA имеются два описанных ниже различных процесса. Обычно, для подготовки полных специфических требований к анализу должны применяться оба процесса.

K.3.2.1 Требования к CMA на основе FTA, DD или MA

Такие требования составляются при исследовании поддерживающих FHA и PSSA анализов применением указанного ниже процесса.

a. Для каждого аварийного или катастрофического события, зарегистрированного в FHA и/или в PSSA, выделяют каждое И-событие (И-символ дерева неисправности) и определяют соответствующие принципы независимости конструкции.

b. Исследуют И-события, полученные на предыдущем шаге для определения того, какие комбинации отказов должны быть гарантированно независимыми.

c. Регистрируют все найденные таким образом требования к CMA.

К.3.2.2 Другие требования к CMA

Вероятно, имеются требования к CMA, которые не выводятся из FTA, DD или MA. Эти требования происходят из специфических контрольных перечней CMA (смотри К.2.1) и опыта разработки или производства. Такие требования формируются рассмотрением контрольных перечней и сопоставлением с используемыми процессами проектирования, конструирования, выбранными компонентами, процессами производства, процессами размещения и обслуживания.

По мере такого рассмотрения и сопоставления каждое найденное условие, которое может содействовать событию общего режима, приводит к требованию CMA и регистрируется в перечне требований. Примерами требований к CMA, которые не могут быть обнаружены из деревьев неисправности, служат общие отказы в сложных компонентах, воздействия окружающей среды, физическое размещение компонентов и т.д.

К.3.3 Решение по отказу/ошибке общего режима

Для каждого требования к CMA из К.3.2 выполняются следующие действия:

a. Определяют связанные с каждым источником возможные отказы/ошибки общего режима.

b. Анализируют каждые отказ/ошибку общего режима для проверки соответствия критериям независимости.

c. В случае неприемлемости на уровне CMA, предлагают возможные решения и начинают уточнение конструкции.

d. После уточнения конструкции определяют приемлемость результатов.

К.4 ДОКУМЕНТАЦИЯ

Результатом Анализа общего режима является отчет по CMA. Предполагается, что этот отчет включает следующее:

a. Ссылки на использованные в анализе документы, чертежи и вспомогательные материалы.

b. Перечень подготовленных требований к CMA.

c. Описание анализируемых системы/компонента.

d. Обоснование соответствия требованиям к CMA.

e. Определение проблем/интересов, выявленных при анализе, если применимо.

f. Решение по определенным проблемам/интересам (действия уточнения и подтверждение приемлемости).

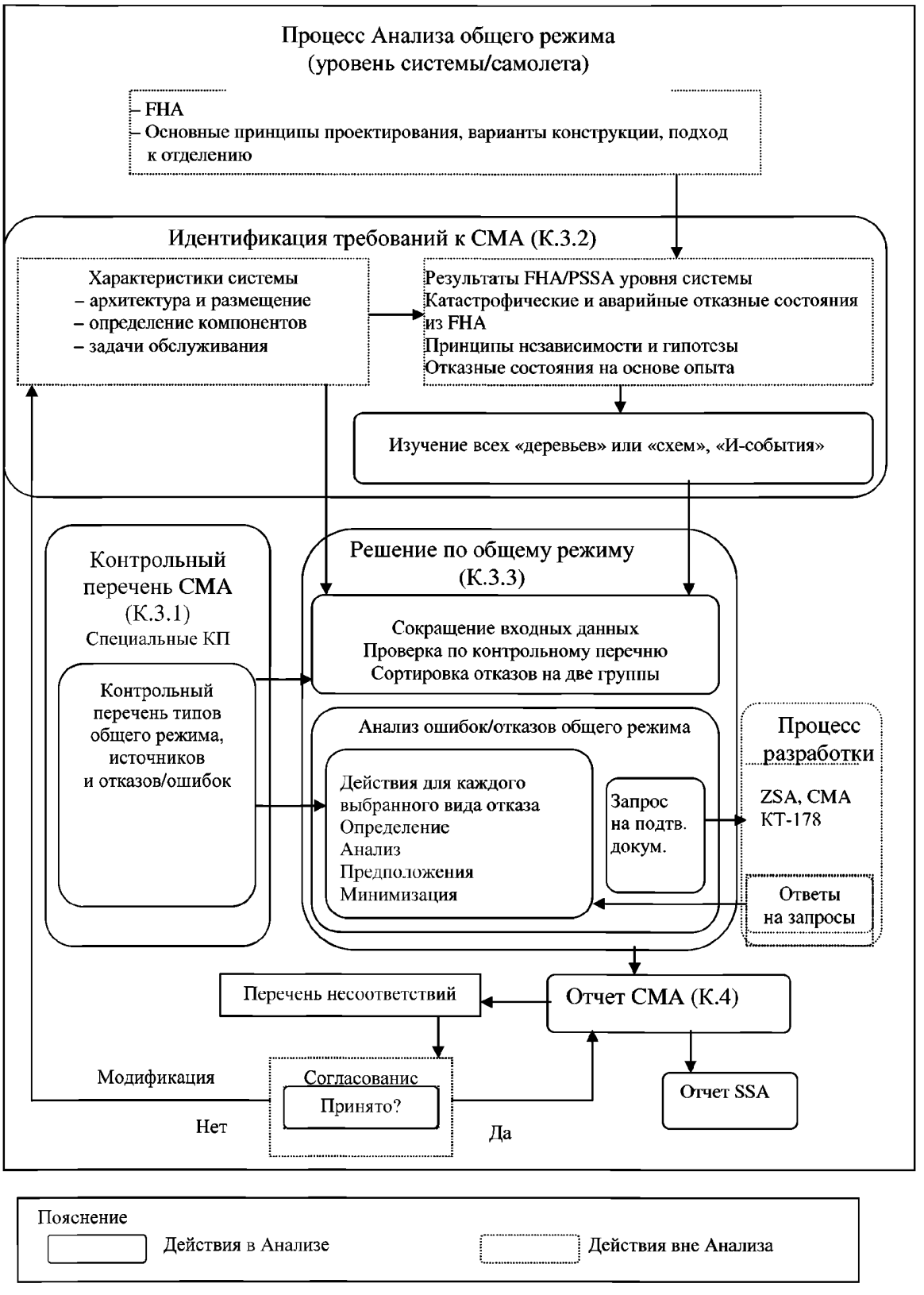
g. Заключение/результат CMA.

К.4.1 Связь с FHA, PSSA и SSA

Анализ общего режима использует результаты FHA/PSSA такие, как перечень катастрофических отказных состояний, предполагаемые критерии независимости и любые директивы для проведения CMA. Сводка результатов анализа включается в SSA. Любые оставшиеся общие режимы следует включить в относящиеся отчеты по FTA, DD или MA.

К.4.2 Связь с ZSA и PRA

Зонный анализ безопасности и Анализ специфического риска не являются специфической частью Анализа общего режима. Однако нельзя игнорировать возможные последствия общего режима от таких источников. Когда ZSA или PRA выявляют возможные связи с общим режимом, то выполняющему CMA следует, если возможно, гарантировать, что выявленные в них проблемы закрыты.



Процесс CMA
Рис. K1

Таблица К1

Пример контрольного перечня основных типов общего режима, источников и отказов/ошибок

Типы общего режима	Подтипы общих режимов	Примеры источников общего режима	Примеры отказов/ошибок общего режима
Концепция и конструкция	Архитектура конструкции	Описание общего выпуска	Отказ общего выпуска
		Общие внешние источники (вентиляция, электрическая мощность)	Отказ общих источников (вентиляция, электрическая мощность)
		Защиты оборудования	Отказ разработчика прогнозировать событие
		Эксплуатационные характеристики (нормальный бегущий, режим холостого хода ...)	
		Другое	
	Технология, материалы, тип оборудования	Новая/чувствительная технология	Ошибка общего проекта
		Тип компонента (размер, материал)	Ошибка аппаратных средств
		Общее программное обеспечение	Ошибка программного обеспечения
		Использование компонента	
		Внутренние состояния (T^0, ранги ...)	Употребление вне эксплуатационных рангов (Т.Р.).
		Начальные состояния	
		Другое	
	Спецификации	Источник спецификации	Ошибка источника (человеческая), недостаток специальной защиты в дизайне оборудования
		Та же самая спецификация	Поврежденная спецификация
		Другое	
Производство	Производитель	Общий производитель	Общая ошибка из-за производителя, ошибка из-за неадекватно обученного персонала
		Другое	
	Процедуры	Та же самая процедура	Некорректная процедура
		Другое	
	Процесс	Тот же самый процесс	Некорректный процесс, неадекватное управление производством, неадекватная инспекция, неадекватное тестирование
		Другое	
Установка/ интеграция и испытание	Сборка	Общий механик	Ошибка установки из-за механика
		Другое	
	Процедуры	Фаза инсталляции	Общая ошибка на фазе
		Другое	
	Расположение	Та же самая зона	Локальный отказ или случай
		Другое	
	Направление	То же направление	Локальный случай

Типы общего режима	Подтипы общих режимов	Примеры источников общего режима	Примеры отказов/ошибок общего режима
		Другое	
Действие	Персонал	Общий персонал	Ошибка из-за неадекватно обученного персонала, перенапряженный или заблокированный оператор
		Другое	
	Процедуры	Та же самая процедура	Ошибочные рабочие процедуры, неправильный диагноз (следующая неправильная процедура). Упущение действия, некорректные или неадекватные полномочия действия
		Другое	
Обслуживание	Персонал	Общий персонал	Ошибка из-за неадекватно обученного персонала, некорректного действия человека.
		Другое	
	Процедуры	Та же самая процедура	Отказ следует за процедурами ремонта, неисправная процедура ремонта, недостаток процедур ремонта ...
		Другое	
Испытание	Персонал	Общий персонал	Ошибка из-за неадекватно обученного персонала, некорректного действия человека
		Другое	
	Процедуры	Та же самая процедура	Неисправная тестовая процедура
		Другое	
Калибровка	Штат	Общий штат	Ошибка из-за неадекватно обученного персонала ...
		Инструменты калибровки	Регулирование неадекватных инструментов
		Другое	
	Процедуры	Та же самая процедура	Отказ следует за процедурами калибровки, неисправная процедура калибровки, недостаток процедур калибровки
		Другое	
Экологический	Механический и тепловой	Температура	Огонь, молния, сварка, и т.д., ошибки системы охлаждения, электрические замкнутые цепи ...
		Песок	Бортовая пыль, фрагменты металла, произведенные движущимися частицами с неадекватными допусками ...
		Воздействие	Трубка канала, водный молоток, ракеты, структурный отказ ...
		Вибрация	Машины в движении, землетрясение ...

Типы общего режима	Подтипы общих режимов	Примеры источников общего режима	Примеры отказов/ошибок общего режима
		Давление	Взрыв, изменения вне системы допуска (сверхскоростной насос, поток, блокировка) ...
		Влажность	Поломки паровой трубы ...
		Влажность	Конденсация, разрыв трубы, дождевая вода ...
		Напряжение	Тепловое напряжение сварки разнородных металлов, тепловое напряжение ...
		Другое	
	Электрический и излучение	Электромагнитный	Сварочное оборудование, вращающие электрические машины, молния, ...
		Излучение	Гамма - излучение, излучение заряженной частицы,...
		Проведение среды	Влажность, проводимые газы,...
		Вне допуска	Напряжение скачка мощности, замкнутая схема, текущий скачок напряжения, ...
		Другое	
	Химический	Коррозия (кислота)	Утечка кислоты, использованной в средстве для удаления ржавчины и очищения, ...
		Коррозия (окисление)	Влажность вокруг металлов
	Разное	Другие химические реакции	Гальваническая коррозия, комплекс взаимодействий контакта с топливом, воды, окисного топлива, ...
		Биологический	Ядовитые газы, живые причины (мидии в теплообменнике теплоты), ...
		Другое	

ПРИЛОЖЕНИЕ L

Сопровождающий пример процесса оценки безопасности

Примечание: *Основной документ содержит информацию со ссылками в контексте на данное приложение. Это приложение должно использоваться вместе с основным документом и его другими приложениями.*

L.1 ВВЕДЕНИЕ

L.1.1 Область охвата:

В данном приложении подробно описан пример оценки безопасности для воображаемой конструкции самолета. Для того чтобы дать ясную картину, функция была разбита на одиночный элемент одной системы. Была выбрана функция, обладающая достаточной сложностью для обеспечения использования всех методологий, но в то же время достаточно простая для представления ясной картины движения через них. Был проведен анализ функции, системы и компонента при помощи всех методов и инструментов, описанных в оставшейся части этого документа. Использовался каждый метод для демонстрации его приложения. На практике для определения потенциальных причин функциональных неисправностей можно выбрать, например, FTA, DD или MA. Тем не менее, здесь использовались все три метода для того, чтобы дать читателю понимание их сходства и различия. Используемые здесь методологии являются примером одностороннего использования принципов, определенных в документе. Для завершения документации могут использоваться другие форматы при том условии, что выполняются принципы, описанные в тексте данного документа.

Данный документ содержит ссылки на все документы, которые компания может использовать для того, чтобы самой обеспечить безопасность ее изделий. Некоторые из этих документов подготовлены для органов государственного регулирования с целью сертификации (например, FHA системы тормозов колес). Другие документы являются внутренними документами компании, и их сертификация не требуется (например, документ с конструктивными требованиями для S-18). Никаких предпосылок не сделано для того, чтобы эти документы были представлены на рассмотрение в органы государственного регулирования, и ничего не должно подразумеваться. Безопасность и сертификация не являются терминами-синонимами. Мы пытаемся показать здесь процесс оценки безопасности, включая такие процессы, которые находятся вне области действия требований к сертификации.

L.1.2 Перечень акронимов для примера в Приложении L:

ACCU	Аккумулятор
ALT	Переменный
APU	Вспомогательная силовая установка
AS	Противоскольжение
B	Голубая гидравлическая система
BSCU	Блок управления тормозной системы
C	Конденсатор
CMD	Команда
COMP	Расчет
CSMG	Двигатель-генератор с постоянной скоростью вращения
ECS	Система контроля влияния окружающей среды
ELEC	Электрический
EMI	Электромагнитные помехи
HIRF	Излучаемые поля высокой интенсивности

HYD	Гидравлический
IC	Интегральная схема
I/O	Вход/выход
CAT IIIb	Всепогодная система посадки категории 3b
CPU	Центральный процессорный блок
F.R.	Частота отказов
G	Зеленая гидравлическая система
L или LH	Слева или левосторонний
LRU	Сменный блок
MLG	Основное шасси
MON	Монитор
MT	Задача периодического технического обслуживания
NLG	Носовое шасси
NORM	Нормальный
PCU	Блок регулирования мощности
POS	Положение
P/S	Электропитание
PTU	Блок передачи мощности
PWM	Модулятор длительности импульсов
PWR	Мощность
R или RH	Правый или правосторонний
R	Резистор
REF	Ссылка
RTO	Прекращенный взлет
STBY	Резервный
SYS	Система
VDC	Напряжение постоянного тока в вольтах
V1	Скорость, начиная с которой самолет не может быть безопасно остановлен на оставшейся части взлетно-посадочной полосы
WBS	Система торможения колес

L.1.3 Общая структура:

Выбранная функция анализируется при помощи методов, описанных в приложениях. Порядок представленных методов является номинальным ходом их разработки на этапе проектирования. Тем не менее, в конце данного примера показана работа CCA, тогда как в последовательности технологических операций она происходит в течение процесса (см. рис. 1, 2 и 3 основной части документа).

Ниже представлена структура примера.

a. FHA самолета

   (1) Предварительный FTA самолета

b. FHA системы тормоза колес

c. PSSA

(1) WBS FTA, DD, MA

(2) BSCU FTA, DD, MA

d. SSA

(1) BSCU FMEA

(2) BSCU FMES

(3) BSCU CMA

(4) BSCU FTA, DD, MA

(5) WBS FMES

(6) WBS FTA, DD, MA

(7) Перекрестный контроль WBS

e. CCA (BSCU CMA адресован по разделу SSA для улучшения непрерывности данного примера)

(1) ZSA (зона ниши шасси)

(2) PRA (разрыв шины)

(3) WBS CMA

В начале каждого нового раздела вверху страницы необходимо прочесть текст колонтитула, который будет изменяться для описания данного конкретного раздела. При этом читатель всегда может точно сказать, на какой стадии процесса оценки безопасности он находится. Например: Приложение L [FHA самолета] или Приложение L [PSSA СТК].

Каждый раздел данного примера написан в виде отдельного представляемого документа. Несмотря на то, что для органов сертификации приемлемыми являются различные форматы, в наших примерах будут использованы следующие форматы:

1.0. Введение

2.0. Ссылки

3.0. Описание функции/системы

4.0. Анализ

4.1. (Как требуется для поддержки описания анализа)

4.2. (Как требуется для поддержки описания анализа)

4.2.1. (Как требуется для поддержки описания анализа)

4.2.2. (Как требуется для поддержки описания анализа)

5.0. Заключение

Редакционные примечания приведены курсивом. Там, где это необходимо, читатель будет направлен к соответствующему приложению для дальнейших инструкций по используемому процессу.

L.1.4 Описание функции примера:

Анализируемой функцией самолета является: «Торможение самолета на земле (остановка на взлетно-посадочной полосе). Данный пример концентрируется на тормозной системе самолета, подробная информация о которой представляется в течение всего примера примерно так, как если бы это была реальная ситуация в жизни.

L.1.5 Перечень рисунков для Приложения L:

Рис 4.1-1 (FHA самолета) Функции самолета

Рис. 4.6-1 (FHA самолета) Предварительное дерево неисправности самолета

Рис. 3.0-1 (PSSA – Система торможения колес) Предварительная схема системы торможения колес

Рис. 4.2.1-1 (PSSA – Система торможения колес – FTA) Дерево неисправности (исходное) несигнализируемой потери торможения всех колес

Рис. 4.2.1-2 (PSSA – Система торможения колес – FTA) Дерево неисправности (редакция A) несигнализируемой потери торможения всех колес

Рис. 4.2.1-3 (PSSA – Система торможения колес – FTA) Дерево неисправности (редакция B) несигнализируемой потери торможения всех колес

Рис. 4.2.2-1 (PSSA – Система торможения колес – DD) Логическая схема несигнализируемой потери торможения всех колес (исходная)

Рис. 4.2.2-2 (PSSA – Система торможения колес – DD) Логическая схема несигнализируемой потери торможения всех колес (редакция A)

Рис. 4.2.2-3 (PSSA – Система торможения колес – DD) Логическая схема зависимости несигнализиуемой потери торможения всех колес (редакция B)

Рис. 4.2.3-1 (PSSA – Система торможения колес – MA) Несигнализируемая потеря всей системы торможения колес (исходная)

Рис. 4.2.3-2 (PSSA – Система торможения колес – MA) Несигнализируемая потеря всей системы торможения колес (редакция A)

Рис. 4.2.3-3 (PSSA – Система торможения колес – MA) Несигнализируемая потеря всей системы торможения колес (редакция B)

Рис. 3.0-1 (PSSA BSCU) Предлагаемая архитектура BSCU

Рис. 4.2.1-1 (PSSA BSCU – FTA) Дерево неисправностей события «Отказ BSCU вызывает потерю команд на торможение» (лист 1 из 2)

Рис. 4.2.1-1 (PSSA BSCU – FTA) Дерево неисправностей события «Отказ BSCU вызывает потерю команд на торможение» (лист 2 из 2)

Рис. 4.2.1-2 (PSSA BSCU – FTA) Дерево неисправностей события «BSCU подает команды на торможение при отсутствии входного сигнала на торможение и вызывает непреднамеренное торможение» (лист 1 из 3)

Рис. 4.2.1-2 (PSSA BSCU – FTA) Дерево неисправностей события «BSCU подает команды на торможение при отсутствии входного сигнала на торможение и вызывает непреднамеренное торможение» (лист 2 из 3)

Рис. 4.2.1-2 (PSSA BSCU – FTA) Дерево неисправностей события «BSCU подает команды на торможение при отсутствии входного сигнала на торможение и вызывает непреднамеренное торможение» (лист 3 из 3)

Рис. 4.2.2-1 (PSSA BSCU – DD) Логическая схема события «Отказ BSCU вызывает потерю команд на торможение»

Рис. 4.2.2-2 (PSSA BSCU – DD) Логическая схема события «BSCU подает команды на торможение при отсутствии входного сигнала тормоза и вызывает непреднамеренное торможение»

Рис. 4.2.3-1 (PSSA BSCU – MA) MA Отказ BSCU вызывает потерю команд на торможение

Рис. 4.2.3-2 (PSSA BSCU – MA) MA «Выявляемый отказ BSCU вызывает непреднамеренное торможение»

Рис. 4.2.3-3 (PSSA BSCU – MA)) MA «Непреднамеренное торможение из-за неисправности системы BSCU 1»

Рис. 4.2.3-4 (PSSA BSCU – MA) MA «Непреднамеренное торможение из-за неисправности системы BSCU 2 и неисправности системы переключения»

Рис. 3.0-1 (SSA BSCU – FMEA) Физическое исполнение BSCU

Рис. 3.0-2 (SSA BSCU – FMEA) Блок-схема электропитания

Рис. 3.0-3 (SSA BSCU – FMEA) Схема монитора электропитания

Рис. 3.0-1 (SSA BSCU – CMA) Схема архитектуры BSCU

Рис. 4.3-1 (SSA BSCU – CMA) Физическое исполнение BSCU

Рис. 5.1-1 (SSA BSCU – FTA) Дерево неисправностей события «Отказ BSCU вызывает потерю команд на торможение» (лист 1 из 2)

Рис. 5.1-1 (SSA BSCU – FTA) Дерево неисправностей события «Отказ BSCU вызывает потерю команд на торможение» (лист 2 из 2)

Рис. 5.1-2 (SSA BSCU – FTA) Дерево неисправностей события «BSCU подает команды на торможение при отсутствии входного сигнала тормоза и вызывает непреднамеренное торможение (лист 1 из 3)

Рис. 5.1-2 (SSA BSCU – FTA) Дерево неисправностей события «BSCU подает команды на торможение при отсутствии входного сигнала тормоза и вызывает непреднамеренное торможение» (лист 2 из 3)

Рис. 5.1-2 (SSA BSCU – FTA) Дерево неисправностей события «BSCU подает команды на торможение при отсутствии входного сигнала тормоза и вызывает непреднамеренное торможение (лист 3 из 3)

Рис. 5.2-1 (SSA BSCU – DD) Отказ BSCU вызывает потерю команд на торможение

Рис. 5.2-2 (SSA BSCU – DD) BSCU подает команды на торможение при отсутствии входного сигнала тормоза и вызывает непреднамеренное торможение

Рис. 5.3-1 (SSA BSCU – MA) Отказ BSCU вызывает потерю команды на торможение

Рис. 5.3-2 (SSA BSCU – MA) Непредвиденное торможение вследствие отказа обеих систем и их мониторов

Рис. 5.3-3 (SSA BSCU – MA) Непредвиденное торможение вследствие отказа системы 1 BSCU (для ясности ремонт компонентов не показан)

Рис. 5.3-4 (SSA BSCU – MA) Непреднамеренное торможение вследствие отказа системы 2 BSCU и отказа механизма переключения (для ясности ремонт компонентов не показан)

Рис. 5.2-1 (SSA Система торможения колес – FTA) Дерево неисправности потери торможения всех колес (лист 1 из 3)

Рис. 5.2-1 (SSA Система торможения колес – FTA) Дерево неисправности потери торможения всех колес (лист 2 из 3)

Рис. 5.2-1 (SSA Система торможения колес – FTA) Дерево неисправности потери торможения всех колес (лист 3 из 3)

Рис. 5.3-1 (SSA Система торможения колес – DD) Потеря торможения всех колес

Рис. 5.4-1 (SSA Система торможения колес – MA) Потеря торможения всех колес

Рис. 4.2.1.2.2-1 (CCA – ZSA) Установка гидравлических трубопроводов в шпангоуте C46/47

Рис. 4.2.1.2.2-2 (CCA – ZSA) Компоненты зеленой гидравлической системы

Рис. 4.2.1.3.4-1 (CCA – ZSA) Вентиляция отсека основного шасси (MLG)
Рис. 3.0-1 (CCA – PRA) Носовое и основное шасси самолета S18
Рис. 4.3-1 (CCA – PRA) Отсек основного шасси
Рис. 4.3-2 (CCA – PRA) Вид сбоку зоны разрыва шины
Рис. 4.3-3 (CCA – PRA) Зона разрыва шины – вид спереди
Рис. 4.3-4 (CCA – PRA) Зона разрыва шины – вид сверху
Рис. 4.4.1-1 (CCA – PRA) Поверхности управления полетом самолета S18

ОЦЕНКА ФУНКЦИОНАЛЬНОЙ ОПАСНОСТИ ДЛЯ САМОЛЕТА S18

1.0 ВВЕДЕНИЕ

Данный анализ включает в себя оценку функциональной опасности функций самолета S18. Это фиктивный самолет, который был создан для данного документа. Рассмотрена работа всех систем, используемых для выполнения функций самолета.

(Примечание редактора: В таблице перекрестных ссылок, представленной ниже, дана связь каждого параграфа примера с соответствующим параграфом приложения FHA).

№ параграфа FHA самолета	№ параграфа Приложения A
4.1	A.3.1
4.2	A.3.2
4.3	A.3.3
4.4	A.3.4, A.3.6
4.5	A.3.7
4.6	A.4

2.0 ЛИТЕРАТУРА

1) Документ с конструктивными требованиями к самолету S18
2) АП 25.1 309
3) Р4754 «Руководство по сертификации высоко интегрированных или сложных авиационных систем»
4) Р4761 «Руководство по методам оценки безопасности бортового оборудования самолетов гражданской авиации»

3.0 АННОТАЦИЯ

Самолет S18 представляет собой пассажирский самолет с четырьмя двигателями, разработанный для перевозки от 300 до 350 пассажиров на расстояние до 5000 морских миль со скоростью 0,86 М. Средняя длительность полета составляет 5 часов.

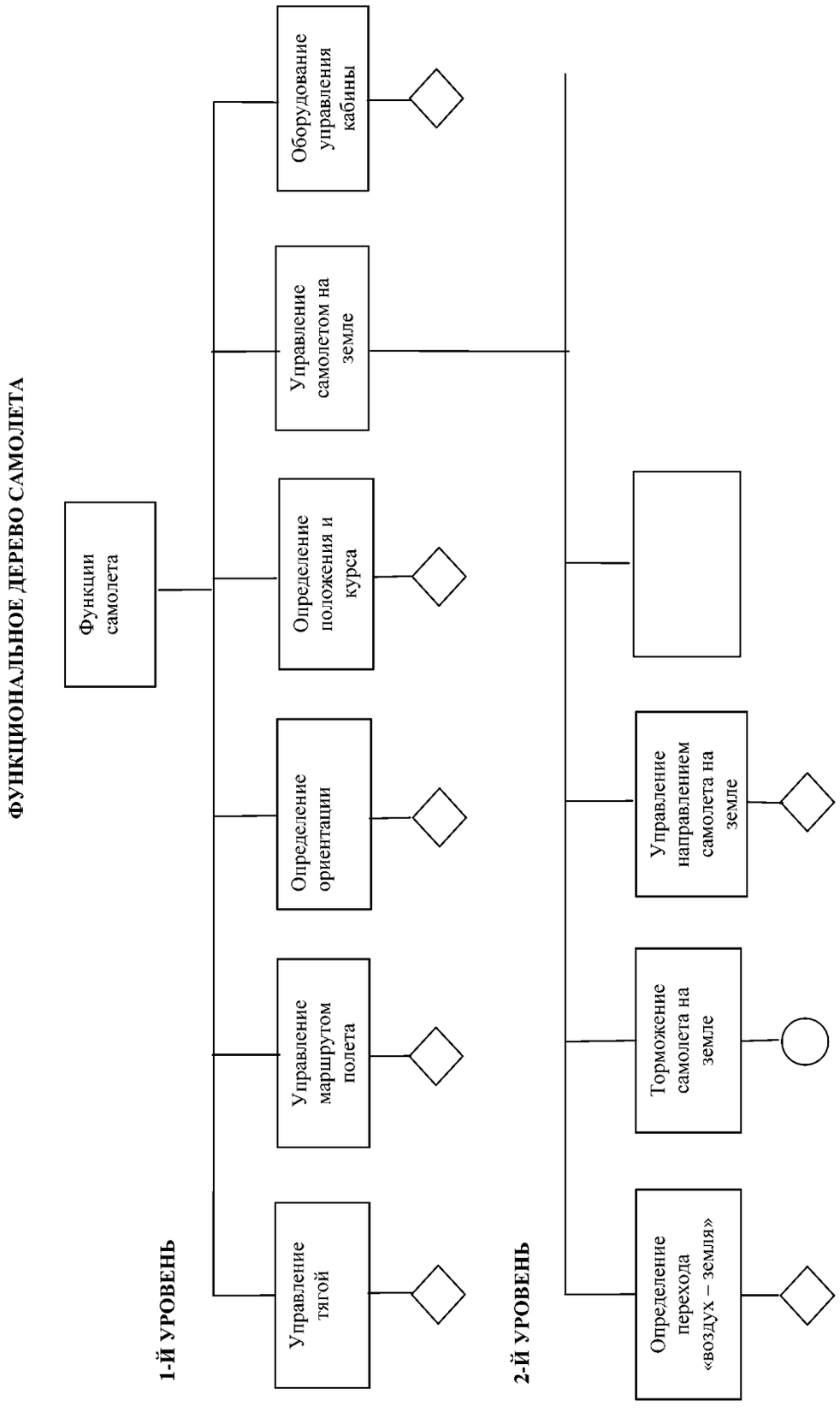
(Примечание редактора: В этот параграф должны ~~бы~~ быть включены и другие основные особенности, определяющие этот самолет, но для краткости они не описываются. Эти особенности в основном обусловлены рыночными и деловыми решениями, принятыми во время начальных маркетинговых мероприятий).

4.0 РЕЗУЛЬТАТЫ ОЦЕНКИ ФУНКЦИОНАЛЬНОЙ ОПАСНОСТИ САМОЛЕТА

4.1 Идентифицированные функции

На рис. 4.1-1 изображены функции самолета в формате простой ярусной иерархии.

(Примечание редактора: Функция «управления самолетом на земле» в данном примере разложена. По такому разложению в примере FHA самолета рассматривается функция «торможения самолета на земле». Анализируемая функция определена в столбце (1) формы примера FHA, показанной в Таблице 4.1.1).



(FHA самолета) Функции самолета
Рис. 4.1-1

4.2 Идентифицированные отказные состояния

Для функции «торможения самолета на земле» определен следующий набор отказных состояний и допущений для оценки.

4.2.1 Функциональные отказные состояния

a. Потеря всех возможностей торможения

b. Уменьшенная способность торможения

c. Непредвиденное торможение

d. Потеря всех функций автоматической остановки

e. Асимметричное торможение

4.2.2 Окружающие условия и аварийные конфигурации

a. Условия взлетно-посадочной полосы (мокрая, обледенелая, и т.п.).

b. Длина взлетно-посадочной полосы

c. Попутный/поперечный ветер

d. Отключение двигателя

e. Потеря гидравлической системы

f. Потеря электрической системы

4.2.3 Применяемые фазы

a. Руление на земле (руление)

b. Взлет до отрыва (взлет)

c. Пробег после посадки (посадка)

d. Прерванный взлет (RTO)

4.2.4 Интерфейсные функции

a. Определение состояния земля/воздух

b. Предупреждение экипажа (аварийные, предупреждающие, уведомляющие)

В столбцах (2) и (3) таблицы 4.1-1 показана та часть формы FHA, которая содержит сформулированные отказные состояния для данной функции.

4.3 Влияние отказного состояния на самолет, экипаж и пассажиров

Для каждого отказного состояния в столбце (4) таблицы 4.1-1 показаны его влияние на самолет и экипаж.

4.4 Классификация/обоснование влияния условий отказа на самолет и экипаж

Для каждого условия отказа его классификация определена в столбцах (5) и (6) табл. 4.1-1.

4.5 План проверки целей безопасности

Для каждого условия отказа план проверки целей безопасности определен в столбце (7) таблицы 4.1-1. В этом столбце перечислены ссылки на требования, деревья неисправностей, анализы и/или испытания.

Таблица 4.1-1 FHA самолета (*частичная – адресована только "торможению самолета на земле")*

Функция	Отказное состояние	Фаза	Влияние отказного состояния на самолет/ экипаж	Классификация	Ссылка на вспомогательные материалы	Обоснование
Торможение самолета на земле	Потеря способности торможения	Посадка/ RTO/ руление	См. ниже			
	a. Несигнализируемая потеря способности торможения	Посадка/ RTO	Экипаж не в состоянии затормозить самолет, что приведет к выбегу за пределы ВПП с высокой скоростью.	Катастрофическое		Дерево отказов самолета S18
	b. Сигнализируемая потеря способности торможения	Посадка	Экипаж выбирает более пригодный аэропорт, извещает наземную аварийную службы и готовит пассажиров к посадке с выбегом за пределы ВПП.	Аварийное	Процедуры аварийной посадки в случае потери способности остановки	Дерево отказов самолета S18
	c. Несигнализируемая потеря способности торможения	Руление	Экипаж не в состоянии остановить самолет на рулежной дорожке, что приводит в результате к контакту на низкой скорости с терминалом, самолетом или транспортными средствами.	Сложное		
	d. Сигнализируемая потеря способности торможения	Руление	Экипаж выруливает самолет от препятствий и вызывает буксир или передвижные лестницы.	Нет влияния на безопасность		
	Непреднамеренное торможение после V1	Взлет	Экипаж не может осуществить взлет вследствие срабатывания тормозов во время высокой тяги, что приводит к выбегу за пределы ВПП с высокой скоростью.	Катастрофическое		Дерево отказов самолета S18
	Частичная потеря способности торможения	Посадка/ RTO	См. ниже			
	a. Несигнализируемая частичная потеря способности торможения	Посадка/ RTO	Экипаж не в состоянии полностью затормозить самолет до конца ВПП, что приведет к потенциальному выбегу за пределы ВПП.	Аварийное		Дерево отказов самолета S18
	b. Сигнализируемая частичная потеря способности торможения	Посадка	Экипаж выбирает более пригодный аэропорт, извещает наземную аварийную службы и готовит пассажиров к посадке с выбегом за пределы ВПП.	Сложное		

Функция	Отказное состояние	Фаза	Влияние отказного состояния на самолет/ экипаж	Классификация	Ссылка на вспомогательные материалы	Обоснование
	c. Несигнализируемая частичная потеря способ-ности торможения	Руление	Экипаж не в состоянии остановить самолет должным образом перед препятствием, что приведет к соударению на низкой скорости.	УУП		
	d. Сигнализируемая частичная потеря способности торможения	Руление	Экипаж выруливает самолет от препятствий и вызывает буксир или передвижные лестницы.	Нет влияния на безопасность		
	Потеря автоматической способности остановки	Посадка/ RTO	См. ниже			
	a. Несигнализируемая потеря автоматической способности остановки	Посадка/ RTO	Экипаж приводит в действие функции автоматической остановки для посадки/RTO. При посадке/RTO функции автоматической остановки не выполняются. Экипаж осознает ситуацию и вручную осуществляет остановку. Время реакции экипажа может привес-ти к потенциальному выбегу за пределы ВПП.	Сложное		Дерево отказов самолета S18
	b. Сигнализируемая потеря автоматической способности остановки	Посадка/ RTO	Экипаж вручную осуществляет остановку при посадке или RTO	Нет влияния на безопасность		
	Асимметричное торможение	Посадка/ RTO	См. ниже			
	a. Несигнализируемое асимметричное торможение	Посадка/ RTO	Экипаж не подготовлен к асимметричному торможению и реагирует слишком поздно для обеспечения контроля направления движения, что в результате приводит к сходу самолета с ВПП.	Сложное		
	b. Сигнализируемое асимметричное торможение	Посадка	Экипаж подготовлен к асимметричному торможению и противодействует при помощи соответствующего положения руля и носового колеса.	УУП		
	c. Потеря автоматической способности остановки	Руление	Самолет немного отклоняется от заданного курса	Нет влияния на безопасность		

4.6 Выводы FHA самолета

(Примечание редактора: FHA на уровне самолета и соответствующее дерево неисправностей обеспечивают предварительный комплект условий отказов и соответствующих требований для рассмотрения на системном уровне. Эти условия отказов и требования будут обоснованы и обновлены при FHA на уровне системы).

На основе целей безопасности FHA на фазе эскизного проектирования были приняты архитектурные решения. Эти архитектурные решения составляют основу предварительного дерева неисправностей, представленного на рис. 4.6-1.

Требование 1E-9 на полетный час для «несигнализируемой потери способности торможения» получено из классификации условия отказа как катастрофического. Данное требование эквивалентно требованию 5E-9 на полет, поскольку средняя продолжительность полета составляет 5 часов.

Требование 5E-7 на полет для «необъявленной потери всех аэродинамических тормозов на загрязненной взлетно-посадочной полосе» и для «несигнализируемой потери торможения всех колес» получено из классификации условия отказа как опасного (эта классификация эквивалентна 1E-7 на час полета). Эти классификации основаны на знаниях и опыте по данным условиям системных отказов. Данные требования дают в результате требуемую вероятность 1E-6 на полет (т.е. 2x5E-7 на час полета) на следующем более высоком уровне «несигнализируемой потери эффективного торможения колес».

Как показано на рис. 4.6-1, назначение указанных выше требований обеспечивает, чтобы уровень для «несигнализируемой потери реверсоров тяги» должен быть установлен на величину 5E-3 на полет. Это равно 5E-9, деленному на 1E-6.

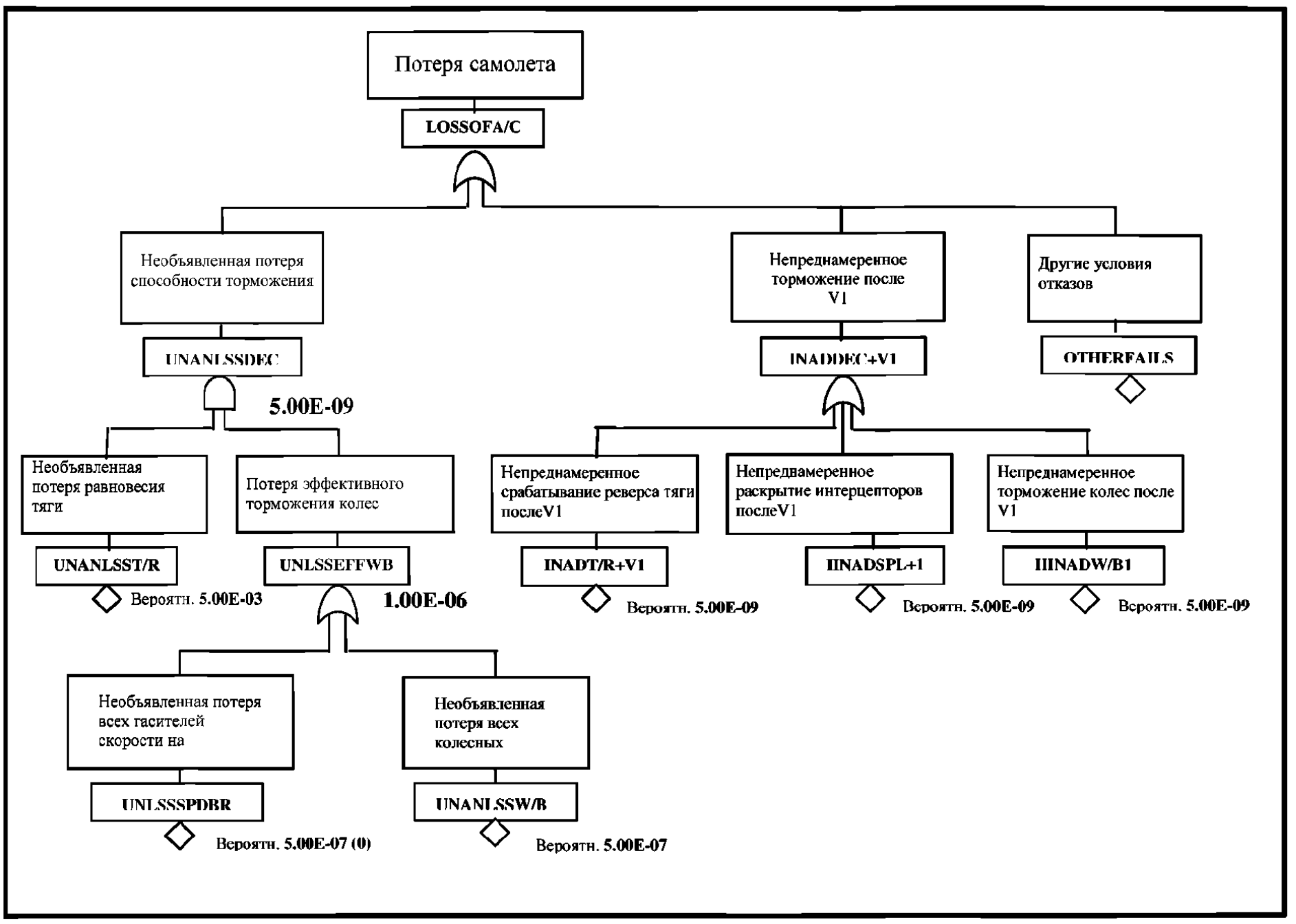
На рис. 4.6-1 также показано ответвление дерева неисправностей, связанное с непреднамеренным торможением после V1. Каждое из условий отказа классифицируется как катастрофическое и должно отвечать требованию 1E-9 на час полета или 5E-9 на полет.

Тем не менее, поскольку эти условия являются катастрофическими только во время специальной фазы полета, то их требования «на час» должны быть разложены на множители. Коэффициент равен средней продолжительности полета 5 часов, деленной на время риска (15 секунд будет представлять собой завышенную оценку времени от V1 до отрыва).

Следовательно, требование к частоте отказов в час для каждого равно 1E-9/отказ час * 5 отказов в час/отказ * 1 отказ/0,25 мин * 60 мин/1 ч = 1,2E-6/ч.

Требования к вероятности после преобразования их в требования к частоте отказов будут иметь следующий вид.

a. Непреднамеренный реверс тяги после V_1	1,2E-6 в час
b. Непреднамеренное раскрытие интерцептора после V_1	1,2E-6 в час
c. Непреднамеренное торможение колеса после V_1	1,2E-6 в час



(FHA самолета) Предварительное дерево неисправности самолета
Рис. 4.6-1

ОЦЕНКА ФУНКЦИОНАЛЬНОЙ ОПАСНОСТИ СИСТЕМЫ ТОРМОЖЕНИЯ КОЛЕС

1.0 ВВЕДЕНИЕ

Данный анализ включает в себя оценку функциональной опасности для системы торможения колес самолета S18. Система торможения колес должна отвечать двум целям проектирования на основе архитектурных конструкционных решений, принятых вместе с разработкой FHA на уровне самолета. Эти цели – остановка вращения колес на земле и остановка вращения колес в нише шасси.

(Примечание редактора: В данном примере анализируется функция остановки вращения колес на земле, поскольку она соответствует функции торможения самолета на земле).

(Примечание редактора: В следующей таблице перекрестных ссылок представлена связь каждого параграфа примера с применяемым параграфом приложения FHA).

№ параграфа FHA системы	№ параграфа Приложения A
4.1	A.3.1
4.2	A.3.2
4.3	A.3.3
4.4	A.3.4, A.3.6
4.5	A.3.7
4.6	A.4.0

2.0 ССЫЛКИ

1) Оценка функциональной опасности для самолета S18

2) Предварительная FTA самолета S18

3) Документ с конструктивными требованиями и проектными параметрами самолета S18

3.0 ОПИСАНИЕ СИСТЕМЫ

Основным назначением системы торможения колес является торможение самолета на земле без скольжения шин. Система торможения колес выполняет эту функцию автоматически при посадке или вручную при ее активизации пилотом. В дополнение к торможению самолета система торможения колес используется для управления направлением движения на земле при помощи дифференциального торможения, остановки вращения колес основного шасси при его уборке и для предотвращения движения самолета во время парковки.

4.0 РЕЗУЛЬТАТЫ ОЦЕНКИ ФУНКЦИОНАЛЬНОЙ ОПАСНОСТИ ТОРМОЗНОЙ КОЛЕСНОЙ СИСТЕМЫ

4.1 Идентифицированные функции тормозной колесной системы

Система торможения колес выполняет следующие функции.

a. Торможение колес на земле

(1) Ручная активизация

(2) Автоматическая активизация

(3) Противодействие скольжению

b. Торможение колес при уборке шасси

c. Дифференциальное торможение для управления направлением движения

d. Предотвращение движения самолета при парковке

(Примечание редактора: В целях данного примера анализируется функция «торможения колес на земле». Эта функция идентифицирована в столбце (1) формы FHA примера, представленной в таблице 4.1-1).

4.2 Идентифицированные состояния отказа

Для функции «торможения колес на земле» для оценки определен следующий состав отказных состояний и допущений.

4.2.1 Функциональные отказные состояния

a. Общая потеря торможения колес

b. Частичная симметричная потеря торможения колес

c. Асимметричная потеря торможения колес

d. Непреднамеренное использование торможения колес

4.2.2 Окружающие и аварийные конфигурации и условия

a. Состояние взлетно-посадочной полосы (мокрая, обледенелая и т.п.)

b. Длина взлетно-посадочной полосы

c. Попутный/поперечный ветер

d. Отключение двигателя

e. Потеря гидравлической системы

f. Потеря электрической системы

4.2.3 Фазы – (наземные)

a. Руление

b. Взлет до отрыва (взлет)

c. Пробег после посадки (посадка)

d. Прерванный взлет (RTO)

4.2.4 Интерфейсные функции

a Предупреждение экипажа (аварийные, предупреждающие, уведомляющие)

b. Управление рулем направления/носовым колесом для контроля направления движения.

В столбцах (2) и (3) таблицы 4.1-1 показана та часть формы FHA, которая содержит сформулированные отказные состояния для данной функции.

4.3 Влияние отказных состояний на самолет, экипаж и пассажиров

Для каждого отказного состояния его влияние на самолет, экипаж и пассажиров показаны в столбце (4) таблицы 4.1-1.

4.4 Классификация/обоснование влияния отказного состояния на самолет, экипаж и пассажиров.

Для каждого отказного состояния его классификация определена в столбцах (5) и (6) таблицы 4.1-1.

4.5 План верификации целей безопасности

Для каждого состояния отказа план проверки целей безопасности определен в столбце (7) таблицы 4.1-1. В этом столбце перечислены ссылки на требования, деревья неисправностей, анализы и/или испытания.

4.6 Результаты FHA CTK

В качестве входных данных для PSSA CTK должен быть представлен следующий перечень существенных требований к безопасности, полученных из FHA CTK

1) Вероятность потери торможения всех колес при посадке или RTO должна быть менее 5E-7 на полет.

2) Вероятность асимметричной потери торможения колес, связанной с потерей рулевого управления или управления носовым колесом во время посадки или RTO должна быть меньше 5E-7 на полет.

3) Вероятность непреднамеренного торможения колес с блокировкой всех колес во время разбега при взлете до скорости V1 должна быть меньше 5E-7 на полет.

4) Вероятность непреднамеренного торможения колес во время разбега при взлете после скорости V1 должна быть меньше 5E-9 на полет.

5) Вероятность не выявленного непреднамеренного торможения одного колеса без блокировки всех колес во время взлета должна быть меньше 5E-9 на полет.

Таблица 4.1-1 – FHA самолета (*частичная – адресована только «торможению колес на земле»*)

1 **Функция**	2 **Отказное состояние (описание опасности)**	3 **Фаза**	4 **Влияние отказного состояния на самолет/ экипаж**	5 **Классификация**	6 **Вспомогательные материалы**	7 **Верификация**
Торможение самолета с использованием торможения колес	Общая потеря торможения колес	Посадка или RTO	См. ниже			
	a. Необъявленная потеря торможения колес	Посадка или RTO	Экипаж выявляет отказ во время работы тормозов. Экипаж использует интерцепторы и реверсоры тяги в максимальной степени. Это может привести к выбегу за пределы ВПП.	Аварийное		FTA самолета S18
	b. Объявленная потеря торможения колес	Посадка	Экипаж выбирает более пригодный аэропорт, извещает наземную аварийную службы и готовит пассажиров к посадке с выбегом за пределы ВПП. Экипаж использует интерцепторы и реверсоры тяги в максимальной степени.	Опасная	Процедуры экипажа для потери нормального и резервного режимов.	FTA самолета S18
	Частичная симметричная потеря торможения колес	Посадка или RTO	См. ниже			
	a. Необъявленная частичная симметричная потеря торможения колес	Посадка или RTO	Экипаж выявляет отказ во время использования тормозов. Экипаж использует имеющееся колесное торможение, интерцепторы и реверсоры тяги в максимальной степени. Температура колес на нагруженных тормозах растет и может достичь такого значения, при котором возникает неисправность колеса/шины. В зависимости от количества потерянных тормозов это может привести к выбегу за пределы ВПП.	От основной до опасной	Для определения классификации должны быть проведены дополнительные исследования.	Должно быть определено

1 Функция	2 Отказное состояние (описание опасности)	3 Фаза	4 Влияние отказного состояния на самолет/ экипаж	5 Классификация	6 Вспомогательные материалы	7 Верификация
	b. Сигнализируемая частичная симметричная потеря торможения колес	Посадка	Экипаж знает о том, что существует частичная потеря торможения колес перед посадкой. Экипаж использует имеющееся колесное торможение, интерцепторы и реверсоры тяги в максимальной степени. Температура колес на нагруженных тормозах растет и может достичь такого значения, при котором возникает неисправность колеса/шины. В зависимости от количества потерянных тормозов это может привести к выбегу за пределы ВПП.	Сложное		
	Асимметричная потеря торможения колес	Посадка или RTO	См. ниже			
	a. Асимметричная потеря колесного торможения – отказ только тормозной системы	Посадка или RTO	Снижение характеристик торможения. Тенденция к сходу с ВПП. Влияние характеристик торможения и температуры тормоза то же самое, что и описанная выше частичная потеря тормозов. Экипаж удерживает самолет на ВПП при помощи руля при высокой скорости и носового колеса при низкой скорости. Последовательности должны быть определены после получения результатов изучения обоснования.	Должна быть определена	Для определения классификации должны быть проведены дополнительные исследования.	
	b. Асимметричная потеря колесного торможения и управления рулем или носовым колесом	Посадка	Снижение характеристик торможения. Тенденция к сходу с ВПП. Влияние характеристик торможения и температуры тормоза то же самое, что и описанная выше частичная потеря тормозов. Экипаж не может удерживать самолет на осевой линии ВПП и в результате происходит сход самолета с ВПП.	Сложное		FTA самолета S18

1 Функция	2 Отказное состояние (описание опасности)	3 Фаза	4 Влияние отказного состояния на самолет/ экипаж	5 Классификация	6 Вспомогательные материалы	7 Верификация
	Непреднамеренное включение колесного тормоза		См. ниже			
	a. Непреднамеренное включение колесного тормоза без блокировки колеса	Взлет до V1	Экипаж останавливает самолет на взлетно-посадочной полосе (ВПП).	УУП		
	b. Непреднамеренное включение колесного тормоза с блокировкой всех колес	Взлет до V1	Потенциальная возможность разрыва всех шин и потери эффективности торможения.	Сложное		FTA самолета S18
	c. Непреднамеренное включение колесного тормоза с блокировкой всех колес или без нее	Взлет после V1	Экипаж не может безопасно взлететь или обеспечить безопасный RTO, что приводит к выбегу за пределы ВПП с высокой скоростью.	Катастрофическое		FTA самолета S18
	d. Несигнализируемое непреднамеренное торможение одного колеса без его блокировки	Взлет	Экипаж не может выявить неисправность по асимметрии, которая очень мала. Температура тормоза может достичь очень высокого значения. Экипаж убирает шасси, что приводит к возможному возгоранию колеса или повреждению шины.	Катастрофическое		FTA самолета S18
	e. Непреднамеренное торможение одного колеса без его блокировки, связанное с выявлением высокой температуры тормоза	Взлет	Экипаж не может выявить неисправность по асимметрии, которая очень мала. Температура тормоза может достичь очень высокого значения. Экипаж выявляет высокую температуру тормоза и оставляет шасси неубранными для охлаждения тормоза.	УУП	Процедура экипажа для оставления шасси в неубранном состоянии в случае выявленной высокой температуры тормоза	
и т.п.	и т.п.					

PSSA СИСТЕМЫ ТОРМОЖЕНИЯ КОЛЕС

1.0 ВВЕДЕНИЕ

Данная PSSA представляет собой краткую сводку по оценкам и анализам, выполненным на стадии эскизного и предварительного проектирования системы торможения колеса. Данный PSSA предназначен для составления перечня требований к безопасности, определения того, что предлагаемая конструкция может приемлемо выполнять требования, и для определения требований к безопасности, которые должны учитываться в конструкции изделий и установок более низкого уровня.

(Примечание редактора: В следующей таблице перекрестных ссылок представлена связь каждого параграфа примера с применяемым параграфом приложения).

№ параграфа PSSA системы	№ параграфа Приложения B
4.1.1	B.3.1.1
4.1.2	B.3.1.2
4.2	B.3.2
4.2.1	Приложение D
4.2.2	Приложение E
4.2.3	Приложение F
4.3.2	B.3.3

2.0 Ссылки

1) Оценка функциональной опасности для самолета S18

2) FTA системы торможения колеса S18

3) Предварительные результаты CCA самолета S18 - PRA, CMA, *ZSA (Примечание редактора: Ссылки на PRA, CMA и ZSA даются в связи с тем, что они представляют методы для определения требований к независимости).*

4) Соответствующие требования к летной годности

3.0 Краткое описание системы

Система торможения колес устанавливается на два основных шасси. Торможение колес основного шасси используется для безопасного замедления самолета во время фаз руления и посадки, а также в случае прерванного взлета. Система торможения колес показана на рис. 3.0-1. Колесные тормоза также предохраняют от непреднамеренного движения самолета при его парковке, и могут использоваться для обеспечения дифференциального торможения для управления направлением движения самолета. Второй функцией системы торможения колес является остановка вращения основного шасси после его уборки.

Торможение на земле управляется либо вручную, при помощи тормозных педалей, либо автоматически (автоматическое торможение) без необходимости использования тормозных педалей. Функция автоматического торможения обеспечивает пилоту предварительную установку скорости торможения до взлета или посадки. Автоматическое торможение имеется только на НОРМАЛЬНОЙ системе торможения.

Восемь колес основного шасси имеют многодисковые углеродные тормоза. С учетом того требования, что вероятность потери всего торможения колес должна быть менее 5E-7 на полет, было принято конструкторское решение, чтобы каждое колесо имело узел тормоза, управляемый двумя независимыми комплектами гидравлических поршней. Один комплект работает от ЗЕЛЕНОЙ гидравлической системы и используется в НОРМАЛЬНОМ режиме торможения. Другой режим является резервным и выбирается автоматически при отказе НОРМАЛЬНОЙ системы. Он работает независимо с использованием ГОЛУБОЙ гидравлической системы и

поддерживается аккумулятором, который также используется для привода парковочного тормоза. Аккумулятор питает АЛЬТЕРНАТИВНУЮ систему в АВАРИЙНОМ режиме торможения, когда происходит отказ ГОЛУБОЙ гидравлической системы, и НОРМАЛЬНЫЙ режим не доступен. Переключение происходит автоматически при различных условиях отказа, либо может быть выбрано вручную. Снижение давление в ЗЕЛЕНОЙ гидравлической системе ниже порогового значения либо от отказа самой ЗЕЛЕНОЙ системы подачи, либо от ее отключения при помощи BSSU вследствие наличия неисправностей, приводит к тому, что автоматический селектор подключает ГОЛУБУЮ систему подачи к АЛЬТЕРНАТИВНОЙ системе торможения. Как в НОРМАЛЬНОМ, так и в АЛЬТЕРНАТИВНОМ режимах имеется устройство против скольжения, которое работает при всех скоростях, превышающих 2 м/с.

В НОРМАЛЬНОМ режиме торможения все восемь колес индивидуально тормозятся от своих собственных сервоклапанов, которые также используются для противоскольжения. В АЛЬТЕРНАТИВНОМ режиме сдвоенный регулятор потока обеспечивает подачу низкого гидравлического давления торможения через четыре сервоклапана, которые обеспечивают функцию противоскольжения для четырех пар колес. Работа АЛЬТЕРНАТИВНОЙ системы исключена, когда используется НОРМАЛЬНАЯ система.

В НОРМАЛЬНОМ режиме электрический сигнал о положении тормозной педали передается на компьютер торможения. Он в свою очередь выдает соответствующие сигналы управления на тормоза. Кроме того, этот компьютер контролирует различные сигналы, которые обозначают определенные критические состояния самолета и системы для обеспечения правильных функций тормоза и повышения отказоустойчивости системы, а также генерирует предупреждения, индикации и информацию о техническом обслуживании для других систем. Соответственно этот компьютер называется «блок управления тормозной системы» (BSCU). Он автоматически обеспечивает следующие функции.

a. Управление ручным торможением (при помощи тормозных педалей) или автоматическими органами управления (активизация автоматического торможения, подача команд автопилота во время посадки CAT IIIb).

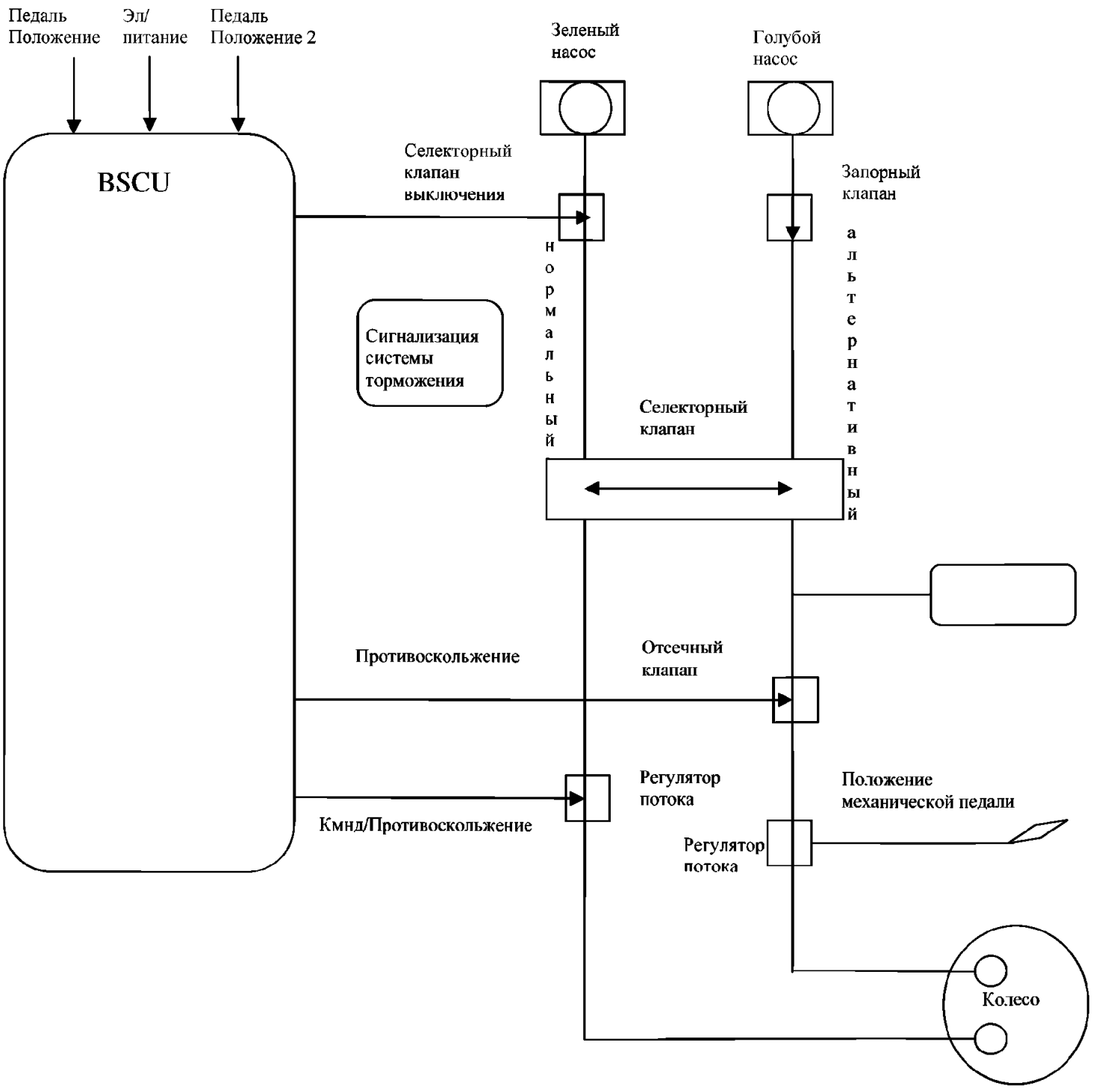
b. Управление интерфейсами с другими самолетными системами.

(Примечание редактора: Интерфейсы с другими системами могут включать в себя интерфейсы с гидравлической системой, системой контроля температуры тормоза и т.п.).

c. Генерация команд торможения в соответствии с принимаемыми командами и состоянием системы.

d. Регулирование торможения во избежание скольжения основных колес.

e. Передача информации (индикации, подсветки, предупреждения и т.п.) на приборной доске кабины и на различные компьютеры самолета, относящиеся к состоянию BSCU.



(PSSA – Система торможения колес). Предварительная схема системы торможения колес
Рис. 3.0-1

4.1 Требования к безопасности системы торможения колеса

4.1.1 Входные данные PSSA

Следующий набор требований по безопасности (работоспособность, интеграция, установка) был получен в результате FHA самолета и системы и анализа общей причины, проведенных на основе средней продолжительности полета 5 часов.

1) Вероятность потери торможения всех колес при посадке или RTO должна быть менее 5E-7 на полет.

2) Вероятность асимметричной потери торможения колес, связанной с потерей управления рулем или управления носовым колесом во время посадки или RTO должна быть меньше 5E-7 на полет.

3) Вероятность непреднамеренного торможения колес с блокировкой всех колес во время разбега при взлете до скорости V1 должна быть меньше 5E-7 на полет.

4) Вероятность непреднамеренного торможения колес во время разбега при взлете после скорости V1 должна быть меньше 5E-9 на полет.

5) Вероятность не выявленного непреднамеренного торможения одного колеса без блокировки всех колес во время взлета должна быть меньше 5E-9 на полет.

Система торможения колеса и система реверсора тяги должны быть разработаны для предотвращения общих опасностей (разрыва шины, кромсания шины, нарушения протектора, конструкционных деформаций, и т.п.).

Система торможения колеса и система реверсора тяги должны быть разработаны для предотвращения отказов общего режима (гидравлической системы, электрической системы, технического обслуживания, текущего ремонта, операций, конструкции, изготовления и т.п.).

Конструкционные особенности системы торможения колеса, удовлетворяющие требованиям к безопасности, представлены в таблице 4.1.1-1.

Таблица 4.1.1-1 (PSSA – Система торможения колес)
Требования к безопасности системы торможения колеса/конструктивные решения

Требование по безопасности	Конструктивные решения	Примечания
1. Вероятность потери торможения всех колес (необъявленная или объявленная) во время посадки или RTO должна быть менее 5E-7 на полет.	Для достижения этой цели требуется более одной гидравлической системы (по опыту эксплуатации). Двухканальный BSCU и многорежимная работа тормоза.	Общая работоспособность системы торможения колеса может приемлемо отвечать этому требованию. См. ниже PSSA FTA.
2. Вероятность асимметричной потери торможения колес, связанной с потерей управления рулем или носовым колесом во время посадки должна быть менее 5E-7 на полет.	Отделить систему управления рулем и носовым колесом от системы торможения колеса. Сбалансировать гидравлическую подачу к каждой стороне системы торможения колеса.	Должно быть показано, что система торможения колеса достаточно независима от систем управления рулем и носовым колесом. Системное разделение между этими системами должно быть показано в зональном анализе безопасности и анализе конкретного риска.
3. Вероятность непреднамеренного торможения колес с блокировкой всех колес во время разбега при взлете до скорости V1 должна быть меньше 5E-7 на полет.	Нет	Требование 4 является более строгим и, следовательно, определяет конструкцию.
4. Вероятность непреднамеренного торможения колес во время разбега при взлете после скорости V1 должна быть меньше 5E-9 на полет.	При этих условиях в результате не должно быть одиночного отказа.	Нет
5. Вероятность не выявленного непреднамеренного торможения одного колеса без блокировки всех колес во время взлета должна быть меньше 5E-9 на полет.	При этих условиях в результате не должно быть одиночного отказа.	Нет

4.1.2 Производные требования по безопасности

Конструктивные решения, описанные в таблице 4.1.1-1, приводят к тому, что первичная и вторичная система должны выполнять функцию торможения колес. В результате этих конструктивных решений был получен следующий набор требований по безопасности (работоспособности, целостности, установке).

1) Первичная и вторичная системы должны быть разработаны таким образом, чтобы предотвратить любые общие опасности (например, разрыв шины, повреждение протектора, конструктивные деформации).

2) Первичная и вторичная системы должны быть разработаны таким образом, чтобы предотвратить любые общие отказы режима (гидравлической системы, электрической системы, технического обслуживания, текущего ремонта, операций, конструкции, изготовления и т.п.).

Таблица 4.1.2-1 – (PSSA – Система торможения колес)
Производные требования по безопасности к системе торможения колес

Требование к безопасности	Конструктивные решения	Примечания
1. Первичная и вторичная системы должны быть разработаны таким образом, чтобы предотвратить любые общие опасности (разрыв шины, повреждение протектора, конструктивные деформации).	Установить гидравлическую подачу к тормозам перед стойкой основного шасси и за ней.	Соответствие должно быть показано при помощи ZSA и PRA. *(Примечание редактора: В этом примере только для зоны отсека основного шасси и конкретного риска разрыва шины).*
2. Первичная и вторичная системы должны быть разработаны таким образом, чтобы предотвратить любые общие отказы режима (гидравлической системы, электрической системы, технического обслуживания, текущего ремонта, операций, конструкции, изготовления и т.п.).	Выбрать две различные гидравлические системы для обеспечения тормозов, аварийного торможения без электропитания.	Соответствие должно быть показано при помощи CMA.

4.2 Оценка отказного состояния

Ниже перечислены отказные состояния, идентифицированные по результатам FHA самолета и системы. Для каждого из этих состояний должны быть разработаны предварительная оценка и ресурсы.

1) Вероятность потери торможения всех колес при посадке или RTO должна быть менее 5E-7 на полет.

2) Вероятность асимметричной потери торможения колес, связанной с потерей управления рулем или управления носовым колесом во время посадки или RTO должна быть меньше 5E-7 на полет.

3) Вероятность непреднамеренного торможения колес с блокировкой всех колес во время разбега при взлете до скорости V1 должна быть меньше 5E-7 на полет.

4) Вероятность непреднамеренного торможения колес во время разбега при взлете после скорости V1 должна быть меньше 5E-9 на полет.

5) Вероятность не выявленного непреднамеренного торможения одного колеса без блокировки всех колес во время взлета должна быть меньше 5E-9 на полет.

4.2.1 Анализ дерева неисправностей для PSSA

(Примечание редактора: Данный раздел должен обычно содержать деревья отказов для всех значительных состояний. В данном примере показана оценка только «несигнализируемой потери торможения всех колес»).

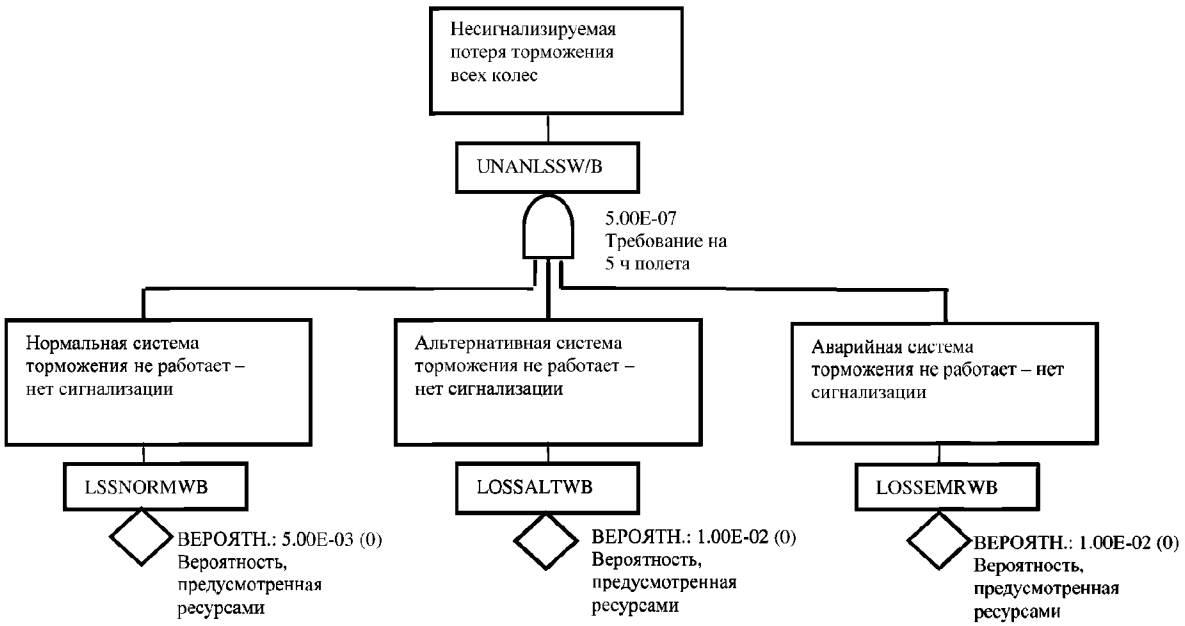
Дерево неисправности для PSSA верхнего уровня, показанное на рис. 4.2.1-1, отражает требования верхнего уровня к системе торможения и изображает три подсистемы торможения и ресурсы для необъявленной потери каждой.

Дерево неисправности на рис. 4.2.1-2 отображает следующий уровень разработки и оценки системы. Это дерево включает идентификацию того факта, что потеря всего торможения является опасной, и было принято решение для охвата всех возможных потерь независимо от сигнализации. Это отражается дополнением события «Потеря возможности сигнализации», которое дополнено событием «Потеря торможения всех колес», показанного на рис. 4.2.1-1. Вероятность «потери возможности сигнализации» установлена на значение 1,0. Также приняты конструктивные решения, требующие, чтобы «нормальная» и «альтернативная» тормозные системы отвечали требованиям работоспособности и целостности без зависимости или содействия от «резервной аварийной системы». На это указывает вероятность отказа такой системы, которая устанавливается на значение 1,0. Результатом этого являются повышенные ресурсы работоспособности для функций «нормальной» и «альтернативной» тормозных систем.

На рис. 4.2.1-2 также показано нисходящее развитие конструкции системы «нормального торможения» по частоте отказов ресурсов для идентифицированных вкладов в неисправности «Нормальная система торможения не работает» (потеря гидравлической подачи, потеря гидравлических компонентов и потеря способности BSCU подавать команды на торможение). Событие «Потеря способности BSCU управления торможением» далее разбивается на два основных элемента: отказ BSCU и потеря электропитания BSCU с применяемыми ресурсами, включая отказы электропитания самолета. Результирующее требование для ресурсов отказов BSCU 6E-6 в час было рассчитано в обратном порядке для обеспечения удовлетворения потерь более высокого уровня ресурсов BSCU. Эти ресурсы целостности BSCU были направлены поставщику BSCU как конструктивное требование к системе.

Опыт поставщика BSCU показывает, что ресурсы частоты отказов 6E-6 не реальны для разработки комплексной функции BSCU, поэтому поставщик вывел требование по резервным расчетам BSCU для того, чтобы отвечать требованиям ресурсов по частоте отказов. Дерево отказов на рис. 4.2.1-3 отображает эволюцию конструкции с резервными BSCU и их дополнительной конфигурацией. Результирующая частота отказов на канал в час равна 1,15E-3.

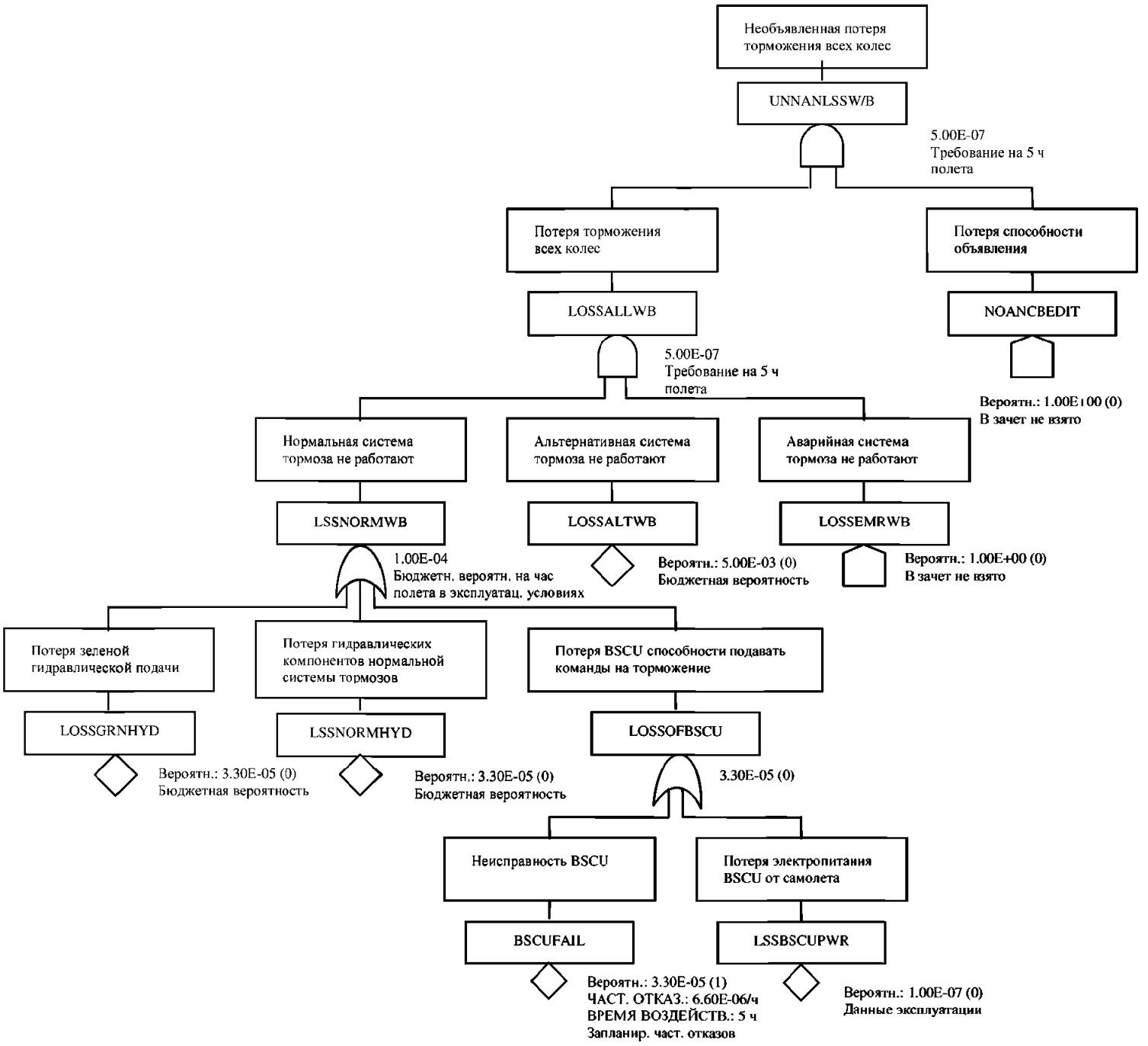
Примечание поставщика: *Принято решение для обеспечения двух средств использования торможения колес для обеспечения полной остановки. Этими средствами являются нормальная и альтернативная системы торможения. Стояночный тормоз необходим для нормальной эксплуатации самолета на земле, и принято решение, чтобы он мог применяться в качестве аварийного тормоза. Это дерево неисправности отображает исходное назначение ресурсов вероятности для каждой из трех систем. Нормальной системе дано наиболее строгое назначение.*



(PSSA – Система торможения колес – FTA)
Дерево неисправности (исходное) несигнализируемой потери торможения всех колес
Рис. 4.2.1-1

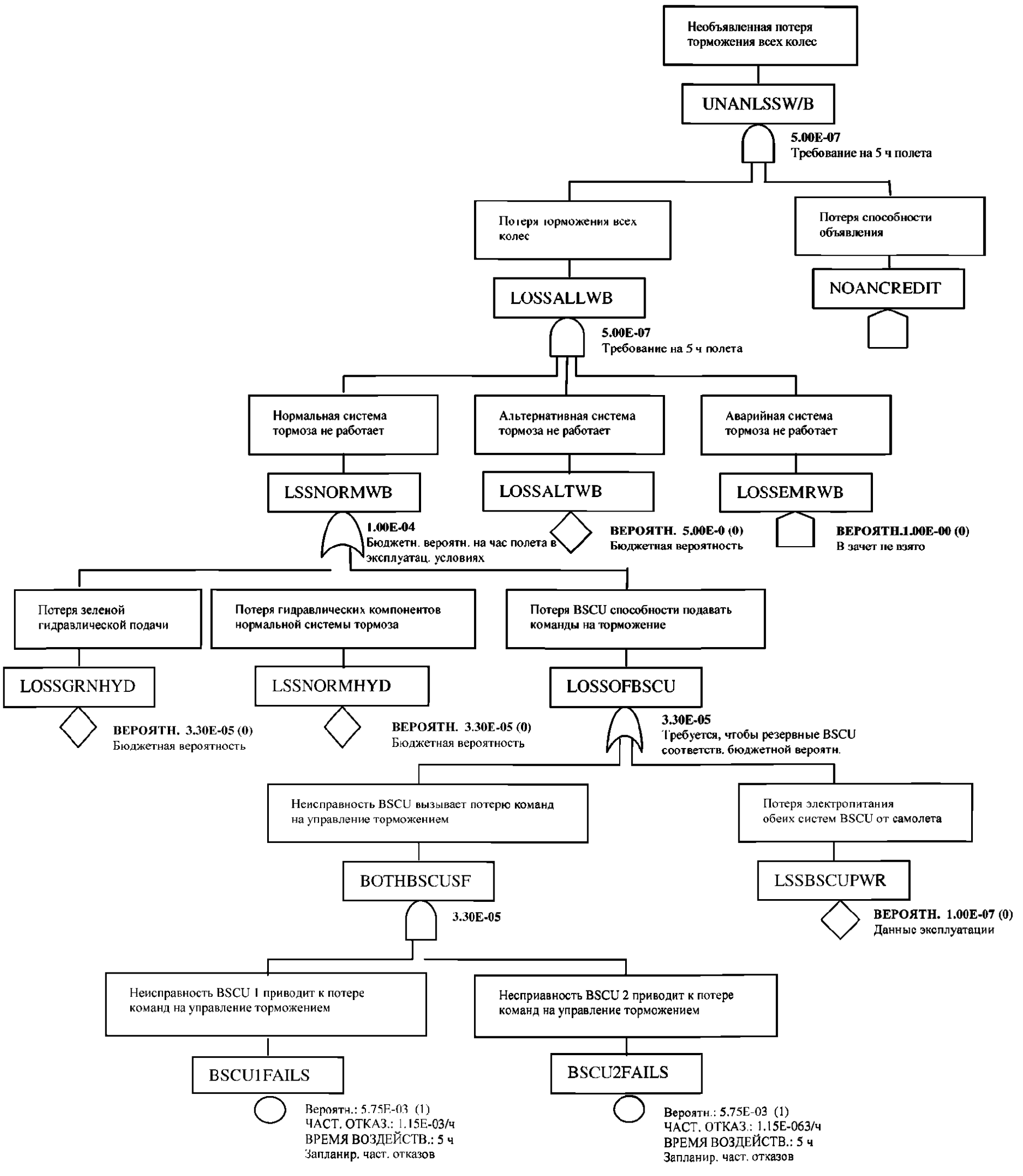
Примечание редактора: *Поскольку несигнализируемая и сигнализируемая потеря торможения колес рассматриваются как сложные отказные состояния, то принято решение о включении всех отказов системы торможения колеса, которые дают в результате потери независимо от того, сигнализируются они или нет.*

- *Принято решение о том, что нормальная и альтернативная системы должны отвечать требованию без учета аварийного (стояночного) тормоза.*
- *В обсуждениях с потенциальными поставщиками BSCU было выявлено, что частота отказов 6,6E-6 не достижима при одном изделии. Принято решение об использовании 2-х BSCU. Это решение отображено на дереве отказов на следующей странице.*



(PSSA – Система торможения колеса – FTA)
Дерево неисправности (редакция A) несигнализируемой потери торможения всех колес
Рис. 4.2.1-2

Примечание редактора: *Это дерево неисправности было модифицировано для включения требования по двум BSCU.*

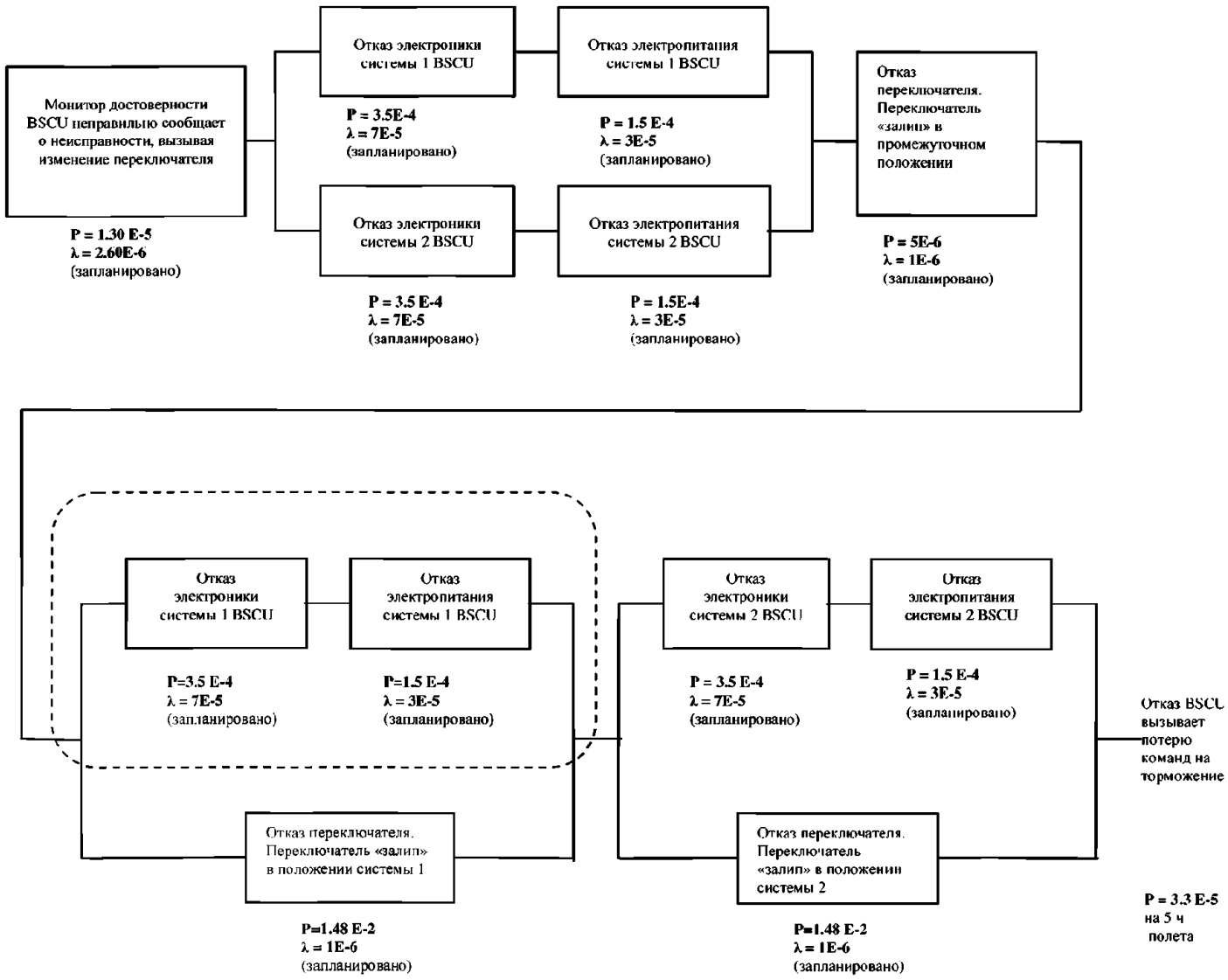


(PSSA – Система торможения колеса – FTA)
Дерево неисправности (редакция B) несигнализируемой потери торможения всех колес
Рис. 4.2.1-3

4.2.2 DD для PSSA

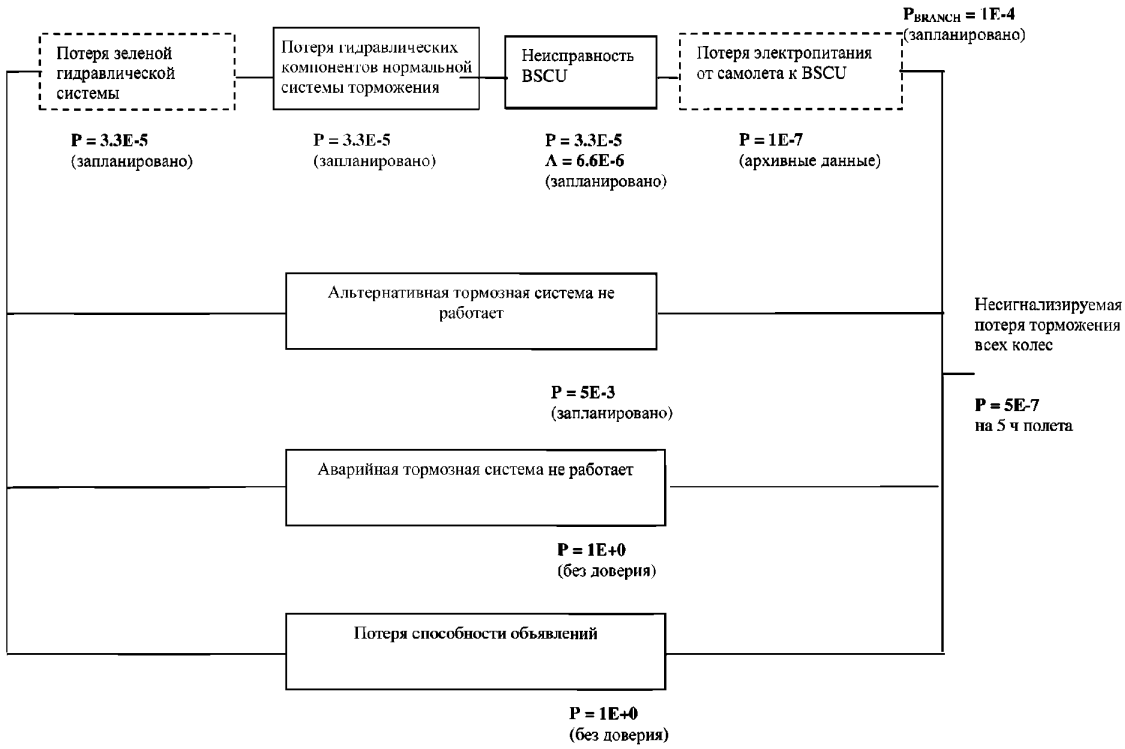
(Примечание редактора: Подробную информацию по процессу DD см. в Приложении E).

(Примечание редактора: Обычно текстовое описание разработки DD должно включаться в анализ. Данный текст аналогичен тому, который включен в предыдущий пример анализа FTA).



(PSSA – Система торможения колес – DD)
Логическая схема несигнализируемой потери торможения всех колес (исходная).
Рис. 4.2.2-1

(Примечание редактора: Принято решение для обеспечения двух средств использования торможения колес для влияния на полную остановку. Этими средствами являются нормальная и альтернативная тормозные системы. Стояночный тормоз необходим для нормальной эксплуатации самолета на земле, и принято решение, чтобы он мог применяться в качестве аварийного тормоза. Эта схема зависимости отображает исходное назначение ресурсов вероятности для каждой из трех систем. Нормальной системе дано наиболее строгое назначение).



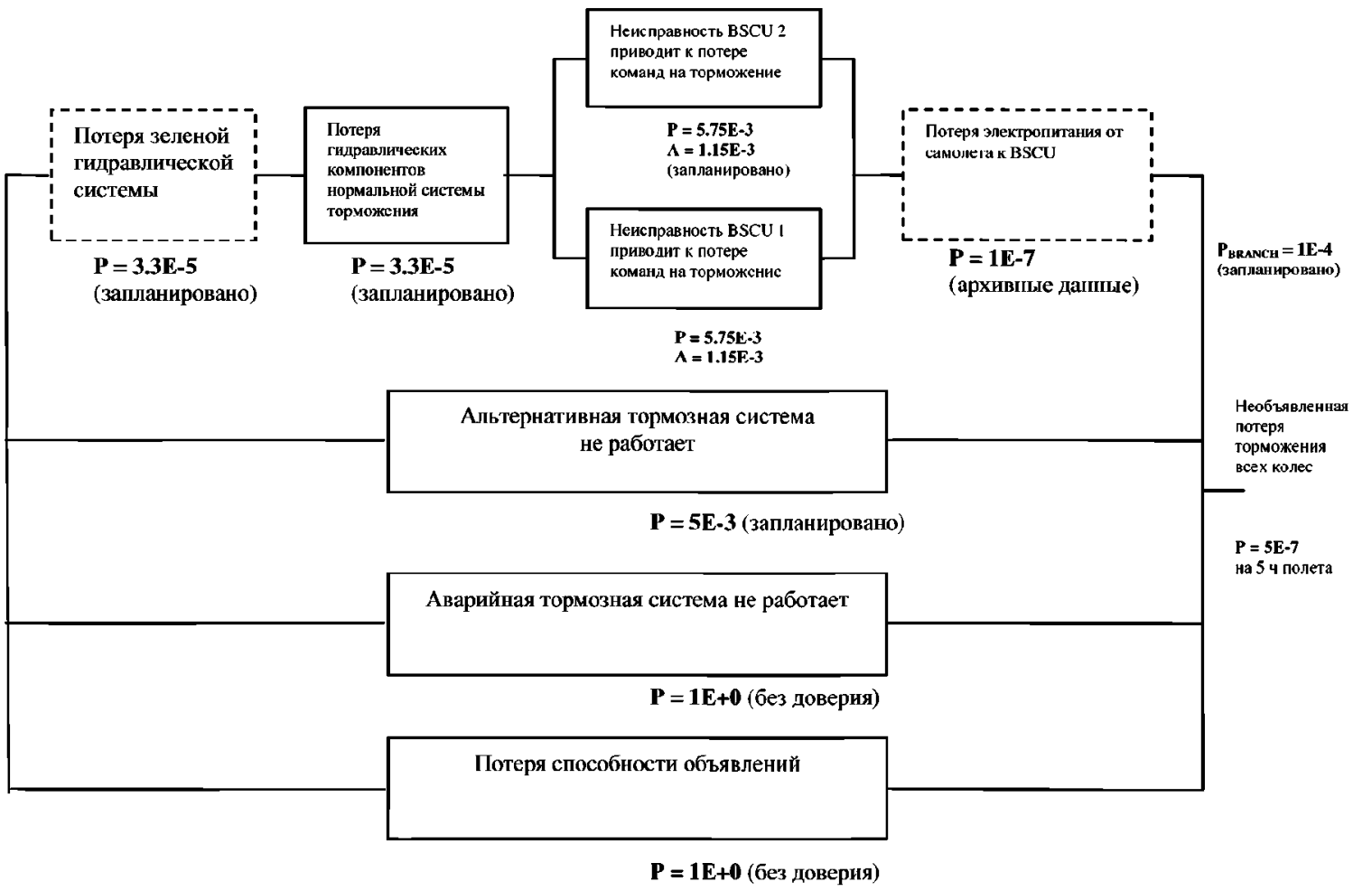
(PSSA – Система торможения колес – DD) Логическая схема несигнализируемой потери торможения всех колес (редакция A).
Рис. 4.2.2-2

(Примечание редактора: Отказное состояние, анализируемое в данной DD системы торможения колеса DD, представляет собой несигнализируемую потерю торможения колеса, поскольку оно содействует состоянию катастрофического отказа. Поскольку несигнализируемая и сигнализируемая потеря торможения колес рассматриваются как опасные состояния отказа, то принято решение о включении всех отказов системы торможения колес, которые дают в результате потери независимо от того, сигнализируются они или нет. Это решение представлено на DD при помощи включения события потери способности сигнализации с вероятностью 1.)

Принято решение о проектировании системы таким образом, чтобы нормальная и альтернативная системы отвечали требованию без учета аварийного (стояночного) тормоза.

Целью для нормальной системы торможения устанавливается частота отказов не более 1E-4 на полет.

В обсуждениях с потенциальными поставщиками BSCU было выявлено, что частота отказов 6,6E-6 не достижима при одном изделии. Принято решение об использовании 2-х BSCU. Это решение отображено в DD на следующей странице.



(PSSA – Система торможения колес – DD)
Логическая схема зависимости несигнализируемой потери торможения всех колес (редакция B)
Рис. 4.2.2-3

4.2.3 Марковский анализ для PSSA

(Примечание редактора: В данном разделе обычно должен содержаться Марковский анализ для всех значительных состояний отказа. В данном примере показана оценка только «несигнализируемой потери торможения колес»).

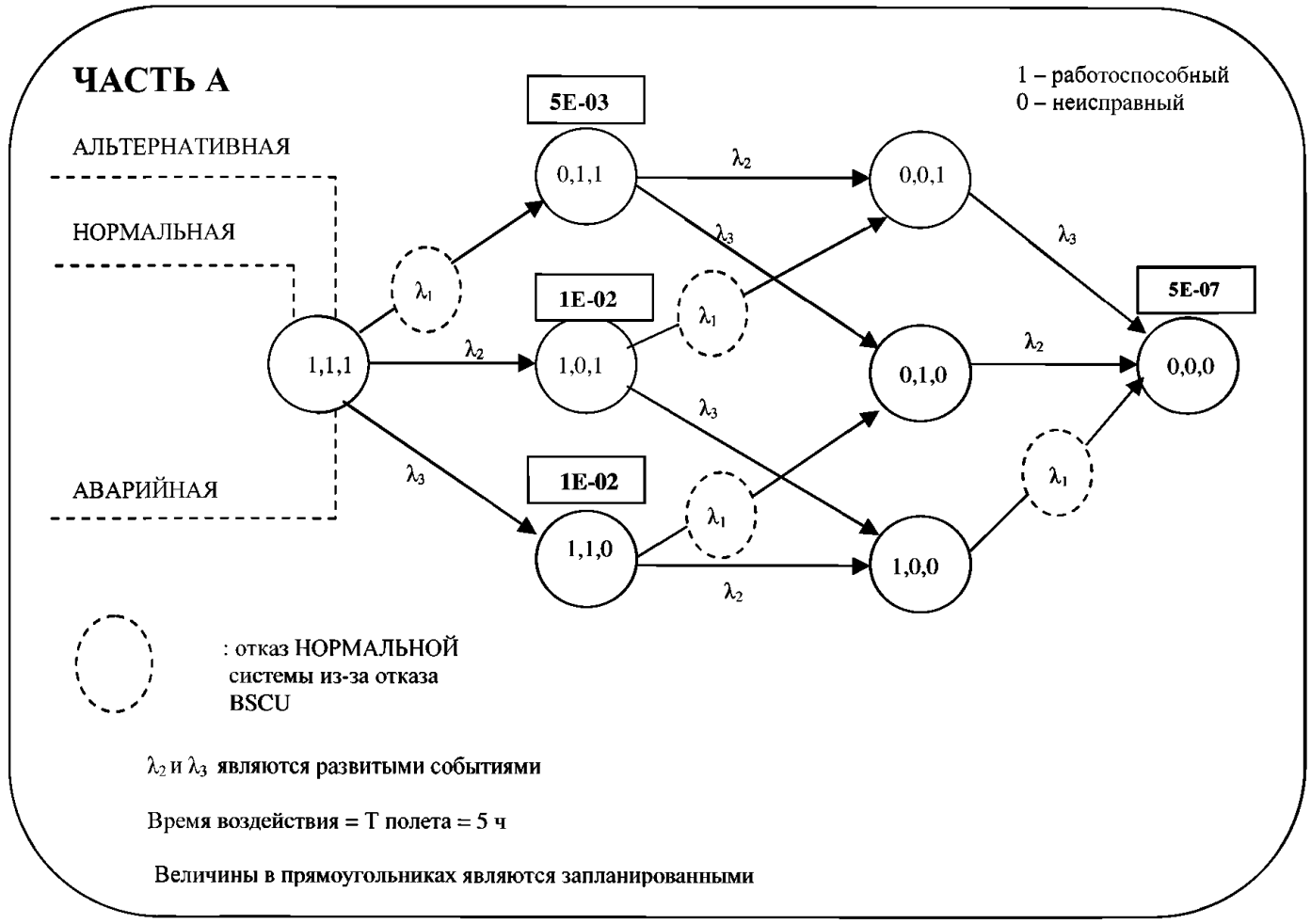
В примере самолета S18 величина λ_1, которая представляет интенсивность отказов НОРМАЛЬНОЙ системы торможения, увеличена для подробного Марковского анализа. Данный анализ может включать в себя проектные итерации.

(Примечание редактора: В данном примере допускается, что АЛЬТЕРНАТИВНАЯ (λ_2) и АВАРИЙНАЯ (λ_3) должны быть развитыми событиями, и, следовательно, не приводится дальнейший анализ для получения частот отказов для этих событий).

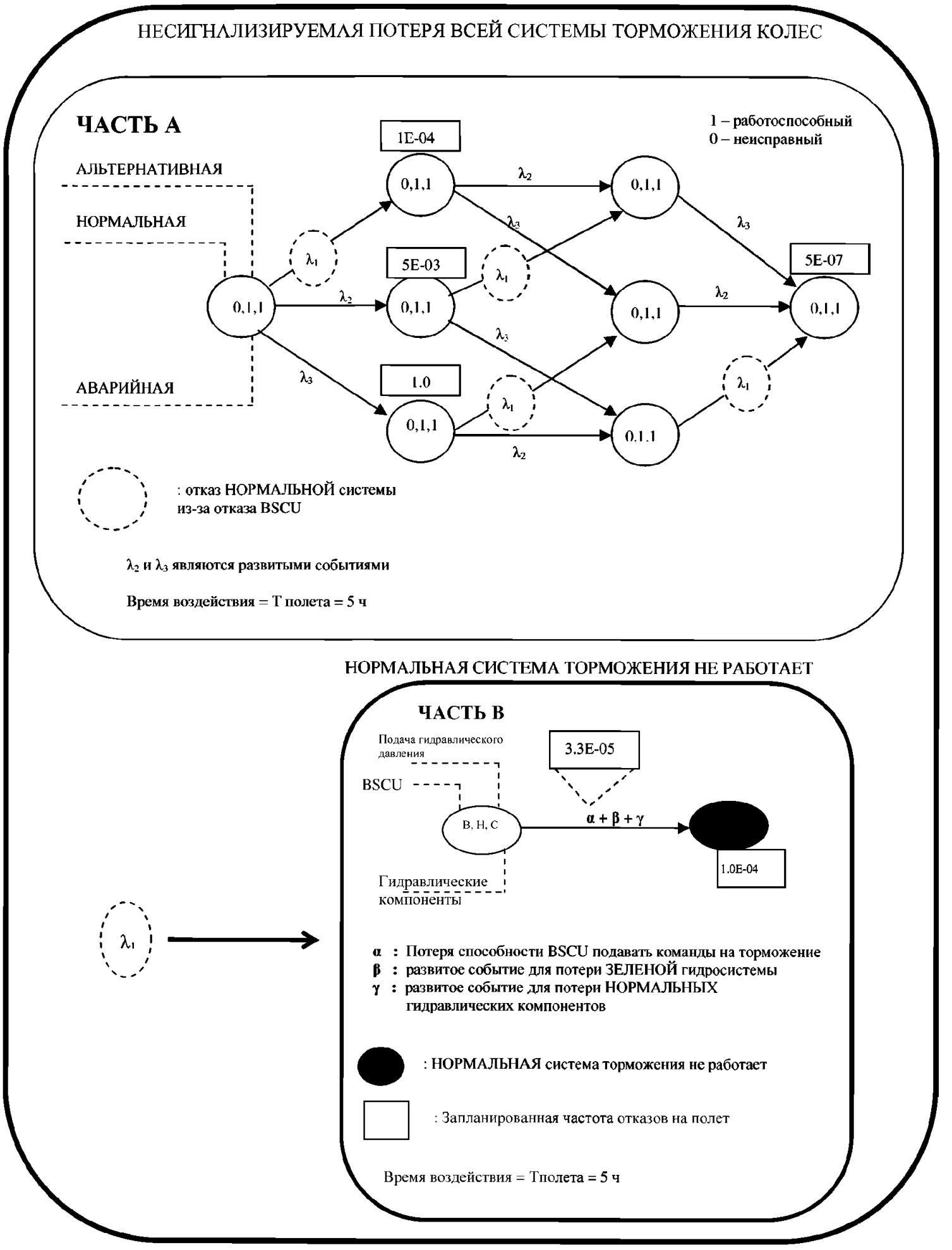
Представление Марковской цепи для системы торможения колеса показано на рис. 4.2.3-1. Оно показывает Марковскую цепь для трех различных систем, которые обеспечивают команды на торможение: НОРМАЛЬНУЮ, АЛЬТЕРНАТИВНУЮ и АВАРИЙНУЮ. Каждое состояние в Марковской цепи определяется тремя группами, показывающими состояние НОРМАЛЬНОЙ, АЛЬТЕРНАТИВНОЙ и АВАРИЙНОЙ систем торможения. «1» в данном состоянии представляет нормально работающую систему, а «0» – неисправную систему. Например, состояние (0 1 1) представляет состояние системы, при котором НОРМАЛЬНАЯ система торможения неисправна, в то время как АЛЬТЕРНАТИВНАЯ и АВАРИЙНАЯ системы торможения работоспособны. λ, λ_2, λ_3 представляют собой частоты отказов НОРМАЛЬНОЙ, АЛЬТЕРНАТИВНОЙ и АВАРИЙНОЙ систем торможения в виде количества отказов в час. Принимается, что система торможения колеса неисправна, когда все три системы – НОРМАЛЬНАЯ, АЛЬТЕРНАТИВНАЯ и АВАРИЙНАЯ, неисправны. Это представляется состоянием (0 0 0). Некоторые состояния в Марковской цепи показывают максимальные вероятности состояния, которые представляют собой распределенные ресурсы для НОРМАЛЬНОЙ, АЛЬТЕРНАТИВНОЙ и АВАРИЙНОЙ систем торможения.

Рис. 4.2.3-2 (Часть A) является таким же, что и рис. 4.2.3-1, за исключением того, что не принято доверия для АВАРИЙНОЙ системы торможения. На рис. 4.2.3-2 (Часть B) показана подробная цепь Маркова для компьютера BSCU, который управляет НОРМАЛЬНОЙ системой торможения. Все пунктирные окружности на рис. 4.2.3-1 заменены результатами анализа Части B рис. 4.2.3-2. На рис. 4.2.3-2 (Часть B) показана НОРМАЛЬНАЯ система торможения как функция «ИЛИ» трех компонентов: BSCU, ЗЕЛЕНОЙ гидравлической системы и гидравлических компонентов нормальной системы торможения.

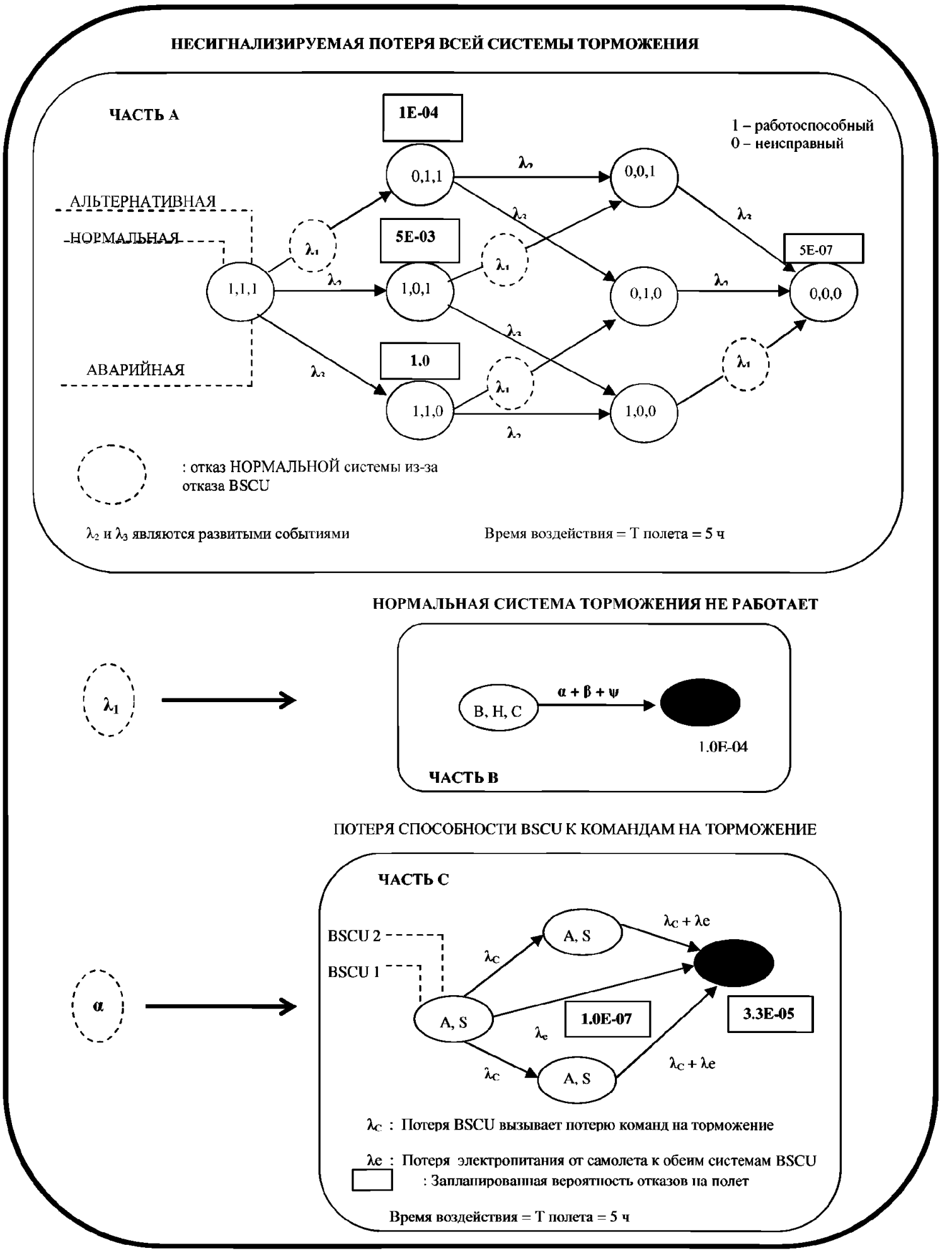
На рис. 4.2.3-2 BSCU разработан как единичное изделие. После обсуждения с потенциальными изготовителями BSCU было сделано заключение, что для выполнения требований по безопасности необходимо иметь два BSCU. Эта модифицированная целевая конструкция BSCU показана на рис. 4.2.3-3. Для выполнения требований по безопасности на рис. 4.2.3-3 (Часть C) показаны два BSCU. В данной цепи Маркова каждое состояние представлено двумя группами (A, S), где «A» представляет собой состояние активного BSCU, который может быть либо BSCU 1 или BSCU 2, а «S» представляет собой состояние резервного BSCU. Предполагается, что каждый компонент должен быть в работоспособном или неисправном состоянии. Неисправные состояния представлены полоской наверху символа. Предполагается, что система BSCU должна быть неисправной, когда оба BSCU неисправны или отсутствует электропитание обоих BSCU.



(PSSA – Система торможения колес – МА)
Несигнализируемая потеря всей системы торможения колес (исходная)
Рис. 4.2.3-1



(PSSA – Система торможения колес – МА)
Несигнализируемая потеря всей системы торможения колес (редакция А)
Рис. 4.2.3-2



(PSSA – Система торможения колес – МА)
Несигнализируемая потеря всей системы торможения колес (редакция В)
Рис. 4.2.3-3

4.3 Установленные требования

Из требований, определенных и перечисленных в разделе 4.1, были получены требования нижнего уровня

4.3.1 Требования к установке

Первичная и вторичная системы гидравлической подачи должны быть разделены, и в ZSA и PRA должна быть проведена их проверка.

(Примечание редактора: По деревьям неисправностей определены дополнительные требования к установке, но для краткости они здесь не показаны).

4.3.2 Требования уровня изделия

1) Вероятность события «Отказ BSCU вызывает потерю команд на торможение» должна быть меньше 3,3E-5 на полет.
2) Вероятность «потери одиночного BSCU» должна быть меньше 5,75E-3 на полет.
3) Вероятность «потери гидравлических компонентов нормальной системы торможения» должна быть меньше 3,3E-5 на полет.
4) *Вероятность «непреднамеренного торможения из-за BSCU» должна быть меньше 2,5E-9 на полет.
5) Никакой одиночный отказ BSCU не должен приводить к «непредвиденному торможению».
6) BSCU должен быть спроектирован для уровня гарантии разработки A вследствие катастрофической классификации события «Непредвиденное торможение из-за BSCU».

*(*Примечание редактора: Данное требование было определено по дереву неисправности, которое не показано в данном примере).*

4.3.3 Требования к другим системам

Вероятность «потери зеленой гидравлической подачи для нормальной системы торможения» должна быть меньше 3,3E-5 на полет.

(Примечание редактора: По деревьям неисправностей определены дополнительные требования к другим системам, но для краткости они здесь не показаны).

4.3.4 Требования по безопасности к техническому обслуживанию

Отказ АЛЬТЕРНАТИВНОГО режима торможения является скрытым, поскольку НОРМАЛЬНЫЙ режим торможения выполняется тогда, когда в нем нет отказов. Следовательно, необходимо разработать задачу технического обслуживания для функциональной проверки АЛЬТЕРНАТИВНОГО режима торможения. Определить периодичность такой проверки таким образом, чтобы выполнялось требование «Вероятность того, что альтернативное торможение не работает, меньше 5E-3 на полет».

(Примечание редактора: По этим деревьям неисправностей могут быть определены дополнительные требования к техническому обслуживанию, но для краткости они здесь не показаны).

5.0 ЗАКЛЮЧЕНИЕ

Как показано, теперь конструкция может удовлетворять требованиям к безопасности, определенным в FHA и предыдущих CCA. Были определены дальнейшие требования к установке, позициям нижнего уровня, другим системам и задачам технического обслуживания, и они переданы соответствующей организации, отвечающей за конструкцию.

1.0 ВВЕДЕНИЕ

Данная PSSA описывает оценки и анализы, выполненные на стадии эскизного и предварительного проектирования блока управления тормозной системы. Данная PSSA предназначена для составления перечня требований по безопасности, определения того, что предлагаемая конструкция может приемлемо выполнять требования и для определения требований к аппаратным и программным средствам.

(Примечание редактора: В следующей таблице перекрестных ссылок представлена связь каждого параграфа примера с применяемым параграфом приложения FHA).

№ параграфа PSSA системы	№ параграфа приложения B
4.1.1	B.3.1.1
4.2	B.3.2
4.2.1	Приложение D
4.2.2	Приложение E
4.2.3	Приложение F
4.3.2	B.3.3

2.0 ССЫЛКИ

1) PSSA системы торможения колес S18

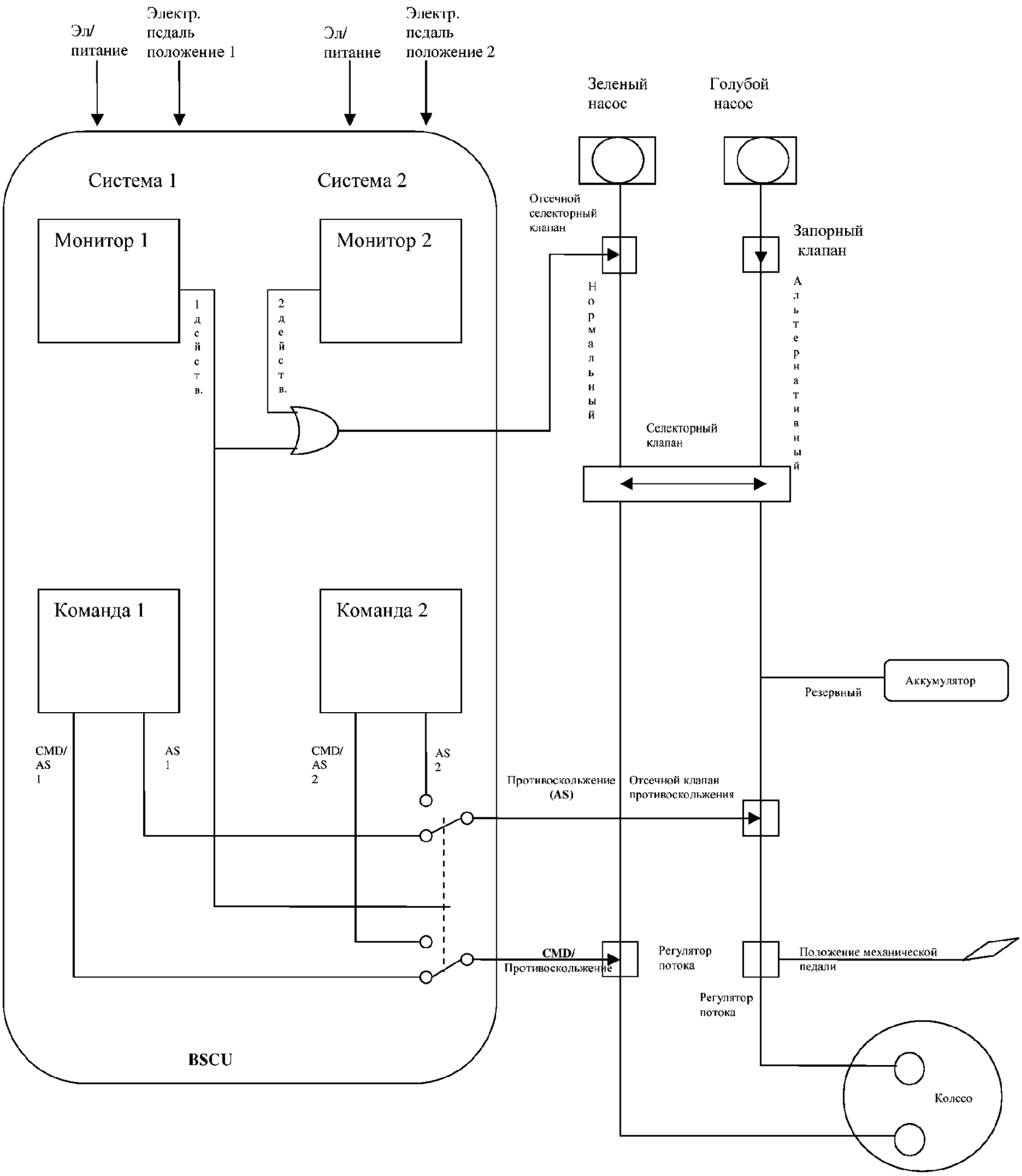
2) Спецификация BSCU

3.0 КРАТКОЕ ОПИСАНИЕ

Требования, предъявляемые к BSCU по работоспособности и целостности, приводят к предложению о том, чтобы BSCU состоял из двух независимых систем, отвечающих требованиям работоспособности, а также к предложению о том, чтобы каждая система содержала канал передачи команд/контроля для выполнения требований по целостности. Блок-схема предлагаемой архитектуры BSCU показана на рис. 3.0-1.

Каждая система BSCU генерирует необходимые напряжения в своем собственном электропитании. Предусмотрен контроль электропитания для выявления условий, выходящих за пределы напряжения, заданного спецификацией. Предусмотрены входные сигналы от тормозных педалей к командным и контрольным каналам, которые используются для расчета необходимых команд на торможение. Команды, генерируемые каждым каналом, сравниваются, и если они не согласуются, то выдается сообщение о неисправности. Результаты контроля электропитания и компаратора также представляются на монитор достоверности системы. Неисправность, о которой сообщается каждой системой в BSCU, приведет к тому, что система отключит свои выходные сигналы и переведет монитор достоверности системы в состояние недействительных значений. Предусмотрен монитор достоверности каждой системы BSCU для общего монитора достоверности BSCU. Отказ как системы 1, так и системы 2 приведет к тому, что селекторный клапан будет переведен на альтернативную систему торможения.

При нормальной работе BSCU системы 1 обеспечивает команды торможения и противоскольжения на колесные тормоза. Когда система 1 сообщает об отказе через монитор достоверности системы, то включается выход системы 2, если он работоспособен, на обеспечение этих команд. В том случае, когда последовательно выходит из строя система 2, все выходы BSCU выключаются, и монитор достоверности BSCU устанавливается в состояние недействительных значений.



(PSSA BSCU) Предлагаемая архитектура BSCU
Рис. 3.0-1

4.0 BSCU PSSA

4.1 Требования по безопасности BSCU

4.1.1 Входные данные PSSA

По результатам PSSA системы торможения колеса получен следующий комплект требований по безопасности.

1) Вероятность события «Отказ BSCU вызывает потерю команд на торможение» должна быть меньше 3,3E-5 на полет.
2) Вероятность «потери одиночного BSCU» должна быть меньше 5,75E-3 на полет.
3) Вероятность «непреднамеренного торможения из-за BSCU» должна быть меньше 2,5E-9 на полет.
4) Никакой одиночный отказ BSCU не должен приводить к «непредвиденному торможению».
5) BSCU должен быть спроектирован для уровня гарантии разработки A вследствие катастрофической классификации события «Непредвиденное торможение из-за BSCU».

Следующие условия эксплуатации самолета были обеспечены его изготовителем:

a. Средняя продолжительность полета – 5 часов

b. Средний интервал включения электропитания – 100 часов

c. Срок службы самолета – 100 000 часов

d. Время между V1 и полетом – 15 секунд (0,004167 часа)

План демонстрации того, каким образом BSCU будет отвечать требованиям безопасности, показан в таблице 4.1.1-1.

Таблица 4.1.1–1 (PSSA BSCU) Требования к безопасности BSCU/Конструктивные решения

Требование по безопасности	Конструктивные решения	Примечания
1. Вероятность события «Отказ BSCU вызывает потерю команд на торможение» должна быть меньше 3,3E-5 на полет.	Двухканальная конструкция BSCU.	Общая работоспособность системы BSCU может приемлемо отвечать этому требованию. См. FTA на рис. 4.2.1-1.
2. Вероятность «потери одиночного BSCU» должна быть меньше 5,75E-3 на полет.	Разработать для соответствующей надежности.	Нет
3. Вероятность «непреднамеренного торможения из-за BSCU» должна быть меньше 2,5E-9 на полет.	Каждая система BSCU содержит независимые командные и контрольные каналы.	Целостность BSCU может обеспечить выполнение этого требования. См. FTA на рис.4.2.1-2 PSSA BSCU FTA.
4. Никакой одиночный отказ BSCU не должен приводить к «непредвиденному торможению».	При этих условиях в результате не должно быть одиночного отказа.	При необходимости выполнить CMA и FMEA.
5. BSCU должен быть спроектирован для уровня гарантии разработки A вследствие катастрофической классификации события «Непредвиденное торможение из-за BSCU».	Разработать командный канал для уровня A обеспечения разработки и контрольный канал для уровня B.	Уровни обеспечения разработки заданы в соответствии с инструкциями, представленными в разделе 5.4 SAE ARP 4754.

4.2 Оценка отказного состояния

Были разработаны и оценены деревья неисправностей для отказных состояний потери BSCU и непреднамеренного торможения из-за BSCU для определения осуществимости предлагаемой конструкции BSCU. Были выполнены распределения вероятностей на основе всей имеющейся информации по конструкции и прошлого опыта.

(Примечание редактора: Здесь снова введено отказное состояние «непреднамеренное торможение колеса», поскольку оно предоставляет лучший пример демонстрации анализа общего режима BSCU, режимов отказов и анализа влияний).

4.2.1 PSSA системы BSCU – Анализ дерева неисправностей

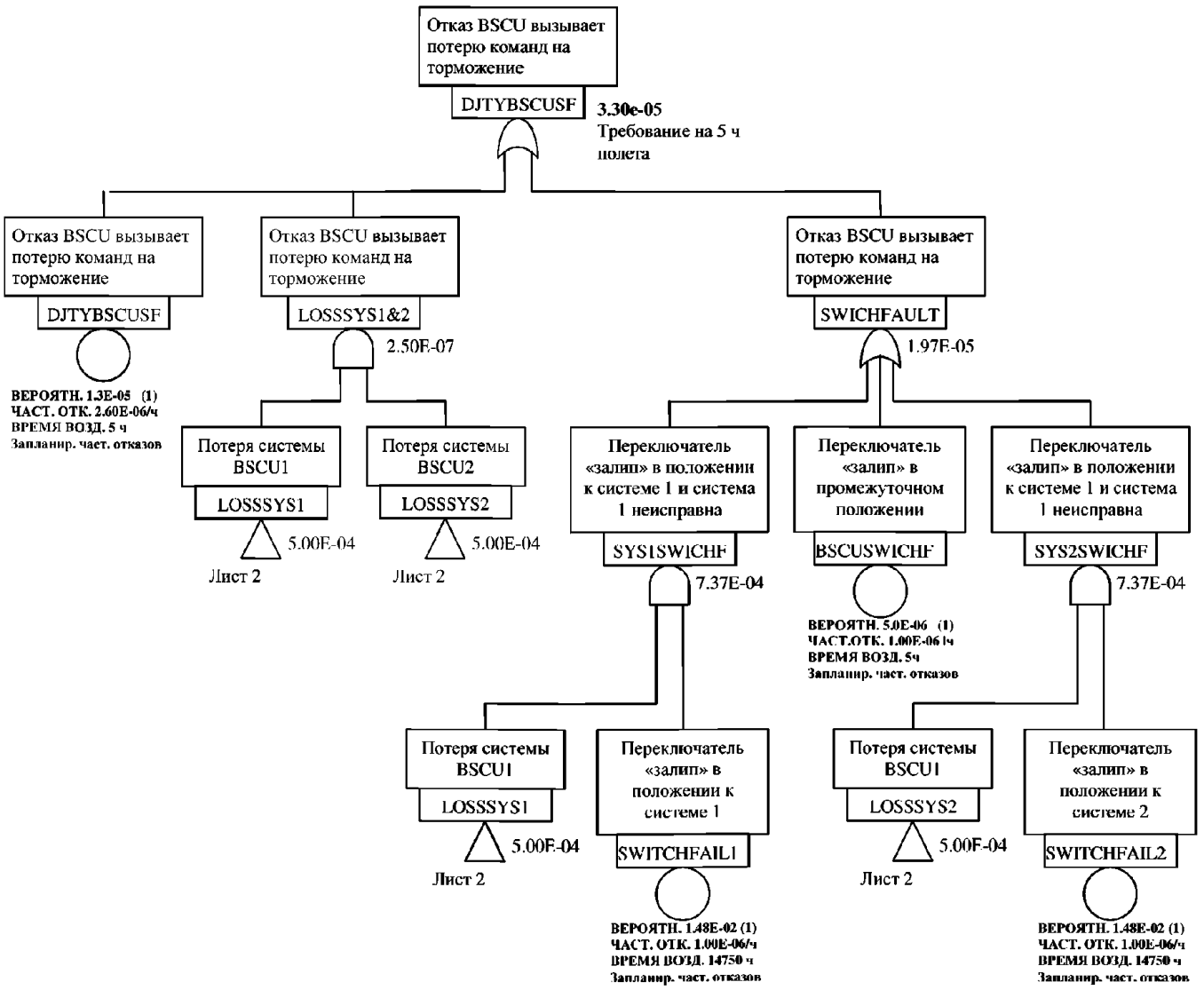
Дерево неисправностей на рис. 4.2.1-1 адресовано состоянию отказа "Потеря BSCU". Поставщик BSCU определил, что резервирование BSCU может быть выполнено посредством включения двух независимых систем BSCU в одиночном BSCU, с устройством монитора/переключения, выбирающего достоверную команду для направления ее к тормозной системе. Как изображено на дереве неисправностей, потеря всей работы BSCU возникает в том случае, когда происходит отказ монитора достоверности BSCU, так что он сообщает недостоверную информацию об отказе обоих BSCU (монитора достоверности BSCU неправильно сообщает о двойном отказе), когда обе системы 1 и 2 BSCU неисправны в одном и том же полете (системы 1 и 2 BSCU не работают), или когда возникает индивидуальная неисправность переключателя вместе с неисправностью выбранного канала (неисправность переключателя способствует потере команд BSCU на торможение). Далее, дерево неисправностей отображает комбинации возможностей неисправности переключателя BSCU и сопровождающих неисправностей системы BSCU, приводящих к потере торможения. Это дерево также показывает разбиение и планирование частоты отказов для вклада в неисправность BSCU одиночной системы либо от расчетного канала, либо от электропитания.

Дерево неисправностей на рис. 4.2.1-2 адресовано непреднамеренному торможению колеса, вызванного BSCU. BSCU может вызвать непреднамеренное торможение только в том случае, когда используется нормальная система торможения. Это дерево неисправностей не относится к аспектам анализа на уровне самолета. В дереве неисправностей предполагается, что не существует не обнаруживаемых неисправностей BSCU, которые могут вызвать команду на непреднамеренное торможение. Для того чтобы отвечать требованиям, данное допущение должно быть проверено на правильность посредством FMEA и/или CMA. Другая ветвь дерева отказов относится к комбинациям контролируемых неисправностей BSCU и неисправностей монитора. Выявляемыми отказами BSCU являются отказы электропитания, которые приводят к отклонению напряжения от значений, заданных в спецификации, выявляемого при помощи монитора электропитания, и к неисправностям входа/выхода командного канала или центрального процессора, что вызывает команду на непреднамеренное торможение, которая выявляется при помощи компаратора. Отказы входа/выхода монитора и центрального процессора не включаются в дерево неисправностей, поскольку контрольный канал не обеспечивает команды на торможение. Неисправности контрольного канала приведут к тому, что компаратор сообщит о неисправности и переключит команды на торможение на другую систему BSCU, если компаратор работает. Если компаратор не работает, то неисправность контрольного канала все равно не приведет к непреднамеренному торможению.

Поскольку система 1 BSCU обычно является активным каналом, то дерево неисправностей (лист 2) демонстрирует то, что не выявленные неисправности электропитания системы 1 могут способствовать непреднамеренному торможению, так как может отказать вычислительный канал. Дерево неисправностей на листе 3 содержит ту же самую информацию о неисправности BSCU, относящуюся к системе 2 BSCU, однако система 2 не может быть применена для тормозов пока не будет активизирован монитор/селекторный переключатель; таким образом, событие нахождения переключателя в положении 2 добавляется неисправностями системы 2. Результатом активизации переключателя могут быть два состояния: предыдущая выявленная неисправность системы 1, или независимая неисправность монитора/переключателя.

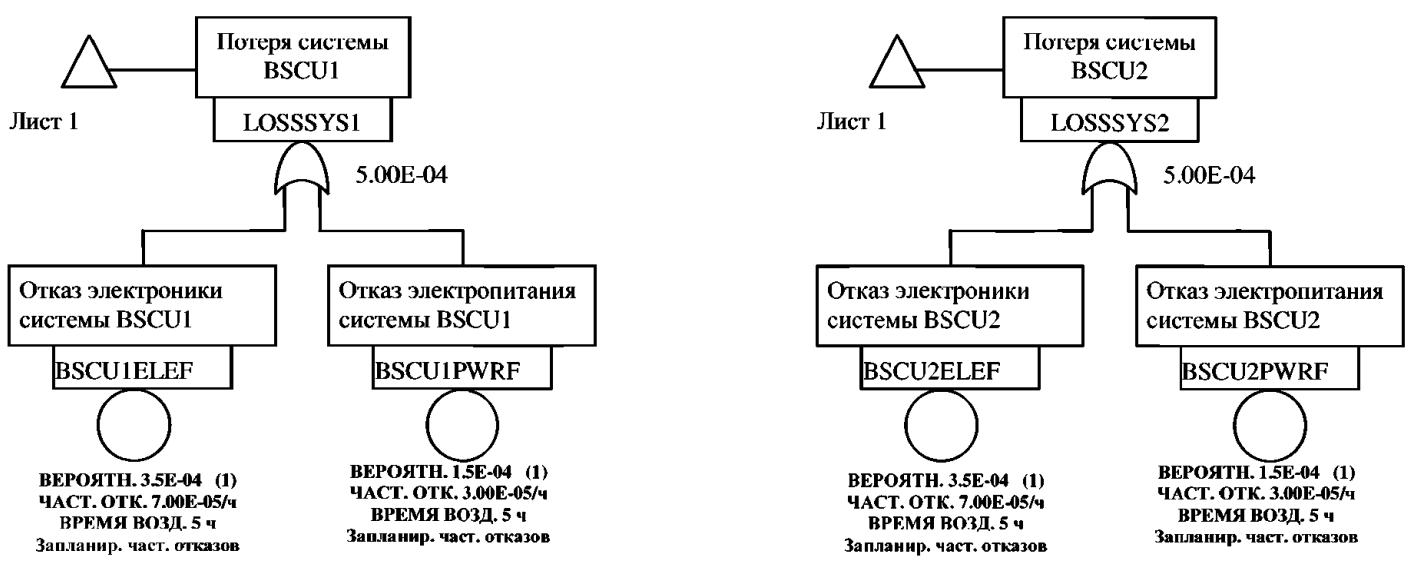
Примечание редактора: FTA «Потери торможения всех колес» использовался изготовителем авиационной конструкции для разработки требований к поставщику BSCU. Поставщик BSCU провел экспертизу требований для двух BSCU и определил, что достаточно будет иметь один BSCU с двумя внутренними системами. Поставщик BSCU разработал следующее дерево неисправностей BSCU PSSA, начиная с основного события «Отказ BSCU вызывает потерю команд на торможение» из PSSA FTA системы торможения колеса.

Для скрытых неисправностей переключателя было запланировано время воздействия 14750 часов. Это минимальное время воздействия, которое обеспечивает выполнение требования к вероятности верхнего уровня.

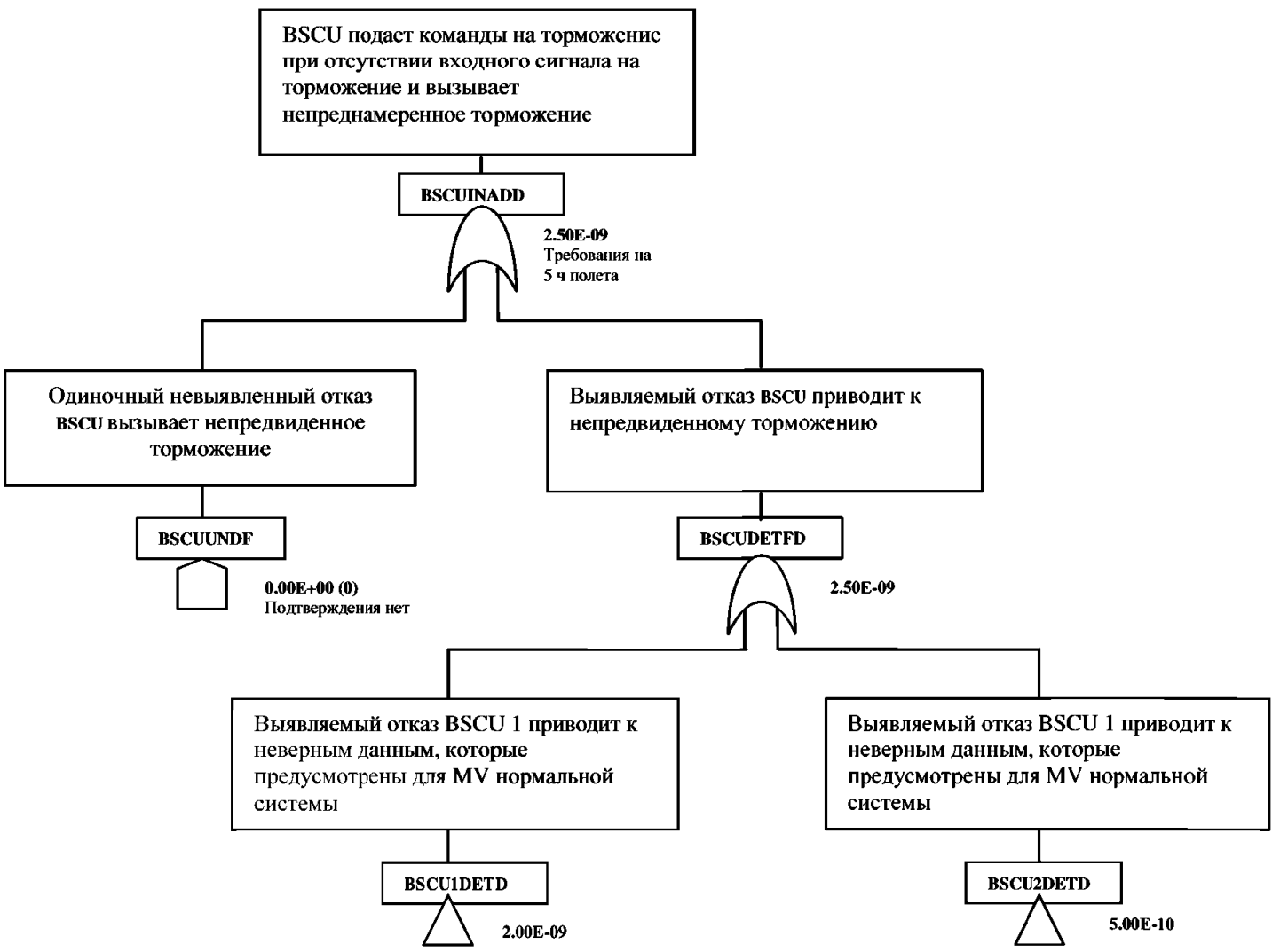


(PSSA BSCU – FTA)
Дерево неисправностей события «Отказ BSCU вызывает потерю команд на торможение»
Рис. 4.2.1-1 (лист 1 из 2)

Примечание редактора: Данный уровень информации обычно не должен представляться на данном дереве неисправностей, поскольку возможно показать, что эти требования выполняются с использованием общей частоты отказов BSCU. Информация по режимам отказов BSCU включена в данный пример для того, чтобы проиллюстрировать особенности Марковского анализа.

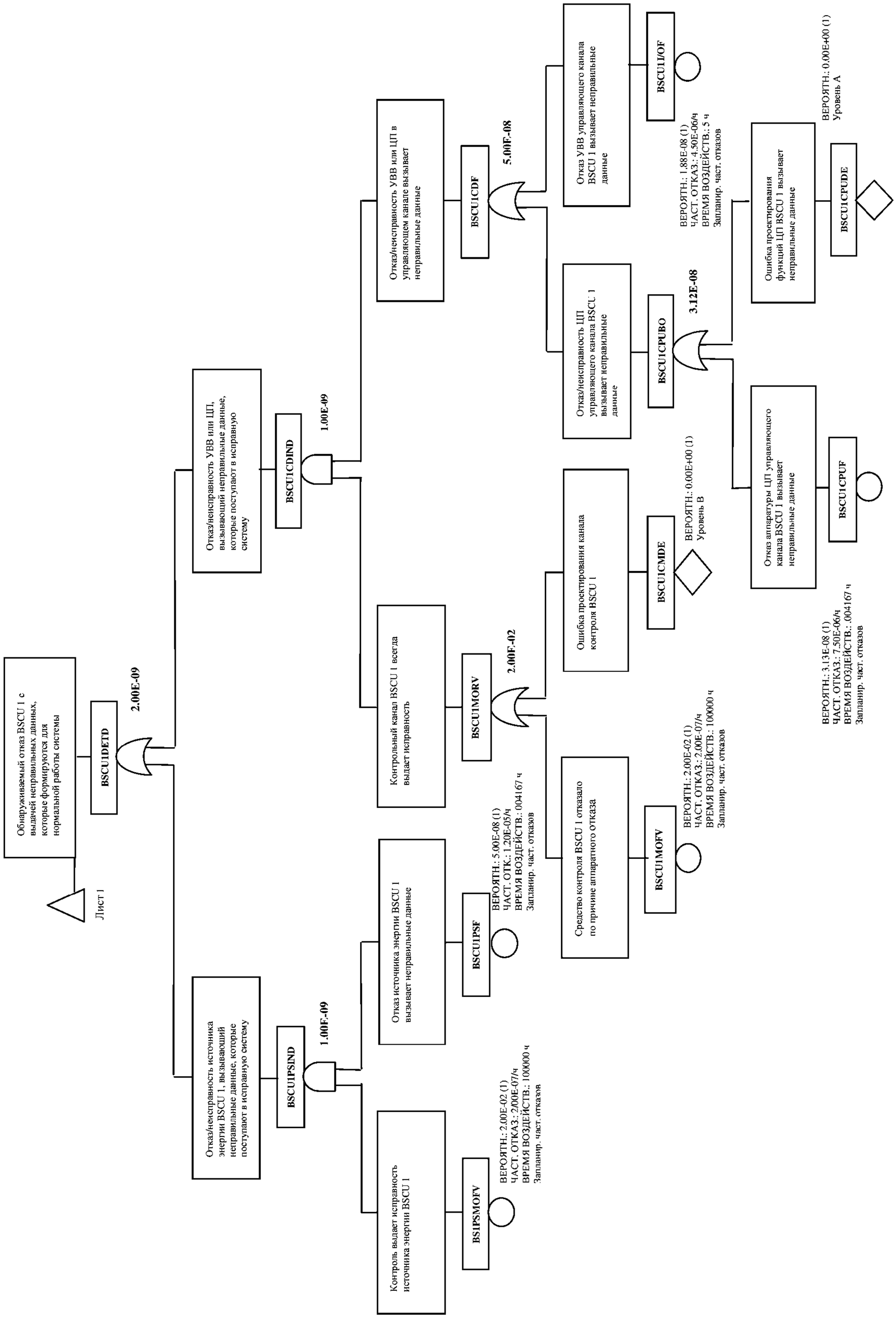


(PSSA BSCU – FTA)
Дерево неисправностей события «Отказ BSCU вызывает потерю команд на торможение»
Рис. 4.2.1-1 (лист 2 из 2)

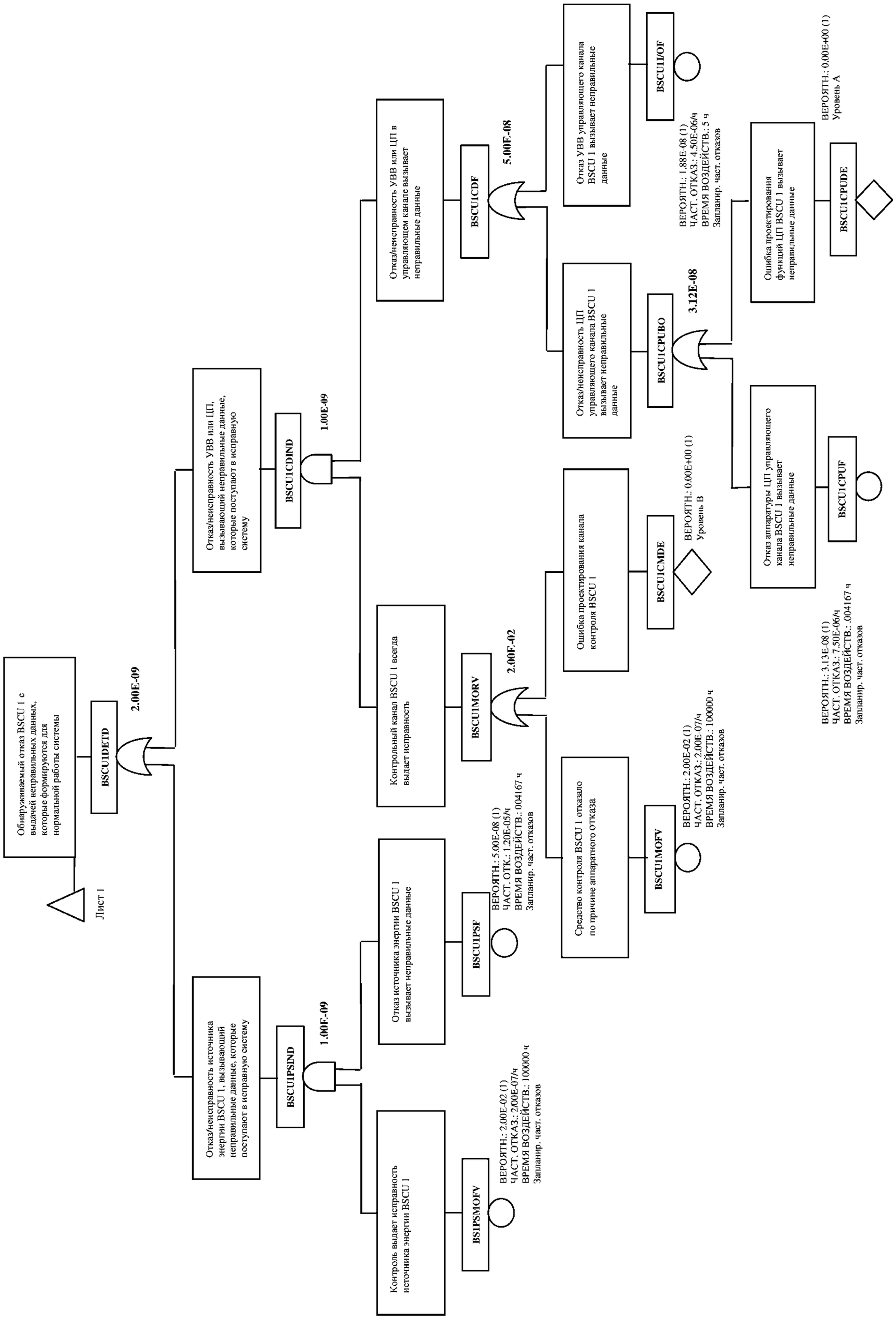


Лист 2 Лист 3

(PSSA BSCU – FTA)
Дерево неисправностей события «BSCU подает команды на торможение
при отсутствии входного сигнала на торможение
и вызывает непреднамеренное торможение»
Рис. 4.2.1-2 (лист 1 из 3)



(PSSA BSCU – FTA)
Дерево неисправностей события «BSCU подает команды на торможение при отсутствии входного сигнала на торможение и вызывает непреднамеренное торможение»
Рис. 4.2.1-2 (лист 2 из 3)



(PSSA BSCU – FTA)
Дерево неисправностей события «BSCU подает команды на торможение
при отсутствии входного сигнала на торможение и вызывает непреднамеренное торможение»
Рис. 4.2.1-2 (лист 3 из 3)

4.2.2 PSSA системы BSCU – Анализ логической схемы

(Примечание редактора: Обычно в анализ должно включаться текстовое описание разработки DD. Данный текст будет аналогичен тому, который включен в предыдущий пример FTA).

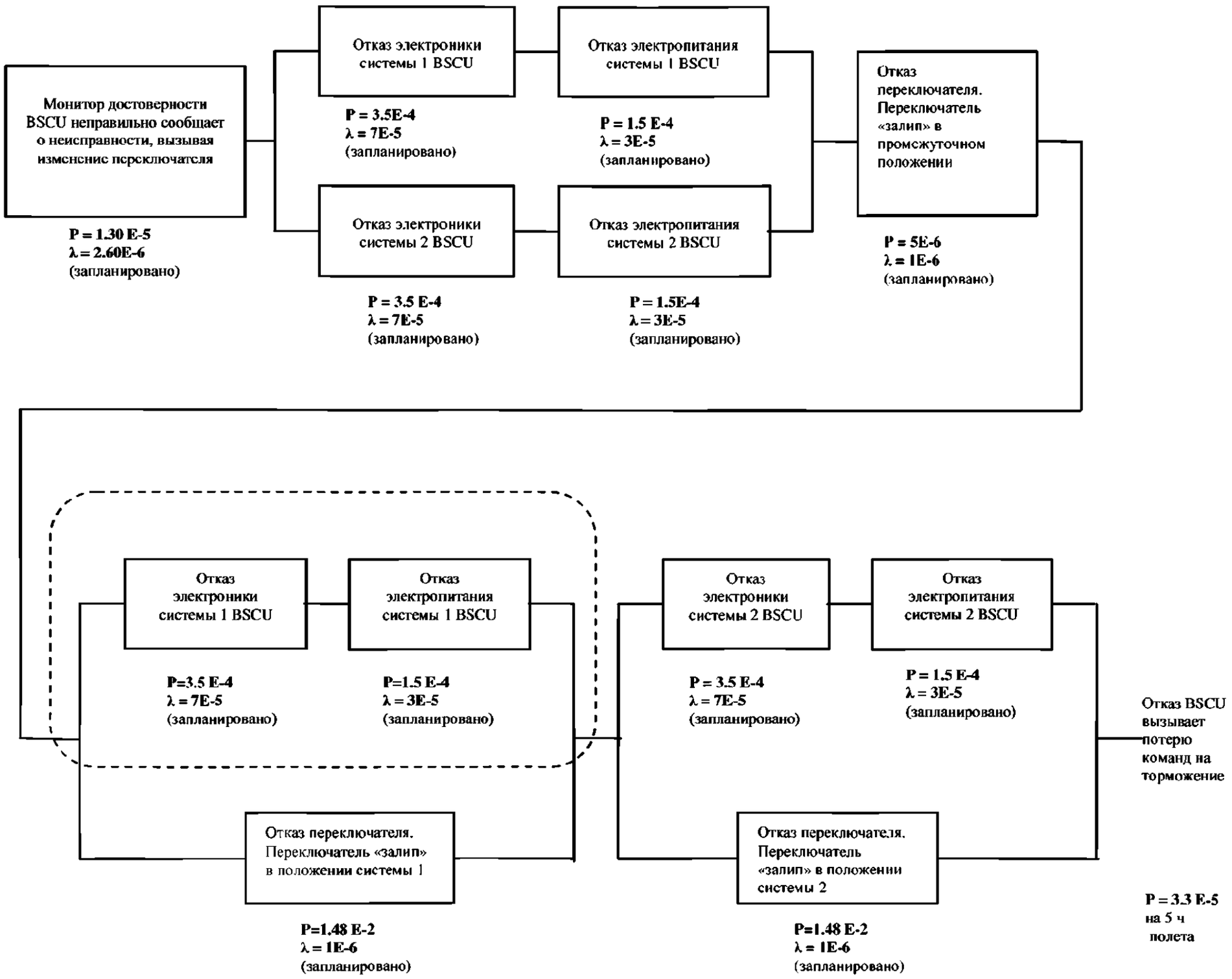
Схема на рис. 4.2.2-1 адресована состоянию отказа «Потеря BSCU». Потеря всей работы BSCU возникает в том случае, когда происходит отказ монитора достоверности BSCU, так что он неправильно сообщает о неисправности обоих BSCU, или когда происходит отказ систем 1 и 2 BSCU.

Схема на рис. 4.2.2-2 адресована непреднамеренному торможению колес, вызванному BSCU. BSCU может вызвать непреднамеренное торможение только в том случае, когда используется нормальная система торможения. Данная схема не имеет отношения к данному аспекту анализа на уровне самолета. Схема предполагает, что нет не обнаруживаемых неисправностей BSCU, которые могут вызвать команду на непреднамеренное торможение. Для того чтобы отвечать требованиям, данное допущение должно быть проверено на правильность посредством FMEA и/или CMA. Схема относится к комбинациям контролируемых неисправностей BSCU и неисправностей монитора.

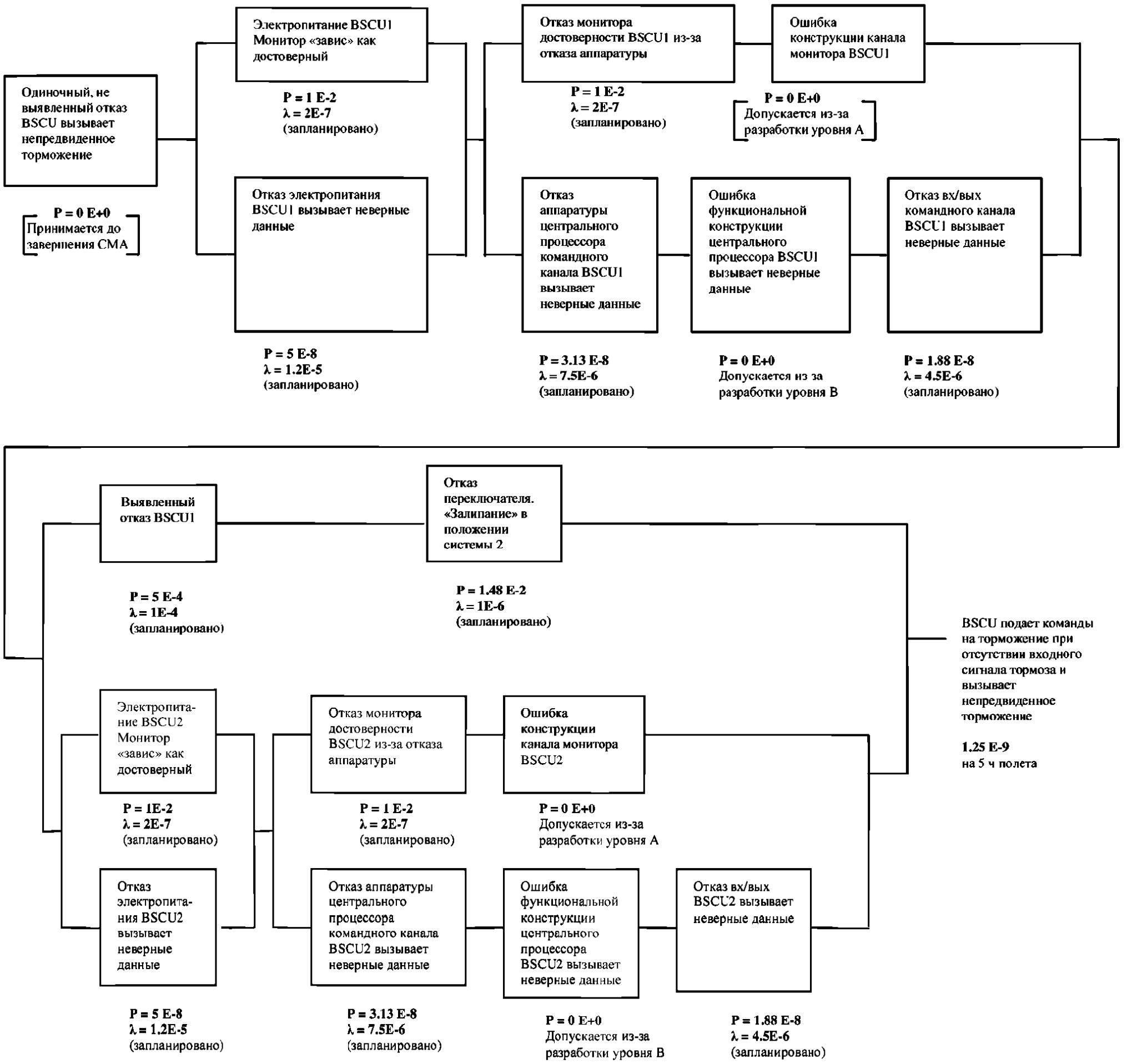
(Примечание редактора: DD «Потеря торможения всех колес» использовался изготовителем авиационной конструкции для разработки требований к поставщику BSCU. Поставщик BSCU провел экспертизу требований для двух BSCU и определил, что достаточно будет иметь один BSCU с двумя внутренними системами. Поставщик BSCU разработал следующую BSCU PSSA DD, начиная с основного события «Отказ BSCU вызывает потерю команд на торможение» из PSSA DD системы торможения колеса.

Для скрытых неисправностей переключателя было запланировано время воздействия 14750 часов. Это минимальное время воздействия, которое обеспечивает выполнение требования к вероятности верхнего уровня.

Данный уровень информации обычно не должен представляться на данном DD, поскольку можно показать, что эти требования выполняются с использованием общей частоты отказов BSCU. Информация по режимам отказов BSCU включена в данный пример для того, чтобы проиллюстрировать особенности Марковского анализа.



(PSSA BSCU – DD)
Логическая схема события «Отказ BSCU вызывает потерю команд на торможение»
Рис. 4.2.2-1



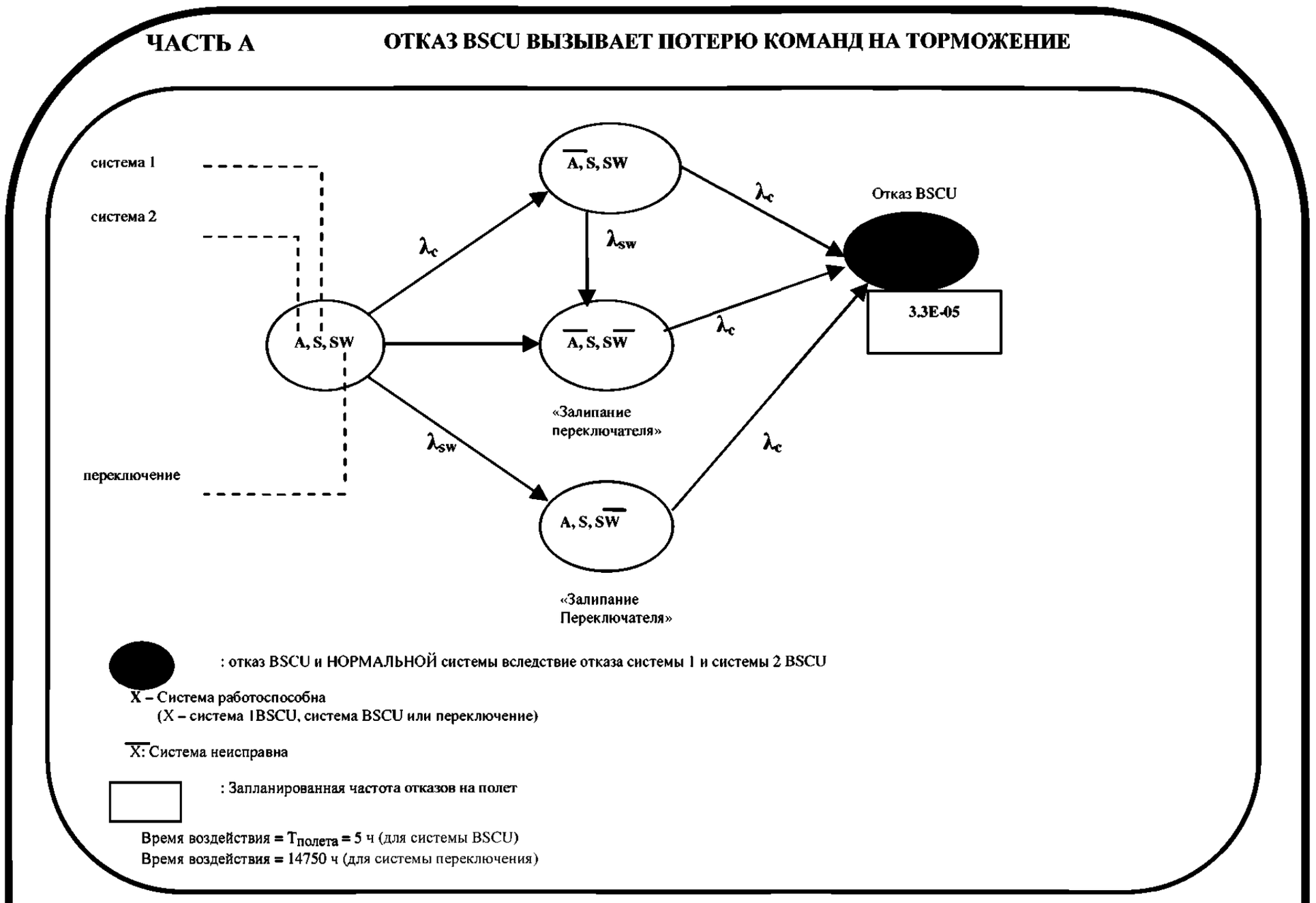
(PSSA BSCU – DD)
Логическая схема события «BSCU подает команды на торможение
при отсутствии входного сигнала тормоза и вызывает непреднамеренное торможение»
Рис. 4.2.2-2

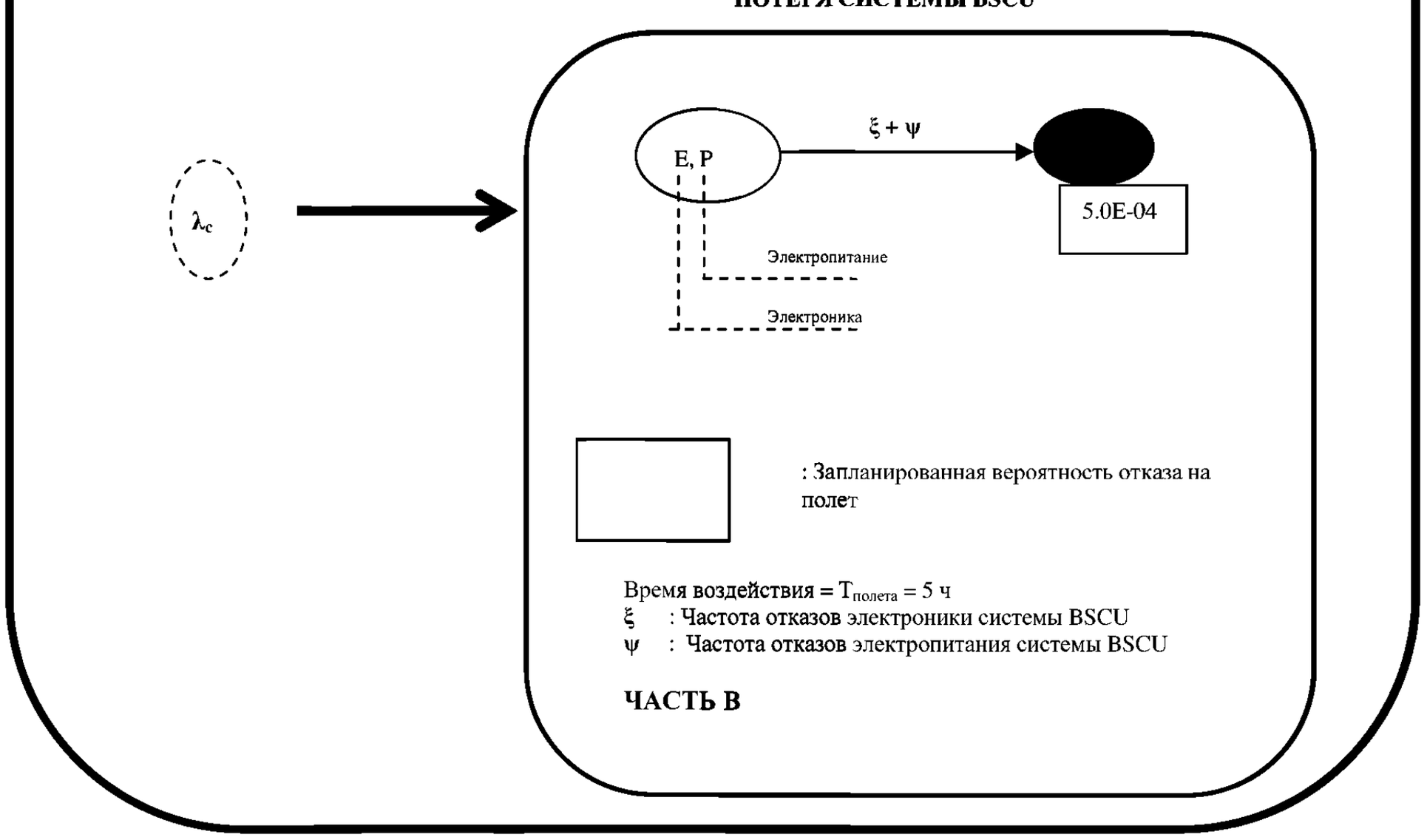
4.2.3 PSSA системы BSCU – Марковский анализ

Марковский анализ для события «Отказ BSCU вызывает потерю команд на торможение», включая механизм переключения, показан на рис. 4.2.3-1 (часть A). В цепи Маркова каждое состояние представляется тройной группой (A, S, SW), где «A» является состоянием активного компьютера BSCU, который может быть либо BSCU 1, либо BSCU 2. «S» является состоянием резервного компьютера BSCU, а «SW» – состоянием переключателя. Предполагается, что каждый компонент находится в работоспособном или неисправном состоянии. Неисправные состояния представлены полосой на верху символа. Как активный, так и резервный компьютеры BSCU могут отказать только в одном режиме. Система переключения может отказать в двух различных режимах, либо залипание при соединении с активным компьютером, либо залипание в разомкнутом состоянии (без подключения ни к одному из компьютеров BSCU). Предполагается, что система BSCU должна отказать, когда в полете отказывают либо оба компьютера, либо система переключения не может выполнить переключение от активной системы на резервную, когда активная система отказывает в полете. На рис. 4.2.3-1 (часть B) показана расширенная Марковская модель для неисправности системы BSCU. Предполагается, что система BSCU должна отказать в любом случае, когда отказывает электроника BSCU или электропитание BSCU. Отказ обоих этих блоков представлен простым переходом в Марковской цепи на рис. 4.2.3-1 (часть B).

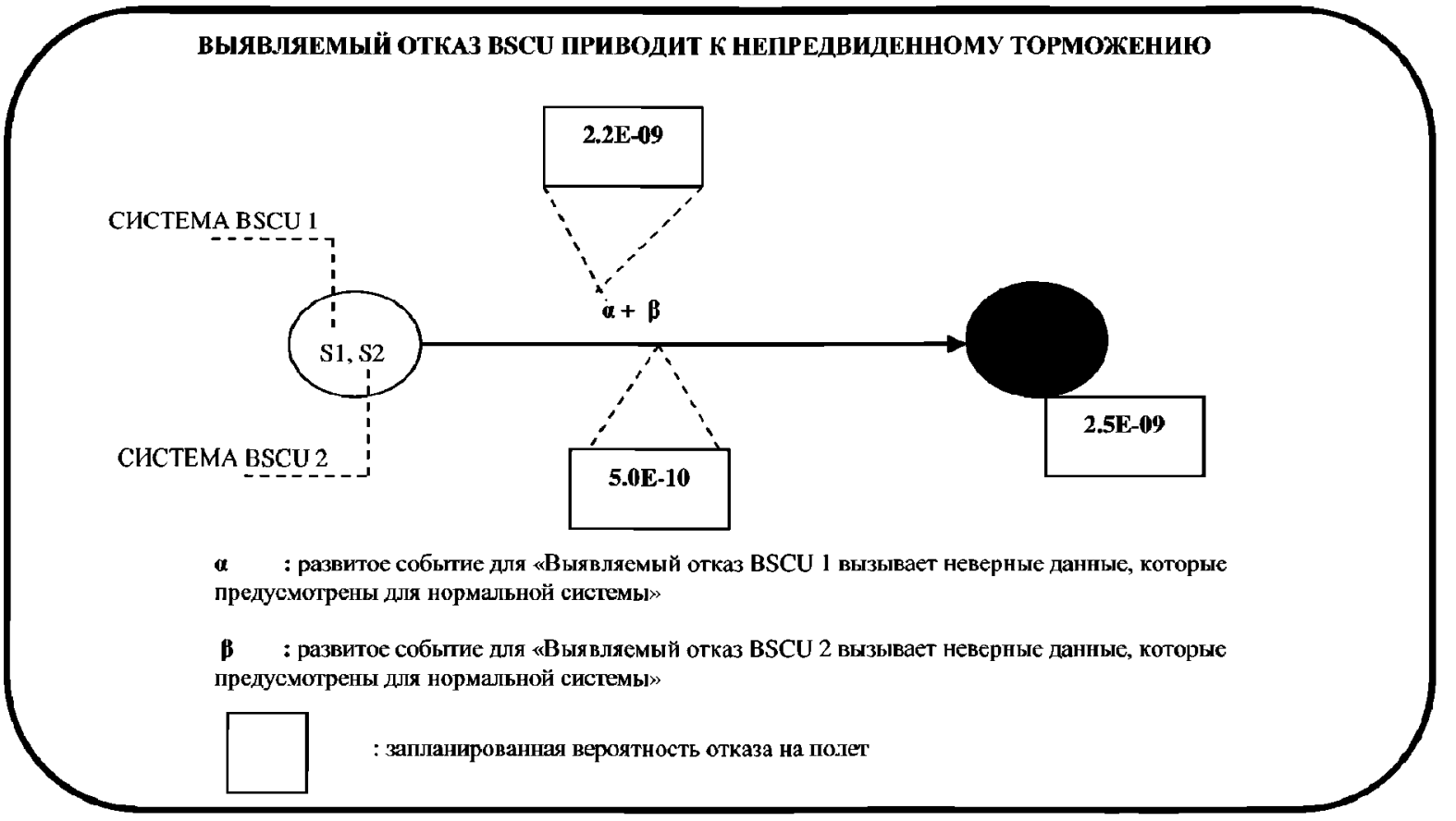
На рис. 4.2.3-2 показана «Выявляемая неисправность BSCU, приводящая в результате к непреднамеренному торможению». Непреднамеренное торможение возникает в том случае, когда происходит отказ как монитора, так и активной системы в любой системе BSCU. Непреднамеренное торможение из-за неисправности системы BSCU 1 показано на рис. 4.2.3-3. В этом случае каждое состояние представляется группой из четырех элементов (A, B, C, D). Первая и третья группы в каждом состоянии соответствуют центральному процессору и входу/выходу системы BSCU и электропитанию. Вторая и четвертая группы в каждом состоянии соответствуют монитору центрального процессора и входа/выхода и монитору электропитания. Непреднамеренное торможение возникает в том случае, когда оба центральных процессора и их монитор отказывают, или когда происходит отказ электропитания и его монитора. Запланированная величина вероятности непреднамеренного торможения из-за неисправности системы BSCU 1 равна 2E-9.

Непреднамеренное торможение из-за неисправности системы BSCU 2 и неисправность механизма переключения показаны на рис. 4.2.3-4. Марковская модель на рис. 4.2.3-4 является той же самой, что и Марковская модель для системы BSCU 1 (рис. 4.2.3-3) за исключением того, что к модели добавлен новый режим отказа для учета механизма переключения. Это неисправность механизма переключения показана на рис. 4.2.3-3 с вероятностью отказа, равной 2,5E-1. Следовательно, общая запланированная вероятность непреднамеренного торможения из-за неисправности системы BSCU 2 равна (2E-9)x(2,5E-1) = 5E-10.

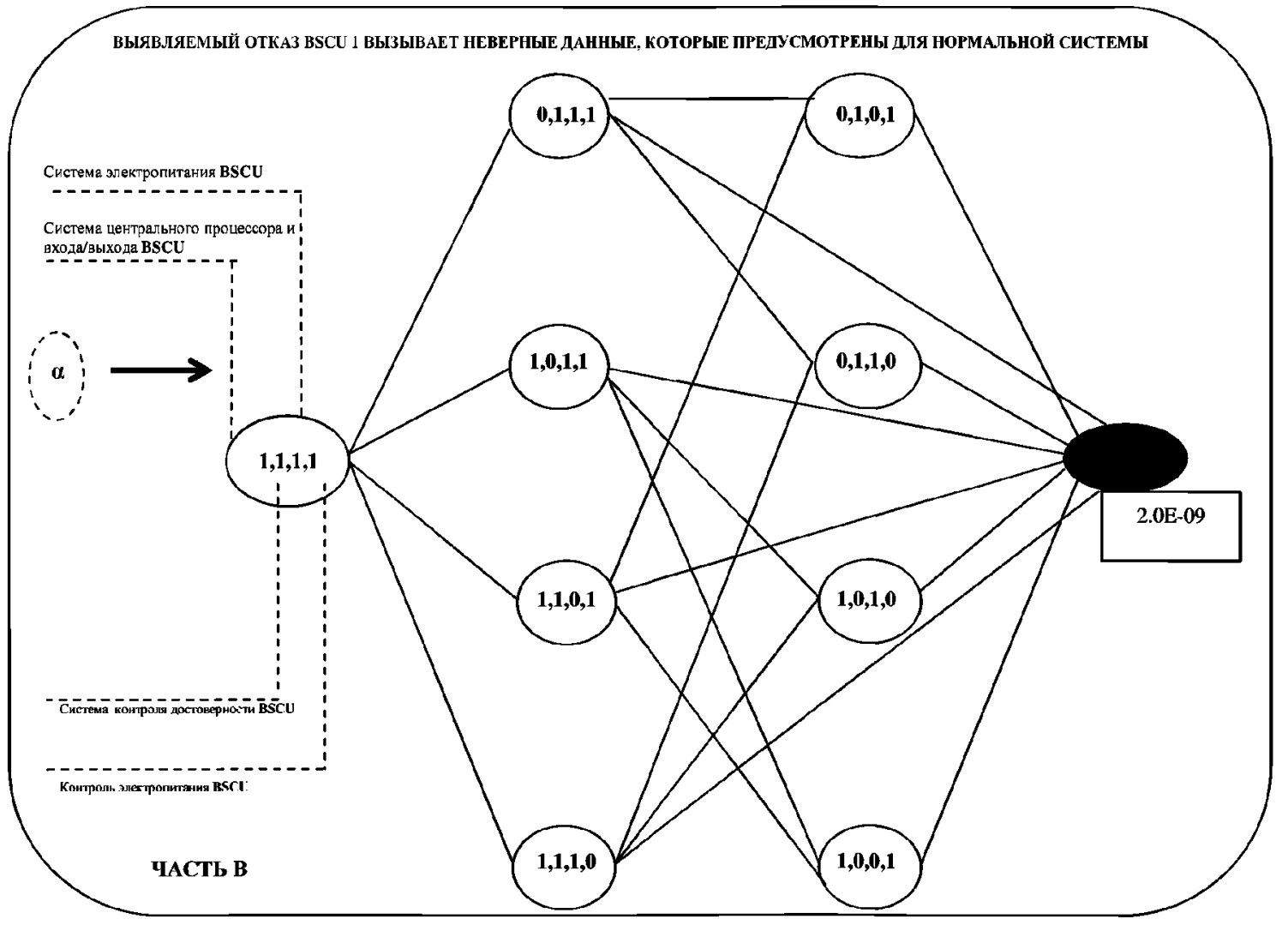




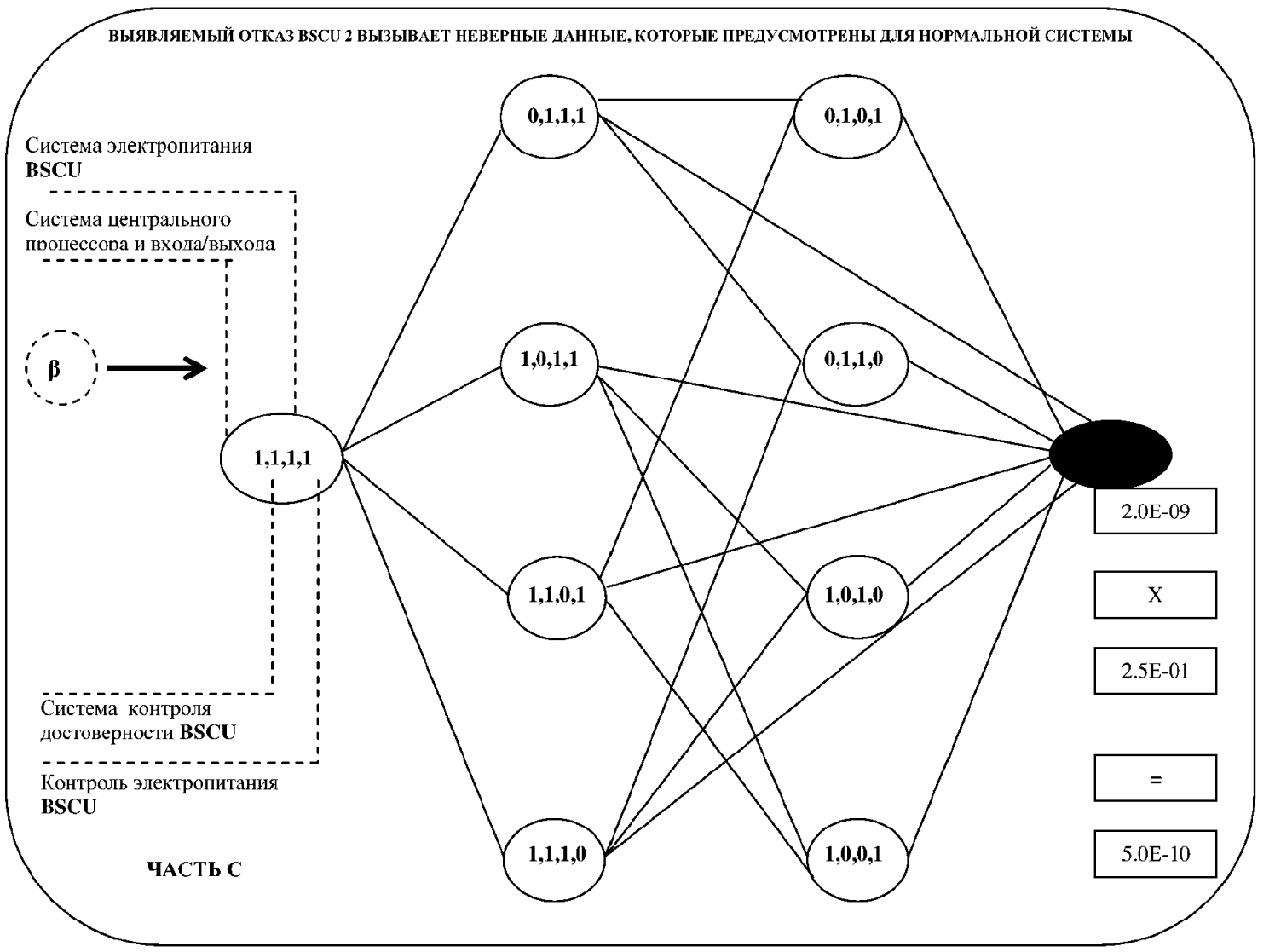
(PSSA BSCU – MA)
MA «Отказ BSCU вызывает потерю команд на торможение»
Рис. 4.2.3-1



(PSSA BSCU – MA)
MA «Выявляемый отказ BSCU вызывает непреднамеренное торможение»
Рис. 4.2.3-2



(PSSA BSCU – MA)
MA «Непреднамеренное торможение из-за неисправности системы BSCU 1»
Рис. 4.2.3-3



(PSSA BSCU – MA)
MA «Непреднамеренное торможение из-за неисправности системы BSCU 2 и неисправности системы переключения»
Рис. 4.2.3-4

4.3 Установленные требования

В результате оценки состояния неисправности были получены следующие требования нижнего уровня.

4.3.1 Требования к установке

Для каждой системы BSCU требуется источник электропитания, независимый от источника электропитания другой системы.

4.3.2 Требования к аппаратным и программным средствам

Были получены следующие требования к аппаратным и программным средствам BSCU, которые должны выполняться для обеспечения общих целей безопасности.

1) Каждая система BSCU должна иметь целевую интенсивность отказов менее 1E-4 1/час.

2) Должны выполняться целевые вероятности для первичных событий отказов дерева неисправностей, показанных на рис. 4.2.1-1 и 4.2.1-2.

Примечание: *Любые события, которые не удовлетворяют данным целевым вероятностям, должны быть утверждены группой системного проектирования до перехода к разработке.*

3) Не должно быть не обнаружимых неисправностей BSCU, которые могут вызвать непреднамеренное торможение.

4) Не должно быть отказов общего режима командного и контрольного каналов системы BSCU, которые могут привести их к тому, что они одновременно выдадут одни и те же неправильные команды на торможение.

5) *Контрольный канал BSCU должен быть разработан для уровня гарантии разработки A.

6) *Командный канал BSCU должен быть разработан для уровня гарантии разработки B.

** (Примечание редактора: Эти назначения можно поменять, задав уровень A обеспечения разработки для командного канала, а уровень B – для контрольного канала).*

4.3.3 Требования по безопасности к техническому обслуживанию

Переключатель, который выбирает систему 1 или систему 2, должен проверяться с интервалом не более 14750 часов.

5.0 ЗАКЛЮЧЕНИЕ

Как показано, теперь конструкция выглядит как удовлетворяющая требованиям к безопасности, определенным в PSSA системы тормоза колеса. Были определены дальнейшие требования к установке, аппаратным и программным средствам, и задачам технического обслуживания, и они переданы соответствующей организации, отвечающей за конструкцию. Требуется провести анализ режимов отказов и эффектов, и анализы общего режима для проверки того, что данная конструкция отвечает требованиям.

(Примечание редактора: В этом месте примера предполагается, что PSSA достаточно разработан для выполнения рабочего проекта. Данный пример подводит итог последующему выполнению рабочего проекта и разрабатывает SSA для обеспечения сертификации. Как представлено на рис. 3 основного текста данного документа, процесс SSA начинается как восходящий анализ на уровне изделия).

Режимы отказа электропитания BSCU и анализ влияний (FMEA)

(Примечание редактора: Данный пример FMEA упрощен за счет ограничения FMEA электропитанием BSCU. На самом деле FMEA может быть затребован на любом уровне от всей системы до небольшой части цепи, выполняющей одну функцию внутри LRU).

1.0 ВВЕДЕНИЕ

(Примечание редактора: В целях данного примера предполагается, что FMEA был выбран для обеспечения SSA FTA. Для процесса и формата FMEA может потребоваться небольшое изменение для обеспечения методологий DD или MA; тем не менее, основные шаги и принципы сохраняются).

Данный FMEA адресован электропитанию BSCU для обеспечения основных событий и целей безопасности, определенных в предварительном FTA события «НЕПРЕДНАМЕРЕННОЕ ТОРМОЖЕНИЕ КОЛЕСА ПОСЛЕ V1», затребованном в ссылке 2.

Данный отчет FMEA дает количественное представление окончательной FTA, представляя частоты отказов для основных событий. Основными событиями FTA, поддерживаемыми данным FMEA, являются «Отказ электропитания BSCU вызывает неправильные данные», «Монитор электропитания BSCU становится недостоверным» и вклад электропитания в событие «Не выявленный отказ BSCU вызывает непреднамеренное торможение». Данный анализ был проведен по выпущенной окончательной документации на конструкцию BSCU и по рабочим чертежам. Данный FMEA будет являться частью вспомогательной документации как для SSA BSCU, так и для SSA системы колесного тормоза.

Требуемый FMEA выполнен в виде двух частей. Функциональный FMEA был проведен для электропитания, а компонентный FMEA был проведен для монитора электропитания, который представляет собой часть системы электропитания. Компонентный FMEA был проведен после того как умеренные результаты функционального FMEA не отвечали целям безопасности.

(Примечание редактора: В таблице перекрестных ссылок, представленной ниже, дана связь каждого параграфа примера с соответствующим параграфом приложения FMEA).

№ параграфа FMEA самолета	№ параграфа приложения G
4.1	G.3.2.1
4.2	G.3.2.2

2.0 ССЫЛКИ

(Примечание редактора: Информация, представленная в этих ссылках, составляет значительную часть документации, требуемую до начала FMEA. См. раздел G.2.7)

1) P4761 «Руководство по методам оценки безопасности бортового оборудования самолетов гражданской авиации».
2) Внутренняя памятка, требующая обеспечения FMEA для дерева неисправностей «Непредвиденное торможение после V1» для самолета S18, включая систему BSCU.
3) Выпущенная конструкторская и технологическая документация на BSCU.
4) MIL-HDBK-217F «Прогноз надежности электронного оборудования».
5) Внутренняя памятка, определяющая режимы отказов компонентов, которые должны использоваться для BSCU FMEA.
6) Результаты лабораторного анализа «Потери фильтрации или пониженной фильтрации».

3.0 ОПИСАНИЕ ЭЛЕКТРОПИТАНИЯ

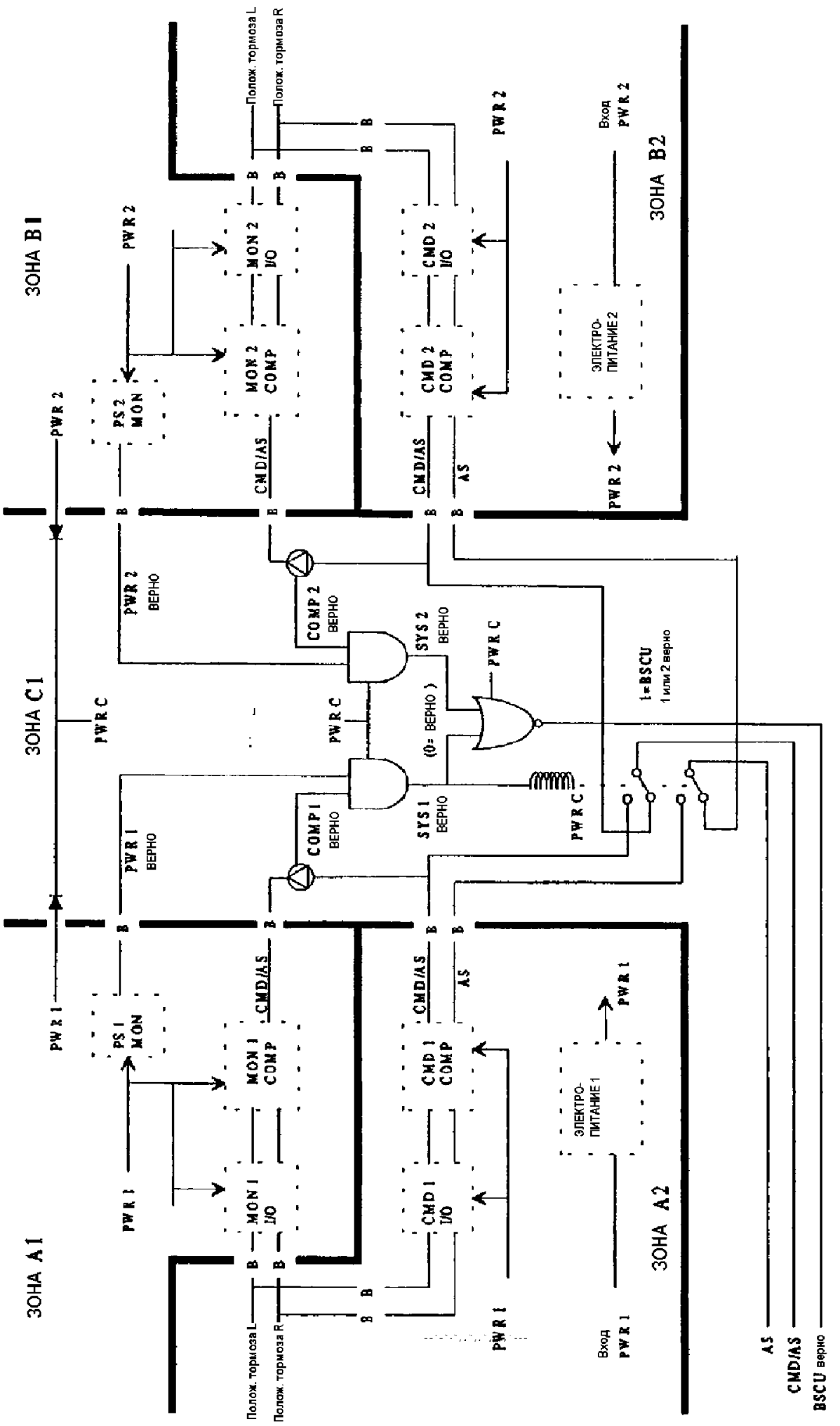
(Примечание редактора: Частью подготовки к FMEA является понимание работы функции. В соответствии с описанием, представленным в G2.1, в отчет должен быть включен краткий обзор работы).

Дан обзор исполнения электропитания BSCU, описанного в ссылке 3. Установлено, что конструкция источников электропитания BSCU 1 и 2 является идентичной. Исполнение выполнено при помощи идентичной конструкции источников электропитания, расположенных в физически разделенных зонах платы модульной конструкции BSCU, как это изображено на схеме архитектуры BSCU на рис. 3.0-1. В каждой системе BSCU функции электропитания и контроля электропитания расположены физически независимо.

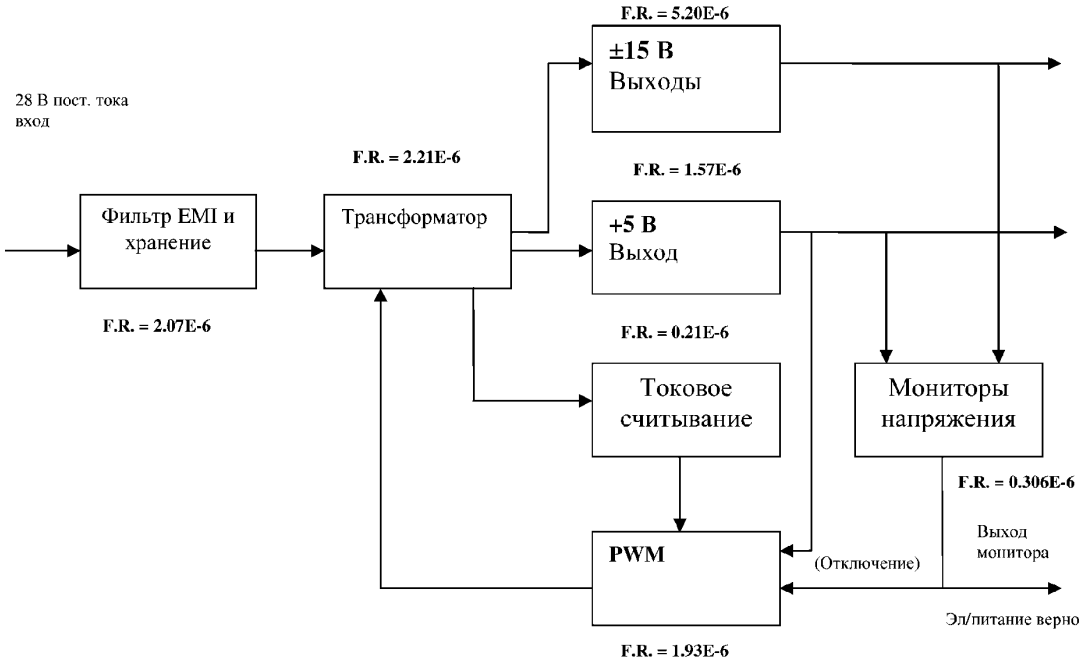
Конструкция электропитания представлена в виде блок-схемы на рис. 3.0-2. Подробная схема конструкции монитора +5 В представлена на рис. 3.0-3.

Электропитание BSCU имеет стандартную конструкцию и представлено в техническом описании аппаратуры BSCU.

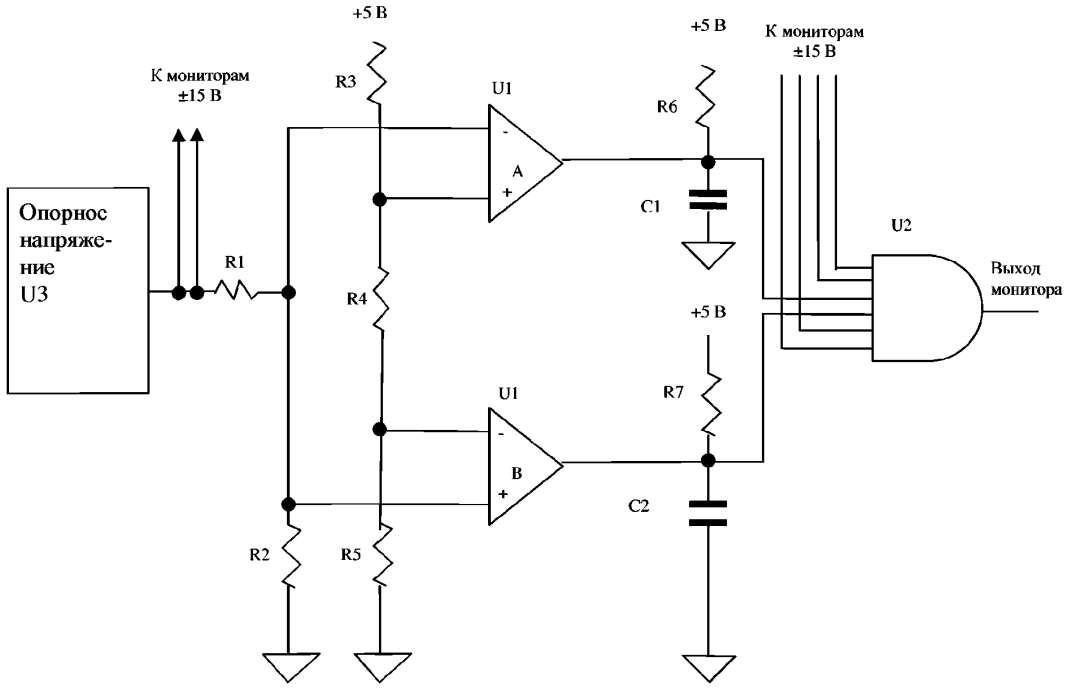
Мониторы электропитания представляют собой двухпороговые компараторы. Как +5, так и +15 В контролируются по верхним и нижним предельным отклонениям напряжения. Выходы соединены вместе, так что если какое-либо напряжение превышает точку отключения (верхнюю или нижнюю), то выходной сигнал монитора отклоняется.



(SSA BSCU – FMEA)
Физическое исполнение BSCU
Рис. 3.0-1



(SSA BSCU – FMEA)
Блок-схема электропитания
Рис. 3.0-2



(SSA BSCU – FMEA)
Схема монитора электропитания
Рис. 3.0-3

Примечание: *Монитор ± 15 В использует то же самое опорное напряжение и схему мониторинга.*

4.0 ПОДРОБНЫЙ АНАЛИЗ ЭЛЕКТРОПИТАНИЯ И ЕГО РЕЗУЛЬТАТЫ

Данный FMEA состоит из двух разделов. Раздел 4.1 представляет собой функциональный FMEA, выполненный для всего электропитания. Функциональный FMEA монитора электропитания был удален из раздела функционального FMEA, поскольку он заменен компонентным FMEA, представленным в разделе 4.2.

4.1 Функциональный FMEA

Исходный анализ электропитания был проведен при помощи расчета интенсивности отказов всего электропитания на основе подсчетов деталей или интенсивности отказов. Консервативный анализ не отвечает требованиям запланированных значений для события «Не обнаруживаемый отказ электропитания приводит к непреднамеренному торможению». Следовательно, функциональный FMEA был проведен для обеспечения лучшего разрешения по интенсивности отказов различных режимов отказов. «Потерей фильтрации/пониженной фильтрацией» является только такой отказ, который может привести к неправильным данным и не может быть выявлен монитором электропитания, который функционирует должным образом. Этот режим отказа может вызвать повышенные пульсации выходного напряжения, которые могут быть на таком уровне и с такой частотой, которые не обнаруживаются монитором. В таблице 4.1-1 представлены результаты функционального FMEA.

(Примечание редактора: Подробно показан только анализ блока +5 В. Результаты FMEA остальной части электропитания включены в краткое описание. Это сделано с целью удаления страниц с таблицами, которые не нужны для представительного примера функционального FMEA).

Таблица 4.1-1 – (SSA BSCU FMEA)

Название функции	Режим отказа	Частота отказов (E-6)	Фаза полета	Последствие отказа	Метод обнаружения	Примечания
+ 5 В	+ 5 В вне ТУ	02143	Все	Возможное отключение электропитания	Монитор электропитания отключается, отключает электропитание и передает сообщение «неисправное электропитание» к другим системам	Неисправность канала BSCU
	КЗ +5 В на землю	0,2857	Все	Отключение электропитания	Монитор электропитания передает сообщение «неисправное электропитание» к другим системам	Неисправность канала BSCU
	Потеря/ снижение фильтрации	0,3571	Все	Повышенные пульсации	Может выходить за заданное напряжение к оставшейся части BSCU, если пульсации таковы, что они не определяются монитором эл/питания	Может вызвать ложное отключение монитора эл/питания
	+5 В разомкнуто	0,5714	Все	Отключение эл/питания	Монитор электропитания передает сообщение «неисправное электропитание» к другим системам	Неисправность канала BSCU
	Нет влияния	0,1429	Все	Нет влияния	Нет влияния	Нет влияния
Общая интенсивность отказов эл/питания +5 В		1,5714				

4.2 Компонентный FMEA монитора электропитания

Проведен исходный анализ монитора электропитания при помощи расчета общей интенсивности отказов монитора электропитания на основе подсчета деталей и интенсивностей отказов. Было установлено, что общая интенсивность отказов монитора электропитания была 3,06E-7 отказов в час, что не соответствует запланированной интенсивности отказов 2,0E-7 для монитора. Проведен подробный компонентный FMEA для обеспечения лучшего разрешения проблемы вероятности условия «Отказ достоверности монитора». В таблице 4.2-2 представлены результаты этого компонентного FMEA для детали. Для улучшения классификации суммарных отказов включены пять основных категорий кода отказа. Эти коды влияния отказов определены в таблице 4.2-1.

Таблица 4.2-1 (SSA BSCU – FMEA) Категории влияния отказов

Код влияния отказа	Категория влияния отказа
1.	Монитор «завис» как достоверный
2.	Отключение монитора вследствие помех
3.	Монитор «завис» отключенный/отключение электропитания
4.	Отклонения чувствительности монитора
5.	Нет влияния

Таблица 4.2-2 (SSA BSCU – FMEA)
Компонентный анализ видов и последствий отказа для монитора электропитания BSCU

Идентификатор компонента	Тип детали	Режим отказа	Частота режима отказа (E-6)	Код влияния отказа	Влияние отказа	Метод обнаружения
C1	Керамический конденсатор	пробой	0,0073	3	Низкое напряжение, монитор зависает отключенный	Отключение электропитания монитором
		разомкнут	0,0013	2	Потеря задержки, ложные отключения монитора	Отключение электропитания
		низкая емкость	0,019	2	Уменьшение задержки отключения	
C2	Керамический конденсатор	пробой	0,0073	3	Высокое напряжение, монитор зависает отключенный	Отключение электропитания монитором
		разомкнут	0,0013	2	Потеря задержки, ложные отключения монитора	Отключение электропитания
		низкая емкость	0,019	2	Уменьшение задержки отключения	
U1A	Компаратор IC	Разомкнутый выход	0,0124	1	Низкое напряжение, монитор зависает отключенный	стендовые испытания
		выход заземлен	0,0056	3	Низкое напряжение, монитор отключается	Отключение электропитания
		высокое напряжение смещения нуля на выходе	0,0062	4	Потеря чувствительности монитора	стендовые испытания
U1B	Компаратор IC	Разомкнутый выход	0,0124	1	Высокое напряжение, монитор зависает отключенный	стендовые испытания
		выход заземлен	0,0056	3	Высокое напряжение, монитор отключается	Отключение электропитания
		высокое напряжение смещения нуля на выходе	0,0062	4	Потеря чувствительности монитора	стендовые испытания

Идентификатор компонента	Тип детали	Режим отказа	Частота режима отказа (E-6)	Код влияния отказа	Влияние отказа	Метод обнаружения
R1	Пленочный резистор	разомкнут	0,0009	3	Высокое напряжение, монитор отключается	Отключение электропитания
		увелич. сопротивл	0,0005	4	Окно отключения смещается вниз	
		уменьш. сопротивл.	0,0004	4	Окно отключения смещается вверх	
R2	Пленочный резистор	разомкнут	0,0009	3	Низкое напряжение, монитор отключается	Отключение электропитания
		увелич. сопротивл.	0,0005	4	Окно отключения смещается вверх	
		уменьш. сопротивл	0,0004	4	Окно отключения смещается вниз	
R3	Пленочный резистор	разомкнут	0,0009	3	Низкое напряжение, монитор отключается	Отключение электропитания
		увелич. сопротивл.	0,0005	4	Окно отключения смещается вверх	
		уменьш. сопротивл	0,0004	4	Окно отключения смещается вниз	
R4	Пленочный резистор	разомкнут	0,0009	1	Монитор зависает в достоверном состоянии	стендовое испытание
		увелич. сопротивл.	0,0005	2	Окно отключения сужается	стендовое испытание
		уменьш. сопротивл.	0,0004	1	Окно отключения расширяется, может привести к зависанию монитора	стендовое испытание
R5	Пленочный резистор	разомкнут	0,0009	3	Высокое напряжение, монитор отключается	Отключение электропитания
		увелич. сопротивл.	0,0005	4	Окно отключения смещается вниз	
		уменьш. сопротивл.	0,0004	4	Окно отключения смещается вверх	
R6	Пленочный резистор	разомкнут	0,0009	3	Низкое напряжение, монитор зависает отключенный	Отключение электропитания
		увелич. сопротивл.	0,0005	5	Нет влияния	
		уменьш. сопротивл.	0,0004	5	Нет влияния	
R7	Пленочный резистор	разомкнут	0,0009	3	Высокое напряжение, монитор зависает отключенный	Отключение электропитания

Идентификатор компонента	Тип детали	Режим отказа	Частота режима отказа (E-6)	Код влияния отказа	Влияние отказа	Метод обнаружения
		увелич. сопротивл.	0,0005	5	Нет влияния	
		уменьш. сопротивл.	0,0004	5	Нет влияния	
U2	Элемент "И"	зависание высокое	0,0108	1	Зависание достоверного монитора	стендовые испытания
		зависание низкое	0,054	3	Зависание отключенного монитора	Отключение электропитания
U2	Опорное напряжение	нерабоч.	0,0110	3	Отключение монитора при перенапряжении	Отключение электропитания
		вне ТУ	0,0058	4	Смещение окна	Отключение электропитания
		кор. замык.	0,0026	3	Отключение монитора	Отключение электропитания
		разомкн.	0,0245	3	Отключение монитора при перенапряжении	Отключение электропитания

Примечание: *Неисправности категории отказа 4 могут привести к снижению эффективности монитора.*

(Примечание редактора: В целях данного примера предполагается, что режимы отказов и частоты отказов для мониторов ±15 В должны быть идентичны монитору + 5 В. В фактическом FMEA тот же самый подробный анализ должен быть закончен на мониторах ± 15 В для определения фактических режимов отказов и частот отказов).

4.3 Выводы FMEA

Влияние на уровне BSCU от «Потери/снижения фильтрации» было неизвестно, и оно могло содействовать событию «Не обнаружимый отказ BSCU вызывает непредвиденное торможение». Предельно осторожным является допущение того, что все неисправности этой категории будут не обнаруживаемыми и способными вызвать событие «Не обнаружимый отказ BSCU вызывает непредвиденное торможение». В связи с этим был проведен отдельный лабораторный анализ влияния на систему. Данный анализ (см. ссылку 6) показывает, что ни один из отказов в категории влияния «Потери/сниженной фильтрации» не может вызвать непреднамеренное торможение.

(Примечание редактора: Для определения фактического влияния режима отказов в некоторых случаях может потребоваться лабораторный анализ. См. раздел G.2.2.3).

Все другие категории влияния отказов за исключением «Нет влияния» могут содействовать событию «Отказ электропитания BSCU вызывает неверные данные». Эти отказы будут выявляться монитором электропитания, функционирующим должным образом. В таблице 4.3-1 приведена сводка результатов FMEA электропитания и монитора электропитания.

Таблица 4.3-1 (SSA BSCU FMEA)

Сводка по режимам отказов и влияниям электропитания BSCU и монитора электропитания

Режимы отказов	Частота отказов (E-6)	Влияние BSCU	Потенциальная причина отказа	Метод выявления	Примечания
Отключение электропитания (э/п)	8,21	Отказы системы BSCU	+5 вне ТУ + 5 к.з. на землю + 5 В разомкнуто +15 вне ТУ …	«Э/п действует» для других BSCU установлен недействит.	Система 2 BSCU обеспечивает команду на торможение
Увеличенные пульсации от э/п	1,86	Неизвестно	Потеря/снижение фильтрации: + 5 В +15 В -15 В	Возможно не выявляется	Был проведен лабораторный анализ, который показал, что данный режим не вызывает непреднамеренное торможение
Э/п работает должным образом Монитор не может отключить э/п	0,57	Э/п не отключается после отказа э/п	Вход PWM от монитора напряжения «завис»	Испытания только на уровне платы	Достоверный сигнал электропитания отключает выходы BSCU 1. Нет очевидного влияния BSCU
Отказ монитора э/п	0,1429	Возможна ошибочная работа после отказа э/п	U1A разомкнуто U1 разомкнуто R4 разомкнуто R4 снижает R U2 высокое…	Стендовое испытание	Скрытый отказ
Монитор э/п отключен	0,1578	Отказ системы BSCU	C1 короткое замык. C1 разомкнуто C2 короткое замык. C2 разомкнуто	«Э/п действует» для других BSCU установлен недействит.	
Нет влияния	2,55554	Нет	Выход 5 В не влияет R6 увеличивает R R6 уменьшает R	Нет	Нет

5.0 ЗАКЛЮЧЕНИЕ

FMEA электропитания был необходим для проверки соответствия исполнения конструкции запланированному значению 1,25E-5 отказа в час для события «Отказ электропитания BSCU вызывает неверные данные». Фактическая интенсивность отказов для события «Отказ электропитания BSCU вызывает неверные данные» равна 1,06E-5 отказов в час.

FMEA монитора электропитания было необходимо для проверки того, что конструктивное исполнение отвечает запланированной величине 2E-7 отказа в час для неисправностей монитора электропитания, когда режим отказов относится к событию «Отказ монитора электропитания выявить неисправность электропитания». Фактическая интенсивность отказов для события «Отказ монитора электропитания выявить неисправность электропитания» равна 1,429E-7 отказа в час.

Электропитание BSCU отвечает требованиям к потере электропитания, не обнаружимого отказа, который вызывает непреднамеренное торможение, и к отказу монитора электропитания обнаружить неисправность электропитания.

FMES ДЛЯ BSCU

1.0 ВВЕДЕНИЕ

В данной FMES представлена сводка результатов всех FMEA. BSCU

(Примечание редактора: Также включены результаты других FMEA, которые могли быть проведены, для обеспечения более полного перечня влияния отказов).

(Примечание редактора: Информацию по процессу FMES см. в Приложении H).

2.0 ССЫЛКИ

При выполнении данного анализа использованы следующие ссылки.

1) P4761 «Руководство по методам оценки безопасности бортового оборудования самолетов гражданской авиации».
2) Внутренняя памятка, документирующая результаты FMEA по отношению к системе BSCU.
3) Выпущенная конструкторская и технологическая документация на BSCU.

3.0 ОПИСАНИЕ BSCU

(Примечание редактора: Обычно здесь должно включаться описание системы. Тем не менее, поскольку оно включено в другом месте в Приложении L, то здесь оно не повторяется).

4.0 ДАННЫЕ FMES

Последствия отказов, полученные из FMEA (см. ссылку 2), были проверены и суммированы в таблице 4.0-1.

Таблица 4.0-1 (SSA BSCU – FMEA) FMES последствия отказов BSCU на уровне выхода

Режим отказа	**Частота отказов**	**Потенциальная причина отказа** ***(источник отказа)***	**Обнаруживаемость**	**Примечания**
Потеря команды на торможение от системы 1	4,35E-5	- отключение э/п системы 1 - отключения монитора э/п системы 1 - отказ команды системы 1	- система подачи сигналов экипажу	Команду на торможение обеспечивает система 2
Потеря команды на торможение от системы 2	4,35E-5	- отключение э/п системы 2 - отключения монитора э/п системы 2 - отказ команды системы 2	- система подачи сигналов экипажу	Команду на торможение обеспечивает система 1
Потеря команды на торможение как от системы 1, так и от системы 2	1,6E-9	- зависание монитора достоверности BSCU - отказ переключателя BSCU в промежуточном положении	Индикация на дисплее системы "Потеря нормального торможения"	Предусмотрен дискретный сигнал
Команда от системы 1 или 2 на непреднамеренное торможение	0,85E-9	- отказы 3,5,9 вх/вых CMD1, вх/вых CMD2 *(FMEA BSCU)*	Очевидно по влиянию	
Команда от системы 1 или 2 на асимметричное торможение	1,6E-8	- отказы 6,11,12 вх/вых CMD1COMP, вх/вых CMD2COMP *(FMEA BSCU)*	Очевидно по влиянию	

(Примечание редактора: В данном приложении примера можно найти не все неисправности, перечисленные в столбце «Потенциальная причина отказа», тем не менее, он показывает принцип FMEA для суммирования всех отказов с одним и тем же влиянием для получения одного режима отказа для следующего более высокого уровня анализа).

АНАЛИЗ ОБЩЕГО РЕЖИМА (CMA) ДЛЯ BSCU

CMA конструктивного исполнения BSCU (CMA уровня изделия/компонента)

(Примечание редактора: процессы и методы, описанные в Приложении К, должны использоваться для разработки отчета LRU CMA, аналогичного следующему. Формат отчета оставлен на усмотрение лица, проводящего анализ, тем не менее, его конкретное содержание должно отражать ожидаемое содержание, описанное в Приложении К и данном примере. Этот пример отображает один формат завершенного анализа общего режима изделия).

1.0 ВВЕДЕНИЕ

В данном отчете представлены результаты анализа общего режима блока управления тормозной системы (BSCU), демонстрирующие то, что в BSCU не существует одиночных отказов, которые могут инициировать опасное или катастрофическое событие. BSCU обеспечивает резервное высоко интегрированное торможение и контроль противоскольжения для самолета S18.

(Примечание редактора: В следующей таблице поперечных ссылок представлена связь каждого параграфа примера с соответствующим параграфом приложения CMA).

№ параграфа CMA изделия	№ параграфа приложения К
4.1	К.3.1
4.2	К.3.2
4.3	К.3.3, К.4

2.0 ССЫЛКИ

При выполнении данного анализа используются следующие ссылки.

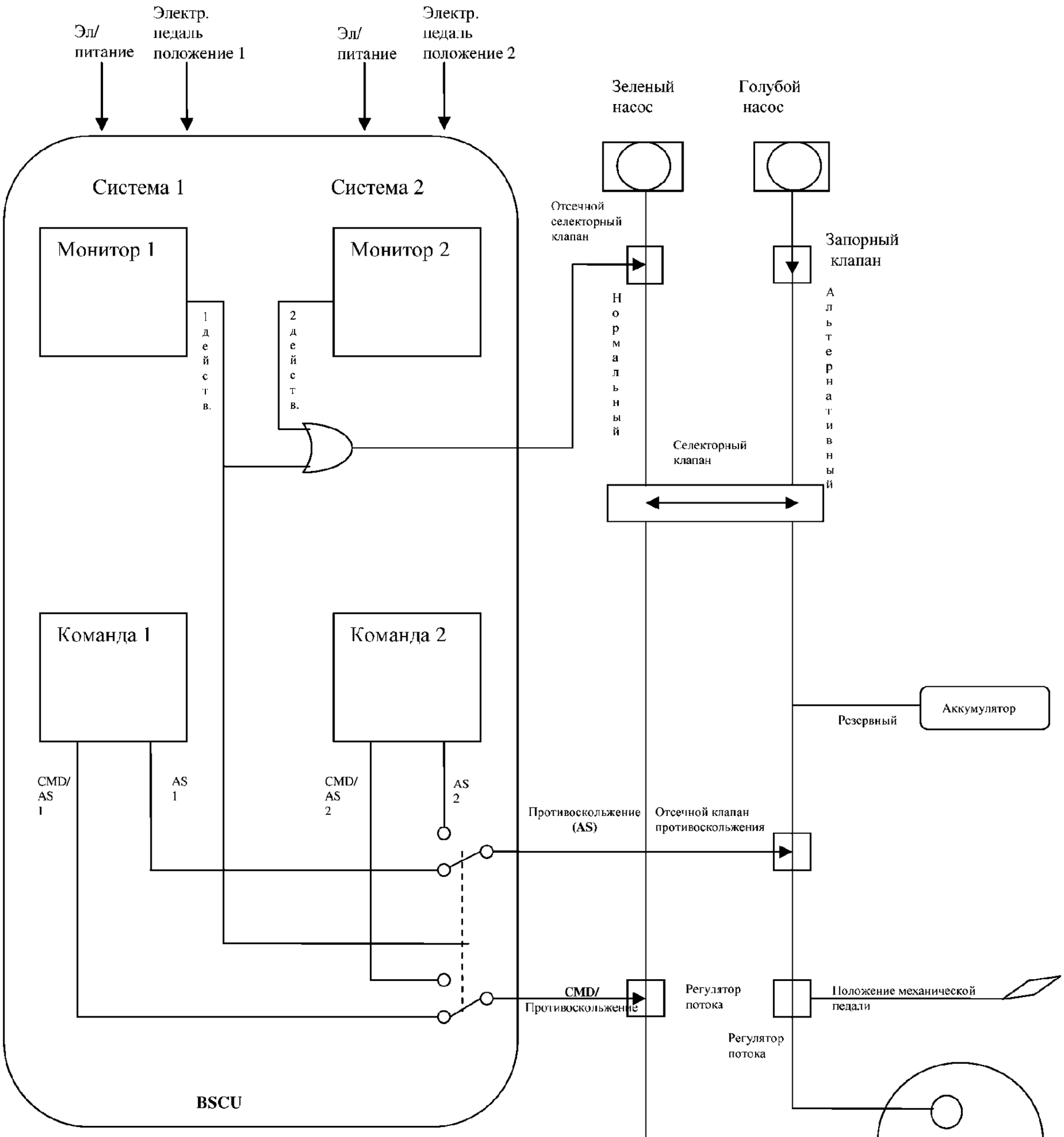
1) Р4761 «Руководство по методам оценки безопасности систем и бортового оборудования самолетов гражданской авиации».
2) Деревья неисправности «Потеря торможения всех колес» и «Непреднамеренное торможение колеса» для самолета S18, включая систему BSCU.
3) Оценка функциональной опасности самолета S18.
4) Предварительная оценка безопасности самолета S18.
5) Конструкторская и технологическая документация на BSCU.
6) «Нормы проектирования с разделением безопасности для LRU в критических по безопасности системах».

3.0 ОПИСАНИЕ ФУНКЦИИ/СИСТЕМЫ

BSCU представляет собой LRU, который обеспечивает команды нормальной системы торможения и команды против скольжения для нормальной и альтернативной систем торможения. Команды нормальной системы торможения обладают возможностью инициировать непреднамеренное торможение; следовательно, требуется анализ этой функции. Команды против скольжения не могут включить тормоза, они могут только удалить команду на тормоз, генерируемую в другом месте, поэтому конструкция противоскольжения не способствует непреднамеренному торможению. Поскольку противоскольжение не может содействовать системе резервного торможения, то оно не дает вклад в общую потерю торможения колеса. Следовательно, анализ функций противоскольжения не требуется.

Выбранная архитектура для BSCU представляет собой четырехканальную конфигурацию, состоящую из двух независимых систем (системы 1 и 2), каждая из которых имеет два независимых вычислительных канала (командный и контрольный). Каждая система сопрягается через заданный разъем LRU (P1 или P2). BSCU работает как активное/ резервное устройство,

когда система 1 нормально активна, а система 2 является резервной системой, которая автоматически переключается на линию при обнаруженных отказах системы 1 при помощи оперативного мониторинга системы 1. Оперативный мониторинг обеих систем 1 и 2 объединен для обеспечения отключения нормальной системы и автоматического переключения на систему альтернативного торможения, когда обе системы BSCU не работают. На рис. 3.0-1 изображена архитектура BSCU и ее интерфейсы с другими элементами тормозной системы.



(SSA BSCU – CMA) Схема архитектуры BSCU
Рис. 3.0-1

4.0 ИНФОРМАЦИЯ ПО CMA BSCU

4.1 Типы общего режима, контрольный перечень источников и неисправностей/ошибок

(Примечание редактора: В разделе 2.1 Приложения К представлены инструкции для установления типов общего режима, контрольных перечней источников и неисправностей/ошибок).

Проведен анализ перечней ошибок/источников общего режима в Приложении К ссылки 1 для идентификации источников общего режима, применимых к BSCU. Следующие источники ошибок/отказов идентифицированы как относящиеся к анализу общего режима BSCU.

a. Конструктивные соображения

(1) Общие внешние источники для резервируемых функций.

(2) Общие электрические интерфейсы (разъемы) с резервными системами.

(3) Родовые ошибки разработки в резервных системах (аппаратных или программных).

(4) Общие неисправности, влияющие на функции вычисления и мониторинга.

b. Технологические соображения

(1) Несоответствующая замена компонента.

(2) Неправильная сборка.

(3) Общий изготовитель компонентов.

(4) Соображения установки.

(5) Неполная установка (разъемы не соединены).

(6) Неправильная установка (разъемы перепутаны).

c. Соображения по окружающей среде

(1) Несоответствие требованиям окружающей среды.

(2) Несоответствие электрическим и радиационным требованиям.

Ожидается, что идентифицированные выше потенциальные источники ошибки/неисправности общего режима можно уменьшить при помощи одного из следующих средств.

a. Анализ/испытание конструкции.

b. Испытание производства.

c. Утвержденные/контролируемые процессы изготовления.

d. Утвержденные/контролируемые процессы ремонта.

e. Сертификация/квалификационные испытания.

4.2 Требования к анализу

(Примечание редактора: Инструкции по разработке требований к анализу представлены в разделе 3.2 (входные данные FHA/PSSA) и разделе 3.3 Приложения К).

Идентифицированы требования к анализу CMA BSCU при помощи экспертизы ссылок 2, 3 и 4, а также идентификации логических схем «И» дерева неисправностей, выполненных в BSCU и дающих вклад в события опасной потери торможения колеса и катастрофического непреднамеренного торможения колеса. Должна быть показана независимость этих функций для того, чтобы обеспечить отсутствие отказов общего режима вследствие ошибки разработки. В результате экспертизы дерева неисправностей получены следующие требования к независимости BSCU.

1. Потеря торможения колеса

Для потери торможения всех колес требуется потеря нормальной тормозной системы, потеря альтернативной тормозной системы и потеря аварийной/резервной тормозной системы.

Выходной командный сигнал против скольжения может давать вклад в потерю как нормальной, так и альтернативной тормозных систем вследствие его способности удалять команду на торможение от других источников. Ни один элемент BSCU не вносит свой вклад в аварийную/резервную тормозную систему, поэтому не может быть отказов BSCU общего режима, которые могут запретить торможение всех колес. Тем не менее, потеря резервных систем BSCU может снизить работоспособность нормального торможения, как это изображено на дереве неисправностей.

2. Непреднамеренное торможение колес

Любая из индивидуальных систем торможения может давать свой вклад в непредвиденное торможение колес, поэтому необходимо показать, что BSCU не содержит отказов общего режима, которые могут непреднамеренно активизировать нормальную систему торможения, в то время как нормальная система активна.

Проведен анализ дерева неисправностей непреднамеренного торможения колес для идентификации отказов, связанных с BSCU, и установление требований независимости BSCU. Следующие функции BSCU должны быть показаны как независимые от отказов общего режима для того, чтобы обосновать дерево неисправностей непреднамеренного торможения колеса.

1) Неисправности вычисления системы BSCU должны быть независимы от неисправностей соответствующих мониторов достоверности и выходных командных сигналов на переключение. При этом обеспечивается, что одиночные отказы не могут вызвать неправильную команду и одновременно запретить контроль и удалить команду.

2) Неисправности каждого из командных и контрольных каналов системы BSCU должны быть независимыми для обеспечения того, что одиночные отказы не смогут воздействовать на оба канала аналогичным образом, отменяя монитор перекрестного сравнения каналов.

3) Отказы каждого электропитания BSCU и соответствующих мониторов электропитания должны быть независимыми для обеспечения того, что никакой одиночный отказ не сможет вызвать аномальную работу электропитания и аннулировать контроль электропитания. (Поскольку электропитание является общим для командного и контрольного каналов данной системы, то отказ электропитания может аналогичным образом влиять на оба канала, аннулируя реакцию компаратора).

4) Необходимо учитывать родовые ошибки аппаратных или программных средств в элементах, общих для командного или контрольного каналов, либо в мониторах достоверности/сравнения.

5) Необходимо учитывать соображения изготовления, включая общие компоненты в системах 1 и 2 BSCU, и контроль качества изготовления.

6) При установке должны учитываться ошибки общего режима, такие как соединения, проверки и т.п.

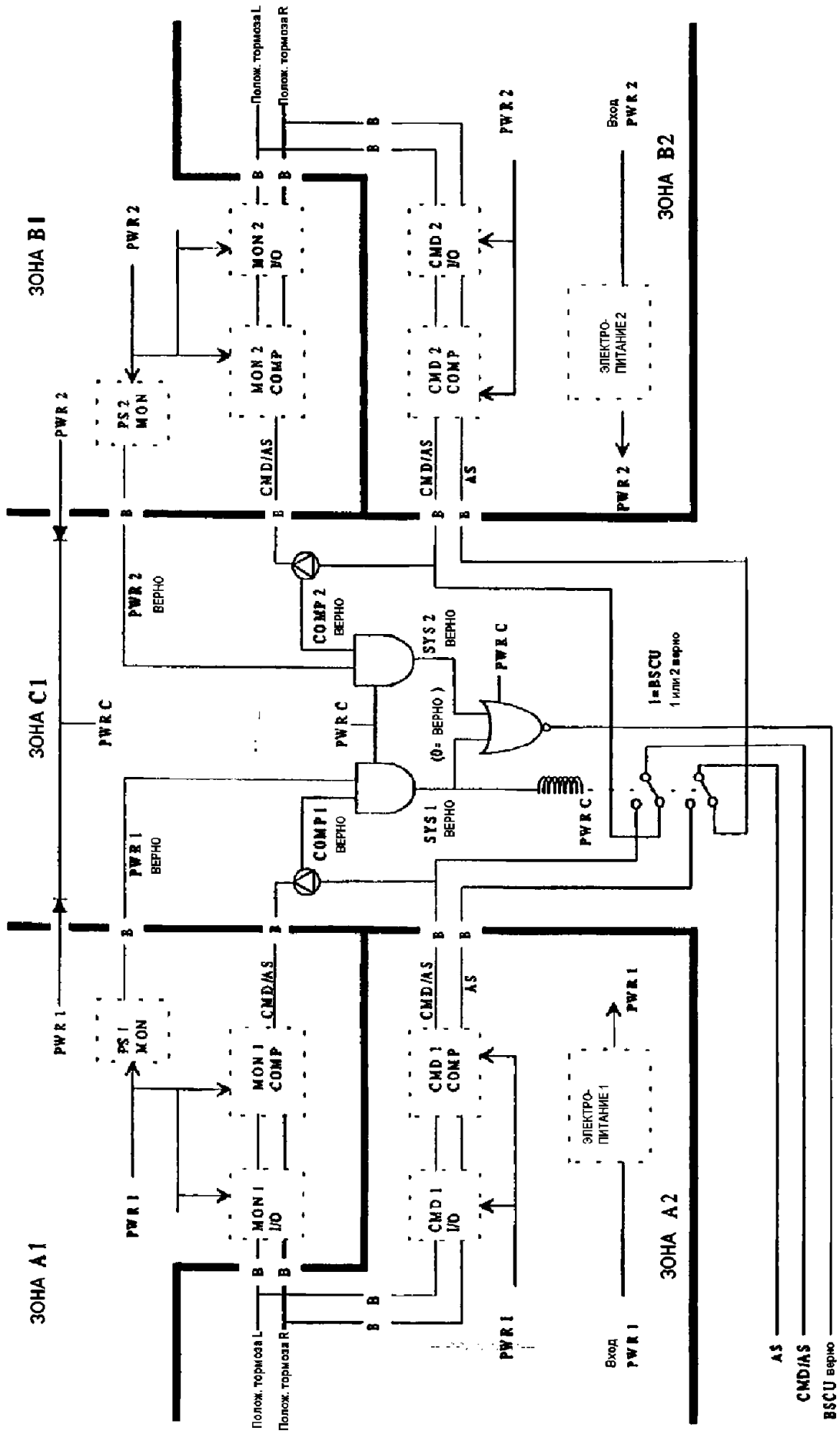
7) BSCU должен быть спроектирован с учетом требований окружающей среды по HIRF и грозовым разрядам.

4.3 Анализ общего режима

С учетом знаний по заданным операциям, описанным в разделе 3.0, была проведена экспертиза фактического исполнения с точки зрения требований независимости, определенных в разделе 4.2, и инструкций по разделению, определенных в ссылке 6. Было рассмотрено определенное количество факторов, которые использовались индивидуально в следующем анализе.

На рис. 4.3-1 изображены физические зоны разделения BSCU, отделяющие функции, для которых должна быть обеспечена независимость. Проведен анализ документации на монтажную печатную плату и другой производственной сборочной документации. Целью конструкции является то, чтобы система 1 BSCU была полностью ограничена в зоне А, в то время как система 2 BSCU была полностью ограничена в зоне В, что обеспечивает независимость систем 1 и 2. Это отделение обеспечивает независимость функций ВЫЧИСЛИТЕЛЯ МОНИТОРА и МОНИТОРА ЭЛЕКТРОПИТАНИЯ в зоне 1 от функций КОМАНДНОГО ВЫЧИСЛИТЕЛЯ и ЭЛЕКТРОПИ-

ТАНИЯ в зоне 2, соответственно. Функции «ДОСТОВЕРНОСТИ» и «ПЕРЕКЛЮЧЕНИЯ» находятся в одной зоне (зоне С) для обеспечения независимости от общих элементов обеих систем 1 и 2. Эта разделенная конструкция обеспечивает независимость элементов в пределах каждой из этих функций. Была проведена экспертиза фактически выполненной конструкции для проверки и гарантии того, что цель разделения была достигнута.



(SSA BSCU CMA) Физическое исполнение BSCU
Рис. 4.3-1

Анализ был начат на входах в BSCU и проведен далее через каждую зону разделения для идентификации непреднамеренных нарушений разделения функций. Ниже представлен перечень сигналов, нарушивших зоны разделения. Затем эти сигналы были проанализированы с точки зрения их приемлемости, а также соединения с точки зрения соответствующей буферизации для предотвращения распространения отказа.

Напряжения электропитания были общими для всех элементов в каждой системе (тем не менее установлено, что напряжения электропитания каждой системы должны быть независимыми). Это обеспечивает приемлемый независимый вход контроля электропитания для проверки достоверности системы.

Выходные командные сигналы/сигналы противоскольжения контрольного и командного вычислительного канала и выходной сигнал противоскольжения командного вычислительного канала проходят из их соответствующей зоны разделения в зону достоверности/контроля. Сравнение и переключение команд между функциями систем выполняются в пределах зоны разделения достоверности/контроля. Командные сигналы должны проходить в ту зону, которая должна быть переключена на соответствующий выход. Предусмотрена соответствующая буферизация для предотвращения распространения отказа между зонами. Таким образом, эти нарушения являются приемлемыми.

Выходные сигналы достоверности, противоскольжения и команды BSCU системы 2/противоскольжения проходят от системы 2 в канал достоверности/контроля системы 1. Так же как и для аналогичных нарушений команд системы 1, это представляет собой ожидаемое нарушение, поскольку выбор той из двух систем, которая направляется на выход, функционально выполняется в пределах зоны достоверности/контроля системы 1. Аналогичным образом, в данной конструкции представлена соответствующая буферизация распространения отказа.

Электропитание и входные сигналы от педалей для каждой системы направлялись через независимые системно ориентированные разъемы, закрепленные дифференциально для предотвращения непредвиденных обменов сигналами к двум системам. Все входные сигналы от BSCU направляются через разъем системы 1. Выходные функции и входные функции системы 1 разделяются заземленными контактами разъема, исключая не определяемые непреднамеренные короткие замыкания между входным сигналом или электропитанием и командой на торможение или выходными сигналами. Выходные сигналы достоверности и команд также изолированы друг от друга в пределах данного разъема.

Независимые требования 1, 2 и 3 раздела 4.2 выполняются разделением функциональности, предусмотренной в конструктивном исполнении. Требования 4, 5, 6 и 7 раздела 4.2 выполняются следующим образом.

Требование 4 к порождению отказов в компонентах, общих для нескольких каналов или систем, включает в себя следующее.

a. Компоненты, включая элементы программных средств, общие для нескольких каналов и/или систем, были проанализированы с точки зрения обеспечения того, что порождающий отказ либо невозможен и не произведет аналогичных влияний отказов в нескольких каналах/системах, либо не повлияет как на выходные сигналы, так и на контроль соответствующих сигналов. Элементы программных средств являются общими для обеих систем BSCU. Были разработаны программные средства для вычислительного и контрольного каналов и строго проверено по уровню A и B обеспечения разработки, соответственно, при помощи гибких процессов DO-178, предотвратив таким образом дефекты рассматриваемой конструкции.

b. Все компоненты, используемые в конструкции BSCU, являются общими и относительно простыми промышленными компонентами, использованными в прошлом в аналогичных системах. На основе обширного промышленного опыта использования таких компонентов неблагоприятные условия отказа не ожидаются. Этот процесс демонстрирует в достаточной степени отсутствие в данном устройстве ошибок разработки родового типа.

Требование 5 к процессу изготовления включает в себя следующее.

Ошибки изготовления, которые могут нарушить независимость функций BSCU, контролируются при помощи комбинации управляемых процессов изготовления, проверки последующих процессов сборки и окончательных испытаний изделия перед поставкой каждого изготовленного блока.

Требование 6 к установке включает в себя следующее.

Ошибки общего режима, относящиеся к установке и техническому обслуживанию, контролируются при помощи заданных процедур технического обслуживания, а также эксплуатационными испытаниями. Кроме того, специальное шпоночное крепление разъема исключает неправильное подключение разъемов BSCU.

Требование 7 к воздействию окружающей среды включает в себя следующее.

Вопросы, связанные с воздействием окружающей среды на режимы общих отказов, исключены при помощи исчерпывающих квалификационных и сертификационных испытаний, проводимых в соответствии со стандартами по воздействию окружающей среды DO-1 60.

4.4 Сводка по CMA уровня LRU

В таблице 4.4-1 представлена сводка результатов анализа общего режима BSCU.

Таблица 4.4-1 (SSA BSCU – CMA) Сводка по анализу общего режима BSCU

Состояние отказа	Источник общего режима	Обоснование конструкции	№ требования раздела 4.2
Потеря торможения всех колес	Отказ BSCU	BSCU связан только с командами нормальной системы торможения и не имеет входных командных сигналов тормоза для альтернативной или аварийной систем.	Не используется
Снижение работоспособности нормальной системы торможения	Одновременный отказ системы 1 и 2 BSCU	Нет общих функций, за исключением переключения выходных сигналов и сигналов достоверности, которые соответствующим образом буферизуются.	1
Непреднамеренное торможение из-за общих отказов в командном и контрольном каналах BSCU	Нарушение зон разделения команд и мониторинга	Общие функции ограничены защитой буферизации, предусмотренной в соответствии с инструкциями по разделению.	2
Непреднамеренное торможение из-за несоответствующей независимости монитора электропитания при наличии аномальных выходных сигналов электропитания системы	Нарушение зон разделения электропитания и мониторинга или несоответствующая конструкция контрольного устройства электропитания	Общие функции ограничены защитой буферизации, предусмотренной в соответствии с инструкциями по разделению. Выходные сигналы контрольного устройства смещаются к недостоверным значениям при отсутствии электропитания или параметрах электропитания, не удовлетворяющих требуемым.	3 и 4
Порождающие неисправности общего компонента	Нарушение любой требуемой независимости или родовые ошибки разработки	Используемые компоненты имеют либо промышленно приемлемую работоспособность или подвергались специальным процессам проверки конструкции.	5

Состояние отказа	Источник общего режима	Обоснование конструкции	№ требования раздела 4.2
Вопросы изготовления	Ошибки изготовления, нарушающие независимость	Сертификационный орган утвердил используемые процессы изготовления и обеспечения качества. Окончательные испытания и проверки предотвращают ошибки изготовления.	6
Дефекты испытаний LRU	Отказ обнаружения скрытых неисправностей во время стендовых испытаний	Проведен анализ стендовых испытаний LRU для обеспечения охвата скрытых неисправностей, критических по безопасности.	6
Вопросы установки	Неправильная установка и/или техническое обслуживание на самолете	Испытания после технического обслуживания для «возврата в эксплуатацию», требуемые перед отправкой, обеспечивают проверку интерфейсов системы и ее работу.	7
Вопросы воздействия окружающей среды	Общие неисправности, вызванные окружающей средой	Предотвращаются при помощи всесторонних квалификационных испытаний воздействия окружающей среды.	8

5.0 ЗАКЛЮЧЕНИЕ

Не выявлено отказов общего режима BSCU, которые могут привести к потере торможения колес или непредвиденному торможению колес.

ОТЧЕТ ПО BSCU – FTA (DD ИЛИ MA)

1.0 ВВЕДЕНИЕ

В данном отчете представлены результаты анализа дерева неисправностей блока управления тормозной системы (анализа логической схемы или Марковского анализа).

(Примечание редактора: В таблице перекрестных ссылок представлена связь каждого параграфа примера с соответствующим параграфом приложения).

№ параграфа изделия SSA	Приложение
4.0	C.3.1.1
5.0	C.3.1.2, 3.3
5.1	Приложение D
5.2	Приложение E
5.3	Приложение F

2.0 ССЫЛКИ

1) BSCU PSSA.

2) Спецификация BSCU.

3) BSCU FMEA.

4) BSCU FMES.

5) BSCU CMA.

6) Отчет по прогнозу надежности BSCU.

3.0 КРАТКОЕ ОПИСАНИЕ

(Примечание редактора: Описание для данного примера аналогично описанию, приведенному в разделе 3.0 BSCU PSSA).

4.0 СВОДКА РЕЗУЛЬТАТОВ АНАЛИЗА BSCU

Во время предварительной оценки безопасности системы BCSU были подготовлены FTA (DD или MA) для значительных нежелательных событий BSCU. В данном отчете формализованы результаты этих анализов и проведено сравнение с фактическими интенсивностями отказов и временами воздействия.

Влияние отказа	Требование	Результат анализа
Отказ BCSU вызывает потерю команд на торможение	< 3,3 E-5/полет	1,5 E-6/полет
Отказ BCSU вызывает непредвиденное торможение после V1	< 2,5 E-5/полет	6,16 E-10/полет

5.0 ДЕТАЛЬНЫЕ РЕЗУЛЬТАТЫ АНАЛИЗА BSCU

Анализ события «Отказ BSCU вызывает потерю команд на торможение»

На рис. 5.1-1, 5.2-1 или 5.3-1 (FTA, DD, MA, соответственно) показаны результаты окончательного анализа события «Отказ BSCU вызывает потерю команд на торможение». Для «отказа системы 1(2) BSCU» использовалась общая интенсивность отказов BSCU. Селекторный переключатель системы проверялся при каждом включении электропитания на способность переключения в оба положения, при этом время воздействия для скрытых отказов переключателя равнялось 100 часов.

Анализ события «Отказ BSCU вызывает непредвиденное торможение после V1»

На рис. 5.1-2, 5.2-2 или 5.3-2 (FTA, DD, MA, соответственно) показаны результаты окончательного анализа события «BSCU подает команды на торможение при отсутствии входного сигнала тормоза и вызывает непреднамеренное торможение». CMA BSCU идентифицировал электропитание как причину потенциального одиночного отказа, вызывающего команды на непредвиденное торможение от активной системы BSCU. Для BSCU был проведен FMEA и было определено, что нет одиночных неисправностей, которые могут вызвать этот отказ.

Цепочки отказов, включая неисправность монитора и неисправность командной цепи тормоза являются последовательно зависимыми. Монитор должен отказать в первую очередь. Во время испытаний самолета проверялись только монитор электропитания BSCU и мониторы достоверности системы BSCU. Время воздействия 100000 часов, т.е. срок службы самолета, заданное для этих неисправностей, рассматривается как умеренное.

Дерево неисправностей показывает, что программные средства, включенные в функцию монитора достоверности системы BSCU, были разработаны для уровня гарантии B. Программные средства, включенные в генерацию команд на торможение в командном канале, были разработаны для уровня A.

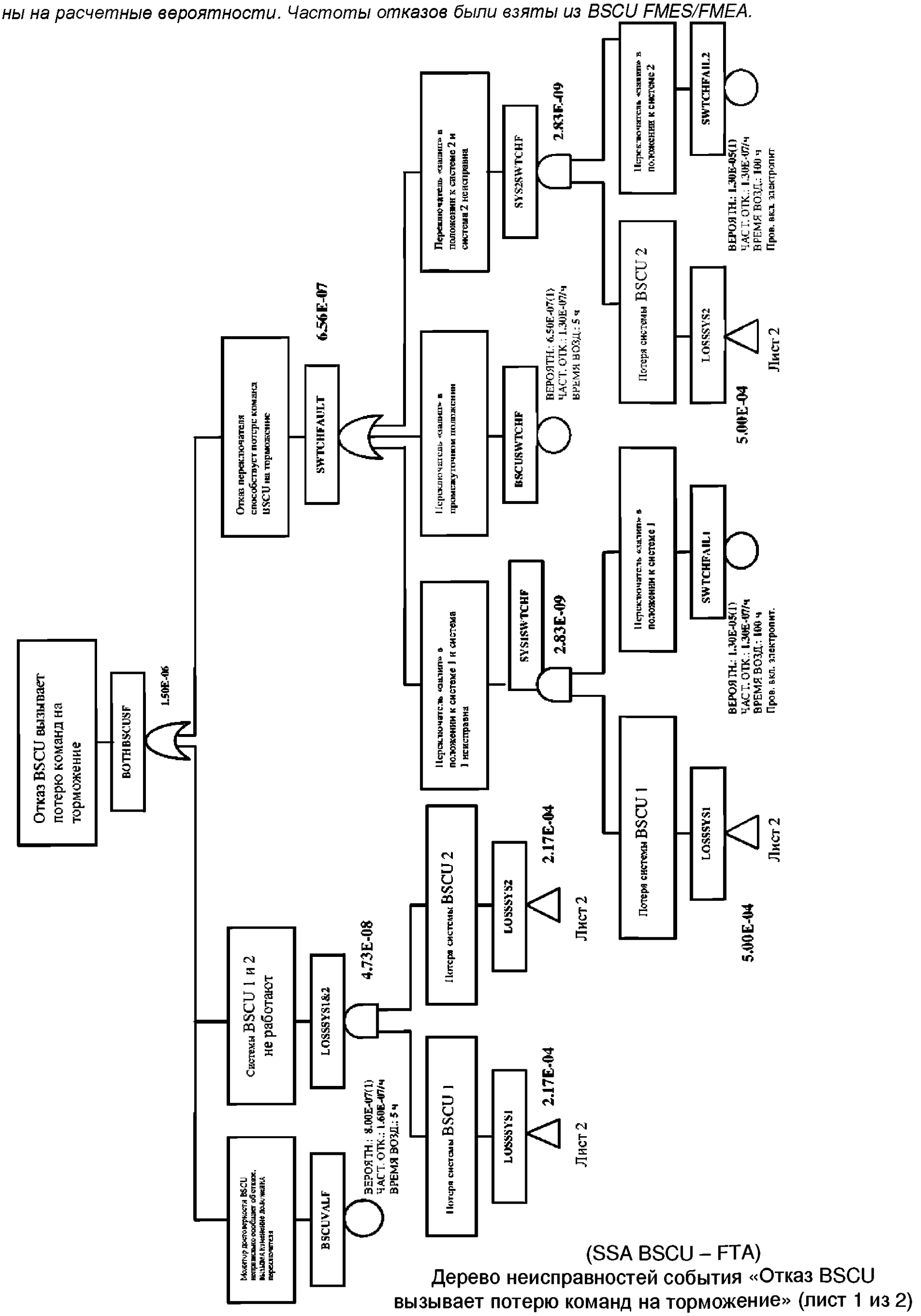
5.1 Анализ дерева неисправностей BSCU

Дерево неисправностей BSCU идентифицировано следующим образом.

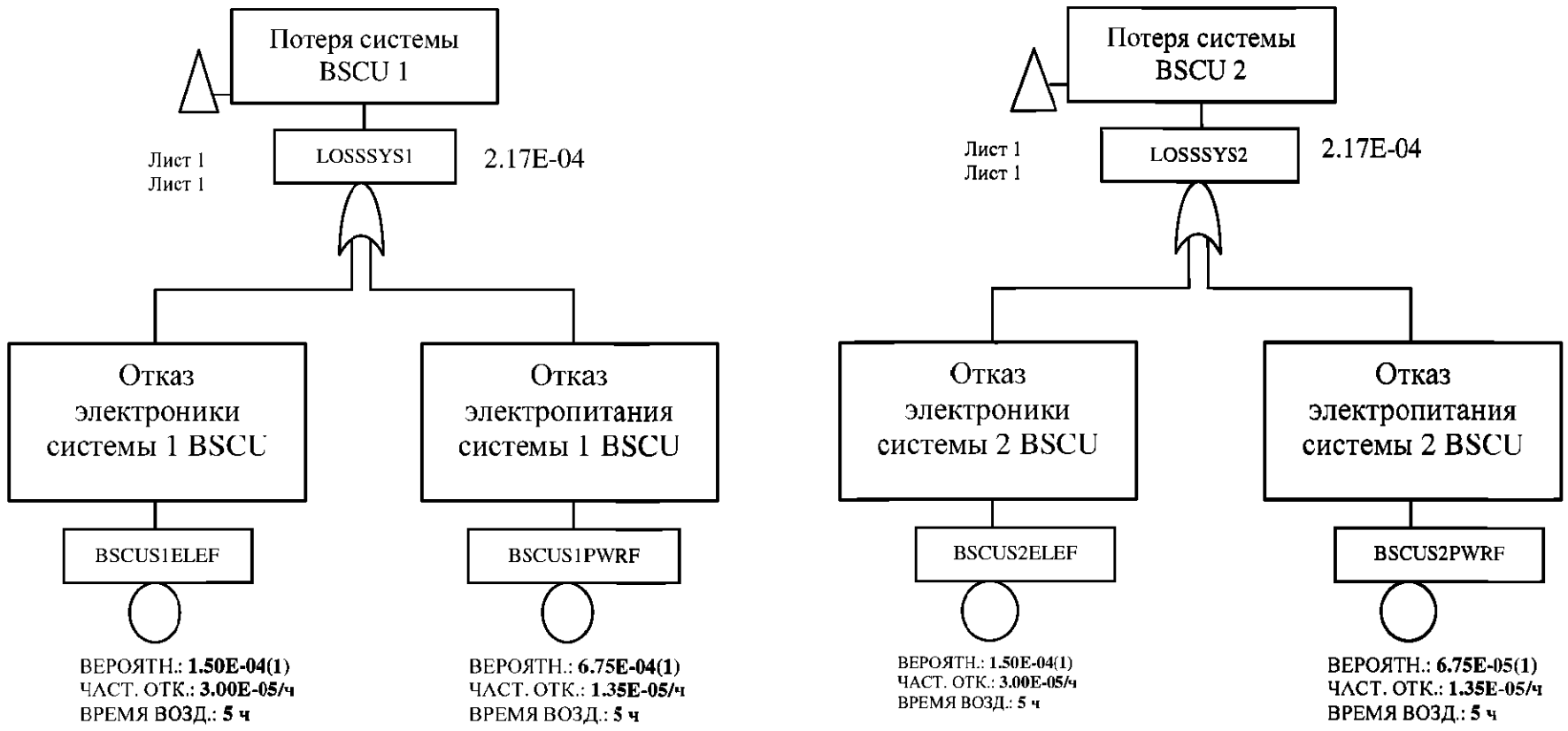
a. Рис. 5.1-1 Отказ BSCU вызывает потерю команд на торможение

b. Рис. 5.1-2 BSCU подает команды на торможение при отсутствии входного сигнала тормоза и вызывает непредвиденное торможение

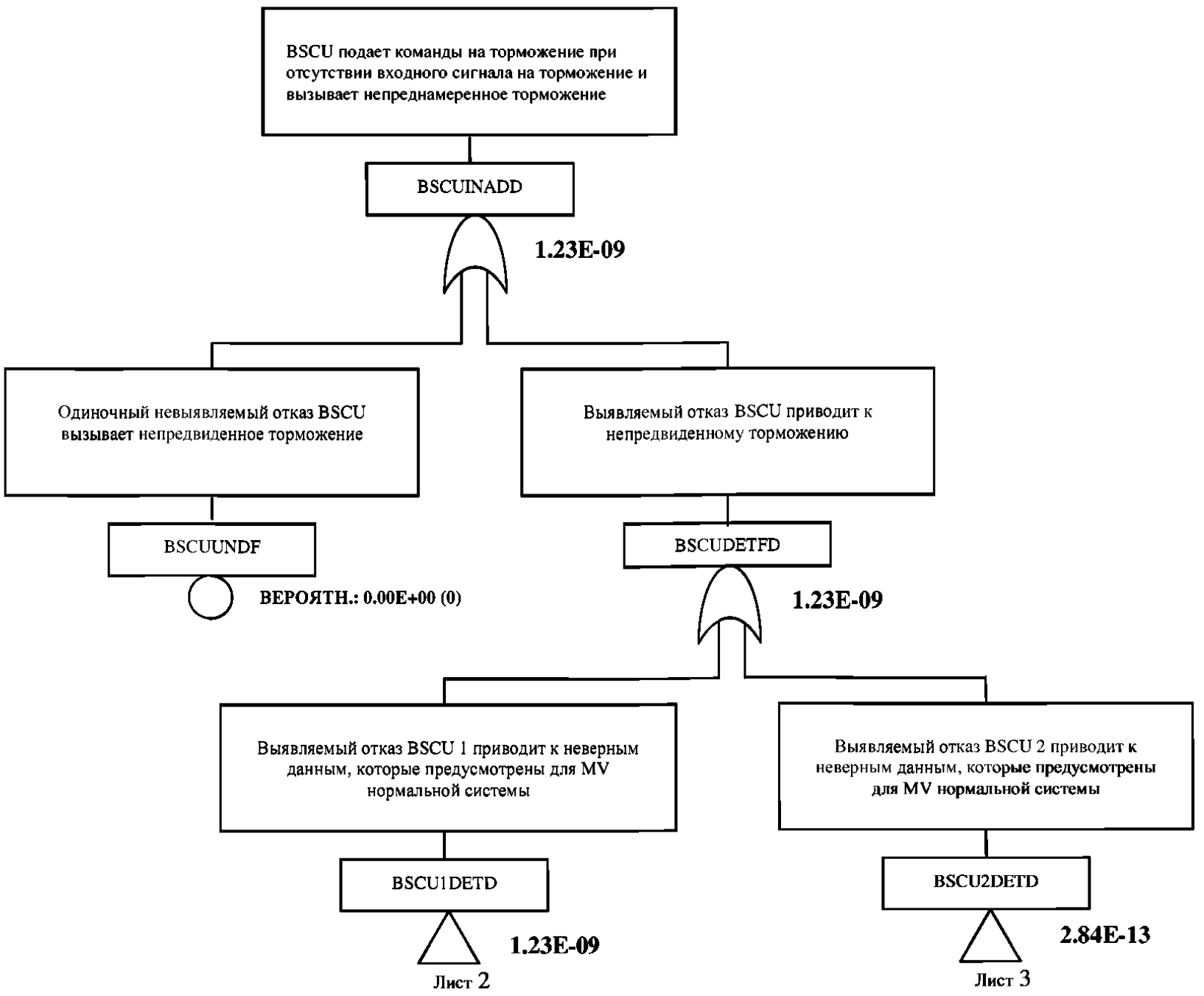
Примечание редактора: BSCU SSA FTA имеет аналогичную структуру как и для BSCU PSSA FTA. Отличием является только то, что для двух деревьев запланированные вероятности были заменены на расчетные вероятности. Частоты отказов были взяты из BSCU FMES/FMEA.



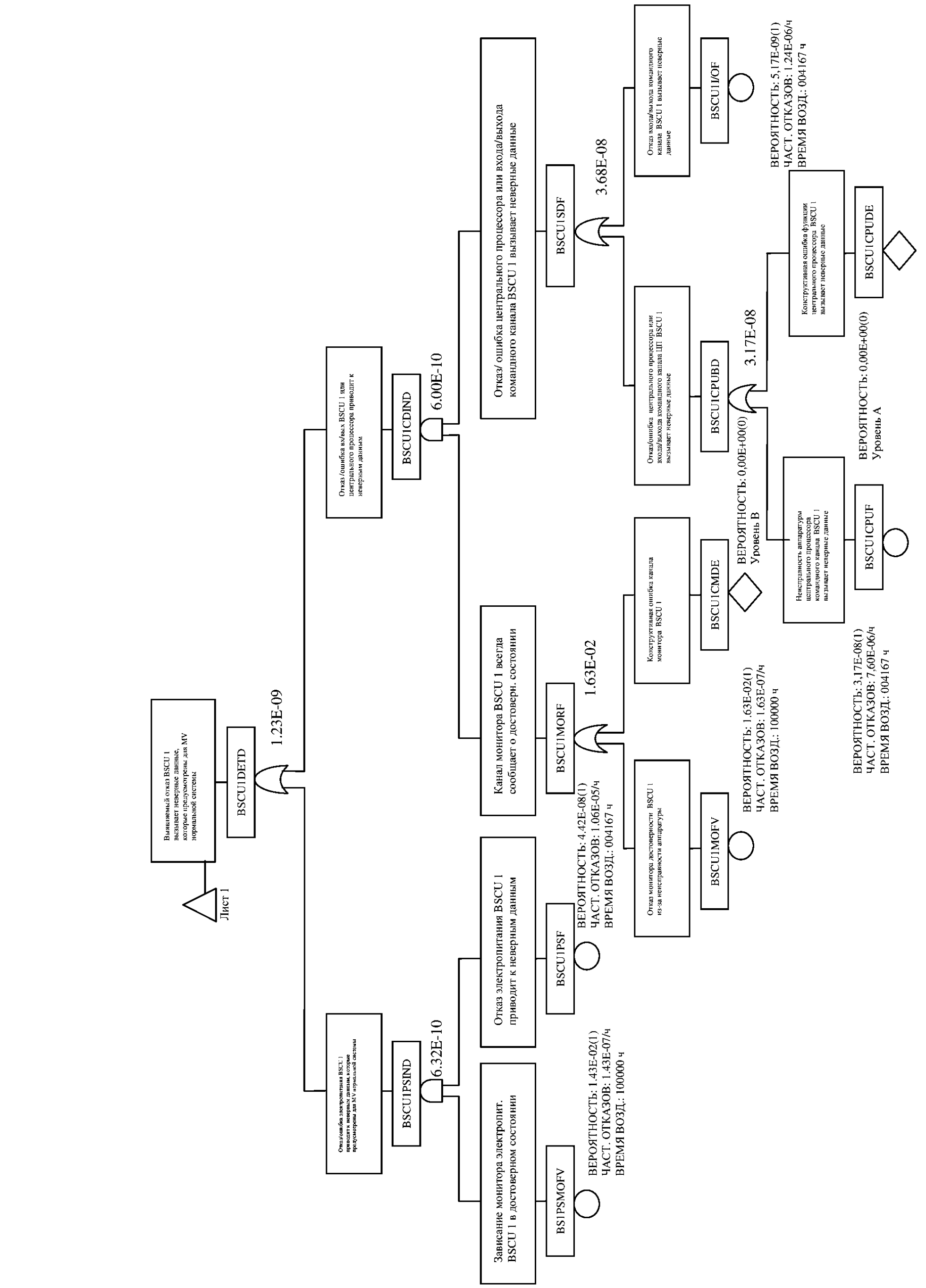
(SSA BSCU – FTA)
Дерево неисправностей события «Отказ BSCU вызывает потерю команд на торможение» (лист 1 из 2)
Рис. 5.1.1



(SSA BSCU – FTA)
Дерево неисправностей события
«Отказ BSCU вызывает потерю команд на торможение» (лист 2 из 2)
Рис. 5.1-1



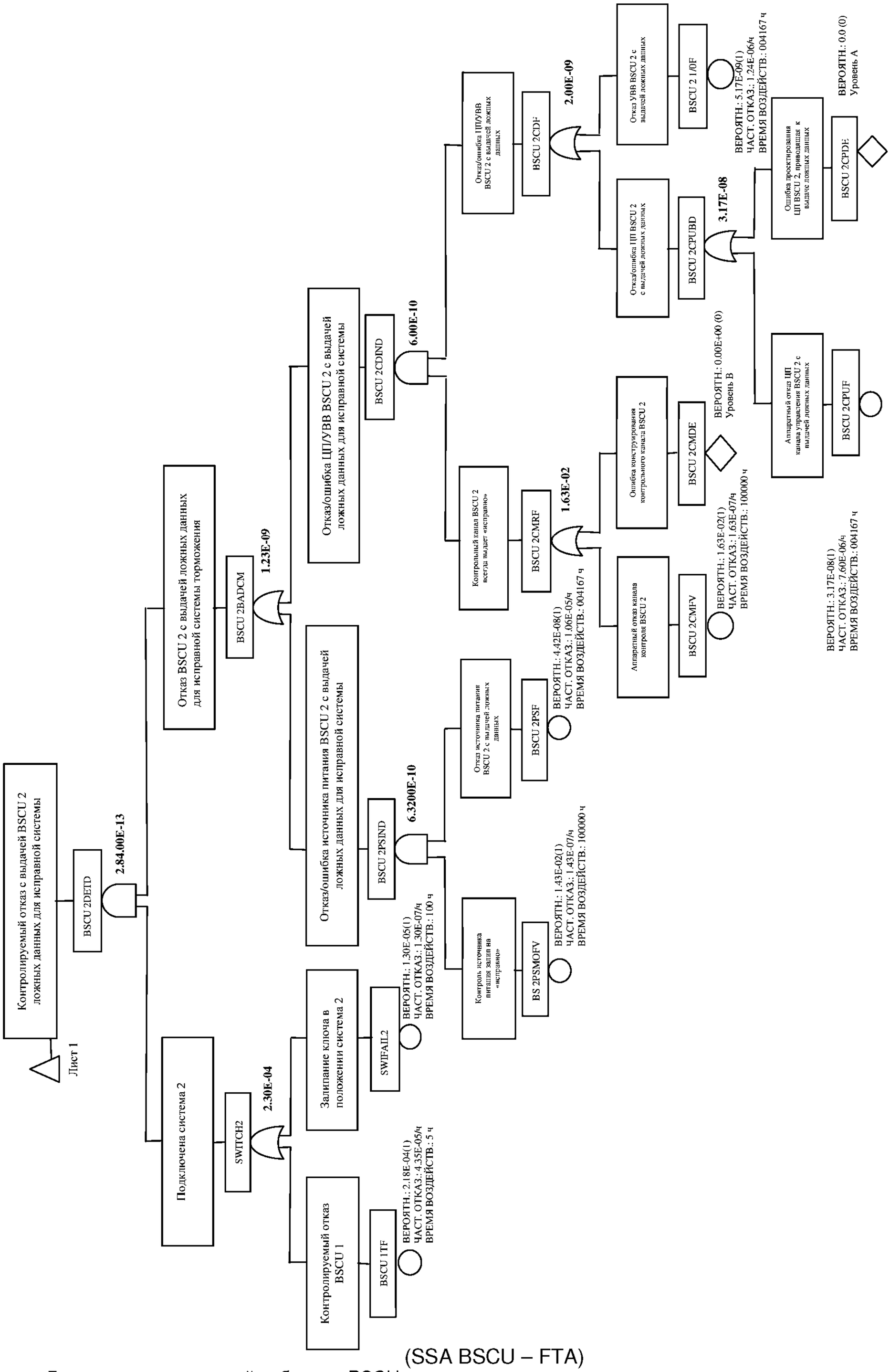
(SSA BSCU – FTA)
Дерево неисправностей события «BSCU подает команды на торможение при отсутствии входного сигнала тормоза и вызывает непреднамеренное торможение» (лист 1 из 3)
Рис. 5.1-2



(SSA BSCU – FTA)

Дерево неисправностей события «BSCU подает команды на торможение при отсутствии входного сигнала тормоза и вызывает непреднамеренное торможение» (лист 2 из 3)

Рис. 5.1-2



(SSA BSCU – FTA)

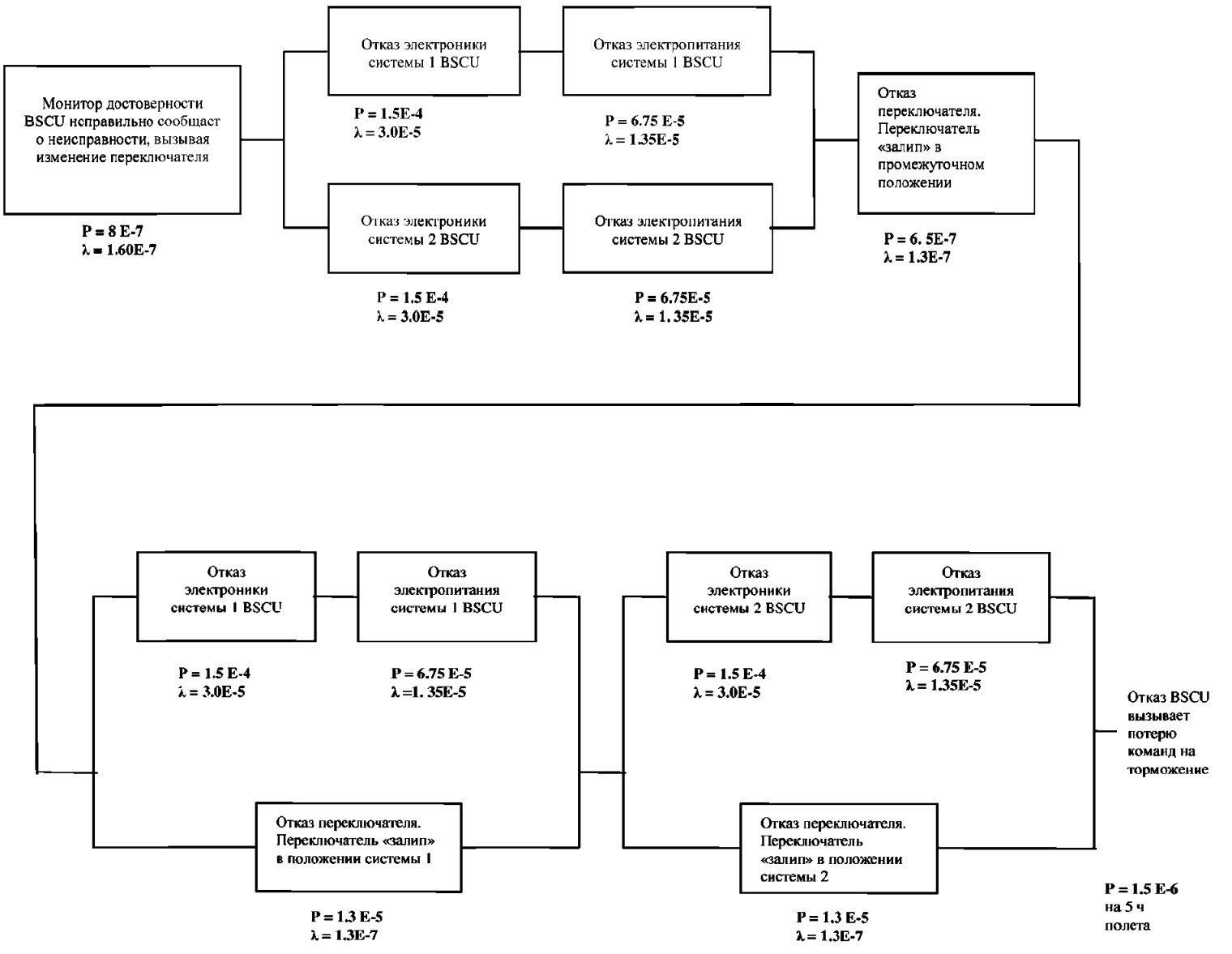
Дерево неисправностей события «BSCU подает команды на торможение при отсутствии входного сигнала тормоза и вызывает непреднамеренное торможение» (лист 3 из 3)

Рис. 5.1-2

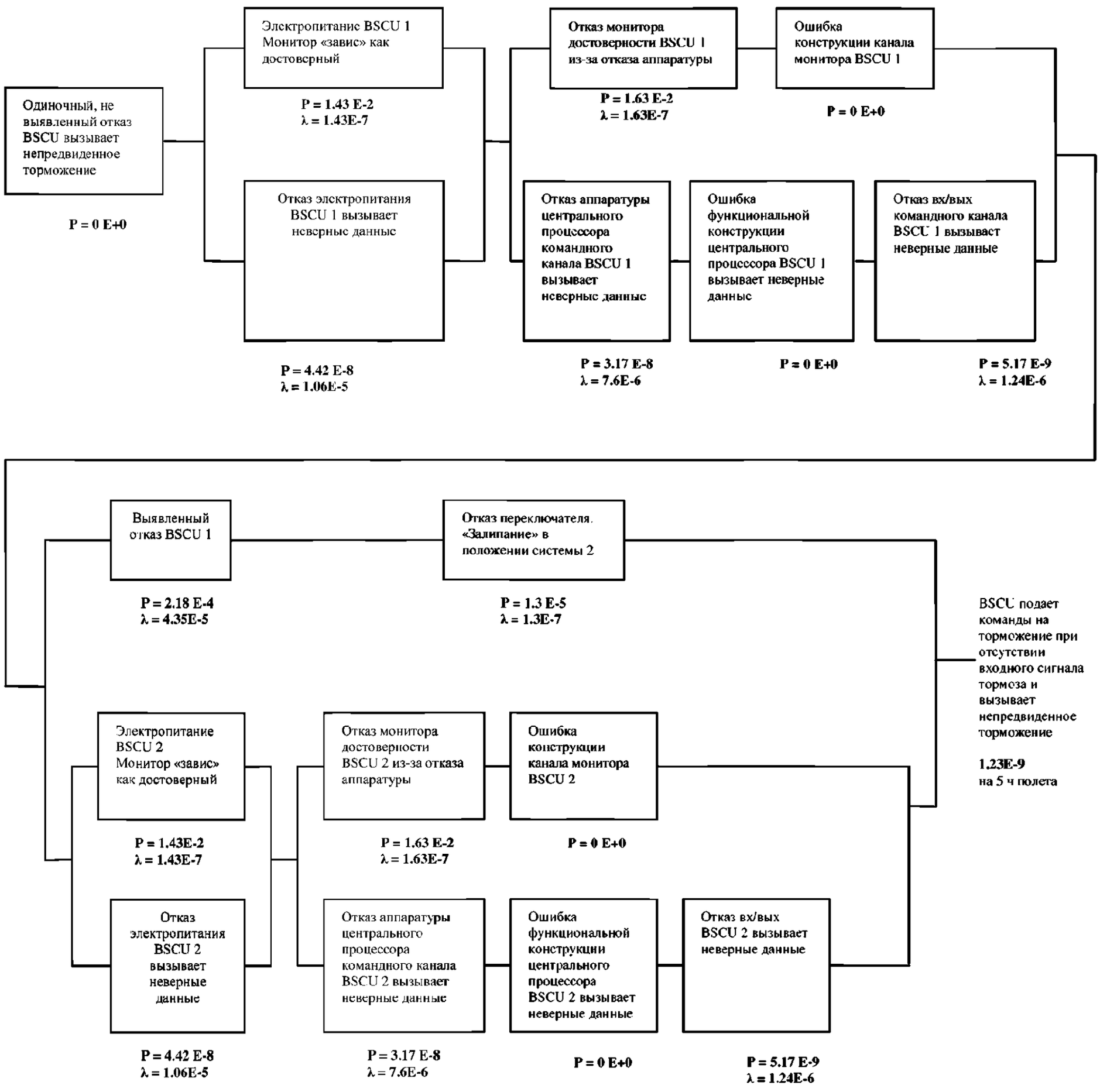
5.2 Логические схемы BSCU

(Примечание редактора: Обычно в анализ должно включаться текстовое описание логических схем. Данный текст будет аналогичен тому, который включен в предыдущий пример FTA).

Удовлетворительное соответствие BSCU его конструктивным целям и запланированным интенсивностям отказов для событий «потеря торможения» и «непреднамеренное торможение» показано на логических схемах, представленных на рис. 5.2-1 и 5.2-2, соответственно. Эти схемы являются теми же самыми, которые получены в PSSA для BSCU. Тем не менее, на схемах SSA запланированные интенсивности отказов заменены на фактические интенсивности отказов, полученные в FMES или в различных FMEA, выполненных по фактической конструкции, на которую выпущена рабочая документация для изготовления.



(SSA BSCU – DD) Отказ BSCU вызывает потерю команд на торможение
Рис. 5.2-1



(SSA BSCU – DD) BSCU подает **команды на торможение при отсутствии входного сигнала тормоза и вызывает непреднамеренное торможение**
Рис. 5.2-2

5.3 Марковский анализ BSCU

(Примечание редактора: Обычно в анализ должно включаться текстовое описание разработки МА. Данный текст будет аналогичен тому, который включен в предыдущий пример FTA).

Удовлетворительное соответствие BSCU его конструктивным целям и запланированным интенсивностям отказов для событий «потеря торможения» и «непреднамеренное торможение» показано на схемах зависимости, представленных на рис. 5.3-1 и 5.3-2, соответственно. Анализировались те же данные, которые получены в PSSA для BSCU. Тем не менее, на схемах SSA запланированные интенсивности отказов заменены на фактические интенсивности отказов, полученные в FMES или в различных FMEA, выполненных по фактической конструкции, на которую выпущена рабочая документация для изготовления.

Марковский анализ события «Отказ BSCU вызывает потерю команды на торможение» показан на рис. 5.3-1. В модели имеется три определенных компонента. Два первых компонента представляют собой систему 1 и систему 2 BSCU, а третьим компонентом является система переключения. Система 1 и система 2 BSCU содержат контрольные устройства (мониторы) и, следовательно, ни один одиночный отказ любого компонента в системе BSCU не сможет вызвать потерю функции торможения колес. Система 1 и система 2 BSCU проверяются в начале каждого полета. С другой стороны, одиночный отказ системы переключения может вызвать потерю НОРМАЛЬНОЙ функции торможения. Это может произойти при отказе переключателя:

a) переключатель «залипает» на неисправную систему BSCU (последовательно зависимый отказ);

b) переключатель разомкнут, так что ни одна из систем BSCU не может обеспечить команды на торможение.

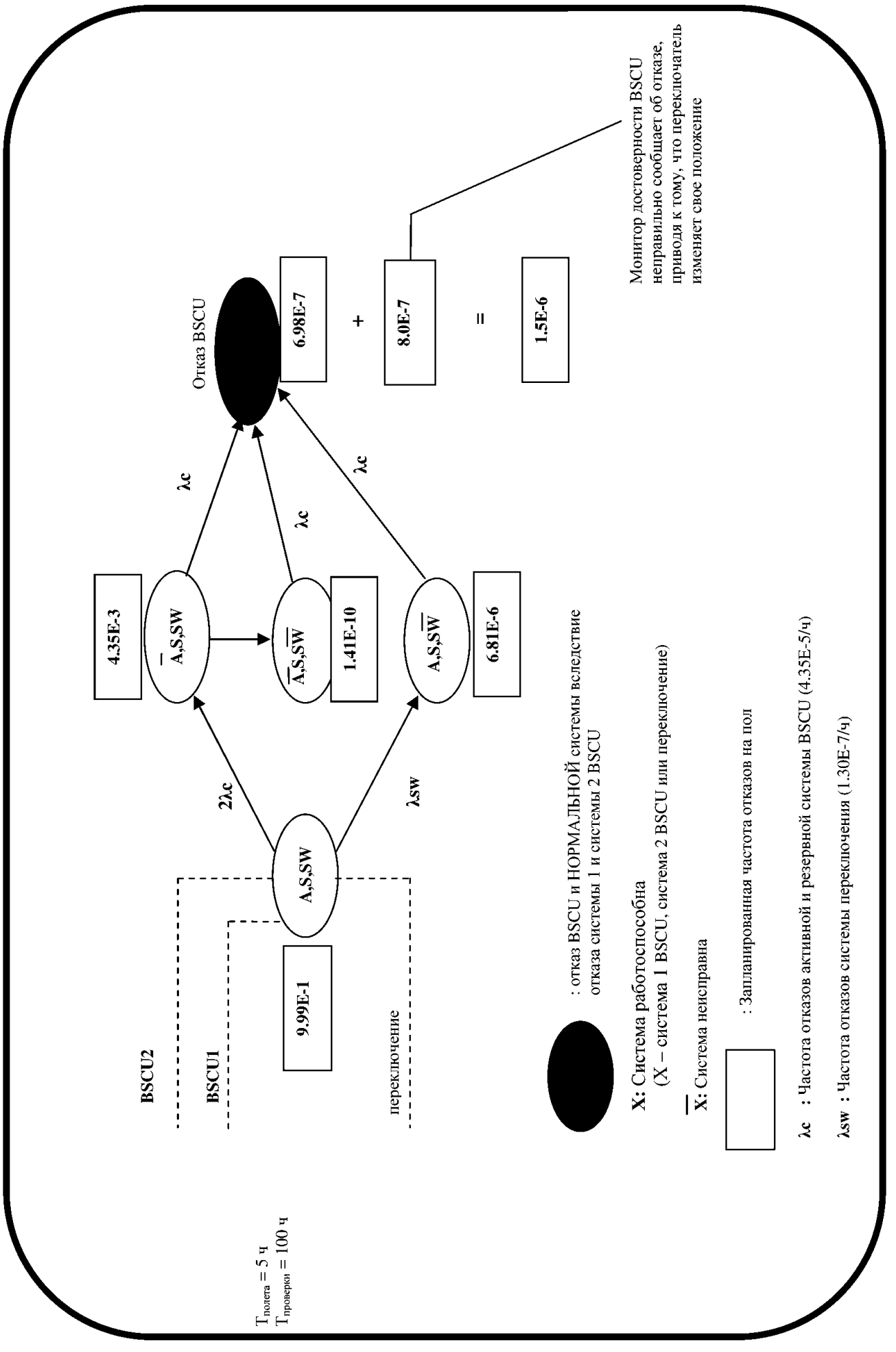
Система переключения проверяется при каждом техническом обслуживании с интервалом T часов, который для данного анализа принимается равным 100 ч. Отказ системы BSCU в полете происходит в том случае, когда:

a) обе системы BSCU отказывают в одном и том же полете;

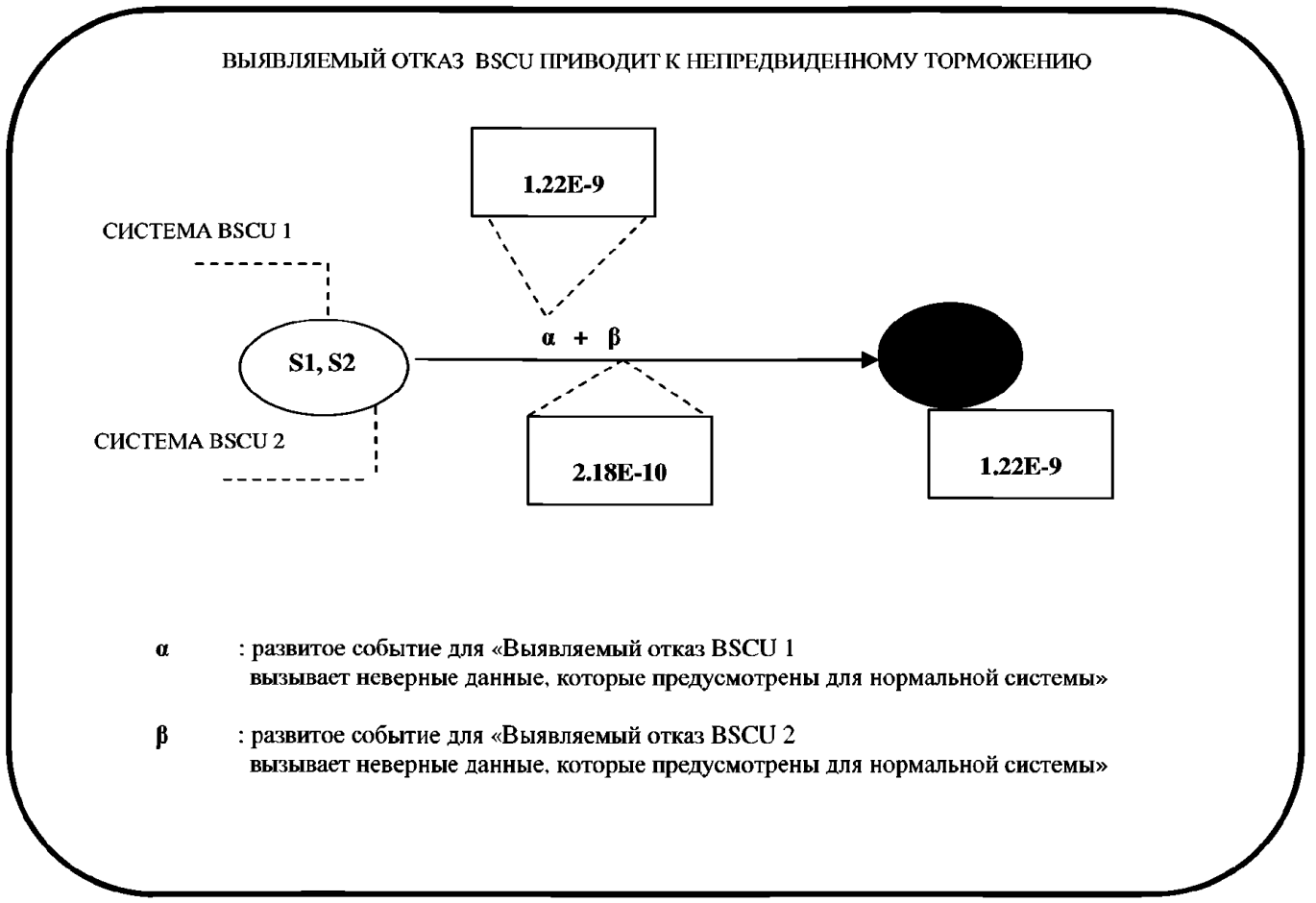
b) отказ системы переключения следует за отказом системы BSCU, к которому подключена система переключения (последовательно зависимый отказ);

c) система переключения «залипает» в разомкнутом состоянии и не может обеспечить никакие команды на торможение.

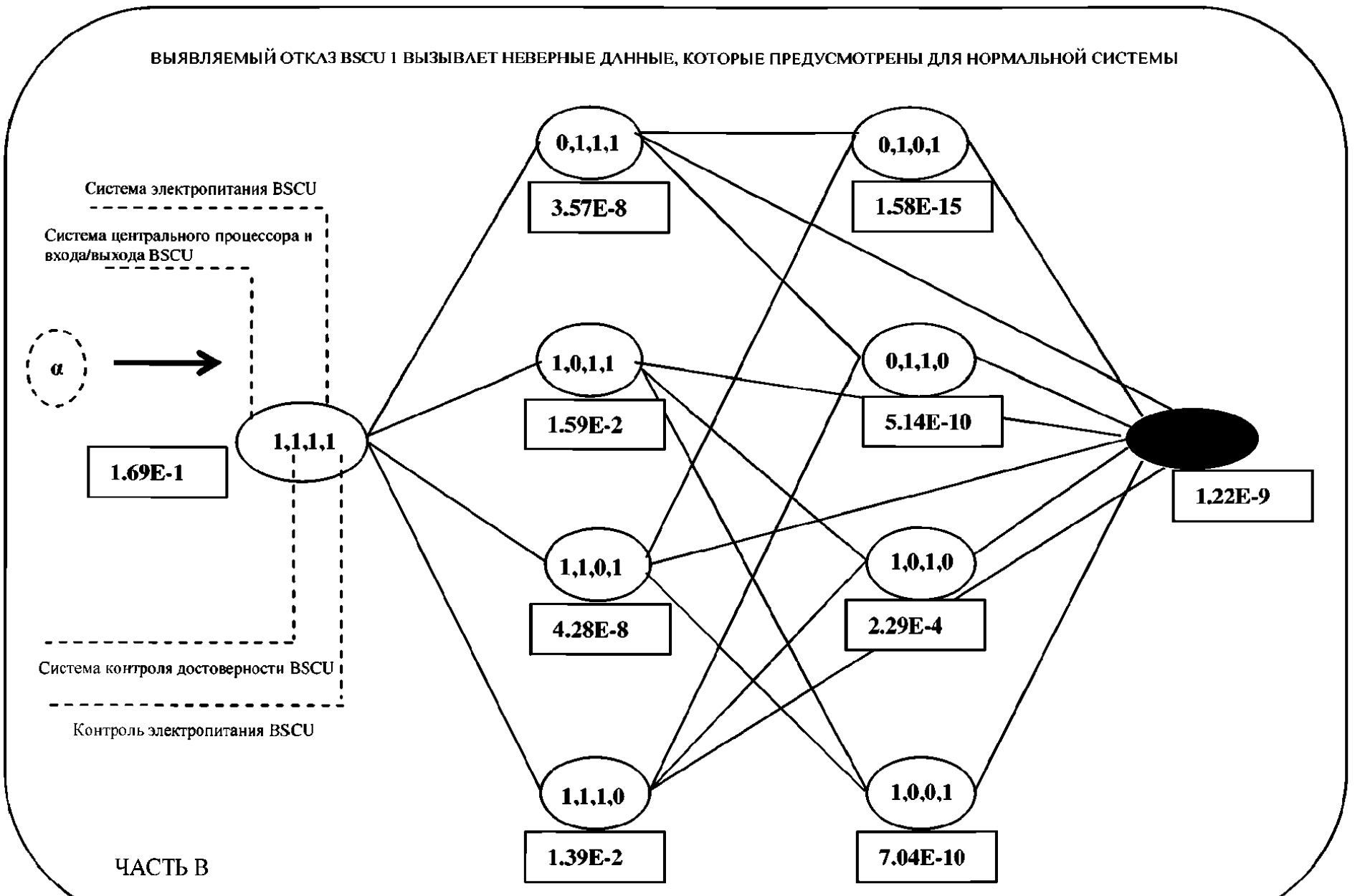
На рис. 5.3-2 – 4 показан МА для непредвиденного торможения из-за монитора и активного отказа в обеих системах BSCU. Данная модель Маркова аналогичная модели, использованной в PSSA системы BSCU, за исключением того, что введена цепочка отказов. В модели, показанной в качестве примера на рис. 5.3-3, предполагается, что система BSCU должна отказать только в том случае, когда монитор системы отказывает до неисправности активного изделия. Следовательно, система входа/выхода и центрального процессора BSCU отказывает только в том случае, когда монитор входа/выхода и центрального процессора отказывает до отказа входа/выхода и центрального процессора в полете. Аналогичным образом, монитор электропитания должен отказать до отказа системы электропитания.



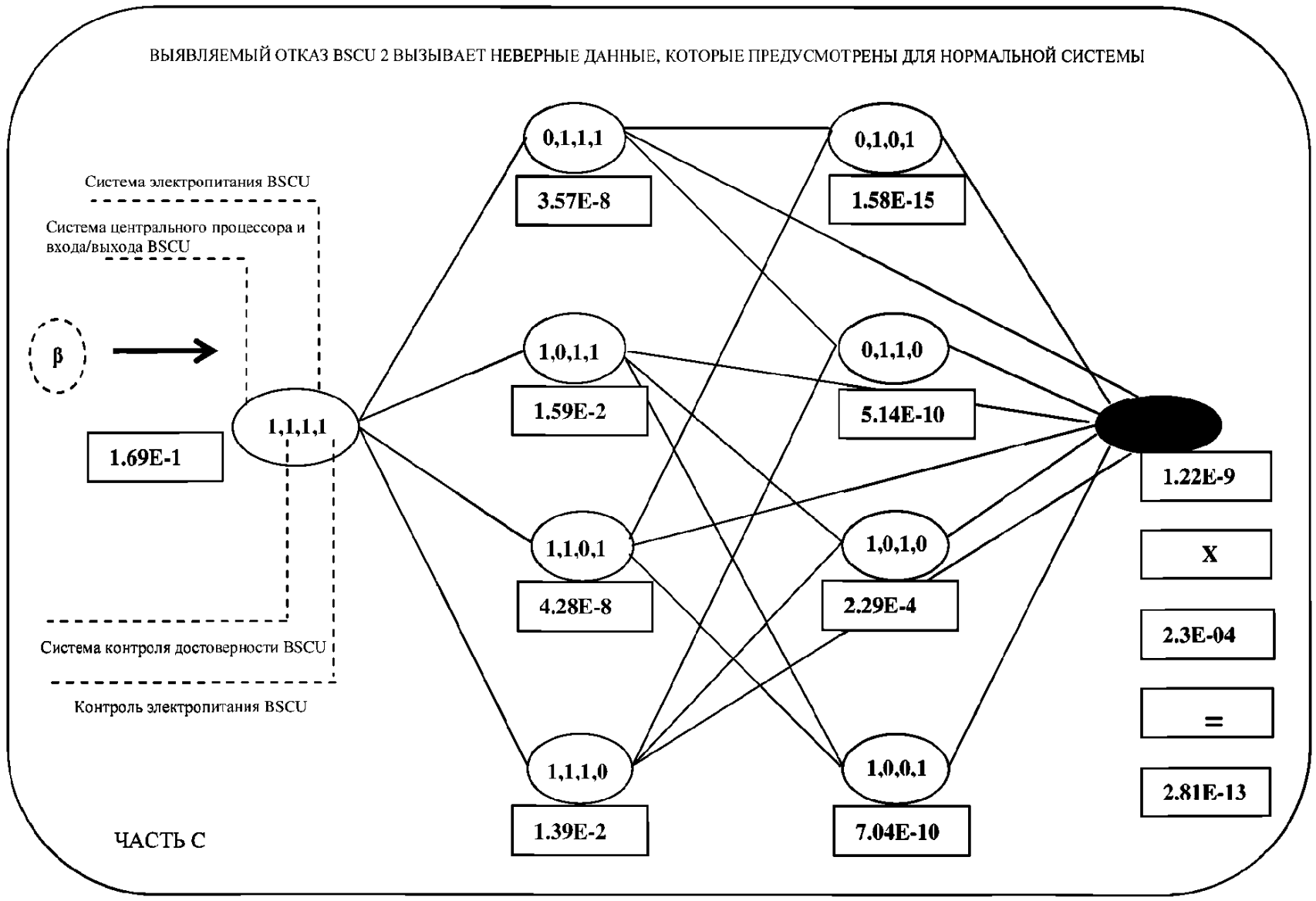
(SSA BSCU – MA)
Отказ BSCU вызывает потерю команды на торможение
Рис. 5.3-1



(SSA BSCU – MA)
Непредвиденное торможение вследствие отказа обеих систем и их мониторов
Рис. 5.3-2



(SSA BSCU – MA)
Непредвиденное торможение вследствие отказа системы 1 BSCU
(для ясности ремонт компонентов не показан)
Рис. 5.3-3



(SSA BSCU – MA)
Непреднамеренное торможение вследствие отказа системы 2 BSCU
и отказа механизма переключения (для ясности ремонт компонентов не показан)
Рис. 5.3-4

ОЦЕНКА БЕЗОПАСНОСТИ СИСТЕМЫ ДЛЯ СИСТЕМЫ ТОРМОЖЕНИЯ КОЛЕС

1.0 ВВЕДЕНИЕ

SSA системы торможения колес представляет собой краткую сводку по оценкам и анализам, выполненным на стадии разработки и обоснования процесса проектирования данной системы. Эти оценки и анализы включают исходные данные из PSSA системы торможения колес. SSA предназначена для обеспечения регистрации данных о том, каким образом конструкция системы торможения колес отвечает требованиям по безопасности, установленным для нее в процессе PSSA.

(Примечание редактора: В следующей таблице перекрестных ссылок представлена связь каждого параграфа примера с применяемым параграфом приложения).

№ параграфа SSA системы	Приложение
4.0	C.3.1.1
5.0	C.3.3
5.1	Приложение H
5.2	Приложение D
5.3	Приложение E
5.4	Приложение F
5.5	C.3.4, Приложение I, J и K

2.0 ССЫЛКИ

1) FHA самолета S18.
2) PSSA системы торможения колес (включая FHA системы).
3) CMA самолета S18.
4) CMA системы торможения колес.
5) BSCU CMA.
6) Анализ специфического риска S18.
7) Анализ зонной безопасности S18.
8) BSCU FMEA/FMES.
9) BSCU FTA.
10) АП-25 25.1309.
11) P4754 «Руководство по сертификации для высоко интегрированных или сложных авиационных систем».
12) P4761 «Руководство по методам оценки безопасности систем и бортового оборудования самолетов гражданской авиации».
13) «Документ с конструктивными требованиям и целями» S18 (Технические требования на проектирование S18).

3.0 КРАТКОЕ ОПИСАНИЕ

(Примечание редактора: Для цели данной инструкции см. описание системы торможения колес в примере PSSA. В случае реальной SSA здесь также должно быть представлено пересмотренное и окончательное описание).

4.0 ТРЕБОВАНИЯ ПО БЕЗОПАСНОСТИ СИСТЕМЫ ТОРМОЖЕНИЯ КОЛЕС

Самолет S18 должен отвечать следующим требованиям к безопасности.

1) Вероятность потери торможения всех колес во время посадки или RTO должна быть менее 5E-7 на полет.

2) Вероятность асимметричной потери торможения колеса, связанной с потерей управления рулем или носовым колесом во время посадки, должна быть менее 5E-7 на полет.

3) Вероятность непреднамеренного торможения колеса при всех заблокированных колесах во время разбега при взлете до V1 должна быть менее 5E-7 на полет.

4) Вероятность непреднамеренного торможения всех колес во время разбега при взлете после V1 должна быть менее 5E-9 на полет.

5) Вероятность не выявленного непреднамеренного торможения одного колеса без блокировки во время взлета должна быть менее 5E-9 на полет.

6) Для предотвращения любых общих опасностей (разрыва шины, кромсания шины, нарушения протектора, конструкционных деформаций, и т.п.) должны быть спроектированы нормальная, альтернативная и аварийная системы.

7) Для предотвращения отказов общего режима (гидравлической системы, электрической системы, технического обслуживания, текущего ремонта, операций, конструкции, изготовления и т.п.) должны быть спроектированы нормальная, альтернативная и аварийная системы.

8) Никакой одиночный отказ BSCU не должен приводить к непреднамеренному торможению.

9) BSCU должен быть спроектирован для уровня гарантии разработки A.

5.0. ПРОВЕРКА ТРЕБОВАНИЙ ПО БЕЗОПАСНОСТИ

Требования по безопасности, идентифицированные в разделе 4.0, определены как корректные и полные для системы торможения колес. Перечень, представленный в таблице 5.0-1, определяет то, каким образом каждое требование было проверено.

Таблица 5.0-1 – (SSA Система торможения колес) Матрица проверки требований к безопасности колесной тормозной системы

Требование по безопасности	Результаты	Метод проверки и примечания
1. Вероятность потери торможения всех колес во время посадки или RTO должна быть менее 5E-7 на полет.	Выполняется (3,2E-8)	Анализ См. CTK SSA FTA 5.2-1
2. Вероятность асимметричной потери торможения колеса, связанной с потерей управления рулем или носовым колесом во время посадки, должна быть менее 5E-7 на полет.	Выполняется (4E-7)	Анализ См. CTK SSA FTA 5.2-X *(Примечание редактора: данный анализ в данном примере не показан)*
3. Вероятность непреднамеренного торможения колеса при всех заблокированных колесах во время разбега при взлете до V1 должна быть меньше, чем 5E-7 на полет.	Выполняется (3E-7)	Анализ См. CTK SSA FTA 5.2-Y *(Примечание редактора: данный анализ в данном примере не показан)*
4. Вероятность непреднамеренного торможения всех колес во время разбега при взлете после V1 должна быть меньше, чем 5E-9 на полет.	Выполняется (4E-9)	Анализ См. CTK SSA FTA 5.2-Z *(Примечание редактора: данный анализ в данном примере не показан)* См. CTK CMA

Требование по безопасности	Результаты	Метод проверки и примечания
5. Вероятность не выявленного непреднамеренного торможения одного колеса без блокировки во время взлета должна быть меньше, чем 5E-9 на полет.	Выполняется (3E-9)	Анализ См. CTK SSA FTA 5.2-AA *(Примечание редактора: данный анализ в данном примере не показан)* См. CTK CMA
6. Для предотвращения любых общих опасностей (разрыва шины, кромсания шины, нарушения протектора, конструкционных деформаций, и т.п.) должны быть спроектированы нормальная, альтернативная и аварийная системы.	Выполняется	Анализ См. разрыв шины -PRA
7. Для предотвращения отказов общего режима (гидравлической системы, электрической системы, технического обслуживания, текущего ремонта, операций, конструкции, изготовления и т.п.) должны быть спроектированы нормальная, альтернативная и аварийная системы.	Выполняется	Анализ См. CTK CMA
8. Никакой одиночный отказ BSCU не должен приводить к непреднамеренному торможению.	Выполняется	Анализ См. BSCU CMA
9. BSCU должен быть спроектирован для уровня A обеспечения разработки.	Выполняется	Процедуры/аудит См. инструкции поставщиков

5.1 Сводка по видам и последствиям отказов (FMES)

В данном отчете представлена сводка по видам и последствиям отказов системы торможения колес, которые определены в анализах FMEA, проведенных для различных изделий в системе.

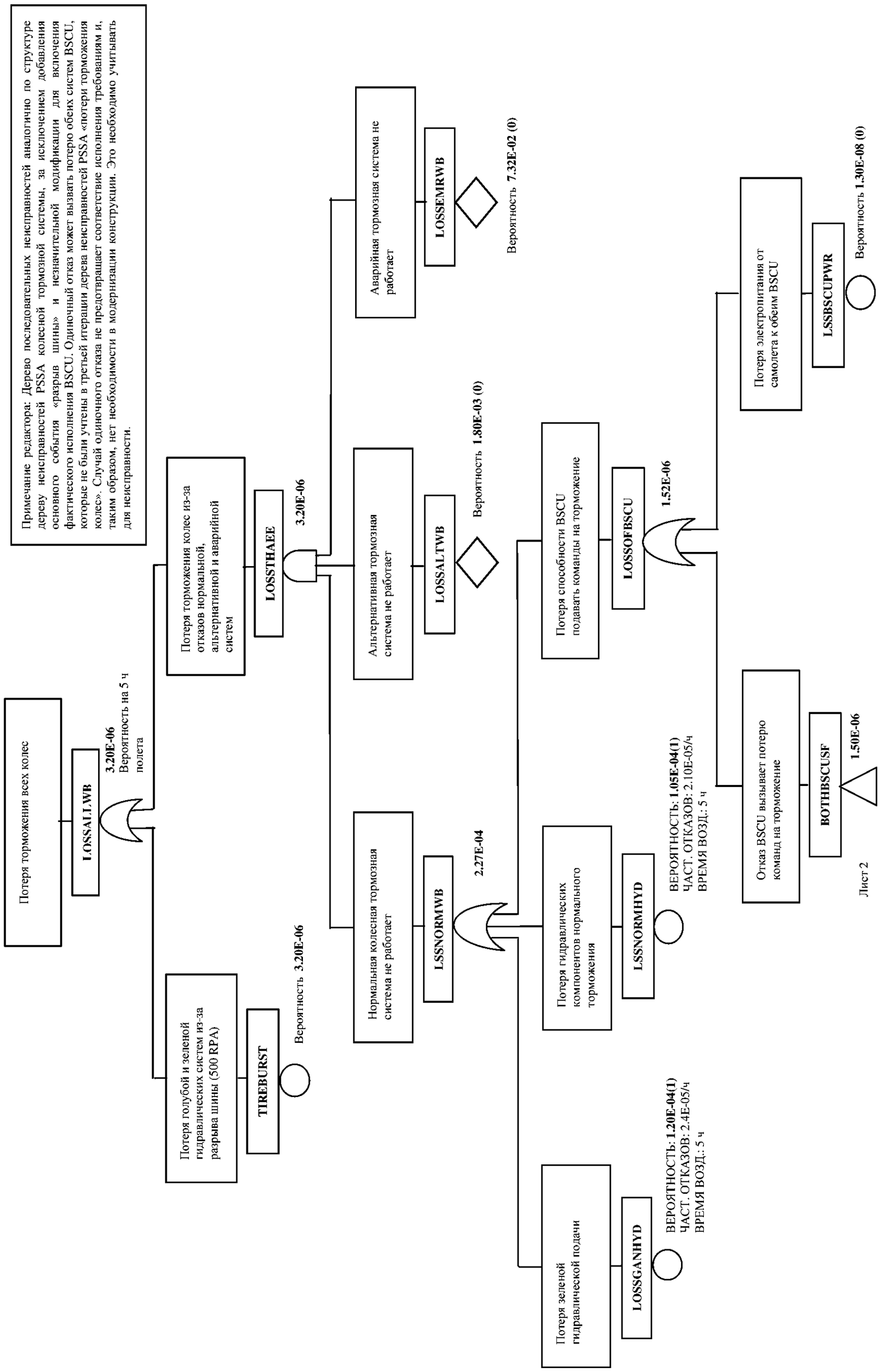
Проведена экспертиза FMEA системы с точки зрения перспективы объединения всех идентифицированных видов отказов, которые имеют то же самое влияние на отказы верхнего уровня системы. Комбинированные интенсивности отказов для этих последствий были рассчитаны при помощи суммирования индивидуальных интенсивностей отказов, дающих вклад в этот отказ. Результаты такого суммирования представлены в таблице 5.1-1.

Таблица 5.1-1 (SSA Система торможения колес – FMES)
FMES влияний отказов торможения

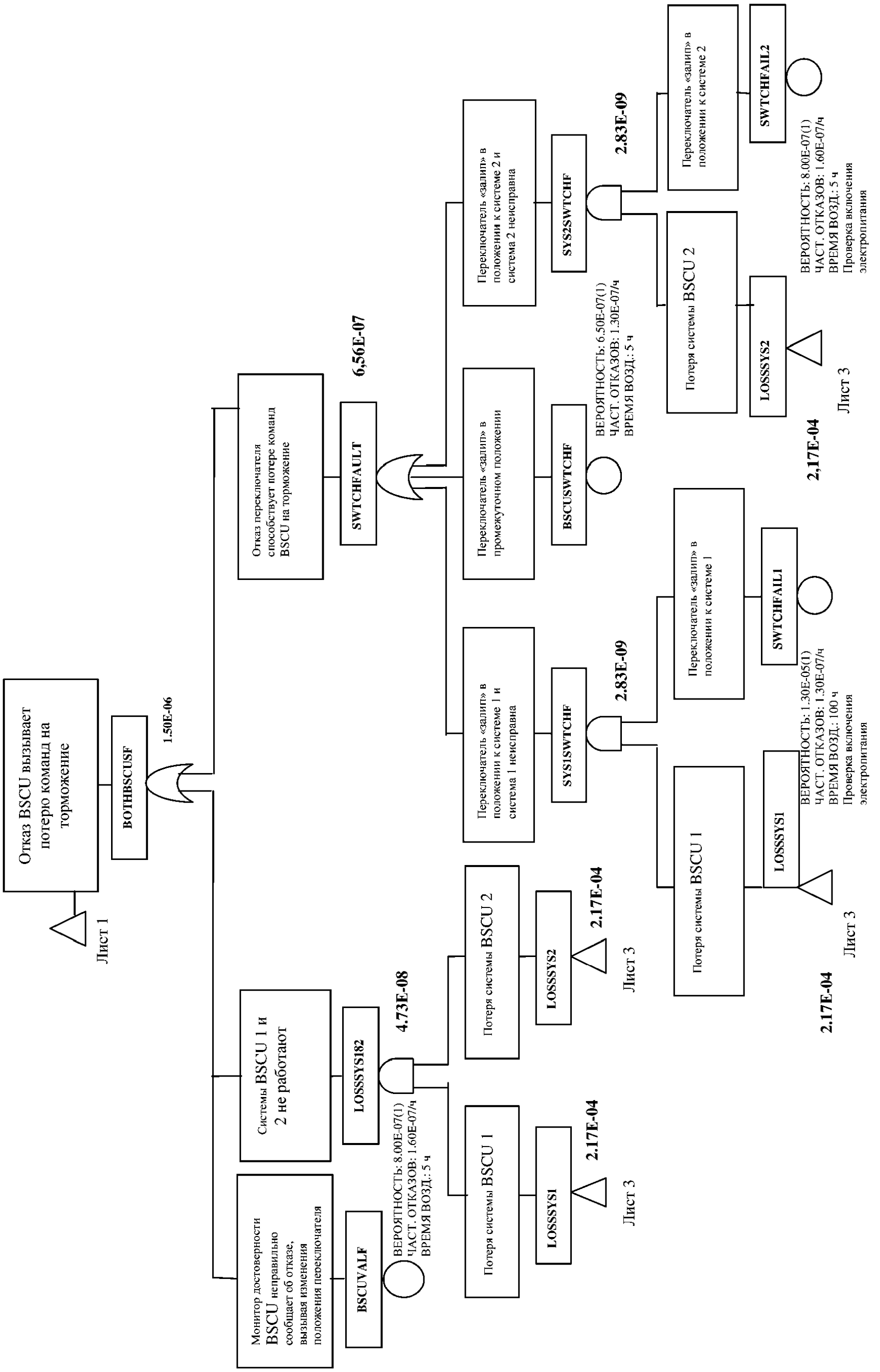
Режим отказа	**Частота отказов**	**Потенциальное влияние на систему торможения**	**Потенциальная причина отказа *(источник отказа)***	**Обнаруживаемость**	**Примечания**
Потеря одиночного командного канала BSCU	8,70-5	Нет	– потеря команды на торможение от канала 1 или 2 *(см. BSCU FMES)*	При помощи BITE, отказ хранится в BSCU	Торможение по командам резервного канала.
Потеря обоих командных каналов BSCU	4,0E-7	Потеря режима нормального торможения	– отказ BSCU *(см. BSCU FMES)* – отказ датчиков тормозной педали *(см. FMEA датчиков педали)*	Идентификация по системному дисплею: «Потеря нормального торможения»	Используется альтернативное торможение. Автоматические тормоза больше не доступны.
			– потеря электропитания BSCU *(см. SSA электрической системы)*		
Команда на непреднамеренное торможение	2,85E-8	Используются тормоза	– отказ BSCU *(см. BSCU FMES)* – отказ датчиков тормозной педали *(см. FMEA датчиков педали)*	Очевидно по влиянию	Самолет может выбежать за пределы взлетно-посадочной полосы с большой скоростью.
Команда асимметричного торможения	3,6E-8	Тормоза прикладываются асимметрично между двумя шасси	отказ BSCU *(см. BSCU FMES)* – отказ датчиков тормозной педали *(см. FMEA датчиков педали)*	Очевидно по влиянию	Самолет не может отслеживать осевую линию взлетно-посадочной полосы.
Потеря зеленой гидравлической системы		Потеря нормального режима торможения			Используется альтернативное торможение. Автоматические тормоза больше не доступны.
Потеря голубой гидравлической системы		Потеря альтернативного режима торможения			Используется нормальное торможение.
…					
…					
…					

5.2 Анализ дерева неисправности системы торможения.

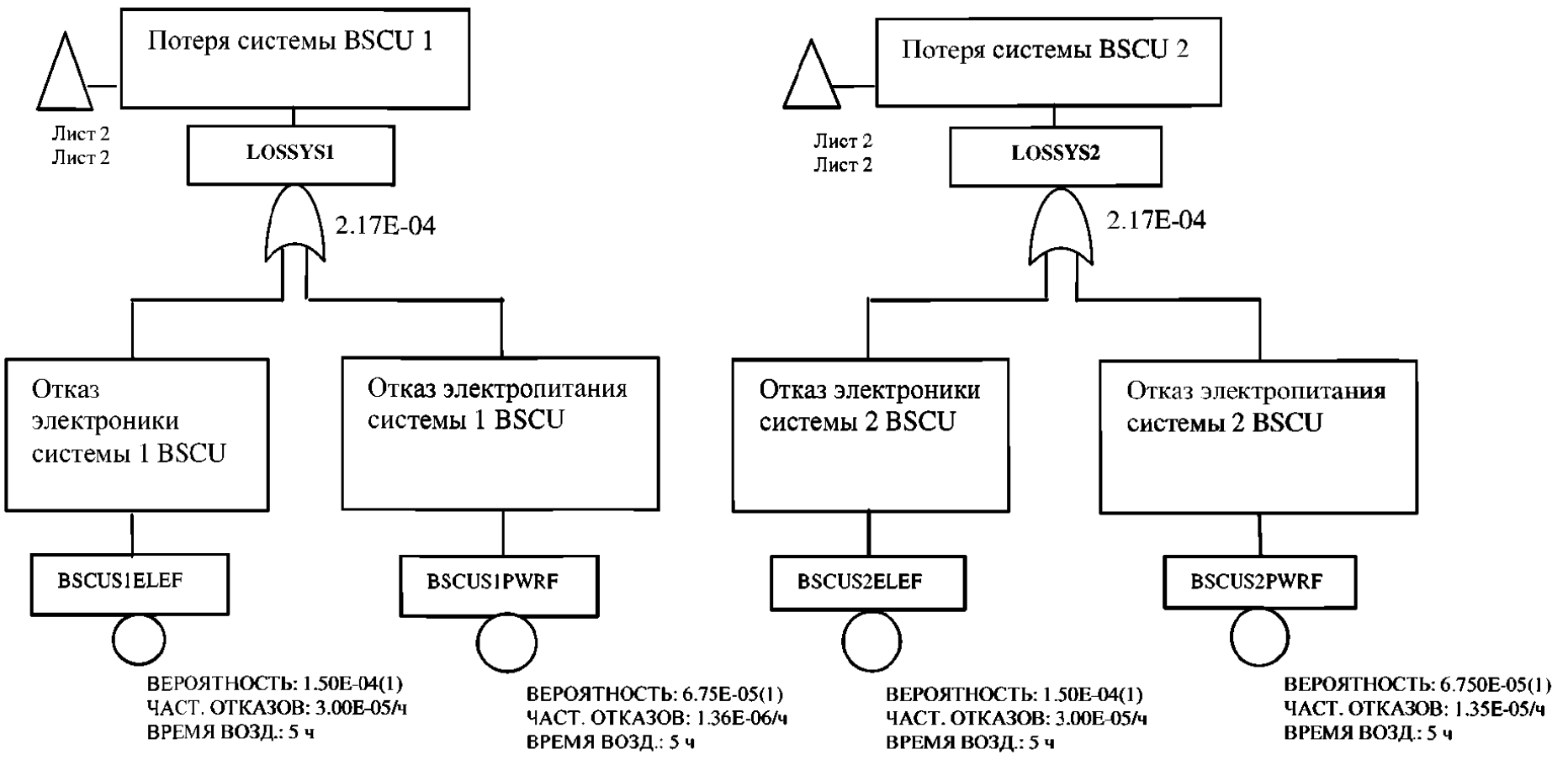
Удовлетворительное соответствие СТК ее проектным требованиям и запланированным интенсивностям отказов для события «Потеря торможения» демонстрируется деревьями неисправностей, представленными на рис. 5.2-1. Дерево неисправностей является таким же, что полученное в PSSA для СТК, тем не менее в деревьях неисправностей, полученные в SSA запланированные интенсивности отказов заменены на фактические, полученные из различных анализов FMEA, проведенных по фактической конструкции, на которую выпущена рабочая документация для изготовления.



(SSA Система торможения колес – FTA)
Дерево неисправности потери торможения всех колес (лист 1 из 3)
Рис. 5.2-1



(SSA Система торможения колес – FTA)
Дерево неисправности потери торможения всех колес (лист 2 из 3)
Рис. 5.2-1



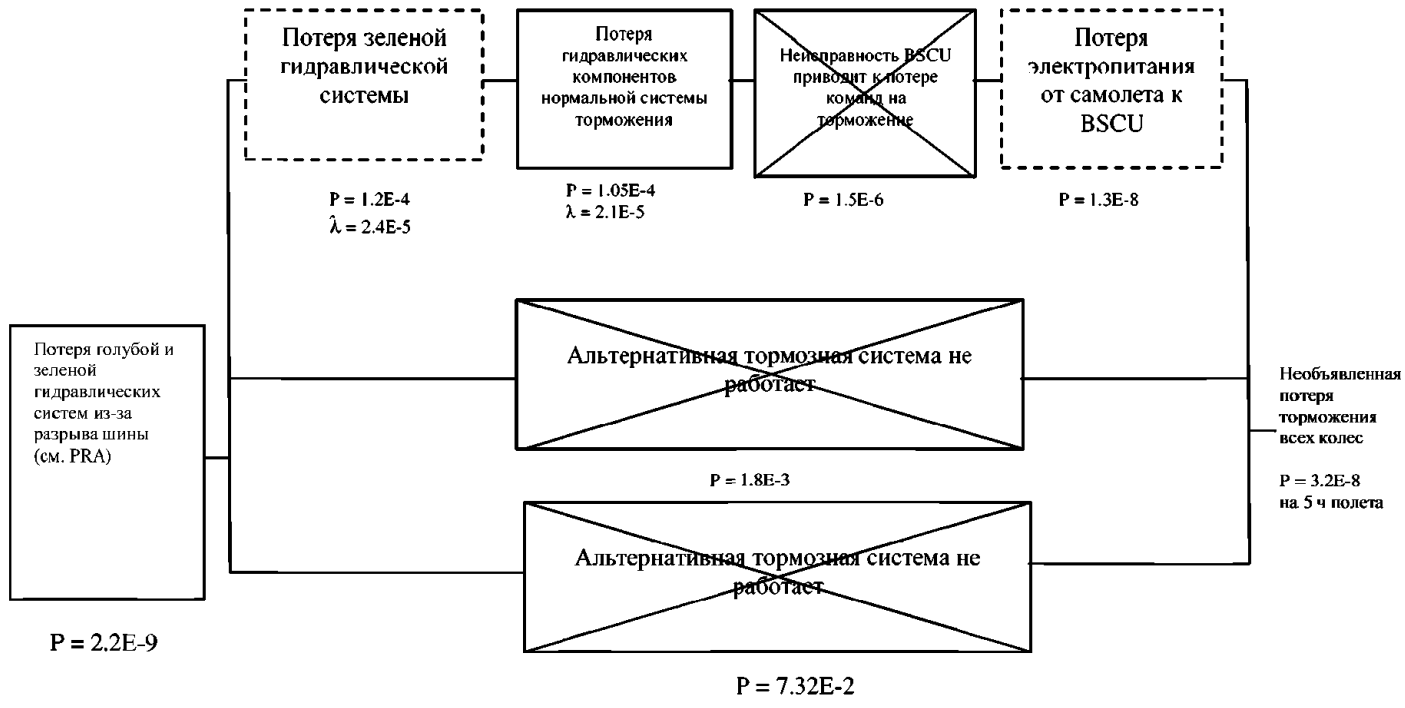
(SSA Система торможения колес – FTA)
Дерево неисправности потери торможения всех колес (лист 3 из 3)
Рис. 5.2-1

5.3 Логические схемы системы торможения

(Примечание редактора: Данный раздел представляет собой прямую замену раздела 5.2 «FTA системы торможения колес» в примере SSA).

Удовлетворительное соответствие СТК ее проектным требованиям и запланированным частотам отказов для события «Потеря торможения» демонстрируется схемой зависимости, представленной на рис. 5.3-1. Схема зависимости является такой же, что полученная в PSSA для СТК. Тем не менее, в SSA запланированные интенсивности отказов заменены на фактические, полученные из различных анализов FMEA, проведенных по фактической конструкции, на которую выпущена рабочая документация для изготовления.

Данный отчет содержит входные данные из FMES тормозной системы и DD BSCU.



(SSA – Система торможения колес – DD) Потеря торможения всех колес
Рис. 5.3-1

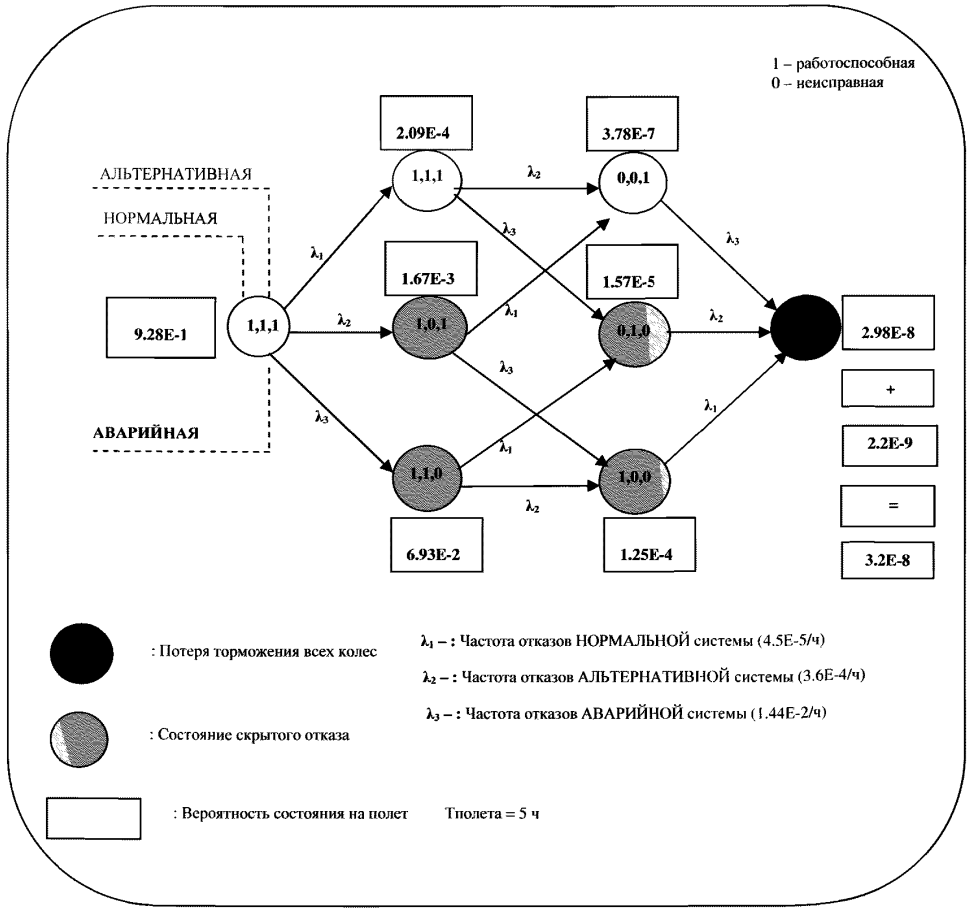
Примечание редактора: Представленная выше логическая схема аналогична по структуре PSSA DD системы, за исключением добавления основного события «разрыв шины» и незначительной модификации для включения фактического исполнения BSCU. Одиночный отказ может вызвать потерю обеих систем BSCU, которые не были учтены в третьей итерации PSSA DD «Несигнализируемая потеря торможения всех колес». Случай одиночного отказа не предотвращает соответствие исполнения требованиям и, таким образом, нет необходимости в модернизации конструкции. Это необходимо учитывать при рассмотрении отказа.

5.4 Марковский анализ тормозной системы

(Примечание редактора: Данный раздел представляет собой прямую замену раздела 5.2 «FTA системы торможения колес» в примере SSA).

Марковский анализ для «Потери торможения всех колес» включает в себя два этапа. Во-первых, рассчитывается среднее время между критическими отказами BSCU – MTBCF. Марковская цепь, показанная на рис. 5.4-1, может использоваться для расчета целиком среднего времени для BSCU. Затем эти результаты могут быть включены в модель SSA системы. Значения среднего времени, рассчитанные на первом этапе, используются для расчета интенсивности отказов НОРМАЛЬНОЙ тормозной системы. Частота отказов НОРМАЛЬНОЙ тормозной системы равна 1/ MTBCF для двухканальной системы BSCU плюс частота отказов зеленой гидравлической системы, плюс частота отказов гидравлических компонентов НОРМАЛЬНОЙ тормозной системы.

Частота отказов НОРМАЛЬНОЙ тормозной системы (λ_1) равна 4,52E-5 в час. Марковская цепь, показанная на рис. 5.4-1, разрешена для расчета средней вероятности за полет «потери торможения всех колес». Частоты отказов, используемые для АЛЬТЕРНАТИВНОЙ и АВАРИЙНОЙ систем, равны 3,6E-4 и 1,44E-2 отказа в час, соответственно. Средние вероятности состояния на полет показаны в Марковской цепи на рис. 5.4-1. Средняя вероятность потери всех трех функций торможения равна 2,98E-8 на 5 часов полета. Таким образом, при добавлении события «Потеря голубой и зеленой гидравлических систем из-за разрыва шины» (вероятность 2,2E-9 на 5 часов полета) в результате получается средняя вероятность отказа для события "Потеря торможения всех колес", равная 3,2E-8 на 5 часов полета. Это хорошо согласуется с запланированной вероятностью события «Потеря торможения всех колес», равной 5E-7 на полет.



(SSA – Система торможения колес – MA) Потеря торможения всех колес
Рис. 5.4-1

5.5 Анализ общих причин системы торможения колес, сводка результатов

5.5.1 Сводка результатов зонного анализа безопасности самолета S18, относящегося к тормозной системе

Зонный анализ безопасности № YYY для самолета S18 показывает, что установка тормозной системы соответствует инструкциям на установку, и что от установки не ожидается неприемлемых отказов с общей причиной.

На дереве неисправности рассмотрены отказы компонентов с влиянием, внешним по отношению к компоненту.

5.5.2 Сводка результатов анализа специфического риска самолета S18, относящегося к тормозной системе

Для самолета S18 проведены следующие анализы, которые относятся к тормозной системе.

1) Анализ специфического риска № XYZ самолета S18.

2) Анализ специфического риска № ZZZ для самолета S18, пожара, разрыва шины, удара молнии.

(Примечание редактора: Для самолета S18 должны быть проведены и другие анализы, но для краткости они здесь не представлены).

Наихудшим влиянием отказа в результате специфического риска является «общая потеря торможения колес» вследствие разрыва шины. Этот отказ был рассмотрен в FTA.

5.5.3 Сводка по анализу общего режима самолета S18 для функции торможения колес.

Анализ общего режима для функции колесного торможения № ZXY и анализы № ZZZ для электрической системы и № WWW для гидравлической системы *(Примечание редактора: В данном примере не показаны)* показали следующее:

a) не было выявлено никаких событий в результате типовой ошибки общего режима, которые имеют катастрофическое влияние;

b) те типовые ошибки общего режима, которые могут привести к опасному влиянию, ограничиваются специальными испытаниями, процессами изготовления, средствами обеспечения качества, или они являются приемлемыми с учетом их вероятности.

5.5.4 Анализ общего режима для основных изделий тормозной системы

Был проведен анализ общего режима для BSCU, который показал, что не существует для BSCU неисправности общего режима, которая может привести к потере торможения колес или непредвиденного торможения колес.

5.5.5 Задача технического обслуживания и интервалы для обеспечения безопасности тормозной системы.

Были определены следующие задачи и интервалы технического обслуживания.

1) Интервал регламентной проверки альтернативной тормозной системы: MT2.

2) Интервал регламентной проверки мониторов A и B электропитания: MT1.

5.6 Перекрестная проверка интеграции системы

В таблице 5.6-1 представлена матрица соответствия, показывающая то, что конструкция системы торможения колес, анализируемая в SSA, соответствует целевым функциям, идентифицированным в параграфах раздела 4.6 по FHA системного уровня.

Таблица 5.6-1 (SSA – Система торможения колес – Перекрестная проверка интеграции)
Матрица соответствия перекрестной проверки интеграции систем

ТРЕБОВАНИЕ FHA			ПРОЕКТНЫЕ РЕЗУЛЬТАТЫ ИЗ SSA		
№	Состояние	Целевая функция	Событие	Вероятность	Ссылка
1	Потеря всего торможения во время посадки или RTO	5E-7	Потеря всего торможения	3,2E-8	SSA FTA Рис. 5.2-1
2	Асимметричная потеря колесного торможения и потеря управления рулем или носовым колесом	5E-7	*(Примечание редактора: Не разработано в данном примере)*		
3	Непредвиденное торможение во время разбега при взлете или пробега после посадки	5E-7	*(Примечание редактора: Не разработано в данном примере)*		
4	Непредвиденное торможение колес во время взлета до V1	5E-9	*(Примечание редактора: Не разработано в данном примере)*		
5	Не определяемое непредвиденное торможение колес во время взлета	5E-9	*(Примечание редактора: Не разработано в данном примере)*		

ЗОННЫЙ АНАЛИЗ БЕЗОПАСНОСТИ ДЛЯ САМОЛЕТА S18

(Примечание редактора: Подробную информацию по процессу ZSA см. в Приложении 1).

1.0 ВВЕДЕНИЕ

Данный анализ представляет собой зонный анализ безопасности для отсека основного шасси самолета S18. Самолет S18 должен выполнять требование, что ни одно событие в результате одиночного отказа из-за установки не приведет к катастрофическому отказу. *(Примечание редактора: В данном примере «потере способности снижения скорости»)*, и что такие отказные состояния с аварийными последствиями имеют соответствующую низкую вероятность.

(Примечание редактора: Документ ZSA может включать в себя более одной зоны. Был выбран пример «отсек основного шасси», поскольку в нем установлено большое количество систем, которые могут влиять как на колесное торможение, так и/или на реверсоры тяги).

2.0 ССЫЛКИ

1) FHA самолета S18.

2) FHA системы торможения колес.

3) FHA гидравлической системы.

4) FHA системы реверсора тяги.

5) FHA системы тормозного интерцептора.

6) Нормы проектирования, общие положения для самолета S-18.

7) Нормы проектирования, гидравлическая установка.

8) Нормы проектирования, электрическая установка.

3.0 ОПИСАНИЕ

Данный пример зонного анализа безопасности включает в себя отсек основного шасси. Подробное описание зоны представлено в разделе 4.2.1. Целью анализа является демонстрация того, что системы, установленные в этой зоне, не могут вызвать опасность для самолета и/или пассажиров. Анализ был проведен для первого изготовленного самолета с использованием соответствующих нормативов для проектирования и установки. Несоответствия данным нормативам и их состояние собраны в разделе 4.2.2 данного анализа. Анализ отказов, внешних по отношению к компонентам, и их влияние на соответствующую систему и смежные системы показаны в разделе 4.3.2.

Рассмотрение внешних событий, например, нелокализованное разрушение двигателя и разрыв шины или разъединение обода колеса, будут представлены в отдельных анализах специфического риска.

4.0 ЗАДАЧИ АНАЛИЗА

4.1 Подготовка инструкций по проектированию и установке

Во время PSSA разрабатываются соответствующие проектные нормативы и контрольные перечни, которые используются для проектирования и установки всех соответствующих систем. Они используются во время ZSA для SSA для демонстрации того, что установка систем отвечает данным требованиям.

(Примечание редактора: контрольные перечни, представленные в данном примере, являются только краткими версиями. Они должны быть разработаны только один раз для конкретного проекта, и могут содержать дальнейшие инструкции для конкретных зон, таких как зон пожара).

4.1.1 Пример общих инструкций на проектирование и установку.

Следующие инструкции являются примерами, которые поддерживают соответствующую установку систем. Этот перечень следует увеличить, пересмотреть и разработать в соответствии с теми нормативами на проектирование и установку, которые применяются пользователем данного документа.

a. Установка оборудования (включая трубы, короба, шланги, провода, кабели и т.п.).

(1) Установка должна обеспечивать отсутствие приложения недопустимых напряжений.

(2) Крепления к подвижным частям должны быть выполнены таким образом, чтобы минимизировать напряжения.

(3) Крепления к подвижным частям должны быть расположены таким образом, чтобы они не создавали препятствия и чтобы для них не было препятствий от смежных конструкций или оборудования.

(4) Пневматические трубопроводы и шланги должны устанавливаться таким образом, чтобы минимизировать накопление воды.

(5) Разделение первичных и вторичных систем должно быть удовлетворительным с точки зрения отказа одной системы, влияющего на другую, и отказа отдельной системы, влияющего на обе системы.

b. Демонтаж и замена компонентов

(1) Замена аналогичных, но не идентичных компонентов, не должна иметь неприемлемое влияние на характеристики системы.

(2) Любые компоненты, которые могут быть установлены с неправильной ориентацией, не должны вызывать проблем (например, вызывать значительное снижение зазоров, или вызвать неприемлемые натяжения любых соединительных проводов, кабелей, шлангов и т.п.)

(3) Перекрестное соединение разъемов, трубопроводов и т.п. должно быть исключено.

c. Техническое обслуживание и ремонт

(1) Все точки соединений для наземного обслуживания должны быть идентифицированы и/или устроены таким образом, чтобы было очевидно, какие жидкости должны быть использованы, или какое оборудование должно быть подсоединено.

(2) Там, где это возможно, конструкция должна обеспечивать замену изделий без демонтажа другого оборудования, в частности оборудования других систем. Если это невозможно, то при наличии риска должна быть проведена проверка всех затрагиваемых систем.

(3) Должны быть учтены любые возможные опасности, которые могли быть следствием инструментов, болтов и т.п., которые были непреднамеренно оставлены в самолете.

d. Дренаж

(1) Должно быть рассмотрено применение неправильного дренажа установленного компонента/оборудования.

(2) В тех зонах или компонентах, где накопление жидкости будет опасным, должен быть предусмотрен дренаж.

Примечание: *Должны рассматриваться такие жидкости, как вода, хлорированная вода, топливо, гидравлическая жидкость, жидкости для чистки и удаления льда, масло, сточные отходы и т.п.*

4.1.2 Пример инструкций по конкретной конструкции и установке для различных систем

Специальные инструкции по конкретной конструкции и установке для каждой системы или глава ATA должны быть получены из опыта, по эксплуатационным данным, соответствующего PSSA, и требований и целевых функций на уровне самолета. Насколько это возможно, их происхождение должно быть отслеживаемым, и они должны быть согласованы всеми сторонами-партнерами. Следующие инструкции взяты из главы 29 ATA и предназначены в качестве примеров.

a. ATA 29 – Гидравлическая система

(1) Трубы кондиционирования воздуха обычно должны проходить над гидравлическими трубопроводами.

(2) Когда близость гидравлической системы и системы кондиционирования воздуха неизбежна, то необходимо защитное экранирование. Система каналов, используемая для воздуха кабины, должна быть нечувствительной к гидравлическим и другим токсичным или химически активным загрязняющим веществам, которые, вероятно, могут контактировать с ней.

(3) Должно быть возможно вручную управлять клапанами без использования специальных инструментов или разборки.

4.2 Сверка установки с инструкциями по проектированию и установке

Пригодность и долговечность материалов, используемых в компонентах, установке или конструкции, рассматриваются как основные параметры конструкции.

Следующие позиции рассматриваются как основные для конструкции.

a. Влияние тепловых изменений.

b. Конструкционные деформации.

c. Изменение давления.

d. Допуск на сборку.

e. Влияние «g».

f. Вибрация.

g. Электролитическая несовместимость.

h. Материалы и отделочные покрытия.

i. Влияние загрязнения жидкости.

j. Дымовыделение, огнестойкость и распространение пламени.

Если в результате зонного анализа безопасности выявлены очевидные или ожидаемые ошибки, связанные с изделиями, то должен быть выпущен лист запроса. Внешние события, когда они имеют отношение к анализу, должны рассматриваться вместе с другими инструкциями, когда это применимо.

4.2.1 Описание зоны

Отсек основного шасси располагается от шпангоута C42 до шпангоута C46/47 в зоне без давления. Он включает в себя люки основного шасси и вмещает в себя шасси при его уборке.

С левой стороны между шпангоутами C46/47 и C50 в зоне без давления находится часть гидравлической системы и канал стравливаемого воздуха APU. Их необходимо рассматривать как часть отсека основного шасси.

4.2.1.1 Секционирование

Потолок:	Класс I (граница герметичной зоны)
Рама C42:	Граница гидравлического отсека: имеются отверстия в этой перегородке в целях вентиляции; центральная коробка; центральный бак
Нижняя часть:	Поперечина киля, люки основного шасси и фюзеляжная конструкция нижнего обтекателя
Рама C46/47:	Класс I (граница герметичной зоны)
Поперечные перегородки:	Фюзеляжная конструкция нижнего обтекателя
Поперечные перегородки между рамой C47 и C50:	Фюзеляжная конструкция нижнего обтекателя и герметичный фюзеляж

4.2.1.2 Установка системы

В отсеке основного шасси устанавливаются следующие системы/компоненты.

a. Трубопроводы голубой гидравлической системы с левой стороны.

b. Трубопроводы желтой гидравлической системы с правой стороны.

c. Трубопроводы зеленой гидравлической системы в нижней части.

d. Резервуар зеленой системы.

e. Оснащенный коллектор зеленой системы.

f. Блок передачи энергии.

g. Коллектора.

h. Освещение для технического обслуживания.

i. Компоненты тормозной системы.

j. Основное шасси.

k. Система свободного падения основного шасси.

l. Бесконтактные датчики.

m. Силовой блок управления привода предкрылка.

n. Силовой блок управления привода закрылка.

o. Трансмиссионные валы привода закрылка.

p. Редуктор для приводных валов предкрылка и закрылка.

q. Двигатель-генератор постоянной скорости (CSMG), приводимый в действие гидросис-темой.

r. Топливная линия APU.

Между шпангоутами C47 и C50 устанавливаются следующие системы/компоненты.

a. Панель наземного обслуживания зеленой гидравлической системы.

b. Панель наземного обслуживания голубой гидравлической системы.

c. Резервуар голубой системы.

d. Канал стравливаемого воздуха APU.

e. Цокольный воздушный клапан обогрева кормового грузового отсека.

f. Цокольный регулятор давления воздуха обогрева кормового грузового отсека.

g. Электрические кабели.

h. Гидравлические трубопроводы.

4.2.1 2.1 Топливная система

Скрытая линия подачи топлива APU расположена в левом боковом боксе. Когда APU не работает, то топливопровод не находится под давлением и содержит только ограниченное количество топлива. Труба дренажа топлива установлена с правой стороны вторичного лонжерона киля. Другие компоненты, такие как клапан и насос APU, являются герметичными.

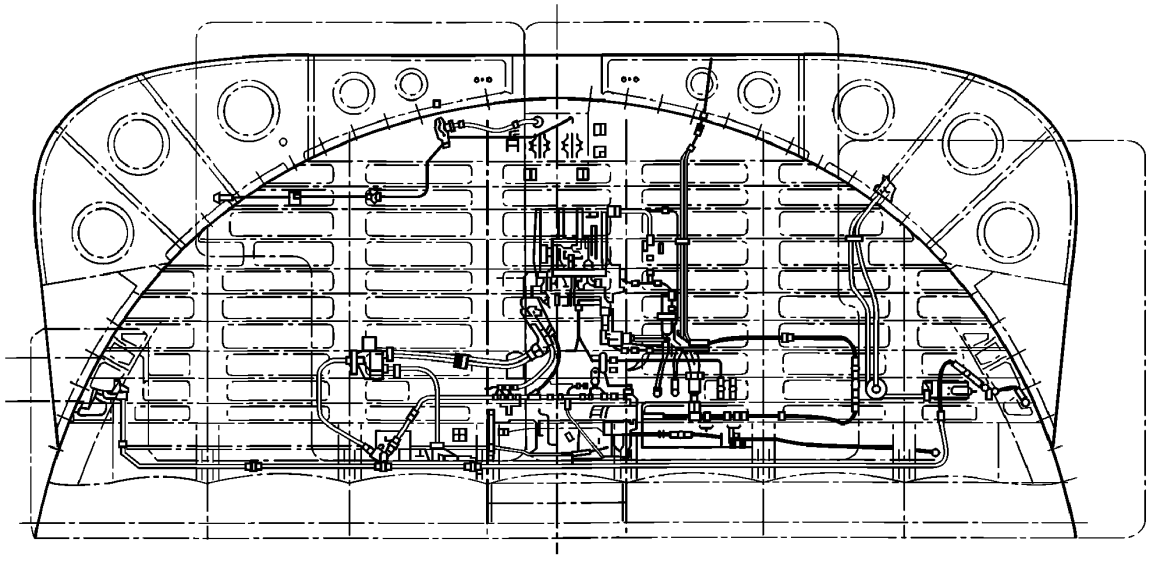
4.2.1 2.2 Гидравлическая система

Трубопроводы гидравлической системы разделены. Голубые трубопроводы расположены с левой стороны на шпангоуте С46/47. Трубопроводы желтой гидравлической системы расположены на шпангоуте С42 на ее обеих сторонах и на шпангоуте С46/47 с правой стороны (см. рис. 4.2.1.2.2-1). Трасса желтых трубопроводов от шпангоута С42 к шпангоуту С45 проходит над герметичным уплотнением.

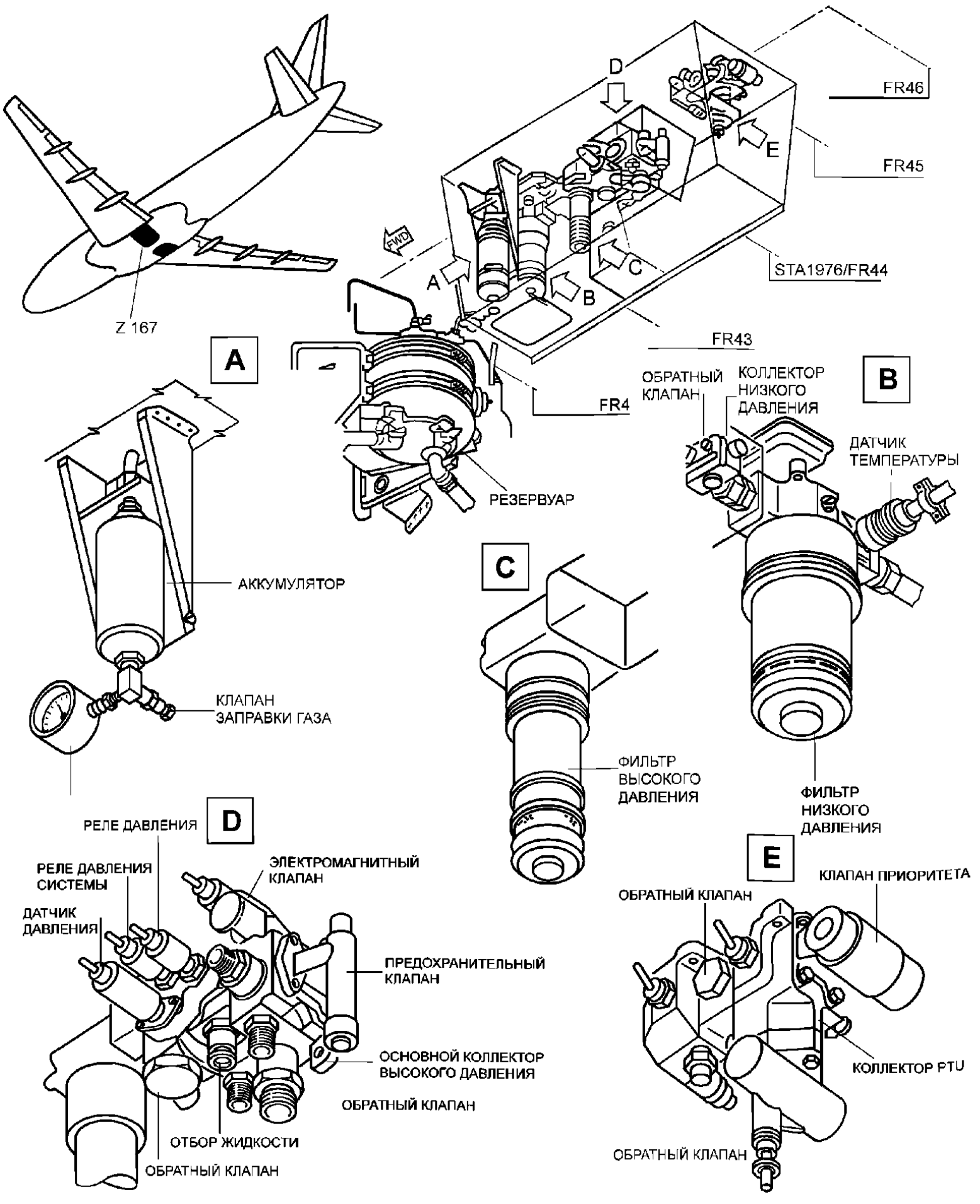
Резервуар зеленой системы установлен на шпангоуте С42, в то время как другие компоненты и трубопроводы зеленой системы расположены посередине под потолком отсека (см. рис. 4.2.1.2.2-2).

Все гидравлические трубопроводы в данной области изготовлены из титанового сплава или нержавеющей стали. Алюминиевый сплав не используется.

В зоне между шпангоутами С46/С47 и С50 гидравлический трубопровод под давлением установлен под каналом выпуска воздуха APU и каналом горячего воздуха дополнительного грузового отсека.



(CCA – ZSA)
Установка гидравлических трубопроводов в шпангоуте С46/47
Рис. 4.2.1.2.2-1



(CCA – ZSA)
Компоненты зеленой гидравлической системы
Рис. 4.2.1.2.2-2

4.2.1.3 Специальные конструктивные соображения для зоны

4.2.1.3.1 Горячие поверхности

Шины рассчитаны на максимальную температуру 120 °C. Запрещается превышать эту температуру на наружных поверхностях тормозов.

Температура стравливаемого воздуха может достигать 260 °C при нормальных условиях эксплуатации системы или при условиях работы с одиночным отказом. Канал стравливания воздуха изготовлен из титана. Он изолирован двумя слоями стекловолокна и уплотнен наружным кевларовым покрытием.

Дополнительный цокольный клапан-регулятор давления воздуха, трубка Вентури и цокольный воздушный клапан не изолированы и могут иметь температуру поверхности до 205 °C.

4.2.1.3.2 Электрические кабели и оборудование

Кабели рассчитаны на непрерывную эксплуатацию с максимальной температурой 200 °C. Кабельные жгуты устанавливаются в кабельных каналах. Кабельные жгуты, ведущие к крыльям, устанавливаются в специальные кабельные каналы для защиты от ударов молнии.

Проходы в перегородках и соединения герметизированы. В электрической проводке, проходящей по потолку, нет разрывов (соединительных шин).

Аварийный генератор расположен на лонжероне руля.

4.2.1.3.3 Конструктивные меры безопасности для предотвращения риска пожара

PCU закрылка и предкрылка, CSMG и PTU имеют герметичный дренаж, а резервуар зеленой системы имеет сливную трубу во избежание утечек гидравлической жидкости.

Трубопровод подачи топлива APU укрыт и имеет дренаж.

Топливные клапаны и насос APU спроектированы таким образом, чтобы не было вероятности попадания утечек топлива в отсек основного шасси.

Любые утечки горючей жидкости сливаются за борт, а любые испарения продуваются воздушным потоком вентиляции.

Перегрев тормоза выявляется через температуру тормоза и систему мониторинга.

Гидравлические трубопроводы из алюминиевых сплавов не используются.

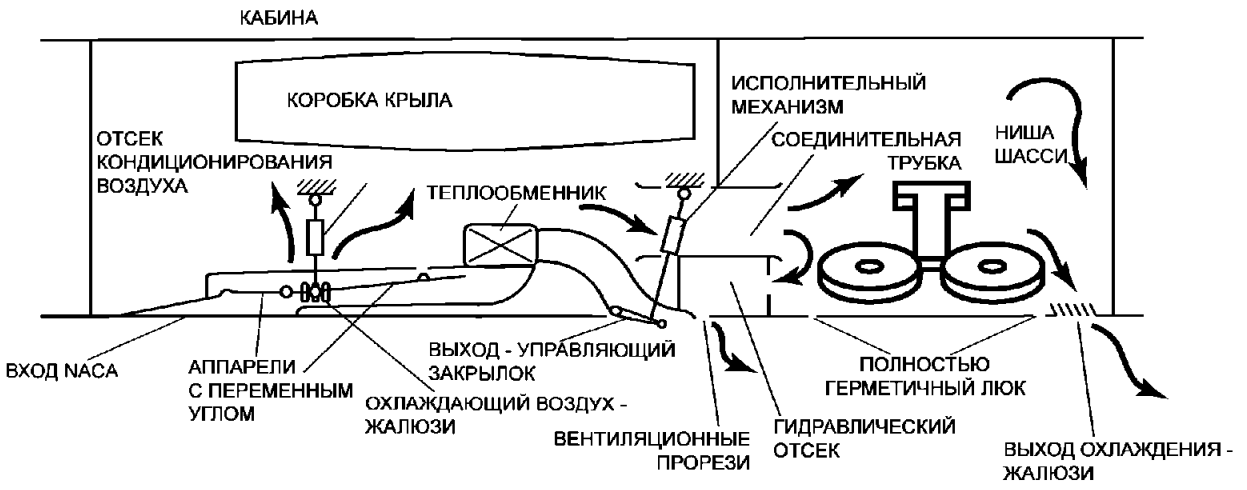
Трансмиссионные валы закрылка спереди шпангоута C46 имеют защиту при помощи фиксаторов на случай разрыва вала.

Установлена двухконтурная система обнаружения утечки воздуха.

В случае разрыва канала сброс давления обеспечивается при помощи жалюзи в отсеке основного шасси и панелей сброса давления в левой части отсека.

4.2.1.3.4 Вентиляция

На рис. 4.2.1.3.4-1 представлена зона вентиляции отсека основного шасси. На земле этот отсек открыт и превалируют наружные условия. В полете наружный воздух втекает в отсек через соединительные трубки из отсека ECS. Часть воздуха вытекает наружу через выходные жалюзи охлаждения, а оставшаяся часть воздуха втекает в гидравлический отсек.



(CCA – ZSA)
Вентиляция отсека основного шасси (MLG)
Рис. 4.2.1.3.4-1

4.2.1.3.5 Дренаж

Кожух трубопровода подачи топлива APU имеет слив через дренажную мачту, расположенную между шпангоутами C46 и C47. Любые жидкости будут сливаться за борт через дренажные отверстия нижнего обтекателя и небольшие зазоры в уплотнениях люков отсека шасси. Так как эта зона не герметична, то дренаж является постоянным в полете и на земле.

4.2.2 Результаты проверки установки по нормативам проектирования и установки

Результаты проверки установки по нормативам проектирования и установки представлены в таблице 4.2.2.-1.

Таблица 4.2.2-1 (CCA – ZSA)
Лист отчета по зонному анализу безопасности

ЛИСТ ОТЧЕТА ПО ЗОННОМУ АНАЛИЗУ БЕЗОПАСНОСТИ			
Тип самолета/стандарт	Зона: Отсек основного шасси	Составил:	Лист: 01 из: 01
		Дата:	Выпуск: 01

№ листа запроса	Причина несоответствия	Предпринятые действия	Примечания
27.01	Болт управления полетом установ-лен головкой вниз		Лист запроса ОТКРЫТ
92.01	Длинные перемычки		Лист запроса ОТКРЫТ
92.02	Трение кабельных каналов	Изменен установочный чертеж	Лист запроса ЗАКРЫТ
92.04	Отсутствие дренажных отверстий в нескольких кабельных каналах		Лист запроса ОТКРЫТ

4.3 Проверка отказных состояний внешних по отношению к компонентам с внешними воздействиями и их влияния на системы, установленные в отсеке основного шасси.

4.3.1 Контрольный лист для взаимодействия систем

Неисправности в системе могут иметь только ограниченное влияние на безопасность самолета с учетом того, каким образом они изменяют работу этой системы. Тем не менее, некоторые неисправности могут иметь значительное влияние на безопасность самолета за счет взаимодействия с другой смежной системой. Влияния таких взаимодействий с использованием анализа типа FMEA на основе перечня установленных компонентов в соответствующей зоне рассматриваются в зонном анализе безопасности и соответствующих PSSA/SSA. Ниже представлены примеры неисправностей, внешних по отношению к компонентам, и их возможных взаимодействий:

a) разрыв трансмиссионных валов, приводящий ко вторичным повреждениям гидравлических линий, кабелей управления, электропроводки, топливных трубопроводов и т.п.;

b) утечки из соединений кислородных трубопроводов в непосредственной близости от электрических компонентов или горючих материалов;

c) отсоединение или отказ оборудования, включая отвинчивание гаек и болтов и т.п., приводящие к возможности последующего заклинивания хода органов управления;

d) осколки от разрушения высокоэнергетического вращающегося оборудования, приводящие ко вторичному повреждению систем(ы) или конструкции самолета;

e) утечки воздуха из линии стравливания двигателя или кондиционирования воздуха могут привести к повышению давления в закрытых зонах и/или к высоким температурам;

f) разрыв аккумулятора может привести ко вторичному повреждению;

g) мусор от протектора шины может повредить конструкцию и системы;

h) дым от неисправного или перегретого электрического оборудования может повлиять на работу экипажа;

i) утечка любой жидкости или газа (горячего воздуха, кислорода, топлива, воды, гидравлической жидкости и т.п.) в непосредственной близости от электрооборудования;

j) утечка горючих жидкостей рядом с источниками тепла;

k) утечка жидкости (топлива, воды, гидравлической жидкости и т.п.), способная загрязнить систему кондиционирования воздуха;

l) система сточных вод, влияющая на другие системы внутренними или внешними утечками.

Некоторые из этих рисков также рассматриваются как специфические риски.

4.3.2 Результаты проверки для режимов отказов, внешних по отношению к компоненту, и их влияния на системы, установленные в отсеке основного шасси.

В таблице 4.3.2-1 перечислены отказные состояния, внешние по отношению к компоненту, и их влияние на системы, установленные в отсеке основного шасси.

Таблица 4.3.2-1 (CCA – ZSA)
Неисправности, внешние по отношению к компоненту, и исполнение

ЗОННЫЙ АНАЛИЗ БЕЗОПАСНОСТИ, НЕИСПРАВНОСТИ, ВНЕШНИЕ ПО ОТНОШЕНИЮ К КОМПОНЕНТУ, И ИСПОЛНЕНИЕ				
Самолет:		**Система: Органы управления полетом** **Зона: Отсек основного шасси**	**Выпуск: 1** **Дата: октябрь 1994 г.**	**Разработал:** **Лист 1 из 4**
№ поз.	**Режим отказа компонента**	**Влияние на самолет**	**Симптомы для:** **1. экипажа самолета** **2. наземной бригады**	**1. совместные действия экипажа** **2. состояние самолета после действия экипажа**
1	Утечка блока управления питанием предкрылка	Гидравлическая утечка сливается за борт. Гидравлические испарения вентилируются за борт. PCU имеет герметичный дренаж. Влияние на ATA 27 (система предкрылков) или ATA 29 (гидравлика) см. в SSA для ATA 27 или ATA 29.	1. Гидравлическое давление (возможно) 2. Повреждение может быть выявлено работами по техническому обслуживанию или зональной инспекцией	См. SSA для ATA 27 (система предкрылков) и ATA 29 (гидравлика).
2	Утечка блока управления питанием закрылка	Гидравлическая утечка сливается за борт. Гидравлические испарения вентилируются за борт. PCU имеет герметичный дренаж. Влияние на ATA 27 (система закрылков) или ATA 29 (гидравлика) см. в SSA для ATA 27 или ATA 29.	1. Гидравлическое давление (возможно) 2. Повреждение может быть выявлено работами по техническому обслуживанию или зональной инспекцией	См. SSA для ATA 27 (система предкрылков) и ATA 29 (гидравлика).
3	Сломан вал закрылка (левый)	Сломанный вал может повредить трубопроводы зеленой гидравлической системы на задней стенке. Потеря зеленой гидравлической системы.	1. Закрылки не работают (потеря давления зеленой гидравлической системы)	См. SSA для ATA 27 (система закрылков) и ATA 29 (гидравлика).
4	Сломан вал закрылка (правый)	Сломанный вал может повредить трубопроводы желтой гидравлической системы на задней стенке. Потеря желтой гидравлической системы.	1. Закрылки не работают (потеря давления желтой гидравлической системы)	См. SSA для ATA 27 (система закрылков) и ATA 29 (гидравлика).

Таблица 4.3.2-1 – (CCA – ZSA)
Неисправности, внешние по отношению к компоненту, и исполнение (продолжение)

ЗОННЫЙ АНАЛИЗ БЕЗОПАСНОСТИ, НЕИСПРАВНОСТИ, ВНЕШНИЕ ПО ОТНОШЕНИЮ К КОМПОНЕНТУ, И ИСПОЛНЕНИЕ				
Самолет:		**Система: Органы управления полетом** **Зона: Отсек основного шасси**	**Выпуск: 1** **Дата: октябрь 1994 г.**	**Разработал:** **Лист 2 из 4**
№ поз.	**Режим отказа компонента**	**Влияние на самолет**	**Симптомы для:** **1. экипажа самолета** **2. наземной бригады**	**1. совместные действия экипажа** **2. состояние самолета после действия экипажа**
1	Утечка задней стенки центрального бака	Утечка топлива будет сливаться за борт. Испарения удаляются вентиляцией.	2. Повреждение может быть выявлено работами по техническому обслуживанию или зональной инспекцией	1. Нет
2	Утечка или разрыв дренажного трубопровода	Данный трубопровод будет содержать топливо только в случае утечки центрального бака или утечки баков в крыльях на входе в центральный бокс крыла. Утечка будет сливаться за борт.	2. Повреждение может быть выявлено работами по техническому обслуживанию или зональной инспекцией	1. Нет
3	Утечка сборного трубопровода APU	Трубопровод находится под давлением только в том случае, если APU работает. Трубопровод в кожухе, утечка топлива будет сливаться за борт.	2. Повреждение может быть выявлено работами по техническому обслуживанию или зональной инспекцией	1. Нет

Таблица 4.3.2-1 – (CCA – ZSA) Неисправности, внешние по отношению к компоненту, и исполнение (продолжение)

ЗОННЫЙ АНАЛИЗ БЕЗОПАСНОСТИ, НЕИСПРАВНОСТИ, ВНЕШНИЕ ПО ОТНОШЕНИЮ К КОМПОНЕНТУ, И ИСПОЛНЕНИЕ				
Самолет:		**Система: Органы управления полетом** **Зона: Отсек основного шасси**	**Выпуск: 1** **Дата: октябрь 1994 г.**	**Разработал:** **Лист 3 из 4**
№ поз.	**Режим отказа компонента**	**Влияние на самолет**	**Симптомы для:** **1. экипажа самолета** **2. наземной бригады**	**1. совместные действия экипажа** **2. состояние самолета после действия экипажа**
1	Утечка или разрыв гидравлического трубопровода	Утечка топлива будет сливаться за борт. Испарения удаляются вентиляцией.	1. Потеря гидравлического давления индикация уровня в резервуаре	См. SSA для ATA 29 (гидравлическая система).
2	Утечка или разрыв дренажного трубопровода	Данный трубопровод будет содержать топливо только в случае утечки центрального бака или утечки баков в крыльях на входе в центральный бокс крыла. Утечка будет сливаться за борт.	1. Пониженное гидравлическое давление	См. SSA для ATA 29 (гидравлическая система).
3	Разрыв гидравлического аккумулятора (зеленая система)	Зеленая гидравлическая система неработоспособна. Гидравлическая утечка сливается за борт. Гидравлические испарения вентилируются за борт. Мусор, содержащий кевларовую обмотку.	1. Потеря гидравлического давления	См. SSA для ATA 29 (гидравлическая система).
4	Разрыв гидравлического аккумулятора (тормозная система)	Влияние на тормозную систему см. в SSA. Гидравлическая утечка сливается за борт. Гидравлические испарения вентилируются за борт. Мусор, содержащий кевларовую обмотку.	1. Гидравлическое давление тормоза	См. SSA для тормозной системы

Таблица 4.3.2-1 – (CCA – ZSA) Неисправности, внешние по отношению к компоненту, и исполнение (продолжение)

ЗОННЫЙ АНАЛИЗ БЕЗОПАСНОСТИ, НЕИСПРАВНОСТИ, ВНЕШНИЕ ПО ОТНОШЕНИЮ К КОМПОНЕНТУ, И ИСПОЛНЕНИЕ				
Самолет:		**Система: Органы управления полетом** **Зона: Отсек основного шасси**	**Выпуск: 1** **Дата: октябрь 1994 г.**	**Разработал:** **Лист 4 из 4**
№ поз.	**Режим отказа компонента**	**Влияние на самолет**	**Симптомы для:** **1. экипажа самолета** **2. наземной бригады**	**1. совместные действия экипажа** **2. состояние самолета после действия экипажа**
1	Утечка канала стравливания воздуха APU		1. Извещение о выявлении перегрева	1. Отключить комплект низкого давления 2. Работоспособна только одна система стравливания воздуха. Система против обледенения крыла не работает.
2	Разрыв канала стравливания воздуха APU (в лонжероне киля)	Горячий стравливаемый воздух будет протекать через вентиляционные отверстия лонжерона киля. Система обнаружения перегрева отключит систему стравливания воздуха низкого давления Давление ограничивается жалюзи	1. Извещение о выявлении перегрева	1. Отключить комплект низкого давления 2. Работоспособна только одна система стравливания воздуха. Система против обледенения крыла не работает.

5.0 ЗАКЛЮЧЕНИЕ

В данном отчете описана установка системы в обследованной зоне. В нем выделены потенциальные проблемы и их влияние на самолет. Если влияние на самолет рассматривалось как неприемлемое в соответствии с нормативами и контрольными перечнями ZSA, то данная проблема была обсуждена с соответствующим лицом, ответственным за проектирование, и, при необходимости, были инициированы модификации. Это гарантирует то, что установка систем обеспечивает требуемый уровень безопасности.

Анализ специфического риска для самолета S18

Оценка отказа, связанного с разрывом шины

(Примечание редактора: Подробную информацию по процессу PRA см. в Приложении J).

1.0 ВВЕДЕНИЕ

Данный анализ проведен для специфического риска разрыва шины.

(Примечание редактора: Для краткости данный пример охватывает только разрыв шин основного шасси при выпущенных шасси. Полный анализ должен также учитывать шины носового колеса, убранное шасси и т.п.).

Данный анализ должен продемонстрировать, что никакой разрыв шины не должен привести к катастрофическому отказному состоянию *(Примечание редактора: В данном примере «потеря способности замедления скорости»)* и что вероятность аварийных отказных состояний является допустимой *(Примечание редактора: В данном примере «потеря торможения всех колес»).*

2.0 ССЫЛКИ

1) FHA самолета S18

2) FHA/PSSA системы торможения колес S18.

3) FHA/PSSA системы управления полета S18.

4) FHA/PSSA системы реверсора тяги S18.

Кроме того, требованиями к годности к летной эксплуатации, применимыми к отказам шин, являются следующие:

5) 25.729(f), который охватывает защиту оборудования на шасси и в нише шасси от влияний одиночного отказа шины.

6) 25.1 309, который охватывает оборудование, системы и установки в общих чертах.

7) 25.963 (e), который охватывает предотвращение проникновения мусора в технологические лючки топливного бака или смотровых окон.

3.0 ОПИСАНИЕ

Данный отчет предназначен для описания последствий отказа шины на выпущенных основных шасси самолета S18 для того, чтобы продемонстрировать соответствие используемым требованиям летной эксплуатации. Самолет S18 оснащен сдвоенным носовым колесным шасси и четырехколесным основным ходовым шасси (см. рис. 3.0-1).

В данном анализе используется стандартизованная модель отказов шины, согласованная с авиационными властями, для оценки адекватности проекта и конструкции самолета по защите от таких неисправностей. В соответствующих местах делаются ссылки на данные испытаний или опыт эксплуатации аналогичных типов самолетов.

Все вероятности событий, установленные в данном анализе, приведены для одного полета.

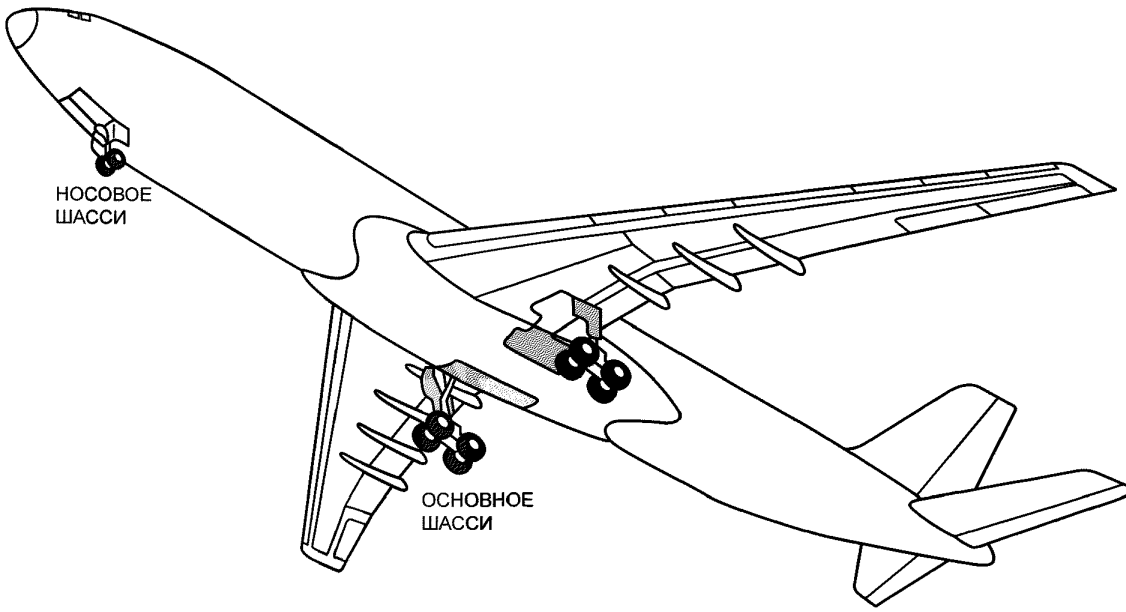
3.1 Описание шасси

Самолет S18 оснащен трехэлементной системой шасси, которая убирается во время полета при помощи гидравлических средств.

Носовое шасси сдвоенного колесного типа убирается в отсек в переднем фюзеляже. После втягивания шасси профиль фюзеляжа восстанавливается при помощи трех механически управляемых люков, связанных с конструкцией шасси, и двух люков, прикрепленных к фюзеляжу и управляемых двумя гидравлическими исполнительными механизмами.

Основное шасси имеет четырехколесную конструкцию и убирается на борт при помощи вертикальных осей, расположенных в крыльях. После втягивания шасси четыре люка (по два на каждое), механически связанных с конструкцией шасси, восстанавливают нижний профиль крыла. Нижний профиль фюзеляжа восстанавливается при помощи двух гидравлически управляемых люков, по одному на каждое шасси.

Все стойки шасси обычно убираются и выдвигаются при помощи зеленой гидравлической системы. Если гидравлическая энергия отсутствует, то шасси не могут быть убраны, а если они уже убраны, то они могут быть только впущены при помощи системы впуска под действием собственного веса с использованием электропитания от аккумулятора. Данная электромеханическая система разблокирует люки носового и основного шасси, открывает замок убранного положения шасси и оно опускается и фиксируется в нижнем положении.



(CCA – PRA)
Носовое и основное шасси самолета S18
Рис. 3.0-1

4.0 АНАЛИЗ

4.1 Модель отказа шасси

4.1.1 Общие положения

Для того чтобы иметь стандартизованный комплект условий для оценки последствий отказа шины, была разработана модель отказа на основе исследований отчетов по возникновению неисправностей и предыдущей практики, принятой для сертификации предыдущего самолета.

В данной модели все вероятности отказов назначены на одно колесо и один полет.

Условия, определенные по данной модели, были использованы в качестве основы для всех оценок специфического риска для колес. Были рассмотрены шесть видов отказов, которые применимы к шасси самолета S18.

(Примечание редактора: В данном примере используется только пример, относящийся к отказам шины на выдвинутом шасси).

4.1.2 Разрыв шины на выпущенном шасси

Разрыв, возникающий в том случае, когда колесо контактирует с землей, приводит к образованию остатков протектора шины. Они могут разлетаться в плоскости колеса под углом от 45° до 180°, измеренного от горизонтальной плоскости земли в обратном направлении. Предполагается, что существует равномерный риск разлета остатков по этой дуге 135°.

Кроме того, куски шины могут разлетаться под углом до 15° к каждой боковой плоскости шины с Гауссовым распределением. Таким образом, вероятность того, что по изделию будут удары остатков, зависит от площади изделия, обращенной к разлетающимся остаткам, и его положения по отношению к шине. По чертежам каждого колеса может быть построена диаграмма или «схема окна», которая определяет площадь, на которой может произойти повреждение. По этим схемам можно рассчитать вероятность для изделия, с которым происходит соударение остатков.

Рассматриваются два следующих размера остатков протектора.

a) Большой кусок с размерами WxW и небольшой кусок 0,5Wx0,5W, где W – ширина протектора шины.

b) В 10% случаев отказ первой шины рассматривается как провоцирующий разрыв и отслоение протектора второй шины вследствие перегрузки.

4.2 Метод оценки соответствия

Проведена оценка влияния удара одиночного большого или небольшого куска шины на оборудование в отсеке шасси и на стойки шасси для демонстрации соответствия 25.729(f).

Выполнена оценка последствий удара одиночным куском шины для конструкции или систем снаружи отсека шасси; или двойных ударов в любом месте для демонстрации соответствия 25.1309.

Проведена оценка воздействия одиночного удара любым куском шины по эксплуатационным панелям топливного бака для демонстрации соответствия 25.963(e).

Средствами оценки является анализ вместе с данными испытаний.

4.3 Определение зон/площадей воздействия

Проведен анализ влияний отслоения протектора в местах, указанных ниже. Для иллюстрации см. рис. 4.3-1 - 4. Повреждение от любого индивидуального куска шины в большинстве случаев является одиночным вследствие геометрии зон, подверженных риску удара, следовательно, для данного анализа рассматривается повреждение только одного места.

a. Обтекатель носовой стойки шасси и навесной люк.

b. Стойка и заделки носовой стойки шасси.

c. Нижняя обшивка крыла.

d. Эксплуатационные панели 541ab, bb, cb, db/641ab, bb, cb, db.

e. Эксплуатационные панели 573db/673db.

f. Фиксированная панель задней части крыла.

g. Коробка бандажа.

h. Панель на крыле.

i. Внутренний задний лонжерон.

j. Бортовой закрылок.

k. Направляющее устройство и обтекатель закрылка № 2.

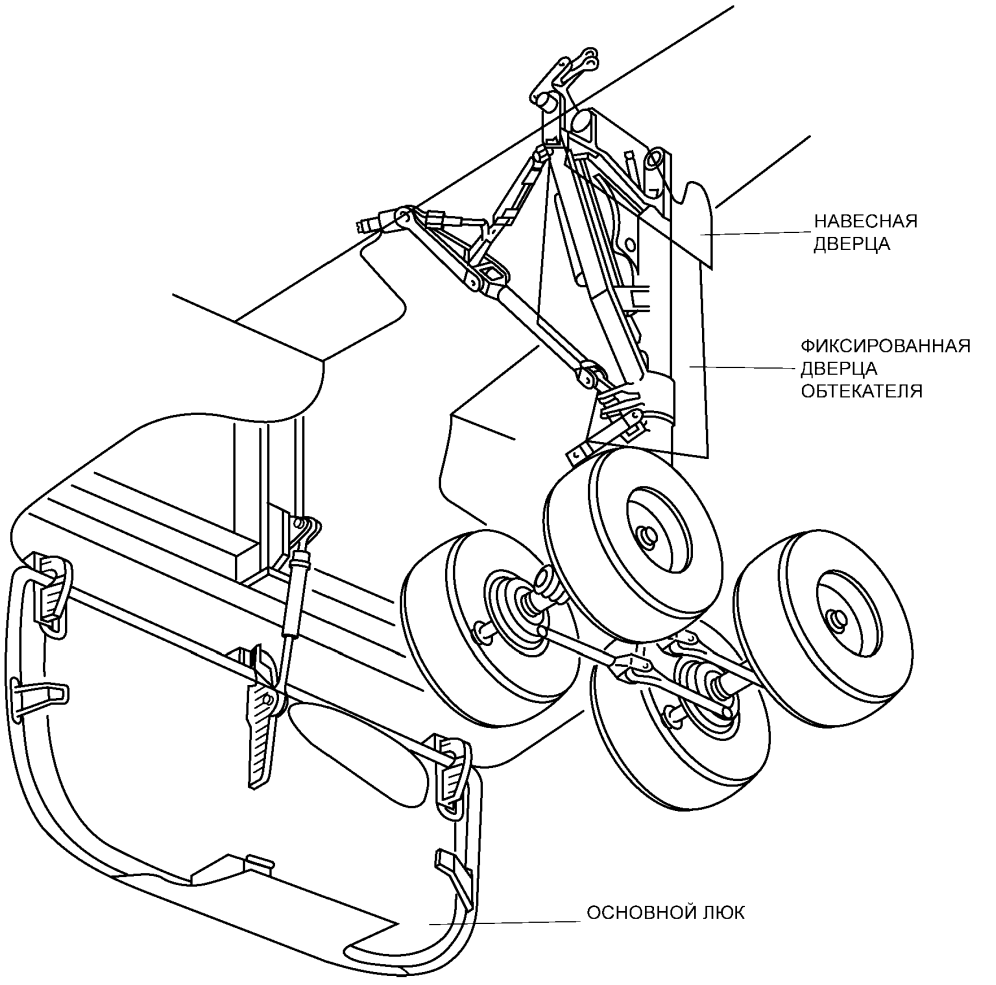
l. Предкрылок № 1.

m. Интерцептор № 1.

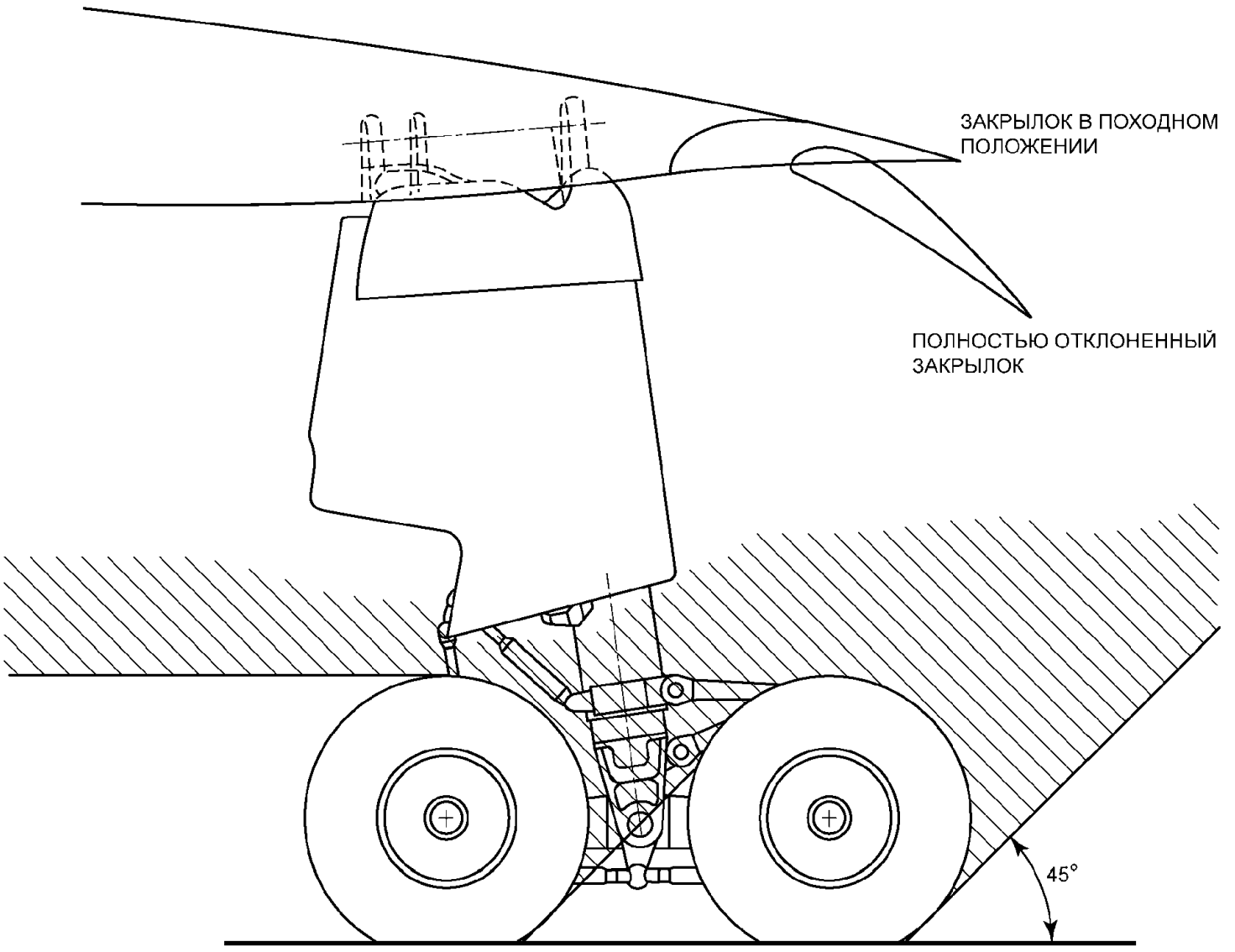
n. Нижняя передняя часть фюзеляжа.

o. Обтекатель фюзеляжа.

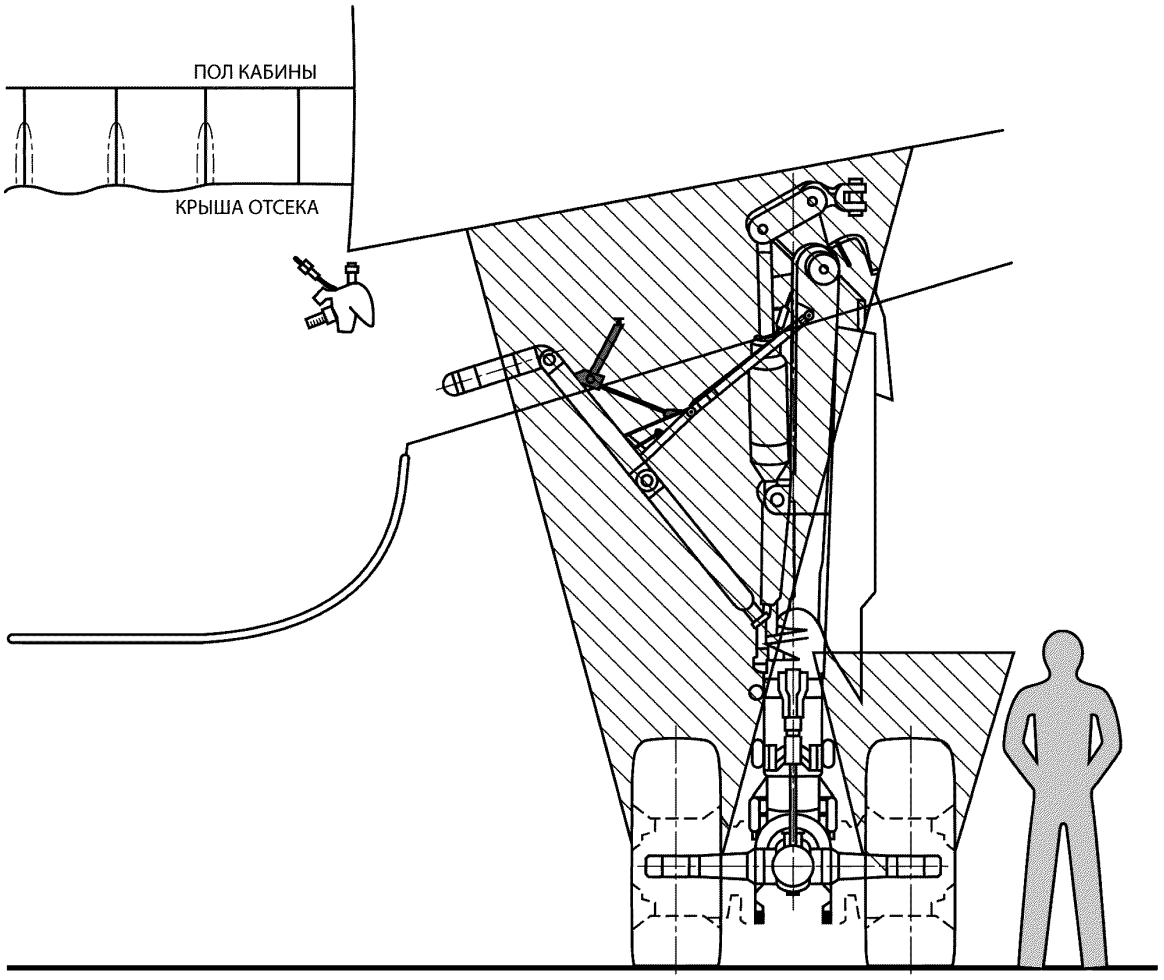
p. Задняя часть фюзеляжа.



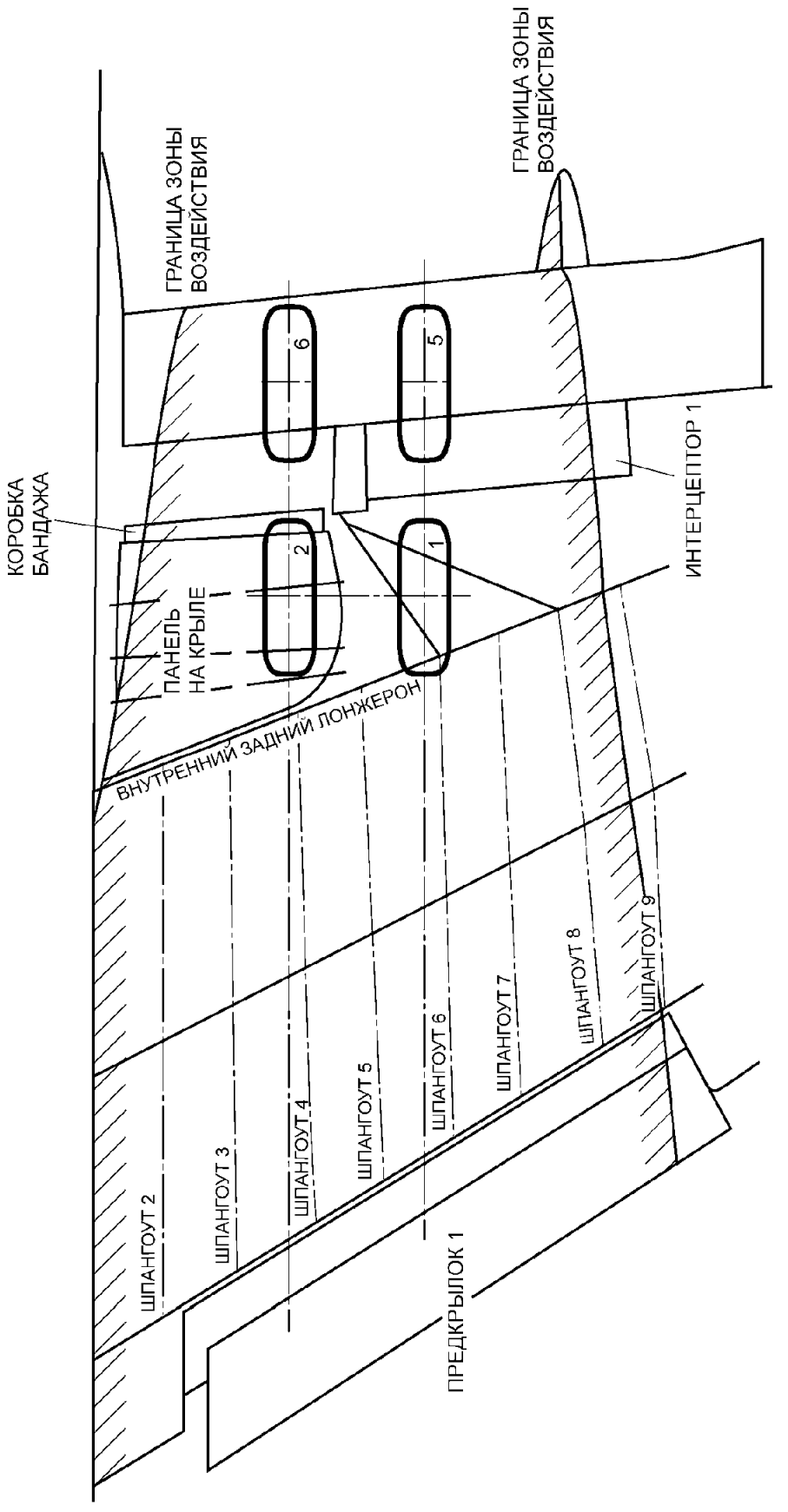
(CCA – PRA)
Отсек основного шасси
Рис. 4.3-1



(CCA – PRA)
Вид сбоку зоны разрыва шины
Рис. 4.3-2



(CCA – PRA)
Зона разрыва шины – вид спереди
Рис. 4.3-3



(CCA – PRA)
Зона разрыва шины – вид сверху
Рис. 4.3-4

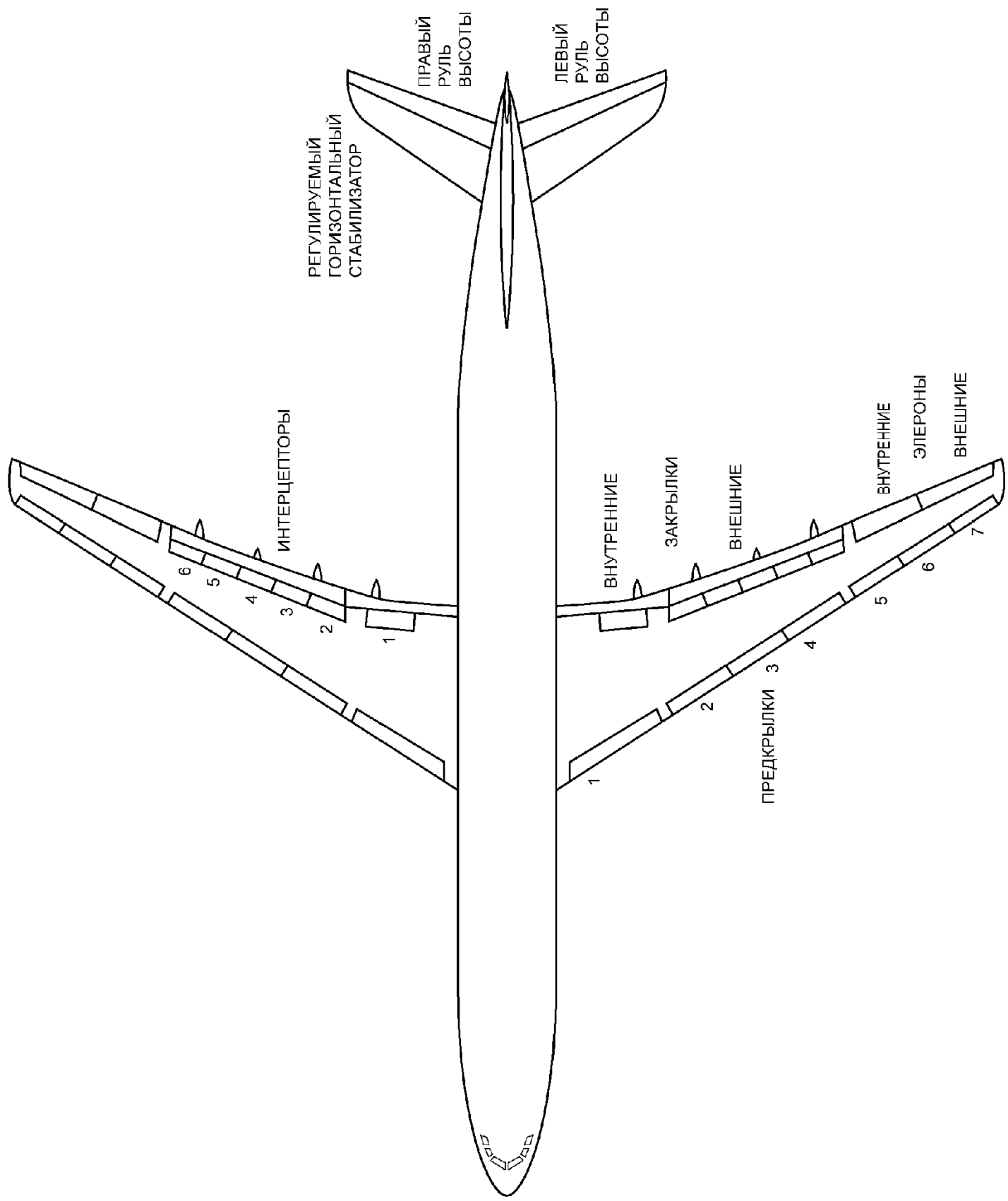
4.4 Определение затронутых систем

Разрыв шины влияет только на гидравлические и электрические системы.

(Примечание редактора: Обычно подробную информацию по вопросам, представленным в следующих главах, можно найти в других PSSA/SSA, и здесь потребуется только классификация отказного состояния и ссылки на эти PSSA/SSA. Представленная здесь информация позволяет укомплектовать пример при отсутствии данных других анализов).

4.4.1 Общие положения

В данном анализе рассматривается, что жесткие и гибкие гидравлические трубопроводы подвергаются тяжелому воздействию при ударе остатками колеса или шины. Вероятным результатом такого события является потеря связанной гидравлической системы. Для ссылки ниже приведены последствия такой потери гидравлической системы для основных систем самолета вместе с классификацией отказного состояния. Идентификацию поверхностей управления см. на рис. 4.4.1-1.



(CCA – PRA)
Поверхности управления полетом самолета S18
Рис. 4.4.1-1

4.4.2 Потери гидравлических систем

a. Потеря зеленой гидравлической системы

(1) ATA27

(a) Работа закрылков на средней скорости.

(b) Работа предкрылков на средней скорости.

(c) Потеря работы интерцептора 1 и 5 (оба крыла).

(2) ATA32

(a) Потеря нормальной тормозной системы, автоматическое переключение на альтернативную (голубую) тормозную систему.

(b) Потеря управления носовым колесом.

(c) Потеря уборки шасси (если шасси выпущены).

(d) Выпуск шасси под действием силы тяжести (если шасси убраны).

(3) ATA78

(a) Потеря реверсора тяги № 2

Классификация отказного состояния – УУП

a. Потеря голубой гидравлической системы

(1) ATA27

(a) Работа предкрылков на средней скорости.

(c) Потеря работы интерцептора 2 и 3 (оба крыла).

(2) ATA32

(a) Потеря альтернативных тормозов. Остается аварийное торможение от аккумулятора (голубого) без противоскольжения, если голубые трубопроводы тормоза не повреждены.

(3) ATA 78

(a) Потеря реверсора тяги № 3.

Классификация отказного состояния – УУП

a. Потеря желтой гидравлической системы.

(1) ATA27

(a) Работа закрылков на средней скорости.

(b) Потеря работы интерцепторов 4 и 6 (оба крыла).

(2) ATA78

(a) Потеря реверсоров тяги № 1 и 4.

Классификация отказного состояния – УУП

a. Потеря зеленой и голубой гидравлической систем

(1) ATA27

(a) Потеря работы предкрылка.

(b) Работа закрылков на средней скорости.

(c) Потеря работы интерцепторов 1, 2, 3 и 5 (оба крыла).

(d) Потеря работы внутреннего элерона.

(2) ATA32

(a) Потеря нормальных и альтернативных тормозов. Остается аварийное торможение при помощи аккумулятора (голубого) без противоскольжения, если голубые трубопроводы тормоза не повреждены вниз по потоку от аккумулятора.

(b) Потеря управления носовым колесом.

(c) Выпуск шасси под действием силы тяжести (если шасси втянуты).

(3) ATA78

(a) Потеря реверсоров тяги 2 и 3.

Классификация отказного состояния – Сложное, (если потеряны все тормоза – Аварийное)

a. Потеря зеленой и желтой гидравлических систем

(1) ATA27

(a) Потеря работы закрылков.

(b) Работа предкрылков на средней скорости.

(c) Потеря работы интерцепторов 1, 4, 5 и 6 (оба крыла).

(d) Потеря работы правого руля высоты.

(e) Потеря работы наружного элерона.

(f) Потеря работы демпфера рыскания.

(2) ATA32

(a) Потеря нормальной тормозной системы, автоматическое переключение на альтернативную (голубую) тормозную систему.

(b) Потеря управления носовым колесом.

(c) Потеря уборки шасси (если шасси выпущены).

(d) Выпуск шасси под действием силы тяжести (если шасси убраны).

(3) ATA78

(a) Потеря реверсоров тяги 1, 2 и 4.

Классификация отказного состояния – Сложное

a. Потеря голубой и желтой гидравлических систем

(1) ATA27

(a) Работа закрылков на средней скорости.

(b) Работа предкрылков на средней скорости.

(c) Потеря работы интерцепторов 2, 3, 4 и 6 (оба крыла).

(d) Потеря управляемого горизонтального стабилизатора.

(2) ATA32

(a) Потеря альтернативных тормозов. Остается аварийное торможение при помощи аккумулятора (голубого) без противоскольжения, если голубые трубопроводы тормоза не повреждены.

(3) ATA78

(a) Потеря реверсоров тяги № 1, 3 и 4.

Классификация отказного состояния – Сложное

a. Потеря зеленой, желтой и голубой гидравлических систем.

(1) ATA27

(a) Полная потеря работы управления полетом.

Классификация отказного состояния – Катастрофическое

4.4.3 Последовательность потери электрической системы

4.4.3.1 Общие положения

В данном анализе рассматривается событие, когда жесткие и гибкие электрические кабельные каналы повреждены при ударе остатками колеса или шины. Вероятным результатом такого события является потеря соответствующего электрического управления или сигналов мониторинга.

Для защиты работы всех основных систем самолета используются не менее двух независимых и разделенных электрических систем и управляющих компьютеров. Все датчики мониторинга задублированы, хотя вследствие необходимости они могут быть установлены рядом друг с другом в месте, которое должно контролироваться.

4.4.3.2 Потери одной электрической системы

Цепи управления и мониторинга сами являются объектами контроля неразрывности при помощи соответствующего управляющего компьютера.

В случае отказа колеса или шины, вызывающего потерю нескольких электрических систем, работа жизненно важных систем самолета будет выполняться альтернативной аварийной системой в большинстве случаев, таких как:

a. Гидромеханическое управление альтернативного торможения (без противоскольжения).

b. Выпуск носового и основного шасси под действием силы тяжести.

В некоторых случаях электрические системы управления могут иметь ограниченную функцию управления со стойкостью к потере всех каналов данных мониторинга для определенных параметров. К таким случаям относится:

a. Гидравлический выпуск шасси после потери обоих каналов данных по событию «люки шасси закрыты».

4.5 Предпринятые конструктивные меры предосторожности

Гидравлическая система, обеспечивающая тормоза, необходимый датчик и провода управления установлены в одной цепи спереди, а другая цепь – сзади стойки основного шасси.

(Примечание редактора: В соответствии с нормативами проектирования и установки могут использоваться другие конструктивные меры предосторожности, однако для краткости они здесь не показаны).

4.6 Обзор последствий

Зоны комбинированного удара осколков от всех восьми шин основного шасси представляют собой обширную область нижней обшивки крыла в области ее корневой части. Включенным в эту область является отсек крыла для основного шасси, который не подвергается воздействию. Следовательно, может возникнуть значительное число событий с классификацией условия отказа как незначительного. Обычно это потеря одного гидравлического контура, электрического канала или небольшие повреждения конструкции. Наиболее представительные примеры таких событий даны в таблице 4.6-1.

Определенное количество событий в комбинации приводят к потере двух контуров, что в результате вызывает потерю работы внутреннего элерона и интерцепторов 1, 2, 3 и 5; или потерю тормозов на 3 колесах затронутой тележки; или альтернативного торможения, имеющего классификацию условия отказа как «основного».

Не было выявлено ни одного события, вызванного одиночным осколком, которое бы имело классификацию условия отказа хуже, чем «основной». Следовательно, требования 25.729(f) выполняются, а классификация условия отказа для одиночного осколка является «основной».

В 10% случаев моделью колеса и шины задается второй осколок. При событии независимого удара двух осколков по голубому и зеленому тормозному контуру произойдет потеря всего торможения, что классифицируется по условию отказа как «опасный отказ». Следовательно, классификация условия отказа для двух осколков является «опасной», а соответствующая вероятность равна 2,2E-9 на полет.

Таблица 4.6-1 – Сводка результатов анализа частного риска отказа шины

АНАЛИЗ ОТКАЗА ШИНЫ СРЫВ ПРОТЕКТОРА, РАЗРЫВ ШИНЫ		**ОСНОВНОЕ ШАССИ - ВЫПУЩЕНО**			
FAR/JAR 25 №	**ЗАТРОНУТЫЕ ИЗДЕЛИЯ**	**ПОСЛЕДСТВИЯ**	**КЛАССИФИКАЦИЯ ОТКАЗНОГО СОСТОЯНИЯ**	**РИСК**	**ПАРАГРАФ ОТЧЕТА**
729(f)	ЛЮК ОБТЕКАТЕЛЯ СТОЙКИ MLG ПАНЕЛЬ ЛЮКА ОБТЕКАТЕЛЯ СТОЙКИ	Крепления сломаны, люк обтекателя (36 кг) отрывается от конструкции самолета и ударяет по бортовому закрылку и движется вниз к горизонтальному стабилизатору (энергия удара закрылка меньше, чем удар птицы)	УУП		
729(f)	НАВЕСНОЙ ЛЮК MLG НАВЕСНАЯ ПАНЕЛЬ ЛЮКА	Крепления сломаны, навесной люк (15 кг) отрывается от конструкции самолета	УУП		
729(f)	СТОЙКА И ОТДЕЛКА MLG ЭЛЕКТР. СИСТ.: Данные тахометра 2M ГИДРАВЛ. СИСТ.: Голубая (или зеленая) к 2 тормозам	Потеря тормозов на 3 колесах на затронутой тележке	Сложное		
1309	НИЖНЯЯ ОБШИВКА КРЫЛА ЭЛЕКТР. СИСТ.: Топливный насос 1M Электропитание 2M	Потеря перекачки к одному двигателю. Двигатель останавливается, если только вручную не выбрана поперечная подача	УУП	1,8E-6	
963(e) (только FAR)	ЭКСПЛУАТАЦИОННЫЕ ПАНЕЛИ 541/641 AB, BB, CB, DB ЭКСПЛУАТАЦИОННЫЕ ПАНЕЛИ ТОПЛИВНОГО БАКА	Дентинг	НЕТ		
1309	ЭКСПЛУАТАЦИОННЫЕ ПАНЕЛИ 573/673 DB ЭЛЕКТРИЧ. СИСТЕМА: 1M к крылу 2M и MLG 1S НОРМАЛЬНЫЙ 2S ТОРМОЖЕНИЕ ГИДРАВЛИЧ. СИСТЕМА: Голубая к управлению полетом КОНСТРУКЦИЯ: эксплуатационная панель, узел	Альтернативное торможение без противоскольжения Потеря голубой гидросистемы Освобождение панели (1,7 кг)	Сложное УУП УУП		
1309	НЕПОДВИЖНАЯ ПАНЕЛЬ НИЖНЕЙ ПОВЕРХНОСТИ КРЫЛА Панель нижней поверхности крыла, узел	Освобождение панели (5,1 кг)	УУП	8,0E-8	

АНАЛИЗ ОТКАЗА ШИНЫ СРЫВ ПРОТЕКТОРА, РАЗРЫВ ШИНЫ		ОСНОВНОЕ ШАССИ - ВЫПУЩЕНО			
FAR/JAR 25 №	**ЗАТРОНУТЫЕ ИЗДЕЛИЯ**	**ПОСЛЕДСТВИЯ**	**КЛАССИФИКАЦИЯ ОТКАЗНОГО СОСТОЯНИЯ**	**РИСК**	**ПАРАГРАФ ОТЧЕТА**
729(f) 1309	КОРОБКА КОЖУХА ГИДРАВЛ. СИСТЕМА: Зеленая к крылу МЕХАНИЧ. СИСТЕМА Трансмиссия закрылка КОНСТРУКЦИЯ: Узел коробки кожуха	 Потеря гидравлической системы Потеря работы закрылка Выброс небольших обломков	 УУП УУП УУП		
729(f) 1309	ПАНЕЛЬ НА КРЫЛЕ ЭЛЕКТРИЧ. СИСТЕМА: 1М к MLG ГИДРАВЛИЧ. СИСТЕМА: Зеленая к MLG КОНСТРУКЦИЯ: Узел панели на крыле	 Альтернативное торможение без противоскольжения Потеря зеленой гидравлической системы Выброс небольших обломков	 УУП УУП УУП		
729(f)	ВНУТРЕННИЙ ЗАДНИЙ ЛОНЖЕРОН ЭЛЕКТРИЧ. СИСТЕМА: 1М к КРЫЛУ 2М и КРЫЛО 1S АЛЬТЕРНАТИВНЫЙ 2S ТОРМОЖЕНИЕ ГИДРАВЛ. СИСТЕМА: Голубая к крылу ИЛИ зеленая к защелке MLG	 Потеря работы внутреннего элерона Потеря работы интерцепторов 1, 2, 3, 5 Потеря навигационных огней Работа закрылков на средней скорости Потеря зеленой гидравлической системы после выбора подъема шасси	 Сложное Сложное УУП УУП УУП УУП		2.1
1309	БОРТОВОЙ ЗАКРЫЛОК Панель бортового закрылка	Локальное повреждение нижней обшивки. Выброс небольших осколков	УУП	1,2E-5	
1309	ОБТЕКАТЕЛЬ ТРАКТА ЗАКРЫЛКА №2 Обтекатель тракта закрылка	Локальное повреждение и выброс осколков	УУП	5,0E-8	
1309	ПРЕДКРЫЛОК № 1 Панель бортового закрылка	Локальное повреждение и выброс небольших осколков	УУП		
1309	ИНТЕРЦЕПТОР № 1 Панель интерцептора № 1 Исполнительный механизм №1	Выброс осколков Потеря зеленой гидравлической системы	УУП УУП	2,96E-6 1,20E-7	

АНАЛИЗ ОТКАЗА ШИНЫ СРЫВ ПРОТЕКТОРА, РАЗРЫВ ШИНЫ		ОСНОВНОЕ ШАССИ - ВЫПУЩЕНО			
FAR/JAR 25 №	**ЗАТРОНУТЫЕ ИЗДЕЛИЯ**	**ПОСЛЕДСТВИЯ**	**КЛАССИФИКАЦИЯ ОТКАЗНОГО СОСТОЯНИЯ**	**РИСК**	**ПАРАГРАФ ОТЧЕТА**
1309	ФЮЗЕЛЯЖ СЕКЦИЯ 13 И 14 Верхняя поперечная обечайка ниже линии окон	Вмятины на обшивке и царапины на краске	УУП	3,4E-8	2.1
	СЕКЦИЯ 15/21 Обтекатель нижнего фюзеляжа	Пробоины, выброс небольших осколков	УУП	7,0E-8	
	СЕКЦИЯ 16 Верхняя поперечная обечайка ниже линии окон	Вмятины на обшивке и царапины на краске	УУП	1,4E-8	

5.0 ЗАКЛЮЧЕНИЕ

Основным допущением, принятым для данного анализа, было то, что электрические и гидравлические системы разрываются при ударе осколка. Следовательно, описанные влияния представляют собой наихудший случай.

a. Ни одно событие в результате отказа шины не было классифицировано как Катастрофическое состояние отказа.

b. Одно событие в результате отказа шины было идентифицировано как Сложное отказное состояние. Данное событие представляет собой потерю торможения, вызванную осколками шины от двух колес основного шасси, ударяющих по голубым и зеленым трубопроводам гидравлической подачи тормоза в области отсека шасси в крыле. Вероятность возникновения этого события была оценена как крайне маловероятное (2,2E-9 на полет).

c. Ни одно событие не было идентифицировано анализом, которое имеет отказное состояние хуже, чем Сложное. Была продемонстрирована обратная зависимость между серьезностью повреждения систем или конструкции и вероятностью возникновения в соответствии с рекомендательными материалами 25.1309.

d. Было показано, что основное оборудование, расположенное на шасси или в нишах шасси, защищено от одиночных отказов шины с классификацией отказного состояния хуже, чем Сложное. Следовательно, требования 25.729(f) выполняются.

e. Были показаны технологические лючки топливного бака, расположенные в зонах, рассматриваемых как подверженные риску удара фрагментов шины, для минимизации пробивания и деформации. Следовательно, требования 25.963(e) выполняются.

В результате анализа показано, что самолет способен продолжать безопасный полет и совершать посадку после одиночного отказа или комбинации отказов, вызванных ударами осколков колеса или шины, которые не показаны как практически невероятные. Следовательно, требования 25.671(c) выполняются.

Анализ общего режима для самолета S18 для системы торможения колес

Примечание редактора: Подробную информацию по процессу CMA см. в Приложении K).

1.0 ВВЕДЕНИЕ

Данный анализ представляет собой анализ общего режима (CMA) на уровне самолета для функции торможения колес. Данный анализ гарантирует, что никакое одиночное событие, ни общие события или неисправности, возникающие на уровне самолета, не смогут привести к катастрофическому событию. Этот пример охватывает только независимость между нормальной и альтернативной системами, рассматривая аварийное торможение как часть альтернативного.

(Примечание редактора: Полный анализ на уровне самолета должен также учитывать другие зависимости (например, между торможением колес и системой реверсора тяги), но здесь они для краткости опущены).

2.0 ССЫЛКИ

При выполнении CMA на уровне самолета/системы использовались следующие документы.

1) P4761 «Руководство по методам оценки безопасности бортового оборудования самолетов гражданской авиации».
2) Дерево неисправностей PSSA события «Потеря торможения всех колес» для самолета S18.
3) Зонный анализ № YYY для самолета S18.
4) Анализ частных рисков № ZZZ для самолета S18: пожар, разрыв шины, удар молнии.
5) Анализ общего режима № ZZZ системы генерации и распределения электроэнергии для самолета S18.
6) Анализ общего режима № WWW системы генерации и распределения гидравлической мощности для самолета S18.
7) Оценка безопасности системы торможения колес.

3.0 КРАТКОЕ ОПИСАНИЕ

(Примечание редактора: В целях данной инструкции см. пример PSSA для описания тормозной системы. В случае реального CMA здесь должно быть представлено пересмотренное краткое описание).

4.0 АНАЛИЗ

4.1 Контрольные перечни

Следующие контрольные перечни очерчивают общие источники и виды отказов, которые рассматриваются в анализе общего режима.

Типы общего режима, источники и контрольный перечень отказов

Архитектура конструкции

Наружный источник: Электропитание

Наружный источник: Подача гидравлической энергии

Рабочие характеристики

Расположение

Трассировка трубопроводов и кабелей

Технология, оборудование

Технология, тип компонента/оборудования

Спецификация

Техническая спецификация и ее происхождение

Установка

Процедуры и слесарь-сборщик

Изготовление

Изготовитель и процесс изготовления

Эксплуатация

Действия и процедуры экипажа

Техническое обслуживание с устранением неисправностей

Процедуры и персонал

Факторы окружающей среды

Грозовые разряды,

Загрязнение водой, снеговой кашей, и т.п.

4.2 Требования к независимости

(Примечание редактора: Выбранный пример основан на логическом элементе «И» с элементом «Потеря торможения всех колес», рассмотренного в дереве неисправностей PSSA (см. ссылку 2)).

Входными данными для данного логического элемента являются следующие неисправности: потеря нормальной тормозной системы, альтернативной тормозной системы и аварийной (резервной) тормозной системы.

Требование к независимости, связанное с данным логическим элементом, представляет собой независимость нормальной и альтернативной систем. Аварийная тормозная система должна рассматриваться как часть альтернативной системы.

(Примечание редактора: Из PSSA могут быть получены другие требования к независимости, однако для краткости здесь они не анализировались и не показаны).

4.3 Анализ общего режима

Для того чтобы показать соответствие перечисленным выше требованиям, была проведена экспертиза конструкции и исполнения тормозной системы с точки зрения уязвимости к ошибкам общего режима. Неисправности компонентов, которые могут привести к потере торможения всех колес, проанализированы в таблице 3.3-1.

(Примечание редактора: таблица 4.3-1 адресована используемым частям таблицы К.3.2.1.1-1 и в ней представлена сводка результатов этих исследований. Рассмотрены возможные источники общего режима, ошибки общего режима и обоснование/меры защиты).

Таблица 4.3-1 – (CCA – CMA Самолет)
Анализ общего режима функции торможения колес

Требование: нормальное и альтернативное торможение должны быть независимы		
Источник общего режима	**Ошибка общего режима**	**Обоснование**
АРХИТЕКТУРА КОНСТРУКЦИИ Внешний источник: Электропитание	Общая точка в электропитании, приводящая к полной потере электропитания для управления и контроля нормальной и аварийной тормозных систем.	Электропитание оборудования нормальной системы (например, BSCU, сервоклапан) обеспечивается основными шинами 1 и 2. Электропитание оборудования альтернативной системы (например, дозирующий клапан, сервоклапаны) обеспечивается аварийной шиной.

Требование: нормальное и альтернативное торможение должны быть независимы		
Источник общего режима	**Ошибка общего режима**	**Обоснование**
		Был проведен анализ общего режима системы генерации и распределения электроэнергии для проверки функциональной независимости этих обеих шин.
Внешний источник: Подача гидравлической энергии	Общая точка в гидравлической подаче, приводящая к полной потере гидравлической энергии для нормальной и аварийной тормозных систем.	Нормальная система снабжается при помощи ЗЕЛЕНОГО гидравлического контура. Альтернативная система снабжается ГОЛУБОЙ гидравлической системой. Был проведен анализ общего режима системы генерации и распределения гидравлической энергии для проверки функциональной независимости ЗЕЛЕНОЙ и ГОЛУБОЙ гидравлических систем. Анализ разрыва шины показывает, что для данного отказа необходимо, чтобы разорвались две шины, и чтобы вероятность была приемлемой (см. ссылку 4).
Рабочие характеристики	Общие рабочие характеристики, нарушающие независимость.	Нормальная тормозная система является номинальной. Во время фазы полета она обычно находится в резервном режиме работы, и ее работа запрашивается в конце каждого полета. Альтернативная тормозная система является резервной. Она всегда находится в резервном режиме, и запрашивается при срабатывании автоматического селектора, когда нормальная тормозная система выключена или отказала. Альтернативная система периодически проверяется. Обе системы имеют различные рабочие характеристики (одна система запрашивается тогда, когда другая неисправна).
Расположение	Локальное событие, приводящее к полной потере торможения колес.	Основное оборудование обеих систем расположено в зоне шасси. Физическое разделение электрических кабелей и гидравлических трасс.
Трассы трубопроводов и кабелей	Локальное событие, влияющее на электрические трассы или гидравлические контуры.	Используются независимые электрические трассы. Каждая трасса имеет свои специализированные разъемы. Физический барьер обеспечивает независимость обоих гидравлических контуров во всю длину зоны основного шасси. Зонный анализ проверяет независимость электрических трасс и гидравлических контуров.
ТЕХНОЛОГИЯ, ОБОРУДОВАНИЕ Технология, тип компонента/ оборудования	Ошибка разработки.	Для компонентов используется обычная технология. В обеих системах устанавливаются компоненты и узлы различного типа, за исключением сервоклапанов. Предыдущий опыт по сервоклапанам и квалификационные испытания после изготовления и фаз установки гарантируют правильность работы.
СПЕЦИФИКАЦИЯ Техническая спецификация и ее происхождение	Неправильная спецификация или исходная ошибка.	Различны технические спецификации для установленного оборудования. Независимая техническая экспертиза спецификаций предотвращает исходные ошибки.
УСТАНОВКА Процедуры и слесарь-сборщик	Ошибка установки.	Качество установки: двойная проверка После фазы установки проводятся визуальный осмотр и эксплуатационные испытания нормальной, альтернативной и аварийной систем.

Требование: нормальное и альтернативное торможение должны быть независимы		
Источник общего режима	**Ошибка общего режима**	**Обоснование**
ИЗГОТОВЛЕНИЕ Изготовитель и процесс изготовления	Неправильное изготовление, влияющее на аналогичное оборудование, установленное в обеих системах.	Один и тот же изготовитель для сервоклапанов (нормальных/альтернативных) и компонентов. Процесс обеспечения качества производителя сертифицирован.
ЭКСПЛУАТАЦИЯ Действия экипажа и процедуры	Неправильная процедура эксплуатации или неверные действия экипажа, приводящие к отсоединению обеих систем торможения.	Обычно в конце полета экипаж использует систему автоматического торможения. Экипаж предварительно выбирает соответствующий уровень торможения. Альтернативная система используется, когда НОРМАЛЬНАЯ система отключена. Действие экипажа заключается в нажатии на тормозные педали. Имеется независимость между обеими эксплуатационными процедурами, поскольку они выполняются при различных условиях и используются различные средства.
ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ С УСТРАНЕНИЕМ НЕИСПРАВНОСТЕЙ Процедуры и персонал	Неправильная процедура или ошибка технического обслуживания.	Ошибки технического обслуживания выявляются эксплуатационными испытаниями после каждого технического обслуживания. Эти испытания гарантируют правильную работу оборудования. Когда техническое обслуживание с устранением неисправностей проводится на нормальной тормозной системе, то альтернативная система выключена. Когда техническое обслуживание с устранением неисправностей проводится на альтернативной тормозной системе, то нормальная система выключена. В обоих случаях окончательные испытания, проводимые на обеих системах, выявляют все возможные ошибки технического обслуживания.
ФАКТОРЫ ОКРУЖАЮЩЕЙ СРЕДЫ Грозовые разряды, загрязнение водой, снеговой кашей	Фактор окружающей среды, действующий одновременно на работу нормальной и альтернативной тормозной систем.	Нормальная и альтернативная тормозные системы защищены от воздействия грозовых разрядов. Оборудование квалифицировано как стойкое к загрязнению взлетно-посадочной полосы. Всесторонние испытания на воздействие окружающей среды проводятся только для одной работающей тормозной системы, другая является резервной и обычно работает в другое время.

5.0 ЗАКЛЮЧЕНИЕ

В результате анализа показано следующее:

a) не было выявлено ни одного события в результате ошибки общего режима, которое имеет катастрофическое влияние;

b) эти ошибки общего режима, которые могут привести к аварийному состоянию, ограничиваются специальными испытаниями, процессами изготовления, средствами обеспечения качества, или являются приемлемыми с учетом их вероятности.

РУКОВОДСТВО 4761

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

Зак. 3154

Издание – ОАО “Авиаиздат”, 2011

gost.e-ecolog.ru