Авторский коллектив Некоммерческого партнерства «Союз авиапроизводителей» под руководством А.Г. Колосова

Конкурс «Авиастроитель года»

Номинация №10 "За вклад в разработку нормативной базы в авиации и авиастроении"

Разработка методики определения соответствия самолетного оборудования требованиям авиационных правил

Рекомендательный циркуляр РЦ25.1309

Конструкция и анализ систем.

1. ЦЕЛЬ.

a. В настоящем Рекомендательном Циркуляре (РЦ) описываются приемлемые методы доказательства соответствия требованиям пункта 25.1309 АП-25.

b. Степень применения более структурированных методов и указаний, содержащихся в данном РЦ, зависит от сложности систем и последствий их отказов. В общем случае, объем и структура анализов, необходимых для демонстрации соответствия требованиям пункта 25.1309 АП-25, увеличиваются с увеличением сложности системы и степени опасности последствий ее отказных состояний. Методы, описанные в настоящем РЦ, не являются единственно возможными. Возможно использование других методов доказательства соответствия требованиям п. 25.1309, согласованных в установленном порядке.

2. *ИСПОЛЬЗУЕМЫЕ ДОКУМЕНТЫ*

В настоящем документе содержатся ссылки на следующие руководства и справочные материалы:

(1) Квалификационные требования КТ-160D (КТ-160G) «Условия эксплуатации и окружающей среды для бортового авиационного оборудования. Требования, нормы и методы испытаний».
(2) Квалификационные требования КТ-178B (КТ-178C) «Требования к программному обеспечению бортовой аппаратуры и систем при сертификации авиационной техники».
(3*) Рекомендательный циркуляр EASA AMC 25.1322 Системы оповещения.
(4*) Рекомендательный циркуляр FAA/EASA AC25.19/AMC25.19 Сертификационные требования к техническому обслуживанию.
(5*) Рекомендательный циркуляр EASA AMC 20-115 Оценка программного обеспечения при сертификации бортовых систем и оборудования.

(6*) Рекомендательный циркуляр FAA/EASA AC/AMC 25-901 Оценка безопасности силовых установок.
(7) Руководство P4754 по процессам сертификации высокоинтегрированных сложных бортовых систем воздушных судов гражданской авиации (на базе документов SAE/ARP4754 и EUROCAE/ED-79) (Руководство P4754A по проектированию гражданских воздушных судов и их систем).
(8) Руководство P4761 по методам оценки безопасности систем и бортового оборудования самолетов гражданской авиации, 2010.

Примечание:
*) – документ рекомендуется к использованию до введения в действие аналогичных документов Авиарегистра МАК.

3. ПРИМЕНИМОСТЬ РЦ 25.1309

Пункт 25.1309 АП-25 является общим требованием, действие которого распространяется на любое установленное на самолете оборудование или систему в дополнение к специфическим требованиям к конкретным системам с учетом указанных ниже исключений и уточнений.

a. Несмотря на то, что требования пункта 25.1309 АП-25 не применяются к требованиям Раздела B к характеристикам устойчивости и управляемости и летным характеристикам самолета, а также к требованиям по прочности конструкции Разделов C и D, он применяется к любым функциональным системам, от которых зависит соответствие любым из этих требований. Например, его действие не распространяется на присущие самолету характеристики сваливания или на их оценку, однако распространяется на систему предупреждения о сваливании, используемую для установления соответствия требованиям п. 25.207 АП-25.

b. Последствия единичных отказов и заклиниваний в системе управления самолетом, рассматриваемых в п.п. 25.671(c)(1) и 25.671(c)(3) АП-25, подлежат оценке вне зависимости от вероятностей возникновения этих отказов в соответствии с критериями, применяемыми при установлении соответствия указанным требованиям п.п. 25.671(c) АП-25. Требования п. 25.1309(b) АП-25 применяются к комбинациям отказов в системе управления самолетом и взаимодействующих с ней системах (гидравлической системе, системе электроснабжения, системах, передающих информацию в систему управления и т.п.) с учетом требований п. 25.671(c)(2).

c. Некоторые единичные отказы, подпадающие под действие п. 25.735(b)(1) АП-25, исключаются из рассмотрения по п. 25.1309(b) АП-25. Основанием для этого является требование к тормозной системе, ограничивающее последствия любого единичного отказа системы увеличением в два раза тормозной дистанции пробега при торможении. Предполагается, что данное требование обеспечивает удовлетворительный уровень безопасности без необходимости анализировать конкретные обстоятельства и условия возникновения единичного отказа.

d. Последствия отказов, подпадающих под действие п.п. 25.810(a)(1)(v) и 25.812 АП-25, исключаются из рассмотрения по п. 25.1309(b) АП-25. Отказные состояния указанного аварийно-спасательного оборудования кабины, связаны с различными сценариями эвакуации, определить вероятность которых невозможно. Возможность определения адекватных сценариев, при которых можно было бы продемонстрировать соответствие требованиям п. 25.1309(b) АП-25, не доказана. Таким образом, более практичным подходом считается установление конкретных требований к конструкции или демонстрации определенных характеристик надежного функционирования и исключение соответствующего оборудования из области применения требований п. 25.1309(b) АП-25. Традиционно такой подход признан приемлемым.

e. Требования п. 25.1309 АП-25 применяются в отношении двигателя, воздушного винта и силовой установки с учетом конкретной области применения и исключений, указанных в п. 25.901(c) АП-25.

f. Зарезервировано.

4. *ОПРЕДЕЛЕНИЯ*

Следующие определения относятся к требованиям к конструкции и анализу систем, которые содержатся в п. 25.1309 АП-25, и к настоящему РЦ. Не следует предполагать их применение к аналогичным или подобным терминам, используемым в других правилах или РЦ.

a. ***Анализ*** *(Analysis),* ***Оценка*** *(Assessment)* В данном циркуляре используются термины "анализ" и "оценка" Каждый термин имеет широкое толкование и оба термина являются в некоторой степени взаимозаменяемыми. Тем не менее, термин "анализ" обычно применяется для обозначения более конкретного, более детализированного изучения, в то время как термин "оценка" может иметь более общее или более широкое значение и может включать в себя один или несколько видов анализа. На практике, значение этих терминов зависит от конкретного случая, например, анализ дерева отказов, Марковский анализ, предварительная оценка безопасности системы и т.д.

b. . зарезервировано

c. ***Средняя вероятность на час полета*** *(Average Probability Per Flight Hour).* Для целей настоящего РЦ представляет собой число случаев, в которых прогнозируется возникновение соответствующего отказного состояния на протяжении всего срока службы всех самолетов данного типа, деленное на ожидаемое общее число часов налета всех самолетов этого типа

> *Примечание: средняя вероятность на час полета обычно рассчитывается как вероятность возникновения отказного состояния в типовом полете средней продолжительности, деленная на эту среднюю продолжительность (см. Приложение 3).*

d. ***Кандидат на Сертификационные требования к техническому обслуживанию (КСТТО)*** ***(****Candidate Certification Maintenance Requirements - CCMR).* Периодические проверки при техническом обслуживании или проверки летным экипажем могут использоваться при анализе безопасности для демонстрации соответствия требованиям п. 25.1309(b) АП-25 для аварийных и катастрофических отказных состояний. Если такие проверки не могут быть приняты в качестве стандартных процедур обслуживания или стандартных процедур, включенных в курс летной подготовки, они становятся кандидатами на Сертификационные требования к техническому обслуживанию. АМС 25.19 представляет методы, на основании которых из кандидатов определяются Сертификационные требования к техническому обслуживанию (*Certification Maintenance Requirements* -CMR). Сертификационные требования к техническому обслуживанию (СТТО) принимаются в качестве обязательных периодических проверок при техническом обслуживании, определяемых как эксплуатационные ограничения Сертификата типа самолета.

e. ***Проверка*** *(Check).* Обследование (например, путем проведения контроля или испытаний) с целью определения физической целостности и/или работоспособности изделия.

f. ***Сложная система*** *(complex system).* Система считается сложной, если определение принципов ее работы, видов отказов и их последствий требует применения специальных аналитических методов. Как правило, к сложным относятся системы, имеющие в своем

составе вычислительные средства и/или обладающие множественными взаимосвязями с другими системами.

g. ***Традиционная система*** *(conventional system).* Система может рассматриваться в качестве традиционной, если ее функционирование, технологические средства, используемые для реализации ее функционирования, и ее предназначение являются аналогичными или весьма сходными с ранее одобренными системами, которые обычно применяются в авиации.

h. ***Оценка конструкции*** *(Design Appraisal).* Качественная оценка полноты учета требований к конструкции системы и ее безопасности.

i. ***Гарантия разработки*** *(Development Assurance).* Все запланированные систематические действия, имеющие целью с достаточной степенью доверия распознать и устранить ошибки в технических требованиях, конструкции и реализации для обеспечения соответствия системы применимым требованиям сертификационного базиса.

j. ***Ошибка*** *(Error).* Упущение или неверное действие члена экипажа или персонала, выполняющего техническое обслуживание, или ошибка в технических требованиях, при проектировании или в реализации.

k. ***Внешнее воздействие (явления)*** *(Event)* — событие, источник происхождения которого не связан с конструкцией самолета, такое, как атмосферные условия (например, порыв ветра, изменения температуры, обледенение, разряды молнии и т. д.), состояние ВПП, условия связи, навигации и диспетчерского обслуживания, столкновение с птицей, пожар в кабине или в багажном отсеке. Предполагается, что этот термин не охватывает саботаж.

l. ***Отказ*** *(Failure).* Событие, которое оказывает неблагоприятное воздействие на работу компонента, детали или элемента таким образом, что он дальше не может функционировать заданным образом (это включает как потерю функции, так и неправильное функционирование).

Примечание: Ошибки могут приводить к возникновению отказов, однако они не рассматриваются как отказы.

m. ***Отказное состояние (***функциональный отказ*,* вид отказа системы*)* *(Failure condition).* Под отказным состоянием понимается состояние системы, характеризуемое конкретным нарушением ее функций независимо от причин, вызывающих это состояние. Отказное состояние определяется на уровне каждой системы через последствия, оказываемые им на функционирование этой системы. Оно также характеризуется влиянием на другие системы и на самолет в целом.

n. ***Оценка установки*** *(Installation Appraisal).* Качественная оценка целостности и безопасности установки компонентов системы на самолете. Любые отклонения от нормальных, общепринятых в отрасли технологий установки, например, отклонения по зазорам и допускам, подлежат анализу, особенно при оценке изменений, внесенных после ввода в эксплуатацию.

o. ***Скрытый отказ (latent failure)***. Отказ, является скрытым до тех пор, пока он не выявлен экипажем или персоналом, выполняющим техническое обслуживание.

Существенный скрытый отказ (significant latent failure) – это такой отказ, который в сочетании с одним или несколькими единичными отказами или событиями приводит к возникновению аварийной или катастрофической ситуации.

p. ***Качественный анализ*** *(Qualitative analysis).* Аналитический процесс, в ходе которого оценка безопасности систем и самолета производится экспертно без определения количественных характеристик.

q. ***Количественный анализ*** *(Quantitative analysis).* Аналитический процесс, в ходе которого для оценки безопасности систем и самолета применяются математические методы.

r. ***Резервирование*** *(Redundancy)* – способ обеспечения выполнения заданных функций за счет использования дополнительных средств и/или возможностей, избыточных по отношению к минимально необходимым для выполнения этих функций.

s. ***Система*** (функциональная система самолета) *(System),*— совокупность взаимосвязанных элементов, узлов (блоков) и агрегатов, предназначенных для выполнения заданных функций.
Перечень функциональных систем и их состав устанавливаются Разработчиком самолета.

t. ***Продолженный безопасный полет и посадка*** — способность продолжить управляемый полет и выполнить посадку в пригодном аэропорту, возможно с применением экстренных действий по парированию отказа и его последствий, но без необходимости применения пилотом исключительного летного мастерства или чрезмерных усилий.

u. ***Особая ситуация*** — ситуация, возникающая в полете в результате воздействия неблагоприятных факторов или их сочетаний и приводящая к снижению безопасности полета. Особые ситуации (эффекты) классифицируются с использованием следующих критериев:
(a) Ухудшение летных характеристик, характеристик устойчивости и управляемости, прочности и работы систем.

> *Примечание: Полет рассматривается с момента начала движения самолета по ВПП при взлете до освобождения ВПП после посадки или остановки самолета.*

(b) Увеличение рабочей (психофизиологической) нагрузки на экипаж сверх нормально допустимого уровня.
(c) Дискомфорт, травмирование или гибель находящихся на борту людей.

v. ***Ожидаемые условия эксплуатации.*** Условия, которые известны из практики или возникновение которых можно с достаточным основанием предвидеть в течение срока службы самолета с учетом его назначения. Эти условия включают в себя параметры состояния и факторы воздействия на самолет внешней среды, эксплуатационные факторы, влияющие на безопасность полета.
Ожидаемые условия эксплуатации не включают в себя:
(a) Экстремальные условия, встречи с которыми можно надежно избежать путем введения эксплуатационных ограничений и правил.
(b) Экстремальные условия, которые возникают настолько редко, что требование выполнять Нормы летной годности в этих условиях привело бы к обеспечению более высокого уровня летной годности, чем это необходимо и практически обосновано.

w. ***Предельные ограничения*** — ограничения режимов полета, при выходе за которые не обеспечено безопасное продолжение и завершение полета. Выход за предельные ограничения недопустим ни при каких обстоятельствах.

x. ***Функция системы*** - один из выходов (результат работы) системы, характеризуемый заданным воздействием на самолет или сигналом, выдаваемым в другие системы или окружающую среду.

y. ***Эксплуатационные ограничения*** — условия, режимы и значения параметров, определяющие разрешенную область для эксплуатации самолета, преднамеренный выход за пределы которой недопустим в процессе эксплуатации самолета.

5. ОБОСНОВАНИЕ.

a. Общие положения.

В течение ряда лет проводилась оценка систем самолета на соответствие определенным требованиям, по критерию "единичного отказа" или с использованием концепции отказобезопасной конструкции.
Создание самолетов новых поколений потребовало выполнения более критичных с точки зрения безопасности полета функций, что, в основном, привело к усложнению конструкции систем, разработанных для выполнения этих функций.
Стали возможны потенциально опасные события для самолета и находящихся на борту людей, связанные с потерей системой одной или нескольких функций или неправильным функционированием этой системы, а также нарушением взаимодействия между системами, выполняющими различные функции.
Это привело к необходимости обеспечения обратного соотношения между вероятностью возникновения отказного состояния и критичностью его последствий для самолета и находящихся на борту людей (см. рисунок 1).
При оценке приемлемости конструкции систем самолета было признано, что должны быть установлены рациональные значения вероятностей отказных состояний в зависимости от критичности (тяжести, степени опасности) их последствий.
Мировой опыт эксплуатации показал, что вероятность авиационного происшествия по причинам, связанным с эксплуатационными факторами и с конструкцией планера и систем самолета, составляет приблизительно один случай на миллион часов налета. При этом, около 10 процентов от общего числа летных происшествий были связаны с отказными состояниями систем самолета.
При проектировании новых самолетов будет целесообразно не допускать более высокую вероятность авиационных происшествий, причиной которых являются отказы систем. Поэтому следует потребовать, чтобы для вновь создаваемых самолетов суммарная вероятность возникновения катастрофы (авиационного происшествия с человеческими жертвами) по причине отказных состояний систем должна быть не больше, чем 1 случай на 10 миллионов летных часов или $1x10^{-7}$ на час полета.
Трудность при этом заключается в том, что до проведения вероятностного анализа отказных состояний всех систем самолета с оценкой их последствий невозможно сказать, будет ли обеспечен такой уровень вероятности.
По этой причине условно приняли, что на самолете существует около 100 потенциальных отказных состояний, которые могут быть катастрофическими.
Принятая допустимая вероятность катастрофы $1x10^{-7}$ на час полета может быть равномерно распределена между этими отказными состояниями. Таким образом,

полученное допустимое значение вероятности каждого катастрофического отказного состояния составляет величину порядка $1x10^{-9}$ на час полета.

Верхнее предельное значение для средней вероятности на час полета катастрофических отказных состояний принимается равным $1x10^{-9}$, и устанавливает примерное значение вероятности для термина "практически (крайне) невероятный" ("Extremely Improbable"). Возникновение отказных состояний, имеющих менее тяжелые последствия, соответственно может быть более вероятным.

b. Концепция отказобезопасной конструкции.

Нормы летной годности АП-25 основаны на принципах обеспечения отказобезопасной конструкции (fail-safe design), которые учитывают вероятности и последствия отказов и их комбинаций.

(1) В отношении отказов установлены следующие основные цели:

(i) В любой системе или подсистеме допускается отказ любого отдельного элемента, компонента или соединения в течение одного любого полета независимо от его вероятности. Эти единичные отказы не должны быть катастрофическими.

(ii) Допускаются также последующие отказы в течение того же полета, будь то выявленные или скрытые, а также сочетания этих отказов, если только не доказано, что их возникновение совместно с первым отказом является практически невероятным.

(2) Концепция обеспечения отказобезопасной конструкции (отказобезопасности конструкции) включает указанные ниже принципы или технические приемы проектирования. Применение только одного из этих принципов или технических приемов редко является достаточным. То есть для обеспечения того, чтобы значительное (Major) отказное состояние было бы редким (Remote), аварийное (Hazardous) отказное состояние было бы крайне маловероятным (Extremely Remote) и катастрофическое отказное состояние было бы практически невероятным (Extremely Improbable) обычно необходимо использовать сочетание двух или более принципов или технических приемов обеспечения отказобезопасности конструкции:

(i) Целостность и качество конструкции, включая установление ограничений по ресурсу/сроку службы для обеспечения заданного функционирования и предотвращения отказов.

(ii) Резервирование или резервные системы, которые обеспечивают продолжение функционирования после любого единичного отказа (или другого заданного числа отказов), например, два или более двигателей, гидравлических систем, систем управления полетом и пр.

(iii) Изолирование и/или разделение систем, компонентов и элементов таким образом, чтобы отказ одной (одного) из них не вызывал отказ других.

(iv) Применение компонентов с подтвержденным уровнем надежности, для того чтобы несколько независимых отказов едва ли возникло в течение одного и того же полета.

(v) Сигнализация или индикация отказов для обеспечения их обнаружения.

(vi) Рекомендации для летного экипажа с указанием корректирующих действий, которые необходимо выполнить после обнаружения отказа.

(vii) Контролепригодность: приспособленность к проверке состояния компонентов.

(viii) Конструктивные меры по локализации (ограничению) последствий отказа, включая способность выдерживать повреждения, ограничить влияние на безопасность или последствия отказов.

(ix) Предусмотренное в конструкции направление развития отказа с целью регулирования и направления последствий отказа таким образом, чтобы ограничить его влияние на безопасность.

(x) Запасы или коэффициенты безопасности для учета любых невыявленных или непредвидимых неблагоприятных обстоятельств.
(xi) Устойчивость к ошибкам, которая учитывает неблагоприятные последствия возможных ошибок при проектировании самолета, его испытаниях, производстве, эксплуатации и техническом обслуживании.

c. Системы с высокой степенью интеграции.

(1) Возникли сомнения относительно эффективности и полноты технических приемов, используемых для оценки безопасности высоко интегрированных систем, которые выполняют сложные и взаимосвязанные функции, особенно с использованием электронных технологий и электронной техники с программным обеспечением.
Сомнения заключаются в том, что методы проектирования и анализа, традиционно применяемые для детерминированных рисков или для общепринятых (традиционных), не являющихся сложными систем, могут не обеспечивать адекватный учет вопросов безопасности для более сложных систем.
По этой причине, для оценки этих более сложных систем были применены другие методы обеспечения соответствия. Например, методы обеспечения гарантии разработки, в которых используется сочетание критериев обеспечения гарантии процесса разработки и критериев полноты верификации, методы структурного анализа, а также методы оценки, применяемые для проведения анализа на уровне самолета (при необходимости) или, как минимум, на уровне интегрированных или взаимодействующих систем.
Их систематическое использование позволяет повысить уверенность в том, что ошибки в требованиях или в конструкции, а также влияние интеграции или взаимодействия систем должным образом выявлены и исправлены.

(2) Принимая во внимание вышеупомянутые разработки, а также изменения, внесенные в пункт АП-25.1309, настоящий РЦ разработан на основе аналогичного АМС 25.1309 к CS-25 с целью включения в него новых подходов, как качественных, так и количественных, которые могут быть использованы при определении требований к безопасности и установлении соответствия этим требованиям, а также для отражения изменений в правилах, как на уровне самолета в целом, так и на уровне его отдельных систем. При этом учтен отечественный опыт разработки и применения Методов определения соответствия требованиям главы 2 НЛГС-3.
В настоящем документе представлены также рекомендации по определению того, когда, или в каких случаях, следует выполнять конкретные виды анализа или действия по подтверждению разработки в рамках процессов разработки и оценки безопасности.
Для вероятностных характеристик, используемых в требованиях, установлены количественные значения, которые следует применять при исследовании влияния отказов систем с помощью количественных методов анализа.
Аналитические методы, используемые при определении количественных значений, предназначены для того, чтобы дополнить, но не заменить, качественные методы, опирающиеся на инженерные и эксплуатационные оценки.

6. КЛАССИФИКАЦИЯ ОТКАЗНЫХ СОСТОЯНИЙ И ВЕРОЯТНОСТНЫЕ ТЕРМИНЫ

a. *Классификация*. Отказные состояния могут быть классифицированы по степени опасности их последствий следующим образом:

(1) *Не влияющие на безопасность* (без возникновения особой ситуации - No Safety Effect): Отказные состояния, которые не влияют на безопасность; например, отказные состояния,

которые не оказывают неблагоприятного воздействия на эксплуатационные возможности самолета или не увеличивают рабочую нагрузку на экипаж.

(2) *Незначительные* (усложнение условий полета - Minor): Отказные состояния, которые незначительно снижают безопасность полета самолета и требуют от экипажа действий, заведомо находящихся в пределах их возможностей. Незначительные отказные состояния, например, характеризуются незначительным снижением запасов по безопасности или функциональных возможностей, незначительным увеличением рабочей нагрузки на экипаж, такое как изменение плана полета, или некоторый физический дискомфорт для пассажиров или бортпроводников.

(3) *Значительные* (сложная ситуация - Major): Отказные состояния, которые снижают способность самолета или возможности экипажа справиться с неблагоприятными условиями эксплуатации до такой степени, что имеют место, например, заметное снижение запасов по безопасности или эксплуатационных возможностей, заметное увеличение рабочей нагрузки на экипаж или появление условий, понижающих эффективность работы экипажа, или дискомфорт для летного экипажа, или ухудшение условий для пассажиров или бортпроводников возможно, с причинением травм.

(4) Аварийные (Hazardous): Отказные состояния, которые снижают способности самолета или возможности экипажа справиться с неблагоприятными условиями до такой степени, что имеет место:
(i) Значительное снижение запасов по безопасности или функциональных возможностей; или
(ii) Ухудшение условий работы или чрезмерная рабочая нагрузка, такие, что нельзя полагаться, что летный экипаж выполнит свои задачи точно и полностью; или
(iii) Серьезные или смертельные ранения относительно небольшого числа находящихся на борту людей, не входящих в летный экипаж.

(5) Катастрофические (Catastrophic): Отказные состояния, которые приводят к многочисленным жертвам, обычно с потерей самолета.

Примечание: "Катастрофическое" отказное состояние ранее было определено как отказное состояние, которое препятствует продолженному безопасному полету и посадке самолета.

b. Вероятностные термины, используемые при проведении качественного анализа.
При использовании качественного анализа для установления соответствия требованиям пункта 25.1309(b) АП-25, стали общепринятыми при инженерной оценке следующие определения вероятностных терминов, используемых пункте 25.1309 АП-25 и в настоящем РЦ:
(1) Вероятные (Probable) отказные состояния - отказные состояния, возникновение которых ожидается один или большее число раз в течение полного срока службы каждого самолета.
(2) Редкие (маловероятные - Remote) отказные состояния - возникновение которых на каждом самолете вряд ли возможно в течение всего срока его эксплуатации, но которые могут возникать несколько раз на протяжении общего срока эксплуатации определенного числа самолетов того же типа.
(3) Крайне маловероятные (Extremely Remote) - отказные состояния, возникновение которых не предвидится на каждом самолете в течение его полного срока службы, но которые могут возникнуть небольшое число раз при рассмотрении полного срока службы всех самолетов данного типа.

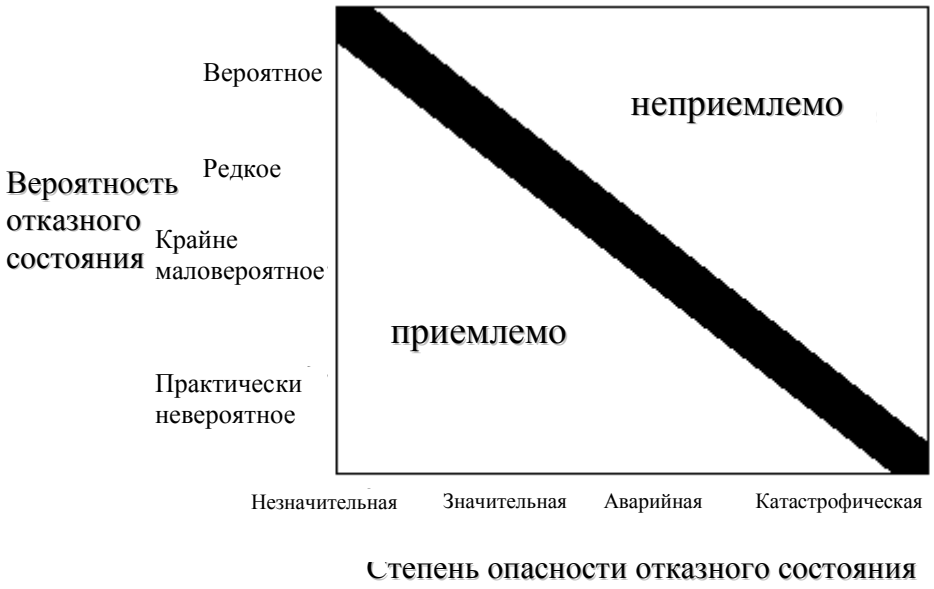
(4) Крайне невероятные (практически невероятные - Extremely Improbable) отказные состояния - состояния, возникновение которых не предвидится в течение полного срока службы всех самолетов данного типа.

c. Вероятностные термины, используемые при проведении количественного анализа.
В случае применения количественного анализа при определении соответствия требованиям п. 25.1309(b) АП-25 являются общепринятыми и используются в ходе инженерной оценки следующие определения вероятностных терминов, применяемых в требованиях указанного пункта и в настоящем параграфе РЦ. Они выражаются в виде приемлемых диапазонов средней вероятности на час полета.
(1) Диапазоны вероятностей.
(i) Вероятные отказные состояния – отказные состояния, средняя вероятность возникновения которых превышает величину порядка 1×10^{-5} на час полета.
(ii) Маловероятные отказные состояния – отказные состояния, средняя вероятность возникновения которых порядка 1×10^{-5} или менее, однако превышает величину порядка 1×10^{-7} на час полета.
(iii) Крайне маловероятные отказные состояния – отказные состояния, средняя вероятность возникновения которых порядка 1×10^{-7} или менее, однако превышает величину порядка 1×10^{-9} на час полета.
(iv) Крайне (практически) невероятные отказные состояния – отказные состояния, средняя вероятность возникновения которых составляет величину порядка 1×10^{-9} или менее на час полета.

7. ЦЕЛИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ.

a. Цели пункта 25.1309 АП-25 заключаются в обеспечении приемлемого уровня безопасности для оборудования и систем, установленных на самолете. Должна существовать логическая и приемлемая обратная зависимость между средней вероятностью возникновения отказных состояний на час полета и степенью опасности отказных состояний, как показано на рисунке 1, и при этом:
(1) Для отказных состояний, не влияющих на безопасность, отсутствуют требования к вероятности возникновения.
(2) Незначительные (Minor) отказные состояния, приводящие к усложнению условий полета (УУП), могут быть вероятными (Probable).
(3) Значительные (Major) отказные состояния, приводящие к сложной ситуации (СС), должны быть не более частыми, чем маловероятными (Remote).
(4) Аварийные (Hazardous) отказные состояния (АС) должны быть не более частыми, чем крайне маловероятными (Extremely Remote).
(5) Катастрофические (Catastrophic) отказные состояния (КС) должны быть крайне (практически) невероятными (Extremely Improbable).

Рисунок 1. Зависимость между средней вероятностью возникновения отказных состояний на час полета и степенью опасности отказных состояний



b. Цели обеспечения безопасности для отказных состояний приведены в таблице 1.

Таблица 1. Зависимость между средней вероятностью возникновения отказного состояния на час полета и степенью опасности отказного состояния

Последствия для самолета	Отсутствие влияния на эксплуатационные характеристики или безопасность	Незначительное уменьшение функциональных возможностей или запасов безопасности	Значительное уменьшение функциональных возможностей или запасов безопасности	Опасное уменьшение функциональных возможностей или запасов безопасности	Потеря управляемости или разрушение фюзеляжа
Последствия для находящихся в самолете людей, за исключением летного экипажа	Неудобство	Физический дискомфорт	Физическое недомогание, возможны травмы	Серьезные или смертельные травмы небольшого числа пассажиров или членов обслуживающего экипажа	Многочисленные жертвы
Последствия для летного экипажа	Отсутствие последствий для летного экипажа	Незначительное увеличение нагрузки	Физический дискомфорт или заметное увеличение нагрузки	Физическое недомогание или чрезмерное увеличение нагрузки, снижающее способность выполнять задачи	Жертвы или потеря работоспособности
Допустимая вероятность (качественная оценка)	Требования к вероятности не устанавливаются	Вероятное	Маловероятное	Крайне маловероятное	Крайне (практически) невероятное
Допустимая вероятность (количественная оценка): Средняя вероятность возникновения отказного состояния на час полета (порядка):	Требования к вероятности не устанавливаются	$\leq 10^{-3}$	$\leq 10^{-5}$	$\leq 10^{-7}$	$\leq 10^{-9}$
Классификация особой ситуации (отказного состояния)	Без возникновения особой ситуации (БП/БС)	Незначительная (УУП)	Значительная (СС)	Аварийная (АС)	Катастрофическая (КС)

c. Цели обеспечения безопасности, связанные с катастрофическими отказными состояниями, могут быть подтверждены посредством демонстрации того, что:
(1) Ни один единичный отказ не приведет к катастрофическому отказному состоянию; и
(2) Каждое катастрофическое отказное состояние является крайне (практически) невероятным событием.
d. В исключительных случаях если обеспечить количественные уровни вероятностей в отношении отказных состояний, приводящих к катастрофической ситуации, невозможно с технологической или практической точки зрения, то обеспечить достижение целей безопасности п. 8(c)(2) можно путем выполнения всех следующих действий:
(1) Применением хорошо апробированных и зарекомендовавших себя методов проектирования и конструирования систем; и
(1*) Техническим обоснованием принятых конструктивных решений и практической невозможности строгого обеспечения количественных уровней вероятностей для отказных ситуаций с катастрофическими последствиями; и
(2) Определением средней вероятности возникновения отказного состояния на час полета для каждого отказного состояния, приводящего к катастрофической ситуации, с использованием структурированных методов, таких как табличный метод, метод логических схем, анализ деревьев отказов, метод Марковского анализа или диаграммы зависимостей; и
(3) Демонстрацией того, что сумма средних вероятностей возникновения отказных состояний на час полета всех катастрофических отказных состояний систем самолета составляет величину порядка 10^{-7} или меньше (для обоснования смотри пункт 6(a)).

e. Цели обеспечения безопасности, связанные с аварийными отказными состояниями, могут быть подтверждены посредством демонстрации того, что:
(1) отказное состояние (функциональный отказ, вид отказа системы) возникает в результате сочетания двух и более независимых последовательных отказов;
(2) отказное состояние является следствием конкретного механического отказа типа заклинивания или разрушения одного из элементов системы и может быть отнесено к событию не более частому, чем крайне маловероятное на основании анализа принятых конструктивных решений и результатов ресурсных испытаний и опыта эксплуатации аналогичных конструкций, учитывающего используемые принципы контроля качества изготовления и применяемые конструкционные материалы в серийном производстве, стабильность технологических процессов, а также предусмотренные эксплуатационной документацией средства, методы и периодичность технического обслуживания.

8. СООТВЕТСТВИЕ ТРЕБОВАНИЯМ ПУНКТА АП-25.1309

Этот параграф описывает специфические методы подтверждения соответствия требованиям пункта АП-25.1309. Заявителю следует на ранних стадиях процедуры сертификации согласовать выбор приемлемых методов подтверждения соответствия с уполномоченным органом по сертификации.

a. *Соответствие требованиям пункта АП-25.1309(a).*

(1) Должно быть показано, что установленные на самолете оборудование и системы, подпадающие под требования пункта АП-25.1309(a)(1), должным образом выполняют заданные функции. Условия эксплуатации самолета и параметры окружающей среды, для которых требуется подтвердить правильное функционирование оборудования, систем и установок, включают область режимов и условий полета, установленную эксплуатационными ограничениями и определенную Летным Руководством самолета

(Airplane Flight Manual), а также любые изменения этой области, связанные с выполнением процедур в особых случаях полета (abnormal and emergency procedures). Должны быть также учтены другие внешние условия эксплуатации, такие как атмосферная турбулентность, воздействие электромагнитных полей высокой интенсивности (HIRF), атмосферные осадки и удары молнии, встречу с которыми следует обоснованно ожидать. Значения параметров внешних условий эксплуатации, которые должны быть рассмотрены, ограничиваются установленными для них сертификационными стандартами и опытом эксплуатации.

(2) Помимо эксплуатационных условий и параметров окружающей среды следует также учесть воздействие среды внутри самолета. Эти воздействия должны включать, например, вибрационные и инерционные нагрузки, изменения давления жидкостей и электрической мощности, загрязнение рабочих жидкостей или образование паров в результате нормальной эксплуатации или случайных утечек, разбрызгивания, а также аспекты технического обслуживания. Документы, указанные в пункте 3, устанавливают ряд стандартных условий и процедур проведения испытаний на воздействие окружающей среды, которые могут быть использованы для подтверждения соответствия. При проведении таких испытаний может быть использовано оборудование, которое указано в соответствующих квалификационных требованиях или Стандартных Технических Требованиях (Technical Standard Orders), содержащих процедуры испытаний на воздействие окружающей среды, или оборудование, квалифицированное в соответствии с другими стандартами испытаний на воздействие окружающей среды. Условия, в которых установленное на самолете оборудование будет работать в эксплуатации, должны быть не более тяжелыми, чем условия окружающей среды, для которых оборудование квалифицировано.

(3) Доказательство правильного функционирования оборудования и систем с учетом их установки на самолете в одобренных условиях эксплуатации самолета и параметрах окружающей среды может быть продемонстрировано испытаниями и/или анализом или ссылками на сопоставимый опыт эксплуатации на других самолетах. Должно быть показано, что сопоставимый опыт эксплуатации применим для предлагаемой установки оборудования на самолете. Для оборудования и систем самолета, на которые распространяются требования параграфа АП-25.1309(a)(1), должно быть также подтверждено, что нормальное (при отсутствии отказов) функционирование такого оборудования и систем не влияет на правильное выполнение заданных функций другого оборудования и систем, подпадающих под требования п. АП-25.1309(a)(1).

(4) Требования пункта АП-25.1309(a)(2) обычно распространяются на оборудование и системы, связанные с обеспечением комфорта пассажиров, например, системы развлечения пассажиров, бортовые телефоны и т.д., отказ или неправильное функционирование которых само по себе не должно влиять на безопасность самолета. Эксплуатационные и квалификационные требования для такого оборудования и систем в части влияния условий эксплуатации и воздействия окружающей среды ограничены испытаниями, которые необходимы для того, чтобы показать, что их нормальное функционирование или функционирование при возникновении отказов не оказывает неблагоприятного воздействия на правильное функционирование оборудования и систем, подпадающих под требования пункта АП-25.1309(a)(1), в местах их установки и не оказывает иного неблагоприятного влияния на безопасность самолета и находящихся на борту людей. Примерами таких неблагоприятных влияний являются: возгорание, взрыв, воздействие на находящихся на самолете людей высокого напряжения и прочее.

b. *Соответствие требованиям пункта АП-25.1309(b).*

Пункт АП-25.1309(b) требует, чтобы системы самолета и соответствующие компоненты, рассматриваемые отдельно и во взаимодействии с другими системами, были спроектированы таким образом, чтобы любое катастрофическое отказное состояние (функциональный отказ) было крайне (практически) невероятным и не возникало в результате единичного отказа. Он также требует, чтобы любое аварийное отказное состояние (функциональный отказ) было крайне маловероятным и чтобы любое значительное отказное состояние (функциональный отказ, приводящий к сложной ситуации) было маловероятным. Анализ всегда должен рассматривать применение концепции отказобезопасной конструкции, описанной в параграфе 6b, и уделять особое внимание обеспечению эффективного использования методов проектирования, которые предотвращают возможность повреждения или другого неблагоприятного воздействия более чем на один канал резервированной системы или более чем на одну систему, выполняющую функционально сходные функции, в результате единичных отказов.

(1) *Общие положения.* Соответствие требованиям пункта АП-25.1309(b) должно быть показано анализом, расчетами, а также, где это необходимо, соответствующими наземными, летными испытаниями или испытаниями на моделирующей установке (пилотажном стенде). Должны быть идентифицированы возможные отказные состояния и оценены их последствия. Максимально допустимая вероятность возникновения каждого отказного состояния определяется последствиями отказного состояния. При оценке вероятностей отказных состояний должны быть объяснены допущения, принятые при анализе.

При проведении анализа должны быть рассмотрены:

(i) Возможные отказные состояния систем и их причины, виды отказов элементов и компонентов системы, а также повреждения от источников, внешних по отношению к системе.

(ii) Возможность возникновения множественных отказов и необнаруженных отказов.

(iii) Возможность ошибок в технических требованиях, конструкции и реализации.

(iv) Влияние обоснованно предвидимых ошибок экипажа после возникновения отказа или отказного состояния.

(v) Последствия обоснованно предвидимых ошибок при выполнении действий по техническому обслуживанию.

(vi) Предупреждающие сигналы для экипажа, требуемые корректирующие действия и возможность распознавания отказов.

(vii) Результирующие последствия для самолета и находящихся на борту людей с учетом этапа полета, эксплуатационных условий и параметров окружающей среды.

(2) *Планирование.* Данный РЦ представляет руководство по методам обеспечения целей безопасности. Подробная методология, необходимая для обеспечения целей безопасности, будет зависеть от многих факторов, в частности, степени сложности и интеграции систем. Для самолетов с большим числом сложных систем или систем с высокой степенью интеграции может потребоваться разработка плана предполагаемого процесса обеспечения целей безопасности. Этот план должен учитывать следующие аспекты:

(i) Функциональные и физические взаимодействия между системами.

(ii) Определение детализированных способов обеспечения соответствия, которые могут включать использование методов обеспечения гарантии разработки.

(iii) Критерии принятия решения о выполнении плана.

(3) Применимость отраслевых стандартов и руководящих материалов. В настоящее время в промышленности используется большое число различных приемлемых методов, ссылки на которые могут быть приведены или отсутствовать в документах, указанных в выше в п.п. 3(7) и 3(8). Настоящий РЦ не требует обязательного применения указанных документов при определении конкретных процедур и методов обеспечения достижения целей данного Циркуляра. Однако эти документы содержат рекомендательные материалы и методы оценки безопасности систем (System Safety Assessment -SSA). Эти методы, при условии их корректного применения, признаются сертифицирующим органом в качестве приемлемых для демонстрации соответствия параграфу АП-25.1309(b). Кроме того, документ, указанный в п. 3(8), содержит рекомендации по применению специфических инженерных методов (например, Марковского анализа, анализа дерева отказов), которые Заявитель может использовать полностью или частично.

(4) Применение методов гарантии разработки (Development Assurance Methods). Приведенный выше параграф 9b(1)(iii) требует, чтобы любой анализ, необходимый для демонстрации соответствия параграфу АП-25.1309(b), принимал во внимание возможность ошибок в технических требованиях, конструкции и реализации. Ошибки, допущенные во время проектирования и разработки систем, традиционно обнаруживаются и устраняются при проведении исчерпывающих испытаний системы и ее компонентов путем непосредственных инспекций, а также путем других прямых методов верификации, способных дать полную оценку характеристик системы. Эти прямые методы по-прежнему могут подходить для простых систем, которые выполняют ограниченное число функций и которые не являются глубоко интегрированными с другими системами самолета. Для более сложных или интегрированных систем исчерпывающие испытания могут быть либо невозможны, поскольку все состояния системы не могут быть определены, либо невыполнимы из-за большого количества испытаний, которые должны быть выполнены. Для таких типов систем соответствие может быть показано путем использования методов гарантии разработки (Development Assurance). Уровень гарантии разработки должен определяться на основании тяжести потенциально возможных последствий для самолета в случае нарушения функционирования системы или потери ее функции. Руководящие материалы, которые могут быть использованы для обеспечения гарантии разработки, описаны для самолета и его систем в документе, указанном в п. 3(7), а для программного обеспечения - в документах, указанных в п.п. 3(2) и 3(5). Поскольку эти документы были разработаны не одновременно, имеют место некоторые различия в содержащихся в них рекомендациях и терминологии. Существенным различием является указание по использованию архитектуры системы для подтверждения соответствующего уровня гарантии разработки для аппаратной части и программного обеспечения. Следует признать, что учет архитектуры системы для этой цели является приемлемым. Если критерии документа, указанного в п. 3(7), не удовлетворяются конкретным процессом обеспечения гарантии разработки, может потребоваться повысить уровень обеспечения гарантии разработки, используя для этого руководящие материалы документа, указанного в п. 3(5).

(5) Действия экипажа и технического персонала.

(i) В тех случаях, когда анализ устанавливает наличие какой-либо индикации (информации, предоставляемой техническими средствами летному экипажу, экипажу в

кабине или персоналу, выполняющему техническое обслуживание) и/или необходимость выполнения каких-либо действий летным экипажем, экипажем в кабине или персоналом, выполняющим техническое обслуживание, должны быть выполнены следующие действия:

1. Убедиться, что любая предусмотренная индикация действительно обеспечивается системой.

2. Убедиться, что любая предусмотренная индикация будет действительно распознана.

3. Убедиться, что следует обоснованно ожидать успешного и своевременного выполнения любых требуемых действий.

(ii) Указанные проверки должны осуществляться путем консультаций с инженерами, пилотами, бортпроводниками, обслуживающим персоналом и специалистами по человеческому фактору (в зависимости от ситуации) с должным учетом последствий того, что предполагаемые действия будут не выполнены или выполнены неправильно.

(iii) В сложных ситуациях может потребоваться подтверждение результатов проведенного специалистами анализа путем проведения испытаний на тренажере (имитаторе) или летных испытаний. Тем не менее, количественная оценка вероятности ошибок экипажа или обслуживающего персонала в настоящее время не считается возможной. Если считается, что индикация об отказах является распознаваемой, а необходимые действия не приводят к чрезмерному повышению нагрузки на экипаж, вероятность выполнения корректирующего действия для целей настоящего анализа можно принять равной единице. Если необходимые действия не могут быть удовлетворительно выполнены, требуется модифицировать (изменить) задачи и/или системы.

c. *Соответствие требованиям пункта АП-25.1309(c).*

Пункт АП-25.1309(c) требует, чтобы экипажу была обеспечена информация о небезопасных условиях работы систем для того, чтобы дать ему возможность предпринять соответствующее корректирующее действие. Соответствие этому требованию обычно демонстрируется анализом, указанным выше в параграфе 9b(1), который также включает рассмотрение предупреждающих экипаж признаков, потребных корректирующих действий и возможности выявления неисправностей (отказов). Пункт АП-25.1309(c) требует, чтобы была обеспечена аварийная (warning) сигнализация, если требуются немедленные корректирующие действия. Параграф 25.1309(c) также требует, чтобы системы и органы управления ими, включая индикацию и сигнализацию, были спроектированы так, чтобы минимизировать ошибки экипажа, которые могут создать дополнительные опасности.

(1) Требуемая индикация зависит от степени срочности распознавания и корректирующих действий экипажа. Она должна быть в форме:

(i) аварийной сигнализации (warning), если требуются немедленное распознавание и корректирующие или компенсирующие действия экипажа;

(ii) предупреждающей сигнализации (caution), если требуется немедленная осведомленность экипажа и потребуются последующие действия экипажа;

(iii) рекомендации (advisory), если требуется осведомленность экипажа и могут потребоваться последующие действия экипажа;

(iv) сообщения (message), в других случаях.

Дополнительные рекомендации и руководства по обеспечению необходимых характеристик информации (визуальной, звуковой и др.), для указанных выше различных категорий представлены в п. АП-25.1322, документе EASA AMC 25.1322, а также в Дополнении 25F.8.9. «Оборудование внутрикабинной сигнализации» АП-25.

(2) Если мониторинг и информация об отказах осуществляются какой-либо системой, уровень ее надежности должен соответствовать требованиям по безопасности, связанным с функцией системы, для которой обеспечивается такая индикация. Например, если какой-либо отказ при отсутствии сигнализации об этом отказе, и как следствие отсутствии необходимых корректирующих действий, может иметь катастрофические последствия, комбинация этого отказа с отказом сигнализации о нем должна быть практически невероятной. Кроме того, следует оценить нежелательное срабатывание сигнализации (например, мешающие предупреждения). Системы мониторинга и информации об отказах должны использовать эффективные и высоконадежные технологические средства, чтобы максимально увеличить вероятность обнаружения реально возникающих отказов при сведении к минимуму вероятности ложного срабатывания индикации об отказах. Любая индикация должна быть своевременной, очевидной, ясной и недвусмысленной.

(3) В случае, если состояние самолета требует немедленных действий экипажа, экипажу должна быть обеспечена соответствующая аварийная сигнализация, если она не обеспечивается присущими самолету характеристиками. В любом случае, сигнализация об отказах должна привлекать внимание и должна подаваться в такой момент в цепи событий, потенциально имеющих катастрофические последствия, когда возможности самолета и способности экипажа остаются достаточными для эффективного выполнения экипажем соответствующих действий.

(4) Процедуры действий экипажа в случае возникновения аварийной или предупреждающей сигнализации должны быть описаны в одобренном Летном Руководстве (ЛР), или в Дополнении к ЛР, если только такие действия не считаются соответствующими стандартным (нормальным) летным навыкам.

(5) Даже если работа систем или характеристики самолета не подвержены воздействию или подвержены незначительному воздействию в момент отказа, требуется информация экипажу, если эта информация рассматривается как необходимая для выполнения экипажем каких-либо действий или соблюдения каких-либо мер предосторожности. В качестве примеров можно привести изменение конфигурации системы, оповещение об уменьшении запасов безопасности, изменение плана или режима полета, а также выполнение незапланированной посадки для снижения риска возникновения более тяжелого отказного состояния в результате возможных последующих отказов, воздействия условий эксплуатации или внешних условий. Информация также требуется в том случае, если отказ необходимо устранить до следующего полета. Если последствия для работы систем или влияние на характеристики отсутствуют или являются незначительными, выдача информации и/или предупреждающей сигнализации на определенных этапах полета может быть заблокирована, если выполнение экипажем корректирующих действий рассматривается более опасным, чем невыполнение этих действий.

(6) Нежелательно полагаться на выполнение периодических проверок при техническом обслуживании или проверок летным экипажем в качестве единственного средства выявления существенных скрытых отказов. Такие проверки не должны заменять собой реальную и надежную систему мониторинга и информации об отказах. Более подробные указания по использованию периодических проверок, выполняемых при техническом обслуживании, или проверок, выполняемых летным экипажем, даны в параграфе 12 данного РЦ.

(7) Особое внимание должно быть уделено размещению переключателей или других органов управления относительно друг друга таким образом, чтобы минимизировать возможность непреднамеренных ошибочных действий экипажа, особенно при выполнении экстренных действий или в моменты высокой рабочей нагрузки. Иногда может быть необходима дополнительная защита, такая как использование защищенных от непреднамеренного использования переключателей.

9. *ИДЕНТИФИКАЦИЯ ОТКАЗНЫХ СОСТОЯНИЙ И РЕКОМЕНДАЦИИ ПО ОЦЕНКЕ ИХ ПОСЛЕДСТВИЙ.*

а. Идентификация отказных состояний.

Отказные состояния должны идентифицироваться на основании рассмотрения потенциального воздействия отказов на самолет и находящихся на борту людей. При этом анализ должен осуществляться в двух направлениях:

(1) должны быть рассмотрены отказы функций (функциональные отказы) на уровне самолета – отказные состояния, идентифицированные на этом уровне, не зависят от способа реализации функций и архитектуры систем.

(2) должны быть также рассмотрены отказы функций на уровне систем – такие отказные состояния идентифицируются путем изучения способа реализации функций конкретными системами и архитектуры (структуры) систем.

Следует отметить, что отказное состояние может явиться результатом комбинации отказных состояний более низкого уровня. Это обстоятельство требует, чтобы анализ сложных систем, особенно систем с высокой степенью интеграции, выполнялся в высокой степени систематизированными и структурированными методами, чтобы гарантировать, что все существенные (significant) отказные состояния, которые возникают в результате множественных отказов и комбинаций отказных состояний более низкого уровня, должным образом определены и учтены. Соответствующие комбинации отказов и отказные состояния должны быть определены путем исчерпывающей процедуры оценки безопасности, которая включает оценку функциональной опасности (functional hazard assessments - FHA) на уровне самолета и его систем и анализы отказов, вызванных общими причинами (common cause analyses - CCA). Последствия комбинаций отказных состояний отдельных систем, возникающих в результате отказов по общим причинам или каскадного отказа, для самолета могут быть более тяжелыми, чем последствия отказов отдельных систем. Например, отказные состояния, классифицированные сами по себе как незначительные (приводящие к усложнению условий полета) или значительные (приводящие к сложной ситуации), на уровне самолета могут иметь аварийные последствия, когда рассматриваются в комбинации.

b. Идентификация отказных состояний с использованием оценки функциональной опасности (Functional Hazard Assessment).

(1) Прежде чем приступить к детальной оценке отказобезопасности систем, следует выполнить Оценку функциональной опасности (*Functional Hazard Assessement - FHA*) функций, выполняемых на уровне самолета и на уровне его систем, для определения необходимости последующего анализа и его объема. Такая оценка может выполняться с использованием анализа опыта эксплуатации, инженерных и эксплуатационных оценок и/или дедуктивного качественного исследования каждой функции "сверху-вниз". Оценка функциональной опасности (FHA) - это систематическое, всестороннее исследование функций самолета и его систем с целью определения потенциальных незначительных, значительных, аварийных и катастрофических отказных состояний, которые могут возникнуть не только как результат нарушения или потери функции, но и как результат реакции системы на необычные или нештатные внешние факторы.

(2) Каждая функция системы должна быть исследована с учетом влияния на другие функции, выполняемые системой, поскольку потеря или неисправность всех или нескольких функций, выполняемых системой, может привести к более тяжелому отказному состоянию, чем потеря единичной функции. Кроме того, для каждой функции системы должно быть оценено ее влияние на функции, выполняемые другими системами самолета, поскольку потеря или нарушение различных, но взаимосвязанных функций, выполняемых отдельными системами, может оказать неблагоприятное воздействие на степень опасности отказного состояния, установленного для конкретной функции данной системы.

(3) Оценка функциональной опасности (FHA) применяется на ранних стадиях проектирования и корректируется по мере необходимости. Такая оценка используется для определения целей безопасности на уровне самолета и/или на уровне систем, которые должны быть реализованы в предлагаемых архитектурах систем. Ее также следует использовать при определении уровней гарантии разработки систем. Для классификации уровня опасности некоторых систем может быть достаточно только простого рассмотрения Заявителем конструкции системы. Оценка функциональной опасности (FHA) требует квалифицированной инженерной экспертизы и ранней координации работ Заявителя с Полномочным органом по сертификации.

(4) В зависимости от сложности исследуемых функций и связей между функциями и системами могут применяться различные подходы к Оценке функциональной опасности. В тех случаях, когда имеется ясная связь между функциями и системами, а взаимосвязи между системами и, следовательно, функциями являются относительно простыми, может оказаться целесообразным проведение Оценки функциональной опасности для каждой системы по отдельности при условии, что все аспекты взаимодействия систем надлежащим образом учтены и поняты. В тех случаях, когда взаимосвязи систем и функций являются более сложными, при планировании и выполнении Оценки функциональной опасности должен быть принят подход "сверху - вниз", при котором анализ начинается с уровня самолета.

c. *Факторы, которые необходимо учитывать при оценке последствий отказных состояний.*

Требования пункта АП-25.1309(b) направлены на обеспечение методичной и тщательной оценки влияния на безопасность предвидимых (возможных) отказов или других событий, таких как ошибки или внешние воздействия, по отдельности или в сочетании, затрагивающих одну или более функций системы. При этом необходимо учесть взаимодействие этих факторов в рамках отдельной системы, а также других систем, на которые данные факторы могут оказывать влияние. При оценке последствий отказных состояний следует рассмотреть факторы, которые могли бы ослабить или усилить прямые последствия исходного отказного состояния. Некоторые из этих факторов включают условия, являющиеся результатом отказного состояния или связанные с ним, которые могут неблагоприятно воздействовать на возможность экипажа справиться с последствиями отказа. К ним, например, относятся такие факторы как присутствие дыма, воздействие перегрузки, прерывание связи, нарушение герметичности кабины и прочее. При оценке последствий конкретного отказного состояния следует учитывать предоставляемую экипажу информацию об отказе, сложность действий экипажа, а также соответствующую подготовку экипажа. Количество отказных состояний, требующих от экипажа действий, отличающихся от инстинктивных, может повлиять на эффективность действий летного экипажа. В некоторых случаях могут потребоваться дополнительные рекомендации по обучению и подготовке летного экипажа.

(1) Степень опасности отказных состояний должна оцениваться в соответствии со следующими критериями:

(i) Воздействие на самолет, например уменьшение запасов безопасности, ухудшение летных характеристик, потеря способности выполнить некоторые летные операции, уменьшение степени защиты от воздействия окружающей среды, потенциально возможное или вызванное отказом влияние на прочность конструкции.
(ii) Воздействие на членов экипажа, такое как увеличение выше нормальной рабочей нагрузки, которое может снизить возможности экипажа справиться с неблагоприятными эксплуатационными или внешними условиями или последующими отказами.

(iii) Последствия для находящихся на борту людей, т.е. пассажиров и членов экипажа.

(2) При выполнении оценки конструкции систем, отказные состояния могут быть классифицированы в зависимости от тяжести их последствий как не влияющие на безопасность (No Safety Effect), незначительные (усложнения условий полета - Minor), значительные (Major), аварийные (Hazardous), или катастрофические (Catastrophic). Принятые определения этих терминов даны выше в параграфе 7a.

(i) Классификация отказных состояний не зависит от того, является ли рассматриваемая система или функция предметом специальных требований или нормы. Некоторые "обязательные" системы, такие как ответчики УВД, аэронавигационные огни и системы оповещения пассажиров потенциально могут иметь только незначительные (Minor) отказные состояния. С другой стороны, системы, которые не являются "обязательными", такие как системы автоматического управления полетом, потенциально могут иметь значительные (Major), аварийные или катастрофические отказные состояния.

(ii) Независимо от используемых методов оценки, классификация отказных состояний всегда должна выполняться с учетом всех относящихся к ним факторов; таких как характеристики системы, требуемые действия экипажа, летные характеристики, эксплуатационные и внешние факторы. Примерами таких факторов являются характер отказов, влияние на летные характеристики или их ограничения, а также любые требуемые или вероятные действия экипажа. Особенно важно учесть факторы, которые

могут ослабить или усилить последствия отказного состояния. Примером фактора, ослабляющего последствия отказного состояния, может служить сохранение рабочих характеристик идентичных или подобных по действию функций других систем самолета, не подверженных воздействию рассматриваемого отказного состояния. Примерами факторов, ухудшающих последствия отказного состояния, являются не связанные с отказным состоянием условия, которые уменьшают возможность экипажа справиться с отказным состоянием, такие как погода или другие неблагоприятные эксплуатационные или внешние условия.

10. ОЦЕНКА ВЕРОЯТНОСТЕЙ ОТКАЗНЫХ СОСТОЯНИЙ И РЕКОМЕНДАЦИИ ПО ПРОВЕДЕНИЮ АНАЛИЗА.

После идентификации возможных отказных состояний и предварительной оценки степени опасности их последствий Заявитель должен определить способ демонстрации соответствия требованиям пункта АП-25.1309(b). Для доказательства соответствия могут использоваться рассмотрение конструкции системы и ее установки на самолете, анализы, летные испытания, наземные испытания, испытания на тренажере или другой моделирующей установке, а также другие одобренные методы.

а. Оценка вероятностей возникновения отказных состояний.

(1) Каждое отказное состояние в зависимости от вероятности своего возникновения в полете может быть оценено как вероятное (Probable), редкое (маловероятное - Remote), крайне маловероятное (Extremely Remote) или крайне (практически) невероятное (Extremely Improbable). Определение этих терминов приведено выше в параграфе 7. Вероятность возникновения каждого отказного состояния должна находиться в обратной зависимости от степени опасности его последствий (см. параграф 8).

(2) Если система обеспечивает защиту от каких-либо опасных событий (например, пожара в грузовом отсеке, порывов ветра и т.п.), надежность такой системы должна соответствовать требованиям безопасности, которые необходимо обеспечить для отказного состояния, связанного с отказом системы защиты, с учетом вероятностей возникновения таких опасных событий (см. параграф 11g настоящего циркуляра и Приложение 4).

(3) Анализы, выполняемые с целью определения видов отказных состояний и их классификации по степени опасности, являются качественными. С другой стороны, оценка вероятностей возникновения отказных состояний может быть как качественной, так и количественной. Анализ может варьироваться от простого отчета, который интерпретирует результаты испытаний или сравнивает две подобные системы, до детального анализа, который может включать (или не включать) расчетные численные значения вероятностей возникновения отказных состояний. Глубина и объем анализа зависят от функций, выполняемых системой, степени опасности последствий отказных состояний, а также от того, является ли система сложной или нет.

(4) При определении того, является ли система сложной или простой, необходимо руководствоваться инженерной и эксплуатационной оценкой, сделанной опытными специалистами. В некоторых случаях может оказаться полезным сравнение с ранее одобренными подобными системами. Необходимо учесть все характерные атрибуты системы; при этом, сложность программного обеспечения и аппаратной реализации не должна являться доминирующим фактором при определении степени сложности на уровне системы. Конструкция системы может быть весьма сложной, (как например, система спутниковой связи), однако выполняемая ей функция может быть достаточно простой.

b. *Рекомендации по анализу единичных отказов*.

(1) Согласно требованиям п. АП-25.1309(b)(1)(ii), катастрофическое отказное состояние не должно возникать в результате отказа одного компонента, детали или элемента системы. Конструкция системы должна обеспечивать локализацию отказов для того, чтобы ограничить распространение последствий любого единичного отказа и предотвратить возникновение катастрофического отказного состояния. Кроме того, не допускается наличие отказов по общей причине, одновременно затрагивающих как отдельный компонент, деталь или элемент, так и влияющих на обеспечение функции локализации его отказа. Необходимо иметь в виду, что понятие «единичный отказ» включает любой набор отказов, для которых нельзя доказать их независимость друг от друга. В Приложении 1 и документе, указанном в п. 3(8), описаны виды анализа общих причин, которые могут выполняться для гарантии того, что обеспечена независимость отказов. Методы локализации отказов, имеющиеся в распоряжении для обеспечения их независимости, могут включать разделение, разнесение и изоляцию.

2) Обычно следует предполагать, что любой единичный отказ может произойти, однако бывают очевидные случаи, когда Заявитель представляет техническое обоснование того, что с реалистичной и практической точки зрения некоторый конкретный вид отказа не может возникнуть, если только он не будет вызван другим независимым отказным состоянием, которое само по себе является катастрофическим. Будучи определенными и принятыми, такие случаи не должны в дальнейшем рассматриваться как отказы в контексте анализа по п. АП-25.1309.

Например, для просто нагруженных статических элементов (таких как корпус гидроцилиндра и т.п.) любой вид отказа, возникающий вследствие усталостной трещины, может считаться предотвращенным, если показано, что этот элемент удовлетворяет требованиям по допустимости повреждений и усталостной прочности п. АП-25.571.

c. Рекомендации по анализу отказов по общим причинам (Common Cause Failure).

Анализ должен опираться на применение описанной в параграфе 6b концепции отказобезопасной конструкции (fail-safe design) и уделять особое внимание обеспечению эффективного использования методов проектирования, которые в случае единичного отказа или другого события предотвращали бы повреждение или иное неблагоприятное воздействие на более, чем один канал резервированной системы, более чем одну систему из числа систем, выполняющих сходные функции, или любую систему и связанное с ней предохранительное устройство (средство защиты). При рассмотрении таких отказов или других событий, потенциально являющихся общими причинами, следует принять во внимание вторичные или каскадные последствия. Примерами таких отказов или других событий, которые необходимо рассматривать в качестве потенциально возможных общих причин, являются:

- быстрое высвобождение (выброс) энергии из сконцентрированных источников, такое как нелокализованные разрушения вращающихся деталей (иных, чем двигатели или воздушные винты) или баллонов высокого давления,
- перепады давления,
- не являющиеся сами по себе катастрофическими разрушения конструкции,
- отказы систем вентиляции и охлаждения оборудования,

– отключение более чем одной подсистемы или компонента устройствами защиты от перегрева,

– загрязнение жидкостями,

– повреждения в результате локализованных пожаров,

– потеря источников энергии или их линий слива (например, механические повреждения или нарушение соединений),

– чрезмерно высокое электрическое напряжение,

– физическое или косвенное (через окружающую среду) взаимодействие между компонентами систем,

– ошибки или другие события, внешние по отношению к системам или самолету.

При проведении анализа отказов по общим причинам целесообразно использование рекомендаций документа, указанного в п. 3(8).

d. Глубина анализа.

Необходимая глубина анализа отказных состояний определяется классификацией степени опасности их последствий. Ниже даны рекомендации по ожидаемой глубине анализа в зависимости от классификации степени опасности отказных состояний.

(1) Отказные состояния, не влияющие на безопасность.
Для оценки безопасности таких отказных состояний необходимо выполнить Оценку функциональной опасности (Functional Hazard Assessment), а также оценку конструкции и оценку ее установки на самолете для доказательства отсутствия влияния рассматриваемых отказных состояний на выполнение других функций. С позиции требований п. АП-25.1309(b) количественную оценку вероятности возникновения таких отказных состояний можно не выполнять.

(2) Незначительные (Minor) отказные состояния.
Для оценки безопасности таких отказных состояний необходимо выполнить Оценку функциональной опасности (Functional Hazard Assessment) совместно с оценкой конструкции и оценкой ее установки на самолете для доказательства отсутствия влияния рассматриваемых отказных состояний на выполнение других функций. Необходимо также рассмотреть возможные последствия комбинаций данных отказных состояний с другими отказными состояниями, как это отмечено выше в параграфе 10. С позиции требований п. АП-25.1309(b) количественную оценку вероятности возникновения таких отказных состояний можно не выполнять.

(3) Значительные (Major) отказные состояния.

Значительные отказные состояния должны быть маловероятными (Remote).

За исключением случаев, указанных ниже в параграфе 11d(3), для каждого значительного отказного состояния, определенного по результатам Оценки функциональной опасности (FHA), необходимо выполнить детальный анализ безопасности. Такой анализ, как правило, будет представлять собой комбинацию качественных и количественных методов оценки конструкции.

(i) Если система в своих атрибутах, относящихся к оценке безопасности, подобна системам, применявшимся на других типах самолетов, и последствия отказов ожидаются такими же, для доказательства соответствия требованиям п. АП-25.1309(b) может быть

достаточно выполнить оценку конструкции и оценку ее установки в соответствии с рекомендациями Приложения 1, а также подтвердить удовлетворительный опыт эксплуатации анализируемого или аналогичного по конструкции оборудования.

(ii) Для систем, которые не являются сложными, в случае, если подобие конструкции не может быть использовано в качестве основания для установления соответствия, соответствие требованиям п. АП-25.1309(b) может быть продемонстрировано, в частности, посредством качественной оценки. Такая качественная оценка должна показать, что все установленные на уровне системы значительные отказные состояния (Major Failure Conditions) соответствуют результатам оценки функциональной опасности (FHA) и являются маловероятными (Remote), например, системы резервированы.

(iii) Для сложных систем без резервирования необходимо выполнить качественный Анализ видов и последствий отказов (Failure Mode and Effect Analysis - FMEA), а также представить данные по интенсивностям возникновения отказов и провести анализ обеспечения выявления (обнаружения) отказов.

(iv) Анализ резервированных систем обычно считается завершенным, если его результаты свидетельствуют о том, что каналы резервированной системы изолированы друг от друга, и подтверждают приемлемую надежность каждого канала. Для сложных систем, где необходимо обеспечить функциональное резервирование, подтверждение того, что резервирование действительно обеспечено (то есть ни один единичный отказ не оказывает неблагоприятного воздействия на все функциональные каналы системы) требуется проведение качественного Анализа видов отказов и их последствий (FMEA), а также анализа дерева отказов или применения эквивалентных методов.

(4) Аварийные (Hazardous) и катастрофические (Catastrophic) отказные состояния.
Аварийные отказные состояния должны быть крайне маловероятными (Extremely Remote), а катастрофические отказные состояния должны быть крайне (практически) невероятными (Extremely Improbable):

(i) За исключением случаев, указанных ниже в параграфе 11d(4)(ii), для каждого аварийного или катастрофического отказного состояния необходимо выполнить детальный анализ отказобезопасности. Такой анализ, как правило, будет представлять собой комбинацию качественных и количественных методов оценки конструкции систем.

(ii) Для простых и традиционно применяемых систем, может оказаться возможным установить, что возникновение аварийного или катастрофического отказного состояния является соответственно крайне маловероятным или практически невероятным, на основании квалифицированной инженерной экспертизы, используя только качественный анализ. Основанием для такой оценки будут обеспеченная степень резервирования, установленные независимость и изоляция каналов, а также подтвержденные данные по надежности используемой техники. Удовлетворительный опыт эксплуатации подобных систем, широко используемых на многих типах самолетов, может быть достаточным, если установлено близкое сходство в отношении конструкции систем, а также в отношении условий эксплуатации.
(iii) Для сложных систем, применительно к которым может быть строго установлена действительная сходность всех значимых атрибутов, включая атрибуты установки системы на самолете, также может оказаться возможной оценка аварийного или катастрофического отказного состояния как крайне маловероятного или крайне (практически) невероятного, соответственно, на основании квалифицированной инженерной экспертизы, используя только качественный анализ. Для этого требуется доказать высокую степень подобия как в отношении самой конструкции, так и ее применения.

e. Вычисление средней вероятности возникновения отказного состояния на час полета (количественный анализ).

(1) Средняя вероятность на час полета - это нормализованная по времени полета вероятность возникновения отказного состояния в течение полета, которая может рассматриваться как осредненная вероятность по всем возможным полетам парка самолетов сертифицируемого типа. При вычислении средней вероятности отказного состояния на час полета следует учитывать:
(i) среднюю продолжительность полета и средний (типовой) профиль полета для сертифицируемого типа самолетов,
(ii) все комбинации отказов и событий, которые приводят к данному отказному состоянию,
(iii) условные вероятности возникновения отказов и событий, приводящих к отказному состоянию, если определенная последовательность событий является необходимой для того, чтобы вызвать рассматриваемое отказное состояние,
(iv) соответствующее время “риска”, если какое-либо событие является значимым (возможно или играет роль) только на определенных этапах полета,
(v) среднее время существования отказа (exposure time), если какой-либо отказ может существовать в течение многих полетов.

(2) Рекомендации по вычислению средней вероятности возникновения отказного состояния на час полета даны в Приложении 3 настоящего циркуляра.

(3) Зарезервировано

(4) Общепризнано, что по различным причинам данные по интенсивностям отказов компонентов не являются достаточно точными для обеспечения точной оценки вероятностей возникновения отказных состояний. Это ведет к некоторой степени неопределенности в расчетах вероятностей отказных состояний, что показано широкой линией на рисунке 1, и выражением "порядка" в представленных выше описаниях количественных терминов вероятностей. При вычислении расчетных значений вероятностей каждого отказного состояния эта неопределенность должна быть учтена таким образом, чтобы оценки уровня безопасности носили консервативный характер.

f. Интегрированные системы.

Взаимосвязи между системами являются характерной особенностью конструкции современных самолетов. Пункт АП-25.1309(b) требует, чтобы при оценке отказобезопасности функциональные системы самолета были рассмотрены во взаимосвязи и взаимодействии с другими системами.
Важно на ранней стадии проектирования предусмотреть способы демонстрации соответствия для того, чтобы гарантировать, что проектирование может быть поддержано эффективной стратегией оценки безопасности. Особое внимание необходимо уделить следующим аспектам рекомендаций настоящего параграфа РЦ:

(1) планирование предлагаемых способов определения соответствия,

(2) учет при проектировании важной роли архитектуры системы для ограничения влияния и распространения воздействия последствий отказов,

(3) потенциальная возможность отказов по общим причинам, каскадных отказов и их последствий, а также необходимость оценки возможных комбинаций нескольких отказных состояний низкого уровня (например, незначительных и/или значительных),

(4) важность привлечения многопрофильных групп специалистов для определения и классификации существенных отказных состояний,

(5) влияние действий экипажа и процедур технического обслуживания на ограничение влияния и распространения последствий отказов.

Кроме того, строгие и хорошо структурированные процедуры проектирования и разработки играют важную роль в обеспечении оценки безопасности и наглядности результатов демонстрации соответствия. При сертификации высоко интегрированных или сложных систем самолета целесообразно использовать рекомендации документа, указанного в п. 3(7).

g. Условия эксплуатации и факторы, относящиеся к окружающей среде.

Вероятности возникновения дискретных условий, на которые проектируется самолет, например, метеоусловий полета по приборам или условий выполнения захода на посадку по категории III, как правило, должны приниматься равными единице. Однако Приложение 4 содержит допустимые значения вероятностей, которые могут быть приписаны различным эксплуатационным и внешним условиям для их использования, без дальнейшего обоснования, при расчете средних вероятностей на час полета отказных состояний, возникающих в результате множественных независимых отказов. Приложение 4 представлено в качестве справочного рекомендательного материала и не претендует на исчерпывающую полноту или обязательное использование. В настоящее время для некоторых факторов не существует общепринятых стандартных статистических данных, на основании которых могут быть получены значения вероятностей. Однако они включены в Приложение 4 либо для учета в будущем, либо как позиции, по которым Заявитель может предложить свои значения вероятностей, опирающиеся на статистически обоснованные данные или подтверждающий опыт эксплуатации. Заявитель может предложить дополнительные условия или отличные от представленных в Приложении 4 значения вероятностей отдельных факторов при условии, что они основаны на статистически достоверных данных или подтверждаются опытом эксплуатации. Если такие условия предполагается включить в анализ, Заявителю следует получить согласие сертифицирующего Полномочного органа на ранней стадии сертификации. При расчете вероятностей возникновения комбинаций таких случайных условий с отказом системы в обязательном порядке следует удостовериться, что такое условие и отказ системы действительно независимы друг от друга, или, что все возможные зависимости были надлежащим образом учтены.

h. Обоснование предположений, источников данных и аналитических методов.

(1) Любой анализ является настолько точным, насколько точны используемые в нем предположения, данные и аналитические методы. По этой причине для демонстрации соответствия требованиям необходимо идентифицировать и обосновать лежащие в основе анализа предположения, данные и методы анализа, чтобы обеспечить достоверность

заключений, сделанных в ходе анализа. Таким элементам анализа, как виды отказов, последствия отказов, интенсивности отказов, функции распределения вероятностей отказов, времена воздействия (существования) отказов, методы обнаружения отказов, независимость отказов, ограничения аналитических методов, процессов и предположений может быть свойственна изменяемость. Поэтому составной частью анализа должно явиться обоснование предположений, сделанных в отношении указанных выше вопросов. Предположения могут быть подтверждены на основании использования опыта эксплуатации идентичных или подобных систем или компонентов с должным учетом различий в конструкции, рабочих циклах и внешних условиях. В тех случаях, когда невозможно полностью обосновать адекватность анализа безопасности и когда данные или предположения являются критическими для принятия решения о приемлемости какого-либо отказного состояния, должен быть принят дополнительный консерватизм либо в отношении анализа, либо в отношении самой конструкции. В качестве альтернативы, любая неопределенность в данных и предположениях должна быть оценена, чтобы показать нечувствительность выводов анализа к такой неопределенности.

(2) В тех случаях, когда при проектировании и сертификации отсутствуют адекватные подтвержденные данные (например, для новых или неприменявшихся ранее систем), при анализе принимаются дополнительные консервативные допущения. Для получения данных, необходимых для смягчения последствий дополнительного консерватизма, может выполняться после сертификационное отслеживание данных эксплуатации. Полученные таким путем данные могут быть, например, использованы для увеличения интервалов осмотра (проверки) системы при техническом обслуживании.

11. *УЧЕТ АСПЕКТОВ ЛЕТНОЙ ЭКСПЛУАТАЦИИ И ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ.*

Настоящий РЦ рассматривает только те аспекты летной эксплуатации и технического обслуживания, которые напрямую связаны с обеспечением соответствия требованиям пункта АП-25.1309. Другие вопросы летной эксплуатации и технического обслуживания здесь не обсуждаются. Процедуры действий летного экипажа и процедуры технического обслуживания, направленные на обеспечение соответствия этим требованиям, должны быть обоснованными и выполнимыми. При этом количественная оценка ошибок экипажа не считается целесообразной. Поэтому к выполнимым процедурам относятся только те процедуры, на выполнение которых можно с уверенностью рассчитывать, потому что можно реально ожидать, что они будут выполнены корректно в том случае, когда они требуются или запланированы. Кроме того, на основании инженерных и эксплуатационных оценок, сделанных опытными специалистами, можно ожидать обнаружение в процессе летной эксплуатации или выполнения технического обслуживания самолета явных отказов, даже если выявление таких отказов не является основной целью действий по летной эксплуатации или техническому обслуживанию самолета.

а. Действия летного экипажа.

При оценке возможности летного экипажа справиться с отказным состоянием должны быть учтены информация, выдаваемая экипажу, и сложность требуемых действий. Если результаты оценки свидетельствуют о возможности ослабления или устранения потенциального отказного состояния без риска для выполнения летным экипажем других задач, связанных с безопасностью, и без необходимости проявления пилотом исключительного мастерства или приложения чрезмерных усилий, такую возможность можно допустить как при качественной, так и при количественной оценке. Аналогично,

можно предположить правильное выполнение летным экипажем периодических проверок, необходимых для обеспечения соответствия требованиям п. АП-25.1309(b), при условии, что общая рабочая нагрузка на летный экипаж в течение времени, доступного для выполнения проверок, не является чрезмерной и эти проверки не требуют от пилота исключительного мастерства или чрезмерных усилий. Действия летного экипажа по парированию последствий отказных состояний должны быть описаны в утвержденном Летном Руководстве (Airplane Flight Manual – AFM), если только они не отнесены к стандартным летным навыкам.

b. Действия по техническому обслуживанию.

Как при качественной, так и при количественной оценке можно предположить правильное выполнение необходимых задач технического обслуживания. При проектировании и анализе должны быть установлены задачи технического обслуживания, необходимые для обеспечения соответствия требованиям п. АП-25.1309(b). В этих целях могут быть использованы следующие сценарии технического обслуживания:

(1) Отказы, выявляемые экипажем по сигнализации, индикации или другим признакам, будут устранены до следующего полета, или будет установлен максимальный интервал времени до того как потребуются действия по техническому обслуживанию. Если последнее является приемлемым, то анализ должен установить максимально допустимый интервал времени до того, как потребуются действия по техническому обслуживанию. Этот максимально допустимый интервал должен быть отражен в Главном перечне минимально необходимого оборудования (MMEL) или в другой одобряемой эксплуатационной документации.

(2) Скрытые отказы (latent failures) будут выявлены при выполнении соответствующих работ по техническому обслуживанию самолета. Если скрытый отказ в сочетании с другими отказами классифицирован как приводящий к аварийным или катастрофическим последствиям, то должны быть установлены задачи по техническому обслуживанию, являющиеся кандидатами на включения в Сертификационные требования по техническому обслуживанию (CCMR).

c. *Кандидат на включение в сертификационные требования по техническому обслуживанию (CCMR).*

(1) Если в результате анализа отказобезопасности определены скрытые отказы, которые в комбинации с одним или большим числом других отказов или событий, установленных на основании анализа, могут привести к аварийному или катастрофическому отказному состоянию, то для обеспечения соответствия требованиям п. АП-25.1309(b) посредством ограничения времени, в течение которого возможна эксплуатация самолета с такими скрытыми отказами, могут использоваться периодические проверки при техническом обслуживании или проверки летным экипажем. Такие проверки становятся кандидатами на включение в Сертификационные требования к техническому обслуживанию (CCMR). При формировании Сертификационных требований к техническому обслуживанию по результатам анализов отказобезопасности целесообразно использовать рекомендации указанного в п. 3(4) документа АС/АМС 25.19 Сертификационные требования к техническому обслуживанию.

(2) Для определения интервалов проверок следует использовать результаты количественного анализа отказобезопасности систем или соответствующий опыт эксплуатации.

d. Выполнение полетов с неработоспособным оборудованием или функциями.

Заявитель может принять решение о разработке перечня оборудования и функций, которые могут быть неработоспособны перед вылетом самолета при условии выполнения установленных компенсирующих мер, например эксплуатационных или временных ограничений, процедур, выполняемых летным экипажем, или проверок, выполняемых наземным техническим персоналом. При разработке такого перечня, который в дальнейшем будет служить основой для формирования Главного перечня минимально необходимого оборудования (ГПМО, Master Minimum Equipment List, MMEL), наряду с любой другой относящейся к данному вопросу информацией должны учитываться документы, используемые для демонстрации соответствия требованиям пункта АП-25.1309. В процессе разработки ГПМО необходимо руководствоваться инженерной и эксплуатационной оценкой опытных специалистов.

12. ОЦЕНКА МОДИФИКАЦИЙ, ВНЕДРЯЕМЫХ В ТИПОВУЮ КОНСТРУКЦИЮ РАНЕЕ СЕРТИФИЦИРОВАННЫХ САМОЛЕТОВ.

Способы подтверждения сохранения соответствия требованиям пункта АП-25.1309 при внедрении модификаций типовой конструкции ранее сертифицированных самолетов должны определяться для каждого конкретного случая и будут зависеть от применимого сертификационного базиса самолета и степени важности изменений, вносимых в типовую конструкцию. Изменение может быть как простой модификацией, затрагивающей только одну систему, так и значительным изменением типовой конструкции многих систем, возможно включающим использование новых технических решений и технологий. Минимально необходимым действием по демонстрации сохранения соответствия требованиям п. АП-25.1309 для любой модификации является оценка влияния такой модификации на исходную оценку безопасности системы. Результат этой оценки может варьироваться от простого утверждения, что для модифицированной системы по-прежнему применима существующая оценка безопасности системы в соответствии с первоначальными способами подтверждения соответствия, до решения о необходимости применения новых способов подтверждения соответствия, включая разработку плана, упомянутого в параграфе 9b(2).

Если разработчик модификации не является Держателем Сертификата типа для соответствующего ВС, и Держатель Сертификата типа не желает опубликовать или передать принадлежащие ему данные, касающиеся вносимого изменения, Заявителю на получение Дополнения к сертификату типа может потребоваться проведение собственной Оценки безопасности систем (System Safety Assessment)). Дополнительные рекомендации могут быть найдены в параграфе 6 документа, указанного в п. 3(7)).

Рекомендуется, чтобы при внедрении модификаций типовой конструкции ранее сертифицированных самолетов разработчик модификации на раннем этапе работ согласовал с Полномочным органом по сертификации способы подтверждения соответствия модифицированной конструкции требованиям п. АП-25.1309.

ПРИЛОЖЕНИЕ 1. МЕТОДЫ ОЦЕНКИ.

Существуют различные методы оценки причин, степени опасности последствий и вероятностей возникновения отказных состояний. Некоторые из этих методов являются структурированными. В основе различных видов анализа лежат индуктивные или дедуктивные подходы. Вероятностные оценки могут быть качественными или количественными. Описания некоторых видов анализа приведены ниже, а также в Документе, ссылка на который приводится в п. 3(8).

a. *Оценка конструкции (Design Appraisal)* – качественная оценка целостности и безопасности конструкции системы.

b. *Оценка установки (Installation Appraisal)* - качественная оценка целостности и безопасности установки компонентов системы на самолете. Любые отклонения от нормальных, общепринятых в отрасли технологий установки, например, отклонения по зазорам и допускам, подлежат анализу, особенно при оценке изменений, внесенных после ввода в эксплуатацию.

c. *Анализ видов отказов и их последствий (Failure Modes and Effects Analysis – FMEA)* - структурированный индуктивный анализ «снизу-вверх», который используется для оценки влияния каждого возможного отказа элемента или компонента системы на функционирование системы и самолета в целом. Такой анализ позволяет выявить скрытые отказы, а также возможные причины каждого вида отказа системы. Документ, указанный в п. 3(8), содержит методологию и подробные указания, которые могут быть использованы при выполнении такого анализа. Анализ видов отказов и их последствий (FMEA) может быть поэлементным или функционально ориентированным (направленным на анализ отдельных функций). Для съемных блоков и систем, выполненных на основе микросхем, исчерпывающий поэлементный FMEA анализ на базе существующих методик практически не выполним. В связи с этим анализ FMEA может быть скорее функционально ориентированным, чем поэлементным. Функционально ориентированный FMEA анализ может привести к некоторым неопределенностям как в качественном, так и в количественном аспектах, которые могут быть компенсированы более консервативной оценкой, например:

- предположением, что все виды отказов элементов приводят к возникновению рассматриваемых отказных состояний,
- тщательным выбором архитектуры системы,
- учетом опыта применения подобных технических решений.

d. Анализ методом дерева отказов (Fault Tree Analysis) или анализ методом логических схем(*) (Dependence Diagram Analysis) – структурированные дедуктивные анализы «сверху - вниз», которые используются для идентификации условий, видов отказов элементов и событий, ведущих к возникновению каждого определенного отказного состояния. Они являются графическими методами идентификации логических взаимоотношений между каждым конкретным отказным состоянием и первичными отказами элементов или компонентов, других событий или их комбинаций, которые могут привести к его возникновению. В качестве источника данных для определения первичных отказов или других событий могут использоваться результаты анализ видов отказов и их последствий (FMEA).

(*) *Примечание: Эквивалентной формой представления логических схем являются логические уравнения.*

Метод логических схем применяется в тех случаях, когда виды, последовательность и зависимость отказов элементов системы не являются существенными факторами, влияющими на результаты анализа безотказности, а виды отказов системы могут быть определены (или известны) заранее. Этот метод заключается в инженерном анализе причин возникновения определенного вида отказа системы, словесном описании этих причин и последующем формализованном представлении данного описания, т.е. представлении события, состоящего в возникновении в полете отказа определенного вида, как функции алгебры логики от некоторых «простых» событий.

e. *Табличный метод анализа* – метод анализа системы «снизу – вверх», который заключается в составлении таблицы несовместных состояний системы и рассмотрении совокупности выходных характеристик системы при этих состояниях. Этот метод позволяет учесть виды, последовательность возникновения и зависимость отказов элементов. При его использовании обеспечивается полнота выявления видов и причин отказов систем, что является существенным для анализа систем с большим числом выходных характеристик.

f. *Анализ Маркова.* Модель Маркова (цепь) представляет различные состояния системы и зависимости между ними. Состояния могут быть работоспособными или неработоспособными. Переходы из одного состояния в другое являются функцией интенсивностей (частот) возникновения отказов и восстановления. Анализ Маркова может применяться вместо анализа методом дерева отказов или анализа методом логических схем, однако он зачастую приводит к более сложному представлению результатов анализа, особенно в том случае, когда система имеет много возможных состояний. Анализ Маркова рекомендуется применять в тех случаях, когда применение анализа дерева отказов или анализа методом логических схем затруднительно, а именно, в случаях, когда необходимо учитывать сложные переходные состояния систем, которые сложно представить и проанализировать путем классического анализа дерева отказов или анализа методом логических схем.

g.*Анализ общих причин (Common Cause Analysis).* Принятие решения о том, что вероятности возникновения отказных состояний соответствуют заданным требованиям, часто производится на основании оценки множества систем в предположении, что их отказы являются независимыми. По этой причине необходимо признать, что такая независимость может не существовать на практике и требуется проведение специальных исследований, чтобы подтвердить, что независимость отказов может быть обеспечена либо считаться приемлемой.

Анализ общих причин подразделяется на три области исследований:

(1) *Зональный анализ безопасности (Zonal Safety Analysis).* Целью данного анализа является обеспечение гарантии того, что установка оборудования в каждой зоне самолета выполнена в соответствии с требованиями обеспечения безопасности в части стандартов проектирования и установки, исключения помех между системами и ошибок техобслуживания.

В зонах самолета, где в непосредственной близости друг от друга установлено много систем и компонентов, необходимо убедиться, что в ходе зонального анализа будут идентифицированы любые отказы или нарушения функционирования, которые сами по себе не ведут к существенным последствиям, однако могут привести к более серьезным

последствиям в случае их неблагоприятного влияния на другие соседние системы или компоненты.

(2) Анализ специфических рисков (Particular Risk Analysis). Специфические риски определяются как события или воздействия, находящиеся вне рассматриваемых систем. Примерами таких событий (воздействий) являются пожар, утечки жидкостей, столкновение с птицей, разрыв пневматика, воздействие электромагнитных полей высокой интенсивности (HIRF), удар молнии, нелокализованные разрушения вращающихся механизмов, обладающих высокой энергией, и т.д. Каждый из таких рисков должен быть проанализирован с тем, чтобы установить и зарегистрировать одновременные или каскадные последствия или воздействия, которые могут привести к нарушению независимости.

(3) Анализ общих видов (Common Mode Analysis). Данный вид анализа производится с целью подтверждения предполагаемой независимости событий, рассматриваемых в комбинации применительно к конкретному отказному состоянию. Необходимо учитывать влияние ошибок в технических условиях, проектировании, реализации, установке, техобслуживании и изготовлении, воздействие факторов окружающей среды, отличных от уже учтенных в ходе анализа специфических рисков, а также отказы компонентов системы.

g. *Процесс оценки безопасности (Safety Assessment Process).* Общая информация относительно процесса оценки безопасности представлена в Приложении 2.

ПРИЛОЖЕНИЕ 2. ОБЗОР ПРОЦЕССА ОЦЕНКИ БЕЗОПАСНОСТИ

При демонстрации соответствия требованиям пункта АП-25.1309(b) следует методично и систематически руководствоваться указаниями, приведенными в настоящем рекомендательном циркуляре. Это позволит гарантировать, что процесс анализа и сделанные по его результатам выводы будут ясны и понятны. Рекомендации, приведенные в данном Приложении, не являются контрольным перечнем сертификационных проверок и не охватывают всю информацию, представленную в настоящем РЦ. Не устанавливается обязательных требований об их применении или об их принятии уполномоченным органом, будь то полностью или частично, при демонстрации соответствия какому-либо нормативному требованию. Они приводятся исключительно с целью оказания помощи путем иллюстрации систематического подхода к оценке безопасности, углубления понимания и связи на основании обобщения информации, приведенной в настоящем РЦ, а также представления некоторых рекомендаций по документированию результатов анализа. Более подробные рекомендации могут быть найдены в документе, указанном в п. 3(8) настоящего РЦ. В документе, указанном в п. 3(7), приведены дополнительные руководства по связи процесса оценки безопасности и процесса разработки систем.

a. Определите систему и ее интерфейсы (устройства сопряжения), идентифицируйте функции, которые должна выполнять система. Определите, является ли система сложной, или сходной с системами, применяющимися на других самолетах. Если оценке подлежат многочисленные системы и функции, рассмотрите взаимосвязи и взаимовлияние между различными системами и функциями.

b. Идентифицируйте отказные состояния и классифицируйте их. В этом процессе должны принимать участие все соответствующие конструкторские подразделения, такие как ответственные за проектирование систем, прочность конструкции, силовую установку, а также летные испытания. Такая идентификация и классификация отказных состояний может быть осуществлена путем выполнения оценки функциональной опасности (Functional Hazard Assessment), которая обычно базируется на одном из следующих методов:

(1) Если система не является сложной, а ее конструкция и характеристики сходны с соответствующими атрибутами систем, применяемых на других самолетах, идентификация и классификация отказных состояний системы могут быть выполнены на основании оценок конструкции и установки (Design and Installation Appraisals), а также опыта эксплуатации сравнимых ранее одобренных систем.

(2) Если система является сложной, необходимо на систематической основе определить последствия (влияние на безопасность самолета и находящихся на борту людей) любых возможных отказов, рассматривая их как индивидуально, так и в комбинации с другими отказами или событиями.

c. Выберите способы определения соответствия требованиям пункта АП-25.1309(b). Глубина и объем анализа зависят от функций, выполняемых системой, степени опасности отказных состояний системы, а также от того, является ли система сложной или простой. Для анализа значительных (Major) отказных состояний приемлемыми могут оказаться инженерная и эксплуатационная оценки системы опытными специалистами, оценки конструкции и установки, а также использование сравнимых данных об опыте эксплуатации сходных систем, которые могут применяться как по отдельности, так и в сочетании с методами качественного анализа или с применением методов

количественного анализа. Для аварийных или катастрофических отказных состояний необходима тщательная оценка безопасности с применением структурированных методов количественного анализа (метод логических схем, метод деревьев отказов или эквивалентных). Выбор методов определения соответствия должен быть предварительно согласован с сертифицирующим органом.

d. Проведите анализ и представьте данные, которые по согласованию с сертифицирующим органом являются приемлемыми для демонстрации соответствия. Типичный анализ должен включать следующую информацию в объеме, необходимом для демонстрации соответствия:

(1) Утвержденный перечень функций, выполняемых системой, границ и интерфейсов системы.

(2) Перечень компонентов (узлов и оборудования), из которых состоит система, включая спецификации их характеристик или стандарты проектирования и уровни гарантии разработки (Development Assurance Level – DAL), если это применимо. Этот перечень может ссылаться на другие документы, например квалификационные требования, спецификации изготовителя, государственные или отраслевые стандарты и т.д.

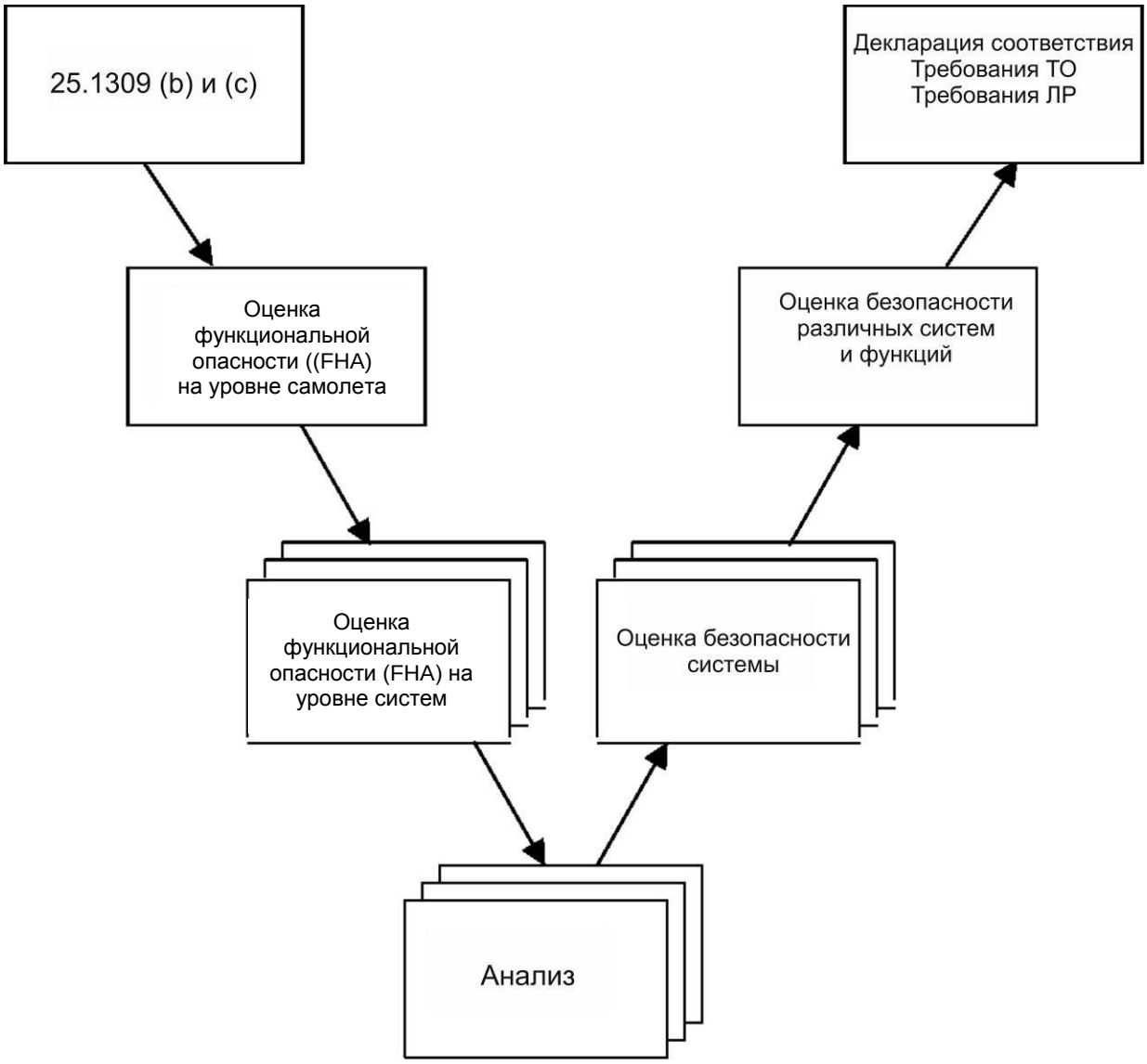
(3) Заключения, включая перечни отказных состояний с их классификацией по степени опасности и вероятностями возникновения (выраженными в качественной форме или количественными значениями), которые демонстрируют соответствие системы требованиям п. АП-25.1309(b).

(4) Отчетную документацию, обосновывающую правильность и полноту проведенного анализа, а также позволяющую проследить последовательность работ и их результатов вплоть до сделанных заключений. Данная документация должна включать обоснования для классификации степени опасности каждого отказного состояния (например, инженерный анализ или наземные, летные испытания или испытания на пилотажном стенде или ином имитаторе). Она также должна содержать описание конструктивных мер, предпринятых для предотвращения возникновения отказов по общим причинам, содержать все необходимые данные, например, данные по частоте (интенсивности) отказов компонентов, источниках этих данных и их применимости, обоснование всех сделанных предположений, а также определять любые требуемые действия летного экипажа или служб по наземному техническому обслуживанию, включая всех кандидатов на сертификационные требования к техническому обслуживанию (CCMR).

e. Выполните оценку анализов и заключений, сделанных по результатам оценки безопасности различных систем, с целью обеспечения соответствия требованиям к отказобезопасности на уровне самолета.

f. Оформите заключение о соответствии требованиям Норм, требования к техническому обслуживанию (CMR) и процедуры действий экипажа для включения в Летное Руководство.

Рисунок А2-1 Общая схема процесса оценки



ПРИЛОЖЕНИЕ 3. РАСЧЕТ СРЕДНЕЙ ВЕРОЯТНОСТИ ОТКАЗНОГО СОСТОЯНИЯ НА ЛЕТНЫЙ ЧАС.

В настоящем приложении представлены рекомендации по расчету «средней вероятности возникновения отказного состояния на час полета» для обеспечения сравнения этой вероятности с количественными критериями допустимых вероятностей возникновения отказных состояний различной степени опасности.

Процесс расчета средней вероятности возникновения отказного состояния на час полета может быть разделен на четыре этапа и основывается на предположении, что жизненный цикл самолета представляет собой последовательность так называемых «средних полетов».

Этап 1: Определение «среднего полета».

Этап 2: Расчет вероятности возникновения отказного состояния для некоторого «среднего полета».

Этап 3: Расчет средней вероятности возникновения отказного состояния на полет.

Этап 4: Расчет «средней вероятности возникновения отказного состояния на час полета».

a. *Определение среднего полета.* Расчет «средней вероятности на час полета должен основываться на определении «среднего полета». Следует оценить продолжительность среднего полета и профиль среднего полета для парка самолетов сертифицируемого типа. Продолжительность «среднего полета» следует определять на основании прогнозов и опыта эксплуатации подобных типов самолетов. Продолжительность «среднего полета» должна отражать верхнюю (оптимистическую) оценку ожидаемого общего налета в летных часах, деленную на общее число полетов в течение всего срока эксплуатации самолета данного типа. Профиль «среднего полета» должен основываться на расчетном эксплуатационном весе и расчетных летно-технических характеристиках среднего самолета при полете средней продолжительности в стандартной атмосфере ИКАО. Продолжительность каждого этапа среднего полета (например, взлета, набора высоты, крейсерского полета, снижения, захода на посадку и посадки) должна определяться на основании профиля среднего полета. В случаях, когда это необходимо, следует учесть среднее время руления перед взлетом и после посадки для среднего аэропорта и прибавить его ко времени среднего полета. Продолжительность и профиль «среднего полета» необходимо использовать в качестве основания для определения средних вероятностей на час полета при количественной оценке безопасности.

Примечание: продолжительность и профиль «среднего полета» устанавливаются Разработчиком самолета.

b. *Расчет вероятности возникновения отказного состояния для некоторого «среднего полета»*. Вероятность возникновения отказного состояния в течение «среднего полета» $P_{полет}$ (Отказное состояние) должна определяться с помощью структурированных методов (например, методов, описанных в Документе, ссылка на который приведена в п. 3(8)) с учетом всех значимых элементов (например, комбинаций отказов и событий), которые способствуют возникновению рассматриваемого отказного состояния. Необходимо учесть следующее:

(1) Интенсивности отказов отдельных деталей, компонентов и узлов, используемые при расчете средней вероятности на летный час, должны представлять собой установившиеся постоянные значения интенсивностей отказов после периода начальной приработки и до

выработки ресурса (износа). Эти значения должны учитывать все причины отказа (эксплуатационные, связанные с внешними факторами и т.д.). При наличии соответствующих данных следует учитывать опыт эксплуатации идентичных или сходных компонентов в идентичных или сходных условиях окружающей среды.

(2) Если отказ может иметь место только на определенных этапах полета, расчет должен основываться на вероятности отказа в течение соответствующего времени риска его возникновения.

(3) Если один или большее число элементов (компонентов) системы могут находиться в состоянии отказа в течение нескольких полетов (латентные, непроявившиеся или скрытые отказы), при расчете вероятностей отказных состояний необходимо учитывать соответствующие времена возможного нахождения таких элементов в состоянии отказа (например, интервалы времени между проведением проверок функционирования/инспекций и восстановления работоспособности соответствующего элемента). В таких случаях вероятность возникновения отказного состояния увеличивается с увеличением периода латентности (числа полетов, в которых могут существовать скрытые отказы).

(4) Если интенсивность отказа какого-либо элемента изменяется в течение различных этапов полета, при расчете следует учитывать изменение значения интенсивности отказа такого элемента и соответствующие приращения времени таким образом, чтобы установить вероятность возникновения отказного состояния в «среднем полете».

Предположим, что «средний полет» может быть разделен на n этапов (фаз) (фаза 1, фаза 2, …., фаза n). Пусть T_n – продолжительность «среднего полета». T_j – продолжительность фазы j, а t_j – момент перехода между фазами j и $j+1$, $j=1, ..., n$. То есть:

$$T_n = \sum T_j \text{ и } T_j = t_j - t_{j-1}, \qquad j = 1, ..., n$$

Обозначим $\lambda_j(t)$ – функция интенсивности отказа элемента в течение этапа (фазы) j, то есть для интервала времени $t \in [t_{j-1}, t_j]$

Примечание: Для некоторого этапа (фазы) полета j интенсивность отказа $\lambda_j(t)$ может быть равна 0 для всего интервала времени $t \in [t_{j-1}, t_j]$.

Пусть

$P_{полет}\ (отказ)$ – вероятность отказа (нахождения в состоянии неработоспособности) какого-либо элемента системы в течение некоторого одного полета;

$P_{фаза\ j}\ (отказ)$ – вероятность отказа этого элемента на j-й фазе (j-м этапе) полета.

Возможны два случая:

(i) Работоспособность элемента проверяется перед началом рассматриваемого полета. Тогда

$$P_{полет}\ (отказ) = \sum_{j=1}^{n} P_{фаза\ j}\ (отказ) = \sum_{j=1}^{n} P\ (отказ \mid t \in [t_{j-1}, t_j]) = 1 - \prod_{j=1}^{n} \exp\left(\int_{j-1}^{j} \lambda_j(x)dx \right)$$

(ii) Состояние элемента перед началом рассматриваемого полета неизвестно. Тогда

$$P_{полет}\ (отказ) = P_{до\ полета}\ (отказ) + (1 - P_{до\ полета}\ (отказ)) \cdot (1 - \prod_{j=1}^{n} \exp\left(\int_{j-1}^{j} \lambda_j(x)dx \right)),$$

где $P_{до\ полета}\ (отказ)$- вероятность того, что отказ соответствующего элемента произошел до рассматриваемого полета.

(5) В тех случаях, когда рассматриваемые последствия (отказное состояние) наступают только тогда, когда отказы возникают в определенном порядке, при расчете вероятности возникновения отказного состояния необходимо учитывать вероятность возникновения отказов в последовательности, необходимой для его возникновения.

c. Вычисление средней вероятности возникновения отказного состояния на полет. Следующим этапом является расчет средней вероятности возникновения отказного состояния на полет. То есть должны быть рассчитаны вероятности возникновения рассматриваемого отказного состояния для каждого полета (которые могут принимать различные значения, несмотря на то, что все полеты представляют собой «средний полет») в течение соответствующего времени (например, наименьшего общего кратного значений времени, в течение которого отказ может существовать, или срока службы самолета), затем эти вероятности должны быть просуммированы и полученная сумма разделена на общее число полетов в течение этого периода. Принципы расчета описаны ниже; а более подробное описание приведено в Документе, ссылка на который приведена в п. 3(8).

$$\mathrm{P}_{\textit{средняя на полет}}(\text{отказное состояние}) = \frac{1}{N}\sum_{k=1}^{N}\mathrm{P}_{\textit{полет k}}(\text{отказное состояние})$$

где N – общее количество полетов в течение соответствующего времени, а $\mathrm{P}_{\textit{полет k}}$ – вероятность возникновения отказного состояния в k-м полете.

d. Вычисление средней вероятности возникновения отказного состояния на час полета. Чтобы рассчитать среднюю вероятность отказного состояния на час полета вычисленное значение средней вероятности возникновения отказного состояния на полет должно быть нормализовано путем его деления на продолжительность «среднего полета» $T_{\textit{полета}}$. Это количественное значение вероятности должно быть соотнесено с классификацией данного отказного состояния по степени опасности его последствий, установленных на основании анализа функциональной опасности (FHA), выполненных анализов и испытаний. Такое сравнение позволит установить, удовлетворяет ли данная вероятность требованиям безопасности для анализируемого отказного состояния.

$$\mathrm{P}_{\textit{средняя на час полета}}(\text{отказное состояние}) = \frac{1}{T_{\textit{полета}}} P_{\textit{средняя на полет}}(\text{отказное состояние})$$

ПРИЛОЖЕНИЕ 4 ПРИНЯТЫЕ ВЕРОЯТНОСТИ СОБЫТИЙ, ВНЕШНИХ УСЛОВИЙ И ЭКСПЛУАТАЦИОННЫХ ФАКТОРОВ.

При количественном анализе безопасности могут использоваться следующие значения вероятности возникновения условий окружающей среды и эксплуатационных факторов:

Факторы окружающей среды

Условие	Модель или другое основание	Вероятность
Нормальное обледенение (следы льдообразования, легкое, умеренное обледенение)	Приложение С к АП-25	1
Встречный ветер >25 узлов (12,5 м/с) во время взлета и посадки	АС 120-28 CS-AWO	10^{-2} на полет
Попутный ветер >10 узлов (5 м/с) во время взлета и посадки	АС 120-28 CS-AWO	10^{-2} на полет
Боковой ветер >20 узлов (10 м/с) во время взлета и посадки	АС 120-28 CS-AWO	10^{-2} на полет
Предельные расчетные условия дискретного порыва ветра и турбулентности	АП-25.341/CS 25.341	10^{-5} на летный час
Удар молнии		Нет общепринятых стандартных данных
Воздействие HIRF (электромагнитных полей высокой интенсивности)		Нет общепринятых стандартных данных

Конфигурации самолета

Конфигурация	Модель или другое основание	Вероятность
Центровка	Стандартная отраслевая практика	Принимается 1 во всем одобренном диапазоне центровок
Посадочный и взлетный вес/масса	Стандартная отраслевая практика	Принимается 1 во всем одобренном диапазоне весов/масс

Условия полета

Условие	Модель или другое основание	Вероятность
Условия полета, требующие выдачи сигнализации о приближении к сваливанию.	Предположение	10^{-2} на полет
Условия полета, приводящие к сваливанию	Предположение	10^{-5} на полет
Превышение V_{MO}/M_{MO}	Предположение	10^{-2} на полет
Условия полета, соответствующие перегрузке, равной или более 1,5 g		Нет общепринятых стандартных данных
Условия полета, соответствующие перегрузке, равной или менее 0 g		Нет общепринятых стандартных данных

События, связанные с изменением плана (режима) полета

Событие.	Модель или другое основание	Вероятность
Любой прерванный взлет по причине, не связанной с отказом двигателя	Анализ опыта эксплуатации в РФ	10^{-4} на полет
Прерванный взлет с большой кинетической энергией	Анализ опыта эксплуатации в РФ	10^{-5} на полет
Необходимость аварийного слива топлива		Нет общепринятых стандартных данных
Уход на второй круг		$5 \cdot 10^{-2}$

Прочие события

Событие.	Модель или другое основание	Вероятность
Пожар в туалете		Нет общепринятых стандартных данных
Пожар в багажно-грузовом отсеке		10^{-7} на час полета
Пожар в отсеке вспомогательной силовой установки		10^{-5} на полет
Пожар двигателя		10^{-5} на час полета
Разгерметизация кабины, при которой требуется подача пассажирам кислорода		10^{-5} на час полета

Примечания:

1. Если в ячейке таблицы указано "Нет общепринятых стандартных данных", Заявитель должен предоставить обоснованное значение вероятности такого события, если при анализе используется значение вероятности меньше 1.

2. Значения вероятностей событий, приведенные в настоящем Приложении, признаны приемлемыми для использования в контексте количественного анализа безопасности, выполняемого для демонстрации соответствия требованиям п. АП-25.1309. Они не всегда могут быть пригодными для использования в контексте других требований. Заявитель имеет право использовать другие значения вероятностей событий, представив соответствующее обоснование.