

РУКОВОДСТВО P-4754A

**МЕЖГОСУДАРСТВЕННЫЙ АВИАЦИОННЫЙ КОМИТЕТ
АВИАЦИОННЫЙ РЕГИСТР**

**РУКОВОДСТВО
Р-4754А**
**по разработке воздушных судов
гражданской авиации и систем**

**Введено в действие с 22.08.16
Директивным письмом № 02-2016
Авиарегистра МАК от 22 августа 2016 г.**

2016

ПРЕДИСЛОВИЕ К РУССКОМУ ИЗДАНИЮ

В последние годы в США и Европе идет активная работа по совершенствованию политики и практики проектирования и сертификации воздушных судов (ВС) гражданской авиации. Это вызвано тем, что современные и перспективные авиационные системы становятся все более сложными, а традиционные методы их сертификации не устраивают ни авиационные, ни сертификационные власти. Отсутствие русскоязычных регламентирующих документов по проектированию и сертификации бортовых систем, гармонизированных с западными, затрудняет сертификацию отечественной авиационной техники, а также взаимопонимание ее разработчиков с западными сертификационными властями при продвижении своей продукции на мировой рынок.

Данное руководство совместно с документами КТ-178 (русскоязычная версия документов DO-178/ED-12), КТ-254 (русскоязычная версия документов DO-254/ED-80) и P-297 (русскоязычная версия документов DO-297/ED-124) направлено на преодоление упомянутых трудностей. Документ P-4754А подготовлен в рамках созданной Авиационным регистром МАК рабочей группы с привлечением специалистов ведущих предприятий и организаций отечественной авиационной отрасли.

Настоящее руководство, разработанное в интересах дальнейшего распространения системного подхода на уровень ВС при создании перспективных образцов отечественной авиационной техники, можно считать развитием предыдущей версии документа, P-4754 AP МАК. Известно, что англоязычная версия руководства P-4761 по методам оценки безопасности в настоящее время также совершенствуется в интересах распространения принципов оценки безопасности на уровень ВС, большего учета «человеческого фактора», конкретизации некоторых положений, а также в других направлениях. Поэтому можно рассчитывать, что после опубликования настоящего варианта руководства P-4754А начнется работа по дальнейшему созданию соответствующего ему руководства P-4761А на базе ARP4761А/ED-135 и других документов, в интересах обеспечения отечественных разработчиков передовыми методами и подходами к проектированию и сертификации авиационной техники.

Текст документа близок к оригиналу, иногда даже не в полном соответствии с принятой в отечественной авиационной отрасли терминологии. При необходимости трактовки используемой в руководстве терминологии следует обращаться к оригинальным текстам SAE/ARP4754А и EUROCAE/ED-79А и/или к сертификационным властям, а также к специалистам, участвующим в подготовке данного документа.

Сделанные редактором вставки по тексту выделены *курсивом*.

ПОЯСНЕНИЕ

Настоящий документ включает обновленные и расширенные инструктивные материалы для процессов разработки воздушных судов гражданской авиации и систем.

СОДЕРЖАНИЕ

1 ОБЛАСТЬ ПРИМЕНЕНИЯ	9
1.1 Назначение документа	10
1.2 История разработки документа	11
2 ССЫЛКИ	13
2.1 Используемые документы	13
2.1.1 Публикации SAE	13
2.1.2 Публикации FAA	13
2.1.3 Публикации EASA	13
2.1.4 Публикации RTCA	14
2.1.5 Публикации EUROCAE	14
2.1.6 Публикации AP MAK	14
2.2 Определения	15
2.3 Аббревиатуры и сокращения	19
3 ПЛАНИРОВАНИЕ РАЗРАБОТКИ	21
3.1 Процесс планирования	21
3.2 Критерии перехода	23
3.2.1 Отклонения от планов	23
4 ПРОЦЕСС РАЗРАБОТКИ ВОЗДУШНОГО СУДНА И СИСТЕМ	24
4.1 Процесс концептуальной разработки воздушного судна/системы	24
4.1.1 Гарантия разработки	26
4.1.2 Введение в процесс гарантии разработки	26
4.1.3 Введение в иерархическую структуру требований безопасности, полученных в результате анализа безопасности	27
4.1.4 Определение функций на уровне воздушного судна, требований к функциям и интерфейсов функций	29
4.1.5 Распределение функций воздушного судна по системам	29
4.1.6 Разработка системной архитектуры	29
4.1.7 Распределение системных требований по объектам	29
4.1.8 Реализация системы	29
4.2 Разработка функций воздушного судна	30
4.3 Распределение функций воздушного судна по системам	32
4.4 Разработка архитектуры системы	32
4.5 Распределение системных требований по элементам	33
4.6 Реализация системы	33
4.6.1 Информационный поток из процессов ЖЦ системы в процессы ЖЦ элемента и обратно	33
4.6.2 Разработка и сборка аппаратуры и программного обеспечения	35
4.6.3 Интеграция аппаратуры и программного обеспечения	35
4.6.4 Интеграция систем на уровне воздушного судна	35
5 ИНТЕГРАЛЬНЫЕ ПРОЦЕССЫ	37
5.1 Оценка безопасности	37

5.1.1	Оценки функциональной опасности.....	39
5.1.2	Предварительная оценка безопасности воздушного судна/системы.....	39
5.1.3	Оценка безопасности воздушного судна/системы.....	40
5.1.4	Анализ общих причин отказа.....	41
5.1.5	План-программа безопасности.....	42
5.1.6	Относящиеся к безопасности задачи летной эксплуатации и технического обслуживания.....	42
5.1.7	Связь с эксплуатационной безопасностью.....	42
5.2	Назначение уровня гарантии разработки.....	43
5.2.1	Основные принципы назначения уровня гарантии разработки.....	43
5.2.2	Уровни гарантии разработки функции (FDAL) и элемента (IDAL).....	44
5.2.3	Подробное руководство по назначению уровней FDAL и IDAL.....	45
5.2.4	Назначение уровня FDAL с учетом внешних событий.....	57
5.3	Формирование требований.....	58
5.3.1	Виды требований.....	59
5.3.2	Получение требований к безопасности из результатов оценки безопасности.....	61
5.3.3	Формирование требований к техническому обслуживанию в период эксплуатации.....	62
5.4	Валидация требований.....	62
5.4.1	Цели процесса.....	63
5.4.2	Модель процесса валидации.....	63
5.4.3	Проверки корректности.....	67
5.4.4	Проверки полноты.....	68
5.4.5	Строгость валидации.....	70
5.4.6	Методы валидации.....	70
5.4.7	Данные валидации.....	73
5.5	Верификация реализации.....	74
5.5.1	Цели процесса верификации.....	74
5.5.2	Модель процесса верификации.....	74
5.5.3	Строгость верификации.....	75
5.5.4	Планирование верификации.....	75
5.5.5	Методы верификации.....	76
5.5.6	Данные верификации.....	79
5.6	Управление конфигурацией.....	80
5.6.1	Цели процесса управления конфигурацией.....	81
5.6.2	Мероприятия процесса управления конфигурацией.....	82
5.7	Гарантия процесса.....	84
5.7.1	Цели процесса.....	84
5.7.2	План гарантии процесса.....	85
5.7.3	Рассмотрения планов проекта.....	85
5.7.4	Свидетельства гарантии процесса.....	85
5.8	Координация с сертифицирующим органом.....	85
5.8.1	Планирование сертификации.....	86
5.8.2	Согласование предлагаемых средств подтверждения соответствия.....	86

5.8.3 Доказательство соответствия.....	86
5.8.4 Данные сертификации.....	87
6 МОДИФИКАЦИИ ВОЗДУШНОГО СУДНА ИЛИ СИСТЕМ.....	90
6.1 Обзор процесса модификации	91
6.2 Процесс управления модификацией.....	91
6.3 Анализ влияния модификации.....	91
6.4 Классификация и управление модификацией	92
6.5 Свидетельство приемлемости модификации	93
6.5.1 Использование опыта эксплуатации.....	93
6.6 Виды модификаций.....	94
6.6.1 Добавление новой функции на уровне ВС	94
6.6.2 Замена элемента или системы на существующем воздушном судне.....	95
6.6.3 Адаптация существующего элемента или системы для другого типа ВС	96
6.6.4 Модификация элемента или системы без добавления функций.....	97
6.6.5 Введение в процесс получения Дополнительного сертификата типа	98
7 ПРИМЕЧАНИЯ.....	100
ПРИЛОЖЕНИЕ А ЦЕЛИ И ВЫХОДНЫЕ ДАННЫЕ ПРОЦЕССОВ	101
ПРИЛОЖЕНИЕ В ПЛАН-ПРОГРАММА БЕЗОПАСНОСТИ.....	110
ПРИЛОЖЕНИЕ С ПРИМЕР ПРОЦЕССА НАЗНАЧЕНИЯ FDAL/IDAL	125
ПРИЛОЖЕНИЕ D Не применяется.....	131
Рисунок 1. Руководящие документы по этапам разработки и эксплуатации.....	10
Рисунок 2. Процесс планирования.....	22
Рисунок 3. ЖЦ разработки	24
Рисунок 4. Модель процесса разработки ВС или системы	25
Рисунок 5. Интеграция между процессом оценки безопасности и процессом разработки ..	28
Рисунок 6. Процесс реализации функции ВС	31
Рисунок 7. Схема процесса оценки безопасности.....	38
Рисунок 8. Процесс назначения FDAL/IDAL	45
Рисунок 9. Независимость функции и независимость разработки элемента	52
Рисунок 10. Независимость разработки нескольких функций для одного и того же отказного состояния.....	55
Рисунок 11. Назначение уровня гарантии разработки функции защиты в зависимости от вероятности внешнего события.....	58
Рисунок 12. Модель процесса валидации	64
Рисунок 13. Модель процесса верификации	75
Рисунок 14. Модель процесса управления конфигурацией	82
Таблица 1. Элементы планирования разработки	23
Таблица 2. Назначение FDAL для функции верхнего уровня	46
Таблица 3. Назначение уровней гарантии разработки элементам группы функциональных отказов (FFS)	50

Таблица 4.	Пример назначения уровня гарантии при независимости разработки нескольких функций одного и того же отказного состояния FC	53
Таблица 5.	Пример назначения уровней гарантии при зависимости разработки элементов нескольких функций одного и того же отказного состояния	56
Таблица 6.	Данные и методы валидации	72
Таблица 7.	Данные и методы верификации	79
Таблица 8.	Мероприятия УК по категориям контроля.....	84
Таблица 9.	Перекрестные ссылки данных сертификации	87

1 ОБЛАСТЬ ПРИМЕНЕНИЯ

В настоящем документе рассматривается разработка систем ВС с учетом общих условий эксплуатации и функций ВС. Речь идет о валидации требований, верификации и гарантии качества разрабатываемого продукта. В нем приводится порядок обеспечения соответствия требованиям нормативных документов. Документ служит также вспомогательным средством при разработке и применении организациями собственных внутренних стандартов с учетом содержащихся здесь инструктивных материалов.

Приведенные в настоящем документе инструктивные материалы разработаны применительно к Части 25 из Раздела 14 Свода нормативных актов федеральных органов власти США (14CFR), Сертификационной спецификации (CS) CS-25 Европейского агентства авиационной безопасности (EASA) и Части 25 Авиационных Правил AP МАК. Они также могут быть применены в отношении других нормативных документов, в частности, Частей 23, 27, 29, 33 и 35 (CS-23, CS-27, CS-29, CS-E, CS-P).

Настоящий документ описывает цикл разработки ВС и систем, реализующих функции ВС. В документ не включены специфические подробности разработки программного обеспечения (ПО) и аппаратуры, процессов оценки безопасности, мероприятий по обеспечению эксплуатационной безопасности и проектирования конструкции ВС; документ также не описывает процесс разработки Основного перечня минимального оборудования (MMEL) и Перечня допустимых отклонений конфигурации (CDL). Более подробное описание аспектов разработки ПО приведено в документе KT-178 AP МАК «Требования к программному обеспечению бортовой аппаратуры и систем при сертификации авиационной техники» и в аналогичных документах DO-178 RTCA и ED-12B EUROCAE. Подробное описание аспектов разработки аппаратуры приведено в документе KT-254 AP МАК «Руководство по гарантии конструирования бортовой электронной аппаратуры» и в аналогичных документах DO-254 RTCA/ED-80 EUROCAE. Инструктивные материалы по проектированию и вопросам сертификации интегрированной модульной авионики содержатся в P-297/DO-297/ED-124 AP МАК/RTCA/EUROCAE. Методологии оценки безопасности описаны в документе AP МАК P-4761 «Руководство по методам оценки безопасности систем и бортового оборудования самолетов гражданской авиации». Подробное описание оценки эксплуатационной безопасности приведены в SAE ARP5150 «Safety Assessment of Transport Airplanes In Commercial Service» и SAE ARP5151 «Safety Assessment of General Aviation Airplanes and Rotorcraft In Commercial Service» (русскоязычные версии этих документов будут разработаны в дальнейшем). Мероприятия после получения сертификата (модификация сертифицированного изделия) описаны в разделе 6 настоящего документа. Нормативные документы и процессы, используемые при разработке и утверждении MMEL, во всем мире различны. Руководство по разработке MMEL может быть получено от местных авиационных властей.

На рисунке 1 показана взаимосвязь различных документов разработки, в которых приведены инструктивные материалы по оценке безопасности, процессам жизненного цикла аппаратуры и ПО, и настоящего документа, описывающего процесс разработки системы.

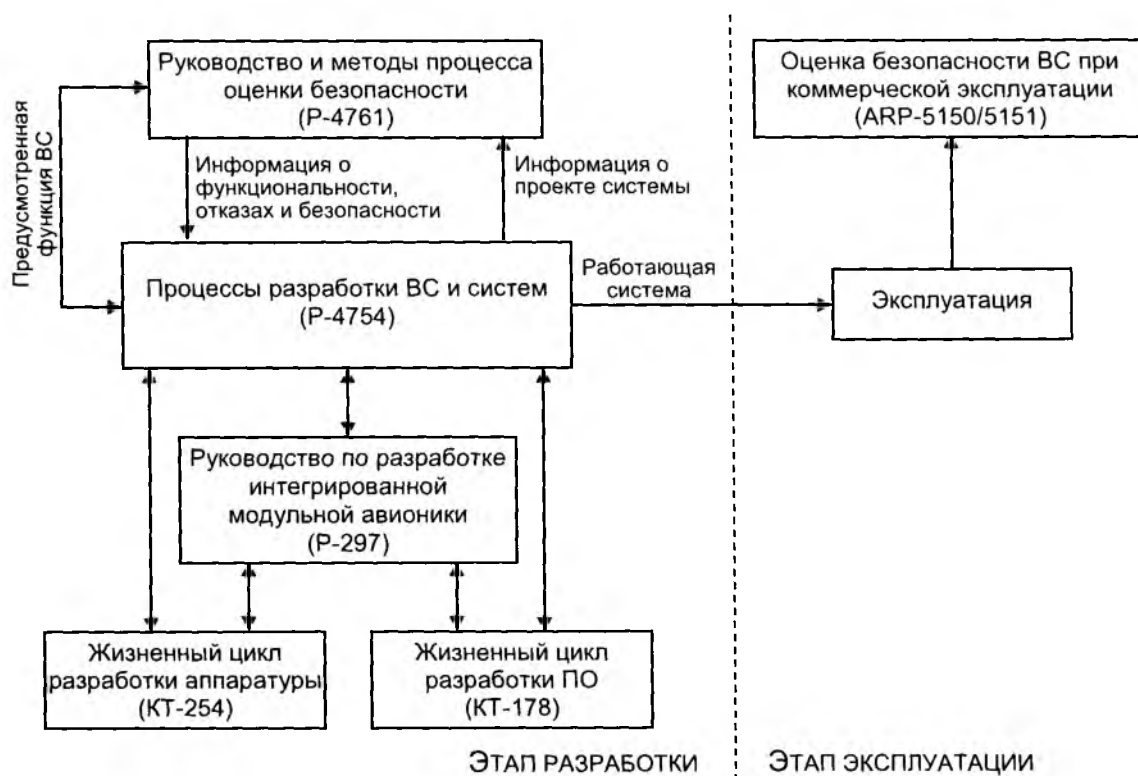


Рисунок 1. Руководящие документы по этапам разработки и эксплуатации

1.1 Назначение документа

Приведенные в настоящем документе инструктивные материалы относятся к системам, обеспечивающим функциональность уровня ВС и имеющим виды отказов, которые могут потенциально повлиять на безопасность ВС. Обычно такие системы в значительной степени взаимодействуют с другими системами в более широкой интегрированной среде. Часто важные элементы этих систем разрабатываются отдельными лицами, группами или организациями. Данные системы требуют повышенной дисциплины проектирования и структурированной разработки для обеспечения того, что требования к безопасности и эксплуатации могут быть полностью выполнены и обоснованы. Итерационный подход сверху вниз от уровня ВС к составляющим его компонентам является ключевым методом для запуска описанных здесь процессов.

Документ содержит практические рекомендации, которые не должны быть истолкованы как нормативные требования. Поэтому такие слова, как «подлежит» или «должен», не используются, либо используются при описании примеров. Признано, что организации, желающие пройти сертификацию, могут использовать методы, альтернативные тем, которые описаны или на которые есть ссылки в данном документе.

Настоящий документ не содержит ни инструктивных материалов, касающихся структуры отдельных организаций, ни рекомендаций по распределению ответственности за мероприятия сертификации. Никакие выводы из приведенных описаний на этот счет делать не следует.

1.2 История разработки документа

При подготовке редакции В документа DO-178/ED-12 RTCA/EUROCAE стало очевидно, что в качестве входных данных процесса разработки ПО потребуется информация уровня системы. Поскольку многие решения на системном уровне являются основополагающими для аспектов безопасности и функциональности систем ВС, нормативное регулирование процессов и их результатов, связанных с такими решениями, является уместным и необходимым.

Основанием для создания настоящего документа являлся запрос FAA в адрес SAE. FAA попросила SAE определить характер и объем информации на уровне системы, необходимой для демонстрации соответствия высокоинтегрированных или сложных авиационных систем нормативным документам. Была сформирована Группа разработки требований к интеграции систем для разработки руководства из серии ARP, которое удовлетворяло бы такую потребность.

Первые члены Группы разработки требований к интеграции систем признали, что достижение взаимопонимания на международном уровне было бы в этом начинании крайне желательным, и поддержали участие представителей как Федерального управления гражданской авиации США (FAA), так и Объединенных авиационных властей (JAA). Для координации европейского участия в деятельности Группы разработки требований к интеграции систем при EUROCAE была создана партнерская группа WG-42. В созданную группу вошли специалисты, имевшие непосредственный опыт в проектировании и эксплуатации магистральных самолетов и самолетов местных воздушных линий, авиационного электронного оборудования для ВС авиации общего и коммерческого назначения, реактивных двигателей и систем управления двигателями. В работе группы принимали участие представители авиационных властей различных направлений деятельности, обладающие разнообразным опытом. Со специальными комитетами RTCA (SC-167 и SC-180) и комитетом SAE (S-18) были установлены и поддерживались как формальные, так и неформальные связи. В ходе создания настоящего документа поддерживалась связь с координационной рабочей группой по подготовке 14CFR/CS 25.1309.

На протяжении всего периода разработки настоящего документа дискуссия неоднократно возвращалась к вопросу о том, насколько конкретными должны быть инструктивные материалы. Серьезные аргументы были выдвинуты в пользу подготовки списка конкретных шагов, необходимых для сертификации, таких как проверочные перечни. Не менее серьезные аргументы выдвигались и в пользу того, что документ должен фокусироваться лишь на фундаментальных вопросах, позволяя Заявителю и сертифицирующему органу самим согласовывать детали, исходя из специфики системы. Было признано, что сертификация любых реальных систем потребует серьезной инженерной оценки с обеих сторон. Качество такой оценки наилучшим образом обеспечивается общим пониманием фундаментальных принципов и вниманием к ним. Решение следовать в указанном направлении было также обусловлено некоторыми другими факторами, наиболее значимыми из них являются следующие: разнообразие возможного применения систем, быстрое развитие системной инженерии и накопленный опыт применения в отрасли инструктивных материалов, приведенных в DO-178/ED-12.

В настоящее время в системном проектировании имеется тенденция к возрастанию уровня интеграции между функциями ВС и системами, которые их выполняют. Хотя интеграция систем может давать существенную выгоду, возросшая сложность приводит к расширению возможности появления ошибок, особенно для функций, выполняемых совместно несколькими системами.

В соответствии с рекомендациями Консультативного комитета по разработке авиационных правил (ARAC), который в стремлении учесть повышение уровня интеграции поместил в рекомендательные циркуляры ссылки на ARP4754/ED-79, для обеспечения соответствия документам 14CFR/CS 23.1309 (см. AC23.1309-1D издания 2009 г.) и 25.1309 (см. AMC 25.1309 издания 2003 г. и AC25.1309-Arsenal draft), документ ARP4754/ED-79 стали все шире использовать в сертификации. Вместе с расширением использования, в частности, раздела 5.4 первого издания ARP4754 «Назначение уровней проектирования» пришло

понимание сильных и слабых сторон содержащихся в нем инструктивных материалов. Основной принцип кратко сформулирован в разделе 5.4 первого издания ARP4754 следующим образом:

«Если предварительная оценка безопасности системы (PSSA) показывает, что архитектура системы ограничивает влияние ошибок разработки так, что на уровне ВС влияние этих ошибок значительно смягчается, то для изделий внутри системы процессы гарантии проектирования могут осуществляться на более низком уровне жесткости».

Опыт показал, что процессы и описания, используемые для определения этих ограничений, явились причиной различного толкования и различных вариантов применения этого основного принципа. Поэтому уточнение процесса назначения уровней гарантии разработки является одним из основных вопросов в настоящей редакции, предлагающей методологию для определения надлежащих уровней гарантии разработки.

После публикации первого издания ARP 4754/ED-79 в 1996 г. Группа разработки требований к интеграции систем и рабочая группа WG-42 были распущены. После того как появилась необходимость пересмотра документа, потребовалось создание соответствующей группы, члены которой должны были иметь достаточный опыт для работы на уровне ВС. В качестве такой группы был выбран Комитет по безопасности воздушных судов SAE S-18, так как его члены были знакомы с первой редакцией документа, а разрабатываемые ими документы были близки данному Руководству. Некоторые члены комитета S-18 ранее входили в Группу разработки требований к интеграции систем, участвовавшую в подготовке первого издания ARP4754. Одновременно при EUROCAE была создана рабочая группа для внесения изменений в ED-79. В состав WG-63 вошли бывшие члены рабочей группы WG-42, а также представители широкого круга промышленных предприятий и научных учреждений, работающих в европейской авиакосмической отрасли. Заключив Меморандум о взаимопонимании в отношении настоящего документа, группа WG-63 работала параллельно S-18, обеспечивая полное соответствие ED-79A и ARP4754A.

Редакция А является обновлением документа с учетом развития отрасли в последние годы. Взаимосвязь ARP 4754/ED-79 с ARP4761, а также с DO-178/ED-12 и DO-254/ED-80 стала более прочной, разночтения между ними были выявлены и устранены. В редакции А применение концепции гарантии разработки распространено на уровень ВС и уровень системы, а также регламентировано использование понятия «гарантия разработки». Как результат, для ВС и авиационных систем вводится Уровень гарантии разработки функции (FDAL), а Уровень обеспечения безопасности проектирования элементов переименован в Уровень гарантии разработки элемента (IDAL). Также проведены улучшения на основе откликов, полученных от специалистов отрасли с момента первой публикации. Кроме того, S-18 и WG-63 согласовали настоящее издание со Специальным комитетом RTCA 205 (SC-205)/EUROCAE WG-71 для обеспечения согласованности используемых терминов и подходов с теми, которые были разработаны для внесения изменений в DO-178/ED-12.

2 ССЫЛКИ

2.1 Используемые документы

Для подготовки настоящего пояснительного материала были использованы документы, которые перечислены в данном разделе. Применяемое издание указанных документов является изданием, приведенным в настоящем разделе. Если существуют более поздние издания указанных документов, заявителям следует проверить их применимость. Следует помнить о том, что при отсутствии необходимости издания использованных документов могут быть не упомянуты в тексте настоящего документа.

2.1.1 Публикации SAE

Документы могут быть получены от SAE International, 400 Commonwealth Drive, Warrendale, Пенсильвания, 15096-0001, тел.: 877-606-7323 (США и Канада) либо 724-776-4970 (из-за пределов США), www.sae.org.

ARP4761 Guidelines and Methods for Conducting the Safety Process on Assessment Civil Airborne Systems

ARP5150 Safety Assessment of Transport Airplanes in Commercial Service

ARP5151 Safety Assessment of General Aviation Airplanes and Rotorcraft in Commercial Service

2.1.2 Публикации FAA

Документы получены от Федерального авиационного агентства, 800 Independence Avenue, SW, Вашингтон, округ Колумбия 20591, тел.: 866-835-5322, www.faa.gov.

14CFR Part 21 Certification Procedures for Products and Parts

14CFR Part 23 Airworthiness Standards: Normal, Utility, Acrobatic and Commuter Category Airplanes

14CFR Part 25 Airworthiness Standards: Transport Category Airplanes

14CFR Part 27 Airworthiness Standards: Normal Category Rotorcraft

14CFR Part 29 Airworthiness Standards: Transport Category Rotorcraft

14CFR Part 33 Airworthiness Standards: Aircraft Engines

14CFR Part 35 Airworthiness Standards: Propellers

AC 23.1309-1D System Safety Analysis and Assessment for Part 23 Airplanes

AC 25.19 Certification Maintenance Requirements

AC 09-1A System Design and Analysis, Advisory Circular

2.1.3 Публикации EASA

Документы могут быть получены от Европейского агентства авиационной безопасности Otto Platz 1, п/я 101253, D-50452, Кельн, Германия, www.easa.eu.in.

IR-21 Certification Procedures for Aircraft, and Related Products & Parts

CS-23 Certification Specifications for Normal, Utility, Aerobatic, Commuter Category Airplanes

CS-25 Certification Specifications for Large Airplanes

CS-27 Certification Specifications for Small Rotorcraft

CS-29 Certification Specifications for Large Rotorcraft

CS-E Certification Specifications for Engines

CS-P Certification Specifications for Propellers

AMC 25.19 Certification Maintenance Requirements

AMC 25.1309 Equipment, Systems and Installations EASA Acceptable Means of Compliance

2.1.4 Публикации RTCA

Документы могут быть получены от Radio Technical Commission for Aeronautics Inc., 1828 L Street, NW, Suite 805, Вашингтон, округ Колумбия, 20036, тел.: 202-833-9339, www.rtca.org.

DO-178 Software Considerations in Airborne Systems and Equipment Certification

DO-178A Software Considerations in Airborne Systems and Equipment Certification

DO-178B Software Considerations in Airborne Systems and Equipment Certification

DO-254 Design Assurance Guidance for Airborne Electronic Hardware

DO-297 Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations

2.1.5 Публикации EUROCAE

Документы могут быть получены от EUROCAE, 102 rue Etienne Dolet 92240, Малакофф, Франция.

ED-12A Software Considerations in Airborne Systems and Equipment Certification

ED-12B Software Considerations in Airborne Systems and Equipment Certification

ED-80 Design Assurance Guidance for Airborne Electronic Hardware

ED-124 Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations

2.1.6 Публикации AP МАК

Документы могут быть получены от AP МАК, 119017, Москва, Россия, ул. Большая Ордынка, 22/2/1, тел.: +7(495)9531244, www.mak-iac.org

АП 21 Сертификация авиационной техники, организаций разработчиков и изготовителей

АП 23 Нормы летной годности гражданских легких самолетов

АП 25 Нормы летной годности самолетов транспортной категории

АП 27 Нормы летной годности винтокрылых аппаратов нормальной категории

АП 29 Нормы летной годности винтокрылых аппаратов транспортной категории

Р-4761 Руководство по методам оценки безопасности систем и бортового оборудования воздушных судов гражданской авиации

КТ-178В Требования к программному обеспечению бортовой аппаратуры и систем при сертификации авиационной техники

КТ-254 Руководство по гарантии конструирования бортовой электронной аппаратуры

Р-297 Руководство по разработке и сертификации интегрированной модульной авионики

2.2 Определения

В этом разделе приведены определения терминов, использующихся в настоящем документе. Цитаты из других источников могут быть использованы в настоящем документе, если определения совпадают с определениями, приведенными в материалах других источников.

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

Анализ общих видов (Common Mode Analysis) – анализ, который выполняется с целью подтверждения того, что установленные по результатам оценки безопасности (ASA/SSA) события, связанные с отказами, действительно являются независимыми для фактической реализации (системы).

Анализ общих причин (Common Cause Analysis) – общий термин, включающий зональный анализ безопасности, анализ специфических рисков и анализ общих видов.

Аппаратура (Hardware) – элемент, являющийся физическим объектом.

Базовая конфигурация (Configuration Baseline) – известная конфигурация ВС, системы или элемента, по отношению к которой выполняется процесс внесения изменений.

Безопасность (Safety) – состояние, в котором риск приемлем.

Валидация (Validation) – определение того, что требования к изделию являются правильными и полными. [Создаем ли мы правильное(ую) ВС (систему, функцию, элемент)?].

Верификация (Verification) – оценка реализации требований с целью определения того, удовлетворены ли эти требования [Мы создали правильное ВС/систему/функцию/элемент?].

Взаимозаменяемость (Interchangeability) – способность к замене одного элемента системы другим при сохранении соответствия характеристик системы техническим требованиям.

Вид отказа (Failure Mode) – характер проявления отказа системы или элемента.

Внешнее воздействие (фактор) (External Event) – событие, источник происхождения которого не связан с конструкцией самолета или системы, 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 вредительство.

Гарантия (Assurance) – запланированные и систематические действия, направленные на достижение достаточного уровня доверия и получение свидетельств того, что продукт или процесс удовлетворяет определенным требованиям.

Гарантия разработки (Development Assurance) – все запланированные и систематизированные действия, подтверждающие с приемлемым уровнем доверия, что ошибки в требованиях, проектировании или реализации выявлены и устранены, так что система удовлетворяет применяемому к ней сертификационному базису (AMC 25).

Гарантия разработки элемента (Item Development Assurance) – все запланированные и систематизированные задачи, служащие для доказательства на достаточном уровне доверия, что ошибки разработки идентифицированы и исправлены так, что элемент удовлетворяет определенному набору требований.

Готовность (Availability) – качественная или количественная характеристика системы или элемента, свидетельствующая о том, что он находится в работоспособном состоянии в определенный момент времени. Иногда выражается как вероятность того, что система (элемент) не может выполнять свои функции (т.е. неготовность).

Группа элементов функциональных отказов (Functional Failure Set) – отдельный элемент или определенная группа элементов, которые считаются независимыми друг от друга (не обязательно в рамках одной системы), отказы которых приводят к отказному состоянию высшего уровня.

Демонстрация (Demonstration) – метод подтверждения характеристик путем наблюдения.

Допущения (Assumptions) – утверждения, принципы и/или предположения, предлагаемые без доказательства.

Единица конфигурации (Configuration Item) – ВС, система, элемент и относящиеся к ним данные, находящиеся под конфигурационным контролем.

Зональный анализ безопасности (Zonal Safety Analysis) – процедура анализа безопасности в отношении установки, взаимовлияния систем и потенциальных ошибок технического обслуживания, способных негативно отразиться на безопасности системы.

Инспекция (Inspection) – проверка системы или изделия/элемента на соответствие определенному стандарту.

Интеграция (Integration) – 1) действия, обеспечивающие совместное функционирование элементов изделия; 2) действия по объединению определенного числа отдельных функций в единую реализацию.

Интенсивность отказов (Failure Rate) – отношение плотности распределения вероятности отказов к вероятности безотказной работы элемента в момент времени t :
 $\lambda(t) = F'(t) / (1 - F(t))$.

Классификация отказных состояний (Classification (Failure Condition)) – дискретная шкала, устанавливающая категории степени опасности последствий отказных состояний. Уровни классификации определены в соответствующих рекомендательных материалах к параграфу 1309 авиационных правил (части 23, 25, 27, 29): катастрофические, аварийные, сложные (значительные), усложнение условий полета (незначительные) и не влияющие на безопасность.

Компонент (Component) – любая автономная часть, совокупность частей, сборка или блок, которая выполняет определенную функцию, необходимую для работы системы.

Элемент группы (Member) – функция или элемент конструкции самолета/системы, которые могут иметь ошибки, приводящие к потере соответствующих функций или к их неправильному выполнению. [Применение данного определения ограничено понятием Functional Failure Set].

Летная годность (Airworthiness) – состояние ВС, системы или компонента, при котором они обеспечивают выполнение возложенных функций безопасным образом.

Метод/методика моделирования (Modeling Technique) – подход, применяемый для моделирования заданного аспекта системы/функции/элемента.

Модель (Model) – абстрактное представление заданного набора аспектов системы/функции/элемента, используемое для анализа, симуляции и/или генерации кода и обладающее точно выраженными и однозначно определенными порядком и семантикой.

Модель требований (Requirements Model) – Модель, полностью или частично представляющая требования на определенном уровне абстракции.

Надежность (Reliability) – вероятность того, что система или элемент будет выполнять требуемую функцию в заданных условиях без отказа в течение определенного периода времени.

Независимость (Independence) – 1) концепция проектирования, позволяющая минимизировать вероятность ошибок общих видов и каскадных отказов между функциями или элементами ВС/системы; 2) разделение ответственности, которое гарантирует выполнение объективной оценки, например, валидация проводится не только разработчиком требований к системе или элементу.

Независимость разработки элемента (Item Development Independence) – свойство, позволяющее минимизировать вероятность ошибки общих видов в процессе разработки элемента.

Неисправность (Fault) – проявление отклонения в работе элемента или системы, которое может привести к отказу.

Обособление (Partitioning) – механизм, разбиения системы или элемента на части, настолько независимые, что в пределах одной части можно подтвердить уровень гарантии разработки.

Одобрение (Approval) – акт формального разрешения применения, который выполняется сертифицирующим органом.

Одобренный (Approved) – признанный сертифицирующим органом годным для определенной цели (ИКАО).

Опасность (Hazard) – состояние, связанное с нарушением безопасности в результате отказов, внешних воздействий, ошибок или сочетания этих факторов.

Орган (власти) (Authority) – организация или лицо, ответственное за выдачу сертификата (одобрения) о соблюдении требований, применяемым на территории государства.

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 (РЦ 25.1309).

Отказное состояние (функциональный отказ, вид отказа системы) (Failure Condition) – состояние, оказывающее непосредственное или косвенное влияние на ВС и находящихся на борту лиц, вызванное или усугубленное одним или несколькими отказами или сбоями, с учетом фазы полета, соответствующих неблагоприятных условий эксплуатации или среды, а также внешних воздействий.

Примечание. Под отказным состоянием понимается состояние системы, характеризующееся 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 (РЦ 25.1309).

Оценка (Assessment) – экспертиза, основанная на инженерном подходе.

Оценка безопасности системы (System Safety Assessment) – систематическая всесторонняя экспертиза реализованной (конструкции) системы для подтверждения того, что применимые к ней требования по безопасности выполнены.

Оценка функциональной опасности (Functional Hazard Assessment) – систематическое, всестороннее исследование функций самолета и его систем с целью определения и классификации отказных состояний этих функций в соответствии с тяжестью их последствий.

Ошибка (Error) – упущение или неверное действие члена экипажа или персонала, выполняющего техническое обслуживание, или ошибка в технических требованиях, при проектировании или в реализации (РЦ 25.1309).

Ошибка общего вида (Common Mode Error) – ошибка, которая оказывает неблагоприятное воздействие на несколько элементов, считающихся в ином отношении независимыми.

Ошибка разработки (Development Error) – ошибка в определении требований, проектировании или реализации.

Последствия отказа (Failure Effect) – последствия, которые вызывает рассматриваемый вид отказа на работу, функции или состояние системы или элемента.

Пояснительные материалы (Guideline) – вспомогательные сведения, которые являются полезными, но не являются руководством к обязательному исполнению.

Предварительная оценка безопасности системы (Preliminary System Safety Assessment) – систематическая оценка предлагаемой архитектуры системы и ее реализации на основании Оценки функциональной опасности и Классификации отказных состояний с целью определения (установления) требований по безопасности для системы и ее элементов.

Принятие (Acceptance) – признание сертифицирующим органом того, что представленные данные, доказательства соответствия или эквивалентного соответствия удовлетворяют применимым требованиям.

Программное обеспечение (Software) – компьютерные программы, процедуры, правила и любая связанная с ними документация, относящиеся к работе вычислительной системы.

Производные требования (Derived Requirements) – дополнительные требования, возникающие в процессе разработки из проектных решений или решений реализации, которые не трассируемы непосредственно к требованиям более высокого уровня.

Процесс (Process) – набор взаимосвязанных мероприятий, выполняемых с целью получения заданного результата или изделия.

Реализация (Implementation) – создание физического объекта по техническим требованиям.

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

Риск (Risk) – комбинация частоты (вероятности) возникновения события и уровня тяжести последствий, связанных с этим событием.

Руководство (Guidance) – рекомендуемая процедура для обеспечения соответствия нормативным документам.

Сертификация (Certification) – юридическое признание того, что продукт, услуга, организация или лицо соответствуют распространяющимся на них требованиям. Такая сертификация включает мероприятия по технической проверке продукта, услуги, организации или лица и формальное признание соблюдения применимых требований путем выдачи сертификата, лицензии, одобрения или другого документа, как требуется национальными законами и процедурами.

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

Система (System) – комбинация взаимосвязанных элементов, предназначенная для выполнения определенной функции(й).

Сложность (Complexity) – свойство функций, систем или элементов, делающее их функционирование, виды отказов или последствия отказов затруднительными для понимания без использования аналитических методов.

Соблюдение (Compliance) – успешное выполнение всех обязательных мероприятий; совпадение ожидаемых или заданных результатов с фактическими результатами.

Соглашение (Agreement) – признание сертифицирующим органом, что план или предложение, относящиеся или поддерживающие заявку на получение одобрения на систему или образец оборудования, является приемлемым заявлением о намерениях с учетом применимых требований.

Соответствие (Conformance) – надлежащее совпадение со стандартом, спецификацией или чертежом.

Спецификация (Specification) – совокупность требований, которые в целом являются критерием, определяющим функции и свойства системы, компонента или элемента.

Специфические риски (Particular Risks) – специфические риски определяются как события или воздействия (факторы), являющиеся внешними для самолета или возникающие внутри самолета, но являющиеся внешними по отношению к анализируемым системам и элементам, но которые могут опровергнуть предположение о независимости отказов.

Средняя наработка между отказами (Mean Time Between Failures (Mtbf)) – математическое ожидание наработки (времени работы) изделия от момента восстановления его работоспособности после отказа до следующего отказа.

Примечание. Данное определение имеет смысл только для ремонтпригодных изделий. Для неремонтпригодных изделий используется термин Средняя наработка до отказа (MTTF).

Сходство (Similarity) – относится к системам, которые по своим характеристикам и использованию подобны системам, используемым на ранее сертифицированных ВС. В принципе предполагается, что ни одна из частей рассматриваемой системы не находится в условиях более высокого риска (в связи с окружающими условиями или установкой) и что эксплуатационные нагрузки не являются более тяжелыми, чем нагрузки на ранее сертифицированном ВС.

Тестирование (Test) – процедура количественной оценки характеристик с использованием объективных критериев, выполняемая для получения результата: «прошел» – «не прошел».

Трассируемость (Traceability) – задокументированная взаимосвязь двух или более элементов процессов разработки. Например, взаимосвязь между требованием и его источником или методом верификации и проверяемым требованием.

Требование (Requirement) – идентифицируемый элемент спецификации функции, который может быть валидирован, и по отношению к которому может быть выполнена верификация его реализации.

Уровень гарантии разработки элемента (IDAL) (Item Development Assurance Level (IDAL)) – уровень строгости выполнения задач гарантии разработки элемента. (Например, IDAL – это соответствующий уровень ПО для целей КТ-178 и уровень гарантии конструирования для целей КТ-254, которые должны быть достигнуты для элемента.)

Уровень гарантии разработки функции (Function Development Assurance Level) – уровень строгости выполнения задач гарантии разработки функций.

Примечание. FDAL используется для определения целей Р-4754А, которые необходимо достигнуть для функций ВС/системы.

Функция (Function) – планируемое поведение изделия, основанное на определенном наборе требований, независимо от реализации.

Функциональная независимость (Functional Independence) – свойство, при котором функции можно считать различными, чтобы минимизировать вероятность общих ошибок в требованиях.

Целостность (Integrity) – качественный или количественный показатель, позволяющий рассчитывать на то, что система или элемент будут работать корректно. Иногда, с точки зрения вероятности, таким образом выражается отклонение от критерия правильной работы.

Элемент/объект/изделие (Item) – составная часть аппаратуры или программного обеспечения, имеющая четко выраженные и определенные интерфейсы.

2.3 Аббревиатуры и сокращения

AC	Консультативный циркуляр
AMC	Приемлемые методы установления соответствия (EASA)
ARAC	Консультативный комитет по разработке авиационных правил (FAA)
ARP	Рекомендации SAE для аэрокосмической промышленности

ASA	Оценка безопасности воздушного судна
CCA	Анализ общих причин
CFR	Свод федеральных нормативных актов США
CMA	Анализ общих видов
CS	Сертификационные спецификации EASA
DAL	Уровень гарантии разработки
DO	Документ RTCA
EASA	Европейское агентство авиационной безопасности
ED	Документ EUROCAE
ETOPS	Расширенные Правила полетов для двухмоторных самолетов
ETSO	Европейская инструкция о применении технических стандартов
EUROCAE	Европейская организация по оборудованию гражданской авиации
F	Функция
FC	Отказное состояние
FAA	Федеральное управление гражданской авиации США
FAR	Федеральные авиационные правила
FDAL	Уровень гарантии разработки функции
FFS	Группа элементов функциональных отказов
FHA	Оценка функциональной опасности
FMEA	Анализ видов и последствий отказов
FMES	Сводка видов и последствий отказов
FTA	Анализ дерева отказов
I	Элемент/Объект/Изделие
IDAL	Уровень гарантии разработки элемента/объекта/изделия
MA	Марковский анализ
MMEL	Основной перечень минимального оборудования
PASA	Предварительная оценка безопасности воздушного судна
PSSA	Предварительная оценка безопасности системы
RTCA	Радиотехническая комиссия по авионавигации
SAE	Сообщество инженеров транспорта
SSA	Оценка безопасности системы
ZSA	Зональный анализ безопасности
АП	Авиационные правила
AP MAK	Авиационный регистр Межгосударственного авиационного комитета
BC	Воздушное судно
ЖЦ	Жизненный цикл
ИКАО	Международная организация гражданской авиации
КИ	Комплекующее изделие
КК	Категория контроля
КТ	Квалификационные требования
ПО	Программное обеспечение
Р	Руководство
РЦ	Рекомендательный циркуляр

3 ПЛАНИРОВАНИЕ РАЗРАБОТКИ

Назначение процесса планирования разработки состоит в определении таких средств создания ВС или системы, которые соответствуют требованиям к ВС/системе и обеспечивают уровень доверия, соответствующий требованиям летной годности. Цели процесса планирования разработки:

- определить мероприятия процессов разработки и интегральных процессов ЖЦ разработки, с учетом требований к ВС/системе и уровней гарантии разработки функций и элементов;
- определить жизненный цикл (жизненные циклы) разработки, включая взаимосвязи между процессами, последовательность их выполнения, механизмы обратной связи и критерии перехода;
- выбрать среду ЖЦ, включая методы и инструменты, которые будут использоваться при выполнении мероприятий каждого процесса ЖЦ;
- определить стандарты разработки, соответствующие целям обеспечения безопасности создаваемого ВС или создаваемой системы;
- разработать планы, соответствующие целям каждого из интегральных процессов (раздел 5).

Выходные данные процесса планирования могут быть представлены в различных форматах, таких как интегрированные план-графики либо формально выпущенные документы планирования. В процессе планирования должна учитываться итеративная природа процесса разработки. Необходимо также надлежащим образом идентифицировать и управлять взаимосвязями между элементами планирования и их обратными связями.

3.1. Процесс планирования

На рисунке 2 приведен пример процесса планирования в целом, включая некоторые общие цели, применимые ко всем элементам планирования. Показанный на рисунке 2 типовой процесс предполагает, что нужно обдумать все элементы планирования до документирования любого из них. В действительности разработка таких элементов планирования может проводиться не одновременно. Поэтому важно убедиться в том, что элементы планирования согласованы между собой и в совокупности представляют полный план всего ЖЦ разработки. Это следует учитывать при рассмотрении отдельных элементов планирования.

В настоящем документе отдельные мероприятия планирования для каждого из процессов подробно описаны в подразделе, посвященном соответствующему процессу. В таблицу 1 сведены элементы, которые должны быть включены на стадии планирования. Они должны относиться к проектированию и сертификации соответствующего ВС, системы или элемента.

Данный процесс может быть выполнен повторно при внесении изменений в ВС или систему, например, при создании новой производной модели или при модификации эксплуатируемого ВС.

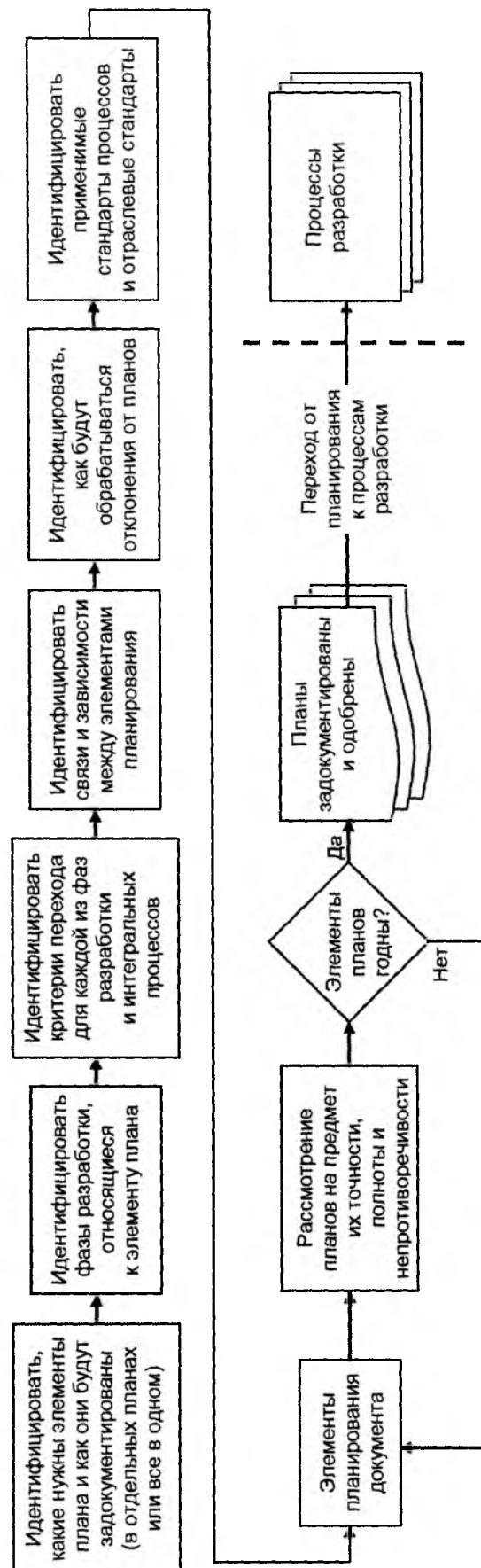


Рисунок 2. Процесс планирования

3.2. Критерии перехода

Ключевым компонентом планирования является установление контрольных точек процессов ЖЦ и рассмотрений, привязанных к этапам и рубежам программы. Планы должны ясно определять ожидаемые степени готовности с тем, чтобы обеспечить прослеживаемость хода выполнения работ и интеграции для основных элементов проектирования, реализации и сертификации. Это может быть выполнено за счет установления четких технических критериев идентификации и критериев начала и завершения процессов. Вопросы, остающиеся открытыми при переходе от одной стадии разработки к другой, должны надлежащим образом отслеживаться и контролироваться.

Таблица 1. Элементы планирования разработки

Элемент планирования	Описание элемента	Раздел 4754A
Разработка	Установить процесс и методы, которые будут использоваться в качестве основы для разработки архитектуры, интеграции и реализации ВС или системы	Данный раздел и 4.0
Программа безопасности	Определить область применения и содержание мероприятий по обеспечению безопасности, связанных с разработкой ВС или системы	5.1.5
Управление требованиями	Определить и описать, как формируются и управляются требования. Иногда эти элементы включаются в сочетании с элементами валидации	5.3
Валидация	Описать, как будет продемонстрирована полнота и правильность требований и допущений	5.4
Верификация реализации	Определить процессы и критерии, которые будут применены при демонстрации того, что реализация удовлетворяет требованиям	5.5
Управление конфигурацией	Описать ключевые единицы конфигурации, относящиеся к разработке, и способы управления ими	5.6
Гарантия процесса	Описать средства гарантии того, что необходимые для разработки системы методики и процедуры применяются	5.7
Сертификация	Описать процесс и методы, которые будут использоваться для достижения сертификации	5.8

3.2.1 Отклонения от планов

При разработке иногда может возникать необходимость отклонения от задокументированных планов. Поэтому при планировании необходимо определить процесс, учитывающий отклонения от планов. В элементах планирования должны быть указаны методы регистрации, получения одобрения и документирования любых отклонений.

4 ПРОЦЕСС РАЗРАБОТКИ ВОЗДУШНОГО СУДНА И СИСТЕМ

В данном разделе приведен обзор общего подхода к разработке воздушного судна и его систем от формирования концепции до реализации. В разделе определяется общая терминология и ожидаемые результаты процессов разработки, а также взаимосвязь между этими процессами для понимания назначения и обоснования их выполнения.

Жизненный цикл разработки имеет свое начало и свой конец и может быть выполнен повторно при внесении изменений в воздушное судно или систему. На рисунке 3 дана простая иллюстрация жизненного цикла разработки. Приведенные в настоящем документе инструктивные материалы относятся в первую очередь к стадии «Разработка».

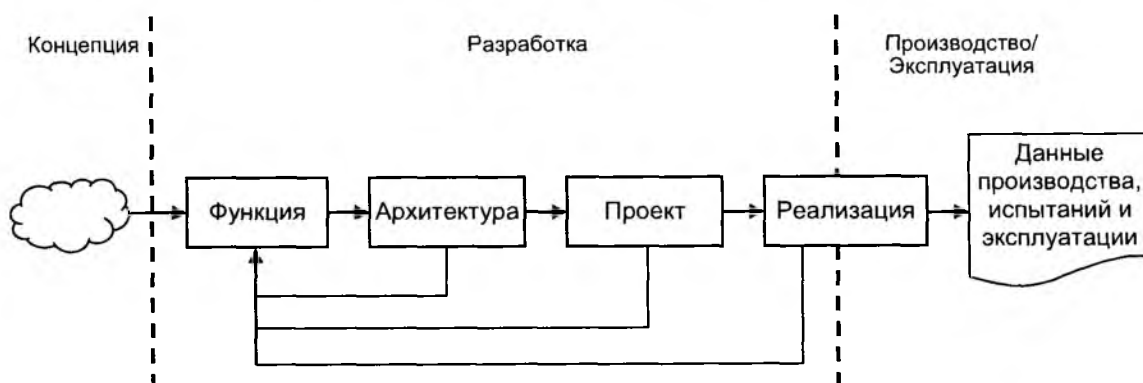


Рисунок 3. ЖЦ разработки

На стадии определения концепции (стадии предварительной разработки и исследований) определяются общие эксплуатационные характеристики воздушного судна и его конфигурация, например, грузоподъемность и дальность полета, размер воздушного судна, количество и расположение двигателей, площадь крыла, применение новых технологий при проектировании и изготовлении. За стадией определения концепции следует стадия разработки, служащая для подготовки к производству/эксплуатации.

Стадия разработки считается завершенной, если выполнены следующие условия:

- в производство передана информация, необходимая для сборки и испытаний;
- предоставлены на рассмотрение и утверждены все данные для подтверждения соответствия требованиям авиационных властей;
- установлено соответствие проекта всем внутренним требованиям организации (при необходимости);
- предоставлены сведения об ограничениях, техническом обслуживании и другие эксплуатационные документы, необходимые эксплуатантам воздушного судна.

4.1 Процесс концептуальной разработки воздушного судна/системы

В данном разделе описан общий процесс разработки воздушного судна/системы. В разделе не указан предпочтительный метод либо процесс и отсутствует указание на наличие какой-либо определенной организационной структуры для выполнения разработки. На рисунке 4 приведена модель процесса разработки системы с указанием для каждого этапа наименования выполняемых действий и номеров соответствующих им разделов, в которых описаны указанные действия.

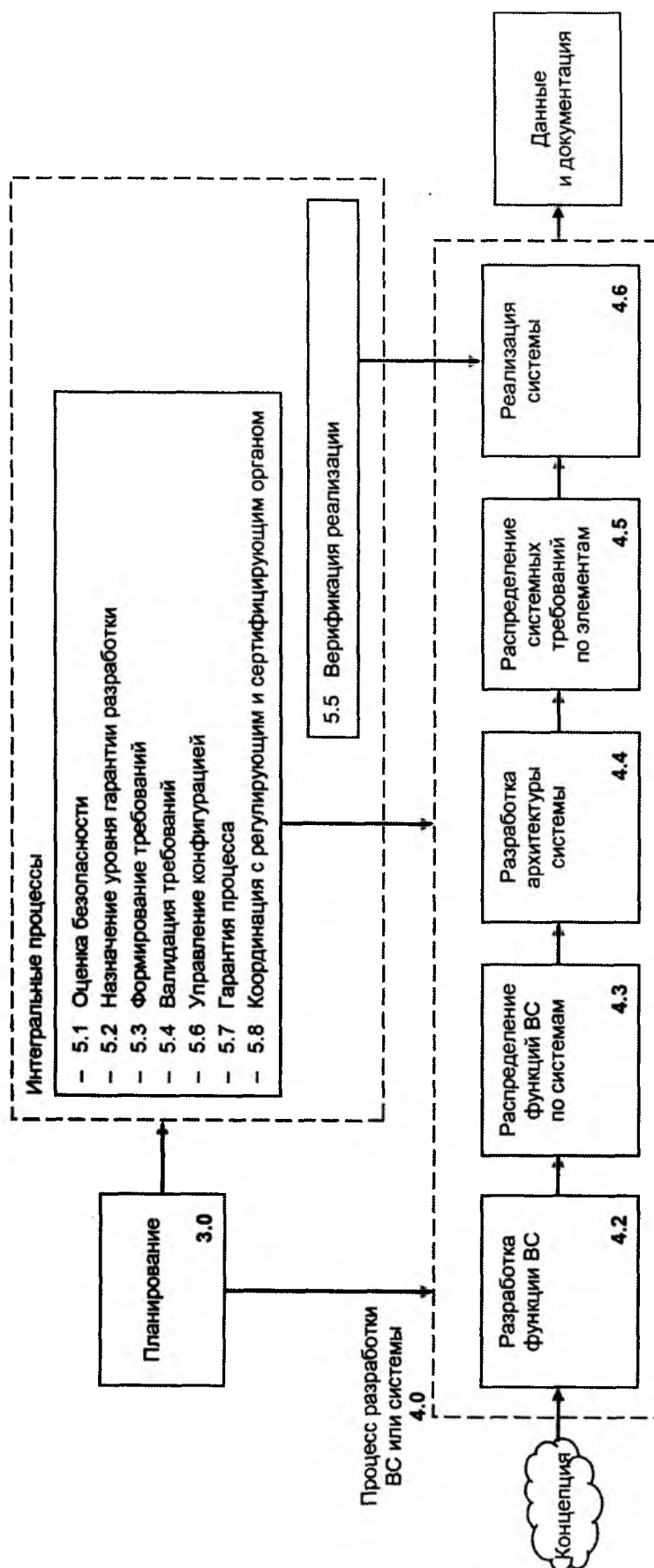


Рисунок 4. Модель процесса разработки ВС или системы

Последовательность разработки конкретной системы «сверху-вниз», начиная с определения требуемой функции воздушного судна, обеспечивает удобную концептуальную модель процесса разработки системы. Стандартные процессы разработки системы выполняются путем согласованных и последовательных итераций, нисходящих (сверху-вниз) и восходящих (снизу-вверх). В настоящем документе внимание прежде всего обращено на нисходящий аспект, так как он обеспечивает необходимую связь между разработкой системы и обеспечением безопасности воздушного судна. Следует отметить, что организации могут вводить в структуру «ВС – система – элемент» дополнительные уровни иерархии. Описанные в настоящем документе процессы могут применяться на уровнях от воздушного судна до отдельного элемента с учетом специфики каждого уровня.

4.1.1 Гарантия разработки

По причине высокой сложности и интегрированности современных авиационных систем особую обеспокоенность Авиационных властей вызывает то, что ошибки разработки могут приводить к отказным состояниям ВС или играть роль в их возникновении. Для снятия этой обеспокоенности необходима методология смягчения влияния ошибок разработки. Приведенный ниже текст отражает эту обеспокоенность, выраженную в действующих сертификационных требованиях и нормах.

- a. Обеспокоенность вызывает эффективность и предметный охват методов, используемых для оценки безопасности высокоинтегрированных систем, которые выполняют сложные и взаимосвязанные функции, в частности на основе электроники и программного обеспечения. Обеспокоенность заключается в том, что методы проектирования и анализа, традиционно применяемые к детерминированным рискам или к несложным традиционным системам, не могут обеспечить достаточный предметный охват при исследовании и гарантии безопасности сложных систем. Итак, для сложных систем применимы иные методы гарантии, такие как гарантия разработки, использующая совокупность гарантии процесса, валидационных и верификационных критериев, либо структурный анализ и методы оценки на уровне воздушного судна, в части интегрированных и взаимодействующих систем воздушного судна. Системное применение этих методов увеличивает уверенность в том, что ошибки в требованиях или проекте, а также при интеграции систем будут определены и исправлены.
- b. С учетом вышеизложенного, а также поправки к пункту 25.1309 циркуляр РЦ-АП25.1309 «Конструкция и анализ систем» был пересмотрен с целью определения новых качественных и количественных подходов, которые могут использоваться для определения требований к безопасности и определения соответствия им, а также уточнения правил, касающихся всего воздушного судна и его систем. Документ также содержит рекомендации для определения условий, когда или в каком случае анализ или действия по гарантии разработки должны быть проведены в рамках процессов разработки и оценки безопасности. Числовые значения вероятностных величин в требованиях применяются в случаях, когда влияние отказов системы проверяется количественными методами анализа. Аналитические инструменты, используемые для определения числовых значений, применяются в дополнение к качественным методам, основанным на экспертной оценке.

Следовательно, требуется процесс, который устанавливает степень уверенности в том, что ошибки разработки, которые могут приводить к функциональным отказам или стать причиной отказных состояний, будут минимизированы с надлежащим уровнем строгости. Далее такой процесс будет называться процессом гарантии разработки.

4.1.2 Введение в процесс гарантии разработки

Представленные в КТ-178 и КТ-254 рекомендации признаны промышленностью и авиационными властями для установления уровней гарантии того, что конкретные элементы программного обеспечения и аппаратуры соответствуют предъявляемым к ним требованиям. Чтобы учредить в проекте уровни доверия для систем воздушного судна в целом, процесс, представленный в данном документе, предлагает рекомендации для разработки требований на уровнях воздушного судна, системы и элементов (*Прим. ред.: архитектура еще не определена*). Процесс включает валидацию требований и верификацию с целью показать

выполнение требований в сочетании с необходимым управлением конфигурацией и действиями по гарантии процесса. В связи с тем, что назначение уровней гарантии разработки зависит от классификации отказных состояний, процесс анализа безопасности используется в сочетании с процессом гарантии разработки, определяемом в настоящем документе, для идентификации отказных состояний и их классификации по степени тяжести, которая используется для получения уровней строгости, необходимых в разработке.

Сложные системы и интегрированные функции на уровне воздушного судна характеризуются повышенным риском ошибки разработки (ошибки определения требований и ошибки проектирования) и нежелательными непредвиденными последствиями. При этом обычно не практикуется (и даже невозможна) разработка ограниченного набора тестов для высокоинтегрированных и сложных систем, чтобы окончательно продемонстрировать отсутствие остаточных ошибок разработки. Так как обычно эти ошибки не являются детерминированными, а любые числовые методы для их определения неприемлемы, то необходимо использовать качественные методы, чтобы установить соответствие системы требованиям безопасности. Более того, отсутствует непосредственная связь между уровнем гарантии разработки функций (FDAL) и числовыми вероятностями. Цели безопасности, связанные с классификацией отказных состояний, могут быть достигнуты как с помощью назначенного уровня строгости гарантии разработки функции, так и количественными методами проведения анализов (при необходимости). Эти два различных метода, в общем, не связаны и не дополняют друг друга.

В этом контексте в Р-4754A документы КТ-178 и КТ-254 рассматриваются в качестве средств внедрения и реализации гарантии строгости разработки элементов – программного обеспечения и аппаратуры соответственно. По отношению к программному обеспечению и аппаратуре процессы гарантии далее не рассматриваются, поскольку процесса гарантии разработки на уровне воздушного судна/системы достаточно для смягчения ошибок разработки. Необходимо выполнение единого процесса гарантии разработки от уровня воздушного судна до уровня элементов, как показано на рисунке 5.

В разделе 5.2 предлагаются рекомендации по определению FDAL и IDAL, начиная с уровня воздушного судна и вплоть до уровня элементов. Цели для достижения соответствия каждому из FDAL изложены в Приложении А. Цели для обеспечения соответствия каждому из IDAL изложены соответствующим образом в КТ-178 и КТ-254 для программного обеспечения и аппаратуры.

В целом гарантия разработки – это процессно-ориентированный подход, дающий уверенность в том, что разработка системы выполняется упорядоченным способом для снижения вероятности возникновения ошибок, которые могли бы повлиять на безопасность воздушного судна.

4.1.3 Введение в иерархическую структуру требований безопасности, полученных в результате анализа безопасности

Требования безопасности существуют на всех уровнях абстракции объектов проекта (воздушное судно, системы и элементы). Типы требований безопасности включают требования к независимости, количеству (вероятностные), качеству, пригодности, целостности, мониторингу, FDAL, эксплуатации и техническому обслуживанию.

Требования безопасности в иерархической структуре распределены функционально и переходят с верхнего уровня на нижние, от функций уровня воздушного судна до функций уровня элементов. На уровне воздушного судна требования безопасности – это все требования, сформированные в результате анализа функциональных опасностей воздушного судна (FHA), таких функций, как, например, управление по курсу, торможение на земле и т.п. На уровне системы требованиями безопасности являются все системные требования, которые получены из FHA системы и представляют собой часть требований безопасности уровня воздушного судна. На нижеследующем уровне требованиями являются все особенности системы, которые обеспечивают достижение целей безопасности согласно классификации отказных состояний FHA системы. На рисунке 5 отображены различные уровни требований.

Требования безопасности также могут быть получены по результатам анализа общих причин (ССА).

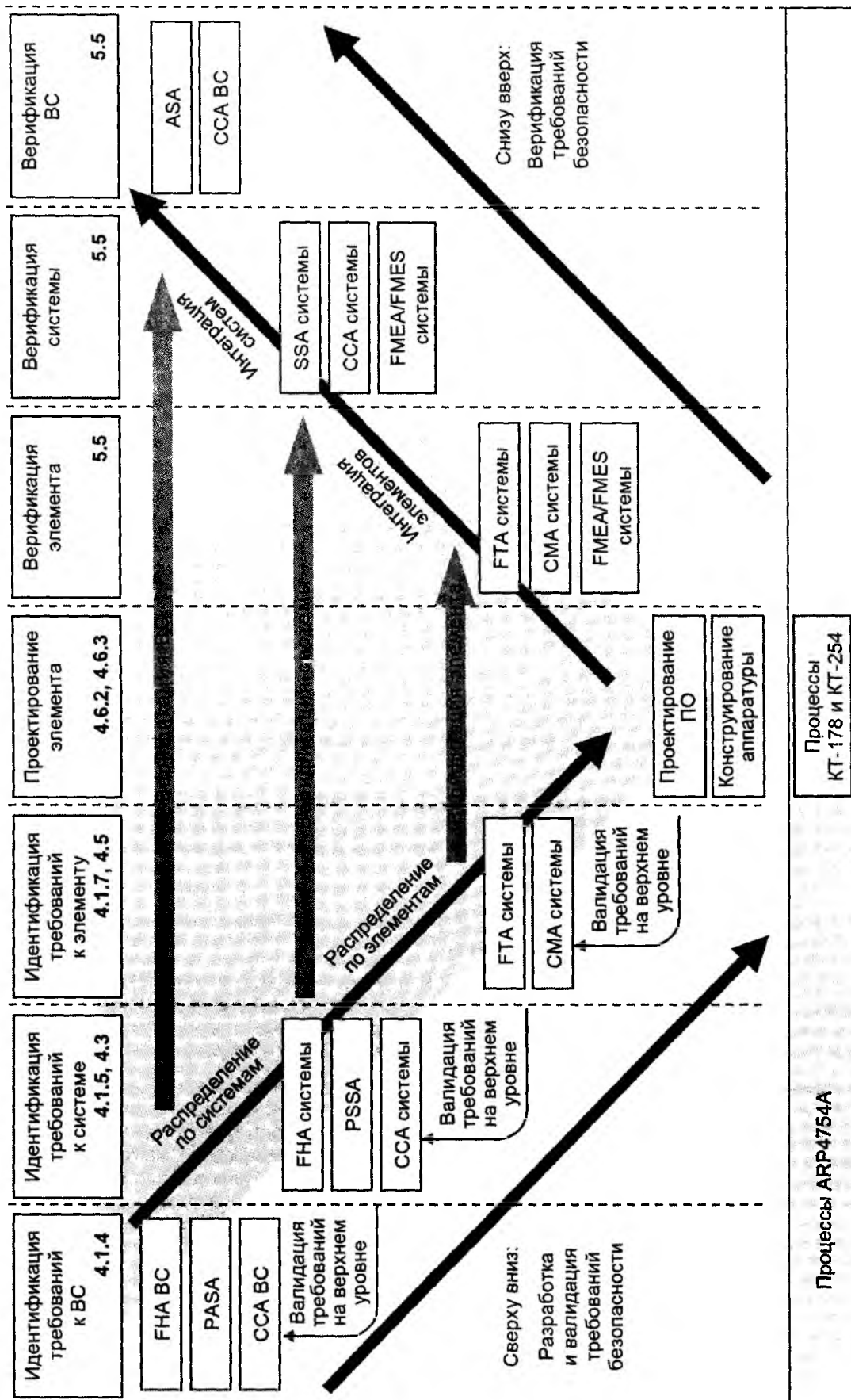


Рисунок 5. Интеграция между процессом оценки безопасности и процессом разработки

4.1.4 Определение функций на уровне воздушного судна, требований к функциям и интерфейсов функций

Эти мероприятия устанавливают основные характеристики уровня воздушного судна и требования к его функционированию. Исходя из этих основных требований, определяются функции воздушного судна и связанные с ними требования, а также определяются интерфейсы функций с учетом внешних физических ограничений и условий эксплуатации. Функции воздушного судна – это действия наивысшего уровня, которые не обязательно связаны с реализацией одной, отдельной физической системы.

В результате этих мероприятий формируется перечень функций воздушного судна, связанных с ними требований к функциям и интерфейсов этих функций.

4.1.5 Распределение функций воздушного судна по системам

Данный уровень мероприятий устанавливает надлежащую группировку функций воздушного судна и распределение требований, предъявляемых к данным функциям, по всем системам. В результате должен сформироваться набор требований для каждой системы воздушного судна, включая относящиеся к ним интерфейсы.

4.1.6 Разработка системной архитектуры

Архитектура системы проектируется в процессе разработки. Она определяет структуру и границы системы, в которых выполняется проектирование отдельных ее элементов для обеспечения всех технических требований и всех требований безопасности. В результате этих мероприятий появляется архитектура системы до уровня элементов и распределение системных функций и требований безопасности к соответствующим элементам, входящим в архитектуру.

4.1.7 Распределение системных требований по объектам

На практике разработка архитектуры системы и распределение требований оказываются тесно взаимосвязаны и являются итерационными процессами. В рамках каждого итерационного цикла идентификация и понимание требований повышаются, и распределение системных требований по элементам программного обеспечения и аппаратуры становится более точным.

В результате усилий по распределению требований по элементам в выходных данных данного процесса учитываются требования к программному обеспечению и аппаратуре, включая цели безопасности, количественные требования к безопасности, уровни гарантии разработки и требования к функциям и характеристикам.

4.1.8 Реализация системы

Этап реализации системы процессной модели, описанной в настоящем документе, увязывает модель системных процессов и рекомендации по жизненным циклам процессов разработки программного обеспечения и аппаратуры, описанных в КТ-178 и КТ-254.

На данной стадии определяются задачи по гарантированию надлежащего функционирования систем воздушного судна совместно и по отдельности.

Результаты включают определение процедур интеграции программного обеспечения и аппаратуры, процедур интеграции систем, оформление и выпуск конструкторских чертежей аппаратуры, исходного кода программного обеспечения и соответствующей документации, применимых данных гарантии разработки, макеты или прототипы аппаратуры, если применимо, а также образцы, протестированные в условиях полета или лаборатории.

4.2 Разработка функций воздушного судна

На рисунке 4 изображена обобщенная схема процесса разработки системы, а рисунок 6 иллюстрирует процесс реализации функций воздушного судна. Модель включает множество процессов разработки системы. Каждый такой процесс может состоять из множества процессов разработки элементов. Существует несколько интегральных процессов, которые повторяются в ходе каждого из процессов разработки системы.

Большинство реальных процессов разработки системы включают множество повторяющихся циклов, что придает действиям разработчика больше циклический, чем последовательный характер. Момент возникновения требования к реализации функции воздушного судна может случиться в любой точке цикла разработки. Для новых функций воздушного судна необходимо начинать с проектирования мероприятий или процессов наивысшего уровня. При добавлении функции воздушного судна вход в процесс может осуществляться в контексте изменения конкретных элементов. Тем не менее, независимо от точки входа в процесс, необходимо проводить оценку влияния новой или модифицируемой функции на прочие функции воздушного судна и требования к ним. На практике большинство мероприятий разработки, показанных на рисунке 6, выполняются параллельно и могут иметь взаимную зависимость, приводящую к изменению ранее установленных требований.

В процессе распределения требований к функции должна быть в явном виде представлена информация по классификации соответствующих отказных состояний. Это обеспечивает трассируемость, для того чтобы обосновывать любые преимущества архитектурного обособления в дальнейшем. В этой части процесса распределения требований также появляются производные требования, которые подлежат валидации и определению их влияния на безопасность.

К типичным функциям воздушного судна могут быть отнесены следующие:

- a. Управление полетом
- b. Руление
- c. Обеспечение взаимодействия с Управлением воздушным движением (УВД)
- d. Автоматическое управление полетом
- e. Обеспечение погрузочно-разгрузочных работ
- f. Управление двигателями
- g. Предотвращение столкновений
- h. Торможение на земле
- i. Защита окружающей среды
- j. Обеспечение комфорта пассажиров;
- k. Обеспечение связи
- l. Определение траектории полета
- m. Навигация
- n. Обеспечение безопасности пассажиров.

Если настоящий документ применяется при разработке двигателя, к типичным функциям двигателя могут быть отнесены:

- a. Регулирование тяги
- b. Управление реверсом тяги
- c. Обеспечение безопасности пассажиров
- d. Обеспечение связи с воздушным судном
- e. Контроль исправности двигателя.

Если настоящий документ применяется при разработке несущего винта, к типичным функциям могут быть отнесены:

- a. Регулирование скорости
- b. Обеспечение безопасности пассажиров
- c. Регулирование шага лопастей.

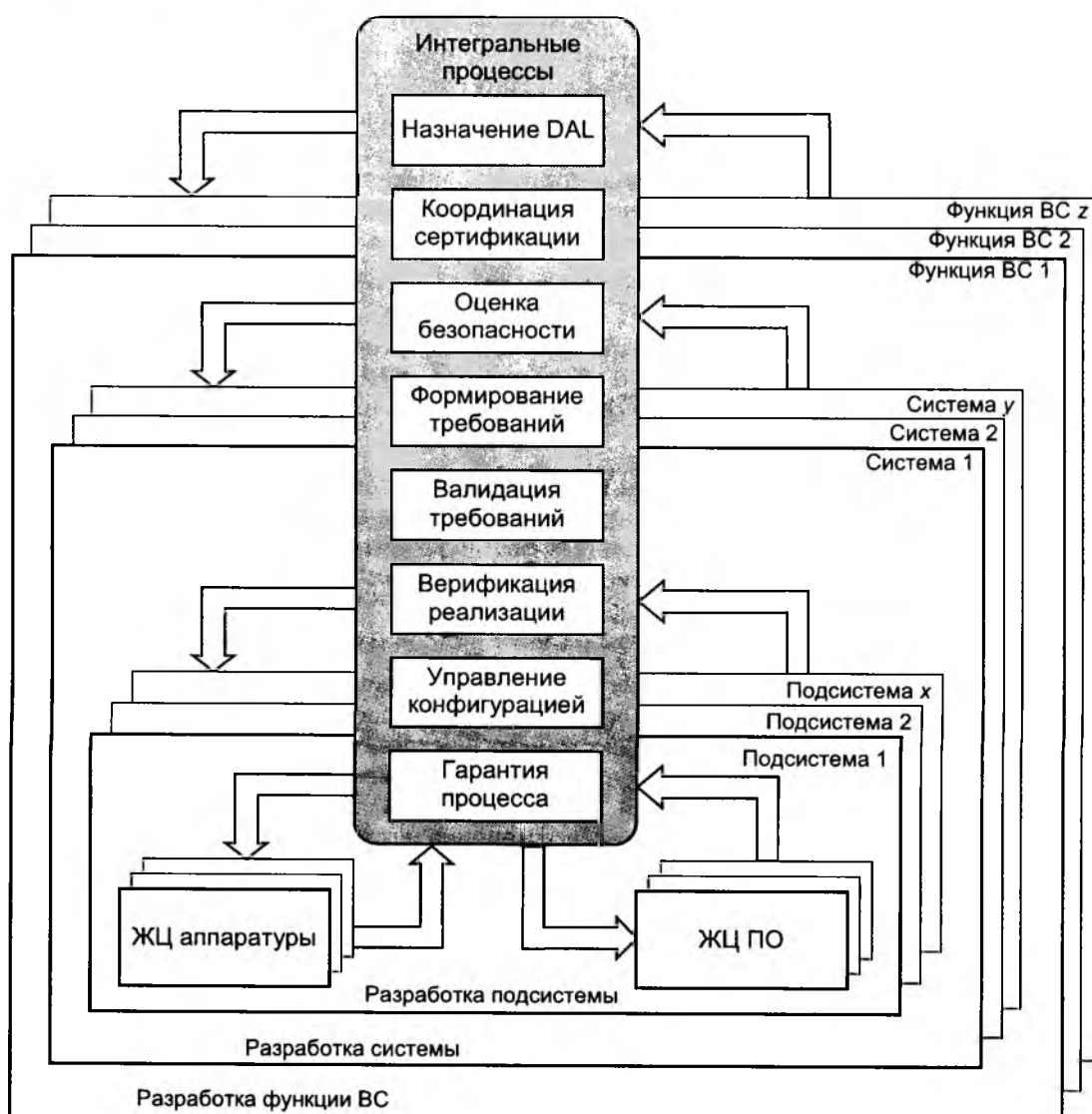


Рисунок 6. Процесс реализации функции BC

4.3 Распределение функций воздушного судна по системам

На этом уровне работа заключается в группировке функций ВС подходящим образом и распределении соответствующих требований по системам (включая требования из FNA воздушного судна). Выбор подходящей функциональной группировки из числа возможных часто бывает сложно сделать. Какие-либо специальные рекомендации по группировке в настоящем документе отсутствуют. Тем не менее особое внимание к лежащим в основе этого выбора решениям, с учетом соответствующих допущений, является важнейшим для успешности последующих процессов. Функциональные группы взаимосвязаны с архитектурой воздушного судна и являются основой для разработки архитектуры системы. Хотя для проведения функциональной группировки нет необходимости знать подробности реализации системы, учет ограничений реализации, учет влияния отказов и поддержка жизненного цикла могут играть важную роль при выборе оптимальных группировок. Распределение также должно определять входные данные, выполняемые процессы и их результаты и предусматривать аспекты поддержки эксплуатации. Допущения, сделанные в рамках этого процесса, становятся важной частью общей совокупности системных требований и требуют такой же валидации, как и прочие требования.

На основании распределения функций и соответствующих последствий отказов определяются конкретные требования к системе, необходимые для достижения целей безопасности. По мере учета различных комбинаций функций и их распределения по системам и по людям на этом этапе будут появляться производные требования и дополнительные допущения. Это, в свою очередь, может привести к изменению требований к функциям на уровне ВС.

Результатом этого мероприятия является набор требований для каждой системы воздушного судна и относящихся к ней интерфейсов. Интерфейсы должны быть определены таким образом, чтобы у всех входных данных был источник, а у всех выходных данных – потребитель; это могут быть как другие системы, так и экипаж/персонал.

4.4 Разработка архитектуры системы

Архитектура системы определяет структуру и границы, в которых выполняются проектирование и реализация отдельных элементов для соблюдения всех установленных требований. Для реализации можно рассматривать несколько вариантов архитектуры. Они подлежат оценке с использованием таких факторов, как технологическая оснащенность, план-график разработки, производственная технологичность, контрактные обязательства, экономические факторы, опыт предыдущего применения и готовность промышленности.

Затем рассматриваемые варианты архитектуры итерационно оцениваются с применением функционального анализа, анализа характеристик, процесса предварительной оценки безопасности воздушного судна (PASA), предварительной оценки безопасности систем (PSSA) и анализа общей причины (CCA) для определения возможности соблюдения установленных для системы функциональных требований и требований безопасности высшего уровня. Рекомендации по проведению PASA/PSSA и CCA приведены соответственно в разделах 5.1.2 и 5.1.4 данного документа.

Производные требования, продиктованные технологией, архитектурой, интерфейсами систем и элементов либо выбором реализации, становятся ясно видимыми по мере разработки архитектуры системы. Потенциальное влияние производных требований на требования более высокого уровня нуждается в оценке.

Результатом этого мероприятия является описание архитектуры системы с детализацией до уровня элементов, а также распределение требований высшего уровня к функциям системы и соответствующих им требований безопасности более низких уровней. Должны быть включены требования, определяющие интерфейсы элементов, ограничения системы (физические, связанные с окружающей средой и т.д.) и интеграцию.

4.5 Распределение системных требований по элементам

На практике разработка архитектуры системы и распределение требований к системе на требования к элементам являются взаимосвязанными и итеративными процессами. С каждой итерацией определение и понимание производных требований улучшается, а основания для распределения требований к системе и их отнесения к ПО или аппаратуре становятся более очевидными. Процесс считается завершенным, когда для всех требований найдено место в окончательной архитектуре. Декомпозиция и распределение требований по элементам должны также обеспечить возможность демонстрации того, что элемент полностью реализует отнесенные к нему требования.

Производные требования, появляющиеся в ходе распределения, могут относиться к системе или к ее элементам. Соответственно верификация реализации распределенных требований может быть выполнена либо на уровне системы, либо на уровне элемента.

Результатом такого распределения являются требования, отнесенные к аппаратуре с учетом соответствующих целей безопасности и уровней гарантии разработки, а также отнесенные к программному обеспечению, включая уровни гарантии разработки для каждого элемента. Требования, обеспечивающие интеграцию аппаратуры и программного обеспечения, также должны быть включены при необходимости. Результаты этого мероприятия используются также для уточнения предварительной оценки безопасности системы.

4.6 Реализация системы

Реализация системы имеет четыре основных аспекта:

- a) информационный поток из процессов ЖЦ системы в процессы ЖЦ аппаратуры и программного обеспечения и в обратном направлении;
- b) разработка аппаратуры и программного обеспечения и их сборка;
- c) интеграция аппаратуры и программного обеспечения;
- d) интеграция системы.

Эти аспекты подробно описаны в следующих ниже подразделах.

4.6.1 Информационный поток из процессов ЖЦ системы в процессы ЖЦ элемента и обратно

4.6.1.1 Информационный поток из процессов ЖЦ системы в процессы ЖЦ аппаратуры и программного обеспечения

Требования к системе декомпозируются и распределяются по аппаратуре и/или программному обеспечению в соответствии с архитектурой системы. Декомпозиция и распределение требований по аппаратуре и/или программному обеспечению проводится в рамках процессов системы. Интерфейс между процессом системы и процессами аппаратуры и программного обеспечения описан в следующих разделах.

Момент, когда требования отнесены к аппаратуре и программному обеспечению, является также моментом перехода от инструктивных материалов настоящего документа к инструктивным материалам КТ-178 (для программного обеспечения), КТ-254 (для аппаратуры) и другим существующим отраслевым инструктивным материалам. В настоящем документе приведены инструктивные материалы по архитектуре, уровням гарантии разработки и функциональной декомпозиции, включая управление избыточностью (в том числе резервированием). Это означает, что распределение требований по аппаратуре и программному обеспечению завершено тогда, когда завершены архитектура, управление избыточностью и декомпозиция требований.

Следующие данные передаются в процессы программного обеспечения и аппаратуры в ходе распределения требований:

- a. Требования, отнесенные к аппаратуре
- b. Требования, отнесенные к программному обеспечению
- c. Уровни гарантии разработки элементов и описание соответствующих отказных состояний, если необходимо
- d. Заданные интенсивности отказов и интервал(ы) между отказами для аппаратуры
- e. Описание системы
- f. Проектные ограничения, включая изоляцию функций, обособление, данные/модели внешних интерфейсов и требований по обособлению и любые требования независимости проектирования элемента
- g. Мероприятия верификации системы, которые должны быть выполнены на уровне разработки программного обеспечения или аппаратуры, если это применимо
- h. Свидетельство приемлемости любых данных, переданных от процессов ЖЦ аппаратуры и программного обеспечения в процессы ЖЦ системы, если эти данные участвуют в мероприятиях или оценке в рамках процессов системы. Примером такого мероприятия является оценка производных требований, появившихся в процессе разработки программного обеспечения, для выявления какого-либо влияния на SSA.

4.6.1.2 Информационный поток из процессов в процессы ЖЦ аппаратуры и ПО в процессы ЖЦ системы реализации системы

Приведенная ниже информация должна быть включена в состав данных, передаваемых в процессы ЖЦ системы для обеспечения мероприятий разработки и интегральных процессов на уровне системы:

- a. Производные требования (и к аппаратуре, и к программному обеспечению) для оценки их влияния на требования к системе или элементам и на результаты оценок безопасности
- b. Описание реализованной архитектуры аппаратуры и программного обеспечения, которое в достаточной степени отображает достигнутую независимость и способность ограничивать распространение последствий неисправностей (в частности, изоляция аппаратуры и обособление программного обеспечения)
- c. Свидетельства проведения мероприятий верификации системы/элемента, проведенных на уровне разработки программного обеспечения и аппаратуры, если они имеются
- d. Данные для аппаратуры по интенсивности отказов, полноте обнаружения отказов, анализу общих причин и времени задержки проявления отказа для применения в SSA
- e. Документация, описывающая проблемы или изменения, которые могут отразиться на требованиях к системе, или к элементам, либо на производных требованиях к аппаратуре и программному обеспечению, для оценки их влияния на требования к системе или элементам и на результаты оценок безопасности
- f. Любые ограничения в использовании, ограничения идентификации или состояния конфигурации, эксплуатационных и временных характеристик, а также характеристик точности
- g. Данные, способствующие интеграции аппаратуры и программного обеспечения в систему (например, установочные чертежи, схемы, спецификации)
- h. Описание мероприятий верификации аппаратуры и программного обеспечения, которые предлагается провести в рамках верификации на уровне системы.

Кроме того, должны быть предоставлены свидетельства того, что проведенные мероприятия процессов отвечают назначенным элементам уровнями гарантии разработки, включая любые гарантии, полученные с помощью инструментов.

4.6.1.3 Информационный поток между процессами жизненного цикла конструирования аппаратуры и жизненного цикла программного обеспечения

Приведенная ниже информация должна быть включена в состав данных, передаваемых между процессами жизненных циклов аппаратуры и программного обеспечения. Эта информация должна передаваться через процессы системы. В нее входят:

- a. Производные требования, необходимые для интеграции аппаратуры и программного обеспечения, в частности, определение протоколов, временные ограничения и схемы адресации для обеспечения взаимодействия между аппаратурой и программным обеспечением
- b. Описание случаев, в которых необходима координация мероприятий верификации аппаратуры и программного обеспечения
- c. Выявленные случаи несовместимости аппаратуры и программного обеспечения, как часть процесса управления изменениями.

4.6.2 Разработка и сборка аппаратуры и программного обеспечения

Процессы разработки и сборки аппаратуры и программного обеспечения должны поддерживать трассируемость до требований, отнесенных к аппаратуре и программному обеспечению. Если реализация аппаратуры и программного обеспечения проходит параллельно с распределением требований и определением архитектуры, то разработчики должны проявить достаточный уровень дисциплинированности для обеспечения того, что производные требования определены и все функциональные требования выполнены при реализации.

Выходные данные этого этапа включают процедуры интеграции аппаратуры и программного обеспечения, выпущенные чертежи аппаратуры, исходный код программного обеспечения вместе с другими данными ЖЦ ПО, необходимые данные гарантии разработки, макеты или прототипы аппаратуры, если они применяются, а также отчеты о лабораторных и летных испытаниях. Документы, на которые есть ссылки в разделах 2.1.4 и 2.1.5, содержат инструктивные материалы по разработке аппаратуры и программного обеспечения.

4.6.3 Интеграция аппаратуры и программного обеспечения

В зависимости от характера системы и применяемого процесса разработки первоначальная интеграция элементов аппаратуры и программного обеспечения может осуществляться на макетах, прототипах, путем компьютерной эмуляции, а также на лабораторных или летных образцах. Результатом является оборудование, находящееся под контролем конфигурации, а также данные по гарантии разработки и данные жизненного цикла аппаратуры и программного обеспечения. Созданные в рамках процесса разработки и сборки детализированные процедуры должны быть использованы для верификации выполнения требований к интеграции аппаратуры и программного обеспечения.

Можно улучшить процесс интеграции аппаратуры и программного обеспечения путем разработки документации на интерфейсы. Это могло бы помочь убедиться в том, что аппаратура и программное обеспечение поддерживают совместное функционирование (в частности, правильную инициализацию аппаратуры, карт памяти и т.п.).

4.6.4 Интеграция систем на уровне воздушного судна

Обычно интеграция систем начинается с интеграции элементов и продолжается до получения интегрированной системы. Поскольку полностью предусмотреть или смоделировать условия эксплуатации ВС трудно, это может привести к необходимости осуществить некоторые мероприятия по интеграции на борту воздушного судна. Хотя достоверность результатов интеграции на борту воздушного судна обычно считается высокой, более значимые или менее дорогостоящие результаты часто достигаются в лабораторных условиях или на эмуляторах. В пределах авиационной отрасли процедуры интеграции систем отличаются большим разнообразием.

Во время процесса интеграции обо всех обнаруженных несоответствиях следует сообщать обратно в породившие их процессы разработки и в интегральные процессы (формирование, распределение и валидация требований, реализация, верификация и т.п.) для их устранения и повторения процесса интеграции. Результатом завершения всех итераций является верифицированная интегрированная система, данные которой демонстрируют ее полное соответствие функциональным требованиям и требованиям безопасности.

Задачей интеграции систем на уровне ВС является обеспечение надлежащего функционирования авиационных систем по отдельности и совместно при установке на борт воздушного судна. Это позволяет обеспечить демонстрацию того, что межсистемные требования, вместе взятые, выполнены. Также это позволяет обнаружить и удалить нежелательные непредусмотренные функции.

5 ИНТЕГРАЛЬНЫЕ ПРОЦЕССЫ

Процессы, описанные в данном разделе, являются неотъемлемой частью всего процесса. Они в значительной степени взаимосвязаны с задачами процесса, описанного в разделе 4.1.

5.1 Оценка безопасности

Процесс оценки безопасности используется компанией для подтверждения соответствия сертификационным требованиям (в частности, Авиационным правилам, Части 23 и 25, раздел 1309) и соблюдения собственных внутренних стандартов безопасности. Процесс содержит отдельные мероприятия оценки, проводимые и обновляемые при разработке системы, включая взаимодействие с другими процессами разработки системы. Подробное описание основных процессов оценки безопасности приведено в P-4761 и обобщено ниже.

- a. Оценка функциональной опасности (FHA): оцениваются функции воздушного судна и систем для выявления потенциальных функциональных отказов и проводится классификация опасностей, связанных с конкретными отказными состояниями. FHA проводится на ранних стадиях процесса разработки, затем обновляется при выявлении новых функций или отказных состояний. Таким образом, результаты FHA представляют собой постоянно актуализируемый в течении всего цикла разработки документ.
- b. Предварительная оценка безопасности воздушного судна/Предварительная оценка безопасности системы (PASA/PSSA): устанавливает требования безопасности для воздушного судна или отдельных систем и элементов и обеспечивает предварительное подтверждение того, что предлагаемая архитектура воздушного судна или системы может обеспечить удовлетворение этих требований. Обновление PASA и PSSA производится в течение всего процесса разработки системы, что в итоге завершается формированием Оценки безопасности воздушного судна и Оценки безопасности системы.
- c. Оценка безопасности воздушного судна/Оценка безопасности системы (ASA/SSA): сбор, анализ и документирование результатов верификации того, что реализованная конструкция воздушного судна и его систем соответствуют требованиям по безопасности, установленным в PASA и PSSA.
- d. Анализ общих причин (CCA): устанавливает и верифицирует требования физического и функционального разделения, изоляции и независимости между системами и элементами и верифицирует соответствие данным требованиям.

Дополнительно, для надлежащего управления процессом оценки безопасности должен быть разработан План-программа безопасности. Выявленные в FHA отказные состояния также могут отслеживаться в рамках процесса разработки для поддержания постоянного соответствия критериям безопасности при реализации проекта.

На рисунке 7 приведены основные взаимосвязи перечисленных четырех отдельных мероприятий оценки и процесса разработки систем. В действительности существует множество контуров обратной связи внутри взаимосвязей и между этими взаимосвязями, которые для простоты не приведены на рисунке.

Уровень детализации различных видов оценок безопасности зависит от классификации отказных состояний на уровне воздушного судна, степени интеграции и сложности реализации системы. Процесс оценки безопасности должен планироваться и управляться так, чтобы была обеспечена необходимая гарантия того, что все релевантные отказные состояния выявлены и что все значимые сочетания отказов, которые могут быть причинами таких отказных состояний, учтены. Процесс оценки безопасности имеет первостепенную важность при определении соответствующих целей в обеспечении безопасности воздушного судна и систем и установлении того, что реализация соответствует этим целям.

Мероприятия оценки безопасности кратко описаны в приведенных ниже разделах настоящего документа.

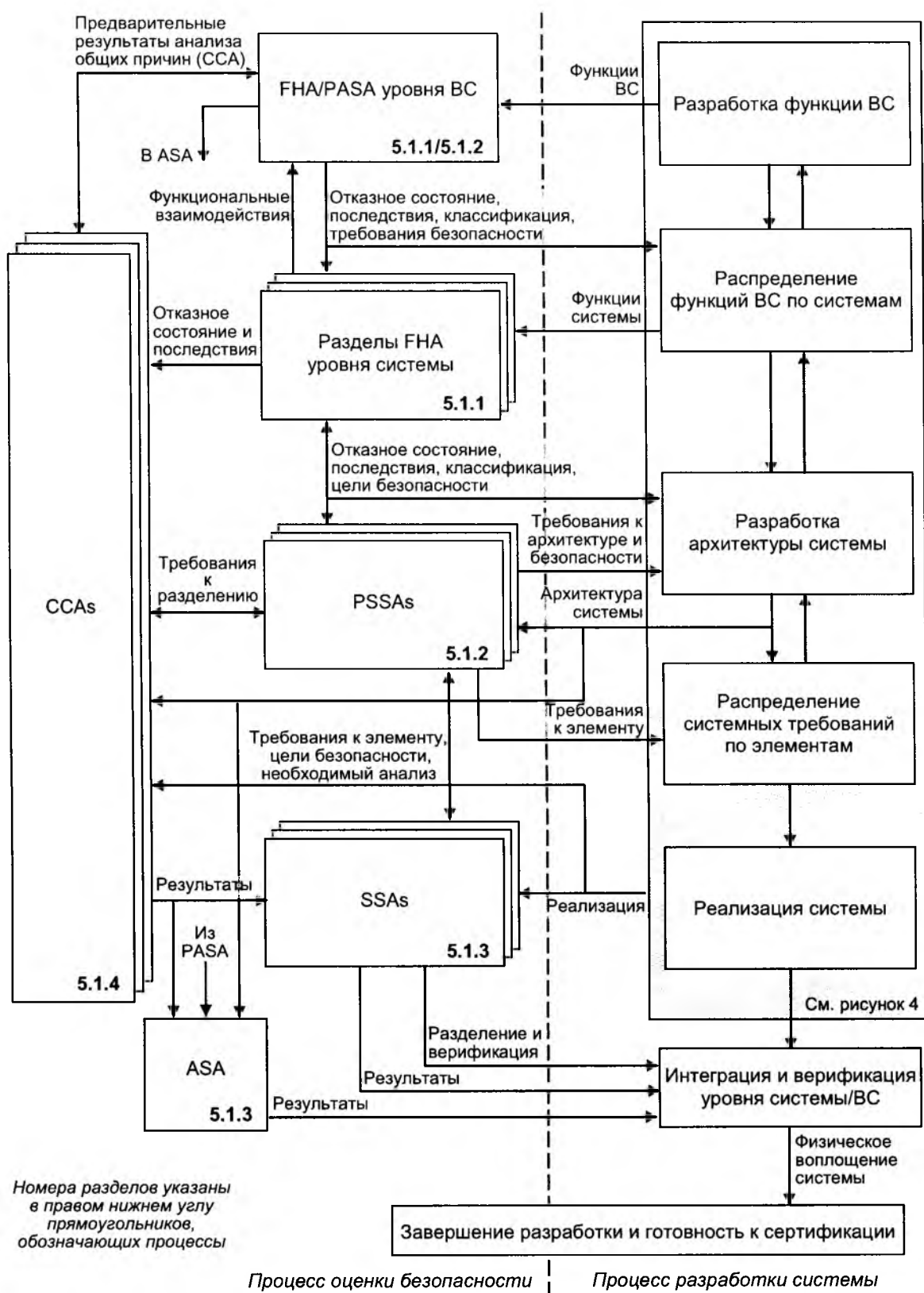


Рисунок 7. Схема процесса оценки безопасности

5.1.1 Оценки функциональной опасности

Оценки функциональной опасности (ФНА) проводятся на уровне воздушного судна и на уровне системы. Они должны обеспечить следующую информацию, относящуюся к каждой функции (на уровне воздушного судна и системы соответственно):

- a. Идентификация соответствующих отказных состояний
- b. Идентификация последствий отказных состояний
- c. Классификация отказных состояний на основе указанных последствий (а именно, Катастрофические, Аварийные, Сложные, Усложнение условий полёта и Не влияющие на безопасность) и определение необходимых целей безопасности, как определено, в частности, в РЦ-АП-25.1309 с добавлением категории Не влияющих на безопасность
- d. Описание того, что учитывалось и какие допущения были приняты при оценке каждого отказного состояния (например, неблагоприятные эксплуатационные и окружающие условия и фаза полета).

Целью данного мероприятия является четкое определение условий и степени опасности каждого отказного состояния с обоснованием его классификации.

Поскольку использование общих архитектур и сложных компонентов для различных систем может приводить к дополнительным отказным состояниям на уровне воздушного судна, затрагивающим множество функций, при проведении ФНА необходимо выявить и классифицировать эти новые отказные состояния. Если функции на уровне воздушного судна выполняются одной системой или совместно несколькими системами, результаты ФНА необходимо пересмотреть для выявления и классификации отказных состояний, затрагивающих множество функций. Если ФНА проводится отдельно для каждой системы, необходимо обеспечить трассируемость опасностей и отказных состояний между уровнями воздушного судна и систем.

Варианты реализации, принятые в процессе разработки, могут привести к общим причинам многих отказных состояний на уровне воздушного судна или к взаимодействию систем, приводящему к отказу. Эти общие причины могут выходить за рамки системы или функции. Должно быть проведено рассмотрение реализации систем для выявления таких отказных состояний и необходимости их учета в ФНА на уровне воздушного судна.

Подробное описание ФНА на уровне воздушного судна или системы приведено в Приложении А Р-4761.

5.1.2 Предварительная оценка безопасности воздушного судна/системы

Предварительная оценка безопасности воздушного судна/системы (PASA/PSSA) представляет собой запланированный анализ предлагаемых архитектур с целью определения того, как отказы могут привести к отказным состояниям, выявленным в ходе в ФНА. Целью проведения PASA и PSSA является обеспечение соответствия требованиям безопасности воздушного судна, системы или элемента, а также оценка соответствия предлагаемой архитектуры требованиям безопасности. По итогам PASA/PSSA может быть определена необходимость применения альтернативных стратегий защиты (в частности, обособление, встроенный контроль, мониторинг, независимость и интервалы проведения технического обслуживания и т.п.). Результаты PASA/PSSA следует использовать в качестве входных данных для ASA/SSA и других документов, включая как минимум требования к системе и требования к программному обеспечению и аппаратуре.

Оценки PASA/PSSA являются итерационными процессами, связанными с проектированием. Они проводятся на нескольких стадиях разработки системы, включая проектирование воздушного судна, систем и элементов. На самом нижнем уровне PSSA определяет требования к программному обеспечению и аппаратуре, связанные с безопасностью.

Подробное описание проведения предварительной оценки безопасности воздушного судна/систем (PASA/PSSA) приведено в Р-4761, Приложение В.

5.1.3 Оценка безопасности воздушного судна/системы

Оценка безопасности воздушного судна/системы (ASA/SSA) представляет собой систематическую всестороннюю оценку реализованной конструкции воздушного судна и систем, с целью подтверждения соответствия предъявленным требованиям безопасности. Разница между PASA/PSSA и ASA/SSA в том, что PASA/PSSA является методом оценки предложенных архитектур и определения производных требований безопасности к системам/элементам, в то время как ASA/SSA – метод подтверждения того, что реализованная конструкция соответствует требованиям безопасности, определенным PASA и PSSA.

ASA/SSA объединяет результаты различных анализов верификации безопасности воздушного судна/системы в целом и соответствия всем специфическим требованиям безопасности, определенным PASA/PSSA. Данные процессов ASA/SSA включают результаты соответствующих анализов и их обоснования. Они могут включать следующую информацию:

- a. Перечень предварительно согласованных вероятностей внешних событий
- b. Описание системы, включая функции и интерфейсы
- c. Перечень отказных состояний (FHA, PASA, PSSA)
- d. Классификация отказных состояний (FHA, PASA, PSSA)
- e. Качественные анализы отказных состояний (в частности, FTA, FMES, Марковский анализ, диаграммы зависимости)
- f. Количественные анализы отказных состояний (в частности, FTA, FMES, Марковский анализ, диаграммы зависимости)
- g. Результаты, полученные при проведении анализа общих причин
- h. Задачи и интервалы, относящиеся к вопросам безопасности (FTA, FMES, Марковский анализ, диаграммы зависимости)
- i. Уровни гарантии разработки для функций воздушного судна и систем (FDAL) (PASA, PSSA)
- j. Уровни гарантии разработки для аппаратуры и программного обеспечения (IDAL) (PSSA)
- k. Верификация того, что требования безопасности PASA, PSSA реализованы в конструкции и/или процессах тестирования
- l. Результаты неаналитических проверочных процедур (в частности, тестирование, демонстрация и обзоры).

Оценка безопасности воздушного судна должна обеспечивать заключение по всем мероприятиям в части оценки безопасности воздушного судна от начала формирования концепции до завершения технического проектирования. Она предназначена для демонстрации соответствия требованиям и целям на уровне воздушного судна и обеспечения гарантии применения надлежащих методов и процессов. Оценка безопасности воздушного судна обеспечивает проверку того, что:

- все мероприятия обеспечения безопасности выполнены в соответствии с Планом безопасности;
- требования безопасности воздушного судна удовлетворены и соответствующая доказательная документация представлена;
- процессы верификации/валидации завершены и их результаты утверждены;
- все выполненные мероприятия образуют логическую цепочку доводов, позволяющую сделать вывод о безопасности воздушного судна.

Эти документы являются частью так называемых «дела безопасности» или «сводки безопасности». Дело безопасности или сводка безопасности формируют четкую, понятную и