Анализ безопасности

Для обеспечения соответствия нового самолета гражданской авиации требованиям по надежности и отказобезопасности (АП25, НЛГС и зарубежным аналогам) необходимо проводить анализ безопасности систем и оборудования воздушного судна (ВС) на всех этапах жизненного цикла. Процесс анализа и методы оценки безопасности систем и оборудования ВС определяются руководством Р4761 (ARP4761).

Процесс оценки безопасности начинается на этапе эскизного проекта ВС, для которого формируются требования по безопасности как к ВС в целом, так и к его составным компонентам (комплектующим изделиям), и завершается проверкой того, что комплекс бортового оборудования (КБО) в составе ВС соответствует требованиям по безопасности.

Взаимосвязь между основными процессами оценки безопасности и процессами проектирования системы приведена на рис. 3.4.

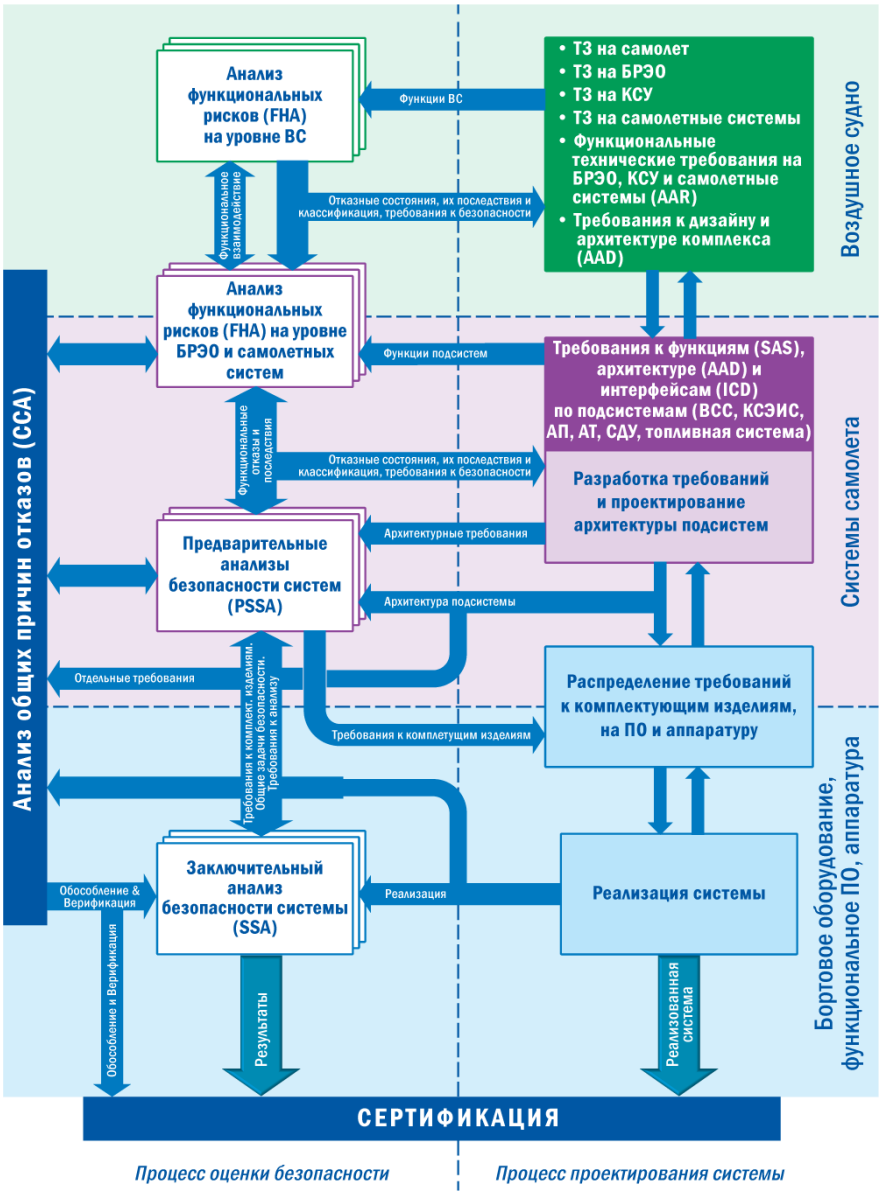

Рис. 3.4. Процесс оценки безопасности систем и оборудования самолета.

К основным процессам оценки безопасности КБО относятся:

1. Оценка функциональных опасностей — ОФО (Functional Hazard Assessment — FHA).

В ходе FHA рассматриваются функции ВС и его систем с целью определения их возможных отказов, а также проводится классификация опасностей связанных с ними отказных состояний.

FHA уровня ВС производится на ранней стадии проектирования и пересматривается по мере появления новых функций или отказных состояний.

После распределения функций ВС в процессе проектирования по системам каждая система или их комбинация, которая объединяет несколько функций самолета, должна быть исследована с использованием процесса FHA уровня системы. ОФО будут повторяться при рассмотрении единичных отказов или комбинаций отказов функций уровня самолета, которые будет выполнять такая система.

Результатом FHA каждой функции ВС, а также их комбинации является:

- идентификация соответствующих отказных состояний;
- идентификация последствий отказных состояний;
- классификация каждого отказного состояния в зависимости от последствий и назначение требуемых показателей безопасности;
- идентификация требуемых уровней гарантии проектирования.

2. Предварительная оценка безопасности системы (Preliminary System Safety Assessment — PSSA).

Результаты FHA используются как исходные данные для проведения PSSA, в ходе которой устанавливаются конкретные требования к безопасности системы и составляющих ее изделий, а также дается первоначальное подтверждение того, что предполагаемая архитектура системы сможет удовлетворить эти требования. Предварительная оценка безопасности уточняется в процессе проектирования системы.

PSSA может выполняться в форме:

- анализа дерева неисправности (FTA);
- анализа логической схемы (DD);
- марковского анализа (MA).

3. Оценка безопасности систем (System Safety Assessment — SSA).

В ходе SSA собираются, анализируются и документируются доказательства того, что реализованная система удовлетворяет количественным и качественным требованиям безопасности, установленным в процессах FHA и PSSA.

SSA объединяет результаты различных анализов для проверки безопасности системы в целом с учетом охвата всех конкретных особенностей обеспечения

безопасности, определенных в PSSA. Процесс документирования SSA при необходимости включает доказательства и результаты уместных анализов.

Выходной документ SSA может содержать следующую информацию для каждой системы КБО:

- перечень одобренных ранее вероятностей внешних отказных событий;
- описание системы;
- перечень отказных состояний (FHA, PSSA);
- классификацию отказных состояний (FHA, PSSA);
- качественный анализ отказных состояний (FTA, DD, MA);
- количественный анализ отказных состояний (FTA, DD, MA, FMES);
- анализ общих причин отказов (CCA);
- задачи обеспечения безопасности и интервалы времени (FTA, DD, MA, FMES);
- уровни гарантии разработки для аппаратных и программных средств (PSSA);
- верификацию того, что требования по безопасности из PSSA учтены в конструкции и/или в процессе испытаний;
- результаты испытаний, демонстрации, инспекционные действия для проверки реализации требований к безопасности (FHA, PSSA).

4. Анализ общих причин отказов (Common Cause Analysis — CCA).

Для удовлетворения требований по безопасности может потребоваться обеспечение независимости между функциями, системами или оборудованием КБО. Следовательно, требуются гарантии, что такая независимость существует, или, что риск, связанный с наличием зависимости, считается приемлемым. Анализ CCA предлагает методы для проверки такой независимости и/или для выявления конкретных зависимостей. В ходе анализа CCA устанавливаются и оцениваются требования по физическому и функциональному разделению и изоляции комплектующих КБО (включая задачи обособления функционального ПО ИМА), а также проверяется, как эти требования выполняются.

В частности, CCA определяет отдельные виды отказов или внешние события, которые могут привезти к катастрофическим (КС), аварийным (АС) или сложным отказным состояниям (СС). Такие отказы (события) должны быть предотвращены для катастрофических отказных состояний и должны иметь назначенную вероятность для аварийных/сложных отказных состояний.

Анализ CCA включает следующие виды оценок безопасности:

- анализ зонной безопасности (ZSA);
- анализ специфических рисков (PRA);
- анализ общих режимов (CMA).

Степень детализации различных оценок безопасности зависит от класса отказного состояния функции или функций ВС, степени интеграции и сложности реализации

системы. В частности, в процессе оценки безопасности следует принимать во внимание все взаимозависимости выбранной архитектуры или применение общих сложных компонентов при межсистемной или внутрисистемной интеграции. Процесс оценки безопасности должен планироваться и управляться таким образом, чтобы обеспечить необходимые гарантии выявления всех отказных состояний и рассмотрения всех существенных комбинаций отказов, вызывающих эти отказные состояния. Процесс оценки безопасности имеет первостепенную важность для установления соответствующих показателей безопасности системы и определения соответствия реализованной системы этим требованиям.

На безопасность полёта также влияет **человеческий фактор**. Исследования, проведенные компанией Airbus, показывают, что опытные экипажи в нормальных условиях допускают от 3 до 5 ошибок в час (неправильный прием информации, выбор кнопок, пропуск радиовызова). В связи с этим разработчикам КБО следует принять во внимание результаты исследований, проведённых с целью выявления типов возможных ошибок, таких как:

- ошибки связи «воздушное судно — пилот»;
- постоянные и переменные ошибки;
- обратимые и необратимые ошибки;
- пропуски, промахи и ошибки;
- поведение, основанное на навыках, правилах, знаниях, и связанные с ними ошибки.

Помимо пропусков и ошибок, в летной практике существуют нарушения, возникающие в связи со стремлением пилота хорошо выполнить работу или же вследствие некомпетентности и лени.

Существуют три типа нарушений, которые должны учитывать разработчики КБО:

- Привычные — нарушения, ставшие нормой (экипаж считает, что процедура слишком сложна, и намеренно нарушает ее с целью упрощения задачи).
- Ситуативные — происходят под действием особых факторов, таких как: дефицит времени, высокая рабочая нагрузка или плохая эргономика кабины. В этом случае пилоты идут на нарушение с целью выполнения задачи (полета).
- Оптимизирующие — предполагают отказ от правил вообще. Иногда они не связаны с выполнением текущей задачи (например, использование своих возможностей пилотом с целью удовлетворения своих потребностей).