

ОЦЕНКА ФУНКЦИОНАЛЬНОЙ ОПАСНОСТИ

Седых К.В.¹, Громов В.С.²

¹Седых Константин Владимирович – кандидат технических наук, доцент;

²Громов Вадим Сергеевич – студент, магистр,
кафедра систем автоматического управления и контроля,
Национальный исследовательский университет
Московский институт электронной техники,
г. Зеленоград

Аннотация: в статье приведено описание процесса оценки функциональной опасности самолета. Приведен пример выполнения оценки функциональной опасности на уровне системы. Также приводится классификация отказных состояний и типовые примеры отказных состояний.

Ключевые слова: оценка функциональной опасности, ФНА, самолет, система, дерево неисправностей, функции системы.

Процесс оценки безопасности начинается на стадии эскизного проекта, на этой стадии формируются требования по безопасности. Далее, по мере развития проекта, в него вносятся изменения, уточнения и корректировки [1, с. 7].

Оценка функциональной опасности проводится в начале цикла разработки самолета или системы. Она позволяет определить и классифицировать отказные состояния, связанные с функциями самолета и комбинациями этих функций.

Целью оценки функциональной опасности (далее по тексту – ФНА) является рассмотрение функций, выявление и классификацию возникающих отказных состояний вследствие потери функции или неправильного выполнения функции.

ФНА выполняется на двух уровнях – на уровне самолета, и на уровне системы. Однако, выполняемые на этих двух уровнях ФНА, используют одни и те же принципы.

ФНА позволяет выявить отказные состояния для каждого этапа полета, если воздействия отказа и классификация состояний изменяется от одного этапа к другому. ФНА так же устанавливает требования по безопасности, которые позволяют ограничить воздействия нарушений функций влияющих на классификацию отказных состояний.

Для выполнения ФНА на приемлемом уровне, необходимо обладать полнотой знания и опыта. Так же выполнение ФНА может потребовать консультацию с большим числом специалистов.

Для примера, приведем функции высокого уровня и связанные вероятные отказы [1, с. 22].

Таблица 1. Пример функции и связанных отказных состояний

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

Отказы, приведенные в таблице 1, могут быть неоднократно разложены на более конкретные отказы, компоненты с использованием ФНА и деревьев неисправности.

Разложим, для примера, отказное состояние «невозможность управления траекторией полета» представлена на рисунке.

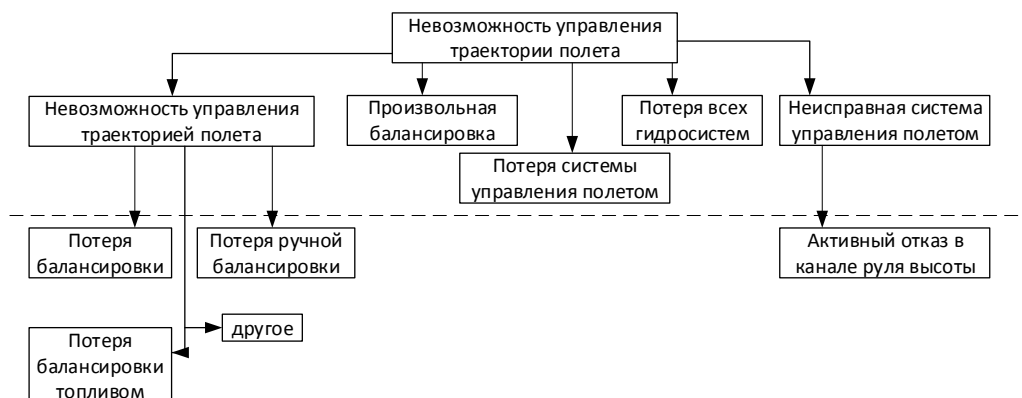


Рис. 1. Пример разложения отказного состояния

В результате должны быть определены все отказные состояния, влияющие на безопасность и предполагаемые методы оценки соответствия.

ФНА на уровне самолета используется для выявления таких возможных отказных состояний одновременно в нескольких системах, которые могут привести к более опасной квалификации результирующего отказного состояния (классификация отказных состояний см. таблица 0) [2, с. 31].

Таблица 2. Классификация отказных состояний

Классификация отказного состояния	Уровень гарантии проектирования системы
Катастрофическое	A
Аварийное	B
Сложное	C
Усложнение условий полета	D
Отсутствие влияния на безопасность	E

Для наибольшей эффективности первым шагом рекомендуется составить базовый перечень функциональных опасностей на уровне самолета, который мог бы использоваться в дальнейших проектах.

ФНА – это первый шаг в процессе оценки безопасности. ФНА устанавливает требования по безопасности для новой или модифицированной конструкции.

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

Порядок выполнения оценки:

1. Идентификация всех функции, относящихся к данному уровню рассмотрения.
2. Идентификация и описание отказных состояний, связанных с этими функциями.
3. Определение последствий отказных состояний.
4. Классификация отказных состояний по уровню последствий.
5. Составление требований к отказным состояниям, подлежащие рассмотрению на более низком уровне.
6. Определение вспомогательных материалов, необходимых для подтверждения классификации последствий каждого отказного состояния.
7. Выбор или составление методов проверки соответствия требованиям к отказным состояниям.

Формирование перечня одиночных отказов включает исследование первоначального перечня. Формирование перечня трудоемкой работой и требует понимания интеграции компонентов системы и взаимодействия анализируемой системы с другими самолетами. Множественные отказы рассматривают в тех случаях, когда последствие некоторого отказа зависит работоспособность другой системы.

Типичные отказные состояния:

1. Потеря функции.
2. Несигнализируемая потеря функции.
3. Неисправное выполнение функции.

Список литературы

1. Руководство 4761: По методам оценки безопасности систем и бортового оборудования воздушных судов гражданской авиации. // Изд. ОАО «Авиаиздат», 2011. 265 с.
2. Руководство Р4754. // Изд. ОАО «Авиаиздат», 2010. 80 с.