УДК 629.7.017 DOI: 10.31799/2077-5687-2022-4-44-51

МЕТОДИКА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРИ РАЗРАБОТКЕ СОВРЕМЕННОЙ АВИОНИКИ

М. П. Корельский
Санкт-Петербургский государственный университет аэрокосмического приборостроения
АО Институт Авиационного Приборостроения «Навигатор»

В статье предложена модель обеспечения безопасности, интегрированная в процесс разработки современной авионики. Рассмотрены основные методы обеспечения безопасности и описана последовательность их применения, способная гарантировать появление устройства, надежность которого будет на порядок выше надежности совокупности электронных компонентов.

Ключевые слова: безопасность полетов, надежность, авионика, гарантия разработки, оценка безопасности.

Для цитирования:
Корельский М. П. Методика обеспечения безопасности при разработке современной авионики // Системный анализ и логистика: журнал.: выпуск №4(34), ISSN 2007-5687. – СПб.: ГУАП., 2022 – с. 44–51. РИНЦ. DOI: 10.31799/2077-5687-2022-4-44-51.

SAFETY PROVIDING METHODS IN THE DEVELOPMENT PROCESS OF MODERN AVIONICS

M. P. Korelskiy
St. Petersburg State University of Aerospace Instrumentation
JSC Institute of Aviation Instrumentation «Navigator»

The article proposes the model of safety providing integrated into development process of modern avionics. The main methods of safety providing and the sequence of their application, which can guarantee the appearance of a device whose reliability will be an order of magnitude higher than the reliability of a combination of electronic components are considered.

Keywords: flight safety, reliability, avionics, development assurance, safety assessment.

For citation:
Korelskiy M. P. Safety providing methods in the development process of modern avionics // System analysis and logistics.: №4(34), ISSN 2007–5687. – Russia, Saint-Petersburg.: SUAI., 2022 –p. 44–51. DOI: 10.31799/2077-5687-2022-4-44-51.

Введение

Высокий темп развития технологий способствует непрерывному усложнению современной авионики. Обратной стороной процесса возрастания интеграции между различными функциями систем на борту летательного аппарата является увеличение критичности возникающих отказов [1]. Классические методы повышения безотказности при их грубом применении на уровне воздушного судна (ВС) хоть и позволяют достичь требуемых показателей, но в случае отсутствия запаса по массогабаритным характеристикам не применимы.

Для современных устройств, таких как система раннего предупреждения близости земли или система предупреждения столкновений в воздухе, вероятность полного отказа на летный час находится в диапазоне от 10-5 до 10-4. Уровень гарантии разработки устройств, отказ которых может привести к возникновению особо сложного состояния, должен быть не ниже уровня В (вероятность отказа на летный час не более 10-7) [2]. С позиции безопасности ставится задача обеспечить требуемую вероятность отказа не самого устройства, а выполняемых им функций. Это позволяет сконцентрировать внимание на определенных структурных элементах разрабатываемого изделия, причем изменения могут вноситься на разных системных уровнях. Так как вносимые архитектурные ослабления или усиления будут обоснованы количественно и могут применяться на разной глубине рассмотрения системы, то

вероятность отказа определенной функции системы может быть значительно меньше вероятности отказа самой системы или совокупности конструктивно-сменных блоков, реализующих эту функцию.

На практике часто встречается ситуация, когда процесс оценки безопасности начинается на заключительных этапах разработки системы. Соответствие предъявляемым требованиям безопасности в такой ситуации становится скорее производственной необходимостью, чем результатом спланированной деятельности, что отрицательно сказывается на качестве и глубине проводимого анализа системы.

Применение методики обеспечения безопасности, описанной в данной статье, поможет обеспечить соответствие разрабатываемой авионики требуемому уровню гарантии разработки за счет проведения анализа и оценки выполняемых функций с позиции безопасности на протяжении всего процесса разработки, а также значительно упростит процесс сертификации оборудования. Важно отметить, что методы обеспечения безопасности сами по себе не способны обеспечить требуемую вероятность возникновения опасных отказных состояний, но позволяют как можно раньше выявить эти опасности, предпринять требуемые меры и получить гарантию того, что существующий риск является приемлемым.

Модель обеспечения безопасности

Стандартная модель процесса разработки системы представлена на рисунке 1 [3]. Последовательность разработки системы «сверху вниз», начиная с определения требуемой функции воздушного судна, обеспечивает удобную концептуальную модель процесса разработки системы.

Рис.1. Модель процесса разработки системы

На этапе разработки функций ВС для каждой функции назначается уровень гарантии разработки (DAL), определяющий задачи и степень строгости процесса разработки, тип и количество рабочих материалов, появляющихся в результате разработки, которые необходимо сохранить, уровень независимости, который необходимо поддерживать при поведении разработки, объем и тип верификации, которую необходимо провести при проектировании. Выделенные функции, требования к ним, а также любые их изменения подлежат валидации и оценке их влияния на безопасность.

Далее выполняется распределение функций уровня ВС по системам. Для каждой системы также назначается уровень гарантии разработки. Для авиационных электронных бортовых систем устанавливается пять уровней гарантии разработки, которые обозначаются буквами с A по E [4]. При этом уровень A соответствует наиболее строгим требованиям, а E – наименее строгим.

В результате выполнения этапа разработки архитектуры появляется описание системы с детализацией до уровня элементов, а также производные требования, определяющие интерфейсы системы, ограничения и уровень интеграции между функциями. На практике разработка архитектуры системы и распределение системных требований на требования к элементам являются взаимосвязанными и итеративными процессами. С каждой итерацией определение и понимание требований улучшается, а основания для распределения требований к системе на требования к аппаратному и программному обеспечениям становятся более очевидными.

Этап реализации системы включает в себя обмен информацией между процессами жизненного цикла системы, аппаратного и программного обеспечений, разработку аппаратуры, программного обеспечения и их сборку, интеграцию аппаратуры и программного обеспечения и интеграцию системы на уровне воздушного судна.

Каждый этап представленной модели может включать в себя множество повторяющихся циклов, состоящих из интегральных процессов. Интегральные процессы в реальном цикле разработки могут выполняться параллельно и приводить к изменению ранее установленных требований не только для рассматриваемого уровня, но и более высоких. Качество их выполнения вносит существенный вклад в обеспечение безопасности и требуемого уровня гарантии разработки.

Процесс оценки безопасности включает в себя применение следующих методов:

1. Оценка функциональных опасностей (functional hazard assessment – FHA);
2. Анализ общих причин (common cause analysis – CCA);
3. Предварительная оценка безопасности (preliminary system safety assessment – PSSA);
4. Анализ/сводка видов и последствий отказов (failure modes and effects analysis/summary – FMEA/FMES);
5. Оценка безопасности (system safety analysis – SSA).

Модель обеспечения безопасности и информационного обмена между процессами разработки системы и обеспечения ее безопасности представлена на рисунке 2.

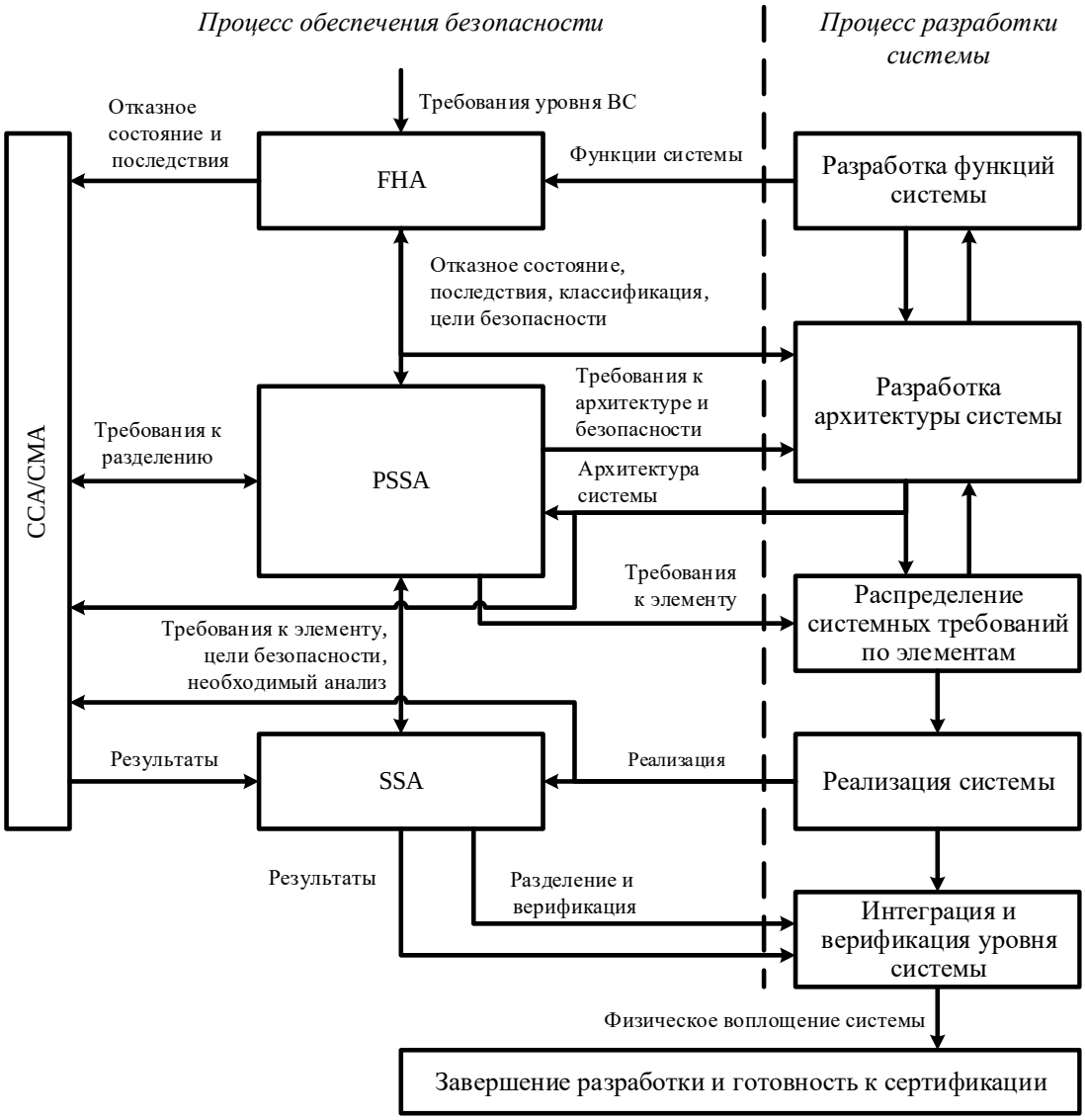

Рис. 2. Модель обеспечения безопасности

Для уровня воздушного судна требования безопасности формируются по результатам FHA воздушного судна и предварительного CCA и документируются в PSSA воздушного судна. Для уровней системы и элементов требования безопасности определяются из FHA и PSSA вышестоящего уровня. При выполнении инициативных разработок, когда требования безопасности верхнего уровня не заданы, разработчик должен самостоятельно или с привлечением экспертов, назначить уровень гарантии проектирования.

Важную роль при распределении требований выполняет валидация. Валидация – это процесс, который обеспечивает гарантию того, что производные требования полны и корректны [1]. Целью валидации является подтверждение того, что заданные для нижнего уровня требования полны и корректны на верхних уровнях. Когда требования распределены, с помощью анализа дерева неисправностей (fault tree analysis – FTA) и CCA выполняется анализ соответствия выбранной структуры ранее установленным требованиям, результат отражается в PSSA системы. При распределении требований на уровне системы вместо CCA разрешается выполнять только анализ общих режимов (common mode analysis – CMA).

Когда проектирование элементов завершено, для каждого уровня методами FMEA/FMES, CCA и FTA выполняется верификация того, что разработанные элементы соответствуют ранее установленным требованиям. Результаты верификации отражаются в

оценке безопасности системы.

Описанный порядок разработки системы неявно связан с существующими стадиями разработки конструкторской документации (КД), определенными в [5]. Документы по оценке безопасности не входят в комплект КД, а порядок и объем их разработки жестко не регламентирован и определяется по согласованию с сертифицирующим органом и разработчиком уровня ВС. В общем случае можно сказать, что первая итерация FHA системы выполняется на стадии разработки эскизного проекта, PSSA – на стадии разработки технического проекта, а SSA – на стадии разработки рабочей КД.

Методы обеспечения безопасности

Подробное описание методов обеспечения безопасности, а также примеров их применения является объемным и рассмотрено в [2]. В рамках данной статьи ограничимся кратким описанием этих методов, позволяющим понять их назначение и взаимосвязь.

Оценка функциональных опасностей выполняется с целью рассмотрения выполняемых системой функций на наиболее приемлемом уровне, выявления и классификации отказных состояний вследствие как потери функций, так и их неправильного выполнения [6]. FHA выполняется в следующем порядке:

1. Определяются все внутренние функции и функции обмена, относящиеся к уровню системы;
2. Определяются и описываются связанные с этими функциями одиночные и множественные отказы, возникающие в нормальных и аварийных условиях эксплуатации;
3. Определяются последствия отказов;
4. Отказы классифицируются в соответствии с их последствиями на уровне воздушного судна;
5. Назначаются требования к отказным состояниям, подлежащие рассмотрению на более низком уровне;
6. Определяются вспомогательные материалы, необходимые для подтверждения классификации последствий каждого отказного состояния;
7. Определяются методы проверки соответствия требованиям к отказным состояниям.

После выявления в FHA отказных состояний функций уровня системы при помощи анализа дерева неисправности, анализа логических схем (dependence diagram – DD) или марковского анализа (markov analysis – MA) исследуются причины их возникновения на нижних уровнях. FTA/DD/MA могут применяться в составе других методов и используются для назначения уровней гарантии разработки функций и элементов, оценки влияния изменений архитектуры или доказательства соответствия качественным или количественным требованиям безопасности. Выбор определенного метода среди перечисленных обусловлен характером решаемой задачи. Важно отметить, что для обеспечения требуемого уровня гарантии разработки выполнять анализ и проверять его должны разные сотрудники, что создает определенные требования к квалификации участников процесса разработки.

Анализ общих причин выполняется для выявления событий общей причины, которые могут привести к катастрофическим или особо опасным состояниям ВС. Причины возникновения катастрофических отказов должны быть устранены, а особо опасных – учтены в бюджете вероятности. CCA состоит из трёх методов: анализ зонной безопасности (zonal safety analysis – ZSA), анализ специфического риска (particular risks analysis – PRA) и анализ общего режима.

Целью ZSA является определение соответствия разрабатываемого оборудования зоне его размещения на ВС. В процессе анализа исследуется влияние на безопасность определенных внешних воздействующих факторов, характерных для данной зоны

размещения, влияние отказов системы на взаимодействующее оборудование и возможные опасности эксплуатационного характера, связанные с ошибками обслуживания.

Анализ специфического риска исследует влияние на безопасность внешних по отношению к рассматриваемой системе событий, которые могут нарушить независимость функций и воздействовать одновременно на несколько зон. Перечень рассматриваемых рисков составляется с учетом требований летной годности и известных экспериментальных воздействий на ВС или систему. Обычно в состав такого перечня включают пожар, удар молнии, электромагнитные поля высокой энергии, столкновение с птицей и т.д.

Анализ общего режима выполняется для проверки независимости И-событий в FTA/DD/MA. В нем исследуется воздействие ошибок проектирования, производства, обслуживания и отказы других компонентов системы на независимость событий, а также выполняется проверка целесообразности применения принципов резервирования и независимости. Например, объекты с общим аппаратным или программным обеспечениями, задействованные в выполнении разных функций, могут нарушать независимость рассматриваемых событий.

Предварительная оценка безопасности предназначена для определения того, как отказы существующей архитектуры могут приводить к функциональным опасностям, идентифицированным в FHA, и как требования FHA могут быть удовлетворены. PSSA включает в себя следующие процессы:

1. Формирование полного перечня требований безопасности (на основании FHA и CCA);
2. Определение соответствия существующей архитектуры и планируемого подхода к проектированию целям и требованиям безопасности;
3. Формирование требований безопасности для конструкции объектов более низкого уровня (вплоть до требований к аппаратному и программному обеспечениям), для размещения на самолете и для эксплуатации.

Результатами PSSA являются требования безопасности (DAL функций, элементов и количественные требования к вероятности возникновения функциональных отказов, распределенные бюджетированием вероятностей) [7].

Анализ видов и последствий отказов является систематическим методом анализа снизу-вверх, который предназначен для определения видов единичных отказов и оценки их влияния на вышестоящий уровень [2, 8]. FMEA может использовать как функциональный, так и поэлементный подходы, а также быть количественным и качественным. В случае, когда вероятность отказов, полученная при использовании функционального FMEA, обеспечивает соответствие бюджету вероятностей PSSA, выполнение поэлементного FMEA может не потребоваться. Обычно FMEA содержит следующую информацию:

1. Определение компоненты, сигнала и/или функции;
2. Виды отказов и соответствующие им интенсивности отказов (численные или по категориям);
3. Последствия отказа (для рассматриваемого уровня или более высокого);
4. Диагностируемость и методы обнаружения отказа;
5. Способ предотвращения отказа;
6. Фазы полета, на которых возникает отказ;
7. Уровень опасности последствий отказа (в соответствии с DAL).

Сводка последствий отказов FMES чаще всего формируется как продолжение FMEA и выполняется с целью группировки единичных видов отказов, которые приводят к одинаковым последствиям.

Оценка безопасности системы является методической всесторонней оценкой созданной системы и, в отличие от PSSA, служит для верификации того, что реализованная система

соответствует как качественным, так и количественным требованиям, установленным в FHA и PSSA. SSA обобщает результаты применения различных методов обеспечения безопасности и может содержать следующую информацию:

1. Перечень одобренных ранее вероятностей внешних событий;
2. Описание системы и выполняемых функций;
3. Перечень отказных состояний (FHA, PSSA);
4. Классификацию отказных состояний (FHA, PSSA);
5. Качественный и количественный анализ отказных состояний (FTA/DD/MA, FMES);
6. Анализ общих причин;
7. Уровни гарантии разработки для аппаратного и программного обеспечений (PSSA);
8. Верификация того, что требования безопасности учтены в конструкции и/или в процессе испытаний;
9. Результаты испытаний, демонстраций и т.д.

Движение процесса SSA представляет собой восходящую по иерархическим уровням верификацию требований безопасности. На нижнем уровне проверяются надежность аппаратного обеспечения, архитектурные требования, уровни гарантии разработки аппаратных средств и программного обеспечения, а также соответствие реализации производным требованиям.

Для расчета вероятностей отказов, рассматриваемых в FTA уровня печатных узлов, выполняется FMEA уровня печатных узлов, результаты которого излагаются в FMES. Результаты FMEA уровня блока суммируются в FMES блока для подтверждения вероятностей отказов, рассмотренных в FTA блока. Результаты FMEA уровня системы суммируются в FMES системы для подтверждения вероятностей отказов, рассмотренных в FTA системы. FTA и CCA уровня системы используются для проверки соответствия отказных состояний и вероятностей их возникновения требованиям FHA системы.

Заключение

Предложенная методика обеспечения безопасности может значительно повысить надежность и безопасность разрабатываемого оборудования. Её практическое внедрение на предприятии хоть и является трудоемким и дорогостоящим процессом, но позволит сделать отечественную авионику конкурентоспособной на зарубежных рынках. В настоящее время существуют значительные трудности в сертификации отечественного бортового оборудования и воздушных судов в международных органах, таких как FAA. Эти трудности вызваны различием процессов разработки отечественного и иностранного оборудования и их выходных документов. Применение описанной методики не только ускорит процесс сертификации, но и значительно сократит связанные с ним затраты за счет выявления и предупреждения некоторых ошибок проектирования еще на ранних этапах разработки.

СПИСОК ЛИТЕРАТУРЫ

1. Fulton R. Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254 / Fulton R., Vandermolen R. – Boca Raton: CRC Press, 2014. – 249 p.
2. SAE ARP4761. Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment. – Warrendale, PA: SAE, 1996. – 331 p.
3. SAE ARP4754A. Guidelines for Development of Civil Aircraft and Systems. – Warrendale, PA: SAE, 2010. – 115 p.
4. RTCA DO-254. Design Assurance Guidance for Airborn Electronic Hardware. – Washington, D.C.: RTCA Inc., 2000. – 137 p.
5. ГОСТ 2.103-2013. Стадии разработки. – Москва: Стандартинформ, 2019. – 10 с.

6. Н.Н. Смирнов Подход к формированию модели отказобезопасности воздушного судна / Н.Н. Смирнов, С.А. Кротов // Научный вестник МГТУ ГА. – 2015. – № 215. – С. 27 – 32.
7. А.С. Савельев Предварительная оценка безопасности функции отслеживания активными органами управления заданных сигналов от системы автоматического управления гражданского самолета / А.С. Савельев, Е.С. Неретин // CREDE EXPERTO: Транспорт, общество, образование, язык – 2020. – № 2. – С. 6 – 14.
8. ГОСТ 27.310-95. Анализ видов, последствий и критичности отказов. – Минск: Межгосударственный совет по стандартизации, метрологии и сертификации, 1997. – 14 с.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Корельский Максим Павлович –
Магистр кафедры аэрокосмических измерительно-вычислительных комплексов[1], инженер[2]
[1]Санкт-Петербургский государственный университет аэрокосмического приборостроения
190000, Санкт-Петербург, ул. Большая Морская, д. 67, лит. А
[2]АО Институт Авиационного Приборостроения «Навигатор»
199106, г. Санкт-Петербург, Шкиперский проток, д. 14, лит. З, к. 19
E-mail: fhtvjdu@gmail.com

INFORMATION ABOUT THE AUTHOR

Korelskiy Maksim Pavlovich –
MA student of the Department of Aerospace Measuring and Computing Complexes[1], engineer[2]
[1]Saint Petersburg State University of Aerospace Instrumentation
190000, St. Petersburg, st. Bolshaya Morskaya, 67, lit. A
[2]JSC Institute of Aviation Instrumentation «Navigator»
199106, St. Petersburg, Shkipersky protok, 14, lit. Z, build. 19
E-mail: fhtvjdu@gmail.com