УДК 519.718.4

ББК 39.56

МЕТОД ОПРЕДЕЛЕНИЯ ПОДХОДА ОТКАЗОБЕЗОПАСНОСТИ КРИТИЧЕСКОГО ОБОРУДОВАНИЯ НА ЭТАПЕ СИСТЕМНОГО ПРОЕКТИРОВАНИЯ*

Артем Сергеевич Савельев

аспирант[1], очное отделение, 3 курс, М7О-306А-18,

ведущий специалист по оценке безопасности [2]

[1]Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский авиационный институт (национальный исследовательский университет)»;

[2] ООО «Лаборатория безопасных систем»

Москва, Россия

artemsaveliev@inbox.ru

Евгений Сергеевич Неретин[1,2]

кандидат технических наук, доцент

[1]Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский авиационный институт (национальный исследовательский университет)»;

[2]филиал ПАО «Корпорация «Иркут» «Центр комплексирования»

Москва, Россия

e.s.neretin@mai.ru

Сергей Александрович Дяченко[1,2]

аспирант[1], очное отделение, 3 курс, М7О-306А-18,

инженер-конструктор 2 категории[2]

© Савельев А.С., Неретин Е.С., Дяченко С.А., Берсуцкая О.Д., Иванов А.С., 2020

[1]Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский авиационный институт (национальный исследовательский университет)»;
[2]филиал ПАО «Корпорация «Иркут» «Центр комплексирования»
Москва, Россия
sergey.dyachenko@ic.irkut.com
Оксана Дмитриевна Берсуцкая[1,2]
аспирант[1], очное отделение, 2 курс, М7О-206А-19,
Главный системный аналитик[2]
[1]Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский авиационный институт (национальный исследовательский университет)»;
[2]ООО «Лаборатория безопасных систем»
Москва, Россия
oksana.bersutskaya@advalange.com
Андрей Сергеевич Иванов[1,2]
аспирант[1], очное отделение, 3 курс, М7О-306А-18,
инженер-конструктор 2 категории[2]
[1]Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский авиационный институт (национальный исследовательский университет)»;
[2]филиал ПАО "Корпорация "Иркут" "Центр комплексирования"
Москва, Россия
andrey.ivanov@ic.irkut.com

Обеспечение безопасности полетов является приоритетом для разработчиков гражданских воздушных судов. В связи с этим, параллельно процессу разработки протекает процесс оценки безопасности, как на уровне самолета, так и на уровне его отдельной системы. Настоящая работа посвящена анализу потенциальных проблем, которые могут возникнуть в ходе выполнения

мероприятий, посвященных оценке безопасности систем на примере комплекса бортового оборудования и способов их решения. Данная работа является первой в цикле статей, посвященных разработке стратегии модельно-ориентированного подхода к оценке безопасности.

Ключевые слова: проектирование, гражданская авиация, бортовое оборудование, оценка безопасности, надежность, модельно-ориентированный подход.

* Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (РФФИ) в рамках научного проекта № 20-31-90028\20 «Применение модельно-ориентированного подхода к оценке безопасности гражданских воздушных судов на примере комплекса бортового оборудования», выполняемого в МАИ. Руководитель проекта – к. т. н., доцент Е. С. Неретин

METHOD FOR DETERMINING THE FAIL-SAFE PERFORMANCE OF CRITICAL EQUIPMENT AT THE STAGE OF SYSTEM ENGINEERING*

Artem Sergeevich Savel'ev
3rd year postgraduate student,
Lead Safety Assessor [2]
[1] Moscow Aviation Institute (National Research University);
[2] OOO «Laboratorija bezopasnyh sistem»
Moscow, Russia
artemsaveliev@inbox.ru
Evgenij Sergeevich Neretin [1,2]
Candidate of Technical Sciences, associate professor
[1] Moscow Aviation Institute (National Research University);
[2] branch of PAO "Korporacija "Irkut" "Centr kompleksirovanija"
Moscow, Russia
e.s.neretin@mai.ru
Sergej Aleksandrovich Djachenko [1,2]
3rd year postgraduate student,

design engineer
[1] Moscow Aviation Institute (National Research University);
[2] branch of PAO "Korporacija "Irkut" "Centr kompleksirovanija"
Moscow, Russia
sergey.dyachenko@ic.irkut.com
Oksana Dmitrievna Bersutskaya[1,2]
2nd year postgraduate student,
chief systems analyst [2]
[1] Moscow Aviation Institute (National Research University);
[2] OOO «Laboratorija bezopasnyh sistem»
Moscow, Russia
oksana.bersutskaya@advalange.com
Andrej Sergeevich Ivanov [1,2]
3rd year postgraduate student,
design engineer [2]
[1] Moscow Aviation Institute (National Research University);
[2] branch of PAO "Korporacija "Irkut" "Centr kompleksirovanija"
Moscow, Russia
andrey.ivanov@ic.irkut.com

To ensure the safety of flight operations is a priority for civil aircraft designers. In this connection, in parallel with the development, the assessment of safety takes place, both at the level of an aircraft and at the level of its separate system. The present paper is devoted to the analysis of potential problems which can arise during procedures of assessing the system safety on the example of onboard equipment and ways of their elimination. The paper is the first in a circle of articles devoted to developing a strategy of the model-based approach to safety assessment.

Key words: engineering, civil aviation, onboard equipment, safety assessment, reliability, model-based approach.

Введение

Развитие технических средств с повышающимся уровнем интеграции систем привело к необходимости систематизации имеющегося опыта разработки воздушных судов и их систем. Были разработаны основные руководства, определяющие процессы и мероприятия разработки воздушных судов, их систем, программного и аппаратного обеспечения: ARP/P-4754, ARP/P-4761, DO/КТ-254, DO/КТ-178. В поддержку им в настоящее время широко применяется модельно-ориентированный подход к разработке (МОПР). Основные принципы МОПР можно применять также и в процессе оценки безопасности, что на текущий момент не развито в достаточной степени и не регламентировано в нормативной документации.

Цикл работ будет посвящен разработке и реализации методологии модельно-ориентированной оценки безопасности (МОПОБ) на примере комплекса бортового оборудования гражданского самолета. По результатам выполнения данных работ ожидается разработка методологии процесса оценки безопасности бортовых систем гражданских воздушных судов с применением модельно-ориентированного подхода и результаты ее реализации на примере комплекса бортового оборудования. Значимость данных результатов заключается в повышении уровня безопасности вновь разрабатываемых бортовых систем отечественных гражданских воздушных судов за счет усовершенствования подходов, применяемых во всем мире и регламентированных международной нормативной документацией (SAE ARP/P-4761).

Целью исследования является повышение безопасности разрабатываемых изделий бортовых систем отечественных гражданских воздушных судов на примере комплекса бортового оборудования. Ожидается, что предлагаемые решения сократят время разработки и минимизируют риск негативного влияния человеческого фактора за счет использования МОПОБ. Для обеспечения данной цели исследования будут решены следующие целевые задачи:

− **Задача №1.** Разработка качественных и количественных методов выполнения специфических анализов безопасности, обеспечивающих обнаружение и предотвращение потенциальных существенных отказов на этапе проектирования.

− **Задача №2.** Разработка модели комплекса бортового оборудования для обеспечения валидации требований безопасности с использованием модельно-ориентированного подхода.

− **Задача №3.** Разработка средства автоматизации верификации отказных расчетных случаев с использованием алгоритмов компьютерной обработки графической и звуковой информации.

В настоящей статье детализируются поставленные целевые задачи, и анализируется текущее состояние их решения в России и мире.

Анализ целевой задачи №1

В настоящее время качественные и количественные методы оценки безопасности (анализ дерева отказов, анализ видов и последствий отказов) широко известны в инженерной практике и описаны как в нормативной документации (ARP/P-4761), так и во множестве научных трудов (например, в работах [Liang, 2017]). Многие работы посвящены реализации данных анализов с применением МОПОБ, в основном для решения задач этапа верификации (см. работы в анализе современного состояния исследований по анализу целевой задачи №2).

Однако, в большинстве работ не рассматривается процесс формирования и валидации требований безопасности, которые могут быть решены с применением МОПОБ. Также в большинстве работ опускают специфику анализа общих причин отказа. Ключевую роль играют качественные и перспективные количественные требования анализа общих причин отказа.

В ходе дальнейших исследований должны быть исследованы и предложены качественные и количественные методы модельно-ориентированной оценки безопасности для этапа формирования и валидации требований безопасности. В частности, анализ общих причин отказа.

Разработка качественных методов МОПОБ для этапа формирования и валидации требований (для анализа общих причин) позволит определять сечения критических и аварийных отказов, для которых будут сформированы соответствующие требования безопасности. В рамках данной задачи также должен быть разработан опросный чек-лист, позволяющий определить перечень источников общих причин (регламентированных нормами ARP/P-4761), по которым могут быть сформулированы требования независимости и разнородности.

Разработка количественных методов МОПОБ, включающих расчет вероятности отказа двух и более компонентов бортового оборудования, произошедшего из-за возникновения одной или нескольких общих причин. Данный метод позволит выполнять расчет вероятностей при анализе деревьев отказов со значительно большей точностью и устранить субъективизм при принятии решения о наличии или отсутствии независимости между компонентами бортового оборудования.

Ожидается, что будут решены следующие подзадачи:

− Разработка условных критериев для определения критичности отказных ситуаций;

− Разработка моделей отказов комплекса бортового оборудования;

− Валидация критичности оценки функциональных опасностей;

− Разработка методологии качественного и количественного анализа;

− Реализация методологии количественного анализа в программной среде;

− Апробация методологии количественного анализа на примере комплекса бортового оборудования.

Анализ целевой задачи №2

Модельно-ориентированный подход широко применяется при разработке бортового ПО. Для авиационной промышленности выпущен нормативный документ DO-331 / P-331. Однако область действия данного документа не распространяется на применение МОПОБ разрабатываемых изделий. Данное

направление является перспективным и активно развивающимся. Для разработки моделей для оценки безопасности был предложен ряд методологий. Их можно разделить на две группы: создание расширений существующих высокоуровневых языков моделирования и разработка новых языков. В рамках первого подхода можно выделить:

1) Расширение языка разработки и анализа архитектур AADL с помощью модели ошибок, описанного в работе [Brunel, 2017];

2) Использование данных по надежности при разработке моделей в Matlab/Simulink с последующей генерацией деревьев отказов и АВПО, описанного в работе [Shao, 2017];

3) Преобразование моделей, разработанных на языках SysML в деревья отказов [Munk, 2020].

В рамках второго подхода выделяются:

1) Язык моделирования SafeDeML, предназначенный для оценки безопасности сложных систем (применяемый в автомобильной промышленности, процессы оценки безопасности в которой схожи с процессами в авиационной промышленности), который описывается в работе [Gonschorek, 2019];

2) Язык AltaRica 3.0 – версия языка AltaRica, разработанная для выполнения оценки безопасности, которая описывается в работе [Batteux, Prosvirnova, Rauzy, 2013].

Развитие данного направления предполагает ожидать, что реализуемая методология будет независима от используемого языка моделирования. Она может быть ограничена только возможностями существующих инструментов моделирования. Однако предполагается, что данные инструменты могут быть доработаны, что позволит использовать все преимущества разрабатываемой методологии. Также разрабатываемая методология может быть применена при оценке безопасности любой системы самолета.

В ходе дальнейших исследований должны быть разработаны модели комплекса бортового оборудования (КБО) на языке SysML, т.к. существует

большое количество инструментов, поддерживающих данный язык моделирования. SysML широко применяется для высокоуровневого моделирования и поддерживает различные виды представления поведения систем, такие как: диаграммы деятельности, состояний, последовательностей, требований и параметрические. Это позволяет выполнять наиболее полное моделирование функционирования КБО.

Ожидается, что будут решены следующие подзадачи:

− Разработка модели архитектуры комплекса верхнего уровня (подсистемы и связи между ними);

− Разработка моделей подсистем КБО;

− Разработка моделей информационных потоков.

Анализ целевой задачи №3

На текущий момент среди методов верификации систем из состава комплекса бортового оборудования широко распространены методы формальной верификации и, в частности, model checking. Они основываются на верификации модели системы, состоящей из конечного числа состояний и выраженной на языке темпоральной логики. К числу решений для проведения формальной верификации относятся программные среды ANSYS SCADE и др. ([Formal Methods for Industrial, 2011; MATLAB & Simulink Design Verifier, 2014; Буздалов, 2014]).

Однако данная верификация направлена на проверку соответствия модели системы требованиям, описанным на формальном языке, и не учитывает особенностей работы на целевой платформе.

Для автоматизации верификации на стендах полунатурного моделирования используются программно-аппаратные средства, позволяющие контролировать потоки данных в кодовых линиях связи, развита автоматизированная обработка указанных данных, формирование отчетов по результатам испытаний. Примером подобного средства является программный диагностический комплекс «ФРЕГАТ» производства АО «УКБП» [Черкашин, 2009].

Однако существует ряд бортовых систем из состава комплекса бортового оборудования, для верификации которых требуется проведение визуального контроля отображаемых данных – в частности, для систем индикации в кабине экипажа. Аналогична ситуация с системами сигнализации, формирующими предупреждения для лётного состава в текстовой и звуковой формах. Указанные системы являются высоко критичными, их отказ может привести к катастрофической и аварийной ситуациям соответственно.

Средства автоматизации верификации данных систем, способные фиксировать и обрабатывать графическую и звуковую информацию, на данный момент не представлены на рынке. Однако алгоритмы обработки изображений и звука широко применяются в IT-сфере, медицине и др.

В рамках данной задачи планируется применить методы компьютерной обработки графической и звуковой информации для автоматизации верификации бортового ПО в рамках полунатурных испытаний с учетом требований нормативной документации к ПО бортовых систем гражданской авиации.

В частности, будет разработано программно-алгоритмическое обеспечение средства автоматизации, проведено его тестирование. Также будет разработана методика проведения испытаний с применением разработанного средства.

Это позволит увеличить долю испытаний с применением моделей динамики и функционирования оборудования (полунатурное моделирование) взамен летных испытаний, что отвечает принципам МОПОБ.

Для задачи разработки средства автоматизации верификации отказных расчетных случаев с использованием алгоритмов компьютерной обработки графической и звуковой информации планируется использовать методы системного анализа, компьютерного зрения (распознавание изображений), обработки информации. Применение данных методов сократит время разработки бортовых систем и минимизирует риск негативного влияния

человеческого фактора за счет использования автоматизированных процедур верификации в поддержку процессов МОПОБ.

Ожидается, что будут решены следующие подзадачи:

− Разработка программно-алгоритмического обеспечения;

− Тестирование разработанного программно-алгоритмического обеспечения;

− Разработка методики проведения испытаний с использованием разработанного средства.

Выводы

В ходе исследования будет разработана методика выполнения модельно-ориентированной оценки безопасности на примере разработки комплекса бортового оборудования.

Преимущества внедрения решения каждой задачи будут заключаться в следующем:

− Разработка качественных и количественных методов выполнения специфических анализов безопасности, обеспечивающих обнаружение и предотвращение потенциальных существенных отказов на этапе проектирования позволит переосмыслить рекомендательные материалы SAE ARP/P-4761 для использования современных методов разработки сложного оборудования – модельно-ориентированный подход;

− Разработка модели комплекса бортового оборудования для обеспечения валидации требований отказобезопасности с использованием модельно-ориентированного подхода позволит сократить время и экономические ресурсы для валидации требований безопасности во время проектирования;

− Разработка алгоритмов обработки графической и звуковой информации для автоматизации верификации отказных расчетных случаев позволит сократить временя и экономические ресурсы для верификации требований во время полунатурных испытаний.

Результаты работ должны помочь осуществить переход к передовым и новым способам конструирования в части разработки и оценки безопасности систем гражданских воздушных судов, что соответствует Стратегии научно-технологического развития Российской Федерации.

Библиографический список

1. *Буздалов Д. В.* Инструментальные средства проектирования систем интегрированной модульной авионики / Д. В. Буздалов, С. В. Зеленов, Е. В. Корныхин, А. К. Петренко, А. В. Страх, А. А. Угненко, А. В. Хорошилов // Труды Института системного программирования РАН. 2014. №1. Том 26. С. 201-230.
2. *Черкашин С. В.* Универсальная система диагностирования бортового радиоэлектронного оборудования / С. В. Черкашин, В. В. Шишкин, Н. А. Долбня // Известия Самарского научного центра Российской академии наук. 2009. Т. 11. № 3-2. С. 392-397.
3. Batteux Michel The AltaRica 3.0 project for Model-Based Safety Assessment / Michel Batteux, Tatiana Prosvirnova, Antoine Rauzy. // 11th IEEE International Conference on Industrial Informatics (INDIN) – Bochum, Germany, 2013. Pp. 741-746.
4. Brunel Julien et al. Performing Safety Analyses with AADL and AltaRica // Model-Based Safety and Assessment. Trento, Italy, 2017. Pp. 67-81.
5. Formal Methods for Industrial Critical Systems // Proceedings of 16th International Workshop FMICS. 2011.
6. Gonschorek T. et al. Integrating Safety Design Artifacts into System Development Model Using SafeDeML // Model-Based Safety and Assessment – Thessaloniki, Greece, 2019. Pp. 93-106.
7. Liang H. et al. System Safety Analysis of a Full Authority Digital Engine Control System // 2017 International Conference on Sensing, Diagnostics, Prognostics, and Control (SDPC). Shanghai, China, 2017. Volume-6 Issue-5, June. Pp. 543-548.
8. MATLAB & Simulink Design Verifier (Software Engineering and Formal Methods) / Proceedings of 12th International Conference SEFM. 2014.
9. Munk Peter et al. Model-based safety assessment with SysML and component fault trees: application and lessons learned // Software and Systems Modeling. 2020. Pp. 889–910.
10. Shao Nian et al. Model-based safety analysis of a control system using Simulink and Simscape extended models // MATEC Web of Conferences – 2017.

References

1. *Buzdalov D. V.* Tools for designing the systems of integrated module avionics / D. V. Buzdalov, C. V. Zelenov, E. V. Kornyhin, A. K. Petrenko, A. V. Strah, A. A. Ugnenko, A. V. Horoshilov // Works of Institute for System Programming of the RAS. 2014. №1. Volume 26. P. 201-230. (in Russian)

2. *Cherkashin S. V.* A generic system for avionic diagnostics / S. V. Cherkashin, V. V. Shishkin, N. A. Dolbnja // Izvestia of Samara scientific center of the RAS. 2009. V. 11. № 3-2. P. 392-397. (in Russian)

3. Batteux Michel The AltaRica 3.0 project for Model-Based Safety Assessment / Michel Batteux, Tatiana Prosvirnova, Antoine Rauzy. // 11th IEEE International Conference on Industrial Informatics (INDIN) – Bochum, Germany, 2013. Pp. 741-746. (in English)

4. Brunel Julien et al. Performing Safety Analyses with AADL and AltaRica // Model-Based Safety and Assessment. Trento, Italy, 2017. Pp. 67-81. (in English)

5. Formal Methods for Industrial Critical Systems // Proceedings of 16th International Workshop FMICS. 2011. (in English)

6. Gonschorek T. et al. Integrating Safety Design Artifacts into System Development Model Using SafeDeML // Model-Based Safety and Assessment – Thessaloniki, Greece, 2019. Pp. 93-106. (in English)

7. Liang H. et al. System Safety Analysis of a Full Authority Digital Engine Control System // 2017 International Conference on Sensing, Diagnostics, Prognostics, and Control (SDPC). Shanghai, China, 2017. Volume-6 Issue-5, June. Pp. 543-548. (in English)

8. MATLAB & Simulink Design Verifier (Software Engineering and Formal Methods) / Proceedings of 12th International Conference SEFM. 2014. (in English)

9. Munk Peter et al. Model-based safety assessment with SysML and component fault trees: application and lessons learned // Software and Systems Modeling. 2020. Pp. 889–910. (in English)

10. Shao Nian et al. Model-based safety analysis of a control system using Simulink and Simscape extended models // MATEC Web of Conferences – 2017. (in English)