На правах рукописи

УДК: 519.873+519.81+519.248:681.51] (043.3)

САВЕЛЬЕВ Артем Сергеевич

РАЗРАБОТКА МЕТОДИКИ СНИЖЕНИЯ ВЕРОЯТНОСТИ ПРЕЖДЕВРЕМЕННОГО ПЕРЕХОДА НА РЕЗЕРВНЫЙ РЕЖИМ КОМПЛЕКСНОЙ СИСТЕМЫ УПРАВЛЕНИЯ ГРАЖДАНСКОГО САМОЛЕТА ПО ПРИЧИНЕ ОТКАЗОВ СОПРЯГАЕМОГО ОБОРУДОВАНИЯ

Специальность 2.3.1. Системный анализ, управление и обработка информации, статистика (технические науки)

Автореферат
Диссертации на соискание учёной степени
кандидата технических наук

МОСКВА - 2024

Работа выполнена в Федеральном государственном бюджетном образовательном учреждении высшего образования «Московский авиационный институт (национальный исследовательский университет)» (МАИ) на кафедре 703 «Системное проектирование авиакомплексов».

Научный руководитель:	кандидат технических наук, доцент Неретин Евгений Сергеевич, начальник отдела систем самолетовождения филиала публичного акционерного общества «Яковлев» – Центр комплексирования, заведующий кафедрой 703 «Системное проектирование авиакомплексов» Института № 7 «Робототехнические и интеллектуальные системы», начальник НИО-703 федерального государственного бюджетного образовательного учреждения «Московский авиационный институт (национальный исследовательский университет)»
Официальные оппоненты:	Ерохин Вячеслав Владимирович, доктор технических наук, доцент, профессор кафедры авиационного радиоэлектронного оборудования Иркутского филиала федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный технический университет гражданской авиации»; профессор кафедры радиофизики и радиоэлектроники федерального государственного бюджетного образовательного учреждения высшего образования «Иркутский государственный университет»; доцент кафедры информационные системы и защита информации» федерального государственного бюджетного образовательного учреждения высшего образования «Иркутский государственный университет путей сообщения». Юков Андрей Валерьевич, кандидат технических наук, заместитель директора научно-технического центра разработок – главный конструктор акционерного общества «Ульяновское конструкторское бюро приборостроения».
Ведущая организация:	Публичное акционерное общество «Московский институт электромеханики и автоматики»

Защита диссертации состоится 10 октября 2024 г. в 13 часов 00 минут на заседании диссертационного Совета 24.2.327.03 при Федеральном государственном бюджетном образовательном учреждении высшего образования «Московский авиационный институт (национальный исследовательский университет)» (МАИ) по адресу: 125993, г. Москва, Волоколамское шоссе, д. 4.

С диссертацией можно ознакомиться в библиотеке МАИ и на сайте МАИ по адресу: https://mai.ru/events/defence/?ELEMENT_ID=180885.

Отзывы на автореферат, заверенные печатью организации, просьба направлять по адресу: 125993, г. Москва, Волоколамское шоссе, д. 4.

Автореферат разослан « » 2024 г.

Учёный секретарь диссертационного совета, д.т.н., доцент **А. В. Старков**

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность работы и степень разработанности темы. Безопасность – качественный интегральный показатель, определяющийся как *состояние, в котором риск приемлем*. Для достижения *безопасности* предусмотрены различные методы: резервирование, обнаружение и изоляция отказов и т.д.

Современные комплексные системы управления (КСУ) гражданских самолетов имеют не менее двух режимов работы: основной и резервный. В обоих режимах реализуются все функции, связанные непосредственно с управлением аэродинамическими поверхностями самолета. Ключевым отличием основного режима управления является наличие дополнительных защитных функций, препятствующих возникновению аварийных и катастрофических ситуаций. К защитным функциям относятся, например, предупреждение о приближении к эксплуатационным ограничениям скоростей, углов и перегрузок, ограничения отклонения поверхностей на разных режимах полета, парирование возмущений и др. Таким образом, стоит задача сохранять функции основного режима управления как можно дольше или, иначе говоря, минимизировать вероятность преждевременного перехода на резервный режим управления.

Структурно-функционально можно представить основной режим управления гражданского самолета как комплекс следующих взаимодействующих систем:

- основных вычислителей КСУ (расположенные в физически независимых блоках: левом и правом),
- трижды резервированных бесплатформенных инерциальных навигационных систем (БИНС),
- трижды резервированных систем воздушных сигналов (СВС),
- пульт с кнопкой перехода на резервный режим (реализующей возможность инициации экипажем перехода на резервный режим в случае необходимости).

В такой архитектуре ключевыми источниками угроз для основного режима управления являются взаимодействующие системы, т.к. основные вычислители КСУ имеют высокий показатель избыточности и независимости. При этом отказы простых электромеханических устройств, таких как кнопки, имеют достаточно низкую интенсивность по сравнению со сложной радиоэлектронной аппаратурой, входящей в состав БИНС и СВС. Из этого следует, что основными потенциальными источниками преждевременных отказов основного режима являются неисправности БИНС и СВС.

Отказы подразделяются на мгновенные, при которых выходной сигнал меняет свое значение с истинного на некорректное за крайне малый промежуток времени (например, обрыв цепи, короткое замыкание), и постепенные, при которых выходной сигнал меняет свое значение за продолжительное время (от нескольких тактов работы встроенных средств контроля). Примерами постепенных отказов могут служить

отклонение от технических условий значения сопротивления в резисторах или износ механических узлов. Если мгновенные отказы алгоритмически легко обнаруживаемы даже в случае исправности всего двух каналов сигнала, то при постепенном отказе, т.е. при обработке встроенными средства контроля двух сигналов с различными характеристиками, очевидного решения в широко распространённых эвристических алгоритмах нет. Отсюда следует, что распространённые эвристические алгоритмы применимы вплоть до второго отказа. Учитывая, что в составе самолета сохраняется исправный источник информации о пространственном положении, такой переход является *преждевременным.*

Практика показывает, что *преждевременные* переходы на резервный режим КСУ при эвристических алгоритмах контроля сопрягаемого оборудования не являются *практически невероятными* (т.е. имеют вероятность возникновения более, чем $1*10^{-9}$/л.ч. в соответствии с АП-25). Данная проблема может быть решена пересмотром подхода к методике контроля исправности сопрягаемого оборудования.

Известны различные перспективные методы контроля исправности сопрягаемого оборудования, включая элементы искусственного интеллекта и включение в контур дополнительного эталонного наземного источника информации. Каждый из методов показывает положительные результаты для некоторых групп видов отказов, но следует отметить, что часть из них сложна в практической реализации на борту или для сертификации. Таким образом актуальным вопросом остается разработка методики контроля сопрягаемого оборудования, не требующей значительного изменения программно-аппаратного комплекса, и вместе с тем логика работы которой может быть верифицирована в соответствии с отраслевыми стандартами.

Целью настоящей работы является повышение безопасности полётов за счет снижения вероятности преждевременного перехода на резервный режим комплексной системы управления.

Объектом исследований является комплексная система управления перспективного гражданского самолета.

Предметом исследования являются встроенные средства контроля комплекса сопрягаемого с системой управления бортового оборудования гражданского самолета.

Задачи диссертационной работы:

1. Сформировать требования к встроенным средствам контроля по результатам анализа функциональных ограничений использующихся средств контроля сигналов сопрягаемого с КСУ оборудования;
2. Разработать методику, обеспечивающую определение исправных сигналов сопрягаемого оборудования вплоть до последнего отказа, т.е. использующую все доступные источники сигналов сопрягаемого оборудования на борту;

3. Разработать методику оценки безопасности системы в соответствии с отраслевыми стандартами Р-4754А, Р-4761;

4. Разработать стенд полунатурного моделирования отказных состояний;

5. Провести имитационное моделирование работы встроенных средств контроля в составе основного режима комплексной системы управления.

Методология и методы исследования, примененные в работе: методы системного анализа, методы экспериментальных исследований, численные методы компьютерного моделирования, методы прогнозирования и оценки надежности сложных систем.

Научная новизна диссертационной работы заключается в следующем:

– разработана методика контроля сигналов в основном режиме комплексной системы управления, обеспечивающая на основе комбинации метода Лорцзака и неравенства Чебышева функционирование сопрягаемого оборудования вплоть до последнего отказа;

– разработаны алгоритмы, реализующие предложенную методику контроля сигналов сопрягаемого оборудования на основе комбинации метода Лорцзака и неравенства Чебышева в среде MATLAB;

– разработана методика выполнения мероприятий оценки безопасности на основе нотации SysML, с учетом повышения точности расчетов показателей надежности и безопасности при использовании предложенной методики контроля сигналов сопрягаемого оборудования.

Положения, выносимые на защиту:

– методика контроля сигналов в основном режиме комплексной системы управления, обеспечивающая на основе комбинации метода Лорцзака и неравенства Чебышева функционирование сопрягаемого оборудования вплоть до последнего отказа;

– алгоритмы, реализующие предложенную методику контроля сигналов сопрягаемого оборудования на основе комбинации метода Лорцзака и неравенства Чебышева в среде MATLAB;

– методика выполнения мероприятий оценки безопасности на основе нотации SysML, с учетом повышения точности расчетов показателей надежности и безопасности при использовании предложенной методики контроля сигналов сопрягаемого оборудования.

Теоретическая и практическая значимость полученных в диссертационной работе результатов состоит в следующем:

– разработана методика контроля сигналов сопрягаемого оборудования в основном режиме комплексной системы управления, позволяющая определить исправные сигналы в случае отказов в двух из трех каналов сигнала сопрягаемого оборудования;

– разработан программно-аппаратный комплекс (стенд полунатурного моделирования), обеспечивающий валидацию степени опасности функциональных отказов;

– полученные методики упрощают процесс взаимодействия инженеров разного уровня иерархии (самолет / система / компонент) и авиационных властей.

Достоверность полученных результатов обеспечивается корректным применением математического аппарата и их экспериментальной проверкой.

Внедрение и реализация. Основные результаты диссертационной работы внедрены при выполнении научно-исследовательских работ в ПАО «Корпорация «Иркут» и учебный процесс на кафедре 703 «Системное проектирование авиакомплексов» Института №7 «Робототехнические и интеллектуальные системы» МАИ, что подтверждается соответствующими актами о внедрении. Работы выполнялись при поддержке Российского фонда фундаментальных исследований грант № 20-31-90028 «Применение модельно-ориентированного подхода к оценке безопасности гражданских воздушных судов на примере комплекса бортового оборудования».

Апробация работы. Основные положения диссертационной работы представлены и обсуждены на 17-й, 18-й, 19-й и 20-й Международных конференциях «Авиация и космонавтика» (г. Москва, 2018, 2019, 2020, 2021 гг.), III и IV Конкурсе научно-технических работ ПАО «Корпорация «Иркут» (г. Москва, 2018, 2019 гг.), 11-м и 12-м Всероссийских межотраслевых молодёжных конкурсах научно-технических работ и проектов «Молодёжь и будущее авиации и космонавтики» (г. Москва, 2019, 2020 гг.), XLV, XLVI и XLVII Международных молодёжных научных конференциях «Гагаринские чтения» (г. Москва, 2019, 2020, 2021 гг.), 3-ей Международной конференции «3rd International Conference on Control, Artificial Intelligence, Robotics & Optimization ICCAIRO» (Греция, г. Афины, 2019 г.), XII и научно-практических конференций студентов и аспирантов «Актуальные проблемы развития авиационной техники и методов ее эксплуатации» (г. Иркутск, 2019, 2020 гг.), XV Международной конференции по электромеханике и робототехнике «Завалишинские чтения» (г. Санкт-Петербург, 2020 г.), XV Международной научно-технической конференции «Автоматизация и энергосбережение в машиностроении, энергетике и на транспорте» (г. Вологда, 2020 г.), XI-й международной научно-технической конференции «Проблемы совершенствования робототехнических и интеллектуальных систем летательных аппаратов» (г. Москва, 2020 г.), IV Международной научно-практической конференции «Производственные технологии будущего: от создания к внедрению» (г. Комсомольск-на-Амуре, 2021 г.), научных семинарах института №7 «Робототехнические и интеллектуальные системы» МАИ.

Публикации. Основные результаты диссертационной работы полностью отражены в 6 статьях (4 из которых – в журналах, рекомендованных Перечнем

ведущих периодических изданий ВАК при Министерстве науки и высшего образования РФ), 5 публикациях Scopus, 18 трудах и тезисах докладов международных и всероссийских конференций и семинаров.

Личный вклад автора заключается в разработке новой методики контроля сопрягаемого оборудования, проведении полунатурных испытаний КСУ при отказах в одном и двух каналах сопрягаемого оборудования, разработке методики оценки безопасности с использованием нотации SysML.

Структура и объем диссертационной работы. Диссертация состоит из введения, четырех глав, заключения и списка использованных источников. Общий объем работы составляет 136 страниц, включая 54 рисунка и 15 таблиц. Список использованных источников содержит 77 наименований.

СОДЕРЖАНИЕ РАБОТЫ

Во **введении** представлена общая характеристика работы, сформулированы основная цель и вытекающие из нее задачи исследования, указаны объект, предмет и методы исследования, приведен обзор исследований по рассматриваемой тематике, отражены актуальность, научная новизна и практическая значимость диссертационной работы. Кратко излагается содержание работы по главам.

В **главе 1** диссертационной работы проведен анализ современных и перспективных подходов к методам контроля бортового оборудования. Классические методы были оценены с точки зрения их подверженности воздействию различных видов отказов, как мгновенных, так и постепенных, а также их комбинаций. Оценивались следующие применяющиеся эвристические методы: метод выбора среднего арифметического значения, метод выбора медианного значения, метод контроля по предыстории.

В ходе работы использовались следующие допущения:

- вычисление сигнала сопрягаемого оборудования, использующегося в алгоритмах основного режима КСУ *и* выполняется мажоритарным элементом (МЭ), реализующим логику контроля в виде функционального программного обеспечения. Входными сигналами МЭ являются трехкратно резервированные одноименные сигналы сопрягаемого оборудования. Выходным сигналом МЭ является сигнал *и,* соответствующий результату работы рассматриваемого метода контроля;
- архитектуры современных КСУ содержат вычислители основного режима с достаточным уровнем избыточности для демонстрации практически невероятной величины их отказа (т.е. вероятность их отказа $<10^{-9}$/час в соответствии с АП-25). В связи с этим рассматриваются исключительно отказы сопрягаемого оборудования, требующегося для реализаций функций основного режима КСУ;
- МЭ выполняет три функции: (1) оценивает состояние датчиков сопрягаемого оборудования, (2) определяет неисправные датчики сопрягаемого оборудования, и (3)

формирует выходной сигнал u, использующийся в алгоритмах основного режима КСУ;

- измеряемые сигналы x_i подвержены нормально распределенным случайным ошибкам с нулевым математическим ожиданием и дисперсией, соответствующей паспортным характеристикам;
- При наличии трех источников одноименного сигнала от сопрягаемого оборудования мажоритарный элемент можно описать, как представлено на рисунке 1.

Рисунок 1. Общий вид мажоритарного элемента сопрягаемого оборудования

Метод выбора среднего арифметического значения заключается в расчете среднего арифметического значения трех одноименных сигналов, поступающих от различных источников сопрягаемого оборудования:

$$u = \frac{1}{3}\sum_{1}^{3} x_i$$

Проблема метода выбора среднего арифметического значения заключается в том, что независимо от количества исправных одноименных каналов сигнала сопрягаемого оборудования, любой отказ приводит к влиянию на результирующий сигнал u. Использование данного метода, расчетная вероятность преждевременного перехода на резервный режим составляет $P_{\text{РР}} = 2{,}53 * 10^{-4}$ на один час полета. Это значение выше, чем требуемая по АП-25 вероятность $1*10^{-9}$ на один летный час для *практически невероятных* событий. Вероятность рассчитана с использованием стандартных математических моделей надежности компонентов в составе оборудования с применением метода анализа дерева отказов на примере значений интенсивности отказов БИНС, СВС и кнопки перехода на резервный режим перспективного гражданского самолета.

Метод выбора медианного значения

Методика расчета медианного значения может быть представлена как:

$$u = median(x);$$

Здесь функция *median(x)* возвращает значение x_i, соответствующее середине упорядоченного по возрастанию ряда измеренных одноименных значений в трех

независимых источниках сопрягаемого оборудования с различными статистическими погрешностями.

Данный метод является наиболее распространенным в гражданской авиации для контроля трехкратно резервированных одноименных сигналов сопрягаемого оборудования КСУ, т.к. не требует значительных вычислительных мощностей, очевиден в работе (и, соответственно, в процессе верификации). Исходя из описания функции следует, что отказ в одном из каналов не влияет на результирующий сигнал. Метод функционирует исправно вплоть до второго отказа. Используя данный метод, расчетная вероятность перехода на резервный режим составляет $P_{\text{РР}} = 1{,}49 * 10^{-8}$ на один час полета. Вероятность рассчитана при тех же исходных данных, что и в случае с методом выбора среднего арифметического значения. Результат расчет также не соответствует критерию *практического невероятного* события по АП-25.

Метод контроля по предыстории

Под контролем по предыстории понимается методика с использованием введенного весового коэффициента для каждого из сигналов, увеличивающегося со временем, если сигнал не отличается больше порогового значения ε от предыдущего значения.

Для каждого датчика вводится коэффициент предыстории – достоверность v_i, изначально равный 1. При получении обновленных данных измеренных значений одноименных сигналов сопрягаемого оборудования коэффициент предыстории v_i увеличивается, если $|u–x_i| < \varepsilon$, где ε – пороговая величина сравнения, определяющаяся паспортными характеристиками сопрягаемого оборудования.

Тогда параметр u можно представить как:

$u = \frac{\sum_1^3 w_i v_i x_i}{\sum_1^3 w_i v_i}$, где весовые коэффициенты w_i вычисляются по методу Лорцзака [9], а параметр предыстории v_i по формуле:

$$w_i = \frac{1}{1+\prod_{j=1,j\neq i}^{3} \frac{(x_i-x_j)^2}{\beta^2}}, \quad \text{где } \beta = \min_{i=1,j=1,i\neq j}(x_i - x_j)$$

$$v_i(k) = \begin{cases} (v_i^{k-1} + \delta) \in [0.1; 1.0], \text{если } \left|x_i^{k-1} - u\right| < \varepsilon \\ (v_i^{k-1} - \delta) \in [0; 0.9], \text{если } \left|x_i^{k-1} - u\right| \geq \varepsilon \end{cases}$$

Здесь k – такт вычислений, δ – параметр изменения коэффициента предыстории v_i, ε – допустимый порог сравнения одноименных сигналов.

Несмотря на то, что результаты испытаний на стенде полунатурного моделирования в режиме реального времени данного метода контроля сопрягаемого оборудования при исследовании отказов в канале крена демонстрируют возможность расчета результирующего значения u при отказах в двух каналах, обнаружено что в комбинации отказов, при которой сначала происходит постепенный отказ в одном канале, а затем мгновенный отказ в другом канале, отсутствует возможность расчет

достоверного значения *u*. Исходя из этого сделан вывод, что метод контроля по предыстории также корректно функционирует до второго отказа, как и метод медианного значения. Соответственно, вероятность преждевременного перехода на резервный режим КСУ также не соответствует критерию *практически невероятного* события.

По результатам анализа использующихся на текущий момент в КСУ эвристических методов контроля сопрягаемого оборудования определено, что ни один из них не соответствует критерию *практически невероятного* события для преждевременного перехода на резервный режим. Таким образом, наличие исправного источника сигнала сопрягаемого оборудования не используется и осуществляется переход на менее безопасный резервный режим КСУ.

В **главе 2** поставлена и решена задача разработки методики контроля сопрягаемого оборудования, обеспечивающая соответствию критерию *практически невероятного* события для преждевременного перехода на резервный режим КСУ. По результатам проанализированных функциональных недостатков методов, описанных в главе 1, сформулированы следующие требования к разрабатываемой методике:

- Расчет результирующего значения *u* при контроле сопрягаемого оборудования должен осуществляться при отсутствии отказов;
- Расчет результирующего значения *u* при контроле сопрягаемого оборудования должен осуществляться при возникновении отказа в одном из каналов (при рассмотрении любого отдельного вида отказа);
- Расчет результирующего значения *u* при контроле сопрягаемого оборудования должен осуществляться при возникновении отказов в двух каналах (при рассмотрении комбинаций мгновенных и постепенных отказов).

Данные требования могут быть достигнуты при комбинации метода Лорцзака, представленного в главе 1, с использованием методов обнаружения аномальных значений в случайных процессах. Были проанализированы различные методы: критерий Шарлье, Томсона и неравенство Чебышева. По результатам анализа определено, что к поставленной задаче наиболее применим метод неравенства Чебышева для определения аномальных значений во временных рядах в связи с ограничением на количество контролируемых сигналов, а также по причине известных статистических параметров ошибок в измеряемых сигналах.

Согласно неравенству Чебышева, любое выборочное значение x_i отклоняется от математического ожидания m_x не более чем на величину $\left|\frac{x_i - m_x}{\sigma_x^2}\right|$ с заданным уровнем доверительной вероятности (здесь σ_x^2 – значение дисперсии случайного процесса).

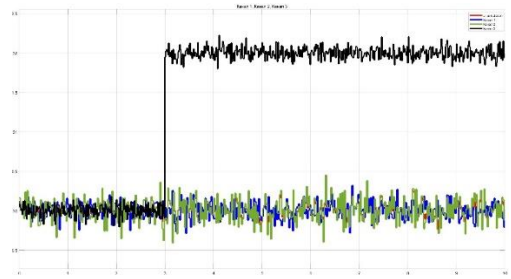
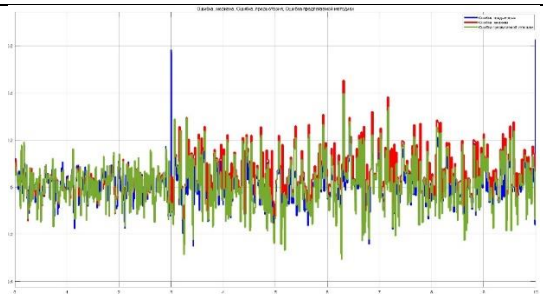
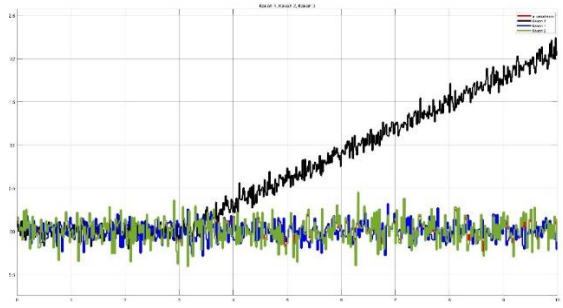
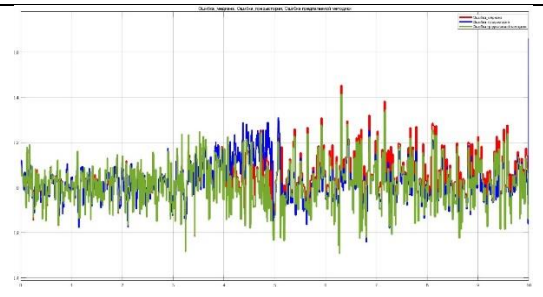
Применительно к поставленной задаче, отказавшим каналом сигнала сопрягаемого оборудования считается тот, который не удовлетворяет неравенству:

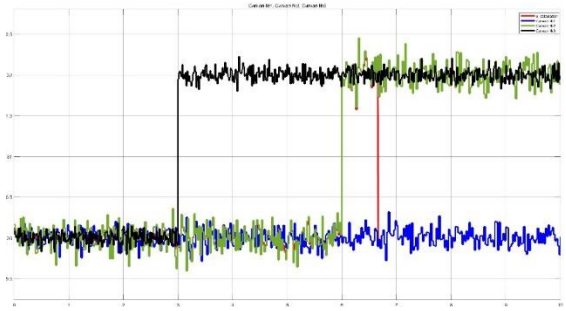
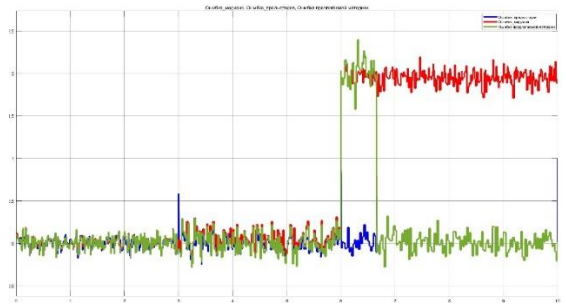
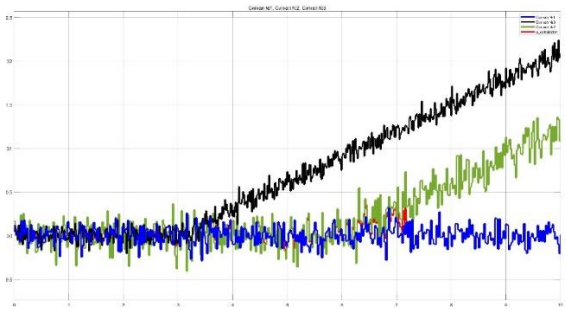
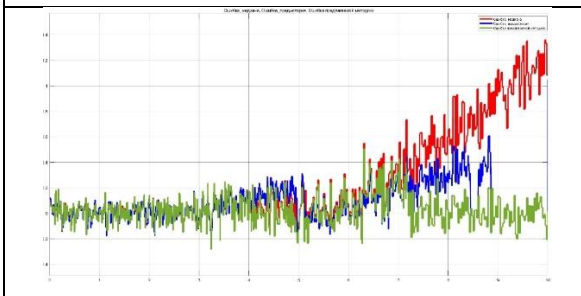
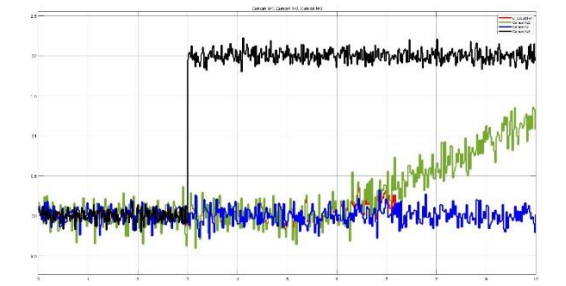
$$\left|\frac{x_i - m_x}{\sigma_x^2}\right| \leq \frac{1}{\sqrt{1-\beta}}$$

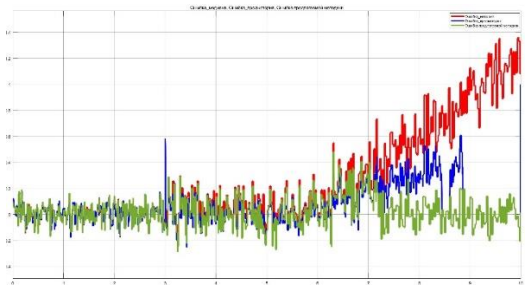
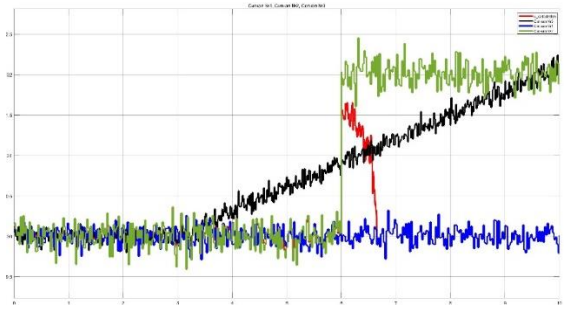
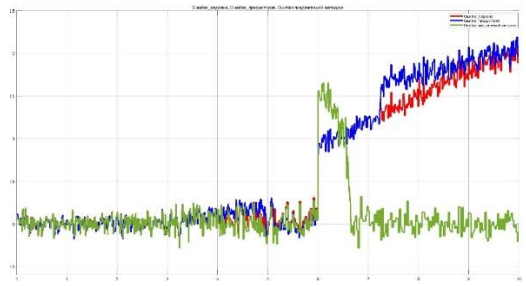
Применительно к поставленной задаче были выбраны следующие параметры:

- m_x – математическое ожидание ошибки измерений, равное 0;
- σ_x^2 – дисперсия распределения ошибки измерений, соответствующее паспортным характеристикам;
- β – доверительная вероятность неравенства Чебышева, равная 0,003 в соответствии с нормативной документацией.

Сравнительный анализ результатов функционирования при отказах данных методов представлен на рисунках 2-13. Метод вычисления среднего арифметического значения не учитывается как не удовлетворяющий заданным требованиям.

	Рисунок 2. Сигналы в каждом из каналов x_i и результирующего u при мгновенном отказе в одном канале при использовании предлагаемой методики контроля **Вывод:** методика обнаруживает отказавший канал и подает в алгоритмы КСУ исправное значение.
	Рисунок 3. Ошибки работы анализируемых методик контроля при мгновенном отказе в одном канале **Вывод:** каждая из методик работает исправно.
	Рисунок 4. Сигналы в каждом из каналов x_i и результирующего u при постепенном отказе в одном канале при использовании предлагаемой методики контроля **Вывод:** методика обнаруживает отказавший канал и подает в алгоритмы КСУ исправное значение.
	Рисунок 5. Ошибки работы анализируемых методик контроля при мгновенном отказе в одном канале **Вывод:** каждая из методик работает исправно.

	Рисунок 6. Сигналы в каждом из каналов x_i и результирующего u при последовательных мгновенных отказах в двух каналах при использовании предлагаемой методики контроля **Вывод:** методика обнаруживает отказавший канал и подает в алгоритмы КСУ исправное значение.
	Рисунок 7. Ошибки работы анализируемых методик контроля при последовательных мгновенных отказах в двух каналах **Вывод:** контроль методом вычисления медианного значения не способен обнаружить второй отказ. Предлагаемая методика показывает кратковременный выброс с последующим восстановлением до корректного значения.
	Рисунок 8. Сигналы в каждом из каналов x_i и результирующего u при последовательных постепенных отказах в двух каналах при использовании предлагаемой методики контроля **Вывод:** методика обнаруживает отказавший канал и подает в алгоритмы КСУ исправное значение.
	Рисунок 9. Ошибки работы анализируемых методик контроля при последовательных постепенных отказах в двух каналах **Вывод:** контроль методом вычисления медианного значения не способен обнаружить второй отказ.
	Рисунок 10. Сигналы в каждом из каналов x_i и результирующего u при последовательных мгновенных и постепенном отказах в двух каналах при использовании предлагаемой методики контроля **Вывод:** методика обнаруживает отказавший канал и подает в алгоритмы КСУ исправное значение.

	Рисунок 11. Ошибки работы анализируемых методик контроля при последовательных мгновенных и постепенном отказах в двух каналах **Вывод:** контроль методом вычисления медианного значения не способен обнаружить второй отказ.
	Рисунок 12. Сигналы в каждом из каналов x_i и результирующего u при последовательных постепенном и мгновенном отказах в двух каналах при использовании предлагаемой методики контроля **Вывод:** методика обнаруживает отказавший канал и подает в алгоритмы КСУ исправное значение.
	Рисунок 13. Ошибки работы анализируемых методик контроля при последовательных постепенном и мгновенном отказах в двух каналах **Вывод:** контроли методом вычисления медианного значения и по предыстории не способны обнаружить второй отказ.

В **главе 3** представлен реализованный программно-аппаратный комплекс, позволяющий обеспечить полунатурное моделирование отказных состояний, проведены испытания при различных конфигурациях самолета. С помощью данного программно-аппаратного комплекса оценивается управляемость воздушного судна при возникновении отказов. Комплекс включает в себя:

- Рабочее место оператора:
  - Рабочий компьютер (ПК или ноутбук);
  - Комплект физических имитаторов органов управления (боковая ручка управления самолетом, блок рычагов управления двигателями, педальный пост);
- Математическая модель комплексной системы управления, учитывающая динамику исполнительных механизмов (приводов) поверхностей, органов управления;
- Банк аэродинамических характеристик самолета МС-21-300;

- Графические средства имитации пульта управления режимами системы автоматического управления (ПУ САУ);
- Графические средства индикации, визуализации закабинного пространства и введения отказов.

В качестве среды моделирования используется MATLAB Simulink. Для выведения оператору рабочего места полетной информации используются Flight Ind, Flight Gear и Пульт ввода отказов с использованием протокола UDP (Universal Datagram Protocol), который не влияет на скорость моделирования, и, соответственно, оператор получает всю необходимую информацию, как ее бы получал пилот в ходе штатного полета.

Функциональное взаимодействие компонентов аппаратного и программного обеспечения испытательного стенда представлено на рисунке 14.

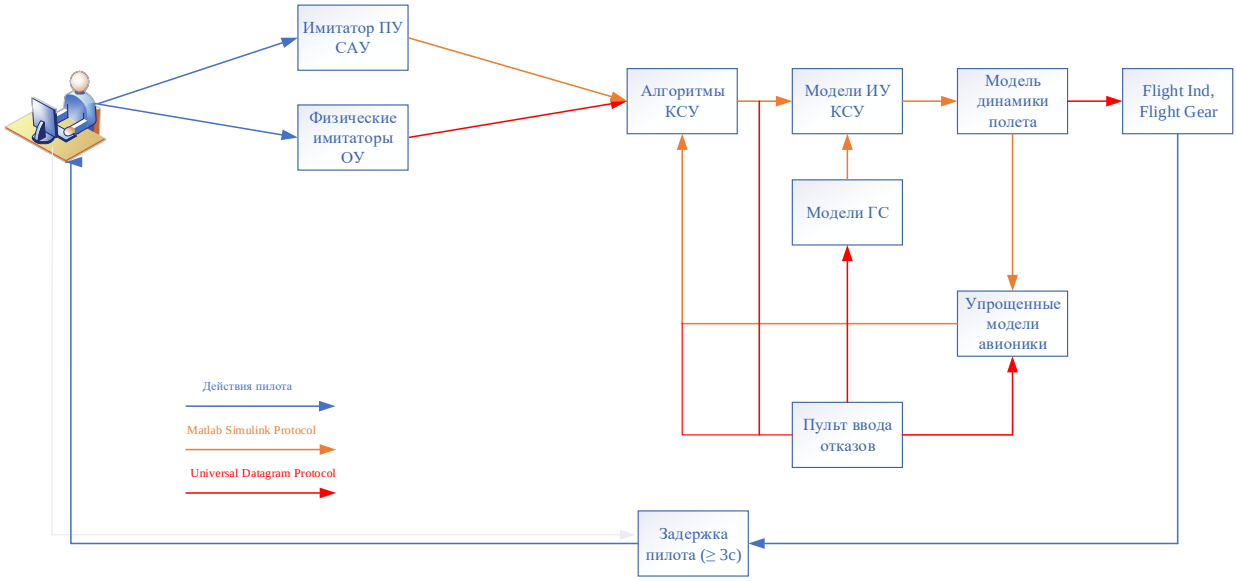


Рисунок 14. Функциональная схема разработанного стенда

С использованием разработанного комплекса проведено 288 испытаний на стенде полунатурного моделирования на наиболее критичных этапах полета – взлете и посадке при различных конфигурациях механизации крыла, массы и центровки для определения качественных показателей пилотирования при использовании различных методов контроля сопрягаемого оборудования при возникновении отказов в одном и двух каналах. Отказы имитировались в канале угла крена КСУ для ручного режима управления системой электродистанционного управления (СДУ) и автоматического режим управления системой автоматического управления (САУ). По результатам проведенных испытаний подтверждены выводы, полученные во второй главе, о наибольшей приемлемости предложенного метода контроля сопрягаемого оборудования как для ручного режима управления, так и при управлении под автопилотом для исключения преждевременного перехода на резервный режим КСУ.

В **главе 4** предложена уточненная методика оценки безопасности, основанная на требованиях Р-4761, дополненная использованием нотаций SysML для соответствия критериям Model-Based Safety Assessment (модельно-ориентированному подходу к оценке безопасности, MBSA) и произведен расчет вероятности преждевременного перехода на резервный режим методами контроля сопрягаемого оборудования, функционирующими до второго отказа, и предложенным методом контроля сопрягаемого оборудования с использованием неравенства Чебышева, функционирующего вплоть до последнего отказа сопрягаемого оборудования.

Уточненная методика выполнения оценки функциональных опасностей (ОФО) представлена в виде последовательности шагов на рисунке 15. Цветом выделены шаги, не требующиеся нормативной документацией.

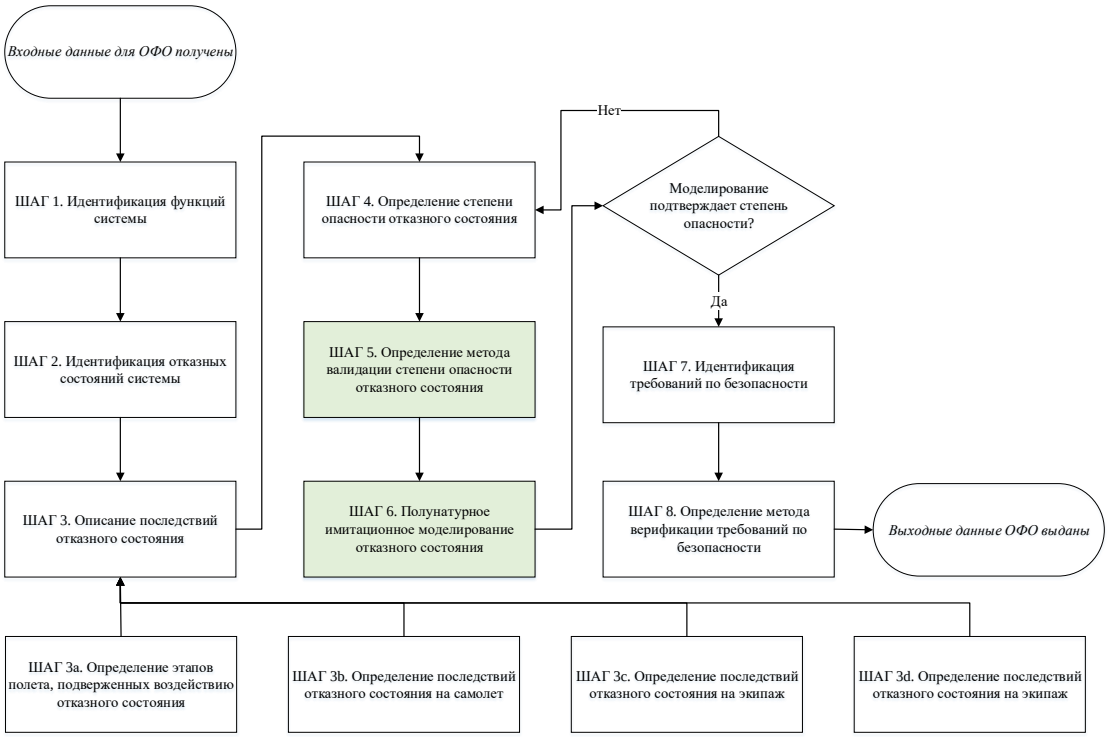


Рисунок 15. Уточненная методика модельно-ориентированного подхода к ОФО

Внедрение полунатурного моделирования для подтверждения степени опасности отказных состояний позволяет определить корректность сделанных предположений в ОФО в соответствии с Р-4761. На текущий момент ошибки назначения степени опасности обнаруживается в период летных испытаний, когда внесение корректировок в алгоритмы работы и конструкцию системы затруднительны и связаны с экономическими рисками.

Уточненная методика выполнения анализа дерева отказов (АДО) представлена в виде в виде последовательности шагов на рисунке 16. Цветом выделены шаги, не требующиеся нормативной документацией.

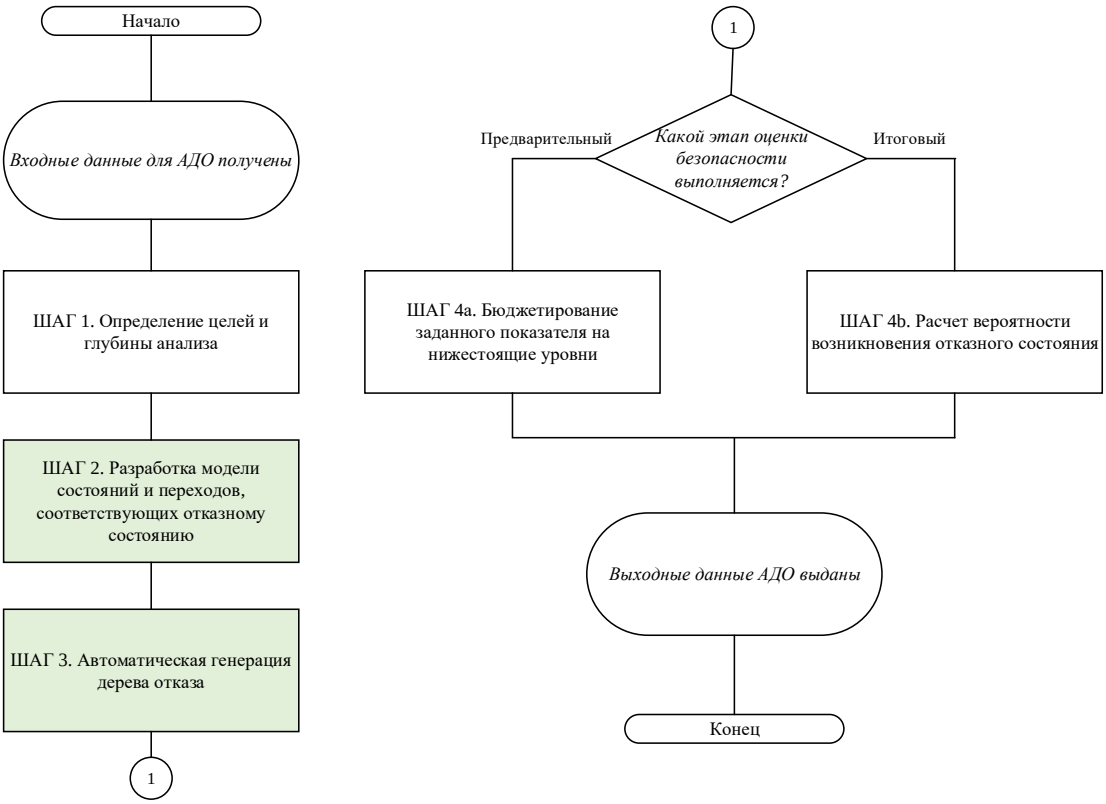


Рисунок 16. Уточненная методика модельно-ориентированного подхода к АДО

Внедрение разработки модели состояний и переходов для каждого отказного состояния, определенного в ходе ОФО, позволяет определить логику отказов и их контроля на ранних этапах проектирования. Автоматическая генерация дерева отказа для данного отказного состояния исключает ошибки при выполнении АДО, связанные с человеческим фактором.

Количественный расчет вероятности отказа автоматически сгенерированных деревьев отказов (параметр недоступности *Q(t)*) выполняется с использованием выражения Шеннона:

$$Q(t) = P(E_i)P(TLE \mid E_i) + P\left(\overline{E_i}\right)P(TLE \mid \overline{E_i}),$$

где E_i – каждое базовое событие в Анализе дерева отказов (АДО), а TLE – Top Level Effect – событие верхнего уровня.

Вероятность базового события зависит от интенсивности отказов компонентов, из которых данное событие складывается, а также показателях ремонтопригодности и обследуемости в зависимости от типа оборудования. В таком случае вероятность каждого базового события принимает вид, как представлено на формулах для обследуемых и для ремонтопригодных изделий.

$$P(E_i) = 1 - e^{-\lambda(t+\tau)} \quad \text{(обследуемые)}$$

$$P(E_i) = \left(\frac{\lambda}{\lambda+\mu}\right)\left(1 - e^{-(\lambda+\mu)t}\right) \quad \text{(ремонтопригодные)}$$

Здесь τ – параметр обследуемости (в часах) и μ - показатель ремонтопригодности (в 1/ч). Параметр интенсивности отказов λ рассчитывается с использованием справочных материалов или статистических данных опытной эксплуатации.

Уточненная методика выполнения анализа видов и последствий отказов (АВПО) представлена в виде в виде последовательности шагов на рисунке 17. Цветом выделены шаги, не требующиеся нормативной документацией.

Уточнение заключается в учете интенсивности воздействия одиночных ионизирующих частиц (ВОИЧ) на элементы радиоэлектронной аппаратуры, приводящие к различным отказам: радиационно-индуцированный сбой в одном бите (Single Event Upset), радиационно-индуцированный сбой в нескольких битах (Multiple Bit Upset), радиационное выжигание (Single Event Burnout) и другие. Интенсивность ВОИЧ зависит от площади поперечного сечения подверженных воздействию атмосферного излучения полупроводников, широты и высоты типового профиля полета.

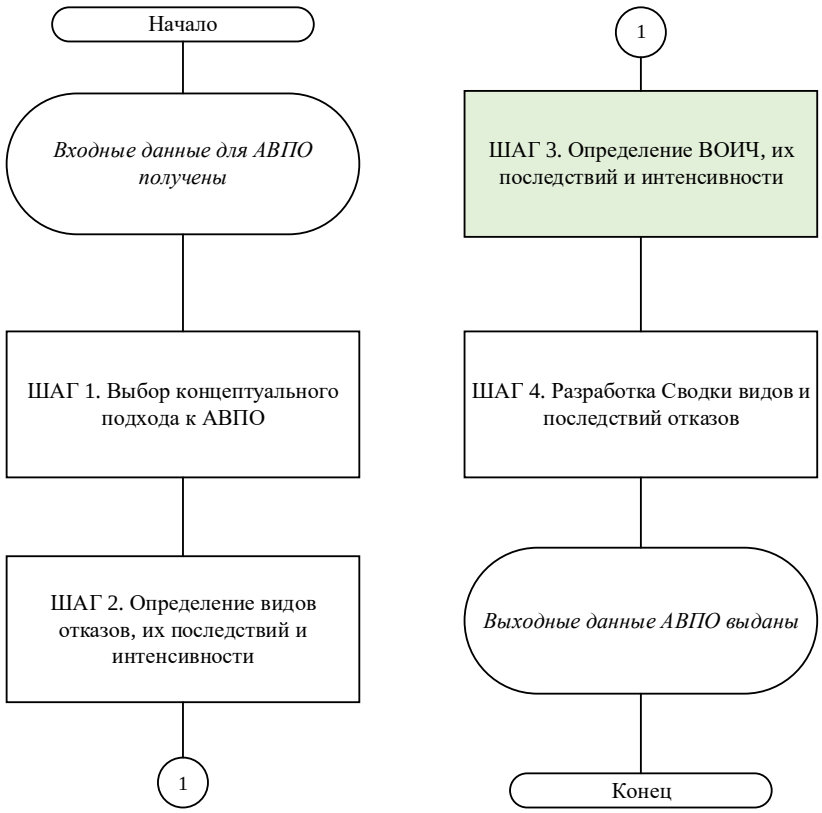


Рисунок 17. Алгоритм модельно-ориентированного подхода к АВПО

Используя данные уточненные по принципу MBSA методики оценки безопасности было сгенерированы дерево, представленное на рисунке 18. Результаты расчета вероятности демонстрируют, что преждевременный переход на резервный режим является ситуацией *практически невероятной* (расчетное значение составляет 5.2e-10 на один час полета, что меньше требуемой 1e-9 на один час полета) при

использовании предложенной методики контроля сопрягаемого оборудования с использованием неравенства Чебышева и метода Лорцзака.

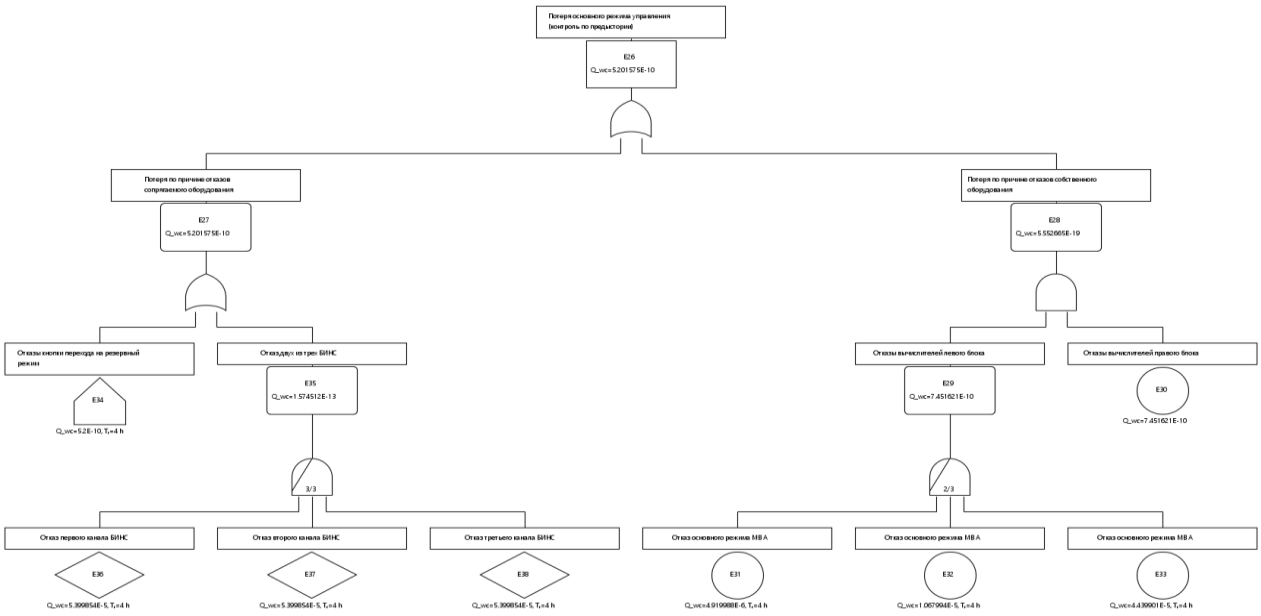


Рисунок 18. Результат расчета вероятности отказного состояния «Преждевременный переход на резервный режим КСУ» при использовании предложенной методики контроля сопрягаемого оборудования

ОСНОВНЫЕ РЕЗУЛЬТАТЫ ДИССЕРТАЦИОННОЙ РАБОТЫ

Целью работы являлось повышение безопасности полетов за счет снижения вероятности преждевременного перехода на резервный режим КСУ.

Было показано, что применяющиеся на текущий момент эвристические методы контроля сопрягаемого оборудования (расчет среднего арифметического значения, расчет медианного значения, контроль по предыстории) не обеспечивают уровень *практической невероятности* (меньше 10^{-9}/летный час) перехода на резервный режим КСУ, т.к. фактически допускают преждевременное отключение основного режима при наличии одного исправного источника сигнала. Такой переход назван преждевременным.

Для снижения вероятности преждевременного перехода на резервный режим КСУ было предложено использовать комбинированный метод контроля сопрягаемого оборудования с использованием неравенства Чебышева для определения отказавших каналов сигнала и метода Лорцзака для расчета результирующего значения трех каналов сигнала.

С целью демонстрации отсутствия негативного влияния на пилотирование при использовании предложенной методики, был разработан стенд полунатурного моделирования с возможностью имитации отказов в полете. По результатам проведенных 288 испытаний при различных начальных условиях и режимах полета (СДУ и САУ) было оценено, что при отказах в одном канале предложенная методика

контроля не ухудшает качество пилотирования, а при наличии отказов в двух каналах сопрягаемого оборудования сохраняется основной режим КСУ.

Для расчета вероятности преждевременного перехода на резервный режим КСУ с учетом требований Р-4761 были разработаны уточнения к методике выполнения оценки безопасности с использованием MBSA на основе нотации SysML. Уточнения для ОФО заключались в проведении полунатурного моделирования, валидирующих степень опасности. Уточнения для АДО заключались в автоматической генерации дерева на основе модели переходов между состояниями. Уточнения для АВПО заключались в учете интенсивности отказов, возникающих в связи с воздействием атмосферного излучения на радиоэлектронную аппаратуру.

В таблице 1 представлено сравнение функционирования и вероятности преждевременного перехода на резервный режим КСУ при использовании различных методик контроля сопрягаемого оборудования

Таблица 1. Сравнение различных методов контроля сопрягаемого оборудования

Параметр	**Среднее арифметическое**	**Медианное значение**	**Контроль по предыстории**	**Предложенная методика**
Вероятность преждевременного перехода на резервный режим КСУ	$2{,}53 * 10^{-4}$	$1{,}49 * 10^{-8}$	$1{,}49 * 10^{-8}$	$5{,}21 * 10^{-10}$
Функционирование	Вплоть до первого отказа	Вплоть до второго отказа	Вплоть до третьего отказа, за исключением ситуации, когда сначала происходит постепенный отказ, а затем мгновенный	Вплоть до третьего отказа при рассмотренных любых комбинациях отказов

На основе Таблицы 1 сделан вывод, что цель работы достигнута, т.к. вероятность преждевременного перехода на резервный режим КСУ снизилась до значения менее, чем 1e-9, т.е. стала событием *практически невероятным* в соответствии с АП-25.

СПИСОК РАБОТ, ОПУБЛИКОВАННЫХ АВТОРОМ ПО ТЕМЕ ДИССЕРТАЦИИ

В рецензируемых журналах и изданиях

1. Савельев А. С. и др. Метод определения подхода отказобезопасности критического оборудования на этапе системного проектирования //Crede Experto: транспорт, общество, образование, язык. – 2020. – №. 4. – С. 32-45.
2. Дяченко С. А., Савельев А. С. Анализ автоматизированных средств верификации систем авионики, применяемых при разработке современных

гражданских самолётов //Crede Experto: транспорт, общество, образование, язык. – 2021. – №. 1. – С. 30-36.
3. Савельев А. С., Неретин Е. С. Методика мажоритарного кворум-контроля резервированных сигналов бортового оборудования в основном режиме системы управления гражданского самолета //Научно-технический и производственный журнал «Вестник компьютерных и информационных технологий». – 2022. – Т.19, №10. – С. 3-14.
4. Савельев А. С. Способ решения известных проблем встроенных средств контроля бортовых систем на примере основного режима системы дистанционного управления гражданского самолета //Журнал «Труды ГосНИИАС, серия – Вопросы авионики». – 2023. – №3(62). – С. 9-21.

В изданиях Scopus

5. Savelev A., Neretin E. Preliminary Safety Assessment for the Sidestick Move from Autopilot Signals Function //WSEAS Transactions on Environment and Development. – 2019. – Т. 15. – С. 485-492.
6. Savelev A., Neretin E. Development of safety requirements for tracking active pilot controls by signals from an Automatic Flight Control System //2019 International Conference on Control, Artificial Intelligence, Robotics & Optimization (ICCAIRO). – IEEE, 2019. – С. 19-24.
7. Savelev A., Lituev N., Olidaev E. Functional hazards assessment of an integrated flight control system validation using model-based design //IOP Conference Series: Materials Science and Engineering. – IOP Publishing, 2020. – Т. 868. – №. 1. – С. 012006.
8. Savelev A. S. et al. Finite-state machine method in the safety assessment process using Stateflow diagrams //Journal of Physics: Conference Series. – IOP Publishing, 2021. – Т. 1958. – №. 1. – С. 012034.
9. Savelev A. S. et al. Development of Failure Modes and Effects Analysis methodology using Model-Based Safety Assessment approach //Journal of Physics: Conference Series. – IOP Publishing, 2021. – Т. 1958. – №. 1. – С. 012033.

В других изданиях

10. Савельев А. С., Неретин Е. С. Перспективные способы повышения надежности и отказобезопасности систем управления летательных аппаратов //Авиация и космонавтика-2018. – 2018. – С. 405-406.
11. Савельев А. С. Влияние порога срабатывания алгоритма контроля методом вычисления взвешенного значения по предыстории среднего //Гагаринские чтения-2019. – 2019. – С. 688-689.
12. Савельев А. С., Неретин Е. С. Архитектура взаимодействия активных органов управления с системами дистанционного и автоматического

управления гражданских самолётов //Молодёжь и будущее авиации и космонавтики. – 2019. – С. 185-186.
13. Литуев Н. А., Савельев А. С., Ольдаев Е. В. Модельно-ориентированное проектирование в задаче валидации оценки функциональных опасностей комплексной системы управления //18-я Международная конференция" Авиация и космонавтика-2019". – 2019. – С. 166-167.
14. Савельев А. С., Неретин Е. С. Проектирование отказобезопасной функции перемещения активной ручки управления по сигналам от системы автоматического управления //18-я Международная конференция" Авиация и космонавтика-2019". – 2019. – С. 172-172.
15. Савельев А. С., Неретин Е. С. Предварительная оценка безопасности функции отслеживания активными органами управления заданных сигналов от системы автоматического управления гражданского самолета //Crede Experto: транспорт, общество, образование, язык. – 2020. – №. 2. – С. 6-14.
16. Савельев А. С. Синтез закона управления активным сайдстиком //Гагаринские чтения-2020. – 2020. – С. 839-840.
17. Савельев А. С., Неретин Е. С. Предварительный анализ безопасности активных сайдстиков при работе автопилота //ЗАВАЛИШИНСКИЕ ЧТЕНИЯ'20. – 2020. – С. 152-158.
18. Литуев Н. А., Савельев А. С., Неретин Е. С. Разработка комплекса моделирования для валидации оценки функциональных опасностей комплексной системы управления с использованием методов модельно-ориентированного проектирования //Crede Experto: транспорт, общество, образование, язык. – 2020. – №. 3. – С. 50-59.
19. Савельев А. С., Берсуцкая О. Д. Возможные способы применения анализа общих причин отказов при проектировании комплекса бортового оборудования //Молодёжь и будущее авиации и космонавтики-2020. – 2020. – С. 171.-172.
20. Берсуцкая О. Д., Савельев А. С. Необходимые пути развития подхода к анализу общих причин отказов при проектировании комплекса бортового оборудования //19-я Международная конференция «Авиация и космонавтика». – 2020. – С. 419-420.
21. Савельев А. С. и др. Анализ применимости методов модельно-ориентированного проектирования к задачам оценки безопасности бортового оборудования самолета //Автоматизация и энергосбережение в машиностроении, энергетике и на транспорте. – 2021. – С. 297-300.
22. Савельев А. С. и др. Применение метода конечных автоматов в задачах оценки безопасности с использованием stateflow-диаграмм //Проблемы

совершенствования робототехнических и интеллектуальных систем летательных аппаратов. – 2021. – С. 82-85.
23. Савельев А. С., Берсуцкая О. Д., Силин Н. Д. Разработка методики выполнения анализа видов и последствий отказов с применением модельно-ориентированного подхода к оценке безопасности комплекса бортового оборудования //Проблемы совершенствования робототехнических и интеллектуальных систем летательных аппаратов. – 2021. – С. 86-89.
24. Дяченко С. А., Савельев А. С. Программное обеспечение для автоматизированного тестирования систем электронной индикации современных гражданских самолётов //Производственные технологии будущего: от создания к внедрению. – 2021. – С. 33-37.
25. Савельев А. С. Исследование влияния атмосферного излучения на безопасность радиоэлектронного оборудования гражданских самолетов //XLVII Гагаринские чтения 2021. – 2021. – С. 736-737.
26. Савельев А. С., Берсуцкая О. Д. Влияние ионизирующего излучения на безопасность гражданских самолетов //Авиация и космонавтика. – 2021. – С. 393-394.
27. Савельев А. С. Внедрение модельно-ориентированных методик в классический V-образный подход к оценке безопасности сложных бортовых систем гражданских воздушных судов //Гагаринские чтения-2022. – 2022. – С. 413-413.