ОТЗЫВ

официального оппонента на диссертационную работу Сарамуда Михаила Владимировича «Модельно-алгоритмическое обеспечение анализа отказоустойчивости программных комплексов встраиваемых систем управления реального времени», представленную на соискание ученой степени кандидата технических наук по специальности 05.13.01 - Системный анализ, управление и обработка информации (космические и информационные технологии)

Актуальность темы

Исследование направлено на решение задачи обеспечения надежности программного обеспечения встраиваемых систем управления для различных классов объектов, в частности, автономных беспилотных объектов (АБО) на всех этапах его жизненного цикла. АБО применяются в решении задач различных сфер жизнедеятельности человека, где человеческая жизнь подвергается опасности, участие человека невозможно или дорогостоящее, а именно: задачи наземной городской среды, подводные задачи, в воздушном и космическом пространстве, военные тактические и стратегические задачи, складское дело и доставка потребительских товаров. Важность повышения надежности программной составляющей таких объектов неоспорима, т.к. сбои в таких критических важных задачах могут привести к большим финансовым потерям, катастрофам и усугублению военных конфликтов.

Поэтому выбранная тема диссертационного исследования по созданию модельно-алгоритмического обеспечения анализа отказоустойчивости программных комплексов встраиваемых систем управления реального времени, является актуальной.

Обоснованность и достоверность результатов и выводов диссертации

Целью диссертационной работы является повышение отказоустойчивости разрабатываемого программного обеспечения (ПО) за счет получения оценок надежности программных модулей на этапе проектирования и алгоритмов принятия решения в мультиверсионных системах.

Для достижения цели автором в диссертационной работе выполнен обширный анализ моделей исследования и предсказания надежности ПО, а также моделей и средств проектирования отказоустойчивых программных комплексов.

По результатам выполненных в диссертационной работе исследований разработано модельно-алгоритмическое обеспечение анализа отказоустойчивости программных комплексов встраиваемых систем управления реального времени.

Автором предложен ряд моделей, методов и их программных реализаций для анализа отказоустойчивости программных комплексов. Предложены модификации алгоритмов принятия решения в мультиверсионных системах, произведено их сравнительное тестирование в разработанной имитационной среде моделирования. Предложена деэвтрафикационная модель предсказания времени наработки на отказ. Разработана практическая реализации мультиверсионной среды исполнения реального времени.

Достоверность полученных результатов подтверждается результатами расчетов в имитационных средах и реализованной мультиверсионной среде исполнения реального времени. Результаты работы были апробированы на девяти международных конференциях. Разработанные программные системы прошли регистрацию в Роспатенте.

Основные научные результаты

Сформирована типовая структура мультиверсионной системы управления реального времени, в том числе ее программной составляющей, что позволит разработать как имитационные среды моделирования, так и практическую реализацию мультиверсионной среды исполнения реального времени.

Предложен комбинированный селективный алгоритм оценки эффективности мультиверсионных моделей, впервые позволивший получить верхнюю и нижнюю границы надежности. Для получения данных оценок предложены модели «деревьев сбоев» и корректности.

Разработаны модифицированные алгоритмы принятия решения в мультиверсионных системах, взвешенные алгоритмы голосования согласованным большинством с элементом забывания в четкой и нечеткой интерпретации, и t/(n-1) алгоритм с нечеткими компараторами.

Предложена деэвтрафикационная модель предсказания времени наработки на отказ и разработан новый программный инструмент её на основе.

Значение для теории

Полученные в диссертационной работе результаты вносят существенный вклад в теорию анализа отказоустойчивости программных комплексов систем управления. Теоритическая значимость состоит в разработке новых моделей оценки надежности мультиверсионных систем, новых взвешенных алгоритмов голосования с забыванием, методики предсказания времени наработки на отказ.

Значение для практики

В диссертационной работе предложен комплекс программных инструментов, основанных на разработанных моделях и алгоритмах, предназначенных для разработчиков отказоустойчивых программных комплексов систем управления, которые позволяют автоматизировать процесс решения задачи компоновки состава мультиверсионного

программного комплекса, выбрать алгоритмы принятия решения, сформировать требования к характеристикам составляющих систему модулей.

Предложенные модификации алгоритмов голосования не только увеличивают устойчивость мультиверсионных систем к межверсионным ошибкам, но и способствуют увеличению надежности системы в целом.

Программный инструмент предсказания времени наработки на отказ существенно сокращает время на этапе тестирования, поскольку дает возможность тестировать систему не в масштабе реального времени, а настолько быстрее, насколько производительна тестовая платформа, что позволяет гарантировать время наработки на отказ в месяцах, затрачивая на тестирование на порядок меньшие промежутки времени.

Имитационная среда моделирования мультиверсионных программных комплексов позволяет тестировать и получать характеристики исследуемых моделей, алгоритмов голосования, а также позволяет сравнить их в одинаковых условиях.

Обзор диссертационной работы

Во *введении* обозначена проблема обеспечения надежности программного обеспечения автономных беспилотных объектов, обоснована актуальность выбранной темы, определены цель и задачи диссертационного исследования. Сформулированы защищаемые положения, научная новизна и практическая значимость результатов исследования.

В *первой главе* диссертационной работы автором приведены характеристики отказоустойчивых сложных систем, работающих в масштабе реального времени. Дана подробная классификация автономных беспилотных объектов и областей их применения.

Проведен анализ этапов жизненного цикла ПО систем управления реального времени с малой и большой длительностью эксплуатации.

Проанализированы известные модели оценки надежности ПО в части их применимости в оценке надежности ПО систем управления реального времени. Приведены результаты применения подхода к оценке надежности ПО на двух программах, реализованных по одному техническому заданию.

Структурированы надежностные характеристики и приведена классификация сбоев ПО. Проведено исследование современных методов повышения отказоустойчивости ПО за счет введения программной избыточности.

В выводах первой главы обоснована необходимость создания типовой структуры программного обеспечения системы управления.

Во *второй главе* рассмотрены преимущества и недостатки операционных систем реального времени (ОСРВ), как платформы для создания отказоустойчивых систем управления реального времени.

Приведены критерии выбора ОСРВ для реализации среды исполнения программных модулей и рассмотрены современные ОСРВ. Сделан выбор в

пользу FreeRTOS и дано ее подробное описание и особенности функционирования.

Приведена концептуальная структура встраиваемой в ОСРВ системы управления реального времени.

Описаны требования к разработке блока принятия решения в ОСРВ и определены типовые программные модули встраиваемой системы управления.

В *третьей главе* описан предложенный комбинированный селективный алгоритм формирования состава мультиверсионного программного комплекса. Описаны модели деревьев сбоя для 4-х вариантов программной избыточности, учитывающие программные сбои, в том числе вызванные аппаратными сбоями. Приведено описание программной реализации моделей деревьев сбоя, позволяющей отследить изменение надежностных характеристик мультиверсионной системы при изменении характеристик отдельных версий.

Описана модель корректности, показывающая разницу между различными вариантами реализации мультиверсионной системы, а также программная реализация этой модели.

В *четвертой главе* обоснована проблема выбора правильного результата выполнения версий в алгоритме голосования. Подробно описаны существующие алгоритмы голосования и модификация алгоритма голосования в части введения динамического веса каждой версии с элементами «забывания». Также предложена модификация t/(n-1) алгоритма, в части введения нечеткой логики при сравнении результатов версий.

Приведено описание программной системы, позволяющей сравнить надежностные характеристики различных алгоритмов голосования и сделать выбор в пользу наиболее подходящего.

Проанализированы результаты имитационного моделирования работы алгоритмов голосования и сделаны выводы об условиях наиболее эффективного применения различных алгоритмов голосования.

В *пятой главе* обоснована необходимость совершенствования методов поддержки принятия решения при выборе оптимального варианта реализации мультиверсионной системы. Приведены примеры, когда введение дополнительных версий модуля нецелесообразно, и можно обойтись реализацией приемочного теста для повышения надежности.

Приведены и проанализированы результаты применения имитационной среды исполнения по различным методологиям программной избыточности и с различными алгоритмами голосования. Программная реализация имитационной среды позволяет сделать выбор оптимальной методологии мультиверсионной системы.

Описана программная реализация мультиверсионной среды исполнения версий в операционной системе реального времени FreeRTOS.

Сделан вывод о том, что результаты имитационной среды совпадают с результатами испытаний программной реализации мультиверсионной среды исполнения.

В мультиверсионной среде исполнения были реализованы 3 версии распознавания голосовых команд для АБО. Надежность системы из 3 версий превысила надежность каждой версии в отдельности.

Автором предложена модель предсказания времени наработки на отказ и ее программная реализация. Также приведена апробация данной модели на реальных результатах тестирования.

В *заключении* работы сформулированы выводы и результаты, полученные при исследовании.

Замечания

По содержанию работы:

1. В первой главе не достаточно подробно рассмотрен этап испытаний программного обеспечения длительной эксплуатации, хотя именно на этом этапе собирается информация для прогнозирования надежности ПО. Не приведено, какие виды тестирования и какие особенности их применения характерны при разработке ПО систем реального времени.
2. В описании подэтапа отладки и этапа испытаний приведено утверждение, что исправляются все обнаруженные дефекты, что не всегда верно. Обнаруженные в ходе тестирования дефекты могут требовать больших затрат на исправление в уже почти готовом программном комплексе, но при этом быть маловероятными для воспроизведения. В этом случае на обнаруженный дефект делается специализированная обработка ошибки («заглушка») и внесение этой информации в базу знаний, или вовсе не обрабатывается.
3. В описании этапа использования ПО не выделен этап опытной эксплуатации, а обучение персонала, внедрение и настройка приведены как часть этапа использования.
4. Вызвали затруднения при чтении отсутствие пояснений к специфичным терминам и аббревиатурам «ИИН», «мьютекс», «FIFO буфер».
5. Во второй главе уделено излишне большое внимание характеристикам и возможностям ОСРВ FreeRTOS а также практической реализации блока принятия решения.
6. В главе 5 при описании результатов испытаний на реальной задаче приведено описание только результатов, связанных с повышением надежности за счет использования версий. Но не приведены результаты сравнения модифицированных алгоритмов голосования, показывающих свою эффективность по сравнению со стандартными алгоритмами при применении на реальной задаче.

7. В примерах применения моделей и их программных реализаций рассматривались только варианты избыточности по какой-то определенной одной задаче, хотя в сложных программных комплексах может возникнуть необходимость введения программной избыточности во множество различных функций, которые взаимосвязаны и нельзя рассматривать их отдельно. Например, версии алгоритма обработки голосовых команд и версии алгоритма управления движением АБО. Соответственно в работе не рассматривается влияние надежности отдельных мультиверсионных взаимосвязанных блоков на надежность всего программного комплекса.

По оформлению:

1. На рисунках 8-12 текстовые пояснения приведены только на английском языке, что может затруднить восприятие читателю.
2. На рисунках 57 и 58 не обозначены оси и единицы измерения, что затрудняет его чтение.
3. На рисунках 19 и 20 в диаграмме последовательности стрелки не подписаны теми данными, которые передаются различными методами, что затрудняет чтение диаграммы, хотя нотация UML позволяет подписывать стрелки хотя бы кратко.
4. Представленные на рисунках 25-42 снимки интерфейса программной реализации моделей деревьев сбоев и модели корректности содержат значения надежностных характеристик для разных вариантов программной избыточности. Эти значения сложно между собой сравнивать поразрядно, т.к. они представлены не в табличном виде. Соответственно для целевого пользователя, принимающего решение о варианте реализации мультиверсионной системы, это будет не удобно.
5. Также в тексте работы обнаружено несколько опечаток и несогласованных предложений.

Заключение

Диссертация Сарамуда Михаила Владимировича является завершенной научно-квалификационной работой. Его работа содержит решение актуальных научных задач в области системного анализа сложных прикладных объектов исследования с целью повышения надежности и качества технических систем. Указанные выше замечания по работе не снижают ее практической ценности и научной значимости.

На все утверждения в работе автором приводились примеры, исчерпывающее теоретическое и практическое обоснование.

Работа изложена последовательно и структурировано. Полученные при исследовании результаты соответствуют поставленным цели и задачам.

Положения, выносимые на защиту и результаты работы прошли всестороннюю апробацию на международных конференциях. По работе опубликовано 19 печатных работ.

Разработанные автором программные системы зарегистрированы в Роспатенте.

Автореферат корректно отражает содержание диссертации. Автореферат и диссертация оформлены в соответствии с требованиями ВАК РФ.

Диссертационная работа удовлетворяет требованиям ВАК РФ, предъявляемым к кандидатским диссертациям по специальности 05.13.01 - Системный анализ, управление и обработка информации (космические и информационные технологии), а ее автор - Сарамуд Михаил Владимирович - заслуживает присуждения ученой степени кандидата технических наук по указанной специальности.

Официальный оппонент:
кандидат технических наук,
старший аналитик
ООО «Сибирские интеграционные системы» Д.А. Шеенок

«01» августа 2018 г.

ООО «Сибирские интеграционные системы»
660032, г. Красноярск, ул. Белинского, 5
www.sis-it.pro
Тел.: 8 (391) 276-77-99
E-mail: mail@sis-it.pro

Подпись Шеенка Дмитрия Александровича заверяю:

Генеральный директор ООО
«Сибирские интеграционные системы»_____ Спиридонова В.А.

01 августа 2018

ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ ОГРН 1032463037079 ИНН 2460209774 "Сибирские интеграционные системы" г. КРАСНОЯРСК