Двойные технологии, №3, 2005

Метод оценивания показателей надёжности и безопасности наземных и бортовых космических систем с шинными структурами

Антонов Ю.В., Белов В.П., Голяков А.Д

Научно-исследовательский институт точной механики, г. Санкт-Петербург

Повышенные требования по надёжности и безопасности наземной и бортовой аппаратуры современных и перспективных космических систем и комплексов совместно с существующими ограничениями на материальные ресурсы и сроки создания делают методологию оценивания соответствующих показателей одной из основных проблем, которые решаются на отечественных предприятиях-разработчиках систем управления, содержащих микропроцессорные средства обработки и преобразования информации.

Современный уровень развития отечественной и зарубежной техники привёл к качественному изменению элементно-технологической базы. Это позволило перейти от устаревших принципов проектирования информационно-управляющих систем (ИУС) к новым перспективным идеям, которые базируются на использовании блочного принципа построения структур из отдельных функциональных блоков (модулей, устройств), связанных между собой с помощью ряда шин. Шина представляет собой совокупность линий (проводников), общих для всех подключённых к ней устройств, и служит для обмена данными или обеспечения электропитания. Блочный принцип приводит к сокращению трудовых и интеллектуальных затрат на проектирование систем, а также упрощает последующие процессы наращивания и реконфигурации информационно-управляющей системы.

Применяемые в настоящее время электронные компоненты перспективных систем управления имеют среднюю наработку до отказа от сотен тысяч до нескольких миллионов часов. При использовании таких компонентов в сложных космических системах реально достижимой является её наработка до отказа около десяти тысяч часов, что не удовлетворяет современным требованиям по продолжительности эксплуатации.

Кроме того, особую значимость имеют системы, у которых отказ отдельного элемента может оказаться «опасным». При стечении определённых обстоятельств такой отказ, являющийся угрозой безопасности, может привести либо к жертвам или травмам людей, либо к серьезным экономическим, экологическим и другим нежелательным последствиям, например, к потере авторитета предприятия-разработчика или к снижению потребительского спроса производимой продукции.

Опыт разработки, создания и эксплуатации наукоёмких систем управления, накопленный в Научно-исследовательском институте «Точной механики», показывает, что эффективными способами решения задачи парирования опасных отказов являются:

применение электронных схем и компонентов с высокой и сверхвысокой степенью интеграции;

обеспечение облегченных режимов работы электронных схем и компонентов;

совершенствование методов сборки, испытаний и эксплуатации изделий;

использование мажоритарных схем типа «два из трёх», «три из четырёх» и т.п., а также схем с безопасными оконечными устройствами или иначе – схем с «несимметричными отказами».

Под схемами с «несимметричными отказами» понимаются собственно схемы и реальные физические их компоненты, обеспечивающие при любых однократных внутренних повреждениях или сбоях перевод системы в безопасное («защитное») состояние путем выдачи соответствующего управляющего воздействия.

Если теперь умозрительно, на уровне функциональных блоков, представить себе, например, двух-трёх уровневую иерархическую систему управления, где на каждом из уровней как по входу, так и по выходу, используются мажоритарные схемы «два из трех», а для приема и выдачи сигналов и команд управления на исполнительные устройства используются дублированные схемы с «несимметричными отказами», и, кроме того, вся система охвачена подсистемой контроля, диагностики и отключения (восстановления) поврежденных компонентов, имеет несколько резервированных автоматизированных рабочих мест и определенную модель технического обслуживания, вопрос о степени сложности методики и собственно расчета показателей надёжности отпадает – ясно, что это чрезвычайно сложная проблема.

Необходимость решения этой проблемы возникла перед учёными и специалистами службы надёжности НИИ «Точной механики» в конце 80-х годов, когда была поручена разработка системы пожаро-взрывопредупреждения для комплекса «Энергия-Буран». Такая система, содержащая бортовую и наземную аппаратуру, обеспечила безопасную подготовку, пуск и полёт ракеты-носителя. В состав системы входила трёхканальная бортовая ЭВМ, специализированные микропроцессоры, включённые по мажоритарным схемам, резервированные блоки питания, усиления и т.п.

Наиболее остро потребность решения проблемы разработки новых подходов к методологии оценивания показателей надёжности и безопасности сложных информационно-управляющих систем встала в середине 90-х годов при создании комплексной системы обеспечения безопасности и автоматизированного управления движением поездов метрополите-

на (система «Движение»). Эта система имеет иерархическую структуру и объединяет в единое целое аппаратные и программные средства управления объектами трех разных уровней.

Верхним уровнем системы «Движение» является центральный диспетчерский пост (ЦДП) линии метрополитена. Ко второму иерархическому уровню комплексной системы управления движением поездов метрополитена относится станционный уровень. Этот уровень состоит из стационарной аппаратуры (СА) станций и перегонов метрополитена, аппаратных и программных средств обеспечения микропроцессорной централизации метрополитена и каналов связи с поездной аппаратурой (ПА) и СА соседних станций. Третий иерархический уровень включает в себя оборудование и средства управления движением поездов метрополитена (поездной уровень).

К числу сложных отказоустойчивых микропроцессорных систем управления несомненно относится и разрабатываемая в НИИ «Точной механики» система управления космическим телескопом. При разработке этой системы предлагается применение перспективной унифицированной "слайдовой" конструкции приборов, построенных с использованием шинных структур, а также наработок в части бесконтактной коммутации сильноточных цепей, построения отказоустойчивых резервированных систем управления и каналов связи.

Для расчёта соответствующих показателей надёжности и безопасности на ранних стадиях жизненного цикла информационно-управляющих систем разработана группа хорошо зарекомендовавших и широко применяемых на практике аналитических методов. В группу этих методов включаются:

структурно-аналитический метод;

логико-графические методы;

логико-вероятностные методы;

аналитико-статистические методы и др.

Структурно-аналитический метод основан на построении структурной схемы надёжности ИУС [2, 3]. Структурная схема надёжности представляет собой логическую схему взаимодействия элементов, определяющая работоспособность ИУС. С помощью этой схемы удаётся однозначно определить состояние (работоспособное или неработоспособное) системы по состоянию (работоспособное или неработоспособное) входящих в неё элементов.

Вид структурной схемы определяется последствиями отказов элементов. В частности, если отказ любого элемента приводит к отказу ИУС, то элементы в структурной схеме соединены последовательно. Параллельное соединение характеризуется ситуацией, при которой отказ информационно-управляющей системы происходит только в случае отказа всех входящих в неё элементов.

Структурно-аналитический метод широко используется при необходимости расчёта показателей надёжности и безопасности ИУС, имеющих простые структуры. В отдельных

случаях удаётся произвести расчёт показателей надёжности достаточно сложных структур, например, «мостиковых схем». Для решения этих задач используются методы прямого перебора или разложения относительно «особого элемента» [2]. Однако эти методы не всегда могут быть практически реализованы.

Кроме того, для сложных систем с большим числом элементов, которые связаны между собой с помощью информационных шин и шин питания, составление структурной схемы является довольно сложной задачей. При этом неизбежны методические ошибки, обусловленные тем, что практически невозможно в условия ограниченных ресурсов времени перебрать все возможные комбинации отказов элементов, приводящие к отказу системы.

Основой логико-графических методов является графическое представление причинно-следственных связей логической последовательности событий, которые описывают развитие процесса, приводящего ИУС к неработоспособному или опасному состоянию. К группе этих методов относятся методы деревьев отказов и деревьев событий [4]. Наибольшее распространение эта группа методов получила при оценивании показателей безотказности.

Метод деревьев отказов является дедуктивным методом, поскольку начинается с установления опасного события с последующим поиском возможных причин его появления, т.е. построение дерева осуществляется сверху вниз на основании, так называемого, «обратного подхода». При построении деревьев отказов сложных систем не всегда удаётся обеспечить независимость исходных событий. Оценивание показателей безопасности в этом случае, производится методами, основанными на построении марковской диаграммы переходов состояний с последующим составлением и решением дифференциальных уравнений, которые описывают вероятности соответствующих состояний ИУС.

В методе деревьев событий в отличие от метода деревьев отказов используется прямая логика анализа последовательности событий, так называемый, «прямой подход». Поэтому этот метод относится к группе индуктивных методов. К недостаткам этого метода следует отнести большие затраты времени как на составление диаграммы дерева отказов сложных систем.

Сущность логико-вероятностных методов [5] заключается в использовании функций алгебры логики для аналитической записи условий работоспособности и безопасности ИУС, а также в разработке строгих способов перехода от функций алгебры логики к вероятностным функциям, объективно выражающим свойства безотказности и безопасности исследуемой системы.

Вычисление с помощью логико-вероятностных методов значений показателей надёжности и безопасности сложных систем, содержащих микропроцессорные элементы, обычно представляет собой достаточно громоздкую задачу. Поэтому для оценивания этих показате-

лей применяются приближённые методы, которые основаны на поиске верхней и нижней границ соответствующих вероятностей.

Аналитико-статистический метод свободен от недостатков рассмотренных ранее методов. Он не требует составления структурно-логической схемы, деревьев отказов или деревьев событий и применяется при наличии в ИУС любых видов резервирования, в том числе резервирования с восстановлением. Расчёт показателей надёжности и безопасности ИУС аналитико-статистическим методом производится на основе информации, получаемой в процессе статистического моделирования потока отказов её элементов [2, 6]. Погрешности оценок искомых показателей определяются числом реализаций случайного процесса.

Выбор расчётного метода производится на основе анализа структуры информационно-управляющей системы, степени трудоёмкости процесса оценивания, опыта и квалификации исполнителей, наличия ресурсов и необходимой информации для выполнения расчёта и других факторов.

Анализ известных методов показал, что расчёт показателей надёжности систем, имеющих иерархические структуры построения и содержащих сотни многополюсных элементов, к которым подключены резервированные информационные и управляющие шины, а также шины питания, целесообразно выполнять с помощью аналитико-табличного метода.

В основу аналитико-табличного метода положен подход, который базируется на построении таблиц состояний (таблиц решений) многополюсного блока [4]. Столбцами этой таблицы являются состояния входов, технические состояния блока и состояния его выходов. В строках этой таблицы приводятся все возможные варианты сочетаний технического состояния блока и состояний его входов.

Вероятности работоспособных состояний выходов блока находятся путём суммирования соответствующих произведений вероятности технического состояния блока и вероятностей состояний его входов. Показатели надёжности системы, содержащей многополюсные элементы, определяются путём последовательного расчёта вероятностей работоспособных состояний выходных полюсов блоков, находящихся на более высоком иерархическом уровне. Исходными данными для расчёта являются вероятности работоспособных состояний выходных полюсов блоков, находящихся на нижестоящем иерархическом уровне, вероятности работоспособных состояний шин питания и вероятности безотказной работы резервированных каналов многополюсного элемента.

В связи с этим, сущность метода, который рассматривается в настоящем докладе, заключается в разделении всех функциональных блоков информационно-управляющей системы (ИУС) на ряд иерархических уровней. Количество уровней определяется сложностью структуры исследуемой системы.

К первому уровню относятся функциональные блоки, информационные шины которых связаны с внешними по отношению к рассматриваемой ИУС системами. Такими блоками, например, являются вторичные источники питания, включение которых осуществляется по командам от внешних управляющих систем. Кроме того, к этому уровню относятся также блоки, не имеющие информационных (входных) шин (например, первичные источники питания, средства измерений параметров окружающей среды, имеющие собственные источники энергии, и т.п.).

Второй иерархический уровень формируется из функциональных блоков, у которых информационные шины и шины питания связаны с управляющими (выходными) шинами блоков первого уровня.

Третий и последующие уровни предлагаемой иерархической структуры содержат блоки, информационными входами которых являются управляющие шины функциональных блоков нижестоящих уровней.

При использовании шинной структуры построения ИУС отдельные многополюсные элементы могут быть связаны между собой не только по информационным и управляющим шинам, но и по шинам питания. В этом случае применяется соответствующая методика расчета искомых вероятностей, которая разработана с учётом взаимосвязи элементов по шинам питания.

Последовательность расчёта показателей надёжности аналитико-табличным методом содержит следующие этапы.

1. Формируется перечень работоспособных состояний всех функциональных блоков системы и рассчитываются вероятности этих состояний по известным значениям вероятностей безотказной работы резервированных каналов. Для решения этой задачи используются, как правило, λ – характеристики элементов и заданные значения времени функционирования и продолжительности хранения системы.

2. Выделяются блоки первого иерархического уровня. Очевидно, что вероятности работоспособных состояний выходных шин этих блоков равны вероятностям соответствующих работоспособных состояний, которые рассчитаны на первом этапе.

3. Формируется второй иерархический уровень функциональных блоков. Для каждого блока этого уровня в соответствии с математической моделью надёжности составляется таблица технических состояний. Такие таблицы в настоящее время сформированы практически для всех многополюсных элементов, которые применяются в современных ИУС. На основании этой таблицы определяются вероятности работоспособных состояний выходных шин блока.

4. Формируются следующие по порядку иерархические уровни блоков и рассчитываются вероятности работоспособных состояний соответствующих выходных шин функциональных блоков.

В результате выполнения описанных процедур находится вероятность работоспособного состояния выходных шин информационно-управляющей системы, т.е. искомый показатель безотказности - вероятность безотказной работы ИУС.

Способ расчёта надёжности и безопасности систем, построенных с использованием шинных структур и многополюсных элементов с внутренним резервированием, как по входу, так и по выходу, а также резервированных блоков питания, реализован в НИИ «Точной механики». В качестве объекта реализации использована комплексная система обеспечения безопасности движения и автоматизированного управления движением поездов Санкт-Петербургского метрополитена. Эта система имеет в своем составе резервированную трех канальную информационную шину, резервированную двух канальную шину управления, резервированные блоки питания, блоки с трехканальным входом и двухканальным выходом.

Конкретные результаты проведённого расчёта надёжности и безопасности системы «Движение» метрополитена, с перечнем всех функциональных блоков, размещённых на платах и стойках этой системы, представлены в монографии, которая написана учёными и сотрудниками научно-исследовательского института «Точной механики» [7].

Материал монографии основан на результатах опытно-конструкторских работ, связанных с разработкой и сертификацией современных информационно-управляющих систем. К таким системам, в частности, относятся:

системы обеспечения безопасности и управления движением поездов метрополитена;

система управления бортовыми робототехническими комплексами космических аппаратов;

системы безопасности, пожаро-взрывопредупреждения и тушения космических комплексов;

системы ликвидации информации и управления подрывом и аналогичные им системы.

Кроме того, монография основана также и на материалах курса лекций, который в течение ряда лет читается в Военно-космической академии имени А.Ф. Можайского.

Изложенные в монографии научные положения, подходы и пути разрешения ряда практических проблем предназначены для специалистов в области обоснования технических требований, проектирования, испытаний и эксплуатации информационно-управляющих систем, отказы которых способны нанести вред жизни и здоровью людей, причинить материальный и экологический ущерб. Она также может быть полезна научным сотрудникам, аспирантам и студентам, в сферу научных интересов которых входят вопросы анализа надёжно-

сти и безопасности. Многие результаты, приведённые в монографии, являются новыми. Обобщённые сведения о путях и способах решения отдельных аспектов теории безопасности, методах оценивания показателей надёжности систем управления потенциально опасных объектов на различных этапах их жизненного цикла опубликованы впервые.

Литература

1. Белов В.П., Голяков А.Д, Старков С.Я. О понятиях «надёжность» и «безопасность» технических систем с позиций разработчиков // Методы менеджмента качества, 2003, №10.

2. Надёжность технических систем: Справочник / Под ред. И.А. Ушакова. – М.: Радио и связь, 1985. – 608 с.

3. Надёжность и эффективность в технике. Т.5. Проектный анализ надёжности: Справочник / Под ред. В.И. Патрушева и А.И. Рембезы. – М: Машиностроение, 1988.- 316 с.

4. Хенли Э. Дж., Кумамото Х. Надёжность технических систем и оценка риска: Пер. с англ. В.С. Сыромятникова, Г.С. Дёминой. Под общ. Ред. В.С. Сыромятникова. – М.: Машиностроение, 1984. – 528 с.

5. Рябинин И.А. Надёжность и безопасность структурно-сложных систем. - С-Пб.: Политехника, 2000. - 248 с.

6. Белов В.П., Голяков А.Д., Старков С.Я. Аналитико-статистический метод оценки надёжности систем управления и навигации подвижных объектов / Сборник докладов НТК «Радиолокация, навигация, связь». - Воронеж, 2003.

7. Антонов Ю.В., Белов В.П., Голяков А.Д. и др. Надёжность и безопасность информационно-управляющих систем (методы оценивания и контроля). – СПб.: ОАО «НИИ ТМ», 2004. – 326 с.