Логико-вероятностная модель надёжности аппаратно-программных средств радиоэлектронных систем управления космическими аппаратами

А. В. Гришин[1], И. А. Козинов[1], А. С. Костарев[1], С. Г. Бурлуцкий[2]
[1]*Военно-космическая академия имени А.Ф. Можайского*
[2]*Санкт-Петербургский государственный университет аэрокосмического приборостроения*

Аннотация. **Рассмотрены современные и перспективные радиоэлектронные системы управления космическими аппаратами как сложные аппаратно-программные комплексы. Для таких систем предложена логико-вероятностная модель надёжности аппаратно-программных средств учитывающая данные оперативного технического диагностирования аппаратно-программных средств.**

Ключевые слова: радиоэлектронная система, надежность, логико-вероятностный метод

I. Введение

Особенностью космических аппаратов (КА), как объектов управления, является то, что они представляют собой дистанционно управляемые объекты, связь с которыми возможна только по радиоканалу. Вследствие этого основным классом наземных средств, непосредственно обеспечивающих решение задач управления КА, являются радиоэлектронные системы (РЭС) управления КА.

Для современных и перспективных РЭС управления КА характерно повышение информатизации, автоматизации и интеграции, включая оснащение полнофункциональной и оперативной системой технического диагностирования (СТД), программным обеспечением для управления различными эксплуатационными процессами, и подключение к системе интегрированной логистической поддержки (ИЛП) их эксплуатации. РЭС строятся по принципам унификации и модульности построения аппаратно-программных средств РЭС, внедряются гибкие стратегии управления надёжностью РЭС (адаптивное техническое обслуживание, профилактические мероприятия по результатам технического диагностирования, оперативный поиск мест и причин возникновения отказов, оперативное пополнение баз данных ИЛП новой информацией об отказах, их диагностировании и устранении).

Все это требует разработки новых моделей надёжности функционирования РЭС, учитывающих особенности РЭС управления КА как интегрированных аппаратно-программных средств, а также данные оперативного технического диагностирования.

II. Комплексная логико-вероятностная математическая модель надёжности функционирования РЭС

Моделирование надёжности структурно и функционально сложных систем, таких как РЭС управления КА, связано со стремлением наиболее полного учёта факторов, влияющих на их надёжность, что входит в противоречие с необходимостью преодоления большой размерности таких моделей. Например, марковское моделирование всей РЭС, как структурно и функционально сложной системы представляется затруднительным ввиду громоздкости и сложности вычислений: число состояний будет равно числу всех возможных комбинаций функционирования всех подсистем, блоков и узлов системы в обеспечение её работоспособности. В то же время и чистое логико-вероятностное моделирование реальных систем приводит к чрезвычайно громоздким логическим и вероятностным функциям надёжности. Данные обстоятельства приводят к целесообразности представить функционирование РЭС в целом и структуру каждой резервированной подсистемы в логико-вероятностной форме, разделив модель по уровням представления, что позволит значительно сократить её размерность. В результате выстраивается многоуровневая модель, состоящая из частных моделей элементов РЭС и учитываемых аспектов её функционирования, агрегированных по своим выходным показателям.

Структуру модели надежности функционирования РЭС можно представить в виде иерархии, на каждом из уровней которой представлено описание необходимого аспекта надёжности функционирования системы (рис. 1).

На рисунке обозначены: ЛВФМ – логико-вероятностная функциональная модель УРЭС; ЛВМП – логико-вероятностная модель подсистемы УРЭС; ПМ – параметрическая модель модуля подсистемы, определяемая как: МНАП – модель надёжности аппаратной платформы (средств), МНПС – модель надёжности программных средств, СМ – статистическая модель эксплуатационных событий).

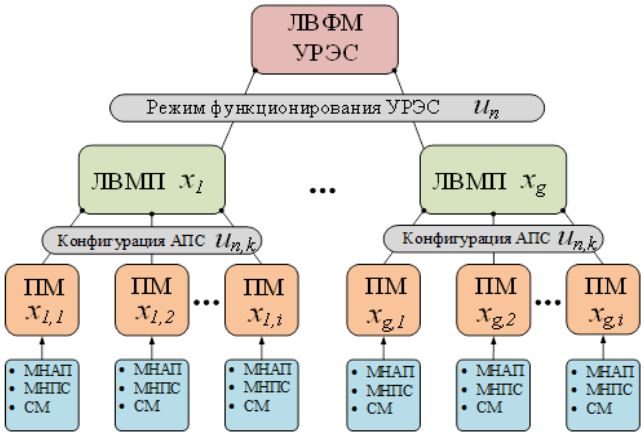

Рис. 1. Структура модели надёжности функционирования РЭС

На первом уровне описывается надёжность функционирования системы в целом при заданном режиме функционирования, например, при передаче на КА командно-программной информации. Особенность состоит в том, что режим функционирования РЭС отображается путём определённой конфигурации аппаратно-программных подсистем, причём в данном случае конфигурация понимается в смысле влияния на надёжность системы. Поэтому на данном уровне выбран аппарат логико-вероятностного моделирования и в частности – общего логико-вероятностного метода [1]. Он как нельзя лучше подходит для надёжностного описания систем с учётом сложности их структуры и функционирования, обладая широкими возможностями алгебры логики, вероятностной логики, комплексирования подмоделей и развитыми графическими средствами.

На втором уровне также используются ЛВМ, но уже для каждой из подсистем. Подсистемы представлены в виде деревьев работоспособности из составляющих их модулей (блоков и узлов) на графическом языке ОЛВМ. Здесь учитывается структурное резервирование модулей, а также наличие в их составе программных средств. Важно отметить, что для любых ЛВМ некоторую сложность представляет отыскание исходных значений вероятностных параметров вершин модели. Исследователи решают эту задачу различными методами [2], но наиболее целесообразным в рамках решаемой научной задачи будет метод вложенных (частных) моделей, которые позволяют рассчитать вероятностные параметры вершин, необходимые для подстановки в результирующие вероятностные соотношения ЛВМ надёжности каждой из подсистем. Кроме того, данный метод, решая проблему исходных данных, существенно расширяет возможности чистого логико-вероятностного моделирования надёжности: появляется возможность учёта разнородных данных и воздействующих факторов.

На третьем уровне используются модели надёжности функционирования, включающие в себя: модели надёжности аппаратных средств, учитывающие данные технического диагностирования (диагностические модели); модели надёжности программных средств, основанные на существенных особенностях их надёжностного поведения в процессе эксплуатации; статистические модели эксплуатационных событий АПС за анализируемый интервал эксплуатации. Данные этих подмоделей комплексируются с помощью ЛВМ.

III. Комплексная логико-вероятностная математическая модель надёжности программных средств РЭС

Другим видом частных моделей, используемых на третьем уровне комплексной логико-вероятностной математической модели надёжности функционирования РЭС управления КА, являются модели надёжности программных средств, основанные на существенных особенностях их надёжностного поведения в процессе эксплуатации.

Программным средством (ПС) называют программное обеспечение, предназначенное для работы в составе конкретного аппаратно-программного комплекса [3]. Программное обеспечение (ПО) – это совокупность программ и соответствующей документации, имеющий определённое функциональное назначение. Программа представляет собой модель на математическом и машинном языке, сообщающая машине порядок и способ её функционирования и взаимодействия с оператором и другими устройствами.

Изменение надёжности ПС и аппаратных средств (АСр) во времени по своей сути различно [4]:

- надёжность аппаратуры определяется во многом случайными физическими процессами (функциями времени), приводящими к внезапным или параметрическим отказам или сбоям;
- надёжность ПС определяется скрытыми ошибками, внесёнными в программный код или алгоритм на этапе разработки в общем случае случайным образом.

Ошибки в программе проявляются как систематические и скорее не случайные события. Случайными, при этом, являются определённые сочетания входных данных и вызовы участков программного кода, содержащих ошибки.

Большинство математических моделей позволяют оценивать и прогнозировать надёжность ПС по экспериментальным данным на этапах автономной и комплексной отладки, т. е. пока надёжность ПС низкая. В этих условиях наработка на отказ измеряется минутами и часами, ошибки появляются достаточно часто, позволяя приближённо описать их потоки как пуассоновские. Для стадии нормальной эксплуатации это практически неприемлемо. Поэтому на этапе тестирования и приработки, т. е. уже при высокой надёжности ПС, представляется целесообразным использовать такую аналитическую модель надёжности, которая напрямую не использует временные зависимости и исходит, например, из вероятности отсутствия ошибок в исполняемом программном коде операций и модулей ПС. Такая модель должна формировать априорную (для последующего этапа эксплуатации) информацию об основных характеристиках надёжности операций и модулей ПС, т. е. об интенсивностях их использования (вызова) и о модельном распределении в них ошибок.

Очевидно, что причинами отказов и сбоев ПС являются ошибки, внесённые в код программы или алгоритмы на этапе разработки. Интенсивность отказов ПС во времени не может быть представлена, как простейший поток событий (т. е. применение марковского моделирования во временной области некорректно) [5], однако случайная величина расположения ошибок в программном коде (в системе координат «строки кода – программные модули») может быть приближённо описана пуассоновским законом распределения для поля точек. В качестве ограничения можно полагать это поле одномерным, рассматривая лишь одну координату – строки программного кода. При этом вероятность попадания m ошибок на участок программного кода ΔC определяется выражением для распределения Пуассона:

$$P_m = \frac{a^m}{m!}\exp(-a) = \frac{(\xi\Delta C)^m}{m!}\exp(-\xi\Delta C)$$

где: ξ=ξ(C) – плотность ошибок в программном коде, обратно пропорциональная числу строк, содержащих одну ошибку, a=ξΔC – параметр распределения Пуассона.

В предельном случае, при m=0, распределение Пуассона сводится к экспоненциальному и определяет вероятность того, что на участок программного кода ΔC не придётся ни одной ошибки. Во временной области аналогичная величина именуется вероятностью безотказной работы за определённое время. В данном случае – это вероятность отсутствия ошибки (ВОО) на определённом участке кода программы [6]:

$$P_{\text{оо}} = \exp(-\xi\Delta C)$$

Тогда, длина участка отсутствия ошибки (УОО) – участка программного кода, на котором с вероятностью $P_{\text{оо}}$ ошибки не содержится:

$$\Delta C_{\text{оо}} = \frac{1}{\xi(C)}$$

При анализе надёжности функционирования ПО целесообразно исходить из длины участка программного кода $\Delta C_{\text{фо}}$, соответствующей выполнению некоторой функциональной операции (ФО) $f_r \in F_{\text{пс}i}$ i-го программного средства. Функциональная операция представляет собой r-й элемент программы, необходимый для решения η-й отдельной функциональной задачи (ОФЗ) ωη и выполнения i-й программы в целом. Функциональная операция – это структурно-функциональный компонент программы, задаваемый последовательностью строк программного кода, состоящей из команд и других синтаксических компонентов и определяющей содержание некоторой самостоятельной операции в составе программы (класс, функция, процедура, подпрограмма). Отдельная функциональная задача – функциональный компонент программы, представляющий собой систему взаимосвязанных по входным и выходным данным ФО, исполнение которой обеспечивает решение некоторой задачи пользователя или вычислительной системы при работе с программой. Последовательное решение ОФЗ образует вычислительный процесс, существующий уже во временной области.

Вероятность безотказной работы ПС $P_{пс}$ за время выполнения ФО $\tau_{\text{фо}}$, таким образом, определяется через ВОО на участке $\Delta C_{\text{фо}}$:

$$P_{\text{пс}}(\tau_{\text{фо}}) = P(\Delta C_{\text{фо}}) = \exp\left(-\frac{\Delta C_{\text{фо}}}{\Delta C_{\text{оо}}}\right)$$

Функциональные операции, составляющие программу, могут выполняться последовательно или параллельно, что эквивалентно последовательному или параллельному «соединению» R элементов i-го программного средства, каждый из которых имеет надёжность P_r. Порядок и последовательность выполнения ФО при решении η-й ОФЗ являются детерминированными, а положительный или отрицательный исход их выполнения – вероятностным, следовательно, для ОФЗ и для ПС в целом можно составить логико-вероятностную модель надёжности в виде схемы функциональной целостности.

Такая модель учитывает не только вид «соединения» ФО, но и наличие временного (повторное выполнение ФО) или логического (альтернативные маршруты решения ОФЗ) резервирования, т. е. структурную и функциональную сложность ПС. Временное резервирование задаётся в форме вершин СФЦ, физической характеристикой которых является период выполнения соответствующей ОФЗ $\tau_{\text{ОФЗ}\eta}$, а вероятностной – вероятность выполнения ОФЗ за требуемое время; при этом число временных вершин, связанных логикой ИЛИ, определяет количество попыток повторного решения ОФЗ. Резерв времени, в свою очередь, необходим для реализации встроенного диагностирования и самовосстановления ПС. Важно отметить, что структура данной модели, а значит и надёжность ПС, является динамической характеристикой.

Результирующее выражение в обобщённой форме для вероятности безотказной работы программного средства за время выполнения N ОФЗ будет выглядеть следующим образом:

$$P_{\text{пс}i}(\tau_{N\text{офз}}) = \prod_{n=1}^{N}\sum_{m=1}^{M}\left(\pm\prod_{r=1}^{R}P_r(\Delta C_{\text{фо}})\right)_m$$

Выражение представляет собой вероятностную функцию надёжности, которая выводится на основе ЛВМ анализируемого ПС по правилам логико-вероятностного метода.

Разработка модели (набора моделей) надёжности ПС в виде СФЦ должна осуществляться в ходе надёжностного проектирования ПС на этапе разработки алгоритмов различных уровней и составления структурно-функциональной схемы ПС. В дальнейшем, по результатам кодирования алгоритмов, автономной и комплексной отладки ПС модель подлежит уточнению с целью формирования априорных данных для этапа эксплуатации.

Изложенный подход к оцениванию показателей надёжности ПС базируется на априорных данных по результатам тестирования, отладки и приработки как отдельных ФО, модулей и подпрограмм ПС, так и ПС в целом. Эти данные представляются в виде моделей априорного распределения ошибок в программах и базах данных, а также интенсивностей использования ФО, модулей и подпрограмм в ходе выполнения пользовательских (системных) задач при работе ПС. В ходе нормальной эксплуатации посредством СТД АПК осуществляется оперативный контроль, оценивание и уточнение показателей надёжности функционирования ПС. Работа СТД в части контроля надёжности ПС основывается на следующих составляющих [7]:

- контроль и статистический анализ определяющих параметров функционирования ПС (скорость обработки запросов, загрузка ОЗУ и ЦП, интенсивность событий отказов и сбоев, места проявления ошибок в программном коде и др.);
- встроенные упреждающие процедуры (контроль корректности входных и выходных данных, контрольные суммы элементов ПС, составление и анализ рейтинга надёжности исполняемых ФО, модулей и подпрограмм, предварительная эмуляция выполнения ФО с целью оценки их надёжности, использование тестовых задач и контрольных примеров, использование временного и логического резервирования и др.).

Необходимость встроенных упреждающих алгоритмов обусловливается трудностью (или практической невозможностью) достоверного прогнозирования надёжности ПС, т. к. последняя не имеет явно выраженной временной закономерности.

Подсистема встроенного диагностирования ПС реализуется за счёт временного и логического резервирования ФО. Процесс диагностирования ПС основан на апостериорном оценивании фактического уровня надёжности ПС и специальных процедурах выполнения программы, учитывающих этот уровень:

- немедленное выполнение ОФЗ при высоком уровне надёжности;
- предварительный тест ОФЗ при среднем уровне надёжности;
- предварительная эмуляция выполнения ОФЗ при низком уровне надёжности или отсутствии данных о надёжности.

Кроме того, в качестве определяющих параметров аппаратуры вычислительных устройств, оказывающих непосредственное влияние на надёжность программных средств, выступают следующие:

- использование оперативной памяти;
- использование ресурсов ЦП;
- скорость выполнения операции;
- скорость информационного обмена между элементами вычислительного комплекса и между вычислительными устройствами и ряд других.

Одним из основных путей повышения надёжности систем является введение избыточности (структурной, функциональной, временной, нагрузочной, информационной). В случае ПО наибольшее применение находит временная избыточность, что объясняется особенностями программ с точки зрения их надёжностного поведения. Резерв времени необходимо использовать для технического диагностирования, парирования отказов и восстановления работоспособности ПО.

IV. Заключение

Таким образом, на основе структурной схемы РЭС составляется модель надёжности её функционирования. Для каждого из обобщённых режимов функционирования РЭС составляется логико-вероятностная функциональная модель, которая позволяет вычислить вероятность безотказного функционирования РЭС за время задействования данного режима. Элементами модели выступают структурные элементы РЭС (подсистемы, блоки, полукомплекты), используемые при реализации заданного режима функционирования и соединённые, исходя из надёжности функционирования РЭС.

Вероятностные параметры элементов ЛВФМ рассчитываются на основе статистических данных технического диагностирования подсистем и блоков РЭС (в соответствующем диагностическом режиме). При этом, шаг расчёта соответствует дискретным моментам времени циклов диагностирования. В рамках исследования (при отсутствии достаточного количества реальных статистических данных технического диагностирования или при наличии статистики эксплуатационных событий) осуществляется имитационное моделирование (марковское или логико-статистическое) случайных процессов изменения технического состояния подсистем и блоков РЭС.

С использованием модели может быть осуществлён расчёт временного ряда значений функции технического использования и проведено её прогнозирование, определён период проведения технического обслуживания, рассчитаны коэффициенты технического использования при использовании календарной и смешанной стратегии технического обслуживания РЭС.

Список литературы

[1] Эксплуатация космических средств: учебник / под ред. А.П. Вышинского. СПб.: ВКА имени А.Ф. Можайского, 2015. 477 с.

[2] Петухов Г.Б., Якунин В.И. Методологические основы внешнего проектирования целенаправленных процессов и целеустремлённых систем. М: АСТ, 2006. 504 с.

[3] Викторова В.С., Степанянц А.С. Модели и методы расчёта надёжности технических систем. М.: ЛЕНАРД, 2016. 256 с.

[4] Гладкова И.А., Можаев А.С., Мусаев А.А. Метод логикодетерминированного моделирования сетевых систем // Известия СПбГТИ. СПб.: СПбГТИ, 2012. Вып.14(40). С. 89–92.

[5] Можаев А.С. Общий логико-вероятностный метод анализа надежности структурно-сложных систем: учебное пособие. Л.: ВМА, 1988. 68 с.

[6] Мусаев А.А., Гладкова И.А. Современное состояние и направления развития общего логико-вероятностного метода анализа систем: тр. СПИИРАН, Отделение нанотехнологий и информацион РАН. СПб.: Анатолия, 2010. Вып.1(12). С. 75–96.