УДК 681.51:629.78

Калентьев А.А., Тюгашев А.А.

МЕТОДОЛОГИЯ ПРОЕКТИРОВАНИЯ НАДЕЖНЫХ АЛГОРИТМОВ УПРАВЛЕНИЯ ДЛЯ КОСМИЧЕСКИХ АППАРАТОВ

При создании космической техники, в силу таких обстоятельств, как уникальность устанавливаемой на их борту аппаратуры, высокая стоимость и т.д., вопросы обеспечения надежности встают особенно остро. Цена ошибки в управляющем программном обеспечении (ПО) является неприемлемо высокой. В случае пилотируемой экспедиции сбой в системе управления космического аппарата (КА) может привести к гибели людей.

Вместе с тем специфика борта накладывает наиболее жесткие среди всех движущихся объектов ограничения на располагаемые ресурсы вычислительных средств. Удовлетворение требований возможно лишь при условии всестороннего анализа функциональных особенностей бортовых подсистем, глубокой оптимизации разработок.

При этом устранение ошибки в ПО на этапе эксплуатации КА затруднено, а в ряде случаев и невозможно [1]. Внесение изменений в программу бортовой вычислительной системы (БВС), например, по радиоканалу, связано, как правило, с остановкой нормального функционирования бортовой аппаратуры (БА) КА.

Широко применяемой и апробированной методикой обеспечения надежности является тестирование программ. Существуют различные подходы к тестированию, и принципиально его можно разделить на тестирование по методу "черного ящика", когда при тестировании не вдаются во внутреннюю структуру программы, и метод "белого ящика", когда во внимание принимается внутренняя структура программы с имеющимися проверками условий, циклами и маршрутами выполнения. Однако проверить действительно *все* возможные варианты исполнения при достаточно сложной схеме программы и количестве логических условий в ней, равно как и правильность исполнения программы на *всех* возможных комбинациях исходных данных, практически невозможно. Таким образом, даже полностью успешное тестирование на некотором подмножестве вариантов исполнения управляющего алгоритма (УА) и на некотором подмножестве возможных исходных данных (ИД) не дает полной гарантии того, что программа правильная.

Более того, в случае управляющего алгоритма реального времени проблема качественно усложняется тем фактором, что алгоритм взаимодействует с непредсказуемой внешней средой, изменения в которой могут происходить в произвольные моменты времени, и необходимо вводить время как важную составляющую набора исходных данных.

Поэтому выглядит весьма привлекательным и практически полезным поиск методов формального доказательства правильности программ, а также, возможно, методологии проектирования гарантированно правильных программ или хотя бы частичного повышения качества и надежности при ее проектировании.

Как правило, ценность алгоритма определяется результатом, который получается по окончании его работы. Под результатом подразумевается некоторый набор выходных данных, полученных в результате обработки поданных на вход ИД. А состояния программы (алгоритма), как начальное и конечное, так и промежуточные, определяются как совокупность значений имеющейся программной памяти. Например, известна общая формализация понятия программы, исходящая из формулировки так называемых постусловий и предусловий [2]. Данные условия есть часть языка *алгоритмических логик*, включающая условия вида

$$\{U\}\ S\ \{B\},$$

читающиеся следующим образом: "**U** – условие, относящееся к исходным данным программы S, истинное до ее выполнения. **B** – условие, относящееся к выходным данным программы S, которое должно быть истинным после ее исполнения".

Данный подход не может быть без модификации применен для случая управляющих алгоритмов реального времени, поскольку в них важным условием правильности является осуществление корректного управления БА на всем промежутке времени активного существования КА. Более того, для данного случая вообще не применим без внесения соответствующих поправок классический подход к алгоритму как к набору действий для получения в конце его работы определенного результата. Управляющий алгоритм должен обеспечивать на некотором непустом множестве временных меток ("включений") выполнение определенных действий по управлению КА, зависящих от текущей ситуации на борту, отражаемой вектором значений логических переменных. Применимой представляется предлагаемая семантика УА реального времени (РВ) в виде набора четверок

$$\text{УА РВ} = \{ \langle f_i, t_i, \tau_i, l_i \rangle, i \in N \}$$

где f_i – функциональная программа (действие), t_i – момент начала исполнения действия, τ_i – длительность действия, l_i – логический вектор, обуславливающий действие.

Вообще, с точки зрения правильности работы УА РВ, его корректность может глобально быть определена как исполнение КА и управляемым комплексом управляющих программ БВС его целевой задачи или в обозначениях пред- и постусловий:

$$\{ U (D_0,t_0) \} YS \{ B (D_k (t_1,t_2,\ldots t_k), t_k) \},$$

то есть в момент времени начала функционирования КА t_0 истинно условие корректного задания исходных данных D_0, а к моменту завершения работы t_k управляющего алгоритма YS истинно условие D_k, означающее успешную отработку всех целевых задач на всех заданных моментах времени $t_1,t_2,\ldots t_k$ на протяжении времени активного существования управляемого КА.

Управляющие алгоритмы реального времени, отвечающие за качественное выполнение бортовой аппаратурой своих функций в рамках программы полета, являются сложной технической системой, а их проектирование – сложной инженерно-технической задачей. На принципе разбиения сложной задачи на более простые основана технология ГРАФКОНТ проектирования качественных и надежных алгоритмов управления реального времени, координирующих согласованную работу БА при комплексном функционировании.

Основная идея заключается в постепенном конструировании УА из априори надежных блоков – более простых программ управления "базового" уровня – так называемых функциональных программ. Если при этом обеспечивается правильность алгоритма конструирования, т.е. соединения функциональных программ (ФП) в единое целое, то можно предполагать высокое качество и надежность получаемого в результате управляющего алгоритма.

Технология ГРАФКОНТ поддерживается специально разработанной программной системой, функционирующей на платформе Windows 95/98/2000/XP. При этом на входе системы проектировщик, исходя из материалов по логике управления, которую должен реализовать алгоритм, осуществляет интерактивное "конструирование" визуального образа в соответствующей графической подсистеме. Выходными данными системы являются техническая документация на УА РВ, требуемая согласно принятой на предприятии-заказчике системе – временная диаграмма управляющего алгоритма и блок-схема программы, а также собственно текст управляющей программы на языке автокода бортовой ЦВМ, реализующей УА РВ.

На протяжении длительного времени на предприятии-заказчике (Государственный научно-производственный ракетно-космический центр «ЦСКБ-Прогресс», г.Самара) выработана методика поэтапной отладки управляющих программ на специальном наземном отладочном моделирующем комплексе, в который входят ЭВМ, эмулирующие БВС и моделирующие

внешние воздействия космического пространства и другие факторы [1]. Отладка включает автономную отладку и комплексную отладку.

При этом для каждой управляющей программы на специальном символьном языке отладки составляется отладочное задание, в которое входит перечень отслеживаемых по значению переменных, необходимых точек останова и т.п.

Созданная на основе работ по проекту ГРАФКОНТ система автоматизированной генерации отладочных заданий ГЕОЗ позволяет на основе внутренних структур данных программного комплекса ГРАФКОНТ автоматически формировать отладочное задание на автономную отладку управляющего алгоритма.

Важными задачами при проведении отладки управляющих алгоритмов реального времени являются автоматизированное выявление всех возможных вариантов исполнения («маршрутов») алгоритма в зависимости от значений компонент вектора логических переменных, а также выявление всех имеющихся в алгоритме информационных и управляющих связей с другими управляющими программами. Эти задачи также решаются в рамках программной системы ГЕОЗ.

В перспективе на основе внутренних системных данных комплекса ГРАФКОНТ-ГЕОЗ планируется автоматически получать временные характеристики выполнения проектируемых управляющих программ для различных логических вариантов исполнения, а также перейти к автоматизации комплексной отладки.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Управление космическими аппаратами зондирования Земли. Компьютерные технологии. // Д.И. Козлов, Г.П. Аншаков, Я.А. Мостовой, А.В. Соллогуб. - М.: Машиностроение, 1998.
2. Логика и компьютер. Моделирование рассуждений и проверка правильности программ. // А.М. Анисов, П.И. Быстров, В.А. Смирнов и др. М.: Наука, 1990.